Asian
Quantum
Information
Science Conference **2019**

Abstract Booklet

TALK

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

Hosted by KIAS (Korea Institute for Advanced Study)

Edited by Shigeru Yamashita and Seung-Woo Lee

PREFACE

These proceedings contain abstracts for the tutorials, talks and posters of the 2019 Asian Quantum Information Science conference, AQIS'19, being held at Korea Institute for Advanced Study, Korea, 19-23 August 2019.

AQIS, the successor to the EQIS conferences held in Japan from 2001-2005, is widely regarded as the foremost Asian conference series covering all aspects of the burgeoning cross-disciplinary field of quantum information science. This includes theoretical and experimental research in all of the following areas: quantum computation and simulation, from programming semantics to gate design; quantum-inspired classical computation and simulation; quantum cryptography, communication, and more general network tasks; device characterisation and decoherence mitigation; quantum information science more broadly; and research influenced by quantum information in related fields such as quantum foundations, quantum metrology, many-body quantum (thermo)dynamics, and quantum space-time.

Though located in Asia, the reach of AQIS is cosmopolitan, serving to foster exchange of methods and experiences and development of the field both in Asia and around the world. Last year's conference at Nagoya University was the largest AQIS ever, and this year's is almost as large. Next year it will be held for the first time in Sydney, Australia, a country on the edge of Asia which is becoming increasingly part of the Asian community in quantum information science.

This year's program comprises 10 invited talks (including the 2 tutorials), 52 contributed talks, and 130 posters. There were 212 submission, only 7% fewer than the record-breaking 2018 conference in Japan. Of these, 162 requested a talk, so the work of the Program Committee was highly selective, with the acceptance rates for talks being 32%. The abstracts selected are of excellent quality and cover a very broad range of topics. The assessment was done by an international Program Committee, chaired by Howard Wiseman, with co-chairs Runyao Duan and Eleanor Rieffel, and comprising Koji Azuma, Kristin Beck, Mario Berta, Michael Bremner, Daniel Burgarth, Areeya Chantasri, Yu Chen, Giulio Chiribella, Oscar Dahlsten, Usha Devi, Daoyi Dong, Omar Fawzi, Marissa Giustina, Mile Gu, Qiongyi He, Itay Hen, Richard Jozsa, Elham Kashefi, Kihwan Kim, Myungshik Kim, Aleks Kissinger, Ping-Koy Lam, Troy Lee, Chuan-Feng Li, Yeong-Cherng Liang, Nana Liu, Xiongfeng Ma, Aikaterini Mandilara, Peter McMahon, Tomoyuki Morimae, Milan Mosonyi, Yasunobu Nakamura, Yoshifumi Nakata, Hidetoshi Nishimori, Sergei Novikov, Kevin O'Brien, Francis Paraan, Stephen Piddock, Ravi Ramanathan, Jacqui Romero, Barry Sanders, Eyob Sete, Urbasi Sinha, Wonmin Son, Nora Tischler, Xin Wang, Zhihui Wang, Paul Warburton, Nathan Wiebe, Andreas Winter, Rebing Wu, Guoyong Xiang, Yanhong Xiao, Peng Xue, and Naoki Yamamoto.

We would like to thank the Program Committee members, the invited speakers, and everyone who submitted an abstract in response to the call for papers. We would also like to thank the conference Steering Committee, chaired by Jaewan Kim, especially its secretary, Shigeru Yamashita, and the Organizing Committee, also chaired by Jaewan Kim.

— Howard Wiseman (PC chair), Runyao Duan (PC co-chair), and Eleanor Rieffel (PC co-chair).

Program Committee

Howard Wiseman (Griffith U, Chair)
Runyao Duan (Baidu/U Tech Sydney, Co-Chair)
Eleanor Rieffel (NASA, Co-Chair)
Koji Azuma (NTT)
Kristin Beck (IonQ)
Mario Berta (Imperial College London)
Michael Bremner (U of Technology Sydney)
Daniel Burgarth (Macquarie U)
Areeya Chantasri (Griffith U)
Yu Chen (Google)
Giulio Chiribella (HKU)
Oscar Dahlsten (Sustech)
Usha Devi (Bangalore U)
Daoyi Dong (UNSW)
Omar Fawzi (École Normale Supérieure de Lyon)
Marissa Giustina (Google)
Mile Gu (NTU)
Qiongyi He (Peking U)
Itay Hen (ISI)
Richard Jozsa (U of Cambridge)
Elham Kashefi (U of Edinburgh)
Kihwan Kim (Tsinghua U)
Myungshik Kim (Imperial College London)
Aleks Kissinger (Radboud U)
Ping-Koy Lam (ANU)
Troy Lee (UTS)
Chuan-Feng Li (USTC)
Yeong-Cherng Liang (National Cheng Kung U)
Nana Liu (CQT)
Xiongfeng Ma (Tsinghua U)
Aikaterini Mandilara (Nazarbayev U)
Peter McMahon (Cornell/Stanford)
Tomoyuki Morimae (YITP)
Milan Mosonyi (Budapest U of Technology and Economics)
Yasunobu Nakamura (U of Tokyo)
Yoshifumi Nakata (Kyoto University)
Hidetoshi Nishimori (Tokyo Institute of Technology)
Sergei Novikov (Northrop Grumman)
Kevin O'Brien (MIT)
Francis Paraan (U of the Philippines)
Stephen Piddock (U of Bristol)
Ravi Ramanathan (HKU)

Jacqui Romero (U of Queensland)
Barry Sanders (U of Calgary)
Eyob Sete (Rigetti)
Urbasi Sinha (RRI)
Wonmin Son (Sogang University)
Nora Tischler (Griffith U)
Xin Wang (U of Maryland)
Zhihui Wang (NASA)
Paul Warburton (UCL)
Nathan Wiebe (U of Washington)
Andreas Winter (UAB)
Rebing Wu (Tsinghua U)
Guoyong Xiang (USTC)
Yanhong Xiao (Fudan U)
Peng Xue (Beijing CSRC)
Naoki Yamamoto (Keio U)

Steering Committee

Charles BENNETT (IBM)
Jozef GRUSKA (Masaryk U)
Guang-Can GUO (USTC)
Hiroshi IMAI (U Tokyo, ex-Chair)
Richard JOZSA (U Cambridge)
Jaewan KIM (KIAS, Chair)
Shigeru YAMASHITA (Ritsumeikan U, Secretary)

Organizing Committee

Jaewan KIM (KIAS, Chair)
Seung-Woo LEE (KIAS)
Jeongho BANG (KIAS)
Arijit DUTTA (KIAS)
Adel SOHBI (KIAS)
Jaehak LEE (KIAS)
June-Koo Kevin Rhee (KAIST)
Hye Mi Kim (KIAS, Secretary)

PROGRAM

Oral Presentations

August 19, 2019 (Mon.)

[Tutorial]

[Tutorial]

[Invited Talk]

[Long Talks]

August 20, 2019 (Tue.)

[Invited Talk]

[Long Talks]

[Short Talks (Parallel session A)]

[Short Talks (Parallel session B)]

[Short Talks (Parallel session A)]

[Short Talks (Parallel session B)]

August 21, 2019 (Wed.)

[Invited Talk]

[Invited Talk]

August 22, 2019 (Thr.)

[Invited Talk]

[Long Talks]

[Short Talks (Parallel session A)]

[Short Talks (Parallel session B)]

[Short Talks (Parallel session A)]

[Short Talks (Parallel session B)]

August 23, 2019 (Fri.)

Embezzlement and Applications

Debbie Leung

Abstract. Embezzlement of entanglement is the (impossible) task of producing an entangled state from a product state via a local change of basis, when a suitable *catalytic* entangled state is available. The possibility to approximate this task was first observed by van Dam and Hayden in 2002. Since then, the phenomenon is found to play crucial roles in many aspects of quantum information theory. In this tutorial, we will explore various methods to embezzle and discuss applications (such as an extension to approximately violate other conservation laws in macroscopically controlled unitary gates, a Bell inequality that cannot be violated maximally with finite amount of entanglement, and the quantum reverse Shannon theorem).

References

[1] Wim van Dam and Patrick Hayden. Universal entanglement transformations without communication. Physical Review A, 67(6):060302, 2003. quant-ph/0201041 https://arxiv.org/abs/quant-ph/0201041

[2] Debbie Leung, Ben Toner, and John Watrous. Coherent state exchange in multi-prover quantum interactive proof systems. Chicago Journal of Theoretical Computer Science, 11:118, 2013. arXiv:0804.4118 https://arxiv.org/abs/0804.4118

[3] Zhengfeng Ji, Debbie Leung, Thomas Vidick. A three-player coherent state embezzlement game. arXiv:1802.04926 https://arxiv.org/abs/1802.04926

[4] Andrea Coladangelo. A two-player dimension witness based on embezzlement, and an elementary proof of the non-closure of the set of quantum correlations. arXiv:1904.02350 https://arxiv.org/abs/1904.02350

Introduction to Quantum Machine Learning

Nathan Wiebe

Abstract. In recent years, quantum machine learning has emerged as one of the most exciting potential applications of quantum computing. This tutorial aims to provide an introduction to machine quantum machine learning that will allow the attendees to understand the goals of machine learning, the promises of the field and the challenges that remain in the field. We will begin with an introduction to machine learning including neural networks, support vector machines and nearest neighbor classification. Next, we will discuss how quantum computing can impact these areas and discuss the different forms of access models that are needed for the data in order to make such algorithms practical. Finally, we will provide a discussion of how to train quantum Boltzmann machines using quantum computers and argue that such quantum neural networks may have a valuable role in characterizing and preparing broad families of quantum states.

References

[1] Biamonte, Jacob, et al. "Quantum machine learning." Nature 549.7671 (2017): 195.

[2] Rebentrost, Patrick, Masoud Mohseni, and Seth Lloyd. "Quantum support vector machine for big data classification." Physical review letters 113.13 (2014): 130503.

[3] Wiebe, Nathan, Ashish Kapoor, and Krysta M. Svore. "Quantum nearest-neighbor algorithms for machine learning." Quantum Information and Computation 15 (2018).

[4] Kieferov, Mria, and Nathan Wiebe. "Tomography and generative training with quantum Boltzmann machines." Physical Review A 96.6 (2017): 062327.

Testing quantum causal structures

Giulio Chiribella

Abstract. Identifying cause-effect relations is a fundamental primitive in a variety of areas. The identification of causal relations is generally accomplished through statistical trials where alternative hypotheses about the causal relations are tested against each other. Traditionally, such trials have been based on classical statistics. However, classical statistics becomes inadequate at the quantum scale, where a richer spectrum of causal relations is accessible. In this talk, I will show that quantum strategies can greatly speed up the identification of causal relations. As a working example, I will analyse the task of iden-tifying the effect of a given variable, and show that the optimal quantum strategy beatsall classical strategies by running multiple equivalent tests in a quantum superposition.The same working principle leads to advantages in the detection of a causal link between two variables, and in the identification of the cause of a given variable. These results open up the study of quantum speedups in causal discovery algorithms, and may have applications to the design of automated quantum machines and new quantum communication protocols. Reference for this work: G Chiribella and D Ebler, Nature Communications 10, 1472 (2019).

Efficiently computable bounds for magic-state distillation

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. Magic state manipulation is a crucial component in the leading approaches to realizing scalable, fault-tolerant, and universal quantum computation. Related to magic state manipulation is the resource theory of magic states, for which one of the goals is to characterize and quantify quantum "magic." In this paper, we introduce the family of thauma measures to quantify the amount of magic in a quantum state, and we exploit this family of measures to address several open questions in the resource theory of magic states. As a first application, we use the min-thauma to bound the regularized relative entropy of magic. As a consequence of this bound, we find that two classes of states with maximal mana, a previously established magic measure, cannot be interconverted in the asymptotic regime at a rate equal to one. This result resolves a basic question in the resource theory of magic states and reveals a fundamental difference between the resource theory of magic states and other resource theories such as entanglement and coherence. As a second application, we establish the hypothesis testing thauma as an efficiently computable benchmark for the one-shot distillable magic, which in turn leads to a variety of bounds on the rate at which magic can be distilled, as well as on the overhead of magic-state distillation. Finally, we prove that the max-thauma can outperform mana in benchmarking the efficiency of magic-state distillation.

Keywords: Magic state distillation, fault-tolerant quantum computing, resource theory

1 Introduction

Quantum computers hold the promise of a substantial speed-up over classical computers for solving certain algebraic problems [1, 2] and simulating quantum dynamics [3]. One of the main obstacles to the physical realization of quantum computation is the decoherence that occurs during the execution of quantum algorithms. Fault-tolerant quantum computation (FTQC) [4, 5] provides a framework to overcome this difficulty and allows reliable quantum computation when the physical error rate is below a certain threshold value.

According to the Gottesman–Knill theorem [6, 7], a quantum circuit comprised of only Clifford gates confers no quantum computational advantage because it can be simulated efficiently on a classical computer. However, the addition of a so-called *magic state* can lead to a universal gate set via a technique called state injection [8, 9], thus achieving universal quantum computation. The key of this resolution is to perform *magic-state distillation* [10] (see [11, 12, 13, 14, 15, 16, 17] for recent progress), wherein stabilizer operations are used to transform a large number of noisy magic states into a smaller number of high quality magic states. Therefore, a quantitative theory is highly desirable in order to fully exploit the power of magic states in fault-tolerant quantum computation.

Quantum resource theories (QRTs) offer a powerful framework for studying different phenomena in quantum physics, and the seminal ideas of QRTs have recently been influencing diverse areas of physics [18]. In the context of the magic-state model of universal quantum computation, the resource-theoretic approach reduces to the characterization and quantification of the usefulness of the resourceful magic states [19, 20]. In the framework of [19, 20], the free operations are the stabilizer operations, those that possess a fault-tolerant implementation in the context of fault-tolerant quantum computation, and the free states are the stabilizer states (STAB). Stabilizer operations include preparation and measurement in the computational basis, as well as a restricted set of unitary operations, called the Clifford unitaries. The free states consist of all pure stabilizer states, which are eigenstates of the generalized Pauli operators, and their convex mixtures. The resource states, namely, the magic states (or non-stabilizer states), are key resources that are required to achieve some desired computational tasks. For quantum computers acting on qudit registers with odd dimension d, the resource theory of magic states (or equivalently contextuality with respect to stabilizer measurements [21, 22]) has been developed [19, 23, 20]. The resource theory of magic states for multiqubit systems was recently developed in [24, 25, 26].

2 Overview of results

In this work, we develop resource-theoretic approaches to study the non-stabilizer resources in fault-tolerant quantum computation. In particular, we establish the following:

(i) We introduce the family of thauma[1] measures to quantify the amount of magic in a quantum state, several of which can be efficiently computed via convex optimization.

(ii) We show that two classes of states with maximal mana, a previously established magic measure, cannot be interconverted asymptotically at a rate equal to one. This resolves an open question in [20] and reveals the difference between the resource theory of magic states and other resource theories.

This submission is based on arXiv:1812.10145.

[1] Greek for "wonder" or "marvel"

(iii) We establish efficiently computable benchmarks for the rate and efficiency of magic-state distillation via thauma measures and quantum hypothesis testing.

3 Background

We now recall the definition of the discrete Wigner function, which is essential in the analysis of the resource theory of magic states. Let $\mathcal{H}_d$ be a Hilbert space of dimension d, and let $\{|j\rangle\}_{j=0,\ldots,d-1}$ denote the standard computational basis. For a prime number d, we define the respective shift and boost operators $X, Z \in \mathcal{L}(\mathcal{H}_d)$ as $X|j\rangle = |j \oplus 1\rangle$ and $Z|j\rangle = \omega^j|j\rangle$, with $\omega = e^{2\pi i/d}$. We define the Heisenberg–Weyl operators as $T_{\mathbf{u}} = \tau^{-a_1 a_2} Z^{a_1} X^{a_2}$, where $\tau = e^{(d+1)\pi i/d}$ and $\mathbf{u} = (a_1, a_2) \in \mathbb{Z}_d \times \mathbb{Z}_d$. For each point $\mathbf{u}$ in the discrete phase space, there is a corresponding operator $A_{\mathbf{u}}$, and the value of the discrete Wigner representation of a quantum state ρ at this point is given by

$$W_\rho(\mathbf{u}) := \operatorname{Tr} A_{\mathbf{u}} \rho / d,$$

where $\{A_{\mathbf{u}}\}_{\mathbf{u}}$ are the phase-space point operators $A_{\mathbf{u}} := T_{\mathbf{u}} A_0 T_{\mathbf{u}}^\dagger$ and $A_0 := \frac{1}{d} \sum_{\mathbf{u}} T_{\mathbf{u}}$.

4 Main results

4.1 Thauma measures for magic states

It is well known that quantum computations are classically simulable if they consist of only stabilizer operations acting on quantum states with a positive discrete Wigner function. Such states are thus useless for magic-state distillation [19] and are analogous to states with a positive partial transpose in entanglement theory. To address fundamental questions in the resource theory of magic states, we are motivated by the idea of the Rains bound from entanglement theory [27]. As developed in [27] and the later work [28], the Rains bound and its variants consider sub-normalized states with non-positive logarithmic negativity [29, 30] as useless resources, and they use the divergence between the given state and such sub-normalized states to evaluate the behavior of entanglement distillation. Thus, inspired by the main idea behind the Rains bound, we introduce the set of sub-normalized states with non-positive mana: $\mathcal{W} := \{\sigma : \mathcal{M}(\sigma) \leq 0,\ \sigma \geq 0\}$, with the mana $\mathcal{M}(\rho)$ of a quantum state ρ defined as [20] $\mathcal{M}(\rho) := \log_2 \|\rho\|_{W,1}$, where the Wigner trace norm of an operator V is defined as $\|V\|_{W,1} := \sum_{\mathbf{u}} |W_V(\mathbf{u})|$. Note that the mana [20] is analogous to the logarithmic negativity [29, 30].

Our *first contribution* is to introduce the family of *thauma* measures to quantify the magic of a state:

Measures	Acronym	Definition
Max-thauma	$\theta_{\max}(\rho)$	$\inf_{\sigma\in\mathcal{W}} D_{\max}(\rho\|\sigma)$
Thauma	$\theta(\rho)$	$\inf_{\sigma\in\mathcal{W}} D(\rho\|\sigma)$
Regularized Thauma	$\theta^\infty(\rho)$	$\lim_{n\to\infty} \theta(\rho^{\otimes n})/n$
Min-thauma	$\theta_{\min}(\rho)$	$\inf_{\sigma\in\mathcal{W}} D_0(\rho\|\sigma)$

We prove that these two members of the thauma family are efficiently computable by semidefinite programs (SDPs) [31] and are particularly useful for addressing fundamental questions in the resource theory of magic states. In particular, we prove that the min- and max-thauma are additive wtih respect to tensor-product states. Additionally, for any pure state $|\psi\rangle$, $\theta_{\min}(\psi) = -\log_2 \max_{\sigma\in\mathcal{W}} F(\psi,\sigma) \leq -\log_2 F_{\text{Stab}}(\psi)$, where $F_{\text{Stab}}(\psi)$ is the stabilizer fidelity [32]. In the following sections, we demonstrate applications of thauma in magic-state conversion and magic-state distillation.

4.2 Inequivalence between magic states with maximal mana

A fundamental problem in any quantum resource theory is to determine whether the resource conversion is asymptotically reversible under the free operations [18]. For example, in bipartite entanglement theory, the maximally entangled state $|\Phi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is a natural choice for a standard resource, and the asymptotic interconversion between Φ and any pure bipartite state is reversible under local operations and classical communication [33].

In any resource theory, maximally resourceful states play a unique role in quantifying the resourcefulness of other states and accessing the performance of resource manipulation. Considering entanglement theory (or coherence theory) as an example, the interconversion between a given state and maximally entangled (coherent) states leads to fundamental tasks such as entanglement (coherence) distillation and dilution. Notably, any two maximally entangled (coherent) states in the same dimension are equivalent under free operations.

However, our *first main result* shows that this is not the case in the resource theory of non-stabilizer states. Surprisingly, we find that even though the Strange state and the Norrell state [20] each have maximum mana and are thus the most costly resource to simulate on a classical computer [20, 34], they are not equivalent even in the asymptotic regime. In particular, recall that mana is a non-stabilizerness measure analogous to logarithmic negativity, and the logarithmic negativity of a bipartite state is equal to its maximal value if and only if the state is maximally entangled.

Solving the asymptotic transformation rate between states is usually very difficult. However, here we utilize the thauma measures to show that the following inequality holds for the Strange state $|\mathbb{S}\rangle$ and the Norrell state $|\mathbb{N}\rangle$:

$$R(\mathbb{N} \to \mathbb{S}) \leq \log_2(3/2)/\log_2(5/3) < 1.$$

This result demonstrates a fundamental difference between the resource theory of non-stabilizer states and the resource theory of entanglement or coherence. Specifically, we show that the maximally resourceful non-stabilizer states cannot be interconverted at a rate equal to one, even in the asymptotic regime, while the maximally resourceful states in entanglement theory or coherence theory can be interconverted equivalently in the single-copy setting.

4.3 Limits for magic-state distillation

The basic task of magic-state distillation [10] can be understood as follows. For any given quantum state ρ, we aim to transform this state to a collection of magic states (e.g., $|T\rangle$) with high fidelity using stabilizer operations. The goal is to maximize the number of target states while keeping the transformation infidelity within some tolerance ε.

Figure 1: Magic state distillation.

Our *second main result* gives the fundamental limit for magic-state distillation of a given pure target magic state. In a realistic setting, the resources are finite, the number of independent and identically distributed (i.i.d.) prepared states is limited. Therefore, it is important to characterize how well we can distill magic states from a finite number of copies of prepared states. In the non-asymptotic setting, one has to make a trade-off between the distillation rate and infidelity tolerance. Formally, for any triplet $(\rho, \phi, \varepsilon)$ consisting of a given initial state ρ, a target pure state ϕ, and an infidelity tolerance ε, the one-shot ε-error distillable ϕ-magic of ρ, denoted by $\mathcal{M}^{\varepsilon}_{\phi}(\rho)$, is defined to be the maximum number of ϕ magic states achievable via stabilizer operations, with an error tolerance of ε:

$$\mathcal{M}^{\varepsilon}_{\phi}(\rho) = \sup\{k : \Lambda(\rho) \approx_{\varepsilon} |\phi\rangle\langle\phi|^{\otimes k},\ \Lambda \in \mathrm{SO}\},$$

where $|\psi\rangle\langle\psi| \approx_{\varepsilon} \sigma$ is a shorthand for $\langle\psi|\sigma|\psi\rangle \geq 1-\varepsilon$ and SO for stabilizer operations.

There are certain qutrit magic states of interest [35, 36]: $|T\rangle = \frac{1}{\sqrt{3}}(\xi|0\rangle + |1\rangle + \xi^{-1}|2\rangle)$ with $\xi = e^{2\pi i/9}$ and the eigenstate $|H_+\rangle$ of the qutrit Hardmard gate with corresponding eigenvalue 1. Here we focus on the one-shot distillable H_+-magic $\mathcal{M}^{\varepsilon}_{H_+}(\rho)$ and the one-shot distillable T-magic $\mathcal{M}^{\varepsilon}_{T}(\rho)$. We establish the following upper bounds:

$$\mathcal{M}^{\varepsilon}_{H_+}(\rho) \leq \frac{\min_{\sigma\in\mathcal{W}} D^{\varepsilon}_{H}(\rho\|\sigma)}{\log_2(3-\sqrt{3})}, \tag{1}$$

$$\mathcal{M}^{\varepsilon}_{T}(\rho) \leq \frac{\min_{\sigma\in\mathcal{W}} D^{\varepsilon}_{H}(\rho\|\sigma)}{\log_2(1+2\sin(\pi/18))}, \tag{2}$$

where $D^{\varepsilon}_{H}(\rho_0\|\rho_1) := -\log_2 \min\left\{\mathrm{Tr}\, M\rho_1 \,\middle|\, 0 \leq M \leq \mathbb{1},\ 1-\mathrm{Tr}\, M\rho_0 \leq \varepsilon\right\}$ is the hypothesis testing relative entropy [37, 38].

We then establish the fundamental limits for magic-state distillation in the asymptotic limit. We show that the distillable non-stabilizerness of a state ρ satisfies

$$\mathcal{M}_{H_+}(\rho) = \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathcal{M}^{\varepsilon}_{H_+}(\rho^{\otimes n}) \leq \frac{\theta(\rho)}{\log_2(3-\sqrt{3})},$$

$$\mathcal{M}_{T}(\rho) = \lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathcal{M}^{\varepsilon}_{T}(\rho^{\otimes n}) \leq \frac{\theta(\rho)}{\log_2(1+2\sin(\pi/18))}.$$

4.4 Efficiency of magic-state distillation

We further consider the *efficiency* of magic-state distillation. The efficiency of distilling a magic state ξ from several independent copies of a resource state ρ is given by the minimum number of copies of ρ needed, *on average*, to produce ξ using stabilizer operations:

$$N_{\mathrm{eff}}(\rho\to\xi) = \inf\left\{\frac{n}{p} : \Lambda(\rho^{\otimes n}) \to \xi \text{ w/ prob. } p,\ \Lambda\in\mathrm{SO}\right\}.$$

We show that the efficiency of distilling magic state ξ from resource states ρ is lower bounded by

$$N_{\theta_{\max}}(\rho,\xi) := \theta_{\max}(\xi)/\theta_{\max}(\rho).$$

We demonstrate that our lower bound can outperform the lower bound in [20] via a certain example, as depicted in Figure 2, thus giving an improved estimation of the efficiency of magic-state distillation.

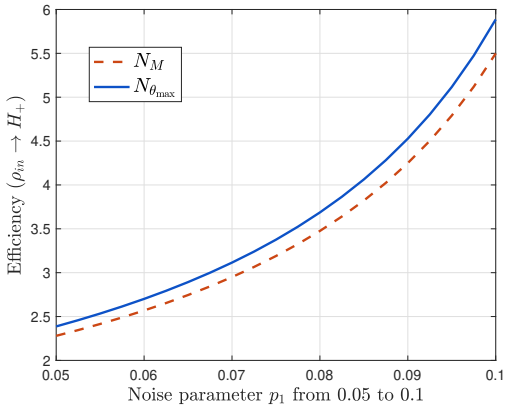


Figure 2: Comparison between $N_{\theta_{\max}}(\rho_{\mathrm{in}} \to H_+)$ and $N_{\mathcal{M}}(\rho_{\mathrm{in}} \to H_+)$ for input $\rho_{\mathrm{in}} = (1-p_1-p_2)|H_+\rangle\langle H_+| + p_1|H_-\rangle\langle H_-| + p_2|H_i\rangle\langle H_i|$ with $p_2 = 1/10$.

5 Conclusions

We have introduced the thauma family of measures to quantify and characterize the non-stabilizerness resource possessed by quantum states that are needed for universal quantum computation. The min- and max-thauma are efficiently computable by semi-definite programming and lead to bounds on the rates at which one can interconvert non-stabilizer states. These bounds have helped to solve pressing open questions in the resource theory of non-stabilizer states. More generally, our work establishes fundamental limitations on the processing of quantum non-stabilizerness, opening new perspectives for its investigation and exploitation as a resource in quantum information processing and quantum technology. Along this line, we suspect that our results will have immediate impact on the quantum optics community working on the resource theory of non-Gaussianity [39, 40, 41] and continuous-variable quantum computing [42, 43], because the main idea behind the thauma measure can be generalized to this setting.

References

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

[2] Andrew M. Childs and Wim van Dam. Quantum algorithms for algebraic problems. *Reviews of Modern Physics*, 82(1):1–52, jan 2010.

[3] Seth Lloyd. Universal Quantum Simulators. *Science*, 273(5278):1073–1078, aug 1996.

[4] 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.

[5] Earl T. Campbell, Barbara M. Terhal, and Christophe Vuillot. Roads towards fault-tolerant universal quantum computation. *Nature*, 549(7671):172–179, sep 2017.

[6] Daniel Gottesman. Stabilizer Codes and Quantum Error Correction. *PhD thesis*, may 1997.

[7] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Physical Review A*, 70(5):052328, nov 2004.

[8] 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.

[9] Xinlan Zhou, Debbie W. Leung, and Isaac L. Chuang. Methodology for quantum logic gate construction. *Physical Review A*, 62(5):052316, oct 2000.

[10] Sergey Bravyi and Alexei Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Physical Review A*, 71(2):022316, feb 2005.

[11] Sergey Bravyi and Jeongwan Haah. Magic-state distillation with low overhead. *Physical Review A*, 86(5):052329, nov 2012.

[12] Cody Jones. Multilevel distillation of magic states for quantum computing. *Physical Review A*, 87(4):042305, apr 2013.

[13] 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.

[14] Earl T. Campbell and Mark Howard. Magic state parity-checker with pre-distilled components. *Quantum*, 2:56, mar 2018.

[15] Matthew B. Hastings and Jeongwan Haah. Distillation with Sublogarithmic Overhead. *Physical Review Letters*, 120(5):050504, jan 2018.

[16] Anirudh Krishna and Jean-Pierre Tillich. Towards low overhead magic state distillation. *arXiv:1811.08461*, pages 1–7, nov 2018.

[17] Christopher Chamberland and Andrew W. Cross. Fault-tolerant magic state preparation with flag qubits. *arXiv:1811.00566*, nov 2018.

[18] Eric Chitambar and Gilad Gour. Quantum Resource Theories. jun 2018.

[19] 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.

[20] 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.

[21] Mark Howard, Joel J. Wallman, Victor Veitch, and Joseph Emerson. Contextuality supplies the magic for quantum computation. *Nature*, 510:351–355, June 2014.

[22] Nicolas Delfosse, Philippe Allard Guerin, Jacob Bian, and Robert Raussendorf. Wigner Function Negativity and Contextuality in Quantum Computation on Rebits. *Physical Review X*, 5(2):021003, apr 2015.

[23] Andrea Mari and Jens Eisert. Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient. *Physical Review Letters*, 109(23):230503, dec 2012.

[24] 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.

[25] Sergey Bravyi, Graeme Smith, and John A. Smolin. Trading Classical and Quantum Computational Resources. *Physical Review X*, 6(2):021043, jun 2016.

[26] Markus Heinrich and David Gross. Robustness of Magic and Symmetries of the Stabiliser Polytope. jul 2018.

[27] Eric M. Rains. A semidefinite program for distillable entanglement. *IEEE Transactions on Information Theory*, 47(7):2921–2933, 2001.

[28] Koenraad Audenaert, Bart De Moor, Karl Gerd H. Vollbrecht, and Reinhard F. Werner. Asymptotic relative entropy of entanglement for orthogonally invariant states. *Physical Review A*, 66(3):032310, sep 2002.

[29] Guifre Vidal and Reinhard F. Werner. Computable measure of entanglement. *Physical Review A*, 65(3):032314, feb 2002.

[30] Martin B. Plenio. Logarithmic Negativity: A Full Entanglement Monotone That is not Convex. *Physical Review Letters*, 95(9):090503, aug 2005.

[31] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge University Press, 2004.

[32] Sergey Bravyi, Dan Browne, Padraic Calpin, Earl Campbell, David Gosset, and Mark Howard. Simulation of quantum circuits by low-rank stabilizer decompositions. jul 2018.

[33] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53(4):2046–2052, apr 1996.

[34] Hakop Pashayan, Joel J. Wallman, and Stephen D. Bartlett. Estimating outcome probabilities of quantum circuits using quasiprobabilities. *Physical Review Letters*, 115(7):070501, August 2015. arXiv:1503.07525.

[35] Hussain Anwar, Earl T. Campbell, and Dan E. Browne. Qutrit Magic State Distillation. *New Journal of Physics*, 14(6):063006, feb 2012.

[36] Mark Howard and Jiri Vala. Qudit versions of the qubit pi/8 gate. *Physical Review A*, 86(2):022316, aug 2012.

[37] Francesco Buscemi and Nilanjana Datta. The Quantum Capacity of Channels With Arbitrarily Correlated Noise. *IEEE Transactions on Information Theory*, 56(3):1447–1460, mar 2010.

[38] Ligong Wang and Renato Renner. One-Shot Classical-Quantum Capacity and Hypothesis Testing. *Physical Review Letters*, 108(20):200501, may 2012.

[39] Francesco Albarelli, Marco G. Genoni, Matteo G. A. Paris, and Alessandro Ferraro. Resource theory of quantum non-Gaussianity and Wigner negativity. *Physical Review A*, 98(5):052350, nov 2018.

[40] Quntao Zhuang, Peter W. Shor, and Jeffrey H. Shapiro. Resource theory of non-Gaussian operations. *Physical Review A*, 97(5):052317, may 2018.

[41] Ryuji Takagi and Quntao Zhuang. Convex resource theory of non-Gaussianity. *Physical Review A*, 97(6):062337, jun 2018.

[42] Seth Lloyd and Samuel L. Braunstein. Quantum Computation over Continuous Variables. *Physical Review Letters*, 82(8):1784–1787, feb 1999.

[43] Daniel Gottesman, Alexei Kitaev, and John Preskill. Encoding a qubit in an oscillator. *Physical Review A*, 64(1):012310, jun 2001.

All fermionic non–Gaussian states are magic states for matchgate computations

M. Hebenstreit[1] * R. Jozsa[2] † B. Kraus[1] ‡ S. Strelchuk[2] § M. Yoganathan[2] ¶

[1] *Institute for Theoretical Physics, University of Innsbruck, Technikerstr. 21A, 6020 Innsbruck, Austria*
[2] *DAMTP, University of Cambridge, Cambridge CB3 0WA, UK*

Abstract. Magic states were introduced in the context of Clifford circuits as a resource that elevates classically simulatable computations to quantum universal capability, while maintaining the same gate set. Here we study magic states in the context of matchgate (MG) circuits, where the notion becomes more subtle. We show that every pure fermionic state which is non–Gaussian, i.e. which cannot be generated by MGs from a computational basis state, is a magic state for MG computations. This result has significance for prospective quantum computing implementation since MG circuit evolutions coincide with the quantum physical evolution of non-interacting fermions.

Keywords: Quantum computing, matchgates, magic states

The full paper version of this submission is at [1].

1 Introduction

Exploring the landscape intermediate between classical and quantum computing is one of the most interesting issues in quantum information science for both theory and potential implementational impact. It provides the natural context for the consideration of novel trade-off possibilities between the individual constituents of the respective theories, that may then provide new applications for emerging near-term quantum hardware of likely limited quantum capability. One fruitful approach in this direction is to determine the classical simulation complexity of a restricted class of quantum processes (that may perhaps enjoy some implementational benefit), and then identify minimal extra resources that would suffice to regain full universal quantum computing power.

The theory of fermionic linear optics underpins a large number of important physical systems, such as Gaussian communication channels [2] and important phenomena in condensed matter physics [3, 4], including Majorana fermions in quantum wires [5] and Kitaevs honeycomb lattice model [6]. Together with the development of experimental systems such as cold atoms [7], atoms in optical lattices [8], and quantum dots [9, 10] it is well-suited for a range of information processing tasks.

Early on, it was shown that the computational capabilities of unassisted fermionic linear optics can be described by matchgate circuits (MGCs) and they are entirely classically efficiently simulatable [11, 12, 13, 14], the latter holding also for some extensions of fermionic linear optics with dissipative processes [15]. Another class of quantum processes that is classically simulatable is given by Clifford circuits, albeit for different reasons in comparison to MGCs [16] and indeed the classically simulatable computational power of MGCs has the neat characterisation of being equivalent to log-space bounded universal unitary quantum computation [17].

Determining extra ingredients for Clifford circuits [19, 18] or for MGCs that suffice to regain universal computational power, can give avenues for boosting the power of corresponding near-term quantum computing devices that are based on implementing such gates. In the case of Clifford circuits a fundamentally important such ingredient is the provision of a so-called magic state [19] i.e. a suitably chosen additional input state whose availability gives universal computing power while still using only the same gate set, via introduction of an associated "gate-gadget" construction.

In this paper we establish and study the notion of magic states for MGCs. We will see that this notion becomes more subtle in the matchgate context, as matchgate actions are subject to a locality constraint, and also the SWAP gate is not available to freely move magic states into arbitrary positions amongst the qubits. Nevertheless a similar picture of gate-gadget constructions applies, and our main result will be to show that *every* pure fermionic state which is non–Gaussian, i.e. which cannot be generated by a MGC from a computational basis state, is a magic state for MGCs. Along the way we will see that the matchgate locality constraint imposes a necessary condition that magic states be fermionic states; and we will give an explicit example of a gate-gadget construction (with associated 4-qubit magic state) for implementing the SWAP gate, which is known to extend the power of MGCs to full quantum universal power [13].

Preliminaries: The Pauli operators are denoted by X, Y, Z. For n qubits, the even (resp. odd) parity subspace, is the subspace spanned by all computational basis states containing an even (resp. odd) number of 1's i.e. the $+1$ (resp. -1) eigenspace of the n-qubit operation $Z^{\otimes n}$. An operator is called *even* if it preserves the even and odd parity subspaces. A matchgate (MG) is a two–qubit unitary even operator $G(A, B) = A \oplus B$ where $A, B \in U(2)$ act on the even and odd parity subspaces respectively and satisfy $\det A = \det B$. Whereas the fermionic SWAP gate, $fSWAP = G(Z, X)$, is a MG,

*Martin.Hebenstreit@uibk.ac.at
†rj310@cam.ac.uk
‡Barbara.Kraus@uibk.ac.at
§ss870@cam.ac.uk
¶my332@cam.ac.uk

the $SWAP$ gate, $SWAP = G(\mathbb{1}, X)$ is not (as the determinants of the two unitaries do not match). A matchgate circuit (MGC) is a quantum circuit which comprises MGs acting only on *nearest neighbor* (n.n.) lines. Correspondingly, in the following the term MG will always refer to a nearest neighbor matchgate. The action of any MGC is always an even operator. It has been shown [21, 11, 13] that for any MGC, if the input is a computational basis state and the output is a final computational basis measurement on any single qubit, then the output is classically efficiently simulatable. Moreover, in [17] it has been shown that MGCs running on n qubits can be compressed into a universal quantum computer running on $\mathcal{O}(\log(n))$ qubits. However, supplementing MGCs with additional gates, such as the SWAP-gate, makes the circuits universal for quantum computing [13, 22, 23, 24]. This is analogous to the situation of classically simulatable Clifford computations being elevated to universal quantum computing power by the inclusion of a non-Clifford gate such as the T gate.

We will use the following terminology. An n qubit state $|\Psi\rangle$ is called *fermionic* if it is an eigenstate of $Z^{\otimes n}$ i.e. it is supported entirely in the even or odd parity subspace. An n-qubit operation W is called *Gaussian* if it arises as the action of a MGC (which in turn always corresponds via the Jordan-Wigner transformation, to evolution under a quadratic fermionic Hamiltonian). An n-qubit state $|\Psi\rangle$ is called *Gaussian* if it arises as the action of a Gaussian operation on a computational basis state. We call two states $|\phi_1\rangle$ and $|\phi_2\rangle$ *MG–equivalent* if there exists a free operation which transforms $|\phi_1\rangle|b_1\rangle$ into $|\phi_2\rangle|b_2\rangle$ where $|b_1\rangle, |b_2\rangle$ are computational basis states. Clearly MG-equivalence is an equivalence relation.

As MGs can be freely applied in circuits without altering the classical simulability of the computational output, we call a product of MGs, i.e. a Gaussian unitary operator, a *free* or *resourceless* operation, and introduce a *resourceful* gate as one which leads to a universal gate set if used in conjunction with free operations. Here quantum computational universality may occur in an encoded sense wherein the logical $|0\rangle, |1\rangle$ states may be represented by suitably simple multi-qubit states upon which the free and resourceful gates act to effect logical gates (e.g. as in [13] where it is shown that n.n. $SWAP$ is a resourceful gate).

2 Magic states

The notion of magic state has been introduced in the context of Clifford circuits [19] which then comprise the free operations. While circuits composed solely of Clifford gates acting on computational basis state inputs are classically efficiently simulatable, adding the T gate makes the gate set universal. But instead of enlarging the gate set, one can alternatively consider allowing more general input states, so-called magic states, and adaptive measurements. In this way one can realize a T gate via the so-called T-gadget [19], that consumes one copy of the magic state $|T\rangle = 1/\sqrt{2}\left(|0\rangle + e^{i\pi/4}|1\rangle\right)$ and uses one adaptive measurement in the computational basis together with only Clifford gates. Let us stress here that neither copies of the magic state, nor adaptive measurements in the computational basis by themselves give rise to universal quantum computation (assuming quantum is more powerful than classical computing). Indeed these situations are classically efficiently simulatable [26, 27, 28, 29, 30]. Henceforth adaptive measurements will alwys be in the computational basis only.

In generality, we introduce the following natural definition: if R is a resourceful k-qubit gate for a set of free operations, we say that an m-qubit state $|M\rangle$ is a *magic state* for R if
(M1): there is a circuit C of free gates and adaptive measurements such that for any k-qubit state $|\alpha\rangle$, C maps $|\alpha\rangle|M\rangle$ to $(R|\alpha\rangle)|\tilde{M}\rangle$ (where $|\tilde{M}\rangle$ is any state, that may depend on the intermediate measurement outcomes too. However, it may not depend on $|\alpha\rangle$.)
Actually we will need a slightly more general version of (M1) as follows. We will require that for any $\epsilon > 0$, C (of circuit size $O(poly(1/\epsilon))$) acting on $|\alpha\rangle$ together with $O(poly(1/\epsilon))$ copies of $|M\rangle$, produces $R|\alpha\rangle$ with probability $1 - \epsilon$ (where the probabilistic randomness here arises from the intermediate measurement outcomes.) For bounded error computations with input size n we take $\epsilon = 1/poly(n)$, which then maintains efficiency of the computation.

We wish to develop the theory of magic states for matchgate computations (so that henceforth free operations will always be Gaussian operations), but note that right from the start there are key differences that will require special care in the MG compared to the Clifford scenario, necessitating a further condition (M2) as below. For Cliffords, $SWAP$ is a free operation, so any free (multi-qubit) gate can be placed to act on any (distant) lines, and magic states can be freely moved to any position amongst the qubit lines when required or else placed there at the outset in the initial input state, all without affecting any action of free gates. But for MGCs none of these features hold! - MGs can act on n.n. lines only and $SWAP$ is not a free gate so states cannot generally be freely moved around amongst the qubit lines. In particular magic states cannot be freely moved into the positions needed for their use in implementing a resourceful gate; and nor can they be placed in their needed positions from the start, as this would partition the circuit lines into sectors that must then remain independent under processing by n.n. gates, at least until the magic state has been suitably disposed of. In view of these features, in addition to (M1) we impose a second condition (M2) on a state $|M\rangle$ for it to be a magic state:
(M2): The state $|M\rangle$ can be swapped through arbitrary states via use of free gates only.

Thus as for Clifford circuits, magic states can be prepared prior to the computation and can then be used whenever and wherever needed.

Magic states for MG computations: To begin our characterisation, we note that magic states for matchgate circuits cannot be single qubit states nor products of single qubit states. This follows from the fact that matchgate

circuits remain classically simulatable even if arbitrary product input states and adaptive measurements are allowed [32]. Next we have the following result relevant for (M2).

Lemma 1 *A multi-qubit state $|\psi\rangle$ on adjacent lines can be swapped through a neighboring line in an arbitrary state using free gates iff it is fermionic.*

The proof (including specification of allowable swapping processes) is given in Appendix A of [1].

Before presenting our main result we give a simple explicit example of a 4-qubit magic state, thus also showing that (M1) and (M2) are not mutually inconsistent. Note that the smallest number of qubits that can be used is 4, as all 2- and 3-qubit fermionic states are Gaussian [33]. The state $|M\rangle = |\phi^+\rangle_{13}|\phi^+\rangle_{24} = 1/2\,(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)_{1234}$ is a magic state. It is the Choi state corresponding to the $SWAP$ gate. In fact one copy of this state can be utilized to deterministically implement the resourceful $SWAP$ gate using MGs and adaptive measurements in a gadget reminiscent of gate teleportation [34], as shown in Figure 1. $|M\rangle$ is a state on four consecutive qubit lines, where its uppermost line (qubit 1) and the lowermost line (qubit 4) are the qubits on which the input will be teleported, and the inner lines, qubits 2 and 3 will carry the output. After teleporting the input with Bell measurements, the swapped input states are available on lines 2 and 3 up to local Pauli corrections. In contrast to Clifford circuits where the Pauli correction operators can be postponed until the end of the computation, here they must be corrected right after the measurement. This can be achieved with the help of an auxiliary line and using MGs solely - one can compensate the Pauli corrections and thus deterministically implement the $SWAP$ gate. Note that in this $SWAP$-gadget, $\sigma_z \otimes I$ and $\sigma_x \otimes \sigma_x$ are MGs (but e.g. $\sigma_x \otimes I$ is not a MG). Note further that the required Bell measurements can be realized by two local computational basis measurements preceded by the MG $G(H,H)$ as shown in the inset of Figure 1. $|M\rangle$ hence fulfills (M1) for $R = SWAP$. Moreover, $|M\rangle$ is a fermionic state and hence (by Lemma 1) fulfills (M2) (see Figure 2). As in the case of Clifford circuits, neither the magic state itself (and copies thereof), nor the adaptive measurement alone results in a circuit which is no longer classically simulatable [35]; it is only the combination of both that makes them resourceful.

Lemma 2 *$|\psi_\phi\rangle = 1/2(|0000\rangle + |0011\rangle + |1100\rangle + e^{i\phi}|1111\rangle)$ is a magic state for matchgate circuits for all $\phi \in (0, 2\pi)$. The resourceful controlled-ϕ-phase gate can be realized with arbitrary high success probability $1-\epsilon$ ($\epsilon > 0$) by consuming $\mathcal{O}(poly(1/\epsilon))$ copies of the state $|\psi_\phi\rangle$.*

The proof is given in Appendix B of [1].

Clearly any state which is MG–equivalent to a magic state is magic too. Next we show that any entangled 4–qubit fermionic state which is non–Gaussian is MG–equivalent to $|\psi_\phi\rangle$ for some $\phi \in (0, 2\pi)$. We show this

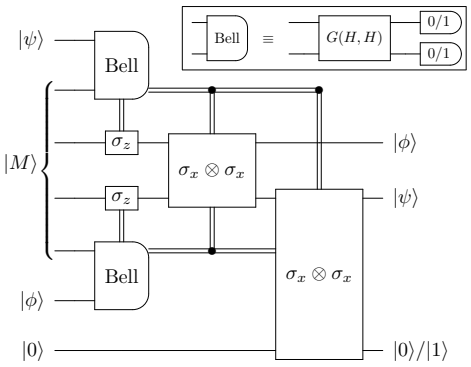


Figure 1: The $SWAP$-gadget deterministically implements a $SWAP$ gate with the help of the magic state $|M\rangle = |\phi^+\rangle_{13}|\phi^+\rangle_{24}$. Inset: the Bell measurements can be implemented by $G(H,H)$ followed by single qubit measurements in the computational basis.

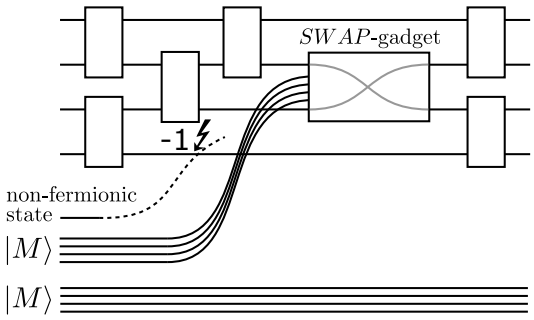


Figure 2: Non-fermionic states do not satisfy (M2). Swapping them through other lines with e.g. $fSWAP$, a relative phase (-1) is picked up. The state $|M\rangle$ satisfies (M2), thus it can be swapped through arbitrary states via free operations. It moreover satisfies (M1), i.e., it allows implementation of a resourceful operation, here the $SWAP$-gate. Our a main result is that actually all non-Gaussian fermionic states can be swapped through arbitrary states via free operations, and moreover they allow the implementation of resourceful gates.

by constructing an explicit MGC of depth three, which transforms any given 4–qubit fermionic state into a state of the form $|\psi_\phi\rangle$. The construction is given in Appendix B of [1]. Hence it follows that any entangled 4–qubit fermionic state which is non–Gaussian is magic.

Finally we use the above results to prove the main result of the paper:

Theorem 3 *Any pure fermionic state which is non–Gaussian is a magic state for matchgate computations.*

The proof is by induction on the number $k \geq 4$ of qubits of the fermionic state, and it is given in Appendix B of [1].

Recall that a Gaussian state can be generated from a computational basis state via a MGC, so it can never be a magic state. Furthermore, we have seen already that (M2) implies that any magic state must be fermionic. Hence Theorem 3 shows that the largest set of possible states is indeed magic.

References

[1] M. Hebenstreit, R. Jozsa, B. Kraus, S. Strelchuk and M. Yoganathan, full paper version of this submission, available at `https://arxiv.org/abs/1905.08584` (2019).

[2] S. Bravyi, Quantum Inf. Comput. **5**, 216 (2005).

[3] Y. Zhang. (2012). PhD thesis. University of California, Berkeley.

[4] A. Botero, B. Reznik. Phys. Lett. A, 331(1-2), 39-44 (2004).

[5] A. Kitaev, Physics-Uspekhi 44, no. 10S (2001): 131.

[6] A. Kitaev , Annals of Physics 321, no. 1 (2006): 2-111.

[7] S. Giorgini, et al. Rev. Mod. Phys. 80(4), 1215 (2008).

[8] R. Jordens, et al. Nature, 455(7210), 204 (2008).

[9] D. Loss, D. P. DiVincenzo, (1998). Physical Review A, 57(1), 120.

[10] R. Hanson., et at. Rev. Mod. Phys., 79(4), 1217 (2007).

[11] B. Terhal and D. DiVincenzo, Phys. Rev. A **65**, 032325 (2002).

[12] E. Knill, Fermionic linear optics and matchgates. Preprint available at arXiv:quant-ph/0108033 (2001).

[13] R. Jozsa and A. Miyake, Proc. R. Soc. A **464**, 3089 (2008).

[14] R. Jozsa, A. Miyake, and S. Strelchuk, Quant. Inform. Comp. **15**, 0541 (2015).

[15] R. Koenig, S. Bravyi, Quant. Inf. Comp., vol. 12, no. 11-12, pp. 925-943 (2012).

[16] R. Jozsa, Springer LNCS 5393, J. Calmet, W. Geiselmann, J. Mueller-Quade (eds.), p43-49. Springer, Berlin, Heidelberg (2008).

[17] R. Jozsa, B. Kraus, A. Miyake, J. Watrous, Proc. R. Soc. A **466**, 809 (2010).

[18] S. Bravyi, G. Smith, and J. A. Smolin, Phys. Rev. X **6**, 021043 (2016).

[19] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).

[20] V. Veitch et al. NJP 14, no. 11 (2012): 113011.

[21] L. Valiant, SIAM J. Computing **31**, 1229 (2002).

[22] D. J. Brod and E. F. Galvo, Phys. Rev. A **84**, 022310 (2011).

[23] D. J. Brod and E. F. Galvo, Phys. Rev. A **86**, 052307 (2012).

[24] D. J. Brod and A. M. Childs, Quantum Information and Computation **14**, 901 (2014).

[25] C. Spee, K. Schwaiger, G. Giedke, and B. Kraus, PRA **97**, 042325 (2018).

[26] D. Gottesman, Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics, 32 (1999).

[27] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).

[28] S. Clark, R. Jozsa, and N. Linden, Quant. Inf. Comp. **8**, 106 (2008).

[29] M. Van den Nest, Quant. Inf. Comp. **10**, 0258 (2010).

[30] R. Jozsa and M. Van den Nest, Quant. Inf. Comp., **14**, 633 (2014).

[31] S. Bravyi, Phys. Rev. A **73**, 042313 (2006).

[32] D. J. Brod, Phys. Rev. A **93**, 062332 (2016).

[33] S. Bravyi, arXiv:0507282[quant-ph] (2005).

[34] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).

[35] M. Hebenstreit et al., Manuscript in preparation (2019).

[36] R. Jozsa and S. Strelchuk, arXiv:1705.02817[quant-ph] (2017).

[37] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, Phys. Rev. Lett. **86**, 544 (2001).

Plug-and-Play Approach to Geometric Quantum Computation

BaoJie Liu[1] Xue-Ke Song[1] Zheng-Yuan Xue[2] * Xin Wang [†3] Man-Hong Yung[1 4 ‡]

[1]*Institute for Quantum Science and Engineering, and Department of Physics, Southern University of Science and Technology, Shenzhen 518055, China*

[2]*Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, and School of Physics and Telecommunication Engineering, South China Normal University, Guangzhou 510006, China*

[3]*Department of Physics, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong SAR, China, and City University of Hong Kong Shenzhen Research Institute, Shenzhen, Guangdong 518057, China*

[4]*Shenzhen Key Laboratory of Quantum Science and Engineering, Shenzhen 518055, China*

Abstract. Non-adiabatic holonomic quantum computation (NHQC) has been developed to shorten the construction times of geometric quantum gates. However, previous NHQC gates require the driving Hamiltonian to satisfy a set of rather restrictive conditions, reducing the robustness of the resulting geometric gates against control errors. Here we show that non-adiabatic geometric gates can be constructed in an extensible way, called NHQC+, for maintaining both flexibility and robustness. Consequently, this approach makes it possible to incorporate most of the existing optimal control methods, such as dynamical decoupling, composite pulses, and shortcut to adiabaticity, into the construction of single-looped geometric gates. Furthermore, we propose experimentally demonstrate that HQC via shortcut to adiabaticity can be constructed with only three energy levels, using a superconducting qubit in a scalable architecture. With this scheme, all holonomic single-qubit operations can be realized non-adiabatically through a single cycle of state evolution. As a result, we are able to experimentally benchmark the stability of NHQC+ against NHQC in the same platform.

Keywords: Geometric quantum gate, NHQC+, optimal control

The related theoretical and experimental articles are arXiv:1806.07904 (2019) and Phys. Rev. Lett. **122**, 080501 (2019).

Introduction.— When a quantum system is driven slowly through a parametric cycle in a degenerate Hilbert space, the state would acquire a non-Abelian geometric phase, which is stable and forms the foundation for holonomic quantum computation (HQC) [1, 2, 3] . However, in the adiabatic limit, the environmental decoherence becomes a significant source of errors. Recently, various nonadiabatic holonomic quantum computation (NHQC) schemes have been proposed [4, 5], but all at the price of increased sensitivity to control errors [6]. Furthermore, the restriction imposed in the previous NHQC schemes excludes the flexibility for incorporating most of the optimization techniques, limiting its applicability. These problems motivate us to search for a new approach to GQC that is non-adiabatic, robust against the control errors, and compatible with other optimization techniques for maximizing the gate fidelity against different types of noises.

Our main contributions are: (i) we demonstrate that non-adiabatic GQC is also possible under much general conditions, relative to traditional NHQC [4, 5]. Our approach leads to a new form of single-looped GQC that is compatible with most of the existing pulse-shape optimization methods, including Derivative Removal by Adiabatic Gate (DRAG) [7], Shortcut to adiabaticity (STA) or counteradiabatic driving (CD) [8, 9], dynamical decoupling (DD) [10, 11, 12], dynamically-corrected gates (DCG) [13, 14, 15], and Floquet optimal control [16, 17], etc, as shown in Fig 1. Given the extensibility of this approach and the fact that the traditional NHQC method can be regarded as a special case, we refer to this method as NHQC+. For example, when combined with STA, we label it as STAHQC.

(ii) We employ a three-level quantum systems to illustrate the working mechanism of NHQC+. In particular, we are interested in comparing our method with the NHQC gates implemented in recent experiments with NV centers [18, 19]. Numerical simulations indicate that our optimized NHQC+ method can achieve a significant improvement over the NHQC gates in Refs. [18, 19], using the experimental parameters.

(iii) We propose experimentally demonstrate that HQC via shortcut to adiabaticity can be constructed with only three energy levels, using a superconducting qubit in a scalable architecture. With this scheme, all holonomic single-qubit operations can be realized non-adiabatically through a single cycle of state evolution [20]. As a result, we are able to experimentally benchmark the stability of STAHQC against NHQC in the same platform.

General framework.— Let us start with a general time-dependent Hamiltonian $H(t)$. For any complete set of basis vectors, $\{|\psi_m(0)\rangle\}$ at $t = 0$, $U(t,0) = \mathcal{T}e^{-i\int_0^t H(t')dt'} = \sum_m |\psi_m(t)\rangle\langle\psi_m(0)|$, where the time-dependent state, $|\psi_m(t)\rangle = \mathcal{T}e^{-i\int_0^t H(t')dt'}|\psi_m(0)\rangle$, follows the Schrödinger equation. Now, at each moment of time, we can always choose a different set of time-dependent basis, $\{|\mu_m(t)\rangle\}$, which satisfies the boundary conditions at time $t = 0$ and $t = \tau$:

$$|\mu_m(\tau)\rangle = |\mu_m(0)\rangle = |\psi_m(0)\rangle \ , \tag{1}$$

but in general their time dependence do not follow Schrödinger's equation. In this way, we can always write, $|\psi_m(t)\rangle = \sum_k v_{km}(t)|\mu_k(t)\rangle$, which means that the time-evolution operator becomes, $U(t,0) = \sum_{m,k} v_{km}(t)|\mu_k(t)\rangle\langle\psi_m(0)|$. Applying the boundary

*zyxue83@163.com
†x.wang@cityu.edu.hk
‡yung@sustech.edu.cn

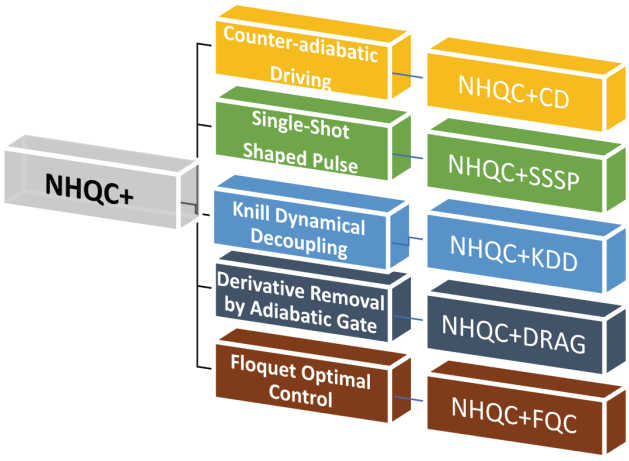


Figure 1: Schematic of combining various optimal control pulses with geometric quantum computation in our scheme.

conditions, we obtain the following unitary transformation matrix at the final time $t = \tau$, $U(\tau,0) = \sum_{m,k} v_{km}(\tau)\,|\psi_k(0)\rangle\langle\psi_m(0)|$. The matrix element $v_{mk}(\tau)$ satisfies the following equation,

$$\frac{d}{dt}v_{km}(t) = i\sum_{l=1}\left(A_{kl}(t) - H_{kl}(t)\right)v_{lm}(t)\ , \qquad (2)$$

where $H_{kl}(t) \equiv \langle\mu_k(t)|\,H(t)\,|\mu_l(t)\rangle$ and $A_{kl}(t) \equiv i\langle\mu_k(t)|\,\frac{d}{dt}\,|\mu_l(t)\rangle$, which can be combined to form an effective Hamiltonian: $H_{\rm eff}(t) \equiv V(t)^\dagger H(t) V(t) - iV^\dagger(t)\frac{d}{dt}V(t)$, where $V(t) \equiv \sum_k |\mu_k(t)\rangle\langle\mu_k(0)|$. In other words, written in the initial basis $\{|\mu_k(0)\rangle\}$, the matrix elements are given by $A_{kl}(t) - H_{kl}(t)$. With these tools, various forms of GQC can emerge as different settings (or approximations) of these equations.

Conditions of NHQC+.— Our strategy is to find an auxiliary basis $\{|\mu_k(t)\rangle\}$ such that for all $k \neq m$, the effective Hamiltonian $H_{\rm eff}$ is always diagonal in the *initial basis*, i.e.,

$$\langle\mu_m(0)|\,H_{\rm eff}(t)\,|\mu_k(0)\rangle = 0\ , \qquad (3)$$

Consequently, Eq. (2) implies that $v_{mk}(t) = \delta_{mk}\,v_{kk}(t)$ is also diagonal and hence the unitary operator,

$$U(t,0) = \sum\nolimits_k v_{kk}(t)\,|\mu_k(t)\rangle\langle\mu_k(0)| \qquad (4)$$

are all diagonal, where $v_{kk}(t) = e^{-i\int_0^\tau \langle\mu_k(t)|H(t)|\mu_k(t)\rangle dt - \int_0^\tau \langle\mu_k(t)|\,\dot{\mu}_k(t)\rangle dt}$. Note particularly that if the following condition,

$$\int_0^\tau \langle\mu_k(t)|H(t)|\mu_k(t)\rangle\ dt = 0. \qquad (5)$$

is further satisfied for *each* k, then the resulting unitary evolution becomes *purely geometric*, i.e.,

$$U(\tau,0) = \sum_k e^{-\int_0^\tau \langle\mu_k(t)|\dot{\mu}_k(t)\rangle dt}\,|\mu_k(0)\rangle\langle\mu_k(0)|\ , \qquad (6)$$

which is the main goal that can be achieved through the following theorem:

Theorem 1 (NHQC+ equation) *The condition in Eq. (3) is satisified only if the Hamiltonian $H(t)$ and the projector $\Pi_k(t) \equiv |\mu_k(t)\rangle\langle\mu_k(t)|$ of the auxiliary basis $\{|\mu_k(t)\rangle\}$ follows the von Neumann equation, i.e.,*

$$\frac{d}{dt}\Pi_k(t) = -i\left[H(t), \Pi_k(t)\right]\ , \qquad (7)$$

The proof of this theorem is given in Ref. [21].

Note that the key difference between the previous NHQC schemes and the NHQC+ approach introduced here is that the Hamiltonians are subject to different constraints. In the NHQC case, the Hamiltonian is required to satisfy a set of constraints: $\langle\psi_m(t)|\,H(t)\,|\psi_k(t)\rangle = 0$, which is required (i) at *each moment of time* and (ii) for *all* possible k, m. However, for NHQC+, the Hamiltonian needs to vanish only in the integral sense (see Eq. (5)). More importantly, the NHQC+ removes the constriants for $k \neq m$, which makes it possible for our method being compatible with most of the optimization schemes (see Fig. 1).

Application of NHQC+ gates.— We focus on the three-level system with a one-photon detuning $\Delta(t)$, in the interaction picture, is given by,

$$H(t) = \Delta(t)|e\rangle\langle e| + \frac{1}{2}\left[\left(\Omega_P(t)|0\rangle + \Omega_S(t)|1\rangle\right)\langle e| + H.c.\right], \qquad (8)$$

where $\Omega_P(t)$ and $\Omega_S(t)$ denote, respectively, the pumping and Stokes pulses driving the $|0\rangle \leftrightarrow |e\rangle$ and $|1\rangle \leftrightarrow |e\rangle$ transitions. Here, we choose the pluses to have the following form, $\Omega_P(t) = \Omega(t)\sin(\theta/2)e^{i\phi_1(t)}$ and $\Omega_S(t) = \Omega(t)\cos(\theta/2)e^{i[\phi_1(t)+\phi]}$, but we maintain the ratio $\Omega_P(t)/\Omega_S(t)$ of the two pulses to be time-independent, i.e., $\Omega_P(t)/\Omega_S(t) \equiv \tan(\theta/2)\,e^{-i\phi}$. Consequently, the Hamiltonian in Eq. (8) can be simplified as,

$$H(t) = \Delta(t)|e\rangle\langle e| + \frac{\Omega(t)}{2}\left[e^{i\phi_1(t)}\,|\Phi\rangle\langle e| + H.c.\right]\ , \qquad (9)$$

where we defined a time-independent bright state as, $|\Phi\rangle \equiv \sin(\theta/2)|0\rangle + \cos(\theta/2)e^{i\phi}|1\rangle$.

Recall that for realizing NHQC+ gates, we need to choose a set of auxiliary states satisfying the boundary conditions in Eq. (1). Here our choice is (i) a dark state $|\mu_0\rangle = \cos(\theta/2)|0\rangle - \sin(\theta/2)e^{i\phi}|1\rangle$ which is decoupled from subspace of $|\Phi\rangle$ and $|e\rangle$, and (ii) an orthogonal state in the following form:

$$|\mu_+(t)\rangle = \sin\tfrac{\chi(t)}{2}|\Phi\rangle + \cos\tfrac{\chi(t)}{2}e^{-i\alpha(t)}|e\rangle\ , \qquad (10)$$

The variables $\chi(t)$ and $\alpha(t)$ are determined by requiring the corresponding projector, $\Pi_+(t) = |\mu_+(t)\rangle\langle\mu_+(t)|$, to satisfy the von Neumann equation in Eq. (7).

Construction of NHQC+ gates.— We are now ready to demonstrate how to build up universal non-Abelian geometric single-qubit gates, i.e., holonomic quantum gates.

Let us start with the following set of basis states, $\{|\mu_0\rangle, |\mu_+(0)\rangle\}$. States $|\mu_+(0)\rangle$ evolve cyclically and gain the phase, i.e., $e^{i\gamma}|\mu_+(0)\rangle$ including both geometric and dynamical components. We can erase the accumulated dynamical phases by using the spin echo pulses, and thus pure geometric phases can be obtained. Under those conditions, we

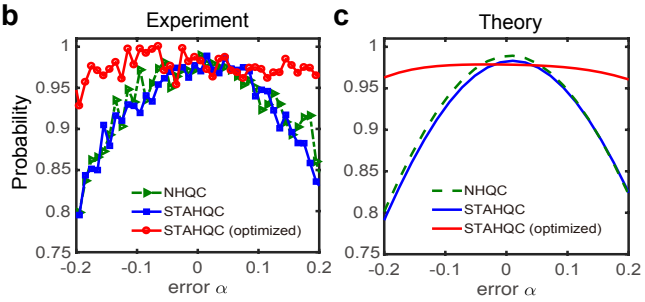


Figure 2: (b) (experiment) and (c) (theory): performance of an X gate with control errors for various HQC schemes. Theoretical results are obtained using master-equation numerical simulation. α represents magnitude of the control error.

obtain the following unitary transformation matrix in the basis states $\{|\mu_0\rangle, |\mu_+(0)\rangle\}$ at the final time $t = \tau$,

$$U(\tau,0) = |\mu_0\rangle\langle\mu_0| + e^{i\gamma}|\mu_+(0)\rangle\langle\mu_+(0)| = e^{i\frac{\gamma}{2}}e^{-i\frac{\gamma}{2}\boldsymbol{n}\cdot\boldsymbol{\sigma}}, \tag{11}$$

where $\boldsymbol{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$, $\boldsymbol{\sigma}$ are the Pauli matrices. Eq. (11) describes a rotational operation around the $\boldsymbol{n}$ axis by a γ angle, up to a global phase factor $e^{-i\frac{\gamma}{2}}$. As both $\boldsymbol{n}$ and γ can take any value, Eq. (11) denotes a set of universal single-qubit gates in the qubit subspace.

Experimental realization with superconducting qubits.— For the purpose of demonstration, we report an experimental realization of our proposal using an Xmon superconducting qutrit, which has a ladder Ξ energy structure in Ref. [20] In the experiment, we constructed noncommutative holonomic gates by varying three independent control parameters to generate the SU(2) transformation group elements, following our STAHQC proposal. The experimental results are in good agreement with our numerical simulations, with both control and environmental noise being taken into account. As a result, both NHQC and STAHQC gate, can now be compared within the same experimental platform.

Before optimization, the performance of NHQC and STAHQC are on par with each other; this is consistent with the results of a recent experimental demonstration of NHQC using superconducting qubits. However, for many gates, the approach in Ref. [22] requires at least two cycles to implement, which takes a longer time, making the system more susceptible to environmental noise and control error. In addition, the noise robustness of STAHQC can be further enhanced by pulse optimization as shown in Fig. 2b-c. Overall, the advantage of STAHQC over NHQC is expected to be more significant as environmental noise and control error become more prominent.

Conclusion.— We have presentedand experimentally demonstrated an extensible framework of non-adiabatic geometric quantum computation, NHQC+, which is compatible with many techniques in optimal control theory, such as SSSP, KDD, and more. Our approach relaxes the constraint imposed for the driving Hamiltonian in the previous approach of NHQC. This method should also be of interest to other platforms such as trapped ions, quantum dots, and nuclear magnetic resonance, etc.

References

[1] P. Zanardi, and M. Rasetti, Phys. Lett. A **264**, 94 (1999).

[2] E. Sjöqvist, Physics **1**, 35 (2008).

[3] Y. Aharonov, and J. Anandan, Phys. Rev. Lett. **58**, 1593 (1987).

[4] E. Sjöqvist, D. M. Tong, L. M. Andersson, B. Hessmo, M. Johansson, and K. Singh, New J. Phys. **14**, 103035 (2012).

[5] G. F. Xu, J. Zhang, D. M. Tong, E. Sjöqvist, and L. C. Kwek, Phys. Rev. Lett.**109**,170501 (2012).

[6] S. B. Zheng, C. P. Yang, and F. Nori, Phys. Rev. A **93**, 032313 (2016).

[7] F. Motzoi, J. M. Gambetta, P. Rebentrost, and F. K. Wilhelm, Phys. Rev. Lett. **103**, 110501 (2009).

[8] M. V. Berry, J. Phys. A: Math. Theor, **42**, 365303 (2009).

[9] X. Chen, I. Lizuain, A. Ruschhaupt, D. Guéry-Odelin, and J. G. Muga, Phys. Rev. lett. **105** 123003 (2010).

[10] K. Khodjasteh, and D. A. Lidar, Phys. Rev. Lett. **95**, 180501 (2005).

[11] A. M. Souza, G. A. Alvarez, and D. Suter, Phys. Rev. Lett. **106**, 240501 (2011).

[12] G. T. Genov, D. Schraft, N. V. Vitanov, and T. Halfmann, Phys. Rev. Lett. **118**, 133202 (2017).

[13] K. Khodjasteh, and L. Viola, Phys. Rev. Lett. **102**, 080501 (2009).

[14] X. Wang, L. S. Bishop, J. P. Kestner, E. Barnes, K. Sun, and S. D. Sarma, Nat. Commun. **3**, 997 (2012).

[15] X. Rong, J. Geng, F. Shi, Y. Liu, K. Xu, W. Ma, F. Kong, Z. Jiang, Y. Wu, and J. Du, Nat. Commun. **6** (2015).

[16] B. Bartels and F. Mintert, Physical Review A **88**, 052315 (2013).

[17] T. Nöbauer, A. Angerer, B. Bartels, M. Trupke, S. Rotter, J. Schmiedmayer, F. Mintert, and J. Majer, Phys. Rev. Lett. **115**, 190801 (2015).

[18] Y. Sekiguchi, N. Niikura, R. Kuroiwa, H. Kano, and H. Kosaka, Nat. Photonics **11**, 309 (2017).

[19] B. B. Zhou, P. C. Jerger, V. O. Shkolnikov, F. J. Heremans, G. Burkard, and D. D. Awschalom, Phys. Rev. Lett. **119**, 140503 (2017).

[20] T. Yan, B.-J. Liu, K. Xu, C. Song, S. Liu, Z. Zhang, H. Deng, Z. Yan, H. Rong, M.-H. Yung, Y. Chen, and D. Yu, Phys. Rev. Lett. 122, 080501 (2019).

[21] B.-J. Liu, X.-K. Song, Z.-Y. Xue, X. Wang, and M.-H. Yung, arXiv:1806.07904.

[22] A. A. Abdumalikov, J. M. Fink, K. Juliusson, M. Pechal, S. Berger, A. Wallraff, and S. Filipp, Nature **496**, 482 (2013).

Achieving the Heisenberg limit in quantum metrology using quantum error correction

Liang Jiang[1 2 *]

[1] *Pritzker School of Molecular Engineering, The University of Chicago, Chicago, IL, USA*
[2] *Yale Quantum Institute, Yale University, New Haven, CT, USA*

Abstract. Quantum metrology has many important applications in science and technology, ranging from frequency spectroscopy to gravitational wave detection. Quantum mechanics imposes a fundamental limit on measurement precision, called the Heisenberg limit, which can be achieved for noiseless quantum systems, but is not achievable in general for systems subject to noise. Here we study how measurement precision can be enhanced through quantum error correction, a general method for protecting a quantum system from the damaging effects of noise. We find a necessary and sufficient condition for achieving the Heisenberg limit using quantum probes subject to Markovian noise, assuming that noiseless ancilla systems are available, and that fast, accurate quantum processing can be performed. When the sufficient condition is satisfied, the quantum error-correcting code achieving the best possible precision can be found by solving a semidefinite program. We also show that noiseless ancilla are not needed when the signal Hamiltonian and the error operators commute. Finally we provide two explicit, archetypal examples of quantum sensors: qubits undergoing dephasing and a lossy bosonic mode.

Coauthors: Sisi Zhou, David Layden, Mengzhen Zhang, Wojciech Grecki, Paola Cappellaro, Rafal Demkowicz-Dobrzanski, John Preskill

*liang.jiang@uchicago.edu

Experimental multi-level quantum teleportation

Xiao-Min Hu,* Chao Zhang,* Bi-Heng Liu,† Yun-Feng Huang, Chuan-Feng Li,‡ and Guang-Can Guo
CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, People's Republic of China and CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, 230026, People's Republic of China

Quantum teleportation provides a way to transmit unknown quantum states from one location to another via previously shared quantum entanglement and classical communications. Teleportation of various physical systems has been completed in experiments, focusing on qubit systems and continuous variables. However, in the quantum world, multi-level systems are more prevalent. Here, we demonstrate the teleportation of multi-level states of a single photon in a three-dimensional six-photon system. We exploit the path mode of a single photon as the multi-level system, use two auxiliary entangled photons to realize a deterministic three-dimensional Bell state measurement. We teleport three-level states to another photon assisted by pre-shared entangled two-photon three-level states and classical communications. The teleportation fidelities are all above 0.630, and obviously exceed the classical limit 0.5. Our work paves the way to rebuild complex quantum systems remotely and to construct complex quantum networks.

Quantum teleportation [1] enables the rebuilding of arbitrary unknown quantum states without the transmission of a real particle. Previous efforts have shown the capability to rebuild qubit states [2–8] and continuous variable states [9–12]. Recent work has also demonstrated the capability of teleporting multiple degrees of freedom of a single photon [13]. However, to teleport quantum states of a real particle, for example, a single photon, one needs to consider not only the two-level states (polarization), but also those multi-level states. For example, the orbital angular momentum [15, 16], the temporal mode [17], the frequency mode [18] and the spatial mode [19, 20] of a single photon are all natural attributes of multi-level states, which are exploited as high-dimensional systems. However, to teleport multi-level quantum states is still a challenge for two reasons. One is the generation of high-quality multi-level entanglement feasible for quantum teleportation. There has been much work on high-dimensional entanglement generation [15–20], including attempts to observe interference between different high-dimensional entangled pairs [21, 22]. Nevertheless, the interference visibility between different pairs is still quite low at 63.5%. The other concerns performing a deterministic high-dimensional Bell state measurement (HDBSM). Here, we use the spatial mode (path) to encode the three-level states that has been demonstrated to extremely high fidelity [20] and use an auxiliary entangled photon pair to perform the HDBSM. We thereby overcome these obstacles and demonstrate the teleportation of a three-level (three-dimensional) quantum state using the spatial mode of a single photon [23–25]. See all the technical details in [26].

[1] Bennett, C. H. *et al.* Teleporting an unknown quantum state via dual classic and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895-1899 (1993).
[2] Bouwmeester, D. *et al.* Experimental quantum teleportation. *Nature* **390**, 575-579 (1997).
[3] Nielsen, M. A., Knill, E. & Laflamme, R. Complete quantum teleportation using nuclear magnetic resonance. *Nature* **396**, 52-55 (1998).
[4] Fattal, D., Diamanti, E., Inoue, K. & Yamamoto, Y. Quantum teleportation with a quantum dot single photon source. *Phys. Rev. Lett.* **92**, 037904 (2004).
[5] Barrett, M. D. *et al.* Deterministic quantum teleportation of atomic qubits. *Nature* **429**, 737-739 (2004).
[6] Riebe, M. *et al.* Deterministic quantum teleportation with atoms. *Nature* **429**, 734-737 (2004).
[7] Sherson, J. F. *et al.* Quantum teleportation between light and matter. *Nature* **443**, 557-560 (2006).
[8] Olmschenk, S. *et al.* Quantum teleportation between distant matter qubits. *Science* **323**, 486-489 (2009).
[9] Furusawa, A. *et al.* Unconditional quantum teleportation. *Science* **282**, 706-709 (1998).
[10] Takei, N., Yonezawa, H., Aoki, T. & Furusawa, A. High-fidelity teleportation beyond the no-cloning limit and entanglement swapping for continuous variables. *Phys. Rev. Lett.* **94**, 220502 (2005).
[11] Yonezawa, H., Braunstein, S. L. & Furusawa, A. Experimental demonstration of quantum teleportation of broadband squeezing. *Phys. Rev. Lett.* **99**, 110503 (2007).
[12] Lee, N. *et al.* Teleportation of nonclassical wave packets of light. *Science* **332**, 330-333 (2011).
[13] Wang, X.-L. *et al.* Quantum teleportation of multiple degrees of freedom in a single photon. *Nature* **518**, 516-519 (2015).
[14] Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S. L. Advances in quantum teleportation. *Nat. Photon.* **9**, 641-652 (2015).

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

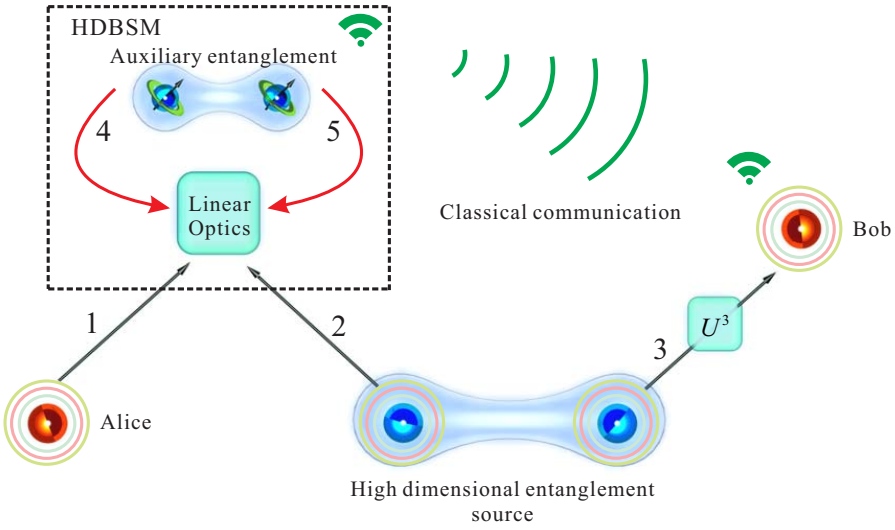


FIG. 1. **Scheme for quantum teleportation of the multi-level states of a single photon.** Alice wishes to teleport the multi-level (three-dimensional) quantum state of single photon 1 to Bob. Initially, Alice and Bob share a three-dimensional entangled photon pair 2–3. Then, Alice performs a high-dimensional Bell state measurement (HDBSM) assisted by another entangled photon pair 4–5 and sends the results to Bob through a classical channel. Finally, according to the results of HDBSM, Bob applies the appropriate three-dimensional Pauli operations on photon 3 to convert it into the original state of photon 1.

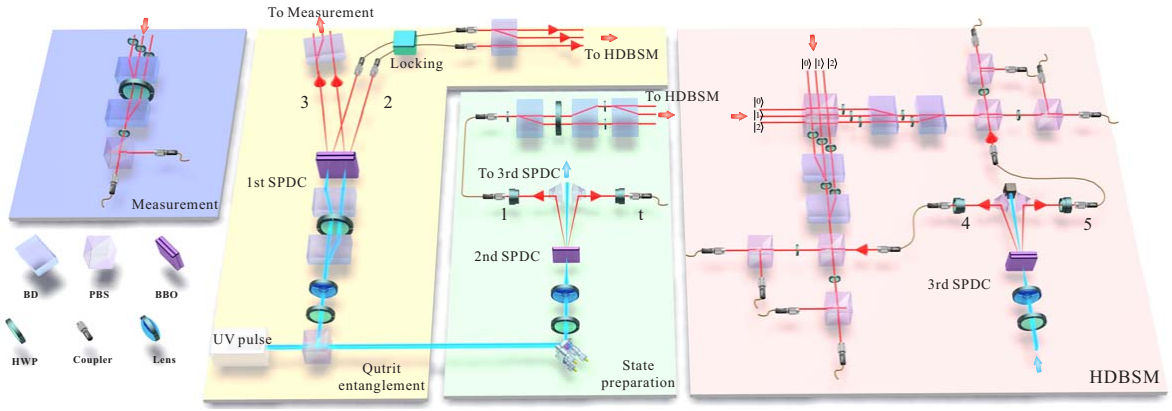


FIG. 2. **Experimental setup for teleporting a qutrit state of a single photon.** A pulsed ultraviolet (UV) laser is focused on three sets of β-barium borate (BBO) crystals and produces three photon pairs in 2–3, 1–t, and 4–5. The first pair, 2–3, is qutrit-qutrit entanglement in path DOF shared by Alice and Bob. The second pair, 1–t, photon 1 is initialized in various states ($|\varphi_1\rangle - |\varphi_{10}\rangle$) to be teleported, triggered by its twisted photon t. The third pair, 4–5, is a polarization-entangled state, used as an ancillary pair for performing a HDBSM on photons 1 and 2. BD-beam displacer, PBS-polarizing beam splitter, HWP-half wave plate.

[15] Dada, A. C., Leach, J., Buller, G. S., Padgett, M. J. & Andersson, E. Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities. *Nat. Phys.* **7**, 677-680 (2011).

[16] Krenn, M. *et al.* Generation and confirmation of a (100 x 100)-dimensional entangled quantum system. *Proc. Natl. Acad. Sci. U.S.A.* **111**, 6243-6247 (2014).

[17] Martin, M. *et al.* Quantifying photonic high-dimensional entanglement. *Phys. Rev. Lett.* **118**, 110501 (2017).

[18] Kues, M. *et al.* On-chip generation of high-dimensional entangled quantum states and their coherent control. *Nature* **546**, 622-626 (2017).

[19] Schaeff, C., Polster, R., Huber, M., Ramelow, S., & Zeilinger, A. Experimental access to high-dimensional entangled quantum systems using integrated optics. *Optica* **2**, 523-529 (2015).

[20] Hu, X.-M. *et al.* Experimental test of compatibility-loophole-free contextuality with spatially separated entangled qutrits. *Phys. Rev. Lett.* **117**, 170403 (2016).

[21] Erhard, M., Malik, M., Krenn, M., & Zeilinger, A. Experimental Greenberger-Horne-Zeilinger entanglement beyond qubits. *Nat. Photon.* **12**, 759-764 (2018).

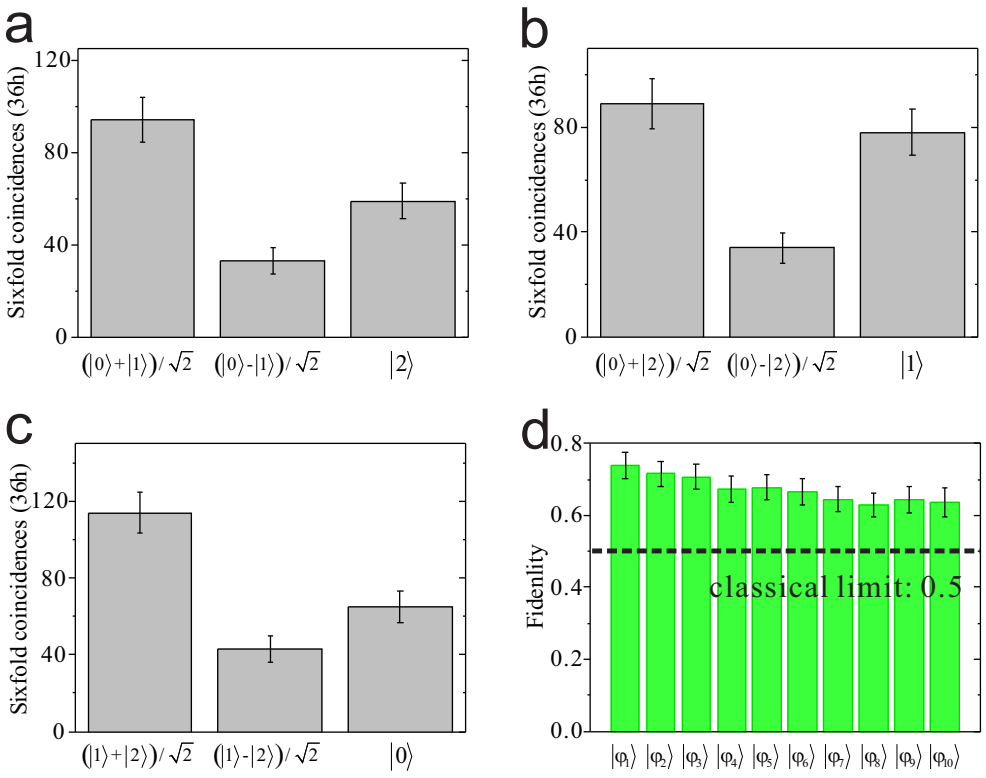


FIG. 3. Experimental results for quantum teleportation of the state $(|0\rangle + |1\rangle + |2\rangle)/\sqrt{3}$ and a summary of the teleportation fidelities for states $|\varphi_1\rangle$-$|\varphi_{10}\rangle$. To determine the fidelity of the teleported state $|\varphi_{10}\rangle$, the results for three measurement settings are required: that for **a**, $(|0\rangle \pm |2\rangle)/\sqrt{2}$, $|1\rangle$, **b**, $(|0\rangle \pm |2\rangle)/\sqrt{2}$, $|1\rangle$, and **c**, $(|1\rangle \pm |2\rangle)/\sqrt{2}$, $|0\rangle$. These settings are used to measure expectation values of the Pauli operators in two-dimensional subspaces. To reduce the statistical error, we took measurements for 36 hours for each setting. **d**, summary of teleportation fidelities for states $|\varphi_1\rangle$-$|\varphi_{10}\rangle$.

[22] Malik, M. *et al.* Multi-photon entanglement in high dimensions. *Nature Photon.* **10**, 248-252 (2016).

[23] Hu, X.-M. *et al.* Beating the channel capacity limit for superdense coding with entangled ququarts. *Sci. Adv.* **4**, eaat9304 (2018).

[24] Hu, X.-M. *et al.* Observation of stronger-than-binary correlations with entangled photonic qutrits. *Phys. Rev. Lett.* **120**, 180402 (2018).

[25] Zhang, C. *et al.* Experimental Greenberger-Horne-Zeilinger-type six-photon quantum nonlocality. *Phys. Rev. Lett.* **115**, 260402 (2015).

[26] XM Hu, C Zhang, BH Liu, YF Huang, CF Li, GC Guo, Experimental multi-level quantum teleportation, *arXiv*:1904.12249 (2019).

Zero-tradeoff multi-parameter estimation from multiple Heisenberg uncertainty relations

Zhibo Hou,[1,2,*] Jun-Feng Tang,[1,2,*] Haidong Yuan,[3,†]
Guo-Yong Xiang,[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, P. R. 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 Mechanical and Automation Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong*

(Dated: July 3, 2019)

High precision parameter estimation is one of the main driving force for science and technology. For the estimation of a single parameter, the fundamental limit, as well as the protocols to achieve it, have been extensively studied. However, for practical applications, such as imaging and spectroscopy, there are typically multiple parameters, for which the fundamental limits remain elusive. It is a wide belief that tradeoffs are unavoidable for the estimation of multiple parameters whose generators do not commute with each other. Here by relating the precision limit directly to the Heisenberg uncertainty relation we show that to achieve the highest precisions for multiple parameters simultaneously is fundamentally equivalent to saturate multiple Heisenberg uncertainty relations at the same time. Guided by this insight, we experimentally demonstrate that, contrary to the wide belief, the highest precisions for the estimation of all three parameters in SU(2) operators can be achieved simultaneously. With eight optimally designed controls, we achieve a 13.8 dB improvement over the shot-noise limit. Our work not only deepens the connection between quantum metrology and the Heisenberg uncertainty relation, but also marks a crucial step towards achieving the ultimate precision of multi-parameter quantum estimation, which has wide implications in magnetometry, quantum gyroscope, quantum reference frame alignment,etc.

One distinct feature of multi-parameter quantum estimation is the tradeoff among the precisions of different parameters, as the optimal strategy to achieve the highest precision for each parameter can be different and incompatible. A wide belief is that the tradeoffs are unavoidable for the estimation of different parameters that have noncommuting generators[1–7]. In particular it is believed that the tradeoff is unavoidable for the estimation of the three parameters in the $SU(2)$ operators, which itself is also a fundamental problem in quantum metrology as it arises frequently in many practical applications, such as quantum gyroscope, quantum reference frame alignments, quantum sensing, etc. Here by experimentally demonstrating the zero-tradeoff estimation for the three parameters in the $SU(2)$ operators we show the contrary to the shared belief.

A general operator in $SU(2)$ can be written as $U_s = e^{-\mathrm{i}\alpha \boldsymbol{n}\cdot\boldsymbol{\sigma}}$ with $\boldsymbol{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ and $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ are the Pauli operators. The three parameters that charaterize the operator are $\alpha \in [0, \pi/2], \theta \in [0, \pi]$ and $\phi \in [0, 2\pi)$, which are the parameters to be estimated in our dynamically controlled scheme as shown in Fig. 1 **a**. For the estimation of a single parameter, the precision is limited by the parameter-based uncertainty relation as [8, 9]

$$\delta\hat{x}^2 \langle \Delta H_x^2 \rangle \geq \frac{1}{4}, \tag{1}$$

where $x \in \{\alpha, \theta, \phi\}$, $\delta\hat{x}^2$ is the variance of the estimator, $\langle \Delta H_x^2 \rangle = \langle \Psi_x | H_x^2 | \Psi_x \rangle - \langle \Psi_x | H_x | \Psi_x \rangle^2$ is the variance of H_x with $H_x \equiv \mathrm{i}(\partial_x U_s) U_s^\dagger$ as the corresponding generator of the parameter[9]. This limit is fundamentally related the general Heisenberg uncertainty principle(see Methods).

The three generators H_α, H_θ and H_ϕ do not commute with each other. To achieve the best precision for each parameter, one should maximize the variance of the corresponding generator. For the three parameters, α, θ, and ϕ, the variance of their generators are bounded respectively as

$$\langle \Delta H_\alpha^2 \rangle \leq 1, \quad \langle \Delta H_\theta^2 \rangle \leq \sin^2\alpha, \quad \langle \Delta H_\phi^2 \rangle \leq \sin^2\alpha \sin^2\theta. \tag{2}$$

These upper bounds can be saturated separately by choosing the corresponding optimal states. The condition for an observable, denoted as O, to achieve the minimal uncertainty in Inequality (1) for a particular parameter is

$$(H_x - \langle H_x \rangle)|\Psi_x\rangle = \mathrm{i}\gamma(O - \langle O \rangle)|\Psi_x\rangle, \tag{3}$$

where γ is arbitrary real scalar[10]. For each particular parameter, by performing the projective measurement on the eigenvectors of such O, the minimum $\delta\hat{x}$ can be achieved(See Methods).

If N copies of the operator can be used in each time, the architecture of arranging the N operators also needs to be optimized. The variance of the generator for N operators is always upper bounded as

$$\langle \Delta \left[H_x^{(N)} \right]^2 \rangle \leq N^2 \langle \Delta H_x^2 \rangle, \tag{4}$$

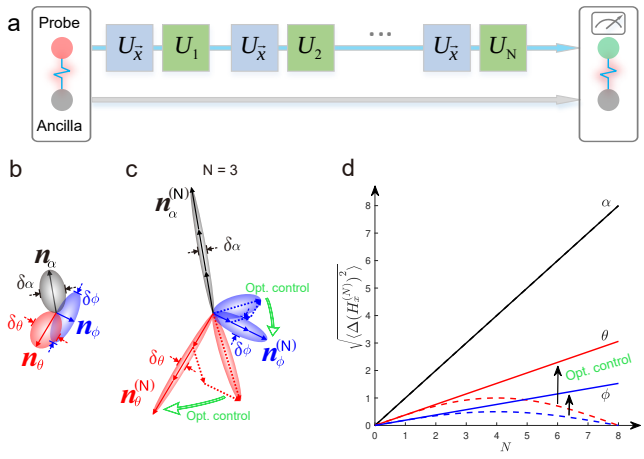


FIG. 1. Control-enhanced sequential simultaneous measurement: **a** Sequential scheme with controls. The system qubit is maximally entangled with an ancilla and operated by N copies of a multi-parameter channel sequentially with controls inserted in between and maximally entangled measurements are performed on the system-ancilla state to measure all parameters simultaneously. **b** Generators of one operator U_s. The Bloch vectors of the three generators, $\boldsymbol{n}_x$ with $x \in \{\alpha, \theta, \phi\}$ are plotted with the length represents its maximal variance. The width in the other direction of the ellipsoid is the minimum variance of the parameter. **c** Generators with N copies of operators ($N = 3$ in **c**). Without the controls, due to the noncommutativity the length of the generators do not all increase linearly with N, but with the optimally designed controls, the length of all three generators increase linearly with N thus minimizing the uncertainty of the corresponding parameters simultaneously. **d** The variances of the three generators with respect to N. While the variance of the generator for α increases linearly with N even without control, the variances of the generators for θ and ϕ increase linearly with N only with the optimally designed control.

which corresponds to the Heisenberg limit of the estimation,

$$\delta\hat{x}^2 \geq \frac{1}{N^2\langle \Delta H_x^2\rangle}. \tag{5}$$

When the procedure is repeated m times, this gives a lower bound on the minimal variance of the estimation as $\delta\hat{x}^2 \geq \frac{1}{mN^2\langle \Delta H_x^2\rangle}$. For each parameter, this lower bound can always be saturated. To achieve these minimal variance for all parameters simultaneously, however, may not be possible, as the conditions for saturating the inequalities are typically different for different parameters. The minimal variance can be achieved simultaneously only if the optimal probe states and the optimal architecture of arranging the N operators are the same for all parameters and the optimal measurements for different parameters are compatible, which is generally believed to be impossible. For example, under the common parallel scheme where N qubits are prepared in a large entangled state with each qubit go through one operator, it is not possible to achieve the minimal variance for all three parameters of the $SU(2)$ operators simultaneously[6]. A wide belief is that the tradeoffs are unavoidable when the generators of the parameters are noncommuting.

Here we implement a dynamically controlled sequential scheme. In this scheme the N operators, U_s, are arranged sequentially where additional controls, U_c, can be inserted in between (see Fig. 1**a**). The total evolution is then U_{cs}^N with $U_{cs} = U_c U_s$. Under this evolution, the generators for the parameters are

$$H_x^{(N)} = \mathrm{i}\left(\partial_x U_{cs}^N\right)\left(U_{cs}^N\right)^\dagger = \sum_{k=0}^{N-1} U_{cs}^k H_x \left(U_{cs}^k\right)^\dagger. \tag{6}$$

The Heisenberg limit in Inequality (4) can be easily obtained with the above equation where the bound is saturated when U_{cs} commute with H_x. As shown in Fig. 1**c,d**, without controls(which corresponds to $U_c = I$), the variance of the generator for θ or ϕ cannot saturate the upper bound in Inequality (4) since U_s do not commute with H_θ or H_ϕ. However, if additional controls are available, one can find proper controls to make $U_c U_s$ commute with H_x, then $H_x^{(N)} = NH_x$, the bound in Inequality (4) is then saturated. To simultaneously achieve the minimal variance of all three parameters, the same control needs to work for all three parameters, i.e., the control should make $U_c U_s$ commute with all three generators H_α, H_θ and H_ϕ. Such control actually exists. Specifically we can choose $U_c = U_s^\dagger$, in this case $U_c U_s = I$, which commutes with all generators. However, as the parameters are not known a-priori, this control can only be implemented adaptively as $U_s(\hat{\alpha}, \hat{\theta}, \hat{\phi})$ with $\hat{\alpha}$, $\hat{\theta}$, $\hat{\phi}$ as the estimators obtained from previous data. In the asymptotical limit the upper bound in Inequality (4) can be saturated simultaneously for all three parameters with noncommuting generators. Additionally with an ancillary qubit, the optimal probe state for each parameter can all be taken as the maximally entangled state, and the optimal O satisfying Eq. (3) for different parameters are compatible.

The experiment consists of three modules: preparing the optimal probe state, implementing the optimal control and performing the optimal measurement. The probe state is first prepared as the maximally entangled state, $\frac{1}{\sqrt{2}}(|H, up\rangle + |V, down\rangle)$, with one qubit encoded in the polarization degree of the photon with the Horizontal (H) and vertical (V) polarization as the basis and the other qubit encoded in the path degree of the photon with the up and down path as the basis. The polarization qubit then goes through the unknown operator, U_s, and the control, U_c, sequentially for N times. The optimal control is chosen as $U_c = U_s^\dagger(\hat{\alpha}, \hat{\theta}, \hat{\phi})$ and updated adaptively with collected data. A projective measurement on the common eigenvectors of three commuting observables, $\sigma_3\sigma_2, \sigma_1\sigma_3$ and $\sigma_2\sigma_1$, which are optimal for the estimation of the three parameters, are performed.

In the first set of experiments, the parameters are as-

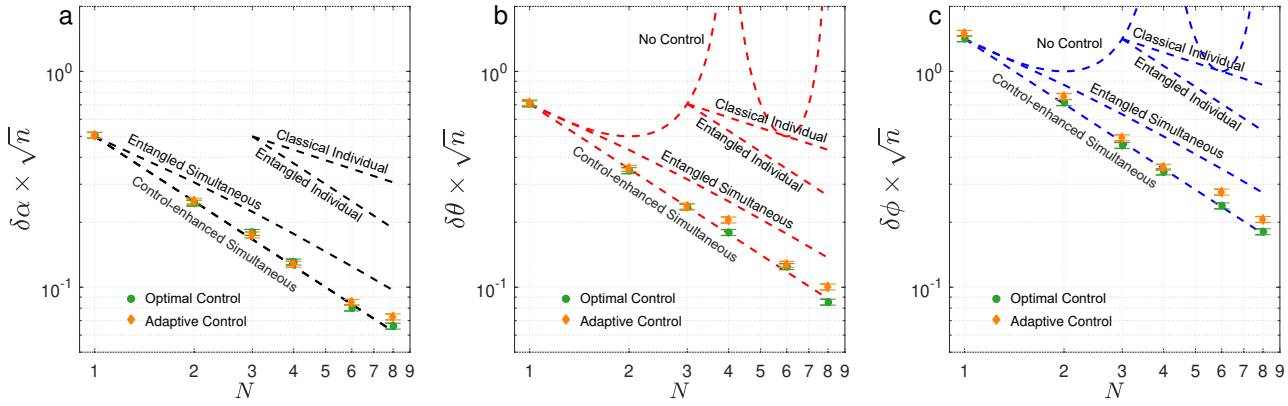


FIG. 2. Experimental results of the control-enhanced sequential simultaneous estimation with the theoretical performances of the classical individual, entangled individual (with $N \geq 3$) and entangled simultaneous estimation(see Supplementary Material for these schemes) plotted for comparison. The three plots **a**, **b** and **c** are the experimental results for U_s with $\alpha = \frac{\pi}{4}$ and $\theta = \phi = \frac{\pi}{6}$. For the experiments with the optimal controls, each measurement is repeated with 1000 times to get one estimate and this process is repeated 1000 times. The standard deviation of the estimation is then obtained from the 1000 estimates. For the experiments with the adaptive controls, each measurement is repeated 250 times during each step of the four-step adaptive process, an estimate is obtained after the same 1000 number of measurements(the estimation is obtained with all measurement results obtained during the four steps). This four-step adaptive process is then similarly repeated for 1000 times to get 1000 estimates, from which we obtain the standard deviation of the estimate. The analyze of the error bars is given in Methods.

sumed to be within a small neighborhood of known values and the adaptive controls are designed with this prior information. A unitary operator is considered with $\alpha = \frac{\pi}{4}$ and $\theta = \phi = \frac{\pi}{6}$. It can be seen in Fig. 2, the experiment reaches the theoretical optimal precision for the three parameters simultaneously, which is $\frac{3N}{N+2}$ times better than the best value achievable under the parallel scheme. This is also the best one can hope to achieve for the simultaneous estimations of all the parameters as the precision of each parameter has reached the highest value. There are zero tradeoffs among the precisions of different parameters.

In the second set of experiments, we do not assume the parameters are within very small neighborhoods and adaptively update the controls after each 250 experiments and 1000 experiments are carried out in each round. The controls are randomly chosen in the first 250 experiments, and then updated based on the obtained data. In each adaptive step, we use maximum likelihood estimation, which maximizes the posterior probability based on all previous data, to update the estimation of the parameters. As shown in Fig. 2, the experiment results (diamonds) are close to the theoretical optimal values for all three parameters for the cases of $N = 1, 2, 3, 4, 6$, which indicates that the controls are already close to be optimal after 4 steps of adaptation. In the case of $N = 8$, the standard deviation of the experiment is slightly larger than the theoretical optimal value due to systematic errors, but still outperforms the theoretical optimal value for the parallel scheme with approximately 1.32-fold improvement (the ideal improvement ratio is 1.55 for comparison).

* These authors contributed equally to this work.
† hdyuan@mae.cuhk.edu.hk
‡ gyxiang@ustc.edu.cn

[1] Helstrom, C. W. & Kennedy, R. S. Noncommuting observables in quantum detection and estimation theory. *IEEE Trans. Inf. Theory* **20**, 16–24 (1974).

[2] Holevo, A. S. *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).

[3] Humphreys, P. C., Barbieri, M., Datta, A. & Walmsley, I. A. Quantum enhanced multiple phase estimation. *Phys. Rev. Lett.* **111**, 070403 (2013).

[4] Zhang, Y.-R. & Fan, H. Quantum metrological bounds for vector parameters. *Phys. Rev. A* **90**, 043818 (2014). URL `https://link.aps.org/doi/10.1103/PhysRevA.90.043818`.

[5] Baumgratz, T. & Datta, A. Quantum enhanced estimation of a multidimensional field. *Phys. Rev. Lett.* **116**, 030801 (2016). URL `https://link.aps.org/doi/10.1103/PhysRevLett.116.030801`.

[6] Szczykulska, M., Baumgratz, T. & Datta, A. Multi-parameter quantum metrology. *Advances in Physics: X* **1**, 621–639 (2016).

[7] Yuan, H. Sequential feedback scheme outperforms the parallel scheme for hamiltonian parameter estimation. *Physical review letters* **117**, 160801 (2016).

[8] Braunstein, S. L., Caves, C. M. & Milburn, G. J. Generalized uncertainty relations: Theory, examples, and Lorentz invariance. *Ann. Phys.* **247**, 135–173 (1996).

[9] Pang, S. & Brun, T. A. Quantum metrology for a general hamiltonian parameter. *Physical Review A* **90**, 022117 (2014).

[10] Griffiths, D. J. & Schroeter, D. F. *Introduction to quantum mechanics* (Cambridge University Press, 2018).

Fundamental building block for scalable photonic quantum communication

Seung-Woo Lee[1] * Timothy C. Ralph[2] Hyunseok Jeong[3]

[1] *Quantum Universe Center, Korea Institute for Advanced Study, Seoul 02455, Korea*
[2] *Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, St Lucia, Queensland 4072, Australia*
[3] *Center for Macroscopic Quantum Control, Department of Physics and Astronomy, Seoul National University, Seoul 08826, Korea*

Abstract. In pursuing scalable quantum communications, naturally arising questions are thus whether or not any ultimate limit exists in all-optical scalability, and whether and how it can be achieved. Motivated by these questions, we derive the fundamental limits of the efficiency and loss-tolerance of the Bell measurement with multiple photons, restricted not by protocols but by the laws of physics, i.e. linear optics and no-cloning theorem. We then propose a Bell measurement scheme in a concatenated manner with linear optics, which enables one to reach both the fundamental limits. Remarkably, the quantum repeater based on our scheme allows one to achieve fast and efficient quantum communication over arbitrary long distances, outperforming previous all-photonic and matter-based protocols. Our work provides a fundamental building block to reach the ultimate limits of all-optical scalability and paves an alternative route towards scalable quantum networks.

Keywords: quantum communication, quantum repeater, Bell-state measurement

1 Introduction

Photons are ideal carriers for quantum communication. However, there have been two major obstacles to scalability in photonic quantum communication. One is *'photon loss'* during transmission. The other is *'non-deterministic Bell measurement'* with single photons. Bell measurement is an essential requirement to extend the communication range by teleportation or entanglement swapping, but its success probability with single photons cannot exceed 50% with linear optics. As a result, all-optical approaches to quantum communication has suffered from exponential scaling in time and resources with distance. To overcome these, a quantum repeater (a device to extend the communication range with polynomial scaling) has been developed. While, in its standard model, transmission losses are circumvented through heralded entanglement generation between nodes with the help of long-lived quantum memories, some recent proposals employ quantum error correction schemes with multiple photons. Quantum repeaters in this direction could enhance the performance further without use of long-lived quantum memories.

Multi-photon encoding approach hence opens the possibility of all-optical scalability, resolving both photon loss and the probabilistic nature of Bell measurement to some extent. In pursuing scalable quantum networks, possible questions that come to mind is thus (i) whether or not any fundamental limits exist in the realization of quantum communication with multiple photons, and (ii) whether and how the limits can be reached (if they exist). In this work [1], we address these questions. We derive, for the first time, the fundamental limits of all-optical scalability in quantum communication. These limits are determined not by protocols but by the laws of physics, i.e., linear optics and the no-cloning theorem. We then propose a Bell measurement scheme with linear optics and multi-photon encoding, which surpasses all the previous schemes and allows us to reach both the fundamental limits. We finally show that the quantum repeater based on our scheme enables fast and efficient quantum communication over arbitrary long distances, outperforming all the previous quantum repeater protocols. Our work provides a fundamental building block for quantum networks towards reaching the ultimate limits of all-optical scalability.

*swleego@gmail.com

2 Fundamental limits

We have derived the fundamental limits of the Bell measurement with linear optics and arbitrary N-photon encoding (see Fig. 1 and [1] for details): (i) We have proved that the success probability of the Bell measurement has the upper bound $1-2^{-N}$ by linear optics, which is the generalization of the 50% limit of the Bell measurement with single photons ($N = 1$). (ii) Then, we have shown that the loss-tolerance of Bell measurement (with any error correction scheme) is fundamentally limited by $\eta\eta' > 0.5$ due to the no-cloning theorem, when two input qubits experience losses with rate η and η'. These two limits not only determine the ultimate limit of all-optical scalability in quantum communication but also are valid for any photonic quantum information processing.

3 Concatenated Bell measurement

We then propose a Bell measurement scheme with linear optics and multi-photon encoding in a concatenated manner in Fig. 2, referred to as *concatenated Bell measurement* (CBM). In our approach, the logical basis $|0_L\rangle = |+^{(m)}\rangle^{\otimes n}$ and $|1_L\rangle = |-^{(m)}\rangle^{\otimes n}$, where $|\pm^{(m)}\rangle = |H\rangle^{\otimes m} \pm |V\rangle^{\otimes m}$ are used. Each logical qubit contains n

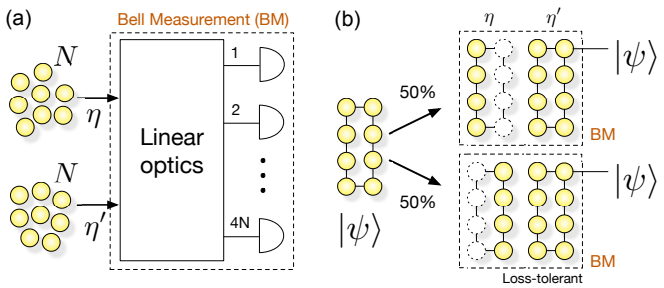


Figure 1: (a) General Bell measurement setup with linear optics and N-photon encoding. (b) If any Bell measurement were able to tolerate 50% (or more) loss of photons, i.e., $\eta\eta' \leq 0.5$, it would violate the no-cloning theorem.

blocks of m (total $N = nm$) photons. The logical Bell states, $|\Phi^{\pm}\rangle = |0_L\rangle|0_L\rangle \pm |1_L\rangle|1_L\rangle$ and $|\Psi^{\pm}\rangle = |0_L\rangle|1_L\rangle \pm |1_L\rangle|0_L\rangle$, can be completely decomposed into the block size Bell states, $|\phi^{\pm}_{(m)}\rangle = |+^{(m)}\rangle|+^{(m)}\rangle \pm |-^{(m)}\rangle|-^{(m)}\rangle$ and $|\psi^{\pm}_{(m)}\rangle = |+^{(m)}\rangle|-^{(m)}\rangle \pm |-^{(m)}\rangle|+^{(m)}\rangle$, which are also completely decomposed into the Bell states with photon pair, $|\phi^{\pm}\rangle = |+\rangle|+\rangle \pm |-\rangle|-\rangle$ and $|\psi^{\pm}\rangle = |+\rangle|-\rangle \pm |-\rangle|+\rangle$ [1]. We denote the logical, block size, photon pair Bell states as the 2nd, 1st, 0th level Bell states, respectively. The Bell states in higher levels can be fully characterized by the type and number of lower level Bell states that appear in the decomposition (see Table 1). CBM enables one to discriminate Bell states near-deterministically and loss-tolerantly, outperforming all other proposals with respect to the attained success probability with given number of photons and loss rate, and is the first and so far the only Bell measurement saturating both fundamental limits by optimization (see Bottom of Fig. 2). This can be implemented by the standard linear-optic Bell measurement scheme and feedforwards.

Table 1: **Bell states decomposition**

Level	Bell states	Decomposed into
2nd (logical)	$\|\Phi^{+(-)}\rangle$	even(odd) number of $\|\phi^{-}_{(m)}\rangle$, and $\|\phi^{+}_{(m)}\rangle$ for others
	$\|\Psi^{+(-)}\rangle$	even(odd) number of $\|\psi^{-}_{(m)}\rangle$, and $\|\psi^{+}_{(m)}\rangle$ for others
1st (block)	$\|\phi^{+(-)}_{(m)}\rangle$	even number of $\|\psi^{+(-)}\rangle$, and $\|\phi^{+(-)}\rangle$ for others
	$\|\psi^{+(-)}_{(m)}\rangle$	odd number of $\|\psi^{+(-)}\rangle$, and $\|\phi^{+(-)}\rangle$ for others

4 Scalable quantum communication

We then construct a building block of long distance quantum communications (either for transmitting information along the network or for distributing entanglement across the network) based on CBM as illustrated in Fig. 3(a). Our repeater model in Fig. 3(b) does not require long-lived quantum memories, photon-matter interactions, nor complicated circuit operations. Each photon survives with probability $\eta_L = \eta_0 e^{-L/L_{att}}$ in one cycle of

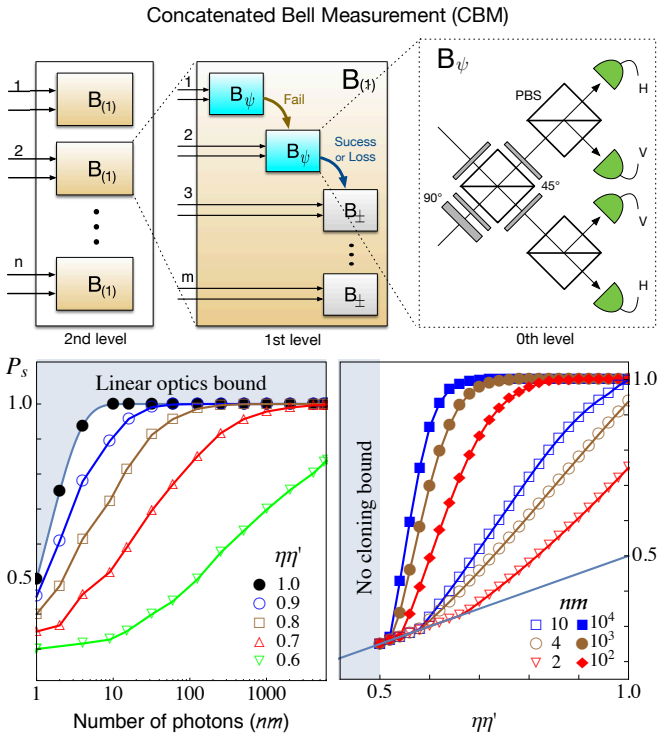


Figure 2: Concatenated Bell measurement scheme. The (logical) 2nd level is composed of n independent $\mathrm{B}_{(1)}$, each of which is performed with m-times of $\mathrm{B}_{(0)} = \{\mathrm{B}_{\psi}, \mathrm{B}_{+}, \mathrm{B}_{-}\}$ (three variations of the standard Bell measurement) with feedforwards. Bottom: The maximum success probability P_s of CBM for $N = nm$ and $\eta\eta'$.

the generation, transmission (over distance L), and measurement process, where η_0 is the loss rate during the stationary process in the repeater. The total distance L between Alice and Bob is divided into L_0 by equally spaced nodes. The success probability of each building block is thus $P_s(\eta_{L_0}, \eta_0)$, and the total success probability of transmission can be obtained by $P_s(\eta_{L_0}, \eta_0)^{L/L_0} \equiv Rt_0$, where R is the transmission rate and t_0 is the time taken in the repeater. The maximum transmission probabilities over 1,000 and 10,000 km are plotted in Fig. 4. It shows that arbitrarily high success probability approaching to unit (≈ 1) can be attained by increasing the encoding size $N = nm$.

We optimize our protocol for the total cost of photons $Q = 2nmL/Rt_0L_0$ to be minimized. The optimized results by numerical searches over $\{n, m, j, L_0\}$ with exemplary parameters are presented in Table 2. For example, for the transmission over 1,000 km (when $\eta_0 = 0.93$), the best choice of encoding parameters and the repeater spacing are $(n, m, j) = (58, 8, 1)$ and $L_0 = 1.8$ km, by which $Rt_0 \sim 0.7$ can be achieved with total $Q_{\min} = 7.38 \times 10^5$ photons. The overall transmission fidelity is estimated as $F = 0.96$ by assuming depolarizing errors. The transmission rate R is determined by the processing time t_0 in the repeater. We first assume that the slowest component in the repeater is the measurement process, and it takes $t_0 = 10$ μs (1 μs) (for fair comparison with [2, 3]). Our protocol then achieves $R \sim 70$ KHz (0.7

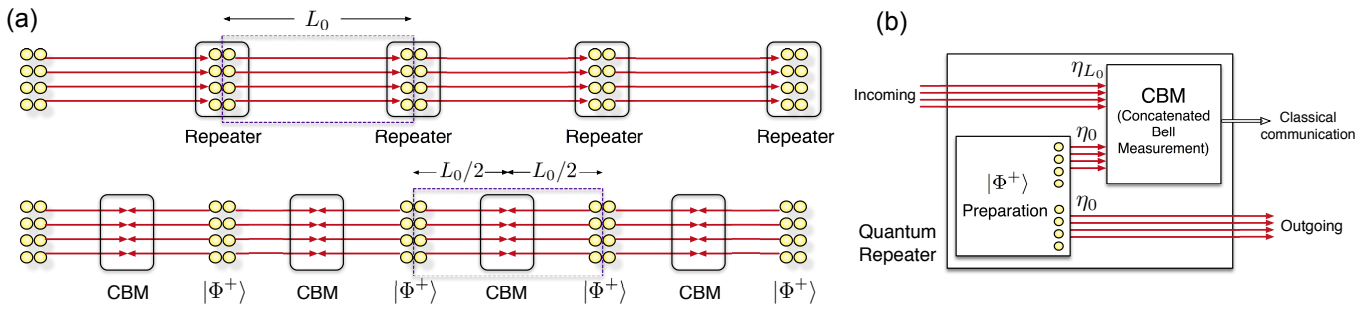


Figure 3: Schematic of building blocks for quantum network. (a) Two designs of building blocks for quantum networks: (Top) for one-way communication to transmit quantum information along the network, in which the qubit carrying information travels L_0 between repeater nodes. The other qubit is staying in the repeater. Then, CBM is performed on the transmitted and stationary qubits. (Bottom) for entanglement distribution between remote places, in which CBM is performed to link the entangled pairs $|\Phi^+\rangle$ from adjacent nodes. Each qubit travels $L_0/2$ to meet in the middle before CBM. (b) A quantum repeater for one-way communication is composed of two parts: the preparation of entangled pair $|\Phi^+\rangle$ and CBM on two qubits (one is received from the previous node and the other from $|\Phi^+\rangle$). The other qubit of $|\Phi^+\rangle$ is transmitted to the next node. The result of CBM is directly sent to Bob via classical communication. Losses during preparation and measurement process also affect the performance. The effective loss rate of photons inside of the repeater is referred as η_0, estimated with source efficiency ϵ_s, detector efficiency ϵ_d, and the loss during the generation time of $|\Phi^+\rangle$.

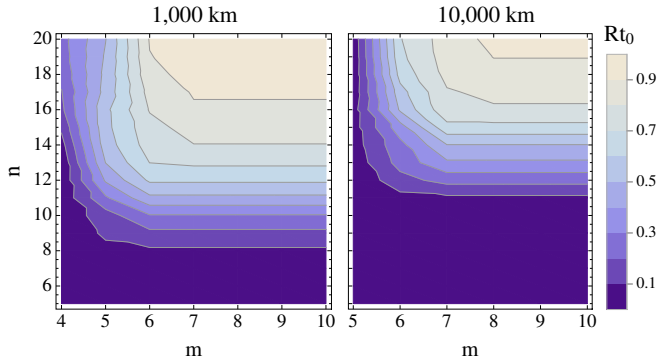


Figure 4: Maximum transition probability Rt_0 over 1,000 (10,000) km with repeater spacing L_0 =1.7 (1.2) km, and 1% inefficiency in each repeater ($\eta_0 = 0.99$). The red circle indicates the optimal choice for minimum cost..

MHz) for 1,000 km transmission (almost the same for 10,000 km). Compared to the standard repeater, it is at least 5 to 6 order of magnitude faster. It also outperforms all the recent advanced matter-based [2] and all-optical [3] protocols; it costs an order of magnitude less ($\sim 18\%$) photons to achieve near the best performance of those protocols, or yields almost unit transmission probability with similar cost. Ultrafast communications with rates up to or beyond GHz may also be expected along with the progress of on-demand entangled photon sources and (sub)nanosecond feedforward technologies.

5 Remarks

Our work addresses both the limits and potentials of all-optical scalability as an alternative route towards long distance quantum communication. While the conventional route based on the standard quantum repeater relies more on the development of the platforms for light-matter interaction and long-lived quantum memories, our approach puts more weight on the photon source technologies. The major challenge of our protocol is the preparation of large, multi-photon entangled encoded states. The recent progress of the technologies of on-demand photon sources and platforms with integrated optics may enhance its feasibility. We also emphasize that our result is not limited to all-optical quantum communication but generally applicable and valid for any photonic quantum information protocols.

Table 2: Optimal strategies to minimize the total cost: η_0 denotes the loss rate in the repeater, Rt_0 and F are the overall transmission probability and fidelity, (n, m, j) and L_0 are the optimal encoding and repeater spacing.

L(km)	η_0	$Q_{\min}$	Rt_0	F	(n, m, j)	L_0
1,000	0.99	1.3e5	0.70	0.98	(13, 6, 2)	1.7
	0.93	7.4e5	0.70	0.96	(58, 8, 1)	1.8
10,000	0.99	2.4e6	0.77	0.97	(16, 7, 2)	1.2
	0.93	1.9e7	0.70	0.92	(92, 10, 2)	1.4

References

[1] S.-W. Lee, T. C. Ralph, and H. Jeong, arXiv.1804.09342

[2] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, Nature Photonics **6**, 777–781 (2012).

[3] K. Azuma, K. Tamaki, and H.-K. Lo, Nature Communications **6**, 6787 (2015).

XY-model: Analytical and Numerical Results for Quantum Algorithms

Zhihui Wang[1 2 *] Nicholas C. Rubin[3 4] Jason M. Dominy[5] Eleanor G. Rieffel[1]

[1] *Quantum Artificial Intelligence Laboratory (QuAIL), NASA Ames Research Center, Moffett Field, CA 94035*
[2] *Universities Space Research Association, 615 National Ave, Mountain View, CA 94043*
[3] *Google Inc., 340 Main Street, Venice, CA 90291, USA*
[4] *Rigetti Quantum Computing, 775 Heinz Ave, Berkeley, CA 94710*
[5] *Department of Applied Mathematics, University of California, Santa Cruz, Santa Cruz, CA 95064*

Abstract. This presentation is based on paper arXiv:1904.09314. The Quantum Alternating Operator Ansatz (QAOA) is a promising gate-model meta-heuristic for combinatorial optimization. Applying the algorithm to problems with constraints poses a significant implementation challenge for near-term quantum resources. In this work we explore enforcing hard constraints by using XY-model Hamiltonians as mixing operators. Performance is validated on graph coloring problems. The general strategy of using XY-mixers is borne out numerically, demonstrating a significant improvement over the standard X-mixer. Despite the complexity of simulating the XY model, we demonstrate that within a relevant subspace, XY mixers can be realized in circuits of linear depth. We also specify general strategies for efficiently implementing QAOA circuits on hardware graphs of ideal (all-to-all) and realistic (limited) connectivity inspired by fermionic simulation techniques.

Keywords: quantum heuristics, QAOA, circuit depth

This presentation is based on paper arXiv:1904.09314. [16]

1 QAOA: a quantum heursitics suitable for near-term quantum hardware

While full fault-tolerant quantum computing is still in the cradle, noisy Intermediate-Scale Quantum (NISQ) [12] hardware is rapidly developing. Current gate-model quantum computing hardware features a few to a few tens of qubits, and the precision in gate implementation, without error correcting schemes built in, can only tolerate a quantum circuit of shallow depth. In spite of these issues, NISQ era hardware is not simply a bridge to the full fault-tolerant future, but is also expected to be useful in exploring applications such as simulating quantum many-body systems, solving classical optimization problems, and sampling for machine learning.

Other than the handful of algorithms with proven quantum advantage, like Grover's algorithm for search an unstructured database and Shor's algorithms for factoring, [6, 14] more general-purpose quantum heuristic algorithms have been proposed that have not yet proven speedup but hold great potential nonetheless. [1, 11, 7] Quantum approximate optimization algorithm (QAOA) [1] is one among them that has attracted significant research interest. Originally proposed for classical optimization problems, QAOA features a simple high level structure that repeats two families of parameterized unitaries, one based on the Hamiltonian that encodes the cost function itself, H_C, and the other Hamiltonian H_M, called the mixer, that generates transitions between the eigenstates of H_C. Among many important results, QAOA has been demonstrated to be able to generate a distribution hard to simulate classically, [4] has inspired a better classical algorithm for certain combinatorial optimization problems, [2], has been studied for approximate solutions to MAXCUT [1, 15, 18], network detection [13], simple machine learning models [5, 10] and sampling [4], has been adapted with different quantum hardware in mind, has been generalized to the Quantum Alternating Operator Ansatz (QAOA) that aims to achieve a broader family of quantum states, [7] has been shown to demonstrate quantum speedup on Grover's problem, [8] and has been proved with well-chosen parameters to be equivalent to universal quantum computing. [9] These studies suggest that there is a path forward to obtaining high quality solutions with QAOA under a noiseless environment. The variational nature of this algorithm implies that noise of physical qubits can be tolerated to some extent. [3, 18]

2 QAOA with XY model: a superior design for optimization problems with hard constraints

For optimization problem with hard constraints, the prototypical method in quantum annealing is to encode constraints as penalty terms in the cost Hamiltonian such that the ground state corresponds to the optimal state with no constraints violated. The method can in principle be implemented for QAOA. However, we will show in this work that the resulting algorithm is extremely inefficient, due to the lack of energy-guidance in the algorithm. [16] It also significantly resource-demanding: often the penalty terms would demand two-qubit gates between all pairs of qubits involved in the constraints. This would lead to significant increase in circuit depth on NISQ hardware, which typically has limited qubit connectivity.

Alternatively, we in this work explore a variant to the original QAOA: using as the mixer a Hamiltonian that has close ties with condensed matter physics: the

*zhihui.wang@nasa.gov

XY model. The XY coupling between two qubits, $\sigma_i^x\sigma_j^x + \sigma_i^y\sigma_j^y$, can be readily realized through the iSWAP gate, which is often considered a natural choice to include in basic gate sets since it can be naturally realized in superconducting systems. [17]

One distinctive feature of the XY interaction is that it preserves the total spin-Z component. We will show that this feature can find broad application in systems in which a subset of qubits are confined to a subspace of fixed total spin-Z. Optimization with hard constraints (i.e., equality constraints) fall in this category. For example, optimization problems with k-ary variables that need to be encoded into binary variables to perform quantum computing – in particular when the variable is encoded into a subspace of k qubits expanded by bit strings of Hamming-distance-1.

Using the graph coloring problem as an example, we first show how the XY mixer significantly outperforms the standard mixer used in QAOA, the single-qubit Pauli X. Figure 1 shows the difference in approximation ratio (a figure of merit for performance) using the two mixers for a small coloring problem. The superior performance is demonstrated numerically and explained by the fact that the XY mixer keeps the quantum evolution in a subspace defined by the constraints in the system and in dimension exponentially smaller than the full Hilbert space. In the case of k-coloring of a graph of size n, the ratio of the feasible subspace sizes to the size of the full Hilbert space is

$$\frac{\dim(\mathcal{H}_{fea})}{\dim(\mathcal{H})} = \frac{k^n}{2^{nk}} = \left(\frac{k}{2^k}\right)^n, \tag{1}$$

which for any $k \geq 1$ shrinks exponentially with the graph size n.

We also show that W state, a well-known 3-qubit entangled state, and its multi-qubit generalization, is a natural choice for the initial state of the QAOA algorithm with XY mixers, and significantly outperforms an intuitive classical initial state. Figure 2 shows such a comparison for 3-coloring of a representative graph (our benchmarking set include 64 and 475 many 3-colorable connected graphs of size 6 and 7 respectively.)

3 Circuit design and compilation of XY models: on ideal and realistic hardware

When a quantum algorithm is executed on hardware, it needs to be broken into single-qubit gates and a given (by hardware design) set of two-qubit gates. To fully realize the theoretical advantage of using XY model for QAOA, circuit complexity for realizing the XY interactions among the relevant subset of qubits needs to be evaluated. Furthermore, NISQ hardware often does not have all-to-all connectivity to facilitate all 2-qubit gates required by the algorithm, hence SWAP gates are needed and quantum compilation needs to be performed to minimize the duration of the final circuit on hardware. In this talk we also describe how to implement the various components of QAOA into short depth circuits, on hardware

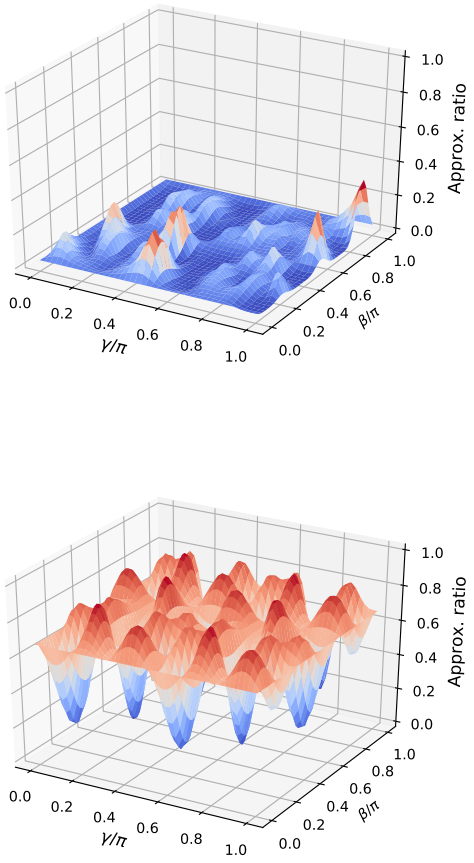


Figure 1: Significantly improved performance for level-1 $QAOA$ on the problem of 3-coloring of a triangle graph using XY mixer (Bottom) compared to (Top) standard QAOA using the X mixer.

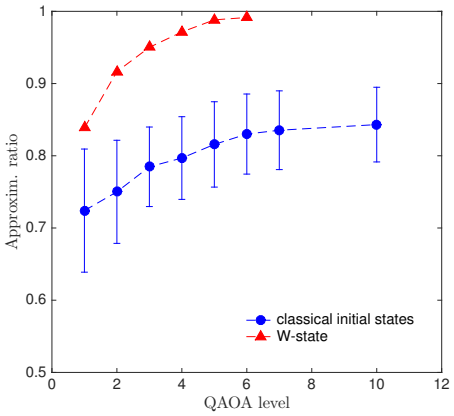


Figure 2: The expected value of QAOA optimized over the parameter sets. Triangles show the results with W-state as initial states. Circles show the results with a feasible classical initial state, averaged over the set of all feasible classical states, the error bar is the standard deviation. For each initial state, optimization over angles are derived from a basin-hopping search.

with ideal (all-to-all) and realistic (limited) connectivity. The major results are highlighted as the following.

- Most notably, on an all-to-all connected hardware platform, we propose a scheme that can generate the exact evolution of the XY-model on a complete graph in linear depth.
- Exploiting the fermionic transformation, we show that the XY model on a ring can be realized in logarithmic depth.
- Due to the commuting nature of the cost Hamiltonians, a SWAP-network, akin to sorting networks, can be used to implement any 2-local cost operator requiring all-to-all connectivity in linear depth on a linearly connected graph of qubits.
- Although the XY-mixer is significantly more complicated than the standard X-mixer, we demonstrate that under numerous scenarios this driver term can be implemented in linear depth by taking a fermionic perspective.
- If approximate evolution of the XY unitary is found to be tolerable, for all-to-all connected architectures, the first-order Trotter implementation of the XY-mixer drops to logarithmic circuit depth.

In summary, We numerically demonstrate and theoretically motivate that the XY Hamiltonian is a natural choice for QAOA on optimization problems with hard constraints. We provide circuit design for efficiently realizing the XY mixers on ideal and realistic hardware layout.

This work establishes the possibility of using more sophisticated mixers in a QAOA framework for naturally enforcing constraints. Our analysis will be helpful for near-term experimental validations of the QAOA algorithm and evaluating its merit for real-world optimization problems.

References

[1] E. Farhi, J. Goldstone, and S. Gutmann. A quantum approximate optimization algorithm. *arXiv preprint arXiv:1411.4028*, 2014.

[2] E. Farhi, J. Goldstone, and S. Gutmann. A quantum approximate optimization algorithm applied to a bounded occurrence constraint problem. *arXiv preprint arXiv:1412.6062*, 2014.

[3] E. Farhi, J. Goldstone, S. Gutmann, and H. Neven. Quantum algorithms for fixed qubit architectures. *arXiv preprint arXiv:1703.06199*, 2017.

[4] E. Farhi and A. W. Harrow. Quantum supremacy through the Quantum Approximate Optimization Algorithm. *arXiv:1602.07674*, Feb. 2016.

[5] E. Farhi and H. Neven. Classification with quantum neural networks on near term processors. *arXiv preprint arXiv:1802.06002*, 2018.

[6] L. K. Grover. A fast quantum mechanical algorithm for database search. *arXiv e-prints quant-ph/9605043*, 1996.

[7] 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. *arXiv preprint arXiv:1709.03489*, 2017.

[8] Z. Jiang, E. G. Rieffel, and Z. Wang. Near-optimal quantum circuit for Grover's unstructured search using a transverse field. *Physical Review A*, 95(6):062317, 2017.

[9] S. Lloyd. Quantum approximate optimization is computationally universal. *arXiv e-prints arXiv:1812.11075*, 2018.

[10] J. Otterbach, R. Manenti, N. Alidoust, A. Bestwick, M. Block, B. Bloom, S. Caldwell, N. Didier, E. S. Fried, S. Hong, et al. Unsupervised machine learning on a hybrid quantum computer. *arXiv preprint arXiv:1712.05771*, 2017.

[11] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O'Brien. A variational eigenvalue solver on a photonic quantum processor. *Nature Communications*, 5:4213, Jul 2014.

[12] J. Preskill. Quantum Computing in the NISQ era and beyond. *arXiv e-prints arXiv:1801.00862*, 2018.

[13] R. Shaydulin, H. Ushijima-Mwesigwa, I. Safro, S. Mniszewski, and Y. Alexeev. Network community detection on small quantum computers. *arXiv preprint arXiv:1810.12484*, 2018.

[14] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *arXiv e-prints quant-ph/9508027*, 1995.

[15] Z. Wang, S. Hadfield, Z. Jiang, and E. G. Rieffel. Quantum approximate optimization algorithm for MaxCut: A fermionic view. *Physical Review A*, 97(2):022304, 2018.

[16] Z. Wang, N. C. Rubin, J. M. Dominy, and E. G. Rieffel. XY-mixers: analytical and numerical results for QAOA. *arXiv e-prints arXiv:1904.09314*, 2019.

[17] G. Wendin. Quantum information processing with superconducting circuits: a review. *Reports on Progress in Physics*, 80(10):106001, Oct 2017.

[18] L. Zhou, S.-T. Wang, S. Choi, H. Pichler, and M. D. Lukin. Quantum approximate optimization algorithm: Performance, mechanism, and implementation on near-term devices. *arXiv preprint arXiv:1812.01041*, 2018.

Approximately recompiling NISQ circuits via energy dissipation

Tyson Jones[1] * Simon C. Benjamin[1] †

[1] *Department of Materials, University of Oxford, Parks Road, Oxford OX1 3PH, UK*

Abstract. Re-expressing noisy intermediate-scale quantum (NISQ) circuits in alternate gate sets can be essential for enforcing hardware constraints or suppressing errors. We describe a method for automatically recompiling a quantum circuit $\mathcal{A}$ into a parameterised target circuit $\mathcal{B}(\phi)$, with the goal that both circuits have the same action on a specific input, i.e. $\mathcal{B}(\phi)\,|\text{in}\rangle = \mathcal{A}\,|\text{in}\rangle$. This is of particular usefulness to hybrid, NISQ-era algorithms which involve many repetitions of imperfect, constrained circuits. Recompilation can be efficiently performed on the quantum device, or otherwise classically simulated, and is driven by a recently introduced variational imaginary-time technique [2]. We demonstrate successful recompilation of 7-qubit spin-chain simulation circuits in order to extend real-time simulation, and are currently investigating its scalability with respect to circuit size, qubit count and noise. The full manuscript is available on arXiv [1].

Keywords: NISQ, VQE, recompilation, variational algorithms, quantum simulation

Contents

1 Introduction

1.1 NISQ recompilation

In conventional computing, compilers are essential to translate programs into efficient low-level instructions for execution at the hardware level. Quantum computers will also benefit greatly from efficient compilation, but the nature of the compilation goal depends on whether the quantum machine is a near-term device or a fully fault-tolerant, code-protected quantum processor.

For the era of Noisy Intermediate Scale Quantum (NISQ) devices, the costly gates are those with the greatest error burden. Typically these are two-qubit gates (and higher degree gates) in today's prototypes, while single-qubit gates are higher fidelity [3, 4, 5, 6]. Moreover a given physical device will have certain operations that are native to it, so that e.g. it may be that a control-NOT is impossible to implement directly but is instead realised though a parity-dependent phase shift together with additional single-qubit gates. Furthermore the device will have a native connectivity: certain qubits will be able to directly link to others, for example in a two-dimensional nearest-neighbour topology or a more flexible networked architecture [7]. Thus one would wish to compile directly to the device's native gate set and connectivity.

A compiler that is capable of targeting an arbitrary family of gates could recompile from a standard 'white board' description of a circuit into a truly native format where the gate operations are bespoke for a specific device. Presently we take this idea further and suggest that one could compile into a device whose gates are an unknown function of the control parameters.

This paper describes a general method of translating one quantum circuit into another, i.e. recompiling it. The approach allows one to do the following:

- Target an arbitrary (user-specified) circuit layout,
- Target an arbitrary (user-specified) set of gates, including bespoke gates not used in analytic treatments,
- Support approximate recompilation, so that if the specified target template is too shallow for perfect recompilation then an approximate circuit will be found,
- Minimise the impact of noise (although in the present paper our examples use noise-free gates).

However the present scheme is also limited in important ways:

- Compilation of circuits beyond the classical simulation limit will require quantum hardware, and will consume considerable time on that hardware. We note that all-classical software to recompile circuits involving parameterised gates does exist [9] and can make significant savings. However no classical compiler can be expected to approach optimality for general circuits since even the task of verifying that two circuits are near-identical is QMA-complete [10].
- Compilation from the original circuit $\mathcal{A}$ is not to an equivalent unitary circuit, but rather to a target circuit $\mathcal{B}$ that (ideally) has the same effect on just one specific input state $|\text{in}\rangle$, so that $\mathcal{B}\,|\text{in}\rangle = \mathcal{A}\,|\text{in}\rangle$. This is a profoundly more permissive goal, but is in fact the *right* goal for many quantum algorithms including so-called hybrid quantum-classical approaches [11].

*tyson.jones@ccc.ox.ac.uk
†simon.benjamin@materials.ox.ac.uk

1.2 Variational algorithms

We here provide a very brief overview of the class of variational algorithms for use on hybrid classical-quantum computers, which is a promising NISQ architecture [13, 12]. In these algorithms, the classical co-processor maintains a tractable set of real parameters $\vec{\theta}$ which control the state $|\psi(\vec{\theta})\rangle$ produced by the quantum co-processor, via an "*ansatz*" circuit $U(\vec{\theta})$. That is,

$$|\psi(\vec{\theta})\rangle = \hat{U}(\vec{\theta})\,|\text{in}\rangle\,. \tag{1}$$

where $|\text{in}\rangle$ is some fixed input state.

Measurements on $|\psi(\vec{\theta})\rangle$, such as the energy under some problem Hamiltonian, can often be efficiently performed and the outcomes used by the classical processor to update $\vec{\theta}$. This can be repeated in iterative strategies to, for example, perform eigensolving [13], simulate realtime dynamics [8] and imaginary time evolution [2].

By costing more circuit evaluations, variational algorithms can often avoid deep circuits and better tolerate noise. Our recompilation technique itself is a variational algorithm, and we also demonstrate its use in recompiling the circuits used in other variational algorithms.

2 Approximate recompilation

2.1 Overview

Consider a fixed state $|\text{out}\rangle$ produced by acting a fixed circuit $\mathcal{A}$ on a fixed input state $|\text{in}\rangle$, i.e. $|\text{out}\rangle = \mathcal{A}\,|\text{in}\rangle$. Given an alternate circuit template $\mathcal{B}(\vec{\phi})$, which is a product of m parameterised unitaries

$$\mathcal{B}(\vec{\phi}) = \hat{b}_1(\phi_1)\,\hat{b}_2(\phi_2)\ldots\hat{b}_m(\phi_m), \tag{2}$$

we seek to find an assignment of $\vec{\phi}$ such that

$$\mathcal{B}(\vec{\phi})\,|\text{in}\rangle \approx |\text{out}\rangle\,. \tag{3}$$

That is, as the 'user', we fix the gate types and the sequence of $\mathcal{B}$, but this template is 'blank' i.e. free of parameter information. Note Equ (3) does not necessitate $\mathcal{B}(\vec{\phi}) \approx \mathcal{A}$, but is instead the weaker constraint that their actions on the specific state $|\text{in}\rangle$ are approximately equal. We assume each gate $\hat{b}_j(\phi_j)$ in $\mathcal{B}$, and its inverse, is a simple function of ϕ_j so that the mapping between $\mathcal{B}$ and its inverse is tractable. For example, if $\hat{b}_j(\phi_j) = \exp(i\phi\sigma_x)$, then $\hat{b}_j^{-1}(\phi_j) = \hat{b}_j(-\phi_j)$ and

$$\mathcal{B}^{-1}(\vec{\phi}) = \hat{b}_m(-\phi_m)\,\ldots\hat{b}_2(-\phi_2)\hat{b}_1(-\phi_1). \tag{4}$$

Since $\vec{\phi}$ which satisfy $\mathcal{B}(\vec{\phi})\,|\text{in}\rangle = |\text{out}\rangle$ must also satisfy $|\text{in}\rangle = \mathcal{B}^{-1}(\vec{\phi})\,|\text{out}\rangle$, recompilation is the task of finding $\vec{\phi}$ such that

$$|\text{in}\rangle \approx \mathcal{B}^{-1}(\vec{\phi})\mathcal{A}\,|\text{in}\rangle\,. \tag{5}$$

Generally finding $\vec{\phi}$ is a hard search problem since there may be thousands of parameters even for NISQ-era machines. One must therefore select the strategy carefully, giving consideration to potential problems with iterative solutions such as becoming 'stuck' in a local minimum as we evolve the parameter set. There are also issues relating to the device size: ideally recompilation will be achieved without the need for additional qubits.

The approach we take here coopts recent ideas relating to finding the ground state energy of a Hamiltonian. It requires no additional qubits, and moreover although the scaling and performance of such approaches are not fully understood there is a developing literature on these topics [11].

2.2 Via energy dissipation

We assume the input state $|\text{in}\rangle$ is sufficiently well understood so that we can construct a Hamiltonian $\hat{H}_{\text{rec}}$ for which $|\text{in}\rangle$ is the unique ground state. Note $|\text{in}\rangle$ is *not* the state to be re-expressed by $\mathcal{B}$; it is the state input to the original circuit $\mathcal{A}$ and is likely to be a well understood state, such as the initial state of a realtime simulation. Furthermore, $\hat{H}_{\text{rec}}$ does not correspond to any physical system of interest; it is a fictitious construct purely to enable the recompilation process. We denote it $\hat{H}_{\text{rec}}$ where the subscript stands for 'recompilation'. Finding $\hat{H}_{\text{rec}}$ is of course trivial for any input that has a product form: for example if $|\text{in}\rangle = |0\ldots0\rangle$, then the obvious choice is $\hat{H}_{\text{rec}} = \sum_j \sigma_j^z$.

Given that we have selected a suitable H_{rec}, then the recompilation process has become an eigensolving task:

> *Given a (fixed) input $\mathcal{A}\,|in\rangle$ to 'ansatz' circuit $\mathcal{B}^{-1}(\vec{\phi})$, find the parameter values $\vec{\phi}$ for which the output has the lowest possible energy with respect to H_{rec}.*

We can adopt any one of several [11] techniques to solve this problem. The technique that we use here is the deterministic imaginary-time evolution which has been recently analysed [2] and found to have good efficiency with respect to a range of other techniques.

A reasonable measure of the success of recompilation is the fidelity between the input state $|\text{in}\rangle$ and its attempted reconstruction $\mathcal{B}^{-1}\mathcal{A}\,|\text{in}\rangle$, equivalent to that between $\mathcal{A}\,|\text{in}\rangle$ and $\mathcal{B}\,|\text{in}\rangle$. In the case that the compilation process is being performed with a quantum computer (rather than a classical emulation of the process), this fidelity can be lowered bounded through measuring the expected energy $\langle H_{\text{rec}}\rangle$; indeed the imaginary-time variational approach involves repeatedly estimating quantities of this kind. This fidelity F satisfies

$$F \geq \frac{E_1 - \langle H_{\text{rec}}\rangle}{E_1 - E_0}. \tag{6}$$

where E_0 and E_1 are the lowest lying energy eigenstates of the fictitious Hamiltonian $\hat{H}_{\text{rec}}$. Note that if, as in the example above, $\hat{H}_{\text{rec}}$ has a gap $E_1 - E_0$ of unity then the accuracy with which we can bound F simply depends on the shot noise in our estimate $\langle H_{\text{rec}}\rangle$. Recall this is the gap of the *fictitious* Hamiltonian, chosen by the user such that $|\text{in}\rangle$ is the ground-state, but is otherwise freely modified. Ergo there is no computational difficulty in resolving this gap; it is instead constructed!

2.3 Further gate elimination

After recompiling $\mathcal{A}|\text{in}\rangle$ into $\mathcal{B}(\vec{\phi})|\text{in}\rangle$, we can attempt to further shrink the circuit by eliminating gates with small parameters (thus deviating from the user-specified template). We choose a parameter ϕ_j whose current value $\phi_j = \delta$ is closest to 0 (or more strictly, since we may be dealing with periodic functions, we identify j for which $\hat{b}_j(\vec{\phi}_j)$ is closest to the identity). We then continue our imaginary-time evolution under modified variational equations, where we additionally constrain

$$\dot{\phi}_j = -\frac{\delta}{N\Delta t}. \tag{7}$$

Here N limits the change in ϕ_j in a single iteration. This simultaneously drives ϕ_j toward zero while retaining the pressure toward the ground state. Generally we will reach $\dot{\phi}_j = 0$ having suffered a small penalty in energy (and thus fidelity of the new circuit). Once zero is reached, we remove gate $\hat{b}_j(\phi_j)$ and then repeat the process. This continues until the energy has unacceptably risen. What is 'unacceptable' will depend on the application, but for the examples here we set the threshold to be twice the gap between true ground and the original energy of $\mathcal{B}^{-1}\mathcal{A}|\text{in}\rangle$ under $\hat{H}_{\text{rec}}$. In other words, we permit the energy defect to double in return for circuit compression. We emphasise that this entire phase is an optional post-process after the main recompilation. We denote the resulting circuit of this additional gate elimination process as $\mathcal{B}_{\text{elim}}$.

3 Demonstration

Having thus described the compilation and optimisation process in general terms, we now illustrate it with a specific example: recompilation of a 7-qubit, 186-gate circuit into a quite different template.

3.1 Choosing an interesting circuit

Rather than randomly generating the circuit $\mathcal{A}$, we focus on the likely application areas for our recompilation technique: hybrid algorithms that aim at dynamical simulation or eigensolving. Given that the recompilation technique itself involves a kind of eigensolver, for clarity we opt instead to make the circuit $\mathcal{A}$ relevant to a dynamical simulation task. Specifically, we assume that we wish to model the evolution of a certain 7−spin network, with the topology of spin-spin interactions shown in the upper right of Fig. 1a. We take it that the Hamiltonian of this system is

$$H_{\text{sys}} = \sum_i B_i \sigma_i^z + \sum_{i,j} \sum_{S\in x,y,z} J_{i,j}^S \sigma_i^S \sigma_j^S \tag{8}$$

where σ are the standard Pauli operators and $B_i < 0$ and $J_{i,j}^S > 0$ are constants. This is therefore a rather general spin network with irregular antiferromagnetic interactions and local fields. In order to create an interesting evolution we select the initial state $|\text{in}\rangle = |\Psi(0)\rangle = |1\rangle|+\rangle^{\otimes 6}$ i.e. a product state where one qubit is orientated such that it has maximum energy with respect to its local field and the others have zero expected energy in their local fields. We choose a simple recompilation Hamiltonian for which $|\text{in}\rangle$ is the ground state, namely

$$\hat{H}_{\text{rec}} = \sigma_1^z - \sum_{j=2}^{7} \sigma_j^x. \tag{9}$$

As a relevant test of our recompilation technique, we stipulate that the purpose of original circuit $\mathcal{A}$ is to model the evolution of this system, i.e. to create (a good approximation to) the state

$$|\Psi(t)\rangle = \exp(iH_{\text{sys}}t)\ |\Psi(0)\rangle \tag{10}$$

for some time t which we presently specify. A naive approach might be to use a number of Trotter 'cycles' i.e. to use a number q of identical circuit blocks each of which contains one gate for each Pauli term in H_{sys}. For sufficiently small t this approach is guaranteed to provide an accurate simulation. Fig. 1a shows a circuit of this kind. Each gate in the Trotter cycle however can be viewed as a parametrised gate with a prescribed value θ_j,

$$\mathcal{T}_j = \exp(-i\theta_j\hat{\sigma}/2) \tag{11}$$

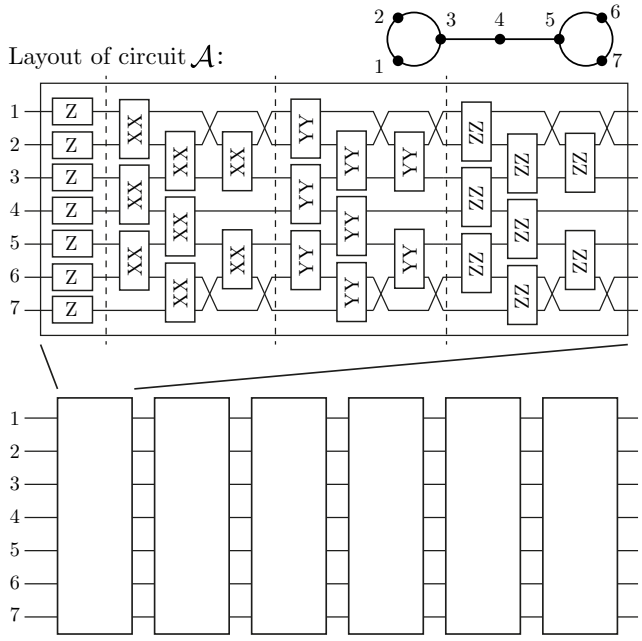
Given the same gate layout, one can instead use the variational algorithm described in Ref. [8] to adjust the 'strength' θ_j of each gate independently of all others in an optimal fashion. We indeed apply this algorithm, which we refer to as Li's algorithm [8] to create our circuit $\mathcal{A}$. We choose the time $t = 1.75$ as this is toward the outer limit of the range for which the circuit structure in Fig. 1a can produce an accurate simulation using Li's algorithm. The resulting parameters successfully replicate the state of the simulated spin system at time $t = 1.75$ with a fidelity of 0.995.

3.2 Recompilation and simulation

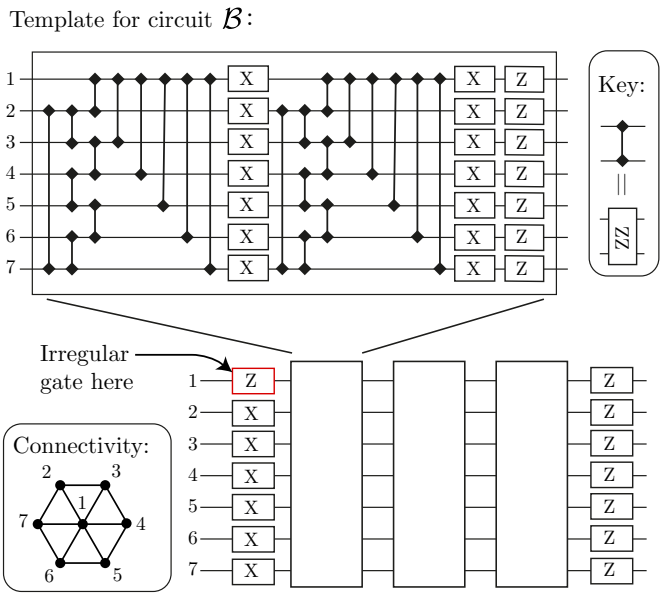
We freeze realtime simulation at $t = 1.75$ and perform approximate recompilation of $\mathcal{A}$, with and without subsequent gate elimination, to discover $\mathcal{B}(\vec{\phi})$ and $\mathcal{B}_{\text{elim}}(\vec{\phi'})$ respectively. The template $\mathcal{B}$ is shown and motivated in Figure 1b; it has a smaller family of gates, 72 two-qubit gates (in lieu of 144 in $\mathcal{A}$) though has 35 additional single-qubit gates. The performance of the iterative recompilation and additional gate removal is shown in Figure 2. Recompiling $\mathcal{A}$ into $\mathcal{B}$ costs a fidelity loss of $\approx 2 \times 10^{-3}$, bringing the fidelity of the ansatz state against the simulated spin system down to 0.994.

By exploiting the shorter depth, we are then able to append additional Trotter cycles (though with freely varying parameters) to $\mathcal{B}$ and $\mathcal{B}_{\text{elim}}$ and continue realtime simulation using Li's algorithm beyond what was possible with the original ansatz circuit. This is demonstrated in Figure 3, along with resource counts of all circuits involved in the realtime simulation and recompilation.

While the results here demonstrate excellent performance for both recompiling and extending variational realtime simulation, we are currently investigating the scaling of the method with qubit count and gate depth, and its resilience to noise.



(a) The circuit $\mathcal{A}$ which we opt to use as the input to our compilation process. The upper right figure summarises the two-qubit gate connections. The circuit has the structure of that that prescribed by Trotterisation for simulating the dynamics of a 7-qubit spin chain, but for recompilation purposes one can regard it as an arbitrary pattern of 186 unique non-Clifford gates (including 144 two-qubit gates). Here $Z(\theta) = \exp(-i\frac{\theta}{2}\sigma_Z)$, $ZZ(\theta) = \exp(-i\frac{\theta}{2}\theta\sigma_Z \otimes \sigma_Z)$, and similarly for the Y and Z gates.



(b) The template for the recompiled circuit $\mathcal{B}(\vec{\phi})$. The template is user-specified, and the recompilation process will determine the ϕ value for each gate. In comparison to the original circuit $\mathcal{A}$, this template has a smaller family of gate types (YY and XX type gates are omitted), has half as many two-qubit gates in total (72 rather than 144), and a larger number of single-qubit gates (77 versus 42). Moreover the topology of the two-qubit gates is different: it is a triangular lattice forming a hexagon as shown in the inset.

Figure 1

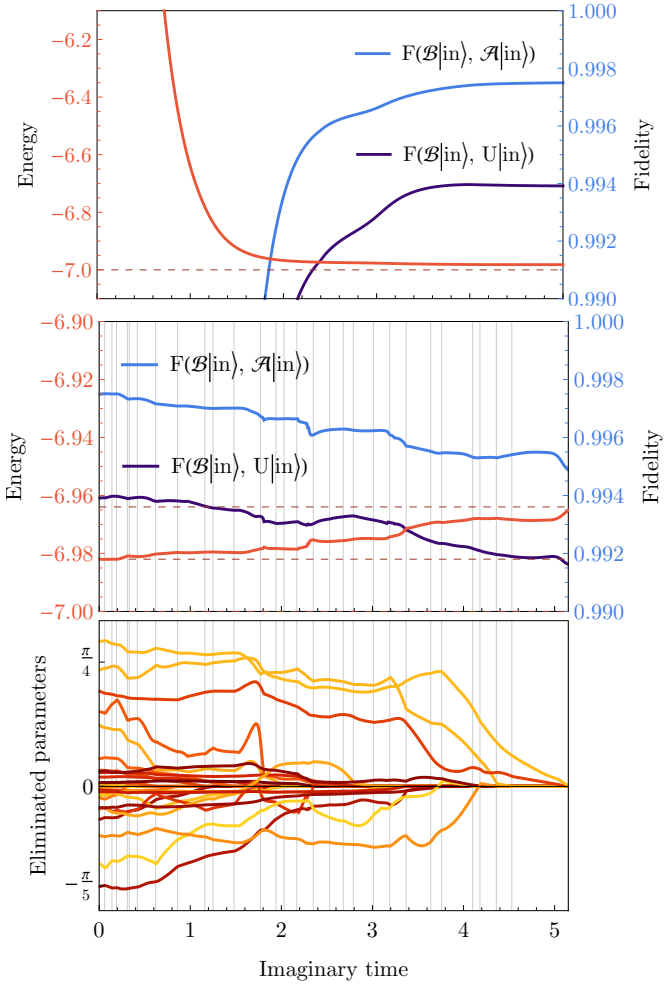


Figure 2: The process of recompiling circuit $\mathcal{A}$ into the template $\mathcal{B}(\vec{\phi})$ (top panel) then additionally eliminating 30 more gates to produce $\mathcal{B}_{\text{elim}}(\vec{\phi}')$ (bottom two panels). The light blue curves show the fidelity with which $\mathcal{B}(\vec{\phi})\,|\text{in}\rangle$ matches the target $\mathcal{A}\,|\text{in}\rangle$, as the parameters $\vec{\phi}$ are evolved under imaginary time evolution [2]. Since this is not necessarily measurable for the user, we also plot the measurable quantity $\langle H_{\text{rec}}\rangle$ in red, which bounds the fidelity as stated in Eqn. (6). (Also shown in dark purple is the fidelity with respect to the true state of the simulated spin system. The circuit $\mathcal{A}$ itself has a finite simulation fidelity of 0.995 and thus the recompiled circuit is somewhat lower.) The bottom panel shows the evolution of parameters which, during the gate elimination post-processing stage, are constrained to become zero (in turn) so that their corresponding gates can be removed. The parameter closest to zero is selected and forced to become zero over several iterations until eliminated (indicated by a vertical line), then the next closest parameter is chosen. This continues until $\langle H_{\text{rec}}\rangle$ deviates from the ideal (-7) by significantly more that it did immediately following the recompile; in this case, the 'defect' with respect to -7 is 0.02, and the elimination process continues until this approaches 0.04 i.e. until it doubles. In total, 30 gates are eliminated, bringing the total number in $\mathcal{B}$ from 149 to 119.

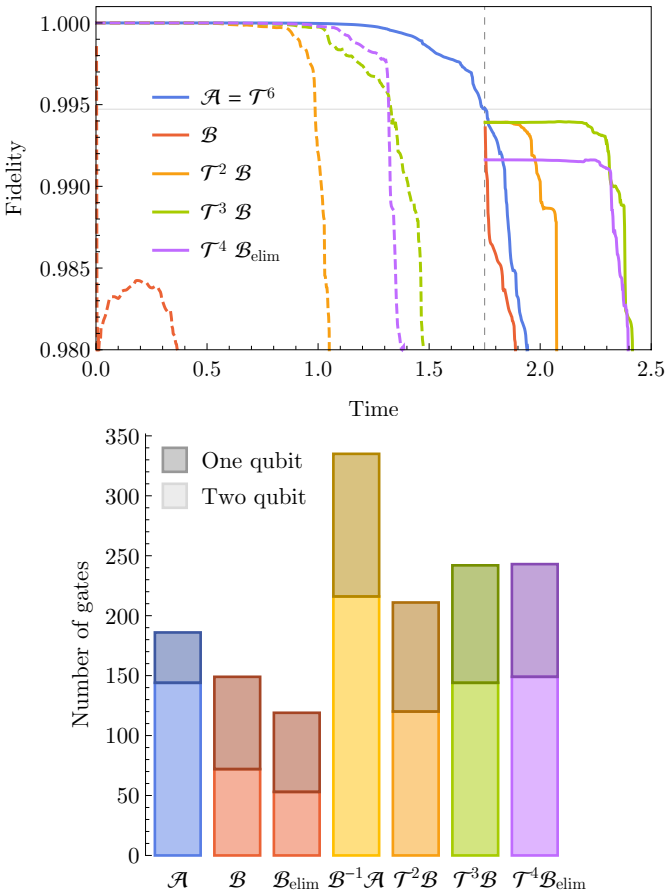


Figure 3: Realtime simulation (top) of the spin system specified in Eqn. (8) using Li's algorithm [8] with various possible circuits, and their resource costs (bottom). $\mathcal{T}^m$ indicates m cycles of the circuit (though with freely varying parameters) prescribed by Trotterisation. In blue, the original structure $\mathcal{A}$ suffers a precipitous drop in fidelity after $t = 1.75$. In red, the recompiled circuit $\mathcal{B}$ (a compacting of $\mathcal{A}(\vec{\theta}_{t=1.75})$) naturally fares worse. However, the green line corresponds to the performance of the recompiled and augmented circuit (appended with 3 Trotter cycles) and is superior: it can sustain high fidelity simulation for a further ~ 0.4 time units. With a near identical total gate cost, the purple line replaces further eliminated gates with an additional Trotter cycle; this has no benefit as expected, since the number of variational parameters has not increased.

References

[1] Tyson Jones and Simon C Benjamin, *Quantum compilation and circuit optimisation via energy dissipation*, arXiv:1811.03147 (2018).

[2] Sam McArdle, Tyson Jones, Suguru Endo, Ying Li, Simon Benjamin and Xiao Yuan, *Variational quantum simulation of imaginary time evolution with applications in chemistry and beyond* arXiv:1804.03023 (2018).

[3] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and J. M. Martinis, *Superconducting quantum circuits at the surface code threshold for fault tolerance*, Nature **508**, 500 (2014).

[4] T. P. Harty, D. T. C. Allcock, C. J. Ballance, L. Guidoni, H. A. Janacek, N. M. Linke, D. N. Stacey, and D. M. Lucas, *High-fidelity preparation, gates, memory and readout of a trapped-ion quantum bit*, Phys. Rev. Lett. **113**, 220501 (2014).

[5] C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, and D. M. Lucas, *High-fidelity quantum logic gates using trapped-ion hyperfine qubits*, Phys. Rev. Lett. **117**, 060504 (2016).

[6] J. P. Gaebler, T. R. Tan, Y. Lin, Y. Wan, R. Bowler, A. C. Keith, S. Glancy, K. Coakley, E. Knill, D. Leibfried, and D. J. Wineland, *High-fidelity universal gate set for $^{9}Be^{+}$ ion qubits*, Phys. Rev. Lett. **117**, 060505 (2016).

[7] Naomi H. Nickerson, Joseph F. Fitzsimons and Simon C. Benjamin, *Freely Scalable Quantum Technologies Using Cells of 5-to-50 Qubits with Very Lossy and Noisy Photonic Links*, Phys. Rev. X **4**, 041041 (2014).

[8] Ying Li and Simon C. Benjamin, *Efficient variational quantum simulator incorporating active error minimization*, Phys. Rev. X **7**, 021050 (2017).

[9] Yunseong Nam, Neil J. Ross, Yuan Su, Andrew M. Childs and Dmitri Maslov, *Automated optimization of large quantum circuits with continuous parameters*, npj Quantum Information **4**, 23 (2018).

[10] Dominik Janzing, Pawel Wocjan and Thomas Beth, *Identity check is QMA-complete*, arXiv:quant-ph/0305050 (2003).

[11] For a recent review describing hybrid variational techniques in chemistry, see e.g. Sam McArdle, Suguru Endo, Alan Aspuru-Guzik, Simon Benjamin and Xiao Yuan, *Quantum computational chemistry*, arXiv:1808.10402 (2018).

[12] John Preskill, *Quantum Computing in the NISQ era and beyond*, Quantum, **2** pp. 79 (201)

[13] Alberto, Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J Love, Alán Aspuru-Guzik and Jeremy L O'Brien, *A variational eigenvalue solver on a photonic quantum processor*, Nature Communications. **5** (2014)

Efficient Online Quantum Generative Adversarial Learning Algorithms with Applications

Yuxuan Du[1] * Min-Hsiu Hsieh[2] † Dacheng Tao[1] ‡

[1] *UBTECH Sydney Artificial Intelligence Centre and the School of Information Technologies, Faculty of Engineering and Information Technologies, The University of Sydney, Australia*

[2] *Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, Australia*

Abstract. The exploration of quantum algorithms that possess quantum advantages is a central topic in quantum computation and quantum information processing. One potential candidate in this area is quantum generative adversarial learning (QuGAL), which conceptually has exponential advantages over classical adversarial networks. However, the corresponding learning algorithm remains obscured. In this paper, we propose the first quantum generative adversarial learning algorithm—the quantum multiplicative matrix weight algorithm (QMMW)—which enables the efficient processing of fundamental tasks. The computational complexity of QMMW is polynomially proportional to the number of training rounds and logarithmically proportional to the input size. The core concept of the proposed algorithm combines QuGAL with online learning. We exploit the implementation of QuGAL with parameterized quantum circuits, and numerical experiments for the task of entanglement test for pure state are provided to support our claims.

Keywords: Quantum Machine Learning, Quantum Information Processing

1 Introduction

The principal interest in quantum computation is the exploration of potential applications that outperform their classical counterparts. The rapid development of quantum hardware divides this interest into short-term and long-term goals. The short-term goal is to devise quantum algorithms that not only possess quantum advantages but can also be implemented on near-term devices [18]. The long-term goal is to employ fault-tolerant quantum computers that are capable of providing remarkable quantum speedups over classical methods [20] to tackle practical real-world problems.

Quantum machine learning is one of the most promising candidates for achieving both short-term and long-term goals [2], and the proposed quantum generative adversarial learning (QuGAL) strengthens this belief [15]. The main theoretical conclusion of QuGAL is that exponential quantum advantages may exist under the assumption that the target data distribution can be efficiently encoded into a density matrix [15]. Conceptually, QuGAL involves two players, a generator and a discriminator, which play a zero-sum game. At each training round, the generator tries to approximate the target data to fool the discriminator, while the discriminator tries to distinguish the fake data from the real data. When the generator and discriminator are both constructed by quantum operations, the adversarial quantum learning game has the potential to converge to Nash equilibrium with an exponential speedup.

Despite promising theoretical results, two issues related to QuGAL have not been explored. First, it is unclear what kinds of learning tasks can be accomplished by QuGAL to potential advantages. Second, an explicit learning algorithm of QuGAL that can fast converge to the equilibrium remains unexplored. Previous studies mainly focus on the implementation of QuGAL under near-term quantum devices as so-called quantum generative adversarial networks (QuGANs) [8, 21, 24, 19, 26]. In particular, the generator and discriminator of QuGANs are constructed by employing parameterized quantum circuits (PQCs) that are composed of a set of trainable parameterized single qubit gates and two-qubit CNOT gates [9]. However, the intrinsic optimization mechanism of PQCs that iteratively updates each gate destroys the required convex-concave property in QuGAL, which implies that the obtained result may not converge to Nash equilibrium and may induce additional training difficulties, e.g., mode collapse and vanishing gradients [1]. Two key issues therefore exist for QuGANs, i.e., how to improve stability and convergence in training QuGANs, and whether QuGANs deliver potential quantum advantage.

To tackle the aforementioned issues, we revisit the theory of QuGAL in this paper from the perspective of online learning [11]. The integration of online learning with QuGAL is motivated by the fact that online learning algorithms can efficiently approximate the optimal result for the zero-sum game associated with the convex-concave property, and the training of QuGAL satisfies this condition. This observation enables us to devise a quantum adversarial learning algorithm with online learning features and to theoretically analyze its potential quantum advantages. Additionally, online learning has been employed as a powerful tool for relieving training difficulties in classical generative adversarial networks (GANs) [10], which motivates us to introduce such a method in optimizing QuGANs. Lastly, we investigate how to use QuGAL to accomplish learning quantum information processing tasks, such as the quantum entanglement test for pure state and quantum state discrimination [12, 6, 4, 5, 7]. Our study opens avenues for exploring quantum information

*yudu5543@uni.sydney.edu.au
†min-hsiu.hsieh@uts.edu.au
‡dacheng.tao@sydney.edu.au

processing tasks using quantum generative adversarial learning models.

We summarize the main results of this work as follows.

- We propose a quantum generative adversarial learning algorithm, the quantum multiplicative matrix weight (QMMW) algorithm, which rapidly converges to Nash equilibrium as expected from QuGAL. QMMW is inspired by the multiplicative matrix weight algorithm, which is a popular online learning algorithm that efficiently finds optimal solutions to the zero-sum game [14]. We prove that the convergence rate of QMMW is $\mathcal{O}(\sqrt{N/T})$, where N is the number of qubits corresponding to the target density matrix and T is the number of training rounds. An attractive feature of QMMW is that the output states of both the generator and discriminator can be viewed as Gibbs states. By exploiting the efficient Gibbs sampling method proposed by [23], we prove that the computational complexity of QMMW is $\mathcal{O}(N^3T^4)$.

- We introduce a multiplicative weight training method to overcome the training difficulty encountered in QuGANs. The core ingredient of this method is to seek the most possible optimized direction for achieving global equilibrium through the inherent mechanism of online learning. In the training process, a multiplicative weight training method puts more weight to the gradient that is more probable to fool the discriminator. Since the multiplicative weight training method only focuses on re-weighting the gradient, it can be seamlessly embedded into other optimization methods used in QuGANs.

- We investigate the potential quantum advantages by applying QMMW and QuGANs to solve quantum information tasks, i.e., the pure state entanglement test and the quantum state discrimination. In particular, we numerically validate that QuGANs are capable of accomplishing the pure state entanglement test with modest quantum resources, which sheds light on using QuGANs to handle other quantum information learning tasks. All numerical simulations demonstrated in this paper are implemented in Python, leveraging the pyQuil and QuTiP libraries to access the numerical simulators [22, 13].

2 Main results

Quantum Multiplicative Matrix Weight—Here we propose a no-regret quantum generative adversarial learning algorithm—the quantum multiplicative matrix weight (QMMW) algorithm—to efficiently reconstruct the given mixed state under the fault-tolerant quantum circuits setting. Conceptually, QMMW is inspired by the multiplicative matrix weight algorithm [14], an advanced meta-algorithm with the no-regret property that is broadly used in online convex optimization [11]. This convergence rate of QMMW is assured by the following theorem:

Theorem 1 *Given a mixed state ρ represented by N qubits, and setting the training rounds as T, QMMW yields*

$$|\mathcal{L}(\bar{\sigma}_G, \bar{\sigma}_D) - \mathcal{L}(\sigma_G^*, \sigma_D^*)| \leq 3\sqrt{\frac{N}{T}}. \tag{1}$$

QMMW can be efficiently executed on fault-tolerant quantum circuits, since both $\sigma_G^{(t)}$ and $\sigma_D^{(t)}$ are Gibbs states that can be prepared by using efficient Gibbs sampling methods [3, 23]. The efficiency of the Gibbs sampling methods proposed in [23] presents another attractive advantage of QMMW:

Theorem 2 *Given an N-qubit state, let U_ρ be the unitary that prepares the purification state of ρ. Denote T as the total number of training rounds. If there is quantum query access to U_ρ, the computation cost of the QMMW algorithm is $\mathcal{O}(N^3T^4)$.*

QuGANs with multiplicative weight training method.— The investigation of applying QuGANs to tackle quantum information processing problems is of practical interest in the near term when there are only limited available qubits and shallow quantum circuit depth [18]. Although several studies have confirmed the feasibility of using QuGANs to achieve certain tasks, the variational optimization method collapses the desired convex-concave property and heavily challenges the performance of QuGANs. The disappearance of the convex-concave property results in an inevitable difficulty, since the optimization may get stuck in local minima. This topic has been widely investigated in classical GANs [25]. Inspired by the weighted training algorithm proposed by [17], which has demonstrated its effectiveness in classical GANs, we propose the multiplicative weight training method [17] to relieve the training difficulty in QuGANs. The proposed training method can be seamlessly embeded into advanced optimization algorithms used to train parameterized quantum circuits (PQCs). The loss function of QuGAN gives the following theorem:

Lemma 3 *The loss function of QuGAN has the convex-concave property with the equilibrium value $\mathcal{L}(U_G^*, U_D^*) = 1/2$.*

3 Numerical Simulation

We employ QMMW is employed to distinguish entanglement from a bipartite pure state, we impose an 'constraint' step in updating the generated state. We define the target state as $\rho_{AB} = |\Psi\rangle\langle\Psi|_{AB}$ at each training rounds, and two copies of σ_G are generated following the rule of QMMW. The 'constrained' step refers to a partial trace step, i.e., by partial trace system A for the first copy and system B for the second copy, we have the product state $\mathrm{Tr}_A(\sigma_G) \otimes \mathrm{Tr}_B(\sigma_G)$. The integration of the 'constraint' step and naive QMMW naturally results in Nash equilibrium being reached if and only if the input state is separable, since the generated state must be separable. Meanwhile, the 'constraint' step satisfies the two standards rules. It is easy to prove that the no-regret

property of the varied QMMW is conserved. The partial trace can be executed with $\mathcal{O}(1)$ complexity. We validate its performance by approximating a separable mixed state $\rho_{sep} = \frac{1}{2}|0000\rangle\langle 0000| + \frac{1}{2}|1111\rangle\langle 1111|$. The total number of training rounds is set as $T = 400$ and $T = 1600$, respectively. As illustrated in Figure 1, the final training loss for $T = 400$ is 0.561 with fidelity of 0.929. The final training loss for $T = 1600$ is 0.532 with fidelity of 0.965. The simulation results indicate that the training loss rapidly converges to the equilibrium value and the fidelity between the generated state and ρ_{sep} tends to be 1 with increased T. The simulation results are in accordance with the conclusion of Theorem 1, where the theoretical results are $1/2 + 3\sqrt{4/400} = 0.7$ and $1/2 + 3\sqrt{4/1600} = 0.65$, respectively. The numerical simulations are implemented in Python in conjunction with QuTiP [13].

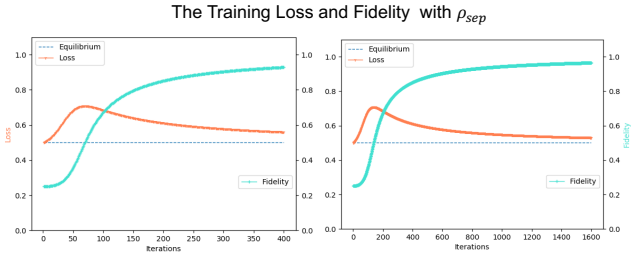


Figure 1: The left panel is the simulation result of QMMW with setting $T = 400$. The right panel is the simulation result of QMMW with setting $T = 1600$.

We then benchmark the performance of the QuGANs to accomplish the entanglement test for bipartite pure states. The detailed procedure for constructing QuGAN is as follows. The trainable parameters $\boldsymbol{\theta}$ (for U_G) and $\boldsymbol{\gamma}$ (for U_D) are randomly initialized and updated by the zero-order differential method [16]. We set the total number of training rounds T as 500. The prior is set as $P(G) = P(R) = 1/2$. The detailed quantum circuit structure is illustrated in Figure 2. The number of blocks required to implement U_G and U_D is set as $L_1 = 7$ and $L_2 = 3$, respectively. The quantum circuit architecture is demonstrated in Figure 2. All numerical simulations are implemented in Python in conjunction with the PyQuil library [22].

When QuGAN is employed to distinguish entanglement from a bipartite pure state, we redesign the arrangement of quantum gates in each block of U_G. No CNOT gate exists whose controlled qubit is in system A and whose target qubit is in system B. The detailed quantum circuit architecture is shown in the right panel of Figure 2. The modified quantum circuit structure indicates that Nash equilibrium can be reached if and only if the input state is separable, since U_G can only generate a separable state.

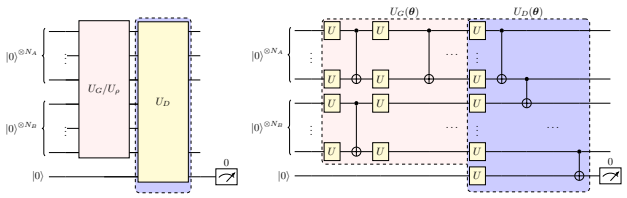


Figure 2: The quantum circuit of QuGAN to accomplish the entanglement test for bipartite pure states. In the left panel, U_ρ (or U_G) is selected to to produce the real (or generated) state with prior $P(R)$ (or $P(G)$). In the right panel, the circuit architecture of U_G and U_D is expanded. The notation U is defined as $U = R_X \circ R_Y \circ R_Z$, where R_X, R_Y, and R_Z are trainable parameterized single qubit gates along X, Y, Z axis.

We now employ QuGAN to accomplish the entanglement test for two bipartite pure states, i.e., a separable state $|\Psi\rangle = (|00\rangle_A + |10\rangle_A) \otimes |00\rangle_B / \sqrt{2}$ and an entangled state $|\text{GHZ}\rangle = (|00\rangle_A \otimes |00\rangle_B + |11\rangle_A \otimes |11\rangle_B)/\sqrt{2}$, where A and B refer to the bipartite system. The simulation results are illustrated in Figure 3. The total number of single and two qubit quantum gates is 143 to implement QuGAN. When the input state is separable state $|\Psi\rangle$, the training loss oscillates around the optimal value after around 100 steps and ranges from 0.444 to 0.559, as shown in the outer plot. The corresponding fidelity between the target state and the generated state is always larger than 0.702. The training loss for the entanglement state case is far away from the optimal value, which oscillates around 0.850 after 300 steps, as shown in the inner plot. The fidelity between the generated state and the given state $|\text{GHZ}\rangle$ is always below 0.250.

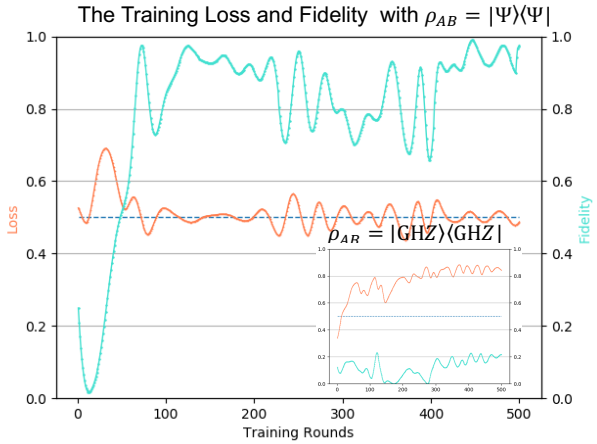


Figure 3: The outer plot is the simulation result of QuGAN when the input is $|\Psi\rangle$. The inner plot is the simulation result of QuGAN when the input is $|\text{GHZ}\rangle$.

The technical version is in Arxiv 1904.09602.

References

[1] Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein generative adversarial networks. In *International Conference on Machine Learning*, pages 214–223, 2017.

[2] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671):195, 2017.

[3] Fernando G. S. L. Brandão, Amir Kalev, Tongyang Li, Cedric Yen-Yu Lin, Krysta M. Svore, and Xiaodi Wu. Quantum SDP solvers: Large speed-ups, optimality, and applications to Quantum Learning. *arXiv e-prints*, page arXiv:1710.02581, October 2017.

[4] Eric Chitambar, Runyao Duan, and Min-Hsiu Hsieh. When do local operations and classical communication suffice for two-qubit state discrimination? *IEEE Transactions on Information Theory*, 60(3):1549–1561, 2014.

[5] Eric Chitambar and Min-Hsiu Hsieh. Revisiting the optimal detection of quantum information. *Physical Review A*, 88(2):020302, 2013.

[6] Eric Chitambar and Min-Hsiu Hsieh. Asymptotic state discrimination and a strict hierarchy in distinguishability norms. *Journal of Mathematical Physics*, 55(11):112204, 2014.

[7] Eric Chitambar and Min-Hsiu Hsieh. Round complexity in the local transformations of quantum and classical states. *Nature Communications*, 8(1):2086, 2017.

[8] Pierre-Luc Dallaire-Demers and Nathan Killoran. Quantum generative adversarial networks. *arXiv preprint arXiv:1804.08641*, 2018.

[9] Yuxuan Du, Min-Hsiu Hsieh, Tongliang Liu, and Dacheng Tao. The expressive power of parameterized quantum circuits. *arXiv preprint arXiv:1810.11922*, 2018.

[10] Paulina Grnarova, Kfir Y Levy, Aurelien Lucchi, Thomas Hofmann, and Andreas Krause. An online learning approach to generative adversarial networks. In *International Conference on Learning Representations*, 2018.

[11] Elad Hazan et al. Introduction to online convex optimization. *Foundations and Trends® in Optimization*, 2(3-4):157–325, 2016.

[12] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865, 2009.

[13] J Robert Johansson, Paul D Nation, and Franco Nori. Qutip: An open-source python framework for the dynamics of open quantum systems. *Computer Physics Communications*, 183(8):1760–1772, 2012.

[14] S. Kale. *Efficient algorithms using the multiplicative weights update method*. Princeton University, 2007.

[15] Seth Lloyd and Christian Weedbrook. Quantum generative adversarial learning. *arXiv preprint arXiv:1804.09139*, 2018.

[16] Kosuke Mitarai, Makoto Negoro, Masahiro Kitagawa, and Keisuke Fujii. Quantum circuit learning. *arXiv preprint arXiv:1803.00745*, 2018.

[17] Yannis Pantazis, Dipjyoti Paul, Michail Fasoulakis, and Yannis Stylianou. Training generative adversarial networks with weights. *arXiv preprint arXiv:1811.02598*, 2018.

[18] John Preskill. Quantum computing in the NISQ era and beyond. *arXiv preprint arXiv:1801.00862*, 2018.

[19] Jonathan Romero and Alan Aspuru-Guzik. Variational quantum generators: Generative adversarial quantum machine learning for continuous distributions. *arXiv preprint arXiv:1901.00848*, 2019.

[20] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, 1999.

[21] Haozhen Situ, Zhimin He, Lvzhou Li, and Shenggen Zheng. Adversarial training of quantum born machine. *arXiv preprint arXiv:1807.01235*, 2018.

[22] Robert S Smith, Michael J Curtis, and William J Zeng. A practical quantum instruction set architecture. *arXiv preprint arXiv:1608.03355*, 2016.

[23] Joran van Apeldoorn and András Gilyén. Improvements in quantum SDP-solving with applications. *arXiv preprint arXiv:1804.05058*, 2018.

[24] Jinfeng Zeng, Yufeng Wu, Jin-Guo Liu, Lei Wang, and Jiangping Hu. Learning and inference on generative adversarial quantum circuits. *arXiv preprint arXiv:1808.03425*, 2018.

[25] Chiyuan Zhang, Samy Bengio, Moritz Hardt, Benjamin Recht, and Oriol Vinyals. Understanding deep learning requires rethinking generalization. *arXiv preprint arXiv:1611.03530*, 2016.

[26] Christa Zoufal, Aurélien Lucchi, and Stefan Woerner. Quantum generative adversarial networks for learning and loading random distributions. *arXiv preprint arXiv:1904.00043*, 2019.

Probing modified commutation relations via quantum noise

Parth Girdhar[1] Andrew C. Doherty[1]

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

Abstract Recent advances in precision measurements have opened the possibility of probing quantum gravity and bounding modifications of quantum mechanics in tabletop experiments. We have studied modifications to a quantum optomechanical effect, radiation pressure noise (RPN), due to corrections to the canonical position-momentum commutator that are present in certain quantum gravity theories. We show that high power driven atomic and nano-scale systems, under suitable control, will allow beating known bounds by several orders of magnitude. This advance in quantum metrology could provide strong evidence to eliminate or support modifications of quantum mechanics, and new perspectives on such models of quantum gravity.

Keywords: quantum metrology, modifications of quantum mechanics, commutation relations, quantum gravity, quantum noise, optomechanics,

In the modern 'effective field theory' view of physics, phenomena are described in terms of quantised fields on a background space-time. But several theories of quantum gravity predict that on scales close to the Planck length L_P i.e. $\sim 10^{-35}$m such a description breaks down; such theories have a 'minimal length' in that it is not meaningful to describe quantities smaller than a certain length [1]. For example this is a feature of string theory, associated with 'T-duality' and manifested in high-energy string scattering [2]. The standard Heisenberg position-momentum uncertainty relation however does not account for such a minimal length. It has been suggested across the literature [1], [2], [3] to modify it, via a dimensionless parameter β_0, such that the associated modified canonical commutation relation is:

$$[x,p] = i\hbar\left(1+\beta_0\left(\frac{p}{M_P c}\right)^2\right)$$

From scratch, we derive and solve the equations describing interaction of a quantum optical field and thermal bath with a macroscopic oscillator under the assumption of this modified commutation relation. Through this we derive the modified mechanical noise spectra for an oscillator in an optomechanical system such as the mirrors in Advanced LIGO or the nanomechanical oscillators in recent optomechanical experiments. The altered shape and magnitude of the spectra allows us to infer a bound that $\beta_0 < 10^{20}$ for the centre-of-mass degree of freedom. This is 10 orders of magnitude better than bounds on centre-of-mass of other systems, such as precision measurements of Lamb shift [6] and ground state of gravitational wave bar detector[5]. It is comparable to bounds on nonlinear effects on macroscopic harmonic oscillators [6] and unlike a recently proposed optomechanical method it does not require achieving challenging cavity finesse or working with cooled nano-oscillators [7]. We examine the bounds for future upgraded experiments and show infact the target bound of $\beta_0 \sim 1$ can be achieved by driving oscillators sufficiently rapidly. We also explore the bounds inferred on commutation relations of constituent

[1] pgir1104@uni.sydney.edu.au

particles of the oscillators and demonstrate the feasibility of parameter regimes required to infer new values approaching the Planck scale.

Overall, our methods show how the scope of quantum metrology achievable in modern experiments is able to penetrate a new realm of fundamental physics.

References

[1] Garay, L. G. Quantum gravity and minimum length. Int. J. Mod. Phys. A10, 145-165 (1995).

[2] Witten, E. Reflections on the fate of spacetime. Phys. To- day 49, 24-31 (1996).

[3] Kempf, A., Mangano, G. & Mann, R. B. Nat. Phys. 8, 393 (2012).

Hilbert space representation of the minimal length uncertainty relation. Phys. Rev. D 52, 1108-1118 (1995).

[4] Ali, A. F., Das, S. & Vagenas, E. C. A proposal for test- ing Quantum Gravity in the lab. Phys. Rev. D 84, 044013 (2011).

[5] Marin. F et. al, Investigation on Planck scale physics by the AURIGA gravitational bar detector, New J. Phys. 16, 085012 (2014).

[6] Bawaj, M. et. al, Probing deformed commutators with macroscopic harmonic oscillators, Nat. Comms 6, 7503 (2015)

[7] Pikovski, I. et. al., Probing Planck-scale physics with quantum optics

Partial Decoupling Approach to Information Leakage Problem from Black Holes with Symmetry

Yoshifumi Nakata[1 2 3 *] Eyuri Wakakuwa[4 †] Masato Koashi[2 ‡]

[1] *Yukawa Institute for Theoretical Physics, Kyoto university, Kitashirakawa Oiwakecho, Sakyo-ku, Kyoto, 606-8502, Japan*

[2] *Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo, 113-8656, Japan*

[3] *JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*

[4] *Department of Communication Engineering and Informatics, Graduate School of Informatics and Engineering, The University of Electro-Communications, Tokyo, 182-8585, Japan*

Abstract. The black hole information paradox was recently investigated from the quantum information theoretic approach. Using the decoupling method, it was shown that radiation carries information away from black holes extremely quickly. The key mechanism is the information scrambling of black holes, but most black holes, in reality, have symmetries so that the dynamics cannot be fully scrambling. Here, we explore information leakage from black holes with symmetry by generalizing the decoupling method to the one applicable without full scrambling. We then consider uncharged rotating black holes and show that extremely quick information leakage continues only when the black hole is sufficiently large.

Keywords: decoupling, black hole information paradox, scrambling, channel coding

1 Introduction and Results

The black hole information paradox has been a long-standing problem since the discovery of Hawking radiation from quantum black holes [1]. The original question was if information in a black hole is eventually carried away by the radiation. However, recent developments of the holographic principle suggests that information should be preserved as a whole and the radiation should necessarily carry the information away. This opens a new question of how, and how quickly, it occurs.

In recent years, an elegant approach based on *decoupling* [2, 3] was proposed from the theory of quantum information [4]. Using a unitary evaporation model of quantum black holes, it was pointed out that complex internal dynamics of black holes leads to *information scrambling* [5, 6] and further to *decoupling* [7], and thus, information leaks out extremely quickly from old black holes. The result was recently demonstrated even in an ion-trap experiment [8]. This approach, rephrasing the information leakage in terms of transmitting quantum information, opens a fruitful interplay between quantum information and high energy physics, such as scrambling [5, 6], OTOCs [9, 10, 11], quantum duality [12, 13], and a new approach to the holographic principle [14, 15, 16].

However, black holes in reality have symmetries and conserved quantities, which prevent the dynamics from being fully information scrambling. It is thus not clear whether information is indeed quickly leaked out from black holes with symmetry. One of the common beliefs is that any global symmetries are weakly violated in the regime of quantum gravity [17, 18]. However, to fully understand information leakage from black holes, analysis that properly takes the symmetry into account is of crucial importance.

Here, based on the first part of Ref. [19] and the technical manuscript, we provide a deep analysis of the information leakage from quantum black holes with symmetry. Since decoupling approach cannot be directly applied due to the absence of full scrambling, we first provide a generalization of decoupling theorem, which we call *partial* decoupling [19]. We then apply partial decoupling to the information leakage problem of uncharged rotating black holes, often referred to as *Kerr* black holes, where the angular momentum in one direction is conserved. Based on the assumption that the dynamics scrambles each subspace with different angular momentum independently, we obtain the following:

1. The information *invariant* under the symmetric action leaks out from old Kerr black holes

*yoshifumi.nakata@yukawa.kyoto-u.ac.jp

†e.wakakuwa@gmail.com

‡koashi@qi.t.u-tokyo.ac.jp

extremely quickly as if there were no symmetry.

2. The information *variant* under the symmetric action, or equivalently, coherence between different angular momenta, leaks out quickly only when the black hole is sufficiently large. Small Kerr black holes keep a part of the symmetry-variant information unevaporated until the last moment.

In short, the larger a quantum Kerr black hole is, the more information the radiation carries away quickly. This is due to various quantum effects, such as quantum fluctuations, entanglement, and an intriguing encoding method that we call *observable imprinting*. Our analysis is fully general and quantitative, so that it can be applied to black holes with any symmetries or even to the problem of channel coding restricted by symmetry.

Our result is insightful not only in high energy physics, providing an information theoretic insight to symmetry in quantum gravity [17, 18], but also in quantum information because our result reveals that symmetry enriches the structure of information transmission, where many quantum effects come into play. Thus, we think that our analysis opens a new playground in quantum information theory in relation with symmetry, which is not only interesting in its own right but also accelerates the fruitful relation between quantum information and complex quantum many-body physics. We also emphasize that our technical contribution, the partial decoupling theorem, is potentially applicable to various problems in quantum information, such as simultaneous transmission of quantum and classical information [20], and the theory of coherence [21].

2 Results in detail

Hereafter, we often write the system on which an operator acts as a superscript.

Our analysis is based on the toy model of black holes proposed in Ref. [4]. The initial black hole $X_{\rm in}$ is composed of N qubits and is in the state $\xi^{X_{\rm in}}$ that is purified by the past Hawking radiation $X_{\rm out}$. Alice throws quantum information source A of k qubits into $X_{\rm in}$. We especially consider the case where the quantum source A is purified by the reference R to be the maximally entangled state Φ^{AR}. After the internal unitary dynamics U^S of the whole black hole $S = AX_{\rm in}$, an ℓ-qubit subsystem S_1 is evaporated from the black hole S. Bob collects the radiation S_1 and tries to recover A by applying recovery operation $\mathcal{D}$. He may additionally make use of the past Hawking radiation $X_{\rm out}$ (see Fig. 1 as well).

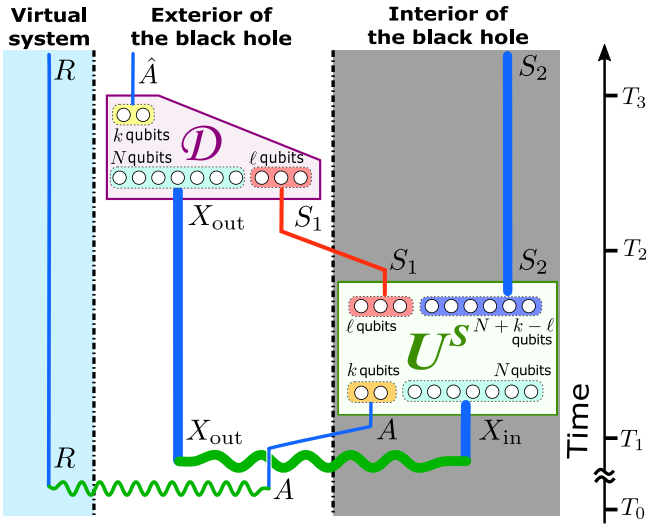


Figure 1: A diagram of the information leakage problem [4]. The blue lines represent the paths of qubits, and the green wave lines indicate that they may be entangled. The red line is the Hawking radiation S_1.

If Bob can successfully recover the quantum source A, it implies that the information has been already carried away by the radiation S_1. Thus, based on this toy model, the information leakage problem can be rephrased by transmitting quantum information via noisy quantum channel, especially via the partial trace channel Tr_{S_2}, which enables us to apply the technique in quantum information theory.

When a system W has symmetry (W is e.g. A or S), the associated Hilbert space $\mathcal{H}^W$ is decomposed into invariant subspaces. For an axiall symmetry, which is the case for Kerr black holes, $\mathcal{H}^W$ is simply decomposed into $\bigoplus_m \mathcal{H}^W_m$, where m is the Z-component of the angular momentum. Accordingly, quantum information on the system W, defined by a purified source $\sigma^{WW'}$, is decomposed into $\sigma^{WW'} = \sigma^{WW'}_{diag} + \sigma^{WW'}_{off}$, where $\sigma^{WW'}_{diag} = \sum_m P^W_m \sigma^{WW'} P^W_m$, and $\sigma^{WW'}_{off} = \sum_{m\neq m'} P^W_m \sigma^{WW'} P^W_{m'}$ with P^W_m being the projector onto $\mathcal{H}^W_m$. This is useful to classify information with respect to the symmetry. Since σ_{diag} is invariant under any symmetric actions, we refer to the information in σ_{diag} as symmetry-invariant ionformation of W. The remaining information is then called *symmetry-variant* information of W, which is closely related to σ_{off}, or more specifically, the coherence of σ between different angular momenta.

Since the unitary dynamics $U^S_{\rm Kerr}$ should respect the symmetry of the Kerr black hole, it is also decomposed into $\bigoplus_m U^S_m$. In the same spirit as Ref. [4], we assume that the dynamics is sufficiently complex that each U^S_m fully scrambles each subspace $\mathcal{H}^S_m$. However, since $U^S_{\rm Kerr}$ does not vary the angular momentum m, it is not fully scrambling and hence, decoupling theorem [7] cannot be directly applied. Thus, we first show a new type of decoupling by the unitary in the form of $\bigoplus_m U^S_m$:

***Theorem* 1 (Simplified and informal)** *Let Ψ^{SR} be a state on $\mathcal{H}^{SR}$, where $\mathcal{H}^S = \bigoplus_m \mathcal{H}^S_m$, and $\mathcal{C}^{S\to E}$ be a quantum channel. If the conditional min-entropy $H_{\min}(S^*|RE)_\Gamma$ for the state Γ^{S^*ER} is sufficiently large, it holds for almost any U^S in the form of $\bigoplus_m U^S_m$ that*

$$\mathcal{C}^{S\to E}\big(U^S\Psi^{SR}U^{S\dagger}\big) \approx \sum_m \frac{D_S}{d_m}\zeta^E_m \otimes \Psi^R_m, \qquad (1)$$

where $D_S = \dim \mathcal{H}^S$, $d_m = \dim \mathcal{H}^S_m$, ζ^{SE} is the Choi-Jamiołkowski state of $\mathcal{C}^{S\to E}$, $\zeta^E_m = {\rm Tr}_S[P^S_m\zeta^{SE}P^S_m]$, and $\Psi^R_m = {\rm Tr}_S[P^S_m\Psi^{SR}P^S_m]$.

The formal and more general statement, including the one-shot version, is given in Theorem 1 in Ref. [19] and the technical manuscript. There, the state Γ^{S^*ER}, which consists of the initial state Ψ, the channel $\mathcal{C}$, and the decomposition of $\mathcal{H}^S$, and the explanation of the system S^*ER are also provided. Note that Theorem 1 reduces to the one-shot decoupling theorem [7] when the decomposition is trivial, implying that this is a proper generalization.

We then investigate the information leakage from Kerr black holes. We first introduce two recovery errors: one is the error in recovering the symmetry-invariant information of A and the other is for the whole information of A, which are respectively denoted by $\Delta_{inv}(\xi : U_{\rm Kerr})$ and $\Delta(\xi : U_{\rm Kerr})$. Both are measured by the average trace distance (see the technical manuscript for the details). Note that the errors depend on the state ξ of the initial black hole $X_{\rm in}$, and also the dynamics $U_{\rm Kerr}$.

In the technical manuscript, we consider various initial states ξ. Here, we show only the case where the black hole is sufficiently old that $\xi^{X_{\rm in}}$ is the completely mixed state [22]. In this case, for almost any $U_{\rm Kerr}$, it holds that

$$\Delta_{inv}(\Phi : U_{\rm Kerr}) \lesssim 2^{\frac{k-c\ell}{2}}, \qquad (2)$$

$$\Delta(\Phi : U_{\rm Kerr}) \lesssim \sqrt{2^{k-c\ell} + N^{-C}}, \qquad (3)$$

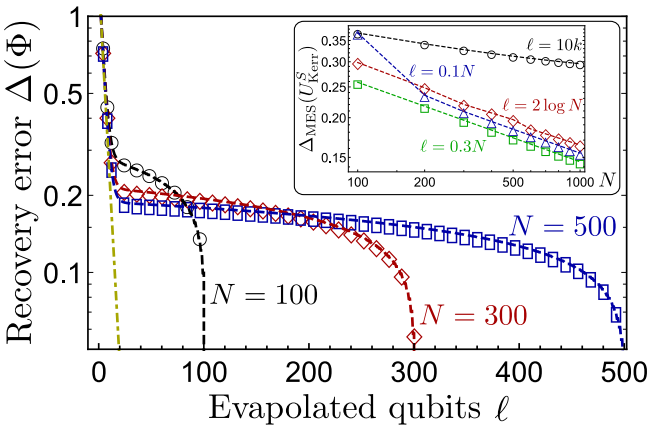


Figure 2: A semi-log plot of upper bounds of $\Delta_{inv}(\Phi)$ (yellow dash-dotted line), and $\Delta(\Phi)$ as a function of ℓ for $k = 1$ and various size N of the initial black hole $X_{\rm in}$, i.e. $N = 100$ (black $\circ$), 300 (red $\diamond$), and 500 (blue $\square$). While $\Delta_{inv}(\Phi)$ decreases exponentially quickly, $\Delta(\Phi)$ first decreases exponentially quickly, then stops decreasing, and eventually drops again when ℓ gets closer to $N + k$. The inset shows $\Delta(\Phi)$ as functions of N for $k = 1$, $\ell = 10k$ (black $\circ$), $2\log N$ (red $\diamond$), $0.1N$ (blue $\triangle$), and $0.3N$ (green $\square$). By fitting these plots, we obtain Ineq. (3).

where $1/2 \lesssim c \lesssim 1$ and $C \approx 0.5$ are numerically evaluated, and depend on k and ℓ only weakly (see also Fig. 2). In the technical manuscript, we argue the mechanism behind these results, which is related to not only partial decoupling, but also an intriguing encoding method, fluctuations of angular momentum in the initial black hole $X_{\rm in}$, and the entanglement between S_1 amd S_2 generated by $U_{\rm Kerr}$.

Since Ineq. (2) is independent of N, we clearly observe that, no matter how large the initial black hole is, symmetry-invariant information of A continues leaking out extremely quickly. On the other hand, the error $\Delta(\Phi)$ can be small only when the initial black hole $X_{\rm in}$ is sufficiently larger compared to the Alice's quantum source A. Otherwise, a certain amount of information of A, which should be mostly symmetry-variant one, remains unevaporated until the last moment.

In the technical manuscript, we also argue that these bounds are likely to be optimal.

References

[1] S. W. Hawking. Particle creation by black holes. *Commun. Math. Phys.*, 43(3):199–220, 1975.

[2] M. Horodecki, J. Oppenheim, and A. Winter. Partial quantum information. *Nature*, 436:673–

676, 2005.

[3] M. Horodecki, J. Oppenheim, and A. Winter. Quantum state merging and negative information. *Comms. Math. Phys.*, 269:107–136, 2007.

[4] P. Hayden and J. Preskill. Black holes as mirrors: quantum information in random subsystems. *J. High Energy Phys.*, 2007(09):120, 2007.

[5] Y. Sekino and L. Susskind. Fast scramblers. *J. High Energy Phys.*, 2008(10):065, 2008.

[6] N. Lashkari, D. Stanford, M. Hastings, T. Osborne, and P. Hayden. Towards the fast scrambling conjecture. *J. High Energy Phys.*, 2013(4):22, 2013.

[7] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner. One-shot decoupling. *Commun. Math. Phys.*, 328:251, 2014.

[8] T. Schuster N. M. Linke B. Yoshida N. Y. Yao K. A. Landsman, C. Figgatt and C. Monroe. Verified quantum information scrambling. *Nature*, 567:61–65, 2019.

[9] H. Shenker and D. Stanfor. Black holes and the butterfly effect. *J. High Energy Phys.*, 2014(3):67, 2014.

[10] D. A. Roberts and D. Stanford. Diagnosing Chaos Using Four-Point Functions in Two-Dimensional Conformal Field Theory. *Phys. Rev. Lett.*, 115(13):131603, 2015.

[11] S. H. Shenker and D. Stanford. Stringy effects in scrambling. *J. High Energy Phys.*, 2015(5):132, 2015.

[12] S. Sachdev and J. Ye. Gapless spin-fluid ground state in a random quantum Heisenberg magnet. *Phys. Rev. Lett.*, 70(21):3339–3342, 1993.

[13] A. Kitaev. A simple model of quantum holography. Talks at KITP, 2015.

[14] F. Pastawski, B. Yoshida, D Harlow, and J. Preskill. Holographic quantum error-correcting codes: toy models for the bulk/boundary correspondence. *J. High Energ. Phys.*, 2015(6):149, 2015.

[15] F. Pastawski, J. Eisert, and H. Wilming. Towards Holography via Quantum Source-Channel Codes. *Phys. Rev. Lett.*, 119(2):020501, 2017.

[16] B. Yoshida. Soft mode and interior operator in hayden-preskill thought experiment. arxiv:1812.07353 (2018).

[17] T. Banks and N. Seiberg. Symmetries and strings in field theory and gravity. *Phys. Rev. D*, 83(8):084019, 2011.

[18] D. Harlow and H. Ooguri. Constraints on symmetry from holography. *Phys. Rev. Lett.*, 122(19):191601, 2019.

[19] E. Wakakuwa and Y. Nakata. One-shot randomized and nonrandomized partial decoupling. arxiv:1903.05796 (2019).

[20] I. Devetak and P. W. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Comm. Math. Phys.*, 256(2):287–303, 2005.

[21] A. Winter and D. Yang. Operational resource theory of coherence. *Phys. Rev. Lett.*, 116(12):120404, 2016.

[22] D. N. Page. Average entropy of a subsystem. *Phys. Rev. Lett.*, 71(9):1291–1294, 1993.

Unconditional steady-state entanglement in macroscopic hybrid systems by coherent noise cancellation

Xinyao Huang[1 2 *] Emil Zeuthen[2] Denis V. Vasilyev[3 4] Qiongyi He[1]
Klemens Hammerer[5] Eugene S. Polzik[2]

[1] *State Key Laboratory of Mesoscopic Physics, School of Physics, Peking University, Collaborative Innovation Center of Quantum Matter, Beijing 100871, China*
[2] *Niels Bohr Institute, University of Copenhagen, DK-2100 Copenhagen, Denmark*
[3] *Center for Quantum Physics, Faculty of Mathematics, Computer Science and Physics, University of Innsbruck, A-6020 Innsbruck, Austria*
[4] *Institute for Quantum Optics and Quantum Information of the Austrian Academy of Sciences, A-6020 Innsbruck, Austria*
[5] *Institute for Theoretical Physics and Institute for Gravitational Physics (Albert Einstein Institute), Leibniz Universität Hannover, Callinstraße 38, 30167 Hannover, Germany*

Abstract. The generation of entanglement between disparate physical objects is a key ingredient in the field of quantum technologies, since they can have different functionalities in a quantum network. Here we propose and analyze a generic approach to steady-state entanglement generation between two oscillators with different temperatures and decoherence properties coupled in cascade to a common unidirectional light field. The scheme is based on a combination of coherent noise cancellation and dynamical cooling techniques for two oscillators with effective masses of opposite signs, such as quasi-spin and motional degrees of freedom, respectively. The interference effect provided by the cascaded setup can be tuned to implement additional noise cancellation leading to improved entanglement even in the presence of a hot thermal environment. The unconditional entanglement generation is advantageous since it provides a ready-to-use quantum resource. Remarkably, by comparing to the conditional entanglement achievable in the dynamically stable regime, we find our unconditional scheme to deliver virtually identical performance when operated optimally.

Keywords: Unconditional entanglement, hybrid system, coherent noise cancellation

1 Theoretical model

We consider a generic hybrid system composed of two subsystems with effective masses $\mathrm{sgn}(m_{\mathrm{S}}) = -\mathrm{sgn}(m_{\mathrm{M}}) < 0$ coupled to a unidirectional optical field $\hat{b}(t) = (2\pi)^{-1/2}\int_{-\infty}^{\infty}\hat{b}(\Omega)e^{-i\Omega t}d\Omega$ (defined in a rotating frame with respect to the optical carrier) [Fig. 1]. Both subsystems are driven by individual thermal reservoirs. The positive/negative mass subsystem is referred to as a motional/collective spin (M/S) degree of freedom and represented by a localized bosonic mode with dimensionless canonical variables $\hat{X}_j = (\hat{a}_j + \hat{a}_j^\dagger)/\sqrt{2}$ and $\hat{P}_j = (\hat{a}_j - \hat{a}_j^\dagger)/(\sqrt{2}i)$, $j \in \{\mathrm{M,S}\}$. The free evolution of the hybrid system is ($\hbar = 1$)

$$\hat{H}_0 = \sum_{j\in\{\mathrm{M,S}\}} \mathrm{sgn}(m_j)\frac{\omega_j}{2}(\hat{X}_j^2 + \hat{P}_j^2), \tag{1}$$

where ω_j is the oscillator resonance frequency, and we specialize to the resonant scenario $\omega_j = \omega$. The Hamiltonian for two-mode quadratic interaction between the localized oscillators and the light field is [1, 2]

$$\hat{H}_{\mathrm{int}} = \sum_{j\in\{\mathrm{M,S}\}} (\sqrt{\Gamma_{j\mathrm{B}}}\hat{a}_j^\dagger\hat{b}(t_j) + \sqrt{\Gamma_{j\mathrm{P}}}\hat{a}_j^\dagger\hat{b}^\dagger(t_j) + \mathrm{H.c.}), \tag{2}$$

where we assume $t_{\mathrm{S}} < t_{\mathrm{M}}$, i.e., the optical field interacts with S first. Equation (2) comprises two kinds of interaction: beam-splitter (B), $\propto (\hat{a}_j^\dagger\hat{b} + \mathrm{H.c.})$, and parametric down-conversion (P), $\propto (\hat{a}_j^\dagger\hat{b}^\dagger + \mathrm{H.c.})$. These processes produce sidebands at rates $\Gamma_{j\mathrm{B}} = \Gamma_j \sin^2\theta_j, \Gamma_{j\mathrm{P}} = \Gamma_j\cos^2\theta_j$ [Fig. 1, inset], which we parametrize by $\Gamma_j = \Gamma_{j\mathrm{B}} + \Gamma_{j\mathrm{P}}$ and $\theta_j \in [0, \pi/2]$, the coupling rates and angles.

Taking the rotating wave approximation in the regime of interest ($\omega \gg \Gamma_j \gtrsim \tilde{\gamma}_{j,0}$), the interaction with the light field is confined to two disjoint sidebands $\hat{b}_-(t) + \hat{b}_+(t) := (2\pi)^{-1/2}(\int_{-\infty}^{0} + \int_0^{\infty})\hat{b}(\Omega)e^{-i\Omega t}d\Omega = \hat{b}(t)$, $[\hat{b}_\pm(t), \hat{b}_\pm^\dagger(t')] = \delta(t-t')$, centered at frequencies $\Omega = \mp\omega$ (relative to the carrier). By eliminating the light field, the Heisenberg-Langevin equations can be expressed in terms of the forces $\hat{f}_j := \sqrt{\gamma_{j,0}}\hat{a}_{j,\mathrm{in}} + \hat{f}_{j,\mathrm{ba}}$ as

$$\begin{aligned}\frac{d}{dt}\hat{a}_{\mathrm{S}} &= -\frac{\gamma_{\mathrm{S}}}{2}\hat{a}_{\mathrm{S}} + \hat{f}_{\mathrm{S}},\\ \frac{d}{dt}\hat{a}_{\mathrm{M}} &= -\frac{\gamma_{\mathrm{M}}}{2}\hat{a}_{\mathrm{M}} + \hat{f}_{\mathrm{M}} + \sqrt{1-\epsilon}R\hat{a}_{\mathrm{S}}^\dagger,\end{aligned} \tag{3}$$

where

$$\begin{aligned}\hat{f}_{\mathrm{S,ba}} :=& -i(\sqrt{\Gamma_{\mathrm{SB}}}\hat{b}_{-,\mathrm{in}} + \sqrt{\Gamma_{\mathrm{SP}}}\hat{b}_{+,\mathrm{in}}^\dagger),\\ \hat{f}_{\mathrm{M,ba}} :=& -i\sqrt{1-\epsilon}(\sqrt{\Gamma_{\mathrm{MB}}}\hat{b}_{+,\mathrm{in}} + \sqrt{\Gamma_{\mathrm{MP}}}\hat{b}_{-,\mathrm{in}}^\dagger)\\ &- i\sqrt{\epsilon}(\sqrt{\Gamma_{\mathrm{MB}}}\hat{b}'_{+,\mathrm{in}} + \sqrt{\Gamma_{\mathrm{MP}}}\hat{b}'^\dagger_{-,\mathrm{in}}).\end{aligned} \tag{4}$$

Here, an additional uncorrelated vacuum $\hat{b}'_{\pm,\mathrm{in}}$ impinges on M due to transmission loss ϵ between the subsystems. $[\hat{a}_{j,\mathrm{in}}(t), \hat{a}_{j,\mathrm{in}}^\dagger(t')] = \delta(t-t')$, represent

*xyhuang.bnu@gmail.com

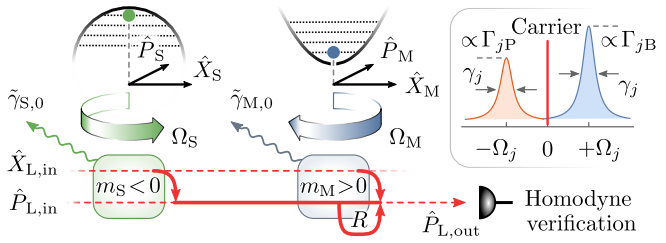


Figure 1: Hybrid system consisting of two oscillators with negative (S) and positive (M) mass, respectively. These are coupled in cascade to a common unidirectional light field via quadratic interactions induced typically by a strong, classical carrier. For each oscillator, this results in Stokes and anti-Stokes sidebands proportional to rates $\Gamma_{jP/B}$ and of width γ_j, $j \in \{\mathrm{S,M}\}$ (see inset); the effective resonance frequency $\Omega_j \equiv \mathrm{sgn}(m_j)\omega$ accounts for, e.g., the fact that energy must be extracted from a negative-mass oscillator to excite it. The negative mass system is driven by $\hat{X}_{\mathrm{L,in}}$ only ($\Gamma_{\mathrm{SP}} = \Gamma_{\mathrm{SB}}$) and its response is mapped onto $\hat{P}_{\mathrm{L}}$. The positive mass system is likewise coupled to $\hat{X}_{\mathrm{L,in}}$, but also to $\hat{P}_{\mathrm{L}}$ ($\Gamma_{\mathrm{MP}} < \Gamma_{\mathrm{MB}}$) at an adjustable rate R, so that the response of the negative mass system drives the positive mass system. Additionally, the oscillators are driven by distinct thermal reservoirs with decoherence rates $\tilde{\gamma}_{j,0}$ (wavy arrows).

the thermal noise fluctuations with $\langle \hat{a}_{j,\mathrm{in}}(t)\, \hat{a}^\dagger_{j,\mathrm{in}}(t')\rangle = (\bar{n}_j + 1)\delta(t-t')$ in terms of the thermal occupancy $\bar{n}_j$. Finally, due to the unidirectionality of the light field, information can only propagate from the first to the second subsystem in the cascade. The corresponding unidirectional coupling rate is $R = \sqrt{\Gamma_{\mathrm{SB}}\Gamma_{\mathrm{MP}}} - \sqrt{\Gamma_{\mathrm{MB}}\Gamma_{\mathrm{SP}}} = -\sqrt{\Gamma_{\mathrm{M}}\Gamma_{\mathrm{S}}}\sin(\theta_{\mathrm{M}} - \theta_{\mathrm{S}})$. $R \neq 0$ gives rise to a nontrivial asymmetry of the cascaded system (3), which is found to be advantageous for improved noise cancellation and entanglement generation.

2 Unconditional steady-state solution

The steady-state solution to Eqs. (3) is

$$\begin{aligned}
\hat{a}_{\mathrm{S}}(t) &= \int_{-\infty}^{t} dt' e^{-(t-t')\gamma_{\mathrm{S}}/2}\hat{f}_{\mathrm{S}}(t'),\\
\hat{a}_{\mathrm{M}}(t) &= \int_{-\infty}^{t} dt' \{e^{-(t-t')\gamma_{\mathrm{M}}/2}\hat{f}_{\mathrm{M}}(t') \\
&\quad + \frac{2\sqrt{1-\epsilon}R}{\gamma_{\mathrm{M}}-\gamma_{\mathrm{S}}}[e^{-(t-t')\gamma_{\mathrm{S}}/2} - e^{-(t-t')\gamma_{\mathrm{M}}/2}]\hat{f}^\dagger_{\mathrm{S}}(t')\}.
\end{aligned} \tag{5}$$

When the second system (M) in the cascade is relatively short-lived, $\gamma_{\mathrm{M}} > \gamma_{\mathrm{S}}$, then for $R \neq 0$ the unidirectional coupling term $\propto R a^\dagger_{\mathrm{S}}$ effectively prolongs the memory time $1/\gamma_{\mathrm{M}}$ by driving M with the spin response contained in the light field, resulting in improved coherent noise cancellation for $R < 0 \Leftrightarrow \theta_{\mathrm{M}} > \theta_{\mathrm{S}}$. Ideal cancellation can be achieved in the adiabatic limit $\gamma_{\mathrm{M}} \gg \gamma_{\mathrm{S}}$ and $2R/\gamma_{\mathrm{M}} \to -1$ (for $\epsilon = 0$) [Eq. (5)], which is compatible with the demand for near-ground-state dynamical cooling of the motional mode $\gamma_{\mathrm{M}} \gg \tilde{\gamma}_{\mathrm{M},0}$.

From Eqs. (5) the entries of the covariance matrix in steady state are

$$\begin{aligned}
\Delta^2\hat{X}_{\mathrm{S}} &= \frac{1}{\gamma_{\mathrm{S}}}\left(\frac{\Gamma_{\mathrm{S}}}{2} + \tilde{\gamma}_{\mathrm{S},0}\right),\\
\Delta^2\hat{X}_{\mathrm{M}} &= \frac{1}{\gamma_{\mathrm{M}}}\left(\frac{\Gamma_{\mathrm{M}}}{2} + \tilde{\gamma}_{\mathrm{M},0} + \sqrt{1-\epsilon}R\langle\hat{X}_{\mathrm{S}}, \hat{X}_{\mathrm{M}}\rangle\right),\\
\langle\hat{X}_{\mathrm{S}}, \hat{X}_{\mathrm{M}}\rangle &= -\frac{2\sqrt{1-\epsilon}}{\gamma_{\mathrm{S}}+\gamma_{\mathrm{M}}}\left(\sqrt{\Gamma_{\mathrm{S}}\Gamma_{\mathrm{M}}}\sin(\theta_{\mathrm{M}}+\theta_{\mathrm{S}}) - 2R\Delta^2\hat{X}_{\mathrm{S}}\right),
\end{aligned} \tag{6}$$

where $\langle\hat{X}_{\mathrm{S}}, \hat{X}_{\mathrm{M}}\rangle := \langle\hat{X}_{\mathrm{S}}\hat{X}_{\mathrm{M}}\rangle + \langle\hat{X}_{\mathrm{M}}\hat{X}_{\mathrm{S}}\rangle - 2\langle\hat{X}_{\mathrm{S}}\rangle\langle\hat{X}_{\mathrm{M}}\rangle$.

As our entanglement figure of merit we consider the variance of generalized EPR variables of the form [3, 4]

$$\xi_g = \frac{\Delta^2(\hat{X}_{\mathrm{S}} + g\hat{X}_{\mathrm{M}}) + \Delta^2(\hat{P}_{\mathrm{S}} - g\hat{P}_{\mathrm{M}})}{1+g^2} < 1, \tag{7}$$

where $g = \sqrt{\Gamma_{\mathrm{M}}/[(1-\epsilon)\Gamma_{\mathrm{S}}]}\cos(\theta_{\mathrm{M}}-\pi/4)/\cos(\theta_{\mathrm{S}}-\pi/4)$.

3 Spin-optomechanical implementation

Considering a spin-optomechanical implementation [5], Fig. 2 presents the optimized unconditional steady-state entanglement [Eq. (7)] as a function of quantum cooperativities $C_j := \Gamma_j/\tilde{\gamma}_{j,0}$, and illustrates the relaxation of parameter requirements compared to dissipative entanglement generation ($R = 0$). Entanglement optimization shows that for θ_{M}, beam-splitter interaction is optimal, $\pi/2 \geq \theta_{\mathrm{M,opt}} > \pi/4$, while for S, the Stokes and anti-Stokes processes should be balanced, $\theta_{\mathrm{S,opt}} \approx \pi/4 \Leftrightarrow \Gamma_{\mathrm{SB}} \approx \Gamma_{\mathrm{SP}}$ (QND interaction) yielding $R < 0$ [Fig. 3, inset]; this is the scenario illustrated in Fig. 1.

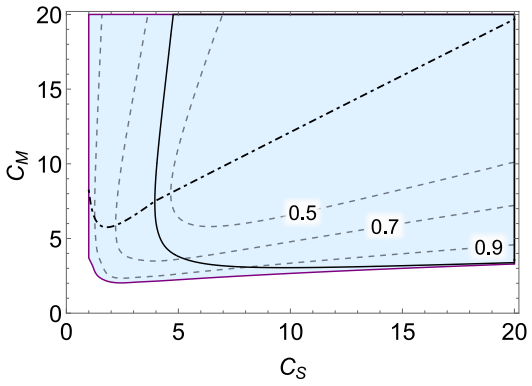


Figure 2: Entanglement ξ_g (< 1 in the colored region) as a function of C_j for optimized θ_{S} and θ_{M} while fixing the parameters $\gamma_{\mathrm{S},0} = 2\pi \times 5\mathrm{kHz}, \bar{n}_{\mathrm{S}} = 1, \gamma_{\mathrm{M},0}\bar{n}_{\mathrm{M}} = 2\pi \times 10\mathrm{kHz}$, and assuming $\epsilon = 0$. Optimal C_{M} for given C_{S} is indicated by the dashed-dotted curve. Imposing the additional constraint $\theta_{\mathrm{S}} = \theta_{\mathrm{M}} \Rightarrow R = 0$, entanglement $\xi_g < 1$ is only possible in the subregion delineated by the solid contour.

The optimal ξ_g is illustrated in Fig. 3. when $\epsilon = 0$, the asymptotic scaling of the unconditional entanglement is $\xi_g \approx \sqrt{[1 + r + 1/(2\bar{n}_{\mathrm{S}}+1)]/(2C_{\mathrm{S}})}$, where $r = \tilde{\gamma}_{\mathrm{M},0}/\tilde{\gamma}_{\mathrm{S},0}$. An improvement by up to a factor of 2 can be found when comparing to the dissipative case ($R = 0$), $\xi_g \approx \sqrt{2(1+r)/C_{\mathrm{S}}}$. The presence of loss $\epsilon > 0$ imposes

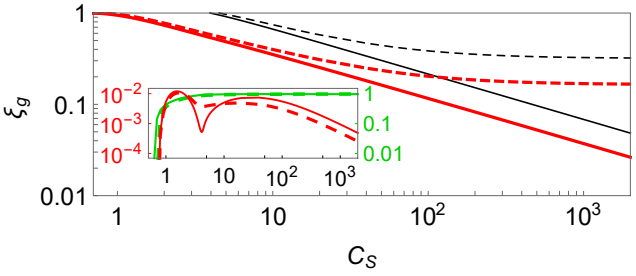


Figure 3: Entanglement ξ_g as a function of $C_{\rm S}$ for optimized $\theta_{\rm S}, \theta_{\rm M}$ and $C_{\rm M}$ when $R = 0$ (thin black curves) and $R \neq 0$ (thick red curves), when $\epsilon = 0$ (solid), and $\epsilon = 0.1$ (dashed). (Inset) Plot of $-2\sqrt{1-\epsilon}R/\gamma_{\rm M}$ (right scale, brighter green curves) as a function of $C_{\rm S}$ used in evaluating the optimized curves of the main plot, and the relative entanglement improvement (left scale, darker red curves) of the conditional scheme over the optimal unconditional scheme (referenced to the latter) for $\epsilon = 0.1$; the conditional performance is evaluated using parameters optimized for the unconditional scheme (dashed) and optimal conditional parameters for QND readout $\theta_{\rm S} = \theta_{\rm M} = \pi/4$ (solid). The fixed parameters are $\gamma_{\rm S,0} = 2\pi \times 5{\rm kHz}$, $\bar{n}_{\rm S} = 1$, and $\gamma_{\rm M,0}\bar{n}_{\rm M} = 2\pi \times 10{\rm kHz}$.

a lower bound $\xi_g \geq \sqrt{\epsilon/(4-3\epsilon)}$, which is also an improvement of up to a factor of 2 compared to $R = 0$.

4 Comparison with conditional scheme

Another benchmark is the conditional steady-state entanglement generated by performing a continuous homodyne measurement of the light field emanating from the hybrid system [2]. The evolution of the system conditioned on the measurement record is described by a stochastic master equation whose steady state can be found numerically and even analytically in our regime of interest, $\bar{n}_{\rm M} \gg 1$ [6]. For the fixed parameters considered above [Fig. 3], we find in the limit of substantial entanglement that, remarkably, the conditional steady-state entanglement matches that of our unconditional scheme within a few-percent margin, even when separately optimized under the same conditions in the dynamically stable regime (see Fig. 3, inset). We thus conclude that our unconditional scheme leaves practically no information in the output light about the noise affecting the squeezed EPR variables. From a practical standpoint this is beneficial as it allows optimal performance without the need to measure the output field nor perform the feedback required to make the conditional entanglement unconditional. Moreover, the dynamical cooling of the motional mode occurring in the unconditional scheme facilitates technical stability in the apparatus.

5 Conclusion

In conclusion, unconditional steady-state entanglement in a cascaded negative-positive mass hybrid system can be efficiently generated by engineering an asymmetric interaction between the subsystems via the light field connecting them. Applications for such a resource of ready-to-use entanglement include quantum teleportation [7] and key distribution [8] in hybrid quantum networks. The scheme can compete with conditional schemes, a fact which we speculate can be elucidated by formally framing our unconditional scheme in terms of a coherent-feedback master equation. Moreover, we have evidence that this sensing enhancement is closely linked to the generation of EPR-type entanglement studied here [6], warranting further study.

References

[1] C. A. Muschik, E. S. Polzik, and J. I. Cirac, *Phys. Rev. A* **83**, 052312 (2011).

[2] D. V. Vasilyev, C. A. Muschik, and K. Hammerer, *Phys. Rev. A* **87**, 053820 (2013).

[3] R. Simon, *Phys. Rev. Lett.* **84**, 2726 (2000).

[4] V. Giovannetti, S. Mancini, D. Vitali, and P. Tombesi, *Phys. Rev. A* **67**, 022320 (2003).

[5] C. B. Møller, R. A. Thomas, G. Vasilakis, E. Zeuthen, Y. Tsaturyan, M. Balabas, K. Jensen, A. Schliesser, K. Hammerer, and E. S. Polzik, *Nature* **547**, 191-195 (2017).

[6] X. Huang, E. Zeuthen, D. V. Vasilyev, Q. He, K. Hammerer, and E. S. Polzik, *Phys. Rev. Lett.* **121**, 103602 (2018).

[7] Q. He, L. Rosales-Zárate, G. Adesso, and M. D. Reid, *Phys. Rev. Lett.* **115**, 180502 (2015).

[8] N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, *Optica* **3**, 634 (2016).

Quantum algorithm for estimating α-Renyi entropies of density matrices in an oracular setting

Sathyawageeswar Subramanian[1] * Min-Hsiu Hsieh[2] †

[1] *DAMTP, Centre for Mathematical Sciences, University of Cambridge, Cambridge CB3 0WA, United Kingdom*
[2] *Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, Australia*

Abstract. We describe a quantum algorithm to estimate the α-Renyi entropy of an unknown density matrix $\rho \in \mathbb{C}^{d\times d}$ for $\alpha \neq 1$ by combining the recent technique of quantum singular value transformations with the method of estimating normalised traces in the one clean qubit model. We consider the oracular input model, where the input state is prepared via a quantum oracle that outputs a purified version of the state. Our method requires $\mathcal{O}(da\alpha/\delta\epsilon^2)$ queries and $\lceil \log d \rceil + 3$ qubits to estimate the α-Renyi entropy to additive precision ϵ, in contrast to results in the sample complexity model that generically require $\mathcal{O}(d^2/\epsilon^2)$ samples. here a is the dimension of the ancillary register used, and δ is a lower bound on the smallest eigenvalue of ρ, assumed to be non-singular.

Keywords: Matrix functions, entropy estimation, DQC1

1 Introduction

Entropy functions are an extremely important characterization of a quantum system. In entanglement theory, they characterize the amount of entanglement contained in bipartite quantum systems. They are also often used as operational measures in quantum information-processing tasks. As one of the most famous examples, they provide the asymptotic lower bound for the quantum systems to be compressed in a noiseless fashion, i.e. Schumacher's noiseless compression (Schumacher (1995)). Hence it stands a fundamental question to evaluate these entropy functions efficiently.

For $\alpha > 0$ and $\alpha \neq 1$, the family of α-Renyi entropies of a positive semidefinite (PSD) operator $\rho \in \mathbb{C}^{d\times d}$ are defined by

$$S_\alpha(\rho) := \frac{1}{1-\alpha} \log \left[\operatorname{Tr}\left(\rho^\alpha\right) \right]. \tag{1}$$

Taking the limit $\alpha \to 1$ gives the familiar von Neumann entropy, $S_1(\rho) = -\operatorname{Tr}(\rho \log \rho)$. Hastings et al. (2010) discuss a quantum Monte Carlo method to measure the 2-Renyi entropy of a many-body system by evaluating the expectation value of a unitary swap operator using a number of samples that scales polynomially number in the system size. More in the flavour of quantum algorithms, Acharya et al. (2017) study the copy complexity of estimating von Neumann and Renyi entropies of mixed states of quantum systems, in a model where as input one gets n independent copies of an unknown d-dimensional density matrix ρ. They allow arbitrary quantum measurements and classical post-processing. The experimental measurement of the entropy of specific quantum systems has also recently been investigated (Islam et al., 2015).

While it enables a tight characterisation of the copy or sample complexity of the problem (table 1), other input models are also possible which are not captured in this picture. In this paper, we consider an oracular input model that is popular in quantum query algorithms, wherein data is accessed in the form of a quantum state. This state may be the output of some other quantum subroutine, in which case that subroutine itself is the oracle. Such input models can also capture the fact that we have access to the process generating the unknown quantum state, which we may *a priori* expect to be useful in reducing the effort required in estimating properties of the state.

2 Main Result

We constructively prove the following theorem:

Theorem 1 *Given a unitary process U_ρ on $\mathbb{C}^{d+a}$ which produces a purification $|\psi_\rho\rangle$ of the actual input state $\rho \in \mathbb{C}^{d\times d}$ with $\mathbb{1}/\delta \preceq \rho \preceq \mathbb{1}$, there exists a quantum algorithm that outputs an estimate of the α-Renyi entropy of ρ to additive precision ϵ, making $\mathcal{O}(da\alpha/\delta\epsilon^2)$ uses of U_ρ and $\mathcal{O}(da\alpha/\delta\epsilon^2)$ additional 1- and 2-qubit gates, where $\alpha > 0$ and $\alpha \neq 1$.*

The algorithm is constructed using the technique of block-encodings and quantum singular value transformations (Chakraborty et al., 2018; Gilyén and Li, 2019) in order to implement unitaries on the system plus ancillary qubit registers that are block encodings of the power functions ρ^α, and subsequently estimating the trace of these unitaries in the DQC1 or "one-clean qubit" model of computation (Knill and Laflamme (1998)).

The key contributions that set our idea apart from previous work are (1) the direct (without projections) use of unitary block encodings of the target operator functions obtained using quantum matrix function implementation techniques, and (2) the replacement of amplitude estimation using the quantum counting techniques of Brassard et al. (2002) with trace estimation in DQC1. In essence, this means that our algorithm outputs a deterministic ϵ-additive approximation of the target quantity, and furthermore, since we use the one-clean qubit model, our

*ss2310@cam.ac.uk
†min-hsiu.hsieh@uts.edu.au

Functional	Copies $\Theta(\cdot)$	Queries $\mathcal{O}(\cdot)$
$\alpha < 1$	$d^{2/\alpha}$	d
$\alpha = 1$ (von Neumann)	d^2	-
$\alpha > 1$ integer	$d^{2-2/\alpha}$	$d\alpha$
$\alpha > 1$ non-integer	d^2	$d\alpha$

Table 1: Dimension dependence of copy complexity characterisations from Acharya et al. (2017) for estimating the Renyi entropies of an unknown d-dimensional mixed state for exponents of various ranges, contrasted with query complexity in this paper (see section 4).

method does not require long coherence times or high circuit depth where powers (controlled on ancillary registers) of an input unitary and need to be performed for phase estimation.

3 Preliminaries

In this section we outline the main technical tools we use, and provide a proof outline of our main result.

3.1 Input model

We assume access to a unitary process U_ρ on $\mathbb{C}^{d+a}$ which produces a purification $|\psi_\rho\rangle$ of the actual input state ρ in $\mathbb{C}^{d\times d}$

$$U_\rho \left|0\right\rangle^{\otimes d+a} = \left|\psi_\rho\right\rangle = \sum_{i=1}^{n} \sqrt{p_i} \left|\phi\right\rangle_a \left|\psi\right\rangle_d , \tag{2}$$

so that $\mathrm{Tr}_a\left(\left|\psi_\rho\right\rangle\!\left\langle\psi_\rho\right|\right) = \rho$. The $\{\left|\phi\right\rangle_a\}$ and $\{\left|\psi\right\rangle_d\}$ are sets of orthonormal vectors on the ancillary and system subspaces respectively. This model, known as the purified quantum query access model, is also discussed by Gilyén and Li (2019) and Belovs (2019) in the context of property testing.

Note that the case of a classical probability distribution on d points with sampling access is subsumed into this model by embedding it into the diagonal state $\rho_p = \sum_{i=1}^{d} p_i \left|i\right\rangle$.

3.2 Implementing power functions of Hermitian matrices

A block-encoding U_A of a Hermitian matrix A is essentially a unitary that encodes a (sub-)normalised version of A in its top left block, i.e.

$$U_A = \begin{pmatrix} A/\|A\| & \cdot \\ \cdot & \cdot \end{pmatrix}, \tag{3}$$

and the behaviour and use of such encodings has been extensively studied in the last two years (Low and Chuang, 2017; Chakraborty et al., 2018; Gilyén et al., 2018). Given access to U_A, a variety of smooth matrix functions (defined on the spectrum of A) may be implemented, in the sense that a new block encoding U_A^f can be obtained such that

$$U_A^f = \begin{pmatrix} f(A)/\beta & \cdot \\ \cdot & \cdot \end{pmatrix}, \tag{4}$$

where $\beta \geq \|f(A)\|$. In particular, here we are interested in power functions $f(x) = x^\alpha$ for an exponent $\alpha > 0$. These can be realised using e.g. Lemma 9 of Chakraborty et al. (2018) or Corollary 67 of Gilyén et al. (2018), with minor modifications. The first step is to notice that by Lemma 45 of Gilyén et al. (2018), the input oracle U_ρ in Eqn. (2) gives an exact block encoding V_ρ on $\mathbb{C}^{d+a}$; indeed we have

$$V_\rho = \left(U_\rho^\dagger \otimes \mathbb{1}_d\right)\left(\mathbb{1}_a \otimes \mathsf{SWAP}_d\right)\left(U_\rho \otimes \mathbb{1}_d\right). \tag{5}$$

With the slightly technical assumption that ρ is full rank, if $\frac{\mathbb{1}}{\delta} \preceq \rho \preceq \mathbb{1}$ for $\delta > 0$, then for $\epsilon \in (0, 1/2]$ and $\alpha > 0$ an ϵ-approximate block encoding of ρ^α can be created with $\mathcal{O}(\frac{\max(1,\alpha)}{\delta} \log \frac{1}{\epsilon})$ uses of V_ρ and $\lceil \log a \rceil + 2$ ancillary qubits. The precision ϵ specifies how close the top left block of the new encoding is to ρ^α in the operator norm. We quote all the lemmata that we use in the appendix for convenience.

The assumption of full rank is reasonable if we expect to deal with noisy or random states, since lower rank indicates being closer to a pure state, as measured by the S_0 or max-entropy. Furthermore, there are ways to implement the matrix function only on the non-singular part of the input (e.g. Harrow et al. (2009)), and for classical distributions, we can consider the restriction to the support of the distribution by pre-processing using e.g. sparse PCA.

3.3 DQC1 Model

The DQC1 or "one-clean qubit" model of computation is based on the use of a single well-controlled or 'clean' qubit, and a number n of noisy qubits that are taken to be in the maximally mixed state (Knill and Laflamme, 1998; Shor and Jordan, 2008). Algorithms in this model are embedded into some controlled n-qubit unitaries, and the outputs are encoded into the probability of observing 0 on measuring the clean qubit. Estimating the normalised trace of a unitary is known to be a DQC1-complete problem (Knill and Laflamme, 1998).

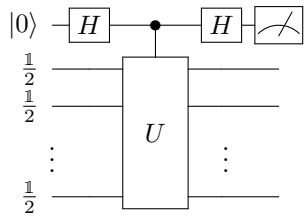


Figure 1: A DQC1 circuit that can be used to estimate $\mathrm{Tr}(U)$, for which no classical efficient algorithm is known. Measurements are made in the computational basis.

The initial state consists of one qubit set to the $|0\rangle$ state, and n qubits in the maximally mixed state, i.e. $\xi_{\text{in}} = |0\rangle\!\langle 0| \otimes \mathbb{1}_n/2^n = \frac{\mathbb{1}+Z}{2} \otimes \mathbb{1}_n/2^n$. We can write the final state after the application of the circuit but before

measurement in figure 1 as

$$\xi_{\text{out}} = \frac{1}{2^{n+1}} \begin{pmatrix} \mathbb{1}_n & U^\dagger \\ U & \mathbb{1}_n \end{pmatrix}, \tag{6}$$

from which we see that the expectation values of the Pauli X and Y operators for the clean qubit give the estimates $\langle X \rangle = 2^{-n}\text{Re}(\,\text{Tr}\,(U))$ and $\langle Y \rangle = -2^{-n}\text{Im}(\,\text{Tr}\,(U))$.

Here we are obtaining an ϵ additive approximation $\tilde{A}$ to some unknown quantity A, i.e. $|A - \tilde{A}| \leq \epsilon$. Often we may be interested in an ϵ multiplicative approximation with $(1-\epsilon)A \leq \tilde{A} \leq (1+\epsilon)A$. Given a lower bound $0 < \lambda \leq |A|$, an appropriate additive precision can be chosen to get a desired precision multiplicative approximation. The complexity of multiplicative approximation increases by a factor of $\mathcal{O}(\lambda^{-1})$ over additive approximation. If we know independent of the problem size that $|A| > 1$, then an ϵ-additive approximation immediately gives a good $\epsilon' < \epsilon$ multiplicative approximation.

4 Outline of the Algorithm

Using the block encoding technique, we first convert the block encoding of ρ into an ε-approximate block encoding for ρ^α (note that for integral values of α we can obtain an exact encoding with $\varepsilon = 0$, e.g. using Chebyshev polynomial methods as in Subramanian et al. (2018)):

$$U_\rho = \begin{pmatrix} \rho & \cdot \\ \cdot & \cdot \end{pmatrix} \mapsto \begin{pmatrix} f_\alpha(\rho) & \cdot \\ \cdot & \cdot \end{pmatrix} \approx U_{\rho^\alpha},$$

where $||f_\alpha(\rho) - \rho^\alpha|| < \epsilon$. This conversion requires $\mathcal{O}\left(\frac{\max(1,\alpha)}{\delta} \log \frac{1}{\varepsilon}\right)$ uses of the block encoding of U_ρ, and $\lceil \log a \rceil + 2$ ancillary qubits, where $\delta > 0$ lower bounds the least eigenvalue of ρ (Corollary 67, Gilyén et al. (2018)).

The trace of this $d + a$-dimensional unitary U_α can be estimated to precision ϵ with probability at least $1 - \eta$ with $\mathcal{O}(\log \frac{1}{\eta}/\epsilon^2)$ uses of the unitary (or more precisely of the DQC1 circuit in Fig. 1).

Since this unitary has the block form

$$U_\alpha = \begin{pmatrix} \rho^\alpha & \cdot \\ \cdot & \cdot \end{pmatrix},$$

its trace contains a contribution from $\,\text{Tr}\,(\rho^\alpha)$. What we would like is to isolate this term alone. Importantly, we know that $\,\text{Tr}\,(\rho^\alpha)$ will be real and positive.

Using the same unitary, but applying an appropriate block-encoded phase operation to convert the target matrix function to $i\rho^\alpha$ allows us to use the difference between the real and imaginary parts of the trace of the two unitaries U_α and U'_α to recover $\,\text{Tr}\,(\rho^\alpha)$, i.e. consider the unitary $U'_\alpha = U_\alpha V_{\text{phase}}$ where the unitary V_{phase} is defined by

$$V_{\text{phase}} = i\,|0\rangle\langle 0| \otimes \mathbb{1} + \sum_{k=1}^{n-1} |k\rangle\langle k| \otimes \mathbb{1}, \tag{7}$$

which can easily be arranged using an ancillary qubit initialised to the $|+\rangle$ state to which a condition rotation of $R_y(\pi/2)$ is applied.

Thus, exploiting the fact that the trace we are interested in is purely real, we can estimate $\,\text{Tr}\,(\rho^\alpha)$ by $\text{Re}(\,\text{Tr}\,(U_\alpha)) - \text{Re}(\,\text{Tr}\,(U'_\alpha))$, using twice as many measurements and uses of U_α as required for estimating $\text{Re}(\,\text{Tr}\,(U_\alpha))$ itself.

Finally, since we get the *normalised* trace, the error in the actual target functional we are estimating increases by the factor of $2^{\log d + \log a}$, which means that we need to choose $\epsilon' = 2^{\log d + \log a}\epsilon$ in the DQC1 step. This results in a net query complexity of $\mathcal{O}(da\alpha/\epsilon^2)$, which is similar to the copy complexity results in Acharya et al. (2017), but closer to linear in the dimension of the input state. The logarithmic factor in ε appearing in the block encoding contributes at most a logarithmic factor to the final complexity, which we leave out of the expression above.

5 Discussion and Outlook

One way to motivate trace estimation in DQC1 is the well-known Hadamard test. The same asymptotic complexity in terms of the number of queries, qubits, and measurements might also be achievable using a SWAP test based approach, scaling as $\mathcal{O}(d/\epsilon^2)$ (although the constants and exact gate complexities are expected to be different, and we hope to perform a thorough analysis). The advantage in using the DQC1 method is that only one well controlled, 'clean' qubit is required. On the other hand, using the SWAP test to estimate measurement outcome frequencies requires the preparation of suitable initial states which introduces additional sources of error and circuit complexity. The same is true of the amplitude estimation methods which have previously been used for entropy estimation in quantum property testing algorithms, which in addition requires long coherence times and the application of U_ρ and $U_\rho^\dagger$ controlled on large ancillary registers, and the quantum fourier transform for phase estimation.

One of the drawbacks of our method is that we obtain estimates of the target entropic quantities to additive precision rather than multiplicative precision — multiplicative precision is particularly preferred when the quantity of interest could be small, and entropies can indeed take values in $[0, 1) \subseteq [0, \log d]$ where d is the dimension of the system — although this happens only when the input is not very random (and close to being a pure state), as quantified by the small entropy.

We do not claim that the method we have proposed is optimal in either the dimension or the precision, and are considering different techniques in ongoing work, in order to improve the query complexity. We remark that the block encoding methods allow the implementation of several other matrix functions, which may facilitate the estimation of other entropy-like matrix functionals; there are also several possible applications of estimating entropic functionals as a subroutine in algorithmic procedures for pattern matching, compression tasks, and so on, that could take advantage of our method.

References

Acharya, J., Issa, I., Shende, N. V., and Wagner, A. B. (2017). Measuring Quantum Entropy.

Belovs, A. (2019). Quantum Algorithms for Classical Probability Distributions. pages 1–14.

Brassard, G., Hoyer, P., Mosca, M., and Tapp, A. (2002). Quantum amplitude amplification and estimation. *Quantum Computation and Information, Contemporary Mathematics*, 305:53–74.

Chakraborty, S., Gilyén, A., and Jeffery, S. (2018). The power of block-encoded matrix powers: improved regression techniques via faster Hamiltonian simulation. pages 1–60.

Gilyén, A. and Li, T. (2019). Distributional property testing in a quantum world. pages 1–18.

Gilyén, A., Su, Y., Low, G. H., and Wiebe, N. (2018). Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics.

Harrow, A. W., Hassidim, A., and Lloyd, S. (2009). Quantum Algorithm for Linear Systems of Equations. *Physical Review Letters*, 103(15):150502.

Hastings, M. B., González, I., Kallin, A. B., and Melko, R. G. (2010). Measuring renyi entanglement entropy in quantum Monte Carlo simulations. *Physical Review Letters*, 104(15):2–5.

Islam, R., Ma, R., Preiss, P. M., Tai, M. E., Lukin, A., Rispoli, M., and Greiner, M. (2015). Measuring entanglement entropy in a quantum many-body system. *Nature*, 528(7580):77–83.

Knill, E. and Laflamme, R. (1998). Power of one bit of quantum information. *Physical Review Letters*, 81(25):5672–5675.

Low, G. H. and Chuang, I. L. (2017). Optimal Hamiltonian Simulation by Quantum Signal Processing. *Physical Review Letters*, 118(1):010501.

Schumacher, B. (1995). Quantum coding. *Phys. Rev. A*, 51:2738–2747.

Shor, P. W. and Jordan, S. P. (2008). Estimating jones polynomials is a complete problem for one clean qubit. *Quantum Info. Comput.*, 8(8):681–714.

Subramanian, S., Brierley, S., and Jozsa, R. (2018). Implementing smooth functions of a hermitian matrix on a quantum computer.

A Implementing power functions of density matrices

The conversion of a purified access oracle as in Eqn. 2 into a block encoding for ρ can be achieved using the following result.

Lemma 2 (Lemma 45, Gilyén et al. (2018)) *Given a unitary U_ρ acting on $n + a$-qubits, which prepares a purification $U_\rho |0\rangle |0\rangle = |\psi_\rho\rangle$ of an n-qubit density operator ρ, such that $Tr_a(\psi_\rho) = \rho$ the unitary $\left(U_\rho^\dagger \otimes \mathbb{1}_n\right)(\mathbb{1}_a \otimes \mathsf{SWAP}_n)(U_\rho \otimes \mathbb{1}_n)$ gives an exact block encoding of ρ.*

A block encoding as above can be used to implement ϵ-approximate block encodings of power functions ρ^α given the promise that the spectrum of $\rho \in [\delta, 1]$ for $\delta > 0$ by using polynomial approximations, resulting in the following corollary.

Lemma 3 (Gilyén et al. (2018)) *Given an exact unitary block encoding V_ρ of a d-qubit density matrix ρ, that uses a- ancillary qubits, we can implement an ε-approximate block encoding of ρ^c for $c > 0$ using $\mathcal{O}(\frac{\max(1,c)}{\delta} \log \frac{1}{\varepsilon})$ applications of V_ρ, and $a + 2$- ancillary qubits. Here we assume that $\|\rho\| \geq \delta > 0$.*

Methodology for replacing indirect measurements with direct measurements

Kosuke Mitarai[1] Keisuke Fujii[1 2]

[1] *Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka 560-8531, Japan.*

[2] *JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama 332-0012, Japan*

Abstract. The indirect measurement of unitary operators such as the Hadamard test plays an important role in many quantum algorithms. In certain cases, the indirect measurement can be reduced to the direct measurement, where a quantum state is destructively measured. Here, we investigate in under what conditions such a replacement is possible and develop a general methodology. The results can be applied to construct quantum circuits to evaluate the analytical derivatives of a parameterized quantum state and one to measure the out-of-time-order correlator. Our protocols can reduce the depth of a quantum circuit by making the controlled operation unnecessary, and thus are suitable for near-term quantum algorithms.

Keywords: Hadamard test, indirect and direct measurement, near-term quantum device

1 Introduction

The output from quantum computation is measured in two ways: indirect and direct measurements of observables. In the former, the measured quantum state is not completely destructed, whereas, in the latter, the state collapses to the basis on which we perform the measurement. The simplest and most important protocol for the indirect method is the Hadamard test (Fig. 1). In the Hadamard test, we add an ancillary qubit and apply a controlled unitary gate, a unitary U to a target quantum state $|\psi\rangle$ conditioned on the ancilla being $|0\rangle$ or $|1\rangle$ to measure the expectation value of U, $\langle\psi|U|\psi\rangle$, as the expectation value of the Pauli Z operator of the ancilla. This measurement allows us to reuse the state $(I\pm U)|\psi\rangle/\sqrt{2}$ after the measurement, which is the property exploited in algorithms like iterative phase estimation [1, 2].

Such indirect approaches can achieve a precision of ϵ in $O(1/\epsilon)$ time. However, the implementation of the controlled-U gate can be a hard task especially for so-called noisy intermediate scale quantum (NISQ) [3] devices. In fact, direct measurements can be satisfiable when only the expectation value of an observable is required. A famous example is the estimation of the energy expectation values in the variational quantum eigensolver (VQE) [4], which is one of the most promising applications of NISQ devices. The time required to achieve a precision of ϵ is $O(1/\epsilon^2)$ in this approach, which is much longer than that of the indirect approach [5, 6].

Another example, which replaces the indirect approach with the direct one, is the destructive swap test [7]. The destructive swap test is a direct version of the swap test [8] which measures the overlap $|\langle\psi|\varphi\rangle|^2$ between two quantum states $|\psi\rangle$ and $|\varphi\rangle$. Initially proposed in [7], this method has been rediscovered by machine learning approach [9], and it is now utilized in the application of NISQ devices [10, 11, 12]. Ref. [13] has proposed to use the destructive swap test to measure $|\langle\psi|U|\psi\rangle|^2$ for an arbitrary U by substituting $|\varphi\rangle$ with $U|\psi\rangle$, and the protocol was extended to measure the quantity $|\langle\psi|P|\varphi\rangle|^2$, where P is a qubit-permutation operator, which can be employed to estimate nonlinear functionals of a quantum state ρ such as $\mathrm{Tr}(\rho^n)$ [14], with a low-depth circuit.

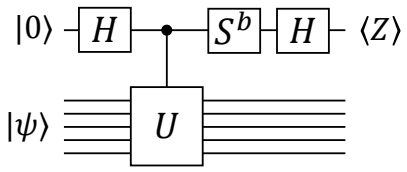


Figure 1: Simplest Hadamard test. In the figure, $b \in \{0,1\}$ and U, H, S are an arbitrary quantum gate, the Hadamard gate, and $e^{-i\pi Z/4}$, respectively. When $b=0$, $\langle Z\rangle = \mathrm{Re}\,\langle\psi_{\mathrm{in}}|U|\psi_{\mathrm{in}}\rangle$ and when $b=1$, $\langle Z\rangle = \mathrm{Im}\,\langle\psi_{\mathrm{in}}|U|\psi_{\mathrm{in}}\rangle$.

Furthermore, methods for gradient estimation employed in variational quantum algorithms (VQA) also illustrate the correspondence between those two approaches for certain cases. VQAs, such as the VQE, employ a parameterized quantum circuit $U(\boldsymbol{\theta})$ and classical optimizer, which minimizes a cost function $\mathcal{L}(\boldsymbol{\theta})$ by iteratively tuning the circuit parameter $\boldsymbol{\theta}$. The cost is usually computed from the expectation values of observables, therefore, their gradient can be a key ingredient for the optimization. We can estimate the gradient in two ways. Indirect and direct schemes have been proposed in Ref. [15] and Refs. [16, 17], respectively. The indirect method uses two different quantum circuits to estimate one element of the gradient.

These examples motivate us to further develop the methodology for replacing the indirect measurement with the direct measurement. In this work, we describe the general protocol for such replacements. The protocols for the Hadamard test involving a single controlled gate are given in Results 1 and 2. Result 1 is a generalization of the method used in VQE, and Result 2 is a generalization of the destructive swap test which can be applied to general local unitary gates. Finally, in Result 3, we

*u801032f@ecs.osaka-u.ac.jp

describe a method to replace the Hadamard test involving multiple controlled gates. It is a generalization of the method to estimate the gradient of observables with direct measurements, that is, we employ multiple quantum circuits to estimate the output of the Hadamard test. The proposed method can significantly reduce the depth of a quantum circuit and the accumulation of noise in the measured quantity. Based on the above results, we propose new methods derivatives including the metric tensor $g_{jk} = \frac{\partial\langle\psi(\boldsymbol{\theta})|}{\partial\theta_j}\frac{\partial|\psi(\boldsymbol{\theta})\rangle}{\partial\theta_j}$ of the variational quantum state $|\psi(\boldsymbol{\theta})\rangle$. Specifically, the metric tensor is a key quantity in variational quantum simulations [18, 19]. Finally, we present a new protocol to measure the multipoint correlator, such as the out-of-time-order correlators (OTOC), which is an important quantity in a quantum many-body system as a possible measure of the quantum chaos [20, 21, 22, 23].

2 Results

2.1 Hadamard test with one controlled gate

A simple case of possible replacements is where the gate U can be decomposed into the sum of the Pauli products $\mathcal{P} = \{I, X, Y, Z\}^{\otimes n}$ consisting of the polynomial number of terms. In this case, we can measure $\langle\psi|U|\psi\rangle$ without the Hadamard test by evaluating each of the Pauli terms separately.

Result 1: *If the gate U can be decomposed into the sum of the Pauli products with the polynomial number of terms with respect to the number of qubits, the output of Fig. 1, $\langle\psi|U|\psi\rangle$, can be estimated by direct measurement by evaluating each Pauli term.*

A prototypical example of the above result is the replacement of the phase estimation with direct measurements in the VQE. The tradeoff of the protocol above is the time required to achieve the precision of ϵ. It scales as $O(1/\epsilon^2)$ in the direct approach and $O(1/\epsilon)$ in the indirect approach, i.e., the phase estimation.

The next result is a method for another case where the quantum gate U is sufficiently local. It is the generalization of the destructive swap test [7]. We say U is k-local if U can be decomposed into a tensor product of unitary matrices as $U = \bigotimes_q U_q$ and each U_q acts on at most k-qubit.

Result 2: *Let k be an integer such that $k = O(\mathrm{poly}(\log n))$, where n is the number of qubits. For any k-local quantum gate U, it is possible to estimate $\langle\psi|\,U\,|\psi\rangle$ up to the precision ϵ in time $O(k^2 2^k/\epsilon^2)$ without the use of the Hadamard test, with classical preprocessing of time $O(\mathrm{poly}(\log n))$.*

Rough reasoning for this result is the following. If we let $k = O(\log n)$, U can be diagonalized on classical computer in time $O(\mathrm{poly}(\log n))$. The classical computation can also find a quantum circuit that transforms eigenvector of U to the computational basis, and a k-qubit circuit in general needs $O(k^2 2^k)$ elementary gates to be constructed [24]. We can apply the circuit to a state $|\psi\rangle$ and measure the resultant state in the computational basis to evaluate.

2.2 Hadamard test with multiple controlled gates

The protocol given below is for the Hadamard test with two controlled gates (Fig. 2 (a)). It is straightforward to generalize the method to the case of more than two controlled gates. In the case of Fig. 2 (a), the measured quantity is $\langle\psi|W^\dagger UW e^{-i\theta_1 G/2}|\psi\rangle$. If we assume $G^2 = I$,

$$\begin{aligned}&\langle\psi|W^\dagger UW e^{-i\theta_1 G/2}|\psi\rangle\\ &= \cos\frac{\theta_1}{2}\langle\psi|W^\dagger UW|\psi\rangle - i\sin\frac{\theta_1}{2}\langle\psi|W^\dagger UWG|\psi\rangle\,. \quad (1)\end{aligned}$$

The first term on the right hand side of the above formula is merely the expectation value of U with respect to the state $W|\psi\rangle$, therefore, if U satisfies one of the conditions mentioned in Results 1 and 2, we can evaluate it efficiently. Even if U does not satisfy either of the conditions, the protocol using the destructive swap test to measure $|\langle\psi|U|\psi\rangle|^2$ [13] can be utilized to estimate it using a quantum computer with $2n$ qubit. For the second term, we present a method involving a projective measurement of G, which we denote by $\mathcal{M}_G$. To evaluate $\langle\psi|W^\dagger UWG|\psi\rangle$, we use the following four quantities,

$$\langle U\rangle_\pm = \langle\psi|e^{\mp i\pi G/4}W^\dagger UW e^{\pm i\pi G/4}|\psi\rangle\,, \quad (2)$$

$$\langle U\rangle_{M_G=\pm1} = \frac{1}{4p(M_G=\pm1)}\langle\psi|(I\pm G)W^\dagger UW(I\pm G)|\psi\rangle\,, \quad (3)$$

where $p(M_G=\pm1)$ is the probability of getting the result $M_G=\pm1$ by performing $\mathcal{M}_G$ on $|\psi\rangle$; $p(M_G=\pm1) = \|\frac{1}{2}(I\pm G)|\psi\rangle\|^2$. Figure 2 (b) and (c) show the quantum circuits to evaluate these quantities. With these, $\langle\psi|W^\dagger UWG|\psi\rangle$ can be reconstructed by,

$$\begin{aligned}&\langle\psi|W^\dagger UWG|\psi\rangle\\ &= p(M_G=+1)\langle U\rangle_{M_G=+1} - p(M_G=-1)\langle U\rangle_{M_G=-1}\\ &\quad + \frac{i}{2}(\langle U\rangle_- - \langle U\rangle_+). \quad (4)\end{aligned}$$

Note that when U is Hermitian, the first two terms correspond to the real part, and the rest correspond to the imaginary part of $\langle\psi|W^\dagger UWG|\psi\rangle$. Therefore, we obtain the following.

Result 3: *Let W and U be unitary matrices, and G be a Hermitian matrix. Suppose U satisfies one of the condition specified in Results 1 or 2, and assume $G^2 = I$. It is possible to estimate the output of the circuit in Fig. 2 (a), $\langle\psi|W^\dagger UW e^{-i\theta_1 G/2}|\psi\rangle$, by using the four quantum circuits in Fig. 2 (b) and (c), and by combining their output with Eq. (4). Especially, if the eigenvalues ±1 of G have equal degeneracy, the protocol works without an ancilla qubit. Even if U does not satisfy either of the conditions specified in Results 1 and 2, the protocol works with the method proposed in Ref. [13] that measures the expectation value of a unitary.*

Note that depending on experimental settings, we may still need an ancilla qubit to perform the nondestructive measurement. However, the technique can reduce the noise as the number of gates is fewer.

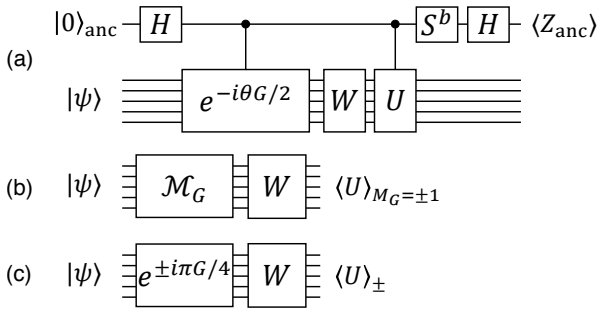


Figure 2: (a) Hadamard test with two controlled gates. In the figure, W is an arbitrary quantum gate. (b), (c) Quantum circuits to estimate the output of (a) with direct measurement. $\mathcal{M}_G$ is the projective measurement of G

3 Application

3.1 Metric tensor measurement

For the first application, we describe the direct measurement of metric tensor of a parameterized quantum state. In VQAs such as the VQE [4], we employ a parameterized quantum circuit $U(\boldsymbol{\theta})$ and an input state $|\psi_{\text{in}}\rangle$ on an n-qubit quantum computer, and optimize the circuit parameter $\boldsymbol{\theta}$ with respect to an expectation value $\langle A(\boldsymbol{\theta})\rangle = \langle\psi_{\text{in}}|U^\dagger(\boldsymbol{\theta})AU(\boldsymbol{\theta})|\psi_{\text{in}}\rangle$ of an observable A. Let us consider the case where the parameterized quantum circuit is constructed as $U(\boldsymbol{\theta}) = U_L(\theta_L)\cdots U_2(\theta_2)U_1(\theta_1)$ and each unitary $U_j(\theta_j)$ is generated by a Pauli product $P_j \in \{I,X,Y,Z\}^{\otimes n}$; $U_j(\theta_j) = \exp(-i\theta_j P_j/2)$. We denote $U_k(\theta_k)\cdots U_j(\theta_1)$ by $U_{k:j}$. In VQAs, we consider A which can be decomposed into a sum of Pauli products, and therefore, without loss of generality, we assume $A \in \{I,X,Y,Z\}^{\otimes n}$.

The metric tensor $g_{jk} = \frac{\partial\langle\psi(\boldsymbol{\theta})|}{\partial\theta_j}\frac{\partial|\psi(\boldsymbol{\theta})\rangle}{\partial\theta_j}$ of a variational quantum state $|\psi(\boldsymbol{\theta})\rangle = U(\boldsymbol{\theta})|\psi_{\text{in}}\rangle$ can be measured in the same manner. This quantity is the key to execute variational quantum simulations. Specifically, the imaginary and the real part of g_{jk} are employed for the simulation of real [18] and imaginary time [19] evolutions, respectively. A quantum circuit for the measurement of g_{jk} from Refs. [18, 19] is shown as Fig. 3 (a). The explicit expression for g_{jk}, when $k > j$, can be written as: $g_{jk} = \frac{1}{4}\langle\psi_{\text{in}}|U_{j:1}^\dagger P_j U_{k:j+1}^\dagger P_k U_{k:1}|\psi_{\text{in}}\rangle$. Figure 3 (a) shows the quantum circuit for the indirect measurement of g_{jk}. Again, from Result 3, this circuit can be replaced with the ones in Fig. 3 (b) and (c). The explicit expression is:

$$\text{Re}(g_{jk}) = \frac{1}{4}\Big(p(M_{P_j}=+1)\langle P_k\rangle_{M_{P_j}=+1} - p(M_{P_j}=-1)\langle P_k\rangle_{M_{P_j}=-1}\Big), \quad (5)$$

$$\text{Im}(g_{jk}) = -\frac{\langle P_k\rangle_+ - \langle P_k\rangle_-}{8}. \quad (6)$$

Figure 3 (a) differs from Fig. 2 (a) with two additional X gates on the ancilla. The consequence of this is a change of sign in the imaginary part (compare Eq. (6) and (4)).

Finally, we propose a method to estimate the OTOC on quantum computers. The OTOC $F(t)$ at time t is defined with two non-commuting operators A and B and a system Hamiltonian H as $F(t) = \langle B^\dagger(t)A^\dagger B(t)A\rangle$, where $B(t) = e^{iHt}Be^{-iHt}$. This is an important quantity in quantum many-body physics which measures how chaotic a given quantum system is [20, 21, 22, 23, 25]. In Ref. [26] a circuit to evaluate $F(t)$ was proposed, which is shown in Fig. 4. If we assume $A^2 = I$, the circuits in Fig. 2 (b) and (c) and Eq. (4) with a change of the sign of the imaginary part, which is the consequence of the X gates performed on the ancilla qubit, can be applied. More concretely, to evaluate $F(t)$, we replace W in Eq. (4) with $U^\dagger(t)BU(t)$, U and G with A. This method can easily be extended to the measurement of higher order correlators.

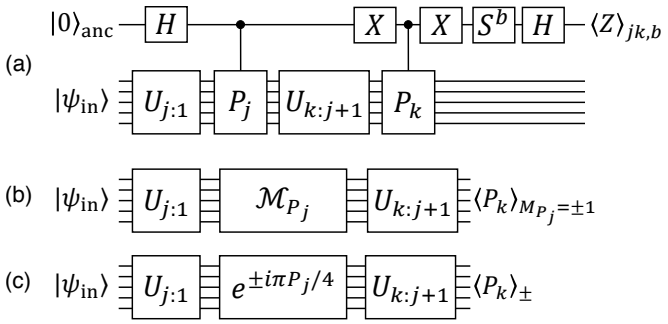


Figure 3: Quantum circuit for the estimation of the real and imaginary part of the metric tensor g_{jk}. (a) Indirect method from Refs. [18, 19]. $b \in \{0,1\}$. When $b = 0$, $\langle Z_{\text{anc}}\rangle_{jk,0} = 4\text{Re}(g_{jk})$ and when $b = 1$, $\langle Z_{\text{anc}}\rangle_{jk,1} = 4\text{Im}(g_{jk})$. (b) Direct method to estimate the real part of g_{jk}. (see Eq. (5).) (c) Direct method to estimate the imaginary part of g_{jk}. (see Eq. (6).)

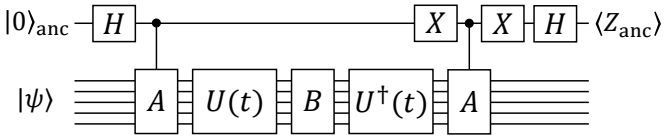


Figure 4: Indirect approach to measure the OTOC of operators A and B from Ref. [26]. In the figure, $U(t) = e^{-iHt}$.

4 Conclusion

We provided general protocols to replace indirect measurements, especially, the Hadamard test, with the direct measurement. The proposed methods to replace the Hadamard test provides a mean to evaluate the analytical gradient, metric tensor, Hessian, and even higher order derivatives with direct measurements for parameter tuning in variational quantum algorithms. They can also be applied for the estimation of OTOC. The presented protocols can significantly reduce the depth of a quantum circuit, and consequently, are important subroutines for quantum algorithms, especially for those of NISQ devices.

The technical version of this work is available on arXiv:1901.00015.

References

[1] Emanuel Knill, Gerardo Ortiz, and Rolando D. Somma. Optimal quantum measurements of expectation values of observables. *Phys. Rev. A*, 75(1):012328, jan 2007.

[2] Miroslav Dobšíček, Göran Johansson, Vitaly Shumeiko, and Göran Wendin. Arbitrary accuracy iterative quantum phase estimation algorithm using a single ancillary qubit: A two-qubit benchmark. *Phys. Rev. A*, 76(3):030306, sep 2007.

[3] John Preskill. Quantum Computing in the NISQ era and beyond. *Quantum*, 2:79, aug 2018.

[4] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik, and Jeremy L. O'Brien. A variational eigenvalue solver on a photonic quantum processor. *Nat. Commun.*, 5(1):4213, dec 2014.

[5] Dave Wecker, Matthew B. Hastings, and Matthias Troyer. Towards Practical Quantum Variational Algorithms. *Phys. Rev. A*, 92(4):042303, jul 2015.

[6] Daochen Wang, Oscar Higgott, and Stephen Brierley. Accelerated variational quantum eigensolver. *Phys. Rev. Lett.*, 122:140504, Apr 2019.

[7] Juan Carlos Garcia-Escartin and Pedro Chamorro-Posada. swap test and Hong-Ou-Mandel effect are equivalent. *Phys. Rev. A*, 87(5):052330, may 2013.

[8] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum Fingerprinting. *Phys. Rev. Lett.*, 87(16):167902, sep 2001.

[9] Lukasz Cincio, Yiit Subasi, Andrew T. Sornborger, and Patrick J. Coles. Learning the quantum algorithm for state overlap. *New. J. Phys*, 20:113022, 2018.

[10] Oscar Higgott, Daochen Wang, and Stephen Brierley. Variational Quantum Computation of Excited States. *Quantum*, 3:156, July 2019.

[11] Tyson Jones, Suguru Endo, Sam McArdle, Xiao Yuan, and Simon C. Benjamin. Variational quantum algorithms for discovering hamiltonian spectra. *Phys. Rev. A*, 99:062304, Jun 2019.

[12] Ryan LaRose, Arkin Tikku, Étude O'Neel-Judy, Lukasz Cincio, and Patrick J. Coles. Variational quantum state diagonalization. *npj Quantum Information*, 5(1):8, 2019.

[13] Yiğit Subaşı, Lukasz Cincio, and Patrick J Coles. Entanglement spectroscopy with a depth-two quantum circuit. *Journal of Physics A: Mathematical and Theoretical*, 52(4):044001, jan 2019.

[14] Artur K. Ekert, Carolina Moura Alves, Daniel K. L. Oi, Michał Horodecki, Paweł Horodecki, and L. C. Kwek. Direct Estimations of Linear and Nonlinear Functionals of a Quantum State. *Phys. Rev. Lett.*, 88(21):217901, may 2002.

[15] Gian Giacomo Guerreschi and Mikhail Smelyanskiy. Practical optimization for hybrid quantum-classical algorithms. *arXiv:1701.01450*, jan 2017.

[16] Kosuke Mitarai, Makoto Negoro, Masahiro Kitagawa, and Keisuke Fujii. Quantum circuit learning. *Phys. Rev. A*, 98(3):032309, sep 2018.

[17] Jun Li, Xiaodong Yang, Xinhua Peng, and Chang-Pu Sun. Hybrid Quantum-Classical Approach to Quantum Optimal Control. *Phys. Rev. Lett.*, 118(15):150503, apr 2017.

[18] Ying Li and Simon C. Benjamin. Efficient Variational Quantum Simulator Incorporating Active Error Minimization. *Phys. Rev. X*, 7(2):021050, jun 2017.

[19] Sam McArdle, Suguru Endo, Tyson Jones, Ying Li, Simon Benjamin, and Xiao Yuan. Variational quantum simulation of imaginary time evolution with applications in chemistry and beyond. *arXiv:1804.03023*, apr 2018.

[20] Efim B. Rozenbaum, Sriram Ganeshan, and Victor Galitski. Lyapunov Exponent and Out-of-Time-Ordered Correlator's Growth Rate in a Chaotic System. *Phys. Rev. Lett.*, 118(8):086801, feb 2017.

[21] Brian Swingle and Debanjan Chowdhury. Slow scrambling in disordered quantum systems. *Phys. Rev. B*, 95(6):060201, feb 2017.

[22] Yichen Huang, Yong-Liang Zhang, and Xie Chen. Out-of-time-ordered correlators in many-body localized systems. *Ann. Phys.*, 529(7):1600318, jul 2017.

[23] Daniel A. Roberts and Beni Yoshida. Chaos and complexity by design. *J. High Energy Phys.*, 2017(4):121, apr 2017.

[24] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2010.

[25] Justin Dressel, José Raúl, González Alonso, Mordecai Waegell, and Nicole Yunger Halpern. Strengthening weak measurements of qubit out-of-time-order correlators. *Phys. Rev. A*, 98(1):012132, 2018.

[26] Brian Swingle, Gregory Bentsen, Monika Schleier-Smith, and Patrick Hayden. Measuring the scrambling of quantum information. *Phys. Rev. A*, 94(4):040302, oct 2016.

Acknowledgements - KM thanks the METI and IPA for their support through the MITOU Target program. KM is supported by JSPS KAKENHI No. 19J10978. KF is supported by KAKENHI No.16H02211, JST PRESTO JPMJPR1668, JST ERATO JPMJER1601, and JST CREST JPMJCR1673. This work is supported by MEXT, Q-LEAP.

Quantum compiling with diffusive sets of gates

Y. Zhiyenbayev[1] V. M. Akulin[2 3] A. Mandilara[1 *]

[1] *Department of Physics, School of Science and Technology, Nazarbayev University, 53, Kabanbay batyr Av., Astana, 010000, Republic of Kazakhstan*

[2] *Laboratoire Aimé-Cotton CNRS UMR 9188, Bât. 505, Campus d'Orsay, 91405 Orsay Cedex, France*

[3] *Institute for Information Transmission Problems of the Russian Academy of Science, Bolshoy Karetny per. 19, Moscow, 127994, Russia*

Abstract. Given a set of quantum gates and a target unitary operation, the most elementary task of quantum compiling is the identification of a sequence of the gates that approximates the target unitary to a determined precision ε. The Solovay-Kitaev theorem provides an elegant solution which is based on the construction of successively tighter 'nets' around the unity comprised by successively longer sequences of gates. The procedure for constructing the nets, according to this theorem, requires accessibility to the inverse of the gates as well. In this work, using the theory of random walks we propose a method for constructing nets around unity without this requirement. The algorithmic procedure is applicable to sets of gates which are diffusive enough, in the sense that sequences of moderate length cover the space of unitary matrices in a uniform way. We prove that the number of gates sufficient for reaching a precision ε scales as $O\left(\log(1/\varepsilon)^{\log 3/\log 2}\right)$ while the pre-compilation time is increased as compared to the Solovay-Kitaev algorithm by a polynomial factor 3/2.

Keywords: Quantum gates, Compiling, Quantum Control

Approximation up to a given accuracy of an arbitrary unitary transformation by a series of standard transformations (gates) is an important ingredient of programming of quantum computers, which was formulated and solved [1, 2] in the case where the set of $\mathcal{M}$ predetermined standard transformations contains both direct operations and their inverses. The so called Solovay-Kitaev (SK) theorem provides the proof of existence together with the method for constructing the solution. Based on the elements in the proof of the SK theorem, the Dawson-Nielsen (DNSK) algorithm [3] provides the exact steps for identifying a series of length L, which scales with the required accuracy ε as $O\left(\log(1/\varepsilon)^{3.97}\right)$, and with running time as $O\left(\log(1/\varepsilon)^{2.71}\right)$.

Here we address the question [3] whether is possible to generalize the results of SK theorem onto the case where the set of the predetermined operations does not contain the inverses. In view of the fast development of quantum technologies, this problem has theoretical but mostly practical interest since experimentalists often do not have access to inverse operations– they are restricted to semigroup rather than group operations. In [4] progress on answering this question has been reported and our answer [5] is also positive and conditional on a specific property of the given set. We require that sequences of gates of moderate length (composed by $15-20$ gates) cover the space of unitary matrices in a uniform way, see Fig.1. More specifically, we propose an algorithmic procedure that is based on diffusion process and justified by the theory of random walks. This method achieves an improved scaling of the length L with the required accuracy ε, $O\left(\log(1/\varepsilon)^{\log 3/\log 2}\right)$.

The improvement in the scaling of length is justified by an observed polynomial counter-increase in precompilation time by a polynomial factor 3/2, as this compares to DNSK algorithm. This confirms the expected interplay between the relations characterizing algorithmic procedures solving similar problems. When the inverses are included in the set, the notion of diffusive sets converges to the notion of ' efficiently computational sets' introduced in [6] and our results partially fulfill the predictions of that work concerning the considerable improvement of the scaling of length with accuracy.

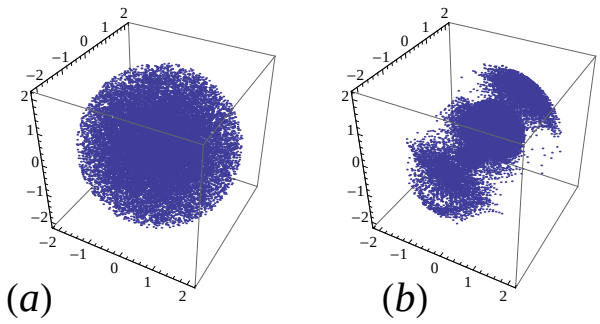


Figure 1: Geometric representation in the space of unitary matrices of all sequences of length 17 generated by two different computationally universal sets of single qubit gates. *(a)* A diffusive set, and *(b)* a non-diffusive one.

In the Fig. 2 we present quantum compiling results obtained with the proposed algorithm versus the 'fast' [7] DNSK and we confirm our theoretical predictions. More precisely, we approximate the phase rotation gates,

$$R_{2^d} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/2^d} \end{pmatrix}, \quad \text{with } d = 1, \dots 7 \qquad (1)$$

using the introduced algorithm and then the fast DNSK keeping the parameters of produced nets very similar in

*mandkat@gmail.com

both cases. For both methods we have used the same pair of diffusive gates, but naturally for the latter we have included the inverses. On each 'column' the seven points describe the approximation of the seven phase rotations Eq.(1). There is no correlation between the precision achieved and the order d of the phase gates and for this reason we have not marked with d the points on the plot. For each method we present three numerical results (three columns) that correspond to three different lengths of the initial sampling net $r = 16, 17, 18$, giving different lengths L to the final sequence that approximate the gate (horizontal axis on Fig. 2). To quantify the accuracy ε we use as measure of distance: $d_F\left(\widehat{U}_1, \widehat{U}_2\right) = \sqrt{\frac{2-\left|\mathrm{Tr}\left(\widehat{U}_1\widehat{U}_2^{-1}\right)\right|}{2}}$. More technical details on this example can be found in the Appendix of [5] while the related programs can be downloaded from the site www.qubit.kz.

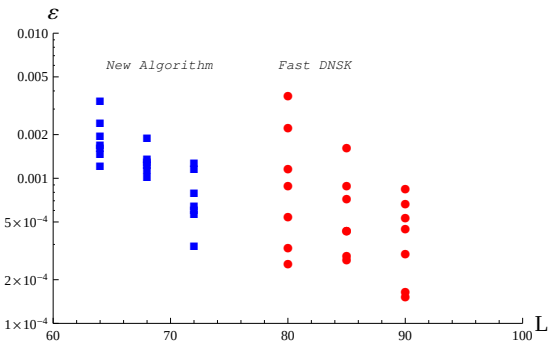


Figure 2: Accuracy of approximation ε of phase rotation gates R_{2^d} for $d = 1, \cdots, 7$ by sequences of two diffusive gates, plotted versus length of the sequence. Blue squares: results obtained with the introduced algorithm. Red circular dots: results of the Fast DNSK. Different 'columns' correspond to different initial lengths r of the sequences in the sampling net. From left to right: $r = 16, 17, 18, 16, 17, 18$.

References

[1] R. Solovay. Proof of Solovay-Kitaev theorem. unpublished, (1995).

[2] A. Y. Kitaev, Russ. Math. Surv. 52, 1191 (1997).

[3] C. M. Dawson and M. A. Nielsen, Quant. Inf. Comp. 6, 81 (2006).

[4] I. S. B. Sardharwalla, T. S. Cubitt, A. W. Harrow and N. Linden, arXiv:1602.07963

[5] Y. Zhiyenbayev, V. M. Akulin and A. Mandilara, Phys. Rev. A 98, 012325 (2018).

[6] A. W. Harrow, B. Recht, and I. L. Chuang, J. Math. Physics 43, 4445, (2002).

[7] In the sense that we ignore the extra step of 'telescoping' [2].

Genuine quantum nonlocality in the triangle network

Marc-Olivier Renou,[1] Elisa Bäumer,[2] Sadra Boreiri,[3] Nicolas Brunner,[1] Nicolas Gisin,[1] and Salman Beigi[4]

[1] *Département de Physique Appliquée, Université de Genève, CH-1211 Genève, Switzerland*
[2] *Institute for Theoretical Physics, ETH Zurich, Wolfgang-Pauli-Str. 27, 8093 Zürich, Switzerland*
[3] *School of Computer and Communication Sciences,*
cole Polytechnique Fdrale de Lausanne, CH-1015 Lausanne, Switzerland
[4] *School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran*

(Dated: 17 July 2019)

Quantum networks allow for completely novel forms of quantum correlations. In particular, quantum nonlocality can be demonstrated without having input settings, only by considering the joint statistics of fixed local measurement outputs. However, previous examples of this phenomenon all come from the usual form of quantum nonlocality, via the violation of a standard Bell inequality. Here we present novel examples of "quantum nonlocality without inputs", which we believe represent a new form of quantum nonlocality, genuine to networks. Our examples, for the triangle network, involve both entangled states and joint entangled measurements. We generalize it to any odd-cycle network.

Introduction.— Bell's theorem is arguably among the most important results in the foundations of quantum theory [1]. It also had a major influence on the development of quantum information science [2], and led recently to the so-called device-independent paradigm [3–6].

An interesting direction is to understand quantum nonlocality in scenarios involving more than two observers. The standard approach to this problem considers many distant observers sharing an entangled state distributed by a common source, and leads to interesting new effects [7]. This represents the simplest generalization of quantum nonlocality to the multipartite case, and most of the concepts and tools developed for bipartite nonlocality can generally be directly extended here.

Recently, a completely different approach to multipartite nonlocality was proposed [8, 9], focusing on quantum networks. Here, distant observers share entanglement distributed by several sources which are assumed to be independent from each other. By performing joint entangled measurements (such as the well-known Bell state measurement used in quantum teleportation [10]), observers may correlate distant quantum systems and establish strong correlations across the entire network. Typically, each source connects here only a strict subset of the observers. It turns out that this situation is fundamentally different from standard multipartite nonlocality, and allows for radically novel phenomena. As regards correlations, it is now possible to witness quantum nonlocality in experiments where all the observers perform a fixed measurement, i.e. they receive no input [9, 16–19]. This effect of quantum nonlocality without inputs is remarkable, and radically departs from previous forms of quantum nonlocality.

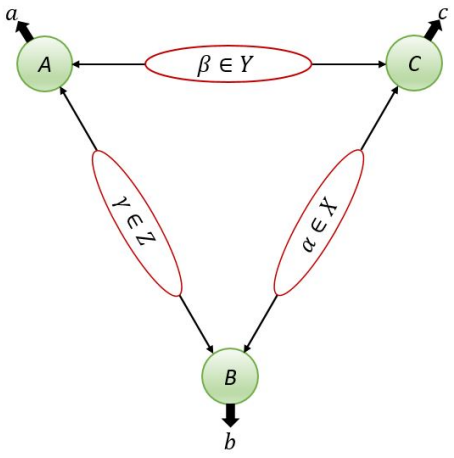


FIG. 1. The triangle network features three observers (green circles), connected by three independent bipartite sources (red ovals). Here the sources distribute local variables (i.e. shared randomness).

So far, however, all known examples of quantum nonlocality without inputs can be traced back to standard Bell inequality violation. This naturally leads to the question of whether completely novel forms of quantum nonlocality, genuine to the network configuration, could arise. Here we address this question, by presenting an instance of quantum nonlocality in the triangle network, which we argue is fundamentally different from previously known forms of quantum nonlocality. In particular, our construction crucially relies on the combination of shared entangled states and joint entangled measurements performed by the observers. We present several generalizations of our main result.

Scenario and main result.— We consider the so-called triangle quantum network sketched in Fig. 1. It features three observers (Alice, Bob and Charlie). Every pair of observers is connected by a (bipartite) source, providing a shared physical system (represented e.g. by a classical variable or by a quantum state). Importantly, the three sources are assumed to be independent of each other. Hence, the three observers share no common (i.e. tripartite) piece of information. Based on the received physical resources, each observer provides an output (a, b and c, respectively). Note that the observers receive no input in this setting, contrary to standard Bell nonlocality tests.

The statistics of the experiment are thus given by the joint probability distribution $P(a,b,c)$.

Characterizing the set of distributions $P(a,b,c)$ that can be obtained from physical resources (in particular classical or quantum) is a highly non-trivial problem. The main difficulty stems from the assumption that the sources are independent. This makes the set of possible distributions $P(a,b,c)$ non-convex, and standard methods used in Bell nonlocality are thus completely unadapted to this problem. Strong bounds on the limits of classical correlations are thus still missing, which in turn renders the discussion of quantum nonlocality in the triangle network challenging.

Here we follow a different approach in order to present instances of quantum nonlocality in the triangle network. Specifically, we first construct explicitly a family of quantum distributions $P_Q(a,b,c)$, using both entangled quantum states (distributed by each of the three sources), and entangled joint measurements performed by each observer. Then we show that these quantum distributions cannot be reproduced by any "trilocal" model, i.e. a local model "a la Bell" where all three sources are assumed to be independent from each other. Formally, we prove that

$$P_Q(a,b,c) \neq \int \mathrm{d}\alpha \int \mathrm{d}\beta \int \mathrm{d}\gamma P_A(a|\beta,\gamma)\, P_B(b|\gamma,\alpha)\, P_C(c|\alpha,\beta) \tag{1}$$

where $\alpha \in X$, $\beta \in Y$ and $\gamma \in Z$ represent the three local variables distributed by each source and $P_A(a|\beta,\gamma), P_B(b|\gamma,\alpha), P_C(c|\alpha,\beta)$ represent arbitrary deterministic response functions for Alice, Bob and Charlie. Our proof does not rely on the violation of some Bell-type inequality, but is based on a logical contradiction. More precisely, we first identify a certain number of necessary properties that any trilocal model should have in order to reproduce $P_Q(a,b,c)$, and then show that these properties cannot all be satisfied at the same time.

Let us now construct explicitly our quantum distributions $P_Q(a,b,c)$. Each source produces the same pure maximally entangled state of two qubits,

$$|\psi_\gamma\rangle_{A_\gamma B_\gamma} = |\psi_\alpha\rangle_{B_\alpha C_\alpha} = |\psi_\beta\rangle_{C_\beta A_\beta} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,.$$

Note that each party receives two independent qubit subsystems; for instance Alice receives subsystems A_β and A_γ. Next, each party performs a projective quantum measurement in the same basis. In the following, we use the basis (a set depending on one real parameter u) given by

$$\begin{aligned} |\uparrow\rangle &= |01\rangle & |\chi_0\rangle &= u\,|00\rangle + v\,|11\rangle \\ |\downarrow\rangle &= |10\rangle & |\chi_1\rangle &= v\,|00\rangle - u\,|11\rangle \end{aligned} \tag{2}$$

with $u^2+v^2=1$ and $0<v<u<1$. For Alice, we label it $\{|\phi_a\rangle_{A_\beta A_\gamma}\}$ for $\phi_a \in \{\uparrow,\downarrow,\chi_0,\chi_1\}$ and adopt similar notations for Bob and Charlie. Remark that only two out of the four states in that basis are entangled. The statistics of the experiment are given by

$$P_Q(a,b,c) = |\,\langle\phi_a|\,\langle\phi_b|\,\langle\phi_c|\,|\psi_\gamma\rangle\,|\psi_\alpha\rangle\,|\psi_\beta\rangle\,|^2,$$

where we did not specify the Hilbert spaces supporting the states. Note that when evaluating $P_Q(a,b,c)$, one should be attentive to which Hilbert space support each state and measurements.

We now state the main result of this letter:

Theorem 1. *The quantum distribution $P_Q(a,b,c)$ cannot be reproduced by any classical trilocal model (in the sense of Eq. (1)) when $u^2_{\max} < u^2 < 1$, where $u^2_{\max} = \frac{-3+(9+6\sqrt{2})^{2/3}}{2(9+6\sqrt{3})^{1/3}} \approx 0.785$*

All details of the proof are given in Appendix A of [29]. A natural question is whether the distribution P_Q is trilocal when $u^2 \leq u^2_{\max}$. In Appendix D of [29], we show that this is the case, by constructing an explicit trilocal model for $u^2 = u^2_{\max}$ (up to machine precision). We conjecture that P_Q remains trilocal up to $u^2 < u^2_{\max}$. Note that this can be proven for the case $u^2 = 1/2$. Here the trilocal model is obtained from Step 1, with χ replaced by a uniformly random choice between χ_0 and χ_1.

Before entering a more general discussion about the implications of Theorem 1 and some natural open questions, we now briefly present several generalizations of the result.

Generalisations.— A first extension considers the same scenario as in Theorem 1, with the difference that all sources now produce the same general entangled two-qubit pure states $\lambda_0\,|00\rangle + \lambda_1\,|11\rangle$ where $\lambda_0^2+\lambda_1^2=1$. A second generalization considers the triangle network where all three sources now produce a maximally entangled two-qutrit state, i.e. $|\phi_3\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$. A third generalization is a generalization of Theorem 1 for any $N-$cycle network, with N being odd.

All are detailed in [29].

Discussion.— We presented novel examples of quantum nonlocality without inputs, mainly for the triangle network. We believe that these examples represent a form of quantum nonlocality that is genuine to the network configuration, in the sense that it is not a consequence of standard forms of Bell nonlocality. These examples fundamentally differ from the one presented by Fritz in [9], relying on the violation of a standard bipartite Bell inequality. Let us first briefly review it.

Fritz's example can be viewed as a standard Bell test, embedded in the triangle network. Consider that Alice and Bob share a two-qubit Bell state, with the goal of violating the CHSH Bell inequality. Testing the CHSH inequality requires of course local inputs for both Alice and Bob. Although the triangle network features no explicit inputs, here effective inputs are provided by the two additional sources: the source connecting Alice and Charlie (resp. Bob and Charlie) provides a shared uniformly random bit, which is used as Alice's (resp. Bob's) input for the CHSH test. All parties output the "input bits" he

receives. The correspondence between these outputs ensures that Alice's (resp. Bob's) output only depends on the source she (resp. he) shares with Charlie. Finally, Alice and Bob both additionally output the output of their local measurement performed on the shared Bell state. If this quantum distribution could be reproduced by a trilocal model, it would follow that local correlations can violate the CHSH inequality, which is impossible.

Let us comment on some significant differences between Fritz's construction and our example of Theorem 1. First, our construction has a high level of symmetry (all sources distribute the same entangled state and all measurements are the same) with only four outputs per party. In particular, it involves an entangled state for each source, whereas the example of Fritz requires entanglement for only one source (it can be symmetrized, but at the cost of adding new outputs). Moreover, our construction appears to rely on the use of joint measurements with entangled eigenstates, while Fritz's model uses only separable measurements. Hence Fritz's construction could be obtained from PR-boxes [24]. As the equivalent of joint measurements does not exist for PR-boxes [25, 26], we believe that our example cannot be obtained from PR-boxes.

Note that all the above arguments are only based on qualitative and intuitive arguments. We have no formal proof that in order to obtain the distribution $P_Q(a,b,c)$ one actually requires all states to be entangled and/or joint entangled measurements. In fact, even formalizing the problem is difficult, any progress in this direction would be interesting. An idea would be to use the notion of "self-testing" [22], for instance by proving that all shared quantum states must be two-qubit Bell states and/or that all local measurements must feature specific entangled eigenstates [27, 28].

Another important aspect of our construction that must be discussed is noise tolerance. As such, Theorem 1 clearly applies only to the exact quantum distribution $P_Q(a,b,c)$, i.e. in the noiseless case. The trilocal set being topologically closed, it is clear that $P_Q(a,b,c)$ must have a certain (possibly very weak) robustness to noise: when adding a sufficiently small amount of local noise to $P_Q(a,b,c)$, one should still obtain a quantum distribution that is incompatible with any trilocal model. A promising method would be to consider the qutrit example, the proof of which involves the Finner inequality that allows in principle for the presence of noise. However we did not succeed in obtaining reasonable noise tolerance of our result so far. Other methods could also help, such as the "inflation" technique [14] [1]. This could provide a nonlinear Bell inequality violated by our example.

The possibility of generating randomness from quantum nonlocality without inputs is a further interesting question. In particular, it seems very likely that our quantum distribution $P_Q(a,b,c)$ contains some level of intrinsic randomness. It would be interesting to see how this randomness could be quantified in a device-independent manner (still assuming independence of the sources).

Acknowledgements.—We thank Alex Pozas and Elie Wolfe for discussions. We acknowledge financial support from the Swiss national science foundation (Starting grant DIAQ, NCCR-QSIT).

[1] J. S. Bell, *Physics* **1**, 195–200 (1964).
[2] A. Ekert, Phys. Rev. Lett. (1991).
[3] J. Barrett, L. Hardy, A. Kent, Phys. Rev. Lett. (2005).
[4] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[5] R. Colbeck, PhD Thesis, Univ. of Cambridge (2007).
[6] S. Pironio et al., Nature **464**, 1021 (2010).
[7] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[8] C. Branciard, N. Gisin and S. Pironio, Phys. Rev. Lett. **104**, 170401 (2010).
[9] T. Fritz, New J. Phys. **14**, 103001 (2012).
[10] C. H. Bennett et al., Phys. Rev lett. **70**, 1895 (1993).
[11] R. Chaves, T. Fritz, Phys. Rev. A **85**, 032113 (2012).
[12] D. Rosset, C. Branciard, T. J. Barnea, G. Pütz, N. Brunner, and N. Gisin, Phys. Rev. Lett. **116**, 010403 (2016).
[13] R. Chaves, Phys. Rev. Lett. **116**, 010402 (2016).
[14] E. Wolfe, R. W. Spekkens, and T. Fritz, arXiv:1609.00672.
[15] M.-X. Luo, Phys. Rev. Lett. **120**, 140402 (2018).
[16] N. Gisin, arXiv:1708.05556.
[17] T. Fraser, E. Wolfe, Phys. Rev. A **98**, 022113 (2018).
[18] N. Gisin, Entropy **21**, 325 (2019).
[19] M.O. Renou, Y. Wang, S. Boreiri, S. Beigi, N. Gisin, and N. Brunner, arXiv:1901.08287.
[20] D. Rosset, N. Gisin, E. Wolfe, arXiv:1709.00707 (2017).
[21] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[22] D. Mayers and A. Yao, Self testing quantum apparatus, Quant. Inf. Comp. **4**, 273 (2004).
[23] M. Navascues, E. Wolfe, arXiv:1707.06476 (2017).
[24] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[25] J. Barrett, Phys. Rev. A **75**, 032304 (2007).
[26] A. J. Short, S. Popescu, N. Gisin, Phys. Rev. A **73**, 012101 (2006).
[27] M. O. Renou, J. Kaniewski, and N. Brunner, Phys. Rev. Lett. **121**, 250507 (2018).
[28] J.-D. Bancal, N. Sangouard, and P. Sekatski, Phys. Rev. Lett. **121**, 250506 (2018).
[29] M.-O. Renou, E. Bäumer, S. Boreiri, N.Brunner, N.Gisin, and S. Beigi, arXiv:1905.04902 (2019).

[1] The inflation method consists of a sequence of tests of rapidly increasing computational complexity. For the first tests in the sequence, implementable on a computer, it appears that even the nonlocality of $P_Q(a,b,c)$ cannot be detected. Nevertheless, as inflation is known to converge in the limit [23], this is still an interesting possibility to explore.

Distribution of multipartite Einstein-Podolsky-Rosen steering in Gaussian systems

Yu Xiang[1 2 3 *] Xiaolong Su[3 4] Gerardo Adesso[5] Yin Cai[6 7] Nicolas Treps[7]
Qiongyi He[1 2 3 †]

[1] *State Key Laboratory for Mesoscopic Physics and Collaborative Innovation Center of Quantum Matter, School of Physics, Peking University, Beijing 100871, China*
[2] *Beijing Academy of Quantum Information Sciences, Haidian District, Beijing 100193, China*
[3] *Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan, Shanxi 030006, China*
[4] *State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China*
[5] *Centre for the Mathematics and Theoretical Physics of Quantum Non-Equilibrium Systems (CQNE), School of Mathematical Sciences, The University of Nottingham, Nottingham NG7 2RD, United Kingdom*
[6] *Laboratoire Kastler Brossel, Sorbonne Université, UPMC, ENS, Collège de France, CNRS, 4 place Jussieu, 75252 Paris, France*
[7] *Key Laboratory for Physical Electronics and Devices of the Ministry of Education & Shaanxi Key Lab of Information Photonic Technique, Xi'an Jiaotong University, Xi'an 710049, China*

Abstract. Understanding how quantum resources can be quantified and distributed over many parties has profound applications in quantum communication. As one of the most intriguing features of quantum mechanics, Einstein-Podolsky-Rosen (EPR) steering is a useful resource for secure quantum networks. By reconstructing the covariance matrix of a continuous variable (CV) Gaussian state, a quantifier of EPR steering under Gaussian measurements is established. With this ability, we precisely validate four types of monogamy relations recently proposed for Gaussian steering in two experiment systems, one is a CV four-mode square Gaussian cluster state [1], and the other one is a multimode Gaussian state via a quantum frequency comb [2]. We observe a very rich structure for the steering distribution, which paves the way for exploiting EPR steering as a valuable resource for multiparty quantum information tasks.

Keywords: EPR steering, multipartite Gaussian system, monogamy relations

Introduction- Schrödinger [3] put forward the term 'steering' to describe the "spooky action-at-a-distance" phenomenon pointed out by Einstein, Podolsky, and Rosen (EPR) in their famous paradox [4, 5]. Wiseman, Jones, and Doherty [6] rigorously defined the concept of steering in terms of violations of local hidden state model, and revealed that steering is an intermediate type of quantum correalation between entanglement and Bell nonlocality, where local measurements on one subsystem can apparently adjust (steer) the state of another distant subsystem [7]. Such correlation is intrinsically asymmetric with respect to the two subsystems [8, 9], and allows verification of shared entanglement even if the measurement devices of one subsystem are untrusted. Due to this intriguing feature, steering has been identified as a physical resource for one-sided device-independent (1sDI) quantum cryptography, secure quantum teleportation and subchannel discrimination.

Recently, experimental observation of multiparty EPR steering has been reported in optical networks [10] and photonic qubits [11, 12]. These experiments offer insights into understanding whether and how this special type of quantum correlation can be distributed over many different systems, a problem which has been recently studied theoretically by deriving so-called *monogamy relations* [13, 14, 15, 16, 17]. However, beyond [10], no systematic experimental exploration of monogamy constraints for EPR steering has been reported to date.

Here, we experimentally investigate properties of multipartite steering within two experiment systems, one is a CV four-mode square Gaussian cluster state [1], and the other one is a multimode state via a quantum frequency comb [2] (see Fig. 1). By reconstructing the covariance matrix of the Gaussian state, we measure the quantifier of EPR steering under Gaussian measurements introduced in [9], then precisely validate four types of monogamy relations recently proposed for Gaussian steering (see Table 1). Our study helps quantifying how steering can be distributed among different parties and linking the amount of steering to the security of channels in a communication network.

Type	Ref.	Inequality	Specifications
I	[13]	$\mathcal{G}^{A\to C}>0 \;\Rightarrow\; \mathcal{G}^{B\to C}=0$	$n_A=n_B=n_C=1$
II	[14, 15]	$\mathcal{G}^{A\to C}>0 \;\Rightarrow\; \mathcal{G}^{B\to C}=0$	$n_A,n_B\geq 1;\, n_C=1$
IIIa	[16]	$\mathcal{G}^{C\to(AB)}-\mathcal{G}^{C\to A}-\mathcal{G}^{C\to B}\geq 0$	$n_A=n_B=n_C=1$
IIIb	[16]	$\mathcal{G}^{(AB)\to C}-\mathcal{G}^{A\to C}-\mathcal{G}^{B\to C}\geq 0$	$n_A=n_B=n_C=1$
IVa	[17]	$\mathcal{G}^{C\to(AB)}-\mathcal{G}^{C\to A}-\mathcal{G}^{C\to B}\geq 0$	$n_A,n_B,n_C\geq 1$
IVb	[17]	$\mathcal{G}^{(AB)\to C}-\mathcal{G}^{A\to C}-\mathcal{G}^{B\to C}\geq 0$	$n_A,n_B\geq 1;\, n_C=1$

Table 1: Classification of monogamy relations for the bipartite quantifier $\mathcal{G}^{j\to k}$ of EPR steerability of party k by party $j$under Gaussian measurements, in a tripartite $(n_A+n_B+n_C)$-mode system ABC. Note: I $\sqsubseteq$ II and III $\sqsubseteq$ IV, where "$\sqsubseteq$" indicates being generalized by; the relations in types II and IVb can be violated for $n_C>1$.

*xiangy.phy@pku.edu.cn
†qiongyihe@pku.edu.cn

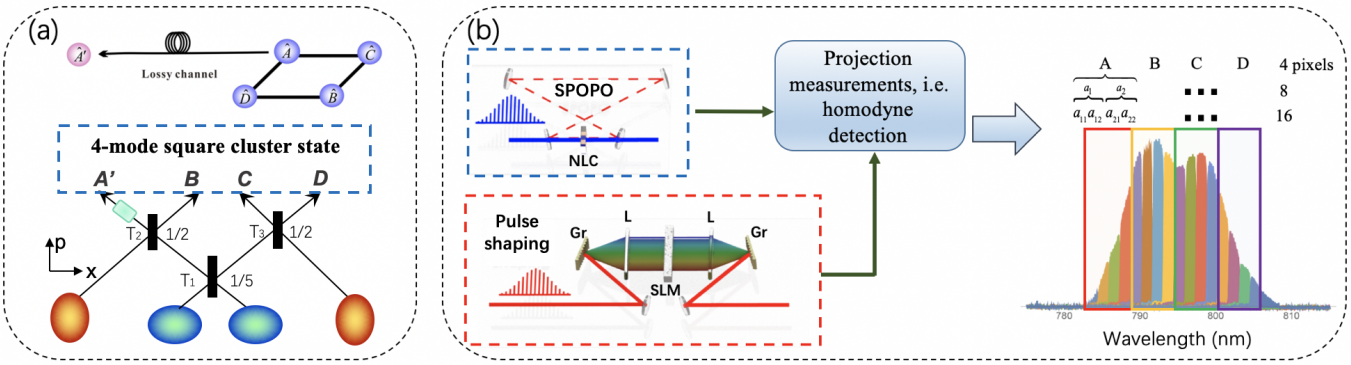


Figure 1: (a) Experimental set-up of a four-mode square cluster state, one mode is distributed over a lossy quantum channel. (b) Experimental set-up of the multimode quantum resource via synchronously pumping an optical parametric oscillator (SPOPO) and pulse shaping on the local oscillator (LO) with controllable spectral resolution. The spectrum of the LO is divided into 4, 8 and 16 spectral bands within homodyne detection, respectively.

Method- The properties of a $(n_A + m_B)$-mode Gaussian state ρ_{AB} of a bipartite system can be determined by its covariance matrix $\sigma_{AB} = \begin{pmatrix} A & C \\ C^\top & B \end{pmatrix}$, with elements $\sigma_{ij} = \langle \hat{\xi}_i \hat{\xi}_j + \hat{\xi}_j \hat{\xi}_i \rangle / 2 - \langle \hat{\xi}_i \rangle \langle \hat{\xi}_j \rangle$, where $\hat{\xi} \equiv (\hat{x}_1^A, \hat{p}_1^A, ..., \hat{x}_n^A, \hat{p}_n^A, \hat{x}_1^B, \hat{p}_1^B, ..., \hat{x}_m^B, \hat{p}_m^B)$ is the vector of the amplitude and phase quadratures of optical modes. The submatrices A and B are corresponding to the reduced states of Alice's and Bob's subsystems, respectively. The steerability of Bob by Alice $(A \to B)$ can be quantified by [9]

$$\mathcal{G}^{A\to B}(\sigma_{AB}) = \max\left\{0, \quad -\sum_{j:\bar{\nu}_j^{AB\setminus A}<1} \ln(\bar{\nu}_j^{AB\setminus A})\right\}, \qquad (1)$$

where $\bar{\nu}_j^{AB\setminus A}$ $(j = 1, ..., m_B)$ are the symplectic eigenvalues of $\bar{\sigma}_{AB\setminus A} = B - C^\mathsf{T} A^{-1} C$, derived from the Schur complement of A in the covariance matrix σ_{AB}. The quantity $\mathcal{G}^{A\to B}$ is a monotone under Gaussian local operations and classical communication [17] and vanishes iff the state described by σ_{AB} is nonsteerable by Gaussian measurements [9].

Results- For the generated CV four-mode square Gaussian cluster state, we find that the two- and three-mode steering properties are determined by the geometric structure of the cluster state. Figure 2 shows a selection of results for the steerability between any two modes [i.e., $(1+1)$-mode partitions] of the cluster state under Gaussian measurements. Interestingly, a given mode of the state can be steered by its diagonal mode which is not directly coupled, but can not be steered even by collaboration of its two nearest neighbors, although they are coupled by direct interaction. This observation can be understood as a consequence of the monogamy relation (type-I) derived from the two-observable ($\hat{x}$ and $\hat{p}$) EPR criterion [13]: two distinct modes cannot steer a third mode simultaneously by Gaussian measurements. Then, using the results of (1+2)-, (1+3)-and (2+2)-mode steerability, we also present the experimental examination of the type-II, type-III and type-IV monogamy relations. Additional results are shown in Ref.[1].

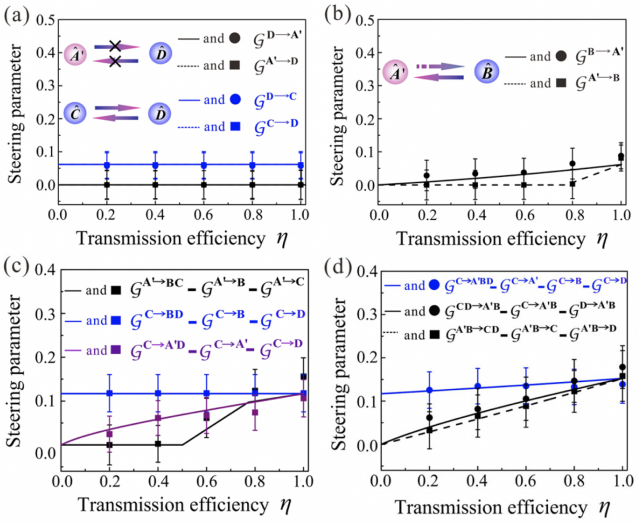


Figure 2: Gaussian EPR steering between two modes of the cluster state. (a) There is no EPR steering between neighboring modes $\hat{A}'$ and $\hat{D}$ under Gaussian measurements, while diagonal modes $\hat{C}$ and $\hat{D}$ can steer each other with equal power. (b) One-way EPR steering between modes $\hat{A}'$ and $\hat{B}$ under Gaussian measurements. (c) Monogamy of steering quantifier for (1+2)-mode partitions. (d) Monogamy of steering quantifier for $(1+3)$- and $(2+2)$-mode partitions. The dots and squares represent the experimental data measured at different transmission efficiencies. Error bars represent ± one standard deviation and are obtained based on the statistics of the measured noise variances.

For the generated multimode state via a quantum frequency comb, we investigate the properties of multipartite EPR steering among the four spectral bands $ABCD$ when the whole spectrum is divided into 4, 8 or 16 pixels. We find that although the spectral components are fixed, the steerability raises sharply with the increase of measurement resolutions, especially when the steering party or the steered party comprises more than one mode, as

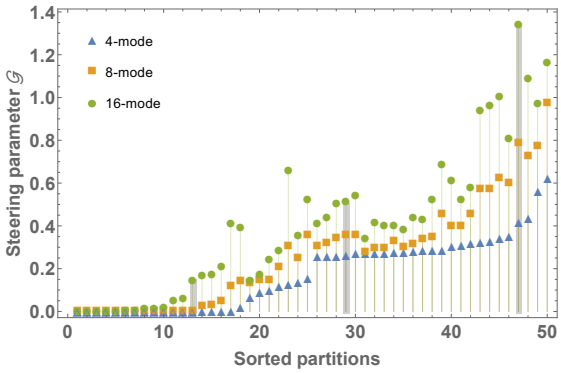


Figure 3: In the multimode state generated by a quantum frequency comb, EPR steering among four spectral bands $ABCD$ are measured experimentally with 4 (blue triangles), 8 (orange squares), 16 (green dots) spectral pixels, respectively. The partitions are arranged from small to large according to the steerability of 4-mode state. Points presented in the same line means the spectral components of their steering party and steered party are same.

shown in Fig. 3. This phenomenon can be understood as a consequence of an unique property of our generation system that more individual squeezed eigenmodes can be extracted from the downconversion process by using higher spectral resolutions of pulse shaping without resorting to modification of the photonics architecture. Then, our experimental results demonstrate that type-I, type-III and type-IV remain valid for all possible nontrivial mode partitions regardless of the spectral resolutions. But type-II monogamy relation can be lifted when the steered party is made of more than one mode, which has been theoretically predicted before [15]. Here, we present an experimental observation that both $C \to (AB)$ and $D \to (AB)$ simultaneously steerable by Gaussian measurements, with their Gaussian steerability $\mathcal{G}^{C\to(AB)} = 0.2836$ and $\mathcal{G}^{D\to(AB)} = 0.2791$ even if the spectrum is divided into only 4 pixels. When the detection spectral resolutions increase, the violation will be stronger with different partitions of spectral band modes.

Conclusion- Our work thus provides a concrete in-depth understanding of EPR steering and its monogamy in paradigmatic multipartite states such as cluster state and multimode state via a quantum frequency comb, and advances our fundamental knowledge of monogamy relations for Gaussian steerability. In turn, this can be useful to gauge the usefulness of these states for quantum communication technologies.

References

[1] X. W. Deng, Y. Xiang, C. Tian, G. Adesso, Q. Y. He, Q. H. Gong, X. L. Su, C. D. Xie, and K. C. Peng, Phys. Rev. Lett. **118**, 230501 (2017).

[2] Yin Cai, Y. Xiang, Yang Liu, Q. Y. He, N. Treps and C. Fabre, in preparation.

[3] E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555–563 (1935).

[4] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777–780 (1935).

[5] M. D. Reid, Phys. Rev. A **40**, 913–923 (1989).

[6] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[7] M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, and G. Leuchs, Rev. Mod. Phys. **81**, 1727–1751 (2009).

[8] Q. Y. He, Q. H. Gong, and M. D. Reid, Phys. Rev. Lett. **114**, 060402 (2015).

[9] I. Kogias, A. R. Lee, S. Ragy, and G. Adesso, Phys. Rev. Lett. **114**, 060403 (2015).

[10] 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).

[11] D. Cavalcanti, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. Souto Ribeiro, and S. P. Walborn, Nat. Commun., **6**, 7941 (2015).

[12] C.-M. Li, K. Chen, Y.-N. Chen, Q. Zhang, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett., **115**, 010402 (2015).

[13] M. D. Reid, Phys. Rev. A **88**, 062108 (2013).

[14] S-W. Ji, M. S. Kim and H. Nha, J. Phys. A: Math. Theor. **48**, 135301 (2015).

[15] G. Adesso and R. Simon, J. Phys. A: Math. Theor. **49**, 34LT02 (2016).

[16] Y. Xiang, I. Kogias, G. Adesso, and Q. Y. He, Phys. Rev. A **95**, 010101(R) (2017).

[17] L. Lami, C. Hirche, G. Adesso, and A. Winter, Phys. Rev. Lett. **117**, 220502 (2016).

Polarization insensitive frequency conversion for a fiber-optic communication of an atom-photon entanglement

Toshiki Kobayashi[1 2 *] Rikizo Ikuta [1 2] Tetsuo Kawakami[2] Shigehito Miki[3 4]
Masahiro Yabuno[3] Taro Yamashita[5 6] Hirotaka Terai[3] Masato Koashi[7]
Tetsuya Mukai[8] Takashi Yamamoto[1 2] Nobuyuki Imoto[1]

[1] *Quantum Information and Quantum Biology Division, Institute for Open and Transdisciplinary Research Initiatives, Osaka University, Osaka 560-8531, Japan*
[2] *Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*
[3] *Advanced ICT Research Institute, National Institute of Information and Communications Technology (NICT), Kobe 651-2492, Japan*
[4] *Graduate School of Engineering Faculty of Engineering, Kobe University, Kobe 657-0013, Japan*
[5] *Graduate school of Engineering, Nagoya University, Nagoya 464-8603, Japan*
[6] *PRESTO, Japan Science and Technology Agency, Saitama 332-0012, Japan*
[7] *Photon Science Center, Graduate School of Engineering, The University of Tokyo, Bunkyo-ku, Tokyo 113-8656, Japan*
[8] *NTT Basic Research Laboratories, NTT Corporation, Atsugi, Kanagawa 243-0198, Japan*

Abstract. Quantum network with a current telecom photonic infrastructure is deficient in quantum storages that keep arbitrary quantum state in sufficient time duration for a long-distance quantum communication with quantum repeater algorithms. Atomic quantum storages have achieved subsecond storage time corresponding to 1000 km transmission time for a telecom photon through a quantum repeater algorithm. However, the telecom photon is not directly accessible to typical atomic storages. Solid state quantum frequency conversions fill this wavelength gap and add more abilities, for example, a frequency multiplexing. Here we report on the experimental demonstration of a polarization-insensitive solid-state quantum frequency conversion to a telecom photon from a short-wavelength photon entangled with an atomic ensemble. Atom-photon entanglement has been generated with a Rb atomic ensemble and the photon has been translated to telecom range while retaining the entanglement by our nonlinear-crystal-based frequency converter in a Sagnac interferometer.

Keywords: Quantum interference, Nonlinear optics

1 Introduction

Quantum frequency conversion [1] (QFC) based on nonlinear optical processes enables us to change the color of photons without destroying the quantum properties. This allows us to transfer quantum properties of a physical system to another one which have different accessible frequencies through a single photon [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]. Besides that, we can use QFC for other purposes such as erasing distinguishability of photons [14], manipulating spectral and temporal modes of photons [15, 16, 17, 18, 19, 20, 21, 22, 23], and performing frequency-domain quantum information processing [24, 25, 26] by tailoring of the pump light. Most of those abilities have been demonstrated with solid-state QFC devices because of its applicability to a wide frequency range, which is similar to the mirrors and beamsplitters (BSs) for the spatial manipulation of the photons.

The extension of the solid-state QFC for the quantum storages have also been actively studied [27, 28, 29]. For a long-distance quantum communication, a long lifetime quantum storage that entangled with a telecom photon is necessary. The cold Rb atomic ensemble is one of the promising quantum storage that has a long lifetime and a high efficiency atom-photon entanglement generation [30, 31, 3, 32, 33, 34, 35]. Recently, solid-state QFC of a single photon from the cold Rb atomic ensemble has been demonstrated [28, 29]. But the quantum state preservation, which is an ability that cannot be mimicked by a classical memory, has never been shown yet. In this work[36], we report a polarization-insensitive QFC (PIQFC), which converts the frequency (wavelength) of a photon while preserving the input polarization state. Our solid-state PIQFC device consists of a waveguided periodically poled lithium niobate (PPLN) crystal installed in a Sagnac interferometer. By using the QFC device, we converted a 780-nm polarized photon entangled with a cold Rb atomic ensemble to a telecom wavelength of 1522 nm. Entanglement between the Rb atoms and the converted telecom photon has been clearly observed.

2 Experimental setup

To prepare a 780-nm signal photon entangled with the Rb atoms, we construct an experimental setup as shown in Fig. 1a. We prepare the Rb atomic ensemble by a magneto-optical trap (MOT) in 20 ms. After the trapping lasers and the magnetic field for the MOT are turned off, we perform the QFC experiment 990 times within 1 ms. A horizontally (H-) polarized 200-ns initialization pulse initializes the atoms into ground level g_a ($F = 1$). Then a vertically (V-) polarized 70-ns write pulse blue-

*kobayashi-t@qi.mp.es.osaka-u.ac.jp

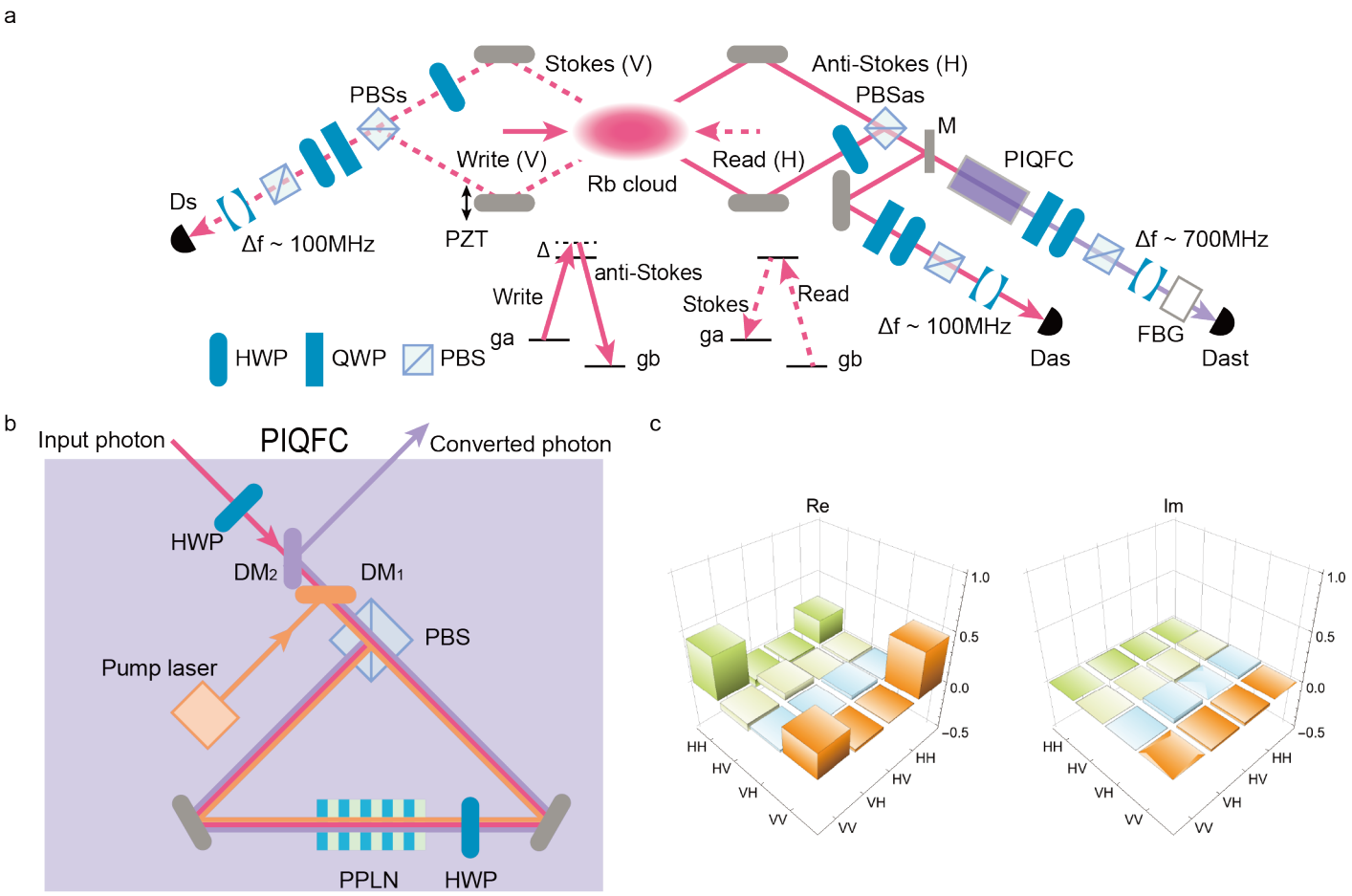


Figure 1: **QFC as a frequency-domain linear optics with the two polarization modes. a**, Our experimental setup for entanglement between Rb atoms and visible/telecom photons without/with QFC. When mirror M is flipped up, AS photon is detected by D_{as} without QFC. When mirror M is flipped down, AS photon is input to polarization-insensitive QFC (PIQFC) in Fig. 1b and then the converted photon is detected by D_{ast}. **b**, The experimental setup of PIQFC. Type-0 quasi-phase-matched PPLN crystal as a nonlinear optical medium which acts on only the V-polarized photons is installed in the Sagnac type interferometer. **c**, The reconstructed density matrix with QFC.

detuned by Δ ~10 MHz from the resonant frequency between g_a and an excited level ($F' = 2$) is injected to the atoms, causing the Raman transition with emission of anti-Stokes (AS) photons.

The momentum conservation guarantees that the wave vector $\boldsymbol{k}_{\rm atom}$ of the collective spin excitation of the atoms satisfies $\boldsymbol{k}_{\rm atom} = \boldsymbol{k}_{\rm W} - \boldsymbol{k}_{\rm AS}$, where $\boldsymbol{k}_{\rm W/AS}$ is the wave vector of the write/AS light. In our experiment, we select the H-polarized AS photons emitted in two directions as shown in Fig. 1a, and use a HWP and a PBS (PBS_{as}) to convert path information of AS photons into polarization information. After the operation, we obtain

$$(|H\rangle_{\rm AS}|k_+\rangle_{\rm atom} + |V\rangle_{\rm AS}|k_-\rangle_{\rm atom})/\sqrt{2}, \qquad (1)$$

where $|k_\pm\rangle$ denotes collective spin excitation of the atoms when the AS light in the upper(+)/lower(−) path in Fig. 1a, respectively.

In order to evaluate the quantum correlation between the atoms and the photons, we inject an H-polarized 100-ns read light at the resonant frequency between a ground revel g_b ($F = 2$) and the excited level into the atoms. The read light provides the transition of the Rb atoms to g_a and generation of the Stokes (S) photons. In our experiment, we collect only the V-polarized component of the S photons. The direction of the emitted S photons is decided by the wave vector of the atomic excitation. Because such a read operation does not access the AS photon, the operation never increase or newly create the entanglement between the atoms and the AS photon. Thus observation of an entangled state of the which-path state of the S photon and the polarizing AS photon is the evidence of the entanglement between the atoms and the AS photon before the read operation.

In the experiment, we inject the read pulse from the direction opposite to the write pulse. The wave vector $\boldsymbol{k}_{\rm R}$ of the read pulse satisfies $\boldsymbol{k}_{\rm R} \sim -\boldsymbol{k}_{\rm W}$, leading to the relation $\boldsymbol{k}_{\rm S} \sim -\boldsymbol{k}_{\rm AS}$ from the momentum conservation. This means the S photons are emitted in a direction at $\sim \mp 3^\circ$ relative to the direction of the read pulse when the AS photons are emitted in a direction at $\sim \pm 3^\circ$ relative to that of the write pulse. By using a HWP and a PBS (PBS_s) shown in Fig. 1a, the path information of the

V-polarized S photons is transformed into the polarization. Finally, we can observe the entanglement between the atoms and the AS photons through the polarization entangled photon pair of the AS and the S photons.

After passing through a polarization analyzer composed of a QWP, a HWP, and a PBS for the quantum state tomography [45], S photon passes through a monolithic cavity-coated lens as a frequency filter and is coupled to a single-mode optical fiber. Then S photon is detected by a silicon avalanche photon detector (APD) denoted by D_s.

When we do not perform QFC, AS photon is detected by another APD (D_{as}) after passing through a polarization analyzer, a cavity-coated lens and a single-mode optical fiber. When we perform QFC, mirror M in Fig. 1a is flipped down in order to send the AS photon to the PIQFC. In the PIQFC setup, we install a type-0 quasi-phase-matched PPLN waveguide in the Sagnac interferometer as the nonlinear optical medium for QFC. The PPLN converts a V-polarized input 780-nm photon to a V-polarized 1522-nm converted photon with the use of the V-polarized pump light at 1600 nm. As shown in Fig. 1b, the input photon with any polarization is converted into telecom photon. The conversion efficiencies of QFC for clockwise and anti-clockwise directions are adjusted by the amplitude of the pump light to be the same. The telecom photon from the QFC passes through a polarization analyser followed by an etalon, and a pair of fiber Bragg gratings. Finally, the telecom photon is detected by a superconducting single photon detector (SSPD) denoted by D_{ast} [47].

3 Experimental result

Without QFC, we performed the quantum state tomography between the S photon and the AS photon, and reconstructed density operator $\rho_{S,AS}$. we estimated entanglement of formation [49] (EoF) E and the purity defined by $P = \mathrm{tr}(\rho_{S,AS}^2)$ as $E = 0.37 \pm 0.11$ and $P = 0.61 \pm 0.06$, respectively. We also estimated a maximized fidelity to a maximally entangled state $U_\theta|\phi^+\rangle$ defined by $F = \max_\theta \langle\phi^+|U_\theta^\dagger \rho_{S,AS} U_\theta|\phi^+\rangle$, whose value was $F = 0.78 \pm 0.05$ for $\theta = \theta_0 = -65°$. Here $|\phi^+\rangle = (|H\rangle_{AS}|H\rangle_S + |V\rangle_{AS}|V\rangle_S)/\sqrt{2}$ and $U_\theta = \exp(-i\theta Z/2) \otimes I$ with $Z = |H\rangle\langle H| - |V\rangle\langle V|$ and $I = |H\rangle\langle H| + |V\rangle\langle V|$. These results show the entanglement between AS photon and the Rb atoms.

With QFC, we performed the quantum state tomography between S photon and the wavelength-converted AS photon. The estimated EoF and purity of reconstructed density operator $\rho_{S,ASt}$ were $E = 0.25 \pm 0.13$ and $P = 0.55 \pm 0.07$, respectively. The maximized fidelity to $U_\theta|\phi^+\rangle$ about θ was $F = 0.69 \pm 0.07$ for $\theta = \theta_1 = 93°$. The matrix representation of density operator $U_{\theta_1}^\dagger \rho_{S,ASt} U_{\theta_1}$ is shown in Fig. 1c. The EoF E is clearly greater than 0, which shows that the state of the Rb atoms and the telecom photon has entanglement. From the result, we succeeded the creation of the entanglement between the Rb atoms and the telecom photon by using the polarization-insensitive QFC.

4 Conclusion

In conclusion, we have shown the entanglement between the wave vector of the collective spin excitation of the Rb atoms and the polarizing telecom photon by using the polarization insensitive QFC composed of the PPLN waveguide installed in a Sagnac interferometer. Combining state-of-the-art quantum memory technologies [35, 50, 51] with our experimental result will be useful for fiber-based quantum communication over long distance. Furthermore, the demonstrated polarization insensitive QFC is applicable to various conversion systems for matter-based quantum storages. The devices will provide various kinds of tasks developed in the linear optical quantum information processing.

Acknowledgements

We thank Yoshiaki Tsujimoto and Motoki Asano for helpful discussions about QFC. This work was supported by CREST, JST JPMJCR1671 and MEXT/JSPS KAKENHI Grant Numbers JP26286068, JP15H03704, JP16H02214, and JP16K17772.

References

[1] P. Kumar, Optics Letters **15**, 1476 (1990).

[2] S. Tanzilli *et al.*, Nature **437**, 116 (2005).

[3] Y. Dudin *et al.*, Physical Review Letters **105**, 260502 (2010).

[4] H. J. McGuinness, M. G. Raymer, C. J. McKinstrie, and S. Radic, Phys. Rev. Lett. **105**, 093604 (2010).

[5] M. T. Rakher, L. Ma, O. Slattery, X. Tang, and K. Srinivasan, Nature photonics **4**, 786 (2010).

[6] R. Ikuta *et al.*, Nature communications **2**, 1544 (2011).

[7] S. Ramelow, A. Fedrizzi, A. Poppe, N. K. Langford, and A. Zeilinger, Phys. Rev. A **85**, 013845 (2012).

[8] S. Zaske *et al.*, Physical Review Letters **109**, 147404 (2012).

[9] S. Ates *et al.*, Phys. Rev. Lett. **109**, 147405 (2012).

[10] K. De Greve *et al.*, Nature **491**, 421 (2012).

[11] R. Ikuta *et al.*, Physical Review A **87**, 010301(R) (2013).

[12] H. Rütz, K.-H. Luo, H. Suche, and C. Silberhorn, Phys. Rev. Applied **7**, 024021 (2017).

[13] S.-L. Liu *et al.*, Optics Express **25**, 24290 (2017).

[14] H. Takesue, Physical Review Letters **101**, 173901 (2008).

[15] D. Kielpinski, J. F. Corney, and H. M. Wiseman, Phys. Rev. Lett. **106**, 130501 (2011).

[16] B. Brecht, A. Eckstein, A. Christ, H. Suche, and C. Silberhorn, New Journal of Physics **13**, 065029 (2011).

[17] J. Lavoie, J. M. Donohue, L. G. Wright, A. Fedrizzi, and K. J. Resch, Nature Photonics **7**, 363 (2013).

[18] K. A. Fisher *et al.*, Nature communications **7** (2016).

[19] N. Matsuda, Science advances **2**, e1501223 (2016).

[20] P. Manurkar *et al.*, Optica **3**, 1300 (2016).

[21] T. Kroh, A. Ahlrichs, B. Sprenger, and O. Benson, Quantum Science and Technology (2017).

[22] M. Allgaier *et al.*, Nature Communications **8**, 14288 (2017).

[23] M. Allgaier *et al.*, arXiv preprint arXiv:1702.03240 (2017).

[24] T. Kobayashi *et al.*, Nature Photonics (2016).

[25] S. Clemmen, A. Farsi, S. Ramelow, and A. L. Gaeta, Phys. Rev. Lett. **117**, 223601 (2016).

[26] T. Kobayashi *et al.*, Optics Express **25**, 12052 (2017).

[27] X. Fernandez-Gonzalvo *et al.*, Optics express **21**, 19473 (2013).

[28] P. Farrera, N. Maring, B. Albrecht, G. Heinze, and H. de Riedmatten, Optica **3**, 1019 (2016).

[29] R. Ikuta *et al.*, Optica **3**, 1279 (2016).

[30] Z.-S. Yuan *et al.*, Nature **454**, 1098 (2008).

[31] R. Zhao *et al.*, Nature Physics **5**, 100 (2009).

[32] S. Ritter *et al.*, Nature **484**, 195 (2012).

[33] X.-H. Bao *et al.*, Nature Physics **8**, 517 (2012).

[34] J. Hofmann *et al.*, Science **337**, 72 (2012).

[35] S.-J. Yang, X.-J. Wang, X.-H. Bao, and J.-W. Pan, Nature Photonics **10**, 381 (2016).

[36] R. Ikuta *et al.*, Nature communications **9**, 1997 (2018).

[37] R. Ikuta *et al.*, Optics Express **22**, 11205 (2014).

[38] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[39] P. G. Kwiat, S. Barraza-Lopez, A. Stefanov, and N. Gisin, Nature **409**, 1014 (2001).

[40] E. Knill, R. Laflamme, and G. Milburn, Nature **409**, 46 (2000).

[41] R. Okamoto, J. L. OBrien, H. F. Hofmann, and S. Takeuchi, Proceedings of the National Academy of Sciences **108**, 10067 (2011).

[42] A. Ling, K. P. Soh, A. Lamas-Linares, and C. Kurtsiefer, Phys. Rev. A **74**, 022309 (2006).

[43] T. Tashima *et al.*, Physical review letters **102**, 130502 (2009).

[44] R. Ikuta *et al.*, Phys. Rev. Lett. **106**, 110503 (2011).

[45] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Phys. Rev. A **64**, 052312 (2001).

[46] P. Palittapongarnpim, A. MacRae, and A. Lvovsky, Review of Scientific Instruments **83**, 066101 (2012).

[47] S. Miki, M. Yabuno, T. Yamashita, and H. Terai, Optics Express **25**, 6796 (2017).

[48] J. Řeháček, Z. Hradil, E. Knill, and A. I. Lvovsky, Phys. Rev. A **75**, 042108 (2007).

[49] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[50] Y. Pu *et al.*, Nature Communications **8** (2017).

[51] Y.-F. Pu *et al.*, arXiv preprint arXiv:1707.09701 (2017).

[52] A. Lenhard, J. Brito, M. Bock, C. Becher, and J. Eschner, Optics Express **25**, 11187 (2017).

[53] V. Krutyanskiy, M. Meraner, J. Schupp, and B. Lanyon, Applied Physics B **123**, 228 (2017).

[54] H. Briegel, D. Browne, W. Dur, R. Raussendorf, and M. Van den Nest, Nature Physics **5**, 19 (2009).

[55] T. D. Ladd *et al.*, Nature **464**, 45 (2010).

[56] I. Buluta, S. Ashhab, and F. Nori, Reports on Progress in Physics **74**, 104401 (2011).

Toward "quantum supremacy" with single photons

Chaoyang Lu

Abstract. Quantum computers can in principle solve certain problems faster than classical computers. Despite substantial progress in the past decades, building quantum machines that can actually outperform classical computers for some specific tasks—a milestone termed as " quantum supremacy "—remained challenging. Boson sampling has been considered as an intermediate step for linear optical quantum computing, and a strong candidate to demonstrate the quantum computational supremacy. The experimental challenge for realizing a large-scale boson sampling mainly lies in the lack of a perfect single-photon sources. In this talk, I will report two routes towards building boson sampling machines with many photons. In the first path, we developed parametric down-conversion two-photon source with simultaneously a collection efficiency of 97% and an indistinguishability of 96% between independent photons [PRL 121, 250505 (2018)]. With this, we demonstrate genuine entanglement of 12 photons, scattershot boson sampling, and Gaussian boson sampling. We also made efforts to generate efficient and indistinguishable entangled photons from quantum dots [PRL 122, 113602 (2019)]. In the second path, using a quantum dot-micropillar, we produced single photons with high purity ($> 99\%$), near-unity indistinguishability for >1000 photons, and high extraction efficiency—all combined in a single device compatibly and simultaneously [PRL 116, 020401 (2016)]. The highest-quality single photons allowed us to perform quantum interference with sunlight with 80% raw visibility, which proved the quantum nature of thermal light [PRL online 2019]. We developed bichromatic laser excitation [Nature Physics online 2019] and elliptical microcavites [Nature Photonics online 2019] to overcome the polarization filtering to create truly optimal single photon sources. We build few photon boson sampling machines which runs 5-7 orders of magnitudes faster than all the previous experiments [Nature Photonics 11, 365 (2017)]. Plan is to achieve boson sampling with 20-30 photons in the near term. More relevant papers can be found at http://staff.ustc.edu.cn/ cylu.

Verification of independent quantum devices

Joe Fitzsimmons

Abstract. Quantum computers are on the brink of surpassing the capabilities of even the most powerful classical computers. This naturally raises the question of how one can trust the results of a quantum computer when they cannot be compared to classical simulation. In this talk, I will discuss an approach to cross-checking the results of independent quantum processors based on the one-way model of quantum computation, which allows circuits of varying complexity to be directly compared. This approach enables consistency checks of quantum computations within a single device, as well as between independent devices. I will report results obtained by implementing the protocol on five state-of-the-art quantum processors, based on four distinct physical architectures: nuclear magnetic resonance, superconducting circuits, trapped ions, and photonics, with up to 6 qubits and more than 200 distinct circuits.

Quantum causal influence

Xiaoliang Qi

Abstract. We introduce a framework to study the emergence of time and causal structure in quantum many-body systems. In doing so, we consider quantum states which encode spacetime dynamics, and develop information theoretic tools to extract the causal relationships between putative spacetime subsystems. Our analysis reveals a quantum generalization of the thermodynamic arrow of time and begins to explore the roles of entanglement, scrambling and quantum error correction in the emergence of spacetime. For instance, exotic causal relationships can arise due to dynamically induced quantum error correction in spacetime: there can exist a spatial region in the past which does not causally influence any small spatial regions in the future, but yet it causally influences the union of several small spatial regions in the future. We provide examples of quantum causal influence in Hamiltonian evolution, quantum error correction codes, quantum teleportation, holographic tensor networks, the final state projection model of black holes, and many other systems. We find that the quantum causal influence provides a unifying perspective on spacetime correlations in these seemingly distinct settings. In addition, we prove a variety of general structural results and discuss the relation of quantum causal influence to spacetime quantum entropies.

Quantum Communications Network Based on Polarization Entanglement at Telecom Wavelength

Sören Wengerowsky[1 2 *] Siddarth Koduru Joshi[1 2 3 †] Fabian Steinlechner[1 2 4 5 ‡]
Hannes Hübel[6 §] Rupert Ursin[1 2 ¶]

[1] *Institute for Quantum Optics and Quantum Information - Vienna, Austrian Academy of Sciences, Vienna, Austria*
[2] *Vienna Center for Quantum Science and Technology (VCQ), Vienna, Austria*
[3] Present Address: *Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, United Kingdom*
[4] Present Address: *Fraunhofer Institute for Applied Optics and Precision Engineering IOF Jena, Germany*
[5] Present Address: *Abbe Center of Photonics, Friedrich Schiller University Jena, Jena, Germany*
[6] *Optical Quantum Technology, Digital Safety & Security Department, AIT Austrian Institute of Technology GmbH, Vienna, Austria*

Abstract. Here we implement a novel network architecture which enables scalable quantum communication networks at telecommunication wavelengths. Our simple scheme uses wavelength multiplexed polarization entangled photon pairs. In our experiment we have demonstrated the network with 4 clients and used 12 wavelength channels to share 6 bipartite entangled states between each pair of clients in a mesh-like network topology using only one fiber per client.

Keywords: quantum communications, entangled photons, network, quantum key distribution

We present a proof-of-principle experiment consisting of four users in a novel network architecture which enables scalable quantum communication based on polarization-entangled photon pairs at telecommunications wavelength. Our scheme uses frequency multiplexing [3, 2, 5] to share 6 two-photon entangled states between each pair of clients in a mesh-like network topology using only one fiber per client.

As clients need minimal resources – one polarization detection module and single-mode fiber each, the physical topology of the network scales linearly if a user is added, while the logical topology scales quadratically with $n(n-1)$ network connections between n users. The quantum correlations and physical topology are illustrated in figure 1.

The source employs type 0 spontaneous parametric down-conversion centered at 1550 nm, pumped by a continuous-wave laser. The resulting 60 nm-wide spectrum is split symmetrically into 6 pairs of wavelength-correlated channels similar to Aktas et al. [1]. Due to energy conservation in the down-conversion process, the partner photons are found at equal frequency distance from the center of the spectrum. Each client receives 3 channels which are polarization-entangled with the channels sent to each of the other clients. Every client measures all three channels in a single polarization analyzer in either the HV or DA basis and records the results using a time tagging unit. Photon pairs were identified by their relative arrival times.

Since only 4 detectors were available, every user only had one detector with a very slow basis choice, imple-

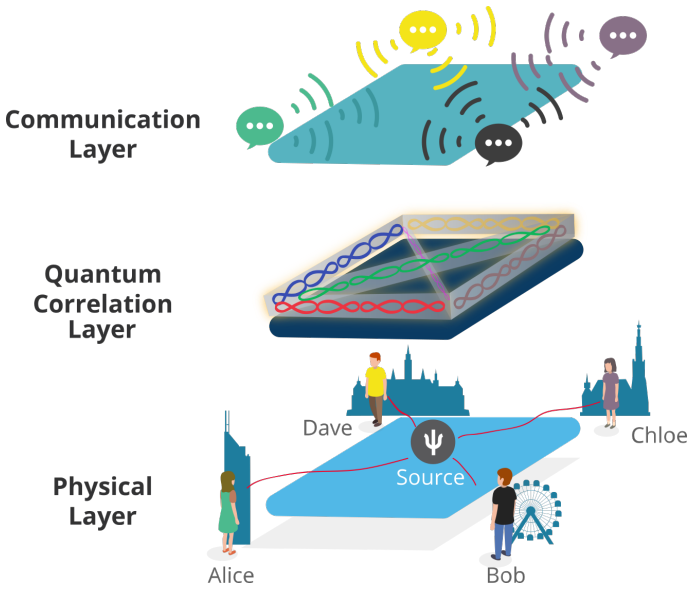


Figure 1: Scheme of our network architecture: Different layers represent different levels of abstraction. *Physical layer:* contains all tangible components. Each of the 4 clients receives a combination of 3 channels via a solitary single mode fiber. Thus, the source distributes 6 bi-partite entangled photon states to the four clients Alice, Bob, Chloe and Dave. *Quantum Correlation layer:* shows the 6 entangled states (each corresponding to a different secure key) that link the 4 clients. *Communications Layer:* Entanglement-based two-party QKD protocols like E91 can be used to generate secure keys between all pairs of clients.

* soeren.wengerowsky@oeaw.ac.at
† siddarthkjoshi@gmail.com
‡ Fabian.Steinlechner@iof.fraunhofer.de
§ Hannes.Huebel@ait.ac.at
¶ Rupert.Ursin@oeaw.ac.at

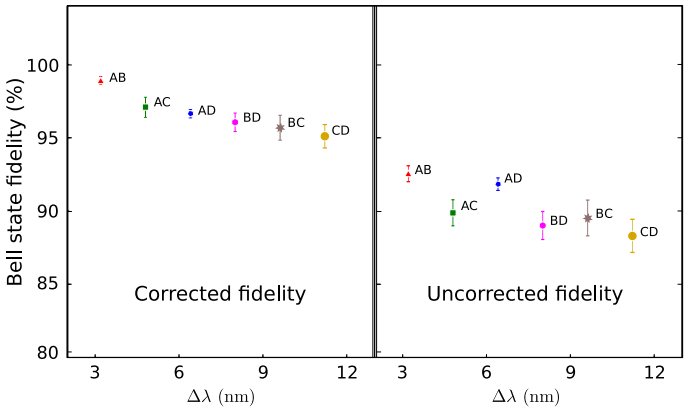


Figure 2: Measured fidelities with and without subtraction of accidental coincidences. Each point is measured using two WDM channels which connect the respective users. The X-axis represents the difference in wavelength between the respective channels of the respective two partner photons.

mented with a motorized half-wave plate. This way, no secret keys could be generated, but we successfully implemented a 4 client network and measured the polarization correlation visibility to assess whether it would be suitable for a quantum communication network. Figure 2 shows the results of the Bell state fidelity measurements. We observed uncorrected polarization correlation fidelities larger than 85% in both bases and for all pairs of clients. Due to the timing uncertainty of the detectors, we are limited to a rather large coincidence windows of 1 ns. This way, detector clicks are falsely identified as pairs and deteriorate the measured fidelity. The left hand side of the graph shows the fidelity corrected for this error while the uncorrected values are shown to the right. Based on these visibilities and count rates, we estimated secure key rates between 2 and 15 bits/s in case the setup would have employed 2 detectors per node and a random basis choice. The network continues to offer all the security benefits of entanglement based QKD and does not require trusted nodes. In contrast to networks based on active switching, the only limit on the communication speed in our passive scheme is given by the brightness of the source and the "quality" of the detector (efficiency, timing jitter and dead time). The finite duty cycle and switching rate of a possible active component do not limit our network.

An alternative method to implement a fully connected quantum network with a similar topology would be to use a 1:N beam-splitter and probabilistically distribute entangled photon pairs between all users. The main benefit of our wavelength multiplexed implementation reveals itself when each user opts to de-multiplex the different wavelength channels onto m polarization analysis modules with detectors (where $1 < m < N$). In this case, due to the deterministic frequency correlations, every pair of frequency channels can be considered an independent communication link and a m-fold increase in the total key generation rate is achieved while maintaining the same signal-to-noise ratio of a two-party communication. Conversely, probabilistic distribution using a 1:N beam-splitter would always reduce the signal-to-noise ratio as users are added.

We have successfully realized a proof of principle demonstration of a quantum communication network. The use of telecommunication wavelengths makes it compatible with existing infrastructure. We observed no detectable cross-talk between adjacent channels. The network architecture can be readily adapted to any other network topology. Furthermore, distributed computation tasks or problems like the millionaire's problem could be implemented on this network. More information about this experiment can be found in [4].

References

[1] D. Aktas, B. Fedrici, F. Kaiser, T. Lunghi, L. Labonté, and S. Tanzilli. Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography. *Laser & Photonics Reviews*, 10(3):451–457, may 2016.

[2] I. Herbauts, B. Blauensteiner, A. Poppe, T. Jennewein, and H. Hübel. Demonstration of active routing of entanglement in a multi-user network. *Opt. Express*, 21(23):29013–29024, Nov 2013.

[3] H. C. Lim, A. Yoshizawa, H. Tsuchida, and K. Kikuchi. Broadband source of telecom-band polarization-entangled photon-pairs for wavelength-multiplexed entanglement distribution. *Optics express*, 16(20):16052–16057, 2008.

[4] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin. An entanglement-based wavelength-multiplexed quantum communication network. *Nature*, 564(7735), 2018.

[5] E. Y. Zhu, C. Corbari, A. V. Gladyshev, P. Kazansky, H.-K. Lo, and L. Qian. Multi-party agile qkd network with a fiber-based entangled source. In *CLEO: 2015*, page JW2A.10. Optical Society of America, 2015.

Black-box quantum state preparation without arithmetic

Yuval R. Sanders[1] * Guang Hao Low[2] Artur Scherer[3] Dominic W. Berry[1] †

[1] *Department of Physics and Astronomy, Macquarie University, Sydney NSW 2109, Australia.*
[2] *Quantum Architectures and Computation Group, Microsoft Research, Redmond WA 98052, USA.*
[3] *1QB Information Technologies (1QBit), Vancouver BC V6C 2B5, Canada.*

Abstract. Black-box quantum state preparation is an important subroutine in many quantum algorithms. The standard approach requires the quantum computer to do arithmetic, which is a key contributor to the complexity. Here we present a new algorithm that avoids arithmetic. We thereby reduce the number of gates by a factor of 286-374 over the best prior work for realistic precision; the improvement factor increases with the precision. As quantum state preparation is a crucial subroutine in many approaches to simulating physics on a quantum computer, our new method brings useful quantum simulation closer to reality.

Keywords: state preparation, Hamiltonian simulation, quantum walks

1 Context

Grover devised [1] the first black-box quantum state preparation procedure as an extension of his more famous search algorithm [2]. Whereas Grover search performs amplitude amplification on a simple procedure, one application of a given oracle (the 'black-box') with a binary output, Grover state preparation prescribes a more complicated procedure per round of amplitude amplification. In addition to applying the oracle, Grover's procedure requires the quantum computer to calculate an inverse trigonometric function during each round of amplitude amplification. Such a calculation is expensive in practice.

The complexity of repeated inverse trigonometric calculations implies a high cost for quantum algorithms that use black-box state preparation as a subroutine. Some example applications include the discrete-time quantum walk approach to Hamiltonian simulation [3, 4, 5] and the linear combination of unitaries (LCU) technique [6, 7, 8, 9, 10]. In this paper, we present a modification to Grover's original state preparation procedure that avoids the need to calculate an inverse trigonometric function, or indeed the need to perform any arithmetic operations at all. Our work has been published [11] and a free version is available online [arXiv:1807.03206].

2 Main Result

The task of black-box quantum state preparation. The scenario for black-box state preparation is as follows. We are given access to a quantum oracle $\mathtt{amp}$ that returns target coefficients as follows: if $\vec{\alpha} := (\alpha_0, \alpha_1, \ldots, \alpha_{d-1})$ is a real vector with $0 \leq \alpha_\ell < 1$ for each $\ell = 0, \ldots, d-1$, then

$$\mathtt{amp}\,|\ell\rangle\,|z\rangle := |\ell\rangle\ |z \oplus \alpha_\ell^{(n)}\rangle\,, \tag{1}$$

where z is an n-bit integer encoded into an n-qubit register, $\oplus$ represents a bitwise XOR, and $\alpha_\ell^{(n)} = \lfloor 2^n \alpha_\ell \rfloor$. The task is to prepare an approximation to the 'target' state

$$|\text{target}\rangle := \frac{1}{\|\vec{\alpha}\|_2} \sum_{\ell=0}^{d-1} \alpha_\ell\,|\ell\rangle\,. \tag{2}$$

Grover's approach. Grover's approach to state preparation uses a subroutine defined as

$$\mathtt{rot}\,|\xi\rangle\,|0\rangle := |\xi\rangle\,(\sin\theta\,|0\rangle + \cos\theta\,|1\rangle)\,, \tag{3}$$

where ξ is one of the values $\alpha_\ell^{(n)}$, the second register is a qubit and θ is a high-precision approximation to $\arcsin(\xi/2^n)$. To implement this procedure, the quantum computer would calculate θ, store the value in an ancillary register, and use that register as the control for a sequence of rotation operations on the qubit. Grover then prescribes roughly $\sqrt{d}/\|\vec{\alpha}\|_2$ rounds of amplitude amplification on the following procedure:

$$\begin{aligned}
&|0\rangle_{\mathtt{out}}^{\otimes \mathcal{O}(\log d)}\,|0\rangle_{\mathtt{data}}^{\otimes n}\,|0\rangle_{\mathtt{flag}} \\
\xrightarrow{\mathtt{unif}_d}\ &\frac{1}{\sqrt{d}}\sum_{\ell=0}^{d-1}|\ell\rangle_{\mathtt{out}}\,|0\rangle_{\mathtt{data}}^{\otimes n}\,|0\rangle_{\mathtt{flag}} \\
\xrightarrow{\mathtt{amp}}\ &\frac{1}{\sqrt{d}}\sum_{\ell=0}^{d-1}|\ell\rangle_{\mathtt{out}}\left|\alpha_\ell^{(n)}\right\rangle_{\mathtt{data}}|0\rangle_{\mathtt{flag}} \\
\xrightarrow{\mathtt{rot}}\ &\frac{1}{\sqrt{d}}\sum_{\ell=0}^{d-1}|\ell\rangle_{\mathtt{out}}\left|\alpha_\ell^{(n)}\right\rangle_{\mathtt{data}}(\sin\theta_\ell\,|0\rangle + \cos\theta_\ell\,|1\rangle)_{\mathtt{flag}}\,.
\end{aligned} \tag{4}$$

Here we use the symbol $\mathtt{unif}_d$ to refer to a procedure that transforms $\mathcal{O}(\log d)$ qubits into a uniform superposition of values from 0 to $d-1$, θ_ℓ is an approximation to the arcsine of $\alpha_\ell^{(n)}/2^n$, and we use the register labels `out`, `data`, and `flag` to denote the intent for each quantum register. We are to perform amplitude amplification to boost the amplitude on $|0\rangle_{\mathtt{flag}}$ at the expense of $|1\rangle_{\mathtt{flag}}$, after which we use $\mathtt{amp}$ one more time to erase the `data` register (whose purpose was merely to record the output of $\mathtt{amp}$). At this point, we can discard the `data` register and measure the `flag` qubit to obtain (approximately) $|\text{target}\rangle_{\mathtt{out}}$ with high probability. Note that in

*yuval.sanders@mq.edu.au
†dmwberry@gmail.com

some applications we need not measure the `flag` qubit and instead control subsequent operations on this qubit.

Our approach. We modify Grover's approach by replacing $\mathtt{rot}$ with a new procedure

$$\mathtt{comp}\,|a\rangle\,|b\rangle\,|0\rangle := \begin{cases} |a\rangle\,|b\rangle\,|0\rangle & \text{if } a < b, \\ |a\rangle\,|b\rangle\,|1\rangle & \text{if } a \geq b. \end{cases} \tag{5}$$

The idea is as follows. Grover uses $\mathtt{rot}$ in order to 'transduce' the value of the `data` register into an amplitude for the `flag` register. This amplitude transduction step can in principle be done some other way. Our approach to amplitude transduction is to compare one value to an equal superposition of values. Thus

$$\frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} \mathtt{comp} \left|\alpha_\ell^{(n)}\right\rangle |z\rangle\,|0\rangle = \underbrace{\frac{1}{\sqrt{2^n}} \sum_{z=0}^{\alpha_\ell^{(n)}-1} \left|\alpha_\ell^{(n)}\right\rangle |z\rangle\,|0\rangle}_{\alpha_\ell^{(n)} \text{ terms}} + \underbrace{\frac{1}{\sqrt{2^n}} \sum_{z=\alpha_\ell^{(n)}}^{2^n-1} \left|\alpha_\ell^{(n)}\right\rangle |z\rangle\,|1\rangle}_{2^n-\alpha_\ell^{(n)} \text{ terms}}. \tag{6}$$

The key observation is that the amplitude of $|0\rangle$ for the last qubit is related to the value encoded in the second register. We then apply $\mathtt{unif}_{2^n}^{-1}$ to the second register and perform amplitude amplification to boost the amplitude of $|0\rangle^{\otimes(n+1)}$ on the final $n+1$ qubits above. This achieves the required amplitude transduction.

Speedup. Our speedup is based on the number of operations to be performed in addition to the oracle $\mathtt{amp}$ per round of amplitude amplification. Whereas $\mathtt{rot}$ requires the quantum computer to perform many arithmetic operations in order to calculate an arcsine, we can perform $\mathtt{comp}$ using $2n-1$ Toffoli gates using a variant of the ripple-carry adder of [12] (see Sec. 4.3). Alternatively, we can use a technique of [13] to reduce this cost to n Toffoli gates and n measurements. These costs are technically identical to that of a single addition circuit, but we do not actually perform the addition and so can technically get away with our paper's title. By contrast, calculation of an arcsine requires many coherent multiplications, which is a far greater cost than addition. A recent paper [14] offers explicit Toffoli counts for an arcsine for a few given precision targets: from Table II, precision 10^{-5} requires 4872 Toffoli gates, 10^{-7} requires 7784, and 10^{-9} requires 11264. We can contrast these numbers to the number of Toffoli gates needed to compare two n-bit numbers for $n = 17, 23, 30$ respectively (so that $2^{-n} \approx 10^{-5}, 10^{-7}, 10^{-9}$, respectively). It is from here that we get our headline numbers for our speedup.

3 Variants

Our method can easily be extended to complex amplitudes. These complex amplitudes could be presented in either polar form or Cartesian form, meaning that we have two amplitude oracles rather than one. For the polar form, we would have one oracle for the magnitude of the amplitude and another oracle for the argument; for the Cartesian form, one oracle for the real part and another oracle for the imaginary. In each case, arithmetic can also be avoided for amplitude transduction.

Remarkably, we also have a way to prepare an approximation to the state $\frac{1}{\sqrt{\|\vec{\alpha}\|_1}} \sum_\ell \sqrt{\alpha_\ell}\,|\ell\rangle$ without requiring the quantum computer to perform arithmetic. This version of the state preparation task arises when constructing quantum walk operators. The idea here is to recognise that the comparison trick above yields an amplitude proportional to $\sqrt{\alpha_\ell^{(n)}}$, rather than $\alpha_\ell^{(n)}$ as required. In the main approach we apply $\mathtt{unif}_{2^n}$ and amplify the state $|0\rangle^{\otimes(n+1)}$ to correct this issue, but we could instead skip $\mathtt{unif}_{2^n}$ and amplify $|+\rangle^{\otimes n}\,|0\rangle$. We still need to erase the middle register following amplitude amplification, but we have an elegant trick to do this. We can use this idea to prepare the state with square-root amplitudes when the amplitudes are complex and given in polar form, but if we have Cartesian form then our approach requires some arithmetic (though not much). Our published paper has the details.

4 Implications

We expect our practical complexity reduction to have broad impact throughout quantum algorithms research. In particular, our approach can replace Grover's in all use cases, including the implementation of quantum walk operators and in the LCU technique. These improvements are likely to lead to reductions in gate complexity for many potential applications for quantum computer. Our technique can also be applied in other circumstances where amplitude transduction is needed.

The complexity reduction we achieve is significant enough for a proof-of-principle experiment to be plausible. Although amplitude amplificaiton would probably lead to a circuit with too high a depth for today's prototypes, we could skip amplitude amplification and keep n small for a demonstration.

References

[1] Lov K. Grover. Synthesis of quantum superpositions by quantum computation. *Phys. Rev. Lett.*, 85:1334–1337, Aug 2000.

[2] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, Jul 1997.

[3] Andrew M. Childs. On the relationship between continuous- and discrete-time quantum walk. *Communications in Mathematical Physics*, 294(2):581–603, oct 2009.

[4] Dominic W. Berry and Andrew M. Childs. Black-box Hamiltonian simulation and unitary implemen-

tation. *Quantum Information and Computation*, 12:0029–0062, 2012.

[5] Guang Hao Low and Isaac L. Chuang. Optimal hamiltonian simulation by quantum signal processing. *Phys. Rev. Lett.*, 118:010501, Jan 2017.

[6] Robin Kothari. *Efficient Algorithms in Quantum Query Complexity*. PhD thesis, University of Waterloo, Waterloo, Ontario, 8 2014.

[7] D. W. Berry, A. M. Childs, and R. Kothari. Hamiltonian simulation with nearly optimal dependence on all parameters. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science*, pages 792–809, Oct 2015.

[8] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Simulating hamiltonian dynamics with a truncated taylor series. *Phys. Rev. Lett.*, 114:090502, Mar 2015.

[9] Andrew M. Childs, Robin Kothari, and Rolando D. Somma. Quantum algorithm for systems of linear equations with exponentially improved dependence on precision. *SIAM Journal on Computing*, 46(6):1920–1950, jan 2017.

[10] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization. *arXiv:1610.06546*, 2016.

[11] Yuval R. Sanders, Guang Hao Low, Artur Scherer, and Dominic W. Berry. Black-box quantum state preparation without arithmetic. *Phys. Rev. Lett.*, 122:020502, Jan 2019.

[12] Steven A. Cuccaro, Thomas G. Draper, Samuel A. Kutin, and David Petrie Moulton. A new quantum ripple-carry addition circuit. *arXiv:quant-ph/0410184*, 2004.

[13] Craig Gidney. Halving the cost of quantum addition. *Quantum*, 2:74, June 2018.

[14] Thomas Häner, Martin Roetteler, and Krysta M. Svore. Optimizing quantum circuits for arithmetic. *arXiv:1805.12445*, 2018.

A Separation of Out-of-time-ordered Correlator and Entanglement (will be on arXiv soon)

Aram W. Harrow[1] Linghang Kong [1] Zi-Wen Liu [2] Saeed Mehraban [3] Peter W. Shor [4]

[1] *MIT Center for Theoretical Physics*
[2] *Perimeter Institute for Theoretical Physics*
[3] *MIT Department of Electrical Engineering & Computer Science*
[4] *MIT Department of Mathematics*

Abstract. The out-of-time-ordered correlator (OTOC) and entanglement are two physically motivated and widely used probes of the "scrambling" of quantum information, which has drawn great interest recently in quantum gravity and many-body physics. By proving upper and lower bounds for OTOC saturation on graphs with bounded degree and a lower bound for entanglement on general graphs, we show that the time scales of scrambling as given by the growth of OTOC and entanglement entropy can be asymptotically separated in a random quantum circuit model defined on graphs with a tight bottleneck. Our result counters the intuition that a random quantum circuit mixes in time proportional to the diameter of the underlying graph of interactions. It also serves as a more rigorous justification for an argument of [1], that black holes may be very slow scramblers in terms of entanglement generation. Such observations may be of fundamental importance in the understanding of the black hole information problem. The bound we obtained for OTOC is interesting in its own right in that it generalized previous studies of OTOC on lattices to the geometries on graphs and proved it rigorously.

Keywords: scrambling, out-of-time-ordered correlator, entanglement, random circuits, black hole information problem, quantum chaos

1 Background

The "scrambling" of quantum information is a fundamental phenomenon, deeply connected to many important research topics in physics, such as black holes [2, 3, 4, 5] and many-body chaos [6, 7]. In recent years, a great amount of research effort has been devoted to the detection and characterization of scrambling. The so-called out-of-time-ordered correlator (OTOC) [8] is a commonly used measure of quantum chaos and scrambling. A variant based on commutators (also known as the OTO commutator) is given by

$$C(t) = \mathrm{Tr}\{[O_1(x,0), O_2(y,t)]^\dagger [O_1(x,0), O_2(y,t)]\}, \quad (1)$$

where $O_1(x,0)$ is an operator acting on site x, and $O_2(y,t)$ is a Heisenberg operator at time t that only acts on y at time 0, i.e. $O_2(y,t) = U^\dagger(t) O_2(y,0) U(t)$ where $U(t)$ is the unitary for the evolution from time 0 to t. Intuitively speaking, it characterizes parameters like sensitivity to initial conditions via the spread of local operators. The equilibration of OTOC is recently linked with the Hayden-Preskill decoding of Hawking radiation [2, 9]. Also notice that the scrambling phenomena exhibit a truly quantum nature—the state of the entire system remains pure during the unitary evolution (although it is effectively randomized), thus no information is really lost; the generation of global entanglement leads to the scrambling of initially localized quantum information spreads and hides it from observers that only have access to part of the system. This observation leads to another fundamental probe of a stronger form of scrambling, namely the entanglement between parts of the system [3, 10, 11, 12].

To understand and characterize the dynamical behaviors of scrambling systems, several explicit models have been proposed and investigated, such as the SYK model [13, 14]. Another leading approach is the random quantum circuit model [2, 11, 15, 16, 17], capturing the key kinematic feature of chaos that the dynamics of the system appears to be random, and the locality of physical interactions. In these previously studied scrambling models, the saturation of OTOC and that of entanglement are expected to occur at a similar time scale [15, 16, 11]. More generally, one could consider the dynamics of many small quantum systems (say qubits) connected according to some graph [18, 19], with random unitary gates being applied to each edge. Suppose that we apply gates in a random order such that on average each edge has one gate applied to it per unit time; e.g. we might imagine they are applied according to independent Poisson clocks on each edge. A natural conjecture here, which would be compatible with all previous results, is that the scrambling time is proportional to the diameter of the graph, i.e. the maximum distance between any two vertices in the graph. This would correspond to information traveling through the graph at a linear velocity and arguably is assumed implicitly by previous work that discusses butterfly velocities, entanglement velocities, etc. However, no proof exists, outside of the special case of Euclidean lattices in a fixed number of dimensions, that the OTOC time is linearly related to the graph diameter. Even for Euclidean lattices in more than one dimension, this result was only recently proven [20].

2 Results

Let G be a graph with V vertices and E edges. The model we study consists of a graph with a d-dimensional Hilbert space associated with each vertex of G. Each

edge has Haar-random unitary gates applied to qudits on its endpoints according to a Poisson clock with rate 1. The mixing times for OTOC and entanglement, $\tau_{\text{OTOC}}^{(x,y)}$ and $\tau_{\text{ent}}^{(A)}$, are defined as follows.

Definition 1 *$\tau_{\text{OTOC}}^{(x,y)}$ is defined to be the minimum amount of time needed for OTOC between vertices x and y to become $\Theta(1)$. Similarly, $\tau_{\text{ent}}^{(A)}$ is the minimum time needed for the von Neumann entropy of set of vertices A to become $\Theta(1)$ times its equilibrium value, that is, $\Theta(\min\{|A|, |B|\})$. Here B is the complement of A.*

1. Our first main result (Theorem 2) shows that for arbitrary graphs with sufficiently low degree, the OTOC time is upper bounded by a constant multiple of the graph diameter. Here by low degree, we mean that if quantum system is d dimensional and is connected to z neighbors, then we should have $d^2 \geq z$.

   Theorem 2 (OTOC upper bound) *Let G be a graph with V vertices and E edges, and suppose the degree for each vertex at most d^2, where d is the Hilbert space dimension for the qudit on each vertex. Then for any pair of vertices x and y, $\tau_{\text{OTOC}}^{(x,y)} = O(D(x,y))$ with probability $1 - e^{-\Theta(D(x,y))}$, where $D(x,y)$ is the distance between x and y. As a consequence the perfect binary tree has $\tau_{\text{OTOC}}^{(x,y)} = O(\ln V)$, where x and y are the farthest pair of vertices.*

2. We prove a converse to the above result showing that for low-degree graphs, the OTOC time is also *lower* bounded by a constant multiple of the graph diameter. Indeed we show a lower bound for graphs with any degree but our bounds become weaker as the graph degree increases.

3. We also give a heuristic argument that this low-degree requirement is necessary for the above two results by exhibiting two families of graphs where $d^2 \ll z$. In one family, the OTOC time appears to grow exponentially more rapidly than the diameter, and in another the OTOC time can grow arbitrarily more slowly than the diameter. These are described in Appendix C in main text.

4. By contrast with the OTOC time, we can use existing bounds on entanglement growth to exhibit graphs where the time to entangle two halves of the system is far larger than the OTOC time (see Theorem 3). The graphs with these properties include e.g. binary trees, which we explicitly analyze in this paper, and discretizations of hyperbolic space around black holes, originally proposed by [1], which are expected to exhibit similar behaviors (as argued below). In other words, we have established an asymptotic separation between the time scales of OTOC and entanglement saturation.

   Theorem 3 *For a general graph G with vertices partitioned into sets A and B, the expected entanglement saturation time is $\Omega(\frac{\min\{|A|,|B|\}}{C(A,B)})$, where $C(A,B)$ is the number of edges with one endpoint in A and one in B.*

3 Implications

1. *Scrambling in non-Euclidean geometries.* Existing work has studied OTOC and scrambling mostly on Euclidean lattices [15, 16, 21]. The general assumption is that after time t, a localized perturbation will affect everything within some ball of radius $v_{\text{butterfly}}t$. However, this has not been proved and previous work gave heuristic arguments for it that included uncontrolled approximations. We consider the random circuit models defined on general graphs. We find that if the local dimension is large relative to the graph degree then indeed there is a linear butterfly velocity. More precisely we find upper and lower bounds $v_{\text{inner}}, v_{\text{outer}}$ such that at time t a perturbation at a single site will affect a region that contains a ball of radius $v_{\text{inner}}t$ and is contained in a ball of radius $v_{\text{outer}}t$. In the regime where d is small relative to the graph degree then our proofs break down. We also find apparent counter-examples which suggest that linear butterfly velocity no longer holds in high-degree graphs. Some of these examples are not rigorously analyzed but we present a heuristic argument suggesting that the scrambling time for some families of graphs should grow more rapidly or more slowly than the diameter of the graphs.

2. *Black hole information scrambling.* Our results can be regarded as a more rigorous argument that fleshes out the idea of a recent paper by one of the authors [1], which concerns whether it is possible for the fast scrambling conjecture of black holes [3] to hold if one assumes that the causality structure of general relativity holds around a black hole, and if the medium by which the information is scrambled is Hawking radiation. In [1], the space around the black hole is divided into cells, each of which contains a constant number of bits of Hawking radiation. It then gives arguments for why the Hawking radiation is not adequate for fast scrambling if the entanglement definition of scrambling is used. The cell structure around the black hole looks like a patch of a cellulation of hyperbolic geometry, where the cells on the event horizon are the boundary of this patch. According to our results the scrambling timescales defined using entanglement and OTOC are different on this geometry. As we shall see, an even stronger separation is found for the much simpler tree graph, where the leaves lie on the event horizon.

   As for the Hayden-Preskill decoding task (to recover quantum information falling into the black hole from Hawking radiation) [2], Yoshida and

Kitaev recently proposed an explicit protocol [9] whose performance is roughly related to the (commutator form of) OTOC by

$$F \geq \Theta\left(\frac{1}{d_A^2(1-C(t))}\right),$$

where F is the decoding fidelity, and d_A is the Hilbert space dimension of input message. By simple calculations one can see that our results imply a possible time window in which the decoding could be achieved with high fidelity without substantial entanglement when the infalling quantum state has small ($O(1)$) size but the black hole is sufficiently large (note that it might still make more sense to consider multiple infalling qubits—for example, adding one bit to the black hole can only be done with a photon whose wavelength equals the size of the black hole, which means that it is already delocalized)

3. *Inequivalence of convergence to 2-designs in different measures.* The speed of convergence of a random circuit to a 2-design (distributions that approximately agree with the Haar measure up to the first two moments, which have found many important applications as an efficient approximation to Haar randomness, in quantum information [22]) has been the subject of a vast amount of research. In particular, [23, 20, 24, 25, 26] show that the speed of convergence depends on the geometry of interactions, and suggest that it should be proportional to the diameter of the graph of interactions. Note that 2-designs are very powerful measures of convergence, in the sense that a distribution being close to a 2-design implies that the distribution has mixed with respect to not only OTOC but also von Neumann and Rényi-2 entanglement entropy [11, 27], and other important signatures of information scrambling such as decoupling [28]. Past work has generally aimed to construct exact or approximate 2-designs using either random or structured circuits, and as a result has focused on proving that the 2-design conditions are met rather than looking for cases where they are not met. Our work gives several examples (see Section V in main text) where a random circuit approximates the OTOC but not entanglement properties of a 2-design, and therefore implies that a strong approximation of 2-designs (in terms of e.g. the frame operator [12]) may not be achieved in time proportional to diameter.

References

[1] Peter W. Shor. Scrambling time and causal structure of the photon sphere of a Schwarzschild black hole, 2018.

[2] Patrick Hayden and John Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 2007(09):120, 2007.

[3] Yasuhiro Sekino and Leonard Susskind. Fast scramblers. *Journal of High Energy Physics*, 2008(10):065, 2008.

[4] Juan Maldacena, Stephen H Shenker, and Douglas Stanford. A bound on chaos. *Journal of High Energy Physics*, 2016(8):106, 2016.

[5] Stephen H Shenker and Douglas Stanford. Black holes and the butterfly effect. *Journal of High Energy Physics*, 2014(3):67, 2014.

[6] Rahul Nandkishore and David A Huse. Many-body localization and thermalization in quantum statistical mechanics. *Annu. Rev. Condens. Matter Phys.*, 6(1):15–38, 2015.

[7] Arijeet Pal and David A Huse. Many-body localization phase transition. *Physical review b*, 82(17):174411, 2010.

[8] AI Larkin and Yu N Ovchinnikov. Quasiclassical method in the theory of superconductivity. *Sov Phys JETP*, 28(6):1200–1205, 1969.

[9] Beni Yoshida and Alexei Kitaev. Efficient decoding for the Hayden-Preskill protocol. *arXiv preprint arXiv:1710.03363*, 2017.

[10] Nima Lashkari, Douglas Stanford, Matthew Hastings, Tobias Osborne, and Patrick Hayden. Towards the fast scrambling conjecture. *Journal of High Energy Physics*, 2013(4):22, 2013.

[11] Pavan Hosur, Xiao-Liang Qi, Daniel A Roberts, and Beni Yoshida. Chaos in quantum channels. *Journal of High Energy Physics*, 2016(2):4, 2016.

[12] Zi-Wen Liu, Seth Lloyd, Elton Zhu, and Huangjun Zhu. Entanglement, quantum randomness, and complexity beyond scrambling. *Journal of High Energy Physics*, 2018(7):41, 2018.

[13] Subir Sachdev and Jinwu Ye. Gapless spin-fluid ground state in a random quantum heisenberg magnet. *Phys. Rev. Lett.*, 70:3339–3342, May 1993.

[14] Alexei Kitaev. `http://online.kitp.ucsb.edu/online/entangled15/kitaev/,http://online.kitp.ucsb.edu/online/entangled15/kitaev2/`, 2015.

[15] Adam Nahum, Sagar Vijay, and Jeongwan Haah. Operator spreading in random unitary circuits. *Physical Review X*, 8(2):021014, 2018.

[16] Adam Nahum, Jonathan Ruhman, Sagar Vijay, and Jeongwan Haah. Quantum entanglement growth under random unitary dynamics. *Physical Review X*, 7(3):031016, 2017.

[17] Vedika Khemani, Ashvin Vishwanath, and David A. Huse. Operator spreading and the emergence of dissipative hydrodynamics under unitary evolution with conservation laws. *Phys. Rev. X*, 8:031057, Sep 2018.

[18] Matthew B Hastings and Tohru Koma. Spectral gap and exponential decay of correlations. *Communications in mathematical physics*, 265(3):781–804, 2006.

[19] Bruno Nachtergaele and Robert Sims. Lieb-robinson bounds and the exponential clustering theorem. *Communications in mathematical physics*, 265(1):119–130, 2006.

[20] Aram Harrow and Saeed Mehraban. Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates, 2018.

[21] Cheryne Jonay, David A Huse, and Adam Nahum. Coarse-grained dynamics of operator and state entanglement. *arXiv preprint arXiv:1803.00089*, 2018.

[22] Richard A Low. Pseudo-randomness and learning in quantum computation. *arXiv preprint arXiv:1006.5227*, 2010.

[23] Aram W Harrow and Richard A Low. Random quantum circuits are approximate 2-designs. *Communications in Mathematical Physics*, 291(1):257–302, 2009.

[24] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. Local random quantum circuits are approximate polynomial-designs. *Communications in Mathematical Physics*, 346(2):397–434, 2016.

[25] Winton Brown and Omar Fawzi. Scrambling speed of random quantum circuits. *arXiv preprint arXiv:1210.6644*, 2012.

[26] Winton Brown and Omar Fawzi. Decoupling with random quantum circuits. *Communications in mathematical physics*, 340(3):867–900, 2015.

[27] Zi-Wen Liu, Seth Lloyd, Elton Yechao Zhu, and Huangjun Zhu. Generalized entanglement entropies of quantum designs. *Phys. Rev. Lett.*, 120:130502, Mar 2018.

[28] Oleg Szehr, Frédéric Dupuis, Marco Tomamichel, and Renato Renner. Decoupling with unitary approximate two-designs. *New Journal of Physics*, 15(5):053022, 2013.

Simulating dynamic quantum phase transitions in photonic quantum walks

Kunkun Wang[1 2] Xingze Qiu[3 4]
Lei Xiao[1 2] Xiang Zhan [1 2] Zhihao Bian [1 2] Wei Yi [3 4] * Peng Xue [1 2 5] †

[1] *Beijing Computational Science Research Center, Beijing 100084, China*
[2] *Department of Physics, Southeast University, Nanjing 211189, China*
[3] *Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China*
[4] *Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, CAS, Hefei 230026, China*
[5] *State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai 200062, China*

Abstract. Signaled by non-analyticities in the time evolution of physical observables, dynamic quantum phase transitions (DQPTs) emerge in quench dynamics of topological systems and possess an interesting geometric origin captured by dynamic topological order parameters (DTOPs). In this work, we report the experimental study of DQPTs using discrete-time quantum walks of single photons. We simulate quench dynamics between distinct Floquet topological phases using quantum-walk dynamics, and experimentally characterize DQPTs and the underlying DTOPs through interference-based measurements. The versatile photonic quantum-walk platform further allows us to experimentally investigate DQPTs for mixed states and in parity-time-symmetric non-unitary dynamics for the first time. Our experiment directly confirms the relation between DQPTs and DTOPs in quench dynamics of topological systems, and opens up the avenue of simulating emergent topological phenomena using discrete-time quantum-walk dynamics.

Keywords: dynamic quantum phase transitions, quantum quench, quantum walk, dynamic topological order parameters

1 Introduction

Proposed as temporal analogues to continuous phase transitions, dynamic quantum phase transitions (DQPTs) are associated with non-analyticities in the time evolution of physical observables. For continuous phase transitions in equilibrium systems, the free energy becomes non-analytic at critical points, associated with complex-partition-function zeros known as Fisher or Lee-Yang zeros. Analogously, DQPT occurs as a consequence of the emergence of dynamic Fisher zeros, where the Loschmidt amplitude $G(t) = \langle\psi(0)|\psi(t)\rangle$, the analogue of the partition function, vanishes at critical times. This leads to non-analyticities in the rate function $g(t) = -1/N \ln|G(t)|^2$, which serves as the dynamic free energy. Here $|\psi(t)\rangle$ is the time-evolved state, and N is the overall degrees of freedom of the system. Whereas it is still unclear to what extent key concepts of continuous phase transitions can be extended to describe DQPTs, an intriguing discovery is the geometric origin of DQPTs, captured by dynamic topological order parameters (DTOPs), which suggests the intimate connection between DQPTs and emergent topological phenomena in dynamic processes.

A relevant dynamic process here is the quench of topological systems, where the ground state $|\psi^{\mathrm{i}}\rangle$ of the initial Hamiltonian H^{i} evolves under the final Hamiltonian H^{f}. Specifically, for quench dynamics of one-dimensional topological systems, topological DQPTs necessarily exist when ground states of H^{i} and H^{f} belong with distinct topological phases. These topological DQPTs provide a crucial link between static topological phases and dynamic topological phenomena.

In this work, we report the experimental simulation of topological DQPTs using discrete-time quantum walks (QWs) of single photons in one dimension. We map single-photon QWs to many-body quench dynamics between Floquet topological phases of fermions, where topological DQPTs naturally emerge. Specifically, we probe inner products of the initial and time-evolved states of the single-photon dynamics via inference-based measurements, from which we construct quantities such as the rate function and DTOPs for the many-body dynamics. An advantage of photonic QW dynamics lies in the relative ease of introducing decoherence and loss, which further allows us to experimentally investigate DQPTs for mixed states and in non-unitary dynamics for the first time.

2 Simulating quench between topological phases:

We study DQPTs in quench dynamics using discrete-time QWs on a one-dimensional homogeneous lattice L ($L \in \mathbb{Z}$), where we use polarization states of single photons $\{|H\rangle, |V\rangle\}$ to represent coin states and spatial modes to encode walker states. The QW dynamics is governed by the Floquet operator [1, 2]

$$\tilde{U} = \gamma C(\theta_1/2) SC(\theta_2/2) MC(\theta_2/2) SC(\theta_1/2), \quad (1)$$

where $M = \mathbb{1}_w \otimes \left(|+\rangle\langle+| + \sqrt{1-l}\,|-\rangle\langle-|\right)$ is the non-unitary elements with $\{|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}\}$ at each

*wyiz@ustc.edu.cn
†gnep.eux@gmail.com

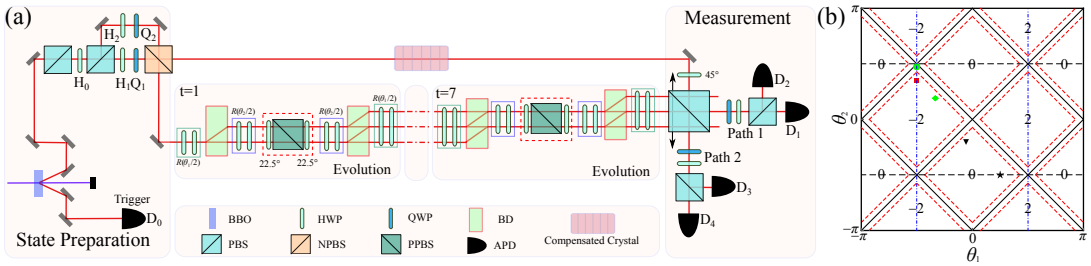


Figure 1: (a) Experimental setup for the simulation of DQPTs using QWs. Pairs of single photons are generated via type-I spontaneous parametric down conversion (SPDC) using a non-linear β-Barium-Borate (BBO) crystal. One photon serves as a trigger and the other signal photon is prepared in an mixed polarization state using polarizing beam splitters (PBSs), wave plates (WPs) and a non-polarizing beam splitter (NPBS). Coin rotations and conditional translations are realized by two half-wave plates (HWPs) and a beam displacer (BD), respectively. For non-unitary QWs, a sandwich-type HWP-PPBS-HWP setup is inserted to introduce the partial measurement, where PPBS is an abbreviation for partially polarizing beam splitters. Avalanche photodiodes (APDs) detect the signal and heralding photons. (b) Phase diagram for QWs governed by Floquet operators U and $\tilde{U}$, labeled by the winding number ν as a function of coin parameters (θ_1, θ_2).

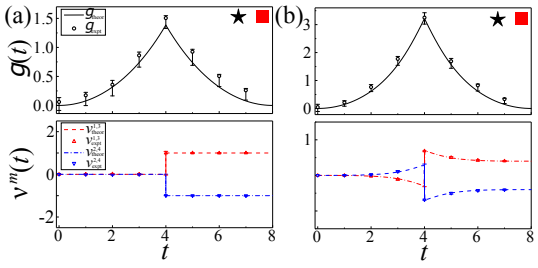


Figure 2: Rate function (upper layer) and $\nu^m(t)$ (lower layer) as functions of time steps with a pure initial state (a) and a mixed state with $p = 0.7$ (b). Error bars are derived from simulations where we consider all the systematic inaccuracies of the experiment.

time step, and $\gamma = (1-l)^{-1/4}$. Here, the coin operator $C(\theta)$ rotates the single-photon polarization by θ about the y-axis. The shift operator S moves the walker in $|H\rangle$ ($|V\rangle$) to the left (right) by one lattice site. In our experiment, we performed the unitary dynamic QW of U with $l = 0$ and also the non-unitary dynamic QW of $\tilde{U}$ with $l = 0.36$.

U have non-trivial topological properties, as the corresponding effective Hamiltonian H_{eff} can have topologically non-trivial Floquet bands characterized by finite winding numbers. Here H_{eff} is defined through $U = e^{-iH_{\text{eff}}}$. As illustrated in Fig. 1(b), winding numbers associated with these Floquet bands are tunable through the coin parameters (θ_1, θ_2).

Crucially, the non-unitary $\tilde{U}$ also possess $\mathcal{PT}$ symmetry, therefore its quasienergy spectra can be entirely real in the $\mathcal{PT}$-symmetry-unbroken regime, in contrast to the regime with spontaneously broken $\mathcal{PT}$ symmetry. The boundary between regimes with unbroken and broken $\mathcal{PT}$ symmetry for is plotted in Fig. 1(b) as red dashed lines, with $\mathcal{PT}$-symmetry-broken regimes surrounding topological phase boundaries.

We initialize the walker photon at $x = 0$ (x is the

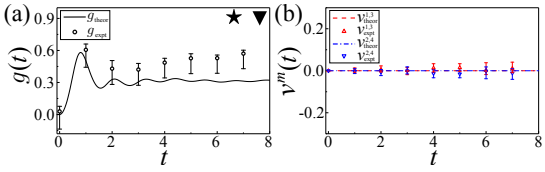


Figure 3: (a) Rate function and (b) $\nu^m(t)$. The QW is governed by the final Floquet operator with the same winding number as that of the initial state.

site index), with its coin state given by the density matrix $\rho_0 = p\,|\psi^{\text{i}}_-\rangle\langle\psi^{\text{i}}_-| + (1-p)\,|\psi^{\text{i}}_+\rangle\langle\psi^{\text{i}}_+|$, where $|\psi^{\text{i}}_\pm\rangle = (|H\rangle \mp i\,|V\rangle)/\sqrt{2}$. The initial state is therefore a pure state when $p = \{0, 1\}$, and a mixed state otherwise. Importantly, $|x = 0\rangle \otimes |\psi^{\text{i}}_\pm\rangle$ are eigenstates of U^{i} with the coin parameters $(\theta^{\text{i}}_1 = \pi/4, \theta^{\text{i}}_2 = -\pi/2)$. We then implement QWs governed by U^{f} with coin parameters $(\theta^{\text{f}}_1, \theta^{\text{f}}_2)$.

As the time evolution in each k-sector is governed by U^{f}_k, the Fourier component of U^{f}, we construct the Loschmidt amplitude $G(k,t)$ from its Fourier component $\bar{P}(p,x,t)$ according to

$$G(k,t) := \text{Tr}\left[\rho_0 \left(U^{\text{f}}_k\right)^t\right] = \sum_x \text{e}^{-ikx}\bar{P}(p,x,t), \qquad (2)$$

where $\bar{P}(p,x,t) = p\langle\psi^{\text{i}}_-|\psi_-(x,t)\rangle + (1-p)\langle\psi^{\text{i}}_+|\psi_+(x,t)\rangle$, and $|\psi_\pm(x,t)\rangle = \sum_k e^{ikx}\left(U^{\text{f}}_k\right)^t|\psi^{\text{i}}_\pm\rangle$. Experimentally, $\bar{P}(p,x,t)$ is measured by performing interference-based measurements at the t-th step.

We then construct the rate function according to $g(t) = -\sum_{k\in 1\text{BZ}} \ln|G(k,t)|^2$, where the overall Loschmidt amplitude of the dynamics $G(t)$ takes the form $G(t) = \prod_{k\in 1\text{BZ}} G(k,t)$. Hence by construction, $g(t)$ is the rate function of a quench between many-body Floquet topological phases of fermions, where the initial state is a direct product of single-particle density matrices ρ_0 at different quasi-momenta in the first Brillouine zone (1BZ).

From the measured $G(k,t)$, we further calculate

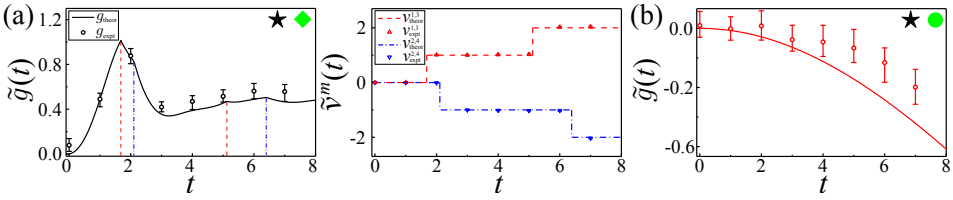


Figure 4: (a) Rate function and $\tilde{\nu}^m(t)$ with a loss parameter $l = 0.36$. (b) Rate function of the QW governed by the final non-unitary Floquet operator in parity-time ($\mathcal{PT}$) symmetry broken region.

DTOPs characterizing DQPTs, which are defined as

$$\nu^m(t) = \frac{1}{2\pi}\int_{k_m}^{k_{m+1}} \frac{\partial \phi_k^G(t)}{\partial k} \mathrm{d}k, \tag{3}$$

where the Pancharatnam geometric phase $\phi_k^G(t) = \phi_k(t) - \phi_k^{\mathrm{dyn}}(t)$. Here $\phi_k(t)$ is defined through $G(k,t) = |G(k,t)|e^{i\phi_k(t)}$, and $\phi_k^{\mathrm{dyn}}(t)$ is the dynamic phase. k_m ($m = 1, 2, ...$) are fixed points of the dynamics, where the corresponding density matrices do not evolve in time and $\phi_k^G(t)$ vanishes at all times. $\nu^m(t)$ therefore characterizes the $S^1 \to S^1$ mapping from the momentum submanifold between k_m and k_{m+1} to $e^{i\phi_k^G(t)}$.

Actually, DTOP can only change value at a topological DQPT with $G(k_c, t_c) = 0$, where the geometric phase becomes ill-defined. Here, k_c lies between adjacent fixed points and $t_c = (2n-1)t_0$ ($n \in \mathbb{N}$), with the critical time scale $t_0 = \pi/(2E_{k_c}^{\mathrm{f}})$ and $\pm E_k^{\mathrm{f}}$ is the quasienergy of U_k^{f}. While topological DQPTs only occur for quenches between distinct topological phases, abrupt jumps in $\nu^m(t)$ can also serve as signals for the dynamic characterization of equilibrium topological phases.

3 Results

We first study DQPTs for pure states in unitary dynamics. We initialize photons in the coin state $|\psi_-^{\mathrm{i}}\rangle$ at $x = 0$. The photons are then subject to unitary time evolutions governed by the Floquet operator U^{f} with $(\theta_1^{\mathrm{f}} = -\pi/2, \theta_2^{\mathrm{f}} = 3\pi/8)$, which simulates a quench between Floquet topological phases with $\nu^{\mathrm{i}} = 0$ and $\nu^{\mathrm{f}} = -2$. Here, the fixed points $k_{1,2,3,4} = \{-\pi, -\pi/2, 0, \pi/2\}$, and $k_c = \{\pm\pi/4, \pm 3\pi/4\}$. Note U_k^{f} has a discrete symmetry $U_k^{\mathrm{f}} = U_{k+\pi}^{\mathrm{f}}$ in addition to the time-reversal symmetry. Under these symmetries, $E_{k_c}^{\mathrm{f}}$ are degenerate and there is only one critical time scale $t_0 = 4$. In Fig. 2(a), we show the rate function, which becomes non-analytic at the first critical time $t_c = t_0$. Whereas it is difficult to directly identify non-analyticities of $g(t)$ in discrete-time dynamics, the measured $g(t)$ peaks at critical times and DQPTs are unambiguously revealed by jumps in the quantized DTOP across t_c. Due to the symmetry of U_k^{f}, we have $\nu^{1,3}(t) = -\nu^{2,4}(t)$, where $\nu^4(t)$ is integrated in the range $(\pi/2, \pi)$.

In the second case study, we initialize photons at $x = 0$ and in a mixed coin state characterized by ρ_0 with $p = 0.7$. The QW is governed by U^{f} with $(\theta_1^{\mathrm{f}} = -\pi/2, \theta_2^{\mathrm{f}} = 3\pi/8)$. As shown in Fig. 2(b), while the occurrence of DQPTs are still signaled by non-analyticities in the rate functions, DTOPs are typically not quantized. This is because $\phi_k^G(t)$ do not vanish at k_m at all times, such that $e^{i\phi_k^G}$ no longer forms a closed S^1 manifold between k_m and k_{m+1}. Consequently, $\nu^m(t)$ is no longer the winding number characterizing such a map.

For comparison, we choose U^{f} with $(\theta_1^{\mathrm{f}} = -\pi/16, \theta_2^{\mathrm{f}} = -3\pi/16)$ and study the case where the quench dynamics is between phases with $\nu^{\mathrm{i}} = 0$ and $\nu^{\mathrm{f}} = 0$. As shown in Fig. 3, the rate function is smooth in time and $\nu^m(t)$ remains zero, indicating the absence of DQPTs. Here $k_m = \{0, \pm\pi/2, \pi\}$.

Similar to the unitary case, we initialize photons in the state $|x = 0\rangle \otimes |\tilde{\psi}_-^{\mathrm{i}}\rangle$, with the corresponding $\tilde{U}^{\mathrm{i}}$ in the $\mathcal{PT}$-symmetry-unbroken regime with $\nu^{\mathrm{i}} = 0$ and $|x = 0\rangle \otimes |\tilde{\psi}_-^{\mathrm{i}}\rangle$ the ground state of $\tilde{U}^{\mathrm{i}}$. The walker is evolved under the final non-unitary Floquet operator $\tilde{U}^{\mathrm{f}}$ with $(\theta_1^{\mathrm{f}} = -\pi/3, \theta_2^{\mathrm{f}} = \pi/5)$, which is in the $\mathcal{PT}$-symmetry-unbroken regime with $\nu^{\mathrm{f}} = -2$. The Loschmidt amplitude, the rate function $\tilde{g}(t)$, and the DTOP $\tilde{\nu}^m(t)$ for non-unitary dynamics can be constructed similarly to the unitary case. As illustrated in Fig. 4(a), non-analyticities in the rate function have two distinct time scales, which correspond to two different DTOPs, both quantized and demonstrating abrupt jumps at odd multiples of the corresponding critical time scale.

The emergence of two critical time scales is due to the breaking of time-reversal symmetry of the non-unitary dynamics. In this case, whereas fixed points still exist when U^{i} and U^{f} are in the $\mathcal{PT}$-symmetry-unbroken regime and have different winding numbers, they are no longer located at high-symmetry points.

Finally, we study the case when the final non-unitary Floquet operator is in the $\mathcal{PT}$-symmetry-broken regime. The resulting rate function is shown in Fig. 4(b), where no DQPTs can be identified. As fixed points are also absent in the dynamics, DTOPs cannot be defined in this case.

References

[1] K. Wang, X. Qiu, L. Xiao, X. Zhan, Z. Bian, W. Yi, and P. Xue Simulating Dynamic Quantum Phase Transitions in Photonic Quantum Walks. *Phys. Rev. Lett.*, **122**, 020501, 2019.

[2] X. Qiu, T.-S. Deng, Y. Hu, P. Xue, and W. Yi Fixed points and emergent topological phenomena in a parity-timesymmetric quantum quench. arXiv:1806.10268.

An approximation algorithm for the MAX-2-Local Hamiltonian problem

Sean Hallgren[1] * † Eunou Lee[1] ‡

[1] *Department of Computer Science and Engineering, Pennsylvania State University*

Keywords: Approximation, randomized rounding, MAX-CSP, Grothendieck inequality, product state

We present a classical approximation algorithm for the MAX-2-Local Hamiltonian Problem. This problem generalizes MAX-2-CSPs, so is NP-hard. It is an optimization version of the QMA-complete Local Hamiltonian problem in quantum computing, with the additional assumption that the local terms are complex positive semidefinite. We work in the product state space, and extend Goemans and Williamson's framework for approximating MAX-2-CSPs. The analysis for rounding does not naturally extend because we round to a set of normalized vectors, not boolean numbers, and we use Grothendieck inequalities for different special cases. For general MAX-2-Local Hamiltonions, we achieve an approximation ratio of 0.564 relative to the best product state. In general, the best product state might be worse than the best entangled state by a factor of two, so our overall approximation ratio is 0.282. This is the first example of an approximation algorithm beating the random quantum assignment ratio of 0.25 by a constant factor.

1 Introduction

Designing approximation algorithms is one of the main tools to deal with computationally hard problems. The maximum constraint satisfaction problems have been especially well-studied with regards to approximation algorithms (see [MM17] for a survey.) The boolean MAX-2-CSPs consider a problem where we have n boolean variables $x_1, x_2, \ldots, x_n \in \{0,1\}$, a set of edges E between x_i's, and functions $f_{ij} : \{0,1\}^2 \to \{0,1\}$ on x_i, x_j for $(i,j) \in E$. The question is to compute the quantity $\mathrm{OPT}_{\mathrm{CSP}} = \max_{x_1,\ldots,x_n} \sum_{(i,j)\in E} f(x_i, x_j)$. This problem is NP-hard. It is possible, however, to find an assignment such that $\sum_{(i,j)\in E} f(x_i, x_j) \geq \alpha \mathrm{OPT}_{\mathrm{CSP}}$ for some $\alpha \in [0,1]$. The number α is called the *approximation ratio*, and the best approximation ratio we have for the MAX-2-CSP is 0.874 [LLZ02]. A special case of MAX-2-CSP is where the Hamming weight of f_{ij}, which is $r = \sum_{(x_i,x_j)\in\{0,1\}^2} f_{ij}(x_i, x_j)$, is constant across all $(i,j) \in E$. Then the best approximation ratios depend on the value r. When $r = 3$, as in MAX-2-SAT, the best ratio is 0.94 [LLZ02]. When $r = 2$, as in MAX-2-LIN or MAX-CUT, the best ratio is 0.878 [GW95]. When $r = 1$, as in MAX-2-AND or the MAX-DI-CUT, the best ratio is 0.874 [LLZ02].

In this paper we consider the quantum generalization MAX-2-local Hamiltonians (MAX-2-LH) on qubits, defined in [GK11] (more generally for k-local and qudits). In this problem a set of 2-local Hamiltonians $\{H_{pq} : 1 \leq p, q, \leq n\}$ is given, where each term is a 2-local positive semidefinite matrix of norm at most 1. Each term H_{pq} is non-trivial on the qubits p, q and trivial on the rest of the qubits. More formally, $H_{pq} = H'_{pq} \otimes I_{[n]\setminus\{p,q\}}$, where H'_{pq} is a Hamiltonian on the qubits p, q and $I_{[n]\setminus\{p,q\}}$ is the identity matrix on the rest of the qubits. The goal of MAX-2-LH is to approximate the maximum eigenvalue of $H = \sum_{pq} H_{pq}$, that is, $\mathrm{OPT} := \max_{|\phi\rangle} \langle\phi|H|\phi\rangle$.

The MAX-2-CSP can be encoded into the problem of finding the maximum eigenvalue: given a 2-CSP instance $\sum_{i,j\in E} f_{i,j}(x_i, x_j)$, consider the 2-local Hamiltonian $\sum_{i,j\in E} P_{ij}$, where P_{ij} is a projector that supports $|x_i x_j\rangle$ on the qubits i, j if and only if $f_{ij}(x_i, x_j) = 1$. The computational basis state that realizes the maximum of the MAX-2-CSP has the same eigenvalue on the Hamiltonian, and there is no better quantum assignment because the computational basis diagonalizes P_{ij}. Therefore, we can say MAX-2-LH is a quantum generalization of MAX-2-CSP. In fact, computing OPT up to inverse polynomial error is QMA-hard [KKR06].

For classical computations it is easier to work with product states because they have polynomial size representations. Therefore we will be focused on approximating the quantity $\mathrm{OPT}_{\mathrm{prod}} = \max_{|\phi_1\rangle,\ldots,|\phi_n\rangle} \langle\phi_1| \ldots \langle\phi_n|H|\phi_1\rangle \ldots |\phi_n\rangle$, which is the highest energy achievable by a product state. The gap between OPT and $\mathrm{OPT}_{\mathrm{prod}}$ is how much better entangled states do, and [GK11] bounded the gap by $\mathrm{OPT}_{\mathrm{prod}}/\mathrm{OPT} \geq 1/2$. $\mathrm{OPT}_{\mathrm{prod}}$ can be realized by a product state, so verification of $\mathrm{OPT}_{\mathrm{prod}}$ is in NP.

We give the first approximation algorithm for MAX-2-LH with general interaction graphs. Our algorithm outputs a product state that achieves the energy 0.564 of the highest energy achievable by a product state ($0.564 \cdot \mathrm{OPT}_{\mathrm{prod}}$), and 0.282 of the highest energy achievable by an arbitrary entangled state ($0.282 \cdot \mathrm{OPT}$).

We analyze the cases when each local terms are projectors. As in the classical case, we divide the cases with the rank of the projectors. When the rank $r = 3$, we get the energy $0.878 \cdot \mathrm{OPT}_{\mathrm{prod}}$. Since we know that $\mathrm{OPT}_{\mathrm{prod}}/\mathrm{OPT} \geq 1/2$, we achieve $0.439 \cdot \mathrm{OPT}$. When the rank $r = 1$, we get a varying ratio depending on how entangled the projectors are. We get the approximation

*hallgren@cse.psu.edu

†Partially supported by National Science Foundation awards CCF-1618287 and CNS-1617802, and by a Vannevar Bush Faculty Fellowship from the US Department of Defense.

‡eul153@psu.edu

ratio 0.40 when the projector is a product of 1 qubit projectors, and in the case with general rank 1 projector local terms, we get the ratio 0.282. Since every 2-local Hamiltonians with PSD local terms can be expressed as a weighted summation of rank 1 projectors, we can extend the analysis to MAX-2-LH yielding the ratio 0.282.

In related work, Bansal, Bravyi, and Terhal [BBT07] proved that a PTAS (an algorithm that runs in polynomial time in problem size and $1/\epsilon$ where ϵ is arbitrary small approximation ratio) exists for Quantum Ising Spin Glass with planar graph with bounded degree. The only results on general interaction graphs are by Gharibian, Parekh, and Ryan-Anderson [GPRA17] and by Bravyi, Gosset, König, and Temme [BGKT19]. [GPRA17] considers a family of physically motivated Hamiltonians, namely $H = \sum_{(p,q)\in E} w_{pq} H_{pq}$ for $w_{pq} \geq 0$, where $H_{pq} = I - \alpha X_p \otimes X_q - \beta Y_p \otimes Y_q - \gamma Z_p \otimes Z_q$, for $\alpha, \beta, \gamma \in \{0, 1\}$. They get approximation ratios $2/(1 + \alpha + \beta + \gamma)$ when $\alpha + \beta + \gamma \geq 2$, and 0.878 otherwise. Furthermore, they show that their ratios are tight in the product state space. [BGKT19] considers traceless 2-local Hamiltonians. They give an algorithm that outputs a seperable state with expected energy OPT $/O(\log n)$, where OPT is the maximum eigenvalue of input Hamiltonian. A limitation of previous works is that they do not give equivalent results to that of classical MAX-2-CSP approximation algorithms, which yield constant approximation ratios on MAX-2-CSP instances.

In terms of techniques, we follow the framework that was first introduced by Goemans and Williamson. We first formulate the problem as an equivalent optimization problem in the real numbers. Then we relax the optimization problem to an SDP. The optimal value of the SDP will be at least the value of the original problem, because the solution space is bigger. Then we randomly round the solution in the bigger space down to original solution space. Analyzing the randomized rounding is considerably more complicated than in the classical cases, because we need to round the solutions to continuous multi-dimensional space, whereas the solution space is the boolean space in the classical cases. Fortunately, the rounding was analyzed in a more general setting in terms of Grothendieck inequality with a PSD matrix [BdOFV10]. It is natural to consider using SDP for the problem, because every but few approximation algorithms for classical MAX-2-CSP use SDP solutions to round [GW95, Zwi00, MM01, LLZ02]. Also [GPRA17] uses SDP to approximate the MAX-2-LH problems. The SDP formulations of [GPRA17, BGKT19] and ours are different. An advantage of the formulation in [GPRA17, BGKT19] is that the optimal value of the program is OPT itself, whereas the optimal value of our program is OPT_{prod}. An advantage of our formulation is that it is simple to round and analyze, which makes it possible to use for general MAX-2-LHs with positive semidefinite local terms. We limit our analysis to positive semidefinite (PSD) local terms for 3 reasons: first, it is analogous to the classical CSP case, because f_{ij} is always non-negative in classical case. Second, without loss of generality, every MAX-2-LH can be turned into MAX-2-LH with PSD local terms by adding a multiple of identity matrix. Third, if local terms are not PSD, it is possible that the highest eigenvalue is negative. Then approximation ratio is no longer well-defined.

References

[BBT07] Nikhil Bansal, Sergey Bravyi, and Barbara M. Terhal. Classical approximation schemes for the ground-state energy of quantum and classical Ising spin Hamiltonians on planar graphs. Quant. Inf. Comp. Vol. 9, No.8, p. 0701 (2009), 2007. arXiv:0705.1115v4.

[BdOFV10] Jop Briët, Fernando Mário de Oliveira Filho, and Frank Vallentin. The positive semidefinite Grothendieck problem with rank constraint. In *Automata, Languages and Programming*, pages 31–42, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[BGKT19] Sergey Bravyi, David Gosset, Robert Koïig, and Kristan Temme. Approximation algorithms for quantum many-body problems. *Journal of Mathematical Physics*, 60(3):032203, 2019.

[GK11] Sevag Gharibian and Julia Kempe. Approximation algorithms for QMA-complete problems. SIAM Journal on Computing 41(4): 1028-1050, 2012, 2011. arXiv:1101.3884v1.

[GPRA17] Sevag Gharibian, Ojas D. Parekh, and Ciaran Ryan-Anderson. Approximate constraint satisfaction in the quantum setting. 2017.

[GW95] Michel X. Goemans and David P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *J. ACM*, 42(6):1115–1145, November 1995.

[KKR06] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local Hamiltonian Problem. *SIAM J. Comput.*, 35(5):1070–1097, May 2006.

[LLZ02] Michael Lewin, Dror Livnat, and Uri Zwick. Improved rounding techniques for the MAX 2-SAT and MAX DI-CUT problems. In *Integer Programming and Combinatorial Optimization*, pages 67–82, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[MM01] Shiro Matuura and Tomomi Matsui. 0.863-approximation algorithm for MAX DI-CUT. In *Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques*, pages 138–146,

Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[MM17] Konstantin Makarychev and Yury Makarychev. Approximation algorithms for CSPs. In *The Constraint Satisfaction Problem: Complexity and Approximability*, volume 7 of *Dagstuhl Follow-Ups*, pages 287–325. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2017.

[Zwi00] Uri Zwick. Analyzing the MAX 2-SAT and MAX DI-CUT approximation algorithms of Feige and Goemans, 2000.

Extended abstract: Nonuniform photonic losses and classical simulation of linear optics

Daniel J. Brod and Michał Oszmaniec

Multi-photon experiments in large linear-optical networks are an attractive platform for demonstrating quantum computational supremacy via the paradigm of Boson Sampling. Unfortunately, large linear-optical networks typically suffer from photonic losses which can undermine the computational hardness of the process. Here we present a comprehensive study of the impact of non-uniform, i.e. path-dependent, losses on the computational complexity of linear-optical processes. Our main result is that, if we assume each beam-splitter in a network induces some loss probability, non-uniform network designs cannot circumvent efficient classical simulation of the corresponding optical processes. This solves an open problem from previous work that assumed losses occurred uniformly.

I. INTRODUCTION

The paradigm of quantum computational advantage, or "quantum supremacy", has been seen in the last few years as a promising route towards demonstrating that quantum computers are more powerful than their classical counterparts [1]. Although systems within this model are not expected to be universal for quantum computation, and indeed neither to perform explicitly useful tasks, they allow us to test quantum mechanics in the limit of high computational complexity. The pursuit of a near-term demonstration of quantum advantage is also aligned with the overarching goals of the field of quantum computing, as it pushes the development of technologies that will undoubtedly be necessary for scalable universal quantum computers and allows us to better understand the effects of real-world imperfections in intermediate-size quantum systems.

One particular candidate for demonstrating quantum advantage is nonadaptive linear optics, or BosonSampling [2]. Besides being an elegant physically-motivated computational model and, arguably, the first proposal of quantum supremacy as we understand it today, BosonSampling also benefits from the technology and expertise that has been independently developed in the quantum optics community in the last few decades. However, as elegant as the theoretical model is, there are many technological and theoretical challenges in realizing it in practice. Several sources of experimental imperfections affect linear-optical systems, and it is essential to understand which can be mitigated and which might degrade the computational power of the model.

Relation to previous works— Much work has been done to investigate the boundary between classical simulability and quantum advantage in linear optics under different models of noise and experimental imperfections. Losses in particular have received the most attention. In [3] it was shown that n-photon BosonSampling retains its computational power as long as only a constant number of photons are lost (or if the loss probability per-photon scales inversely with the number of photons). Recently, several papers analyzed lossy BosonSampling from the other extreme, showing it becomes classically simulable when less than $\sqrt{n}$ photons are left [4, 5] for arbitrary interferometers, or even when a suitably high *constant fraction* of the photons is lost for typical Haar-random interferometers [6]. The complexity of BosonSampling has also been investigated under the effect of fabrication noise in the linear-optical components [7, 8], losses combined with dark counts [9], and general Gaussian noise in the experimental data [10].

In [5] we investigated the issue of linear-optical losses from the point of view of classical simulation. Our main result stated that, when less than $\sqrt{n}$ out of n photons are left, it is possible to approximate a lossy BosonSampling state by a state of distinguishable photons, which is known to be classically simulable. Furthermore, the error of the approximation (measured in total variation distance) decreases for larger experiment sizes. Interestingly, this approximation is done at the level of the *input* state to a linear-optical network, and so holds for arbitrary linear-optical experiments (it could, in principle, be much smaller for typical or specific interferometers).

This result assumes that losses happen at the input to the network. This is a very common assumption in the linear optics literature because mode-independent losses commute with linear-optics and so can, in fact, be taken to happen at the input. However this is not always realistic, as it is possible to build highly unbalanced networks where losses are very mode-dependent [11]. Motivated by this, in [5] we also formalized this standard assumption and showed under which conditions losses can in fact be "commuted" to the input of a network. Specifically we showed it is always possible to commute s layers of losses to the input of a network, where s is the smallest number of beam splitters in any path connecting an input and an output mode. This strengthened the previous results where this assumption is made informally [3, 4, 9, 12].

II. INFORMAL DESCRIPTION OF OBTAINED RESULTS

In this work we extend our previous results contained in [5] in different directions, with new results that might also be of independent interest to the more general quan-

tum optics community, as follows.

Result 1: Extracting nonuniform losses from the network. We improve the procedure of [5] that allows us to commute losses to the input of a network. For simplicity, we make the following assumption regarding losses in linear optics. We assume that all losses happen within the network and are located at the beam splitters, and that every beam splitter carries the same amount of loss. Although losses due to imperfect sources and detectors are experimentally important, they are in principle constant, whereas losses due to linear-optical elements dictate how overall transmissivity of the network scales as the experiments become more complex (in particular, as the depth of the networks increase). Furthermore, the geometry of a network is the main source of nonuniformity of losses which we wish to study. Experimentally, beam splitter losses are also relevant e.g. in integrated photonic devices, since waveguide bends required to build the directional couplers that implement beam splitters can cause photons to leave in unguided modes [13]. We thus represent a lossy linear-optical as in Fig. 1(a).

The main figure of merit for the result of [5] is the *length* of input-output paths inside a network, measured in the number of beam splitters a photon has to traverse along that path. The previous result stated that, if the shortest input-output path inside a network has length s, we can rewrite the network in such a way that it has s layers of mode-independent losses at the input. However this is not particularly useful to describe an unbalanced network such as that of Reck *et al* [11], depicted in Fig. 1(a), as in that case we can only pull out one layer of uniform losses.

Our new result improves on this by showing how to extract *nonuniform* loss layers. **More specifically, let s_i be the shortest path between input i and any output within some network. We show how to write an equivalent network that is preceded by a round of losses where input i suffers the effect of s_i consecutive loss elements**. The formal statement of this result can be found in Theorem 1 of the appended technical notes. Our proof is efficient and constructive, and works for general networks. The final result is illustrated in Fig. 1(b). This gives a more efficient description of the network where asymmetry is taken into account, and which we use to prove result 4 described later.

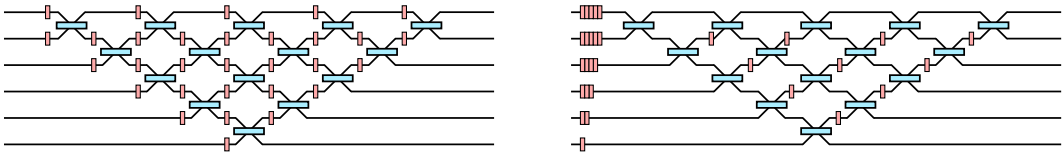
Result 2: Classical simulation of BosonSampling with highly concentrated input states. It is well known that BosonSampling is efficiently classically simulable if all n photons are initialized in a single mode, i.e., we have input state $|n, 0, 0, \ldots, 0\rangle$. This follows from the fact that the permanent of a matrix of n repeated columns can be computed trivially in linear time, or alternatively from the fact that if all photons are initialized in the same mode they behave as distinguishable particles. In our work we prove a stronger version of this statement by giving an efficient classical simulation for BosonSampling when input photons are sufficiently concentrated on a few modes.

We combine techniques from [14, 15] to construct an efficient classical simulation of (non-lossy) BosonSampling for two types of input. The first (type A) is when we have n photons concentrated in a constant number of input modes. The second (type B) is when all but $\log n$ photons are concentrated on a single input mode, while an additional $\log n$ modes contain one photon each. We provide an algorithm for strong simulation (i.e. computing probabilities) by showing that an expansion for the permanent function described in [14] can be computed efficiently in these two regimes (the authors of [14] pointed out this fact for inputs of type A, but not type B). We then use this simulation to adapt a result of [15] for weak classical simulation (i.e. producing samples from the correct distribution) of BosonSampling with collision inputs, showing that it is also efficient for inputs of types A and B. Our adaptation of the result of [15] is also based on a physical description of the state (via first quantization) rather than combinatorial considerations, and we believe it could make the original result more transparent for researchers with a stronger physics background. The precise formulation of this result can be found in Theorem 2 of the appended technical notes.

Besides giving us a new understanding of the regimes where efficient classical simulability of BosonSampling is possible, and ruling out attempts at demonstrating a quantum advantage with highly concentrated bosonic input states, this result also serves as a nontrivial stepping stone towards result 3 described below.

Result 3: Classical simulation of lossy BosonSampling with lossless modes. We improve the classical simulation algorithm of [5] by allowing the lossy BosonSampling instance to be coupled to some lossless modes. **Concretely, suppose that n photons pass through a lossy channel in such a way that less than $\sqrt{n}$ survive, and are then combined with up to $\log n$ photons input in modes that have perfect transmission. We show that the simulation of [5] works for this setting as well.** The formulation of this result can be found in Theorem 3 of the appended technical notes.

We now sketch the proof of the above result. The classical simulation strategy from [5] was based on approximating a lossy bosonic state ρ by the best particle-separable state, i.e., the closest state where particles effectively behave as distinguishable. In [5] we obtained the closest particle-separable state σ to our target state and computed the trace distance between them. We showed that this trace distance decreases with n if losses are large enough such that less than $\sqrt{n}$ photons survive on average. It is well known that the trace distance between two input states is an upper bound on the total variation distance between output distributions of any linear-optical experiment performed with those states. Therefore, we can simulate the target BosonSampling distribution by simulating the action of the same interferometer on σ with an error that decreases with the size of the exper-



(a) (b)

FIG. 1. Example of the algorithm in result 1. Blue rectangles correspond to beam splitters and associated phase shifters, orange rectangles are loss elements. We assume all loss elements are equal, and use the fact that two equal loss elements in the arms of a beam splitter commute with it. We apply our result 1 to the triangular decomposition of Reck *et al* [11] of (a) as an example. It is possible to commute to each input in the network different amounts of losses according to the shortest path between that input and any output, leading to the equivalent network represented in (b).

iment. We show this by using result 2 described previously. More specifically, our previous classical simulation was efficient because the state σ we obtained could be generated by the action of a linear-optical channel on a state where all n photons start in the same mode, which is known to be classically simulable. If we now append to σ another $\log n$ photons one in each mode, this is equivalent to a simulation of our original target lossy state ρ with an additional $\log n$ photons input in modes that have perfect transmission. However, this procedure generates a state of type B described in result 2 above, and so an efficient classical simulation is still possible.

Result 4: Nonuniform losses do not avoid classical simulation. By combining results 1–3 we obtain our main result. **Informally it states that the classical simulation algorithms of [4, 5] cannot be circumvented by the design of unbalanced networks such as that of Reck *et al* [11]** (see Theorem 4 in the technical notes for the formal statement). This was left as an open question in [5]. The idea was that, in an unbalanced network, there might be some input modes where losses are very mild, and the high chance of survival of these photons might break the assumptions behind the simulation algorithms. Here we show, focusing for concreteness on the particular construction of Reck *et al* [11], that classical simulation remains possible in those cases as well, likely closing one avenue for scaling up BosonSampling experiments. This is also relevant for current experiments, since networks with this geometry are common in integrated-photonic implementations [13, 16].

Our claim follows from the previous three results by the following argument. The triangular decomposition of Reck *et al* [11] (cf. Fig. 1(b)) has the property that the shortest path from mode i to any output has length i (if we label modes starting from the lowest one). Now separate the inputs in two sets: the bottom $c\log n$ ones, and the top $m - c\log n$ ones, for some c to be determined later. Suppose the input state we wish to simulate occupies the bottom n modes in an attempt to avoid losses as much as possible. To simplify the argument, suppose now that the bottom $c\log n$ modes are lossless (or include their loss channel as part of the network rather of the input state). By result 1 we can extract more than $c\log n$ loss elements for all modes above mode $c\log n+1$. However, as discussed in [5], given a per-beamsplitter loss parameter η, there is always some c such that, if an n-photon state suffers $c\log n$ rounds of losses, we expect less than $\sqrt{n}$ photons to survive on average. Therefore, the input to the network is amenable to approximation by a convex combination of states of type B, as described in result 3, and so efficient classical simulation is possible.

Conclusion— Results 1-4 above are relevant for the BosonSampling community due to the new theoretical ideas they introduce, but also to guide experimental efforts moving forward, in particular with regards to linear-optical network design. However, they can also be of independent interest to the quantum optics community in general. Result 1 in particular shows to which extent one can extract nonuniform losses from a linear-optical network. This is a major improvement over the similar result in [5]. While that result formalized a commonly-used assumption in the quantum optics community, our new result allows more realistic assumptions to be made that include nonuniform losses (which no longer commute with linear optics).

[1] A. Harrow and A. Montanaro, Nature **549**, 203 (2017).
[2] S. Aaronson and A. Arkhipov, Theory of Computing **4**, 143 (2013).
[3] S. Aaronson and D. J. Brod, Phys. Rev. A **93**, 012335 (2016).
[4] R. García-Patrón, J. J. Renema, and V. Shchesnovich, (2017), arXiv:1712.10037 [quant-ph].
[5] M. Oszmaniec and D. Brod, New Journal of Physics **20**, 092002 (2018).
[6] J. Renema, V. Shchesnovich, and R. García-Patrón, (2018), arXiv:1809.01953 [quant-ph].
[7] A. Arkhipov, Phys. Rev. A **92**, 062326 (2015).
[8] A. Leverrier and R. García-Patron, Quant. Inf. Comp. **15**, 489 (2014).

[9] S. Rahimi-Keshari, T. C. Ralph, and C. M. Caves, Phys. Rev. X **6**, 021039 (2016).
[10] G. Kalai and G. Kindler, arXiv e-print (2014), arXiv:1409.3093 [quant-ph].
[11] M. Reck, A. Zeilinger, H. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[12] A. Neville, C. Sparrow, R. Clifford, E. Johnston, P. M. Birchall, A. Montanaro, and A. Laing, Nature Physics **13**, 1153 (2017).
[13] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvão, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, Nat. Photon. **7**, 545 (2013).
[14] S. Chin and J. Huh, arXiv e-print (2017), arXiv:1710.05551 [quant-ph].
[15] P. Clifford and R. Clifford, "The classical complexity of boson sampling," in *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms* (2018) p. 146.
[16] J. Carolan, C. Harrold, C. Sparrow, E. Martín-López, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. O'Brien, and A. Laing, Science **349**, 711 (2015).

A Classical Algorithm for Quantum $SU(2)$ Schur Sampling

V. Havlíček[1] * S. Strelchuk[2] † K. Temme[3] ‡

[1] *Department of Computer Science, University of Oxfordw, Oxford OX1 3QD, UK*
[2] *DAMTP, University of Cambridge, Cambridge CB3 0WA, UK*
[3] *IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA*

Abstract. Many quantum algorithms can be represented in a form of a classical circuit positioned between quantum Fourier transformations. In our work, we study the case where quantum Fourier transformations are replaced by the quantum Schur Transform – a global transformation which maps the computational basis to a basis defined by angular momenta. It underpins Permutational Quantum Computing (PQC), which is a computational model believed to have supra-classical power. We show that the output distributions of PQC circuits can be approximately classically sampled in polynomial time if they are sufficiently close to being sparse, thus isolating a regime in which these Quantum $\mathsf{SU}(2)$ Schur Circuits could lead to algorithms with exponential computational advantage. Our work is primarily motivated by a conjecture that underpinned the hardness of Permutational Quantum Computing, a restricted quantum computational model that has the above circuit structure in one of its computationally interesting regimes. The conjecture stated that approximating transition amplitudes of Permutational Quantum Computing model to inverse polynomial precision on a classical computer is computationally hard. We disprove the extended version of this conjecture – even in the case when the hardness of approximation originated from a difficulty of finding the large elements in the output probability distributions.

Keywords: Quantum computing, sampling, classical simulation

The full paper version of this submission is at [1].

1 Introduction

Charaterizing the power of quantum computers is one of the two major challenges in quantum computation, with the other being their scalable implementation. A seminal approach to the former problem is the study of conditions which make quantum algorithms amenable to methods of efficient classical simulation. A number of important quantum algorithms can be cast in a form of classical circuit positioned between a pair of circuits which implement quantum Fourier transformation. These are, for example, algorithms for the Hidden Subgroup Problem which in particular include the Shor's factoring algorithm [2, 3]. While the latter provides strong evidence that quantum computers outperform the classical ones, Schwarz and van den Nest [4] showed that the respective quantum circuit could be efficiently classically simulated if its output distribution was sufficiently close to being sparse.

In our current work, we aim to characterize a different class of circuits that instead of the quantum Fourier transform contain the quantum Schur transform (QST) as depicted on Fig. 1. QST is a map from the computational basis to a basis defined by angular momentum [5, 6, 7] and it underpins a variety of quantum information processing tasks, including spectrum estimation [8, 9], hypothesis testing [10, 11, 12, 13], quantum computing using decoherence-free subspaces [14], communication without a shared reference frame [15, 16], and quantum color coding [17]. A quantum circuit that efficiently implements this transform was first described in [5, 6, 7] and recently improved by Kirby and Strauch [18, 19]. The extent to which circuits using QST could be used to devise new quantum algorithms is, to our knowledge, largely unexplored - possibly with the exception of [20] and [21].

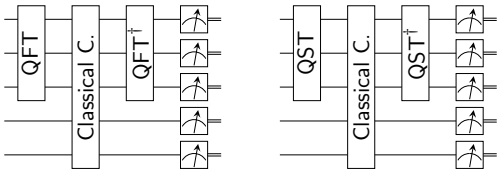


Figure 1: Schematic diagrams of the quantum circuit used in Shor's factoring algorithm (Left) and the circuits we consider here (Right). QST denotes the $\mathsf{SU}(2)$ Quantum Schur Transformation. The classical circuits between the transforms can represent, for example a polynomially-long sequence of Toffoli gates.

QST is a centerpiece in the analysis of Permutational Quantum Computing (PQC) [22] – a restricted quantum computational model based on recoupling of angular momenta [21, 23]. It has been conjectured that PQC has supra-classical computational power. One of the conjectures supporting this belief stated that an approximation of its transition amplitudes in the regime where they encode matrix elements of the symmetric group irreps in the Young's orthogonal form [24, 21] is hard to compute classically if we require inverse polynomial precision (in the number of input qubits). While in our previous work we presented an efficient classical algorithm for approximating such transition amplitudes [22], an intriguing question remained: Is it also possible to identify all PQC transition amplitudes that can be approximated using classical methods with the inverse polynomial precision? Since the expected output probability of an n-qubit quan-

*vojtech.havlicek@keble.ox.ac.uk
†ss870@cam.ac.uk
‡kptemme@gmail.com

tum circuit C with an input state $|y\rangle$ is given by:

$$\mathbb{E}_x\left(|\langle x|C|y\rangle|^2\right) = \frac{1}{2^n}\sum_x |\langle x|C|y\rangle|^2 = \frac{1}{2^n},$$

approximating these values with an inverse polynomial precision cannot distinguish the majority of $\langle x|C|y\rangle$ amplitudes from zeroes.

Could we exploit the difficulty that arises from finding large matrix elements encoded in the output of the algorithm and thus demonstrate the (exponential) quantum computational advantage?

We show that this is *not* the case by describing a classical method that finds all large output probabilities in polynomial time.

2 Preliminaries and main results

Consider n qubits indexed by $[n] := \{1, 2 \ldots n\}$. The spin of the k-th qubit is defined by a triple of operators:

$$\vec{S}_k = \frac{1}{2}\left(X_k,\, Y_k,\, Z_k\right),$$

where X_k, Y_k, Z_k denote the Pauli X, Y, Z operators on the k-th qubit. The *total spin operator* on a qubit subset $A \subseteq [n]$ is given by:

$$S_A^2 := \sum_{k\in A} \vec{S}_k \cdot \sum_{k'\in A} \vec{S}_{k'}.$$

We write $S^2 := S^2_{[n]}$. The operators S_A^2 and S_B^2 commute if and only if the sets A and B are disjoint or one is contained in the other. Let:

$$Z_A := \frac{1}{2}\sum_{k\in A} Z_k,$$

denote the *azimuthal spin operator* on a qubit subset A. We again use $Z_{[n]} := Z$. The operators Z_A and S_A^2 commute for any $A \subseteq [n]$ and share an eigenspace labeled by quantum numbers j_A and m_A. The quantum number j_A is the *total spin* of qubits in A and m_A is the *azimuthal spin*. Both spin numbers are subject to constraints: the azimuthal spin m_A only takes values in integer steps between $-j_A$ and j_A, while the total spin numbers are either integer or half-integer and combine according to the angular momentum addition rules [27, 28]:

$$j_{A\cup B} \in \{|j_A - j_B|,\, |j_A - j_B| + 1, \ldots,\, j_A + j_B\}. \quad (1)$$

Sets of commuting spin operators can be used to define complete orthonormal bases [21]. A particular basis is given by coupling a qubit at a time; that is by the joint eigenstates of:

$$S^2_{[2]},\, S^2_{[3]},\, \ldots S^2, Z.$$

We call it the *sequentially coupled basis*. The basis states are labeled by eigenstates $j_{[2]}, j_{[3]} \ldots, j_{[n-1]}, J$ and M of the spin operators. By Eq. 1, these are subject to:

$$j_{[1]} = \frac{1}{2}, \qquad j_{[k+1]} = \left|j_{[k]} \pm \frac{1}{2}\right|, \quad (2)$$

which can be expressed diagrammatically by a *branching diagram* (see Fig. 4 in [1]). Up to the quantum number M, the sequential basis states correspond to paths in this diagram that start at $j_{[1]} = \frac{1}{2}$.

Let $\mathcal{A}_k$ be the set of all such paths on k qubits. For the sequentially coupled basis, the $\mathsf{SU}(2)$ Schur-Weyl duality gives rise to the $\mathsf{SU}(2)$ Quantum Schur Transform as described in [6, 7, 18, 5, 19, 30]. It is a sequence of the Clebsch-Gordan transformations, that couple j and j' eigenspaces into a $|J, M, j, j'\rangle$ state by:

$$|J, M, j, j'\rangle = \sum_{m,m'} C^{J,M}_{j,m;\, j',m'} \,|j, m\rangle\,|j', m'\rangle\,,$$

where the summation over m runs from $-j$ to j in integer steps (and similarly for m') and the $C^{J,M}_{j,m;\, j',m'}$ are the Clebsch-Gordan coefficients. The transform between the computational and the sequentially coupled basis is given by a cascade of the Clebsch-Gordan transforms [5, 18]. We label the sequentially coupled basis states on n qubits by $|\boldsymbol{J}, M\rangle$, where $\boldsymbol{J}$ is a path in $\mathcal{A}_n$.

Permutational Quantum Computing in the sequentially coupled basis uses the permutation gate between two sequentially coupled basis states. Its transition amplitudes are:

$$\langle \boldsymbol{J}, M|U_\pi|\boldsymbol{J}', M'\rangle\,,$$

where the permutation gate U_π is defined by its action on a computational basis state $|x_1 \ldots x_n\rangle$ as:

$$U_\pi\,|x_1 x_2 x_3 \ldots x_n\rangle = |x_{\pi(1)} x_{\pi(2)} x_{\pi(3)} \ldots x_{\pi(n)}\rangle\,.$$

Both Z and S^2 operators commute with U_π and consequently, $M = M'$ and $J = J'$. The matrix $\langle \boldsymbol{J}, M|U_\pi|\boldsymbol{J}', M'\rangle$ block-diagonalizes to J, M blocks; each of which corresponds the an irreducible representation of the symmetric group in the Young's orthogonal form. The transition amplitudes are then the matrix elements of these matrices [21]. Approximating them to polynomial precision was conjectured hard classically in [21, 24] but an efficient classical algorithm was found by two of the co-authors [22].

The methods we present here work for a broader family of quantum circuits we call the $\mathsf{SU}(2)$ *Quantum Schur Sampling* circuits. These have transition amplitudes:

$$\langle \boldsymbol{J}, M|W|\boldsymbol{J}', M'\rangle\,,$$

where W is defined by its action on a computational basis state $|x\rangle\,, x \in \{0,1\}^n$:

$$W\,|x\rangle = |w(x)\rangle\,,$$

with $w : \{0,1\}^n \to \{0,1\}^n$ being a classical function given by a sequence of Toffoli gates – we consider only such W where this sequence is $\mathsf{poly}(n)$ long. To formally state our results, we introduce the measurement output distributions which arise after we measure the qubits after a computational run. Given a path $\boldsymbol{j} \in \mathcal{A}_k$ for $k \le n$,

$|\phi\rangle = W|\boldsymbol{J}, M\rangle$, define the *output marginal* $p(\boldsymbol{j})$:

$$p(\boldsymbol{j}) := \sum_{\boldsymbol{J}\supseteq\boldsymbol{j}} \sum_{M} p(\boldsymbol{J}, M)$$
$$= \langle\phi| \sum_{\boldsymbol{J}\supseteq\boldsymbol{j};M} |\boldsymbol{J}, M\rangle \langle\boldsymbol{J}, M|\phi\rangle := \langle\phi|\Pi(\boldsymbol{j})|\phi\rangle,$$

where the summation $\sum_{\boldsymbol{J}\supseteq\boldsymbol{j}}$ sums all paths $\boldsymbol{J} \in \mathcal{A}_n$ that contain $\boldsymbol{j} \in \mathcal{A}_k$. The summation $\sum_M$ runs from $-J$ to J in integer steps. We use $\sum_{\boldsymbol{J}\supseteq\boldsymbol{j};M}$ as a shorthand for $\sum_{\boldsymbol{J}\supseteq\boldsymbol{j}} \sum_M$. The projector has the form:

$$\Pi(\boldsymbol{j}) := \sum_{\boldsymbol{J}\supseteq\boldsymbol{j};M} |\boldsymbol{J}, M\rangle \langle\boldsymbol{J}, M|.$$

2.1 Main results

In our work, we derive a classical algorithm that finds large elements in the output distribution of quantum Schur circuits with the following performance:

Theorem 1 *Let $p(\boldsymbol{J}) : \mathcal{A}_n \to [0,1]$ be a probability distribution on paths. There is a classical algorithm that outputs a set $L \subseteq \mathcal{A}_n$ in $\mathsf{poly}\left(n, \frac{1}{\theta}, \log\frac{1}{\gamma}\right)$ time, such that for some $\theta > 0$:*

$$\begin{aligned} &\forall\, \boldsymbol{J} \in L:\ p(\boldsymbol{J}) \geq \frac{\theta}{2}, \\ &\forall\, \boldsymbol{J} \in \mathcal{A}_n:\ p(\boldsymbol{J}) > \theta \implies \boldsymbol{J} \in L, \end{aligned} \tag{3}$$

with probability at least $1-\gamma$.

One may view this theorem as an adaptation of the Kushilevitz-Mansour algorithm [25] to a new setting where instead of decision trees, we work with branching diagrams. The proof is given in Section III of [1].

The theorem below shows that there exists an efficient classical sampler when the requisite distribution is close to sparse. It will be convenient to explicitly represent the probability distribution as follows: $p(\boldsymbol{J}) = \sum_M p(\boldsymbol{J}, M)$.

Definition 2 (ϵ-approximate t-sparsity) *A probability distribution $p(\boldsymbol{J}, M)$ is t-sparse if it has at most t non-zero elements $p(\boldsymbol{J}, M)$. A probability distribution $\tilde{p}(\boldsymbol{J}, M)$ is ϵ-approximately t-sparse if there exists a t-sparse distribution $p(\boldsymbol{J}, M)$ such that:*

$$\|p - \tilde{p}\|_1 \leq \epsilon.$$

Theorem 3 *Assume that $p(\boldsymbol{J}, M)$ is ϵ-approximate t-sparse. Then one can sample from $p(\boldsymbol{J}, M)$ classically in $\mathsf{poly}(n, \frac{1}{\epsilon}, t)$ time to 6ϵ error in the total variational distance.*

The proof is given in Section IV of [1].

Our results additionally imply that sampling from the quantum Schur circuits can only lead to exponential computational advantage if the individual elements of the output distribution *cannot* be resolved by polynomial approximation with the quantum device by taking polynomially many samples. A way to circumvent this restriction, similarly to the case of circuits that use the quantum Fourier transform, could be to use a technique utilized in the Shor's algorithm that reconstructs group generators by sampling $\log|G|$ group elements for a superpolynomially large $|G|$. There is no meaningful counterpart to this approach for the QST as of now.

3 Discussion

Circuits using the QST underpin a diverse range of protocols in quantum information processing, from state discrimination to computational models such as Permutational Quantum Computing. While studying the computational power of the transform, we singled out a class of circuits with QST blocks that extend a computationally interesting regime of Permutational Quantum Computing. The key result that enabled this analysis was the efficient approximation of quantum Schur sampling circuits studied in [22] as means to characterize its computational power. Building on the work of Schwarz and Van den Nest [32, 4], we showed that large elements of the output distributions can be efficiently found, which precludes the possibility that the circuits could encode quantities that would be hard to classically approximate by taking polynomial number of samples. We subsequently proved that these circuits can be classically efficiently approximately sampled from if their output distribution becomes sufficiently close to a sparse one.

Our algorithm may be viewed as a random walk on the angular momentum branching diagram associated with the computation. One distinctive feature of the algorithm is then that it is not limited to the angular momentum and can be extended to other branching diagrams. It will remain efficient as long as the counterparts of the Clebsch-Gordan coefficients remain efficiently computable to high precision and the out-degree of any vertex of the branching diagram will be bounded by a constant (see also the discussion in [22]). One of the interesting cases where our techniques could apply with little adaptation is the case of q-deformations of the $\mathsf{SU}(2)$ branching diagrams, applied in the study of topological phases of matter [34, 35].

Circuits using similar structure but using an $\mathsf{SU}(d)$ Schur-Weyl transformation for $d > 2$ were recently applied in study of Boson Sampling with partially distinguishable bosons in the first quantization [36]. The possibility of leveraging the simulation techniques proposed here in this context remains open.

References

[1] V. Havlicek, S. Strelchuk, K. Temme, full paper version of this submission, available at `https://arxiv.org/abs/1809.05171` (2018).

[2] P. W. Shor. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, SFCS '94, pages 124–134, Washington, DC, USA, 1994. IEEE Computer Society.

[3] A. Y. Kitaev. *eprint arXiv:quant-ph/9511026*, November 1995.

[4] M. Schwarz and M. Van den Nest. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:154, 2013.

[5] A. W. Harrow. *eprint arXiv:quant-ph/0512255*, December 2005.

[6] D. Bacon, I. L. Chuang, and A. W. Harrow. *Phys. Rev. Lett.*, 97:170502, Oct 2006.

[7] D. Bacon, I. L. Chuang, and A. W. Harrow. In *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '07, pages 1235–1244, Philadelphia, PA, USA, 2007. Society for Industrial and Applied Mathematics.

[8] R. D. Gill and S. Massar. PRA, 61(4):042312, April 2000.

[9] M. Keyl and R. F. Werner. *Phys. Rev. A*, 64:052311, Oct 2001.

[10] M. Hayashi and K. Matsumoto. *eprint arXiv:quant-ph/0109028*, September 2001.

[11] M. Hayashi and K. Matsumoto. PRA, 66(2):022311, August 2002.

[12] M. Hayashi and K. Matsumoto. *eprint arXiv:quant-ph/0209124*, September 2002.

[13] M. Hayashi and K. Matsumoto. *eprint arXiv:quant-ph/0209030*, September 2002.

[14] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley. PRA, 63(4):042307, April 2001.

[15] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. *Phys. Rev. Lett.*, 91:027901, Jul 2003.

[16] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. *Reviews of Modern Physics*, 79:555–609, April 2007.

[17] A. Hayashi, T. Hashimoto, and M. Horibe. PRA, 71(1):012326, January 2005.

[18] W. M. Kirby and F. W. Strauch. *Quantum Information and Computation*, 18, 09 2017.

[19] W. Kirby. Undergraduate thesis, Williams College, 2017.

[20] A. M. Childs, A. W. Harrow, and P. Wocjan. In Wolfgang Thomas and Pascal Weil, editors, *STACS 2007*, pages 598–609, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[21] S. P. Jordan. *Quantum Info. Comput.*, 10(5):470–497, May 2010.

[22] V. Havlíček and S. Strelchuk. *Phys. Rev. Lett.*, 121(6):060505, August 2018.

[23] A. Marzuoli and M. Rasetti. *Annals of Physics*, 318:345–407, August 2005.

[24] S. P. Jordan. *ArXiv e-prints*, November 2008.

[25] E. Kushilevitz and Y. Mansour. *SIAM Journal on Computing*, 22(6):1331–1348, 1993.

[26] O. Goldreich and L. A. Levin. In *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC '89, pages 25–32, New York, NY, USA, 1989. ACM.

[27] P. Woit. *Quantum Theory, Groups and Representations: An Introduction (Final draft version)*. 2017.

[28] J. J. Sakurai. *Modern quantum mechanics; rev. ed.* Addison-Wesley, Reading, MA, 1994.

[29] R. Pauncz. *Alternant Molecular Orbital Method*. Studies in physics and chemistry, no. 4. Saunders, 1967.

[30] H. Krovi. *ArXiv e-prints*, March 2018.

[31] These circuits extend the notion of quantum Schur sampling circuits introduced in [22], where we only considered circuits of the form $\langle \boldsymbol{J}, M|\Lambda|\boldsymbol{J}', M'\rangle$ with Λ being a Z-diagonal gate with efficiently computable elements. Our technique works for these circuits as well.

[32] M. Van Den Nest. *Quantum Info. Comput.*, 11(9-10):784–812, September 2011.

[33] C. Greene, A. Nijenhuis, and H. S. Wilf. *Advances in Mathematics*, 31(1):104 – 109, 1979.

[34] L. Hormozi. PhD thesis, The Florida State University, 2007.

[35] R. Fern, J. Kombe, and S. H. Simon. *ArXiv e-prints*, June 2017.

[36] A. E. Moylett and P. S. Turner. *Physical Review A*, 97(6):062329, 2018.

Unifying theory of quantum state estimation using past and future information

Areeya Chantasri[1] *, Ivonne Guevara [1] †, Kiarn T. Laverick [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. We propose a unifying theory for estimating unknown quantum states using observed data, both before (past) and after (future) the estimation time. Considering a partially observed quantum system, in which there exist both observed and unobserved records from continuous monitoring of the system, we give a common formulation for seven types of state estimators. The state estimators are calculated based on the expected cost minimization, either in the state space or the unknown record space. Our theory also establishes the connection among three existing formalisms that use past-future information, and suggest new estimators that can be applied in practical scenarios.

Keywords: Quantum state estimation, cost function, quantum measurement, quantum trajectory

1 Introduction

There is much to learn from the state estimation theory for classical systems, where various techniques are used for estimating a probability distribution for unknown parameters, given data from observation. Since, in practical systems, observation is mostly incomplete or corrupted by noises, techniques for estimation need to be tailored to specific scenarios, such that it utilizes the information gained from the observed data, to minimize some defined cost functions for the state. In the quantum information community, however, "quantum state estimation" is still mostly thought of as identical to quantum state tomography. Therefore, as the field of quantum dynamics has been rapidly advancing, we should now be developing the estimation theory for states of individual quantum systems, in a systematic way as in the classical case.

In this work, we consider the problem of state estimation for quantum dynamical systems, where observation is performed quasi-continuously in time [1, 2, 3]. Thus, the information used in estimating the state at time τ can be maximized by including observed data, both before (past) and after (future) that time. This past-future information conditioning is the core of classical Bayesian state smoothing [4]. For quantum systems, the past-future idea, first explored by Watanabe [5], was formulated as the Two-State Vector formalism by Aharonov *et al.* [6]. Since then, there have been numerous proposals related to using past-future information (or observation) to improve quantum estimation: for system parameters [7, 8]; for quantum measurement results [9]; and for the quantum state itself [10]. The past-future information was also implicitly applied in deriving the most-likely path for quantum diffusive dynamics, between two quantum states in Refs. [11, 12]. The formalisms in Refs. [8, 10, 11] give rise to different quantum states conditioned on the past-future observation; therefore, one of the most interesting questions is whether they can be unified under a general theory of state estimation with distinct cost functions.

We here propose a unifying theory, where the existing formalisms can be defined with suitable expected cost functions, conditioning on past-future information. Consider a quantum system undergoing an incomplete continuous observation, with observed (O) and unobserved (U) records from diffusive-type measurements. If both records are specified (complete observation), then one can compute a trajectory of the true quantum state [3] $\rho_{\rm T}(\tau) = \rho_{\overleftarrow{O},\overleftarrow{U}}$ for any time τ, using the records up to that time. The back arrow over a record (R) is defined as $\overleftarrow{R} = \{R_t : t \in [t_0, \tau)\}$ (a past record from the initial time t_0 to time τ). The goal is to derive quantum state paths that minimize various expected cost functions, conditioned only on the observed records, but both before and after the estimation time, i.e., conditioned on $\overleftrightarrow{O} = \{O_t : t \in [t_0, \tau) \cup [\tau, T)\}$, where T is a final time. We note that in the process of making the connection among the existing formalisms, we also introduce new estimators. These estimators may be useful in specific systems or experimental setups.

2 Existing formalisms

2.1 Two-State Vector and related formalisms

The Two-State Vector formalism (TSVF) [6] has led to the formulation of a weak value [13]. Let us use $A_w = A_w^{\rm re} + iA_w^{\rm im}$ as a detector's linear response, in phase space, of a *weak* von Neumann measurement of an observable $\hat{A}$. The weak value formulated in Ref. [13], ${}_\phi\langle A_w\rangle_\psi = \langle\phi|\hat{A}|\psi\rangle/\langle\phi|\psi\rangle$, represents an average of detector's responses, conditioning on pre-selected $|\psi\rangle$ and post-selected $|\phi\rangle$ states. The formula was later generalized to mixed states and arbitrary measurements [14, 8, 15, 9], where the conditional average of detector readouts, represented by the real part of the weak value, is given by,

$$ {}_{\hat{E}}\langle A_w^{\rm re}\rangle_\rho = \frac{{\rm Tr}\left[(\hat{E}\rho + \rho\hat{E})\hat{A}\right]}{{\rm Tr}\left[(\hat{E}\rho + \rho\hat{E})\right]}. \tag{1}$$

*a.chantasri@griffith.edu.au
†i.guevaraprieto@griffith.edu.au
‡kiarn.laverick@griffithuni.edu.au
§h.wiseman@griffith.edu.au

Here, for the generalized version, assuming that the weak measurement of $\hat{A}$ occurs at time τ, the state ρ is a quantum state computed from observed (known) measurement results up to time τ, and $\hat{E}$ is a POVM representing observed measurement results after τ. For the partially observed quantum system considered in this work, we then have the two matrices: $\rho = \rho_{\overleftarrow{O}}$ and $\hat{E} = \hat{E}_{\overrightarrow{O}}$ carrying the past-future information.

From Eq. (1) and the analysis in [8, 9, 16], we can also define a Weak-Value state (WVS) in a symmetrized form, $\varrho_{\mathrm{WVS}} \propto \hat{E}_{\overrightarrow{O}}\rho_{\overleftarrow{O}} + \rho_{\overleftarrow{O}}\hat{E}_{\overrightarrow{O}}$, such that the weak value is an expectation value of the observable $\hat{A}$, i.e.,

$$\hat{E}_{\overrightarrow{O}}\langle A_w^{\mathrm{re}}\rangle_{\rho_{\overleftarrow{O}}} = \mathrm{Tr}\left[\varrho_{\mathrm{WVS}}\hat{A}\right]. \tag{2}$$

However, we note that ϱ_{WVS} is, in general, not positive-semi definite, and therefore cannot represent a proper quantum state.

For an arbitrary-strength measurement of $\hat{A}$ at time τ, its unknown result can also be estimated using the past-future observation, using both $\rho_{\overleftarrow{O}}$ and $\hat{E}_{\overrightarrow{O}}$ as shown in Ref. [9].

2.2 Quantum State Smoothing

In the observed-unobserved records scenario, the quantum state smoothing proposed by Guevara and Wiseman (GW) [17] can be used to optimally estimate the system's state using observed records, both before and after the estimation time. However, it was not shown in the original work that their smoothed state, defined as a conditional average over all possible true states, $\rho_{\mathrm{S}} = \sum_{\overleftarrow{U}} \wp(\overleftarrow{U}|\overrightarrow{O})\rho_{\overleftarrow{O},\overleftarrow{U}}$, is simply an estimator that minimizes the expected Trace Square Deviation from true states, i.e.,

(A) $\langle \mathbf{TrSDf}\rho_{\overleftarrow{O},\overleftarrow{U}}\rangle$:

$$\rho^*(\tau) = \arg\min_{\rho_\tau} \left\langle \mathrm{Tr}\left[\left(\rho_\tau - \rho_{\overleftarrow{O},\overleftarrow{U}}\right)^2\right]\right\rangle_{\overrightarrow{O}}, \tag{3}$$

where we have defined $\langle\cdots\rangle_{\overleftrightarrow{O}} \equiv \sum_{\overleftarrow{U}} \wp(\overleftarrow{U}|\overrightarrow{O})\cdots$ as an expectated value weighted with a conditional probability distribution $\wp(\overleftarrow{U}|\overrightarrow{O})$ of the unobserved record.

2.3 Quantum Most-Likely path

Originally introduced as a tool to investigate statistics of quantum trajectories for diffusive continuous quantum measurement, the most likely path proposed by Chantasri, Dressel and Jordan (CDJ) [11, 12] is a variational solution of a stochastic path integral. The path integral is constructed from joint probability density functions of measurement records; thus, the variational solution gives a quantum state path arising from the most likely (by a natural measure) complete record $\overleftrightarrow{R} = \{R_t : t \in [t_0, T)\}$. We here generalize the approach to the partially observed system. The backaction from the observed record $\overleftrightarrow{O}$ is now included in the deterministic dynamics, and the joint probability density functions of the unobserved record $\overleftrightarrow{U}$ are modified to reflect the conditioning of the observed

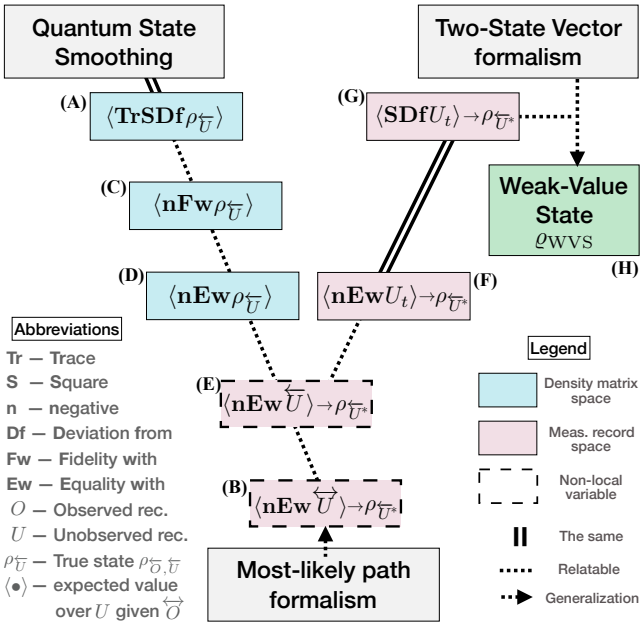


Figure 1: Diagrams showing different optimal estimators, connecting the existing formalisms: Quantum state smoothing, the CDJ most-likely path formalism, and the Two-State vector formalism. Blue and pink boxes represent cost functions defined on the quantum state space and unobserved record space, respectively. The Roman letters **(A)**, **(B)**, ... are related to formulas in the text. Since the observed record is fixed in the minimization of expected cost function, we omitted the O-dependence in the definition of any true states.

record. As a result, the most likely path can be considered as a state estimator that minimizes the expected negative Equality with the whole Unobserved record,

(B) $\langle \mathbf{nEw}\overleftrightarrow{U}\rangle$:

$$\rho^*(\tau) = \rho_{\overleftarrow{O},\overleftarrow{U}^*}, \text{ where}$$
$$\overleftarrow{U}^* : \ \overleftrightarrow{U}^* = \arg\min_{\overleftrightarrow{u}} \left\langle -\delta\left(\overleftrightarrow{u} - \overleftrightarrow{U}\right)\right\rangle_{\overrightarrow{O}}. \tag{4}$$

The delta function of a string of numbers, which in this case is a complete record for $t \in [t_0, T)$, is defined as a product of delta functions, e.g., $\delta(\{u_1, u_2\} - \{U_1, U_2\}) = \delta(u_1 - U_1)\delta(u_2 - U_2)$, as an example of records with two time steps.

3 Connection via cost functions and new estimators

The existing formalisms presented above can be regarded as giving solutions that minimize expected cost functions, though in different variable spaces, of different forms. For examples, the GW smoothed state **(A)** minimizes the expected cost defined in the density matrix space, and the CDJ path **(B)** minimizes the cost in the record space (the latter is for diffusive records only). Moreover, the former cost is defined locally in time, and the latter non-locally in time.

Following the diagram in Fig. 1, we can start by introducing cost functions that connect the estimators **(A)** and **(B)**. The first natural cost from **(A)** remains in the state space, but uses instead the Fidelity as a measure of the distance between any two states. That is, we define an estimator that minimizes the expected negative Fidelity with true states, i.e.,

(C) $\langle$**nFw**$\rho_{\overleftarrow{O},\overleftarrow{U}}\rangle$:

$$\rho^*(\tau) = \arg\min_{\rho_\tau} \left\langle -F\left(\rho_\tau, \rho_{\overleftarrow{O},\overleftarrow{U}}\right)\right\rangle_{\overrightarrow{O}}. \tag{5}$$

If the Jozsa [18] Fidelity is used, which gives $F[\rho_{\rm T},\rho_{\rm C}] \equiv {\rm Tr}\left[\rho_{\rm T}\rho_{\rm C}\right]$ for $\rho_{\overleftarrow{O},\overleftarrow{U}}$ pure, the estimator is the lustrated smoothed state, defined in Ref. [19], which is itself also pure.

Classically, an equivalent cost function of the Fidelity cost in the state space is a delta function, which leads to an estimator that minimizes the expected negative Equality with true states,

(D) $\langle$**nEw**$\rho_{\overleftarrow{O},\overleftarrow{U}}\rangle$:

$$\rho^*(\tau) = \arg\min_{\rho_\tau} \left\langle -\delta\left(\rho_\tau - \rho_{\overleftarrow{O},\overleftarrow{U}}\right)\right\rangle_{\overleftrightarrow{O}}. \tag{6}$$

We note that, in the quantum case, however, the most likely (by the Haar measure) state at any time τ, is not the same as the lustrated state in general.

Let us then move towards the measurement record space. As mentioned earlier, a pure quantum state $\rho_{\overleftarrow{O},\overleftarrow{U}}$ at time τ can be constructed given both observed $\overleftarrow{O}$ and unobserved $\overleftarrow{U}$ records. Therefore, we can define an optimal state estimate by first finding an optimal estimator for the unobserved record. Similar to **(D)**, an intuitive option is a quantum state computed from a $\overleftarrow{U}$ estimator that minimizes the expected negative Equality with past Unobserved records,

(E) $\langle$**nEw**$\overleftarrow{U}\rangle$:

$$\rho^*(\tau) = \rho_{\overleftarrow{O},\overleftarrow{U}^*}, \text{ where}$$
$$\overleftarrow{U}^* = \arg\min_{\overleftarrow{u}} \left\langle -\delta\left(\overleftarrow{u} - \overleftarrow{U}\right)\right\rangle_{\overleftarrow{O},\overrightarrow{O}}. \tag{7}$$

We note that this cost function is naturally generalized from the past record $\overleftarrow{U}$ to the string of the whole record $\overleftrightarrow{U}$, which then leads to the most likely path **(B)** in Eq. (4).

Now that a clear connection between **(A)** has been established, we now begin to extrapolate the cost function idea to the TSVF and the weak value. Since the weak value is mathematically the average of unknown records conditioned on the past and future information [14], the most direct connection is via cost functions of the unknown records locally in time (see Fig. 1). We can then define a quantum state that is computed from a string of joined record estimators that locally minimize the expected negative Equality with Unobserved record,

(F) $\langle$**nEw**$U_t\rangle$:

$$\rho^*(\tau) = \rho_{\overleftarrow{O},\overleftarrow{U}^*}, \text{ where}$$
$$\overleftarrow{U}^*: \; U_t^* = \arg\max_{u_t} \left\langle -\delta\left(u_t - U_t\right)\right\rangle_{\overleftrightarrow{O}}, \tag{8}$$

where the estimated unobserved record is optimized locally in time.

Similarly, the cost function in the record space, locally in time, can be defined with a mean square deviation function. This cost then leads to an unknown record estimator presented in the "past quantum state" formalism [9]. However, in their original work, a semi-positive definite quantum state was not defined. We then propose a state path calculated from a string of record estimators that minimize the expected Square Deviation from Unobserved records locally in time,

(G) $\langle$**SDf**$U_t\rangle$:

$$\rho^*(\tau) = \rho_{\overleftarrow{O},\overleftarrow{U}^*}, \text{ where}$$
$$\overleftarrow{U}^*: \; U_t^* = \arg\max_{u_t} \left\langle \left(u_t - U_t\right)^2\right\rangle_{\overleftrightarrow{O}}. \tag{9}$$

We note that, since we are considering the diffusive measurement of a quantum system, the distribution of the unobserved record is Gaussian and the estimators in **(F)** and **(G)** then coincide. Moreover, if we assume that a measurement giving the unobserved record at time τ is an infinitely weak measurement of a Hermitian observable $\hat{U}$, then the record estimator in Eq. (9) becomes a weak value Eq. (1),

$$\arg\min_{u_\tau} \left\langle \left(u_\tau - U_\tau^{\rm weak}\right)^2\right\rangle_{\overleftrightarrow{O}} = {}_{\hat{E}_{\overrightarrow{O}}}\langle U_\tau^{\rm weak}\rangle_{\rho_{\overleftarrow{O}}}, \tag{10}$$

where $U_\tau^{\rm weak}$ is a weak measurement result at time τ. The right hand side is ${\rm Tr}\left[(\hat{E}_{\overrightarrow{O}}\rho_{\overleftarrow{O}} + \rho_{\overleftarrow{O}}\hat{E}_{\overrightarrow{O}})\hat{U}\right]$.

For completeness, we can also define the Weak-Value state (WVS), $\varrho_{\rm WVS}$, as an estimator corresponding to the weak value in Eq. (1). Considering the weak von Neumann measurement of an observable $\hat{A}_j$ at time τ, the weak value of this observable is an estimator that minimizes the expected Square Deviation from the weak measurement results, $(A_j)_w^{\rm re}$. To define a state, we first define a complex matrix estimator ϱ^* such that,

(H) Weak-Value state:

$$\varrho^*(\tau) = \arg\min_{\varrho_\tau} \left\langle \left({\rm Tr}\left[\varrho_\tau \hat{A}_j\right] - (A_j)_w^{\rm re}\right)^2\right\rangle_{\overleftrightarrow{O}}, \tag{11}$$
$$= \arg\max_{\varrho_\tau} \left\langle -\delta\left({\rm Tr}\left[\varrho_\tau \hat{A}_j\right] - (A_j)_w^{\rm re}\right)\right\rangle_{\overleftrightarrow{O}}, \tag{12}$$

where ϱ_τ is a dummy complex matrix, and both lines Eqs. (11)-(12) are equivalent because of the Gaussian properties of the weak measurement records. The solution ϱ^* for each observable $\hat{A}_j$ is not unique; however, there is a solution for all observables $\hat{A}_j$'s (defined for a quantum system), and this solution coincides with the WVS $\varrho_{\rm WVS} = \varrho^*_{\forall \hat{A}_j}$. As noted earlier, the WVS is not constrained in a valid quantum state space, which is in the similar sense that the weak value can have its value outside the eigenvalue range of its observable.

References

[1] M. B. Mensky. Decoherence and the theory of continuous quantum measurements. *Phys.-Usp.*, 41:923, 1998.

[2] A. Barchielli and M. Gregoratti. *Quantum trajectories and measurements in continuous time*. Springer-Verlag Berlin Heidelberg, 2009.

[3] H. M. Wiseman and G. J. Milburn. *Quantum measurement and control*. Cambridge University Press UK, 2010.

[4] N. Wiener. *Extrapolation, Interpolation, and Smoothing of Stationary Time Series: With Engineering Applications*. Martino Fine Book, 2013.

[5] S. Watanabe. Symmetry of physical laws. part iii. prediction and retrodiction. *Rev. Mod. Phys.*, 27:179–186, Apr 1955.

[6] Y. Aharonov, P. G. Bergmann, and J. L. Lebowitz. Time symmetry in the quantum process of measurement. *Phys. Rev.*, 134:B1410–B1416, Jun 1964.

[7] M. Tsang. Time-symmetric quantum theory of smoothing. *Phys. Rev. Lett.*, 102:250403, Jun 2009.

[8] M. Tsang. Optimal waveform estimation for classical and quantum systems via time-symmetric smoothing. *Phys. Rev. A*, 80:033840, Sep 2009.

[9] S. Gammelmark, B. Julsgaard, and K. Mølmer. Past quantum states of a monitored system. *Phys. Rev. Lett.*, 111:160401, Oct 2013.

[10] I. Guevara and H. Wiseman. Quantum state smoothing. *Phys. Rev. Lett.*, 115:180407, Oct 2015.

[11] A. Chantasri, J. Dressel, and A. N. Jordan. Action Principle for Continuous Quantum Measurement. *Phys. Rev. A*, 88:042110, 2013.

[12] A. Chantasri and A. N. Jordan. Stochastic path-integral formalism for continuous quantum measurement. *Physical Review A*, 92:032125, Sep 2015.

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

[14] H. M. Wiseman. Weak values, quantum trajectories, and the cavity-qed experiment on wave-particle correlation. *Phys. Rev. A*, 65:032111, Feb 2002.

[15] J Dressel, S Agarwal, and Andrew N Jordan. Contextual values of observables in quantum measurements. *Phys. Rev. Lett.*, 104(24):240401, 2010.

[16] K. T. Laverick, A. Chantasri, and H. M. Wiseman. Quantum state smoothing for linear gaussian systems. *Phys. Rev. Lett.*, 122:190402, May 2019.

[17] H. Wiseman and I. Guevara. Quantum state smoothing. *Phys. Rev. Lett.*, 115:180407, 2015.

[18] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[19] I. Guevara. *Quantum State Smoothing*. Doctoral thesis, Griffith University, 2016.

Remote Time Manipulation

David Trillo[1], Benjamin Dive[1*], and Miguel Navascués[1]

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

Abstract. Harnessing the flow of proper time of arbitrary external systems over which we exert little or no control has been a recurring theme in both science and science-fiction. Here we present heralded, non-relativistic scattering experiments which, freeze out, speed up or even reverse the free dynamics of an ensemble of identical quantum systems. This "time warping" effect is universal: it is independent of the particular interaction between the scattering particles and the target systems, or the (possibly non-Hermitian) Hamiltonian governing the evolution of the latter. The protocols require careful preparation of the probes which are scattered, and success is heralded by projective measurements of these probes at the conclusion of the experiment. We fully characterize the possible time translations which we can effect on n target systems through a scattering protocol of fixed duration; the core result is that time can be freely distributed between the systems, and reversed at a small cost. For high n, our protocols allow one to quickly send a single system to its far future or past.

Introduction

Since the advent of the special theory of relativity, our modern understanding of time has been "that which clocks measure" [1]. With this in mind, the relativistic effect by which two clocks go out of sync if one of them is translated through space is regarded as a "time dilation". What makes relativistic time dilation extraordinary is the fact that, in order to make one of the clocks tick more slowly, we do not need any control of its inner workings: it suffices to push it. The ability to manipulate the proper time of a physical system in such a high level way, a phenomenon know as *time warp*, has inspired numerous works of science fiction (e.g., [2]).

There have been several proposals to achieve command of the proper time of arbitrary external systems, all of them based on special or general relativity. Most of them rely on the existence of natural "time machines" [3, 4]. More realistic schemes, like the time translator of Aharonov et al. [5], while theoretically feasible, would operate under an astronomically small probability of success.

To address this issue, we propose here a class of non-relativistic scattering experiments. In these experiments, a number of particles are produced, let to propagate freely and subsequently measured after some time T'. Depending on the outcome of this measurement, the experiment is regarded as either a "success" or a "failure". When the scattering region holds n identical quantum systems of a dimension d and the experiment succeeds, then each system i will leap to the quantum state it would have had if it had been evolving unperturbed for time $T_i \neq T'$, where T_i can be negative. The experiment does not rely on any knowledge on the Hamiltonian of the target systems or their interaction with the scattered particles. Since they effect a high-level manipulation of the proper time of each system in the scattering region, such prepare-and-measure protocols can be regarded as a non-relativistic form of time warp.

*benjamindive@gmail.com

We find that, in this scenario, evolution time behaves as a resource: it cannot be created, but it can be transferred for free between identical systems. Hence, with a scattering experiment of duration T' we can transfer all the evolution time accumulated by the n systems to a single system, "fast-forwarding" the latter nT' time units to its future. Time can also be inverted, at a ratio of $\frac{1}{d-1}$. Combining the two approaches, we can invert such an aggregated time, thus projecting that same system $\frac{nT'}{d-1}$ time units to its past. By taking higher values of n, we can make these time warping effects increasingly dramatic.

In the special case of $n = 1$ our results resonate with those of [6]. In this regard, our present work shows that a single system can be rewinded to its past much faster than the protocols introduced in [6] allowed. The ability to speed up the evolution of a system by using multiple identical copies of it is, to the best of our knowledge, a wholly novel approach. Note that there exist other methods to invert an unknown unitary [7, 8, 9, 10], but they demand the ability to effect controlled quantum operations on the target system. We, however, only indirect control over the systems in the way detailed below.

Scenario

We consider a scenario where the experimental setup consists in two parts: a *controlled lab*, where we can prepare any quantum state and conduct any quantum operation; and a *scattering region*. The latter contains n identical physical *target systems* of Hilbert space dimension d at separate locations, see Fig.I. We assume that they remain in the same place during the course of the experiment. The initial (internal) quantum state of the n systems is unknown; for simplicity, we will take it pure and denote it by $|\psi_{1,\ldots,n}\rangle$.

If left unperturbed, each of these systems will independently evolve according to a (unknown) time-independent Hamiltonian H_0. That is, after time T the state of the n systems will evolve to

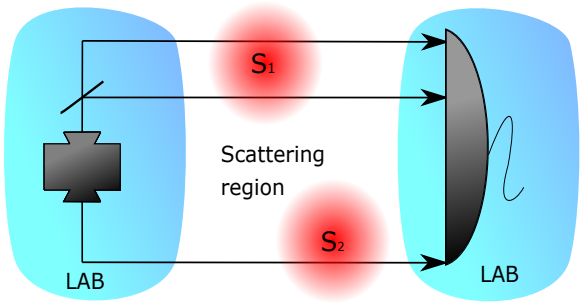


Figure I: **The setup.** The red circles represent the systems and their interaction radius, which are well separated to ensure the probes only interact with one at a time. The left section is the 'preparation' part of the the lab, where the probes in various quantum internal and external states can be created. After scattering with one of the systems, these probes are then measured (in the right section) in order to herald a successful run of the experiment.

$e^{-i\sum_{k=1}^{n} H_0^{(k)} T} |\psi_{1,...,n}\rangle$. To incorporate decay processes in this framework, we allow H_0 to be non-Hermitian.

In order to influence systems $k = 1, ..., n$, we can prepare a particle in the controlled lab and let it propagate within the scattering region. While in the scattering region, these particles or *probes* interact with each system k via the Hamiltonian $H_I(\vec{r} - \vec{q}_k)$, where $\vec{r}$ ($\vec{q}_k$) denotes the probe's (system k's) position. The joint state of systems $1, ..., n$ and P thus evolves as

$$i\frac{\partial}{\partial t} |\psi_{1,...,n,P}\rangle = H_P + \sum_{k=1}^{n} H_0^{(k)} + H_I^{(k,P)} |\psi_{1,...,n,P}\rangle \,, \tag{1}$$

where H_P denotes the free Hamiltonian of the probe. For technical reasons, H_I is assumed a bounded operator; otherwise H_I, H_0 and H_P are arbitrary and unknown.

We will allow multiple probes at a time within the scattering region. Although this could give rise to complex many-body interaction, we impose the additional condition, called the *targeting assumption*, that it is possible to prepare a probe in such a way that it interacts with a single uncontrolled system (its target) and nothing else. Such a probe will either return to the lab within a given time Δt and through a given channel or else be absorbed by the environment or lost in free space. Moreover, if several probes with different targets are prepared simultaneously, then the evolution of each probe and its target will be independent and identical among the different pairs of probe-uncontrolled system. Meanwhile, those uncontrolled systems without a targeting probe will keep evolving through H_0.

While they are in the lab, we have the ability to create probes in any state (such as entangling multiple probes together or with a quantum memory), and to perform arbitrary measurements on them. Note that the targeting assumption can be justified in many experimental setups where the uncontrolled systems are sufficiently separated in space. Throughout the text, we will further assume that Δt can be taken arbitrarily small.

The scattering protocol ends at time $t = T'$, when we conduct a dichotomic heralding measurement over the quantum registers present in the lab. If the outcome is "success", we expect the state of systems $1, ..., n$ to be

$$|\psi'_{1,...,n}\rangle = U(T_1, ..., T_n) |\psi_{1...,n}\rangle \,, \tag{2}$$

with $U(T_1, ..., T_n) = \bigotimes_{k=1}^{n} e^{-iH_0 T_k}$.

We will be mainly interested in whether such a time-warping experiment is possible, disregarding its actual probability of success: we just demand that the latter is non-zero for generic H_0, H_I, H_P. Note, e.g., that if the probes do not interact with the uncontrolled systems at all, then Eq.(2) can only hold if $T_1 = T_2 = ... = T_n = T'$.

Results

We have proved that, within the broad constraints described above, a scattering experiment of duration T' leading to Eq.(2) can only be possible if

$$\sum_{i:T_i>0} T_i + \sum_{i:T_i<0} |T_i|(d-1) \leq nT'. \tag{3}$$

Furthermore, we have shown that any set of T_i that satisfy this relation with time T' can be reached in a physical time of $T' + \epsilon$ for arbitrarily small ϵ, and provide an explicit protocol to realize it. The proof for these statements is available in the authors' paper [11] and its appendices.

The meaning behind Eq.(3) is best demonstrated by considering a few different cases. For $n = 1$, this implies that $T_1 \in [-\frac{T'}{d-1}, T']$. It means that, in principle, we could invert the evolution of the uncontrolled system in the scattering region. This is similar to what was done in [6], however, they required an experiment of duration $T' = O(d^2)|T_1|$, as opposed to $T' = (d-1)|T_1|$. The latter bound is consistent with the work of [10], where the authors prove that, in order to invert a unitary probabilistically (in a controlled system), at least $d-1$ uses thereof are needed.

For $n = 1$, Eq.(3) also implies that one cannot *fast-forward* the uncontrolled system. That is, in order to effect the transformation $|\psi_1\rangle \to U(T_1)|\psi_1\rangle$, with $T_1 > 0$, then one needs to invest, at least, time T_1. That this is impossible for unknown Hamiltonians was already established in [12, 13, 14]; we show that this is also true even for arbitrarily small probabilities of success.

Fast-forwarding is compatible with Eq.(3) only when there is more than one uncontrolled system within the scattering region, such as with configuration $T_1 = nT', T_2 = ... = T_n = 0$. This opens the door to projecting a single uncontrolled system to its far future at the cost of freezing the evolution of the rest during the scattering process. A second plausible configuration is $T_1 = -\frac{nT'}{d-1}, T_2 = ... = T_n = 0$. For $n \gg d$, this configuration would propagate system 1 to its far past while

keeping the rest of the systems unchanged. Indeed, provided that enough systems are available and we are content with a small probability of success, there is not limit as to how much the evolution of a system can be sped up.

With this, we interpret Eq.(3) as being equivalent to the following postulates about evolution time:

1. It cannot be created,
2. It can be destroyed,
3. It can be transferred between two identical systems at no cost,
4. It can be inverted at a cost $(d-1)$.

Examples

We now give some simple examples to demonstrate protocols which realize the maximal time reversal or time concentration permitted by Eq.(3). To do this it is useful to introduce some notation. The free evolution of a single system for time δT is denoted by $V = \exp^{-iH_0\delta T}$. If the system is however interacting with a probe originally in the state $|a\rangle$, and eventually post-selected to the state $|b\rangle$, for time δT then the evolution of the probe is given by $|\psi(\delta T)\rangle = W_{b,a}\,|\psi(0)\rangle$ where

$$W_{b,a} = \langle b|\, W\, |a\rangle = \langle b|\, \mathcal{T} e^{-i\int_0^{\delta T} H_0 + H_I(t)dt}\, |a\rangle\,. \qquad (4)$$

By sending (or not sending) probes in various states the systems can be made to evolve under a product of V's and $W_{b,a}$'s. Going beyond that, by entangling the probes before sending them out the a sum of such sequences can also be realized. Constructing a protocol to manipulate time remotely therefore comes down to constructing polynomials of V's and $W_{b,a}$'s with the desired properties.

Consider the case where we place a single qubit in the scattering area, $n = 1, d = 2$, where we wish to send the system backwards. That is, we want it to evolve according to V^{-m}. This can be done using the following relation

$$V^{-m} \propto [W_{a,a}, V]V^m[W_{a,a}, V] \qquad (5)$$

which holds for any 2×2 matrices $W_{a,a}, V$. This can be proved by an explicit parameterization of the matrices, but more generally can be shown using the theory of matrix polynomials as is done in our paper [11]. If the protocol is a success then the system behaves as if it had evolved backwards for $m\delta T$, while the lab time taken to do this is $(m+4)\delta T$. By taking m large the constant factor can be neglected and we can reach the bounding case of Eq.(3).

To implement this protocol with linear optics, one can use photons as probes and their polarization as the internal degree of freedom.The protocol and a schematic of the experimental set up is detailed step-by-step in Fig.II.

Assuming that the unitaries describing the evolution of the system and its interaction with the photon are chosen randomly according to the Haar measure, the average probability of success of this scheme, which happens to be independent of m, is $4.24\% \pm 0.06\%$. This figure can be substantially improved to $12.6\% \pm 0.1\%$ by allowing higher-rank measurements, such that the final evolution is $[W_{V,H}, V]V^m[W_{V,H}, V] + [W_{H,H}, V]V^m[W_{H,H}, V]$.

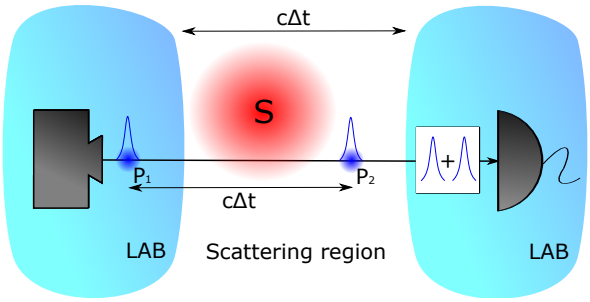


Figure II: **Schematic of the resetting protocol with photonic probe.** We prepare a photon in a superposition of positions, $\frac{1}{\sqrt{2}}(|p_1\rangle - |p_2\rangle)$, and in the polarization state $|H\rangle$ where $|p_1\rangle$ is a sufficiently delayed version of $|p_2\rangle$ The photon's path degree of freedom is post-selected to the state $\frac{1}{\sqrt{2}}(|p_1\rangle + |p_2\rangle)$, and its polarization to $|H\rangle$, then the state of the system will evolve as $|\psi_1\rangle \to \frac{1}{2}[W_{H,H}, V]\,|\psi_1\rangle$. Next, we let the system evolve by itself for time $T' = m\Delta t$; hence evolving the new state to $\frac{1}{2}V^m[W_1, V]\,|\psi_1\rangle$. Third, we repeat the first operation with a new photon. If the outcome of the measurements are the same, then the final state of the system will be $\frac{1}{4}[W_{H,H}, V]V^m[W_{H,H}, V]\,|\psi_S\rangle \propto V^{-m}\,|\psi_S\rangle$

As well as reversing time, we considered the experimental feasibility of implementing a fast-forwarding protocol using two qubit systems, $n = 2, d = 2$. A primitive tool necessary to do this is to a swap operator, S, between the two qubit systems. This requires a minimum of 5 qubit probes in a highly entangled initial state. Combining two such swaps and some periods of free evolution, it is possible to realise an operator proportional to

$$V^{2m} \otimes \mathbb{I} \propto (V^m \otimes \mathbb{I})S(\mathbb{I} \otimes V^m)S. \qquad (6)$$

This can be done in physical time $(m+k)\delta T$ for a fixed k. By taking m large, this results in one system not evolving at all, while the other evolves twice as fast, thereby also reaching the limit imposed by Eq.(3)

In summary, we have characterized how one can probabilistically warp the evolution time of an ensemble of uncontrolled systems of known dimensionality by means of scattering experiments. We have seen that, in such scenarios, evolution time behaves like a material resource, in the sense that it can be transferred and wasted, but not created. It can also be inverted, at a cost, via an irreversible process. Although at the end of the paper we provided simple instances of scattering protocols with a reasonably high (average) probability of success, our general constructions most likely represent very improbable processes, although we do not know of any bounds on the maximum possible likelihood of success.

Seeing evolution time as a resource with known rules governing how it can be manipulated presents a fundamentally new viewpoint on one of most fundamental physical concepts - time.

References

[1] D. Ivey and J. Hume, *Physics*, no. v. 1 in Physics (Ronald Press, 1974).

[2] C. Simak, *Time is the Simplest Thing*, Gateway Essentials (Orion, 2011), ISBN 9780575122383.

[3] K. Gödel, Rev. Mod. Phys. **21**, 447 (1949).

[4] K. Thorne, *Black Holes and Time Warps: Einstein's Outrageous Legacy*, Commonwealth Fund Book Program (W.W. Norton, 1994), ISBN 9780393312768.

[5] Y. Aharonov, J. Anandan, S. Popescu, and L. Vaidman, Phys. Rev. Lett. **64**, 2965 (1990).

[6] M. Navascués, Phys. Rev. X **8**, 031008 (2018).

[7] I. S. B. Sardharwalla, T. S. Cubitt, A. W. Harrow, and N. Linden (2016), `arXiv:1602.07963`.

[8] E. L. Hahn, Phys. Rev. **80**, 580 (1950).

[9] W.-J. Kuo and D. A. Lidar, Phys. Rev. A **84**, 042329 (2011).

[10] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao (2018), `arXiv:1810.06944`.

[11] D. Trillo, B. Dive, and M. Navascues (2019), `arXiv:1810.06944`.

[12] Y. Atia and D. Aharonov, Nat. Comm. **8**, 1572 (2017).

[13] C. Arenz, D. I. Bondar, D. Burgarth, C. Cormick, and H. Rabitz (2018), `arXiv:1806.00444`.

[14] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. **101**, 180504 (2008).

Semi-device-independent certification of indefinite causal order

Jessica Bavaresco[1] * Mateus Araújo[2] † Časlav Brukner[1 3] ‡ Marco Túlio Quintino[4] §

[1] *Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria*
[2] *Institute for Theoretical Physics, University of Cologne, Zülpicher Strasse 77, 50937 Cologne, Germany*
[3] *Vienna Center for Quantum Science and Technology (VCQ), Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria*
[4] *Department of Physics, Graduate School of Science, The University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo 113-0033, Japan*

Abstract. When transforming pairs of independent operations, the fundamental rules of quantum theory allow for transformations that may act on the input operations in an indefinite causal order. The formalism of process matrices predicts statistics that ensure this phenomenon in a device-independent scenario, nevertheless, all physical implementations proposed so far are fully device-dependent. We introduce a semi-device-independent framework for certifying noncausal properties of process matrices in a intermediate regime and use it to analyse the quantum switch. We show that, although it can only lead to causal statistics in a device-independent scenario, it can exhibit noncausal properties in semi-device-independent scenarios.

Keywords: Semi-device-independent, causal order, higher-order operations, process matrix formalism

A common quantum information task consists in certifying that some uncharacterised source is preparing a system with some features. By making the assumption that the measurement devices are completely characterised, that is, that they are known exactly, it is possible to infer properties of the system. In this *device-dependent* scenario, fidelity of a quantum state with respect to a target state can be estimated, entanglement witnesses can be evaluated, and even complete characterisation of the source via state tomography is possible.

Remarkably, it is possible to certify properties of systems even without fully characterizing the measurement devices. In such a *device-independent* scenario it is only assumed that the measurements are done by separated parties and compose under a tensor product, which is justified by implementing them with a space-like separation. Under these circumstances, Bell scenarios can be used to certify properties like entanglement of quantum states, incompatibility of quantum measurements, or to perform device-independent state estimation via self-testing.

Since the assumptions are weaker, demonstrations of device-independent certification are usually experimentally challenging. For instance, although experimental device-independent certification of entanglement has been reported, its experimental difficulty has so far prevented its use in practical applications such as device-independent quantum key distribution and randomness certification.

An interesting middle ground is the *semi-device-independent* scenario, where assumptions are made about some parties but not others. Semi-device-independent schemes have been developed and extensively studied for the certification of entanglement and measurement incompatibility, known as EPR-steering, and applied to quantum key distribution protocols where some but not all parties can be trusted.

A close analogy can be developed with regard to the certification of indefinite causal order, as encoded in a *process matrix* [1]. A process matrix is a higher-order operation [2, 3, 4] – *i.e.* a transformation of quantum operations – that acts on independent sets of operations. Fundamental laws of quantum theory predict the existence of process matrices that act on these operations in a such a way that a well-defined causal order cannot be established among them. Process matrices with indefinite causal order were proven to be a powerful resource, outperforming causally ordered ones in tasks such as quantum channel discrimination, communication complexity, quantum computation, and inverting unknown unitary operations.

To certify that a process matrix in fact does not act in a causally ordered way, there are two standard methods available in the literature. The first is to evaluate a causal witness [5, 6]. Analogous to the evaluation of an entanglement witness, this method relies on detailed knowledge of the quantum operations being implemented, and, as such, it allows for a device-dependent certification. All experimental certifications of indefinite causal order to date either measure a causal witness [7, 8] or rely on similar device-dependent assumptions. The second method is the violation of a causal inequality, phenomenon which is also predicted by quantum mechanics [1, 9]. Analogous to the violation of a Bell inequality, this method does not rely on detailed knowledge of the quantum operations implemented by the parties, but rather only that they compose under a tensor product. As such, it allows for a device-independent certification. Although it would be highly desirable to perform such device-independent certification of indefinite causal order, no physical implementation of process matrices that would violate a causal

*jessica.bavaresco@oeaw.ac.at
†mateus.araujo@uni-koeln.de
‡caslav.brukner@univie.ac.at
§quintino@eve.phys.s.u-tokyo.ac.jp

inequality is currently known.

In this work, we introduce a semi-device-independent framework for certifying noncausal properties of process matrices that allows for an experimental certification of indefinite causal order that relies on fewer assumptions than previous ones.

Let us consider the following task: we are given a behaviour – a set of probabilty distributions – that describes the statistics of a quantum experiment. We analyse this behaviour in the process matrix formalism, that is, we assume that there exists a process matrix W and sets of local instruments $\{A_{a|x}\}$ and $\{B_{b|y}\}$ that give rise to this behaviour according to the rules of quantum theory. Without any information about W – *i.e.*, without direct assumptions about the process matrix – the goal is to verify whether it is *causally nonseparable*. Additionally, information about the instruments which were performed may or may not be given.

Causal nonseparability is the property that captures the notion of indefinite causal order in process matrices: a causally nonseparable process matrix is one that cannot be described as a classical mixture of process matrices that can only give rise to causally ordered behaviours [1]. In turn, the notion of causal order for behaviours is defined by the marginals independence of the other parties' choices of input [1].

The assumptions about the instruments can be split in three: device-dependent, -independent, and semi-device-independent. A device-dependent certification scenario is one in which the operations of all parties are fully characterised, *i.e.*, the whole matrix description of the elements of all applied instruments is known. A device-independent certification scenario is the opposite, no knowledge or assumption is made regarding the operations performed by any parties, not even the dimension of the linear spaces used to describe them. Finally, a semi-device-independent certification scenario is one in which at least one party is device-dependent, which is often called trusted, and at least one is device-independent, often called untrusted.

Definition 1 (Device-dependent certification) *Given a process behaviour $\{p^Q(ab|xy)\}$, that arises from known instruments $\{\overline{A}_{a|x}\}$ and $\{\overline{B}_{b|y}\}$ and an unknown bipartite process matrix, one certifies that this process matrix is causally nonseparable in a device-dependent way if*

$$p^Q(ab|\overline{A}_{a|x}\,,\overline{B}_{b|y}) \neq \mathrm{Tr}\left[(\overline{A}_{a|x}\otimes\overline{B}_{b|y})W^{sep}\right], \quad (1)$$

for all a,b,x,y, and for all causally separable process matrices W^{sep}.

Definition 2 (Device-independent certification) *Given a process behaviour $\{p^Q(ab|xy)\}$, that arises from unknown instruments and an unknown bipartite process matrix, one certifies that this process matrix is causally nonseparable in a device-independent way if*

$$p^Q(ab|xy) \neq \mathrm{Tr}\left[(A_{a|x}\otimes B_{b|y})W^{sep}\right] \quad (2)$$

for all a,b,x,y, and for all causally separable process matrices W^{sep} and all general instruments $\{A_{a|x}\}$ and $\{B_{b|y}\}$.

Definition 3 (Semi-device-independent certification) *Given a process behaviour $\{p^Q(ab|xy)\}$, that arises from unknown instruments on Alice's side, known instruments $\{\overline{B}_{b|y}\}$ on Bob's side, and an unknown bipartite process matrix, one certifies that this process matrix is causally nonseparable in a semi-device-independent way if*

$$p^Q(ab|x\,,\overline{B}_{b|y}) \neq \mathrm{Tr}\left[(A_{a|x}\otimes\overline{B}_{b|y})W^{sep}\right] \quad (3)$$

for all a,b,x,y, and for all causally separable process matrices W^{sep} and all general instruments $\{A_{a|x}\}$.

We remark an analogy with the entanglement certification problem in which behaviours are assumed to arise from quantum measurements performed on a quantum state. In the entanglement certification case, device-dependent scenarios are related to entanglement witnesses [10], device-independent scenarios to Bell nonlocality [11], and the semi-device-independent ones to EPR-steering [12].

The three definitions above set the basis of our framework. In this framework, we prove that, although all causally nonseparable process matrices can be certified in a device-dependent way, not all of them can be certified in semi-device-independent or fully device-independent scenarios. We characterize the sets of processes matrices that can be certified in each scenario and provide explicit examples.

In all three scenarios, we formulate our certification problems in terms of semidefinite programming (SDP), implying that they can be efficiently solved.

We then extend our framework to a tripartite case in which the third party is always in the future of the other two, and provide an extensive machinery that may be generalized to other multipartite scenarios. We apply our methods to study the noncausal correlations of the notorious *quantum switch* [13, 14].

On its first appearance, the quantum switch was defined as a higher-order transformation that maps quantum channels into quantum channels and it can be defined as the following. Let U_A and U_B be two unitary operators that act on the same space of a target state $|\psi\rangle^t$. Let $|c\rangle^c := \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, be a 'control' state that is able to coherently control the order in which the operations U_A and U_B are applied. The quantum switch acts as following:

$$\mathrm{switch}(U_A,U_B) = |0\rangle\langle 0|^c\otimes U_A\,U_B + |1\rangle\langle 1|^c\otimes U_B\,U_A. \quad (4)$$

When applied to the state $|c\rangle^c\otimes|\psi\rangle^t$, we have

$$\begin{aligned}\mathrm{switch}(U_A,U_B)|c\rangle\otimes|\psi\rangle = \alpha\,|0\rangle\otimes U_A\,U_B\,|\psi\rangle \\ + \beta\,|1\rangle\otimes U_B\,U_A\,|\psi\rangle.\end{aligned} \quad (5)$$

Physically, the equation above can be understood as the control qubit determining which unitary is going to

be applied first on the target state $|\psi\rangle$. If the control qubit is in the state $|0\rangle$ ($\alpha = 1, \beta = 0$), the unitary U_B is performed before the unitary U_A. If the control qubit is in the state $|1\rangle$ ($\alpha = 0, \beta = 1$), the unitary U_B is performed before the unitary U_A. In general, if the control qubit is in the state $|c\rangle = \alpha|0\rangle + \beta|1\rangle$, $\alpha \neq 0, \beta \neq 0$, the output state will be in a coherent superposition of two different causal orders.

We analyze the quantum switch in the process matrix formalism, similarly to Ref. [5]. We describe the quantum switch by a family of tripartite process matrices that is shared among three parties, Alice, Bob, and Charlie, for which Charlie is always in the future of Alice and Bob, and the causal order between Alice and Bob may or may not be well defined. An interesting property of the quantum switch is that it is a tripartite causally nonseparable process matrix, however, when the third party, Charlie, is traced out, it becomes a bipartite causally separable process matrix.

Since it is causally nonseparable, the quantum switch can be certified in a device-dependent scenario. However, remarkably, the quantum switch cannot produce noncausal correlations in a device-independent scenario [5].

In order to determine whether the quantum switch can be certified to be causally nonseparable in a semi-device-independent scenario, much like in the bipartite case, we make different assumptions about the knowledge of the operations performed by each party. We call *untrusted* (U) a party that is treated in a device-independent way and *trusted* (T) a party that is treated in a device-dependent way, and we use the convention Alice Bob Charlie for denoting the parties. For example, a scenario TTU means Alice = T (device-dependent), Bob = T (device-dependent), and Charlie = U (device-independent). The four inequivalent semi-device-independent tripartite scenarios are, hence, TTU, TUU, UTT, and UUT.

Firstly, we prove that in the UUT scenario, that is, a scenario in which only Charlie is trusted, the quantum switch cannot be certified to be causally nonseparable, just like in the fully device-independent way.

Secondly, we prove that the quantum switch can indeed be certified in the remaining semi-device-independent scenarios, TTU, TUU, and UTT, proving that it can demonstrate stronger noncausal properties than it was previously known.

We then calculate bounds for the robustness of the quantum switch's noncausal properties with respect to white noise in each scenario to show that they can, in principle, be certified in practical situations.

With this motivation in mind, we analise the recently reported experiments [15, 7, 8, 16] that claim to implement the quantum switch using optical interferometers to check whether, with their implemented setups, one could certify the causal nonseparability of the quantum switch in a semi-device-independent way. Up to now, all experimental results rely on, among other assumptions, complete knowledge of the instruments to certify of causal nonseparability, *i.e.*, they are fully device-dependent.

Using our machinery to analyse the experiments of Refs. [7] and [8], we concluded that the instruments used in these experiments could allow us to make a stronger claim than what was reported. More precisely, the instruments used to certify that the quantum switch is causally nonseparable on refs. [7] and [8] can lead to a semi-device-independent certification of the noncausal properties of the quantum switch in the TTU scenario, that is, even if the measurements of Charlie were not trusted.

The technical details and further results of this work can be found in the preprint article arXiv:1903.10526 [quant-ph] at https://arxiv.org/abs/1903.10526.

References

[1] O. Oreshkov, F. Costa, and Č. Brukner. Quantum correlations with no causal order. *Nat. Commun.* **3**, 1092 (2012).

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

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

[4] M. Araújo, A. Feix, M. Navascués, and Č. Brukner. A purification postulate for quantum mechanics with indefinite causal order. *Quantum* **1**, 10 (2017).

[5] M. Araújo, C. Branciard, F. Costa, A. Feix, Christina Giarmatzi, and Č. Brukner. Witnessing causal nonseparability. *New Journal of Physics* **17**, 102001 (2015).

[6] C. Branciard. Witnesses of causal nonseparability: an introduction and a few case studies. *Scientific Reports* **6**, 26018 (2016).

[7] Giulia Rubino, L. A. Rozema, A. Feix, M. Araújo, J. M. Zeuner, L. M. Procopio, Č. Brukner, and P. Walther. Experimental verification of an indefinite causal order. *Science Advances* **3**, 3 (2017).

[8] K. Goswami, Christina Giarmatzi, M. Kewming, F. Costa, C. Branciard, Jacquiline Romero, and A. G. White. Indefinite causal order in a quantum switch. *Phys. Rev. Lett.* **121**, 090503 (2018).

[9] C. Branciard, M. Araújo, A. Feix, F. Costa, and Č. Brukner. The simplest causal inequalities and their violation. *New Journal of Physics* **18**, 013008 (2016).

[10] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A* **223**, 1–8 (1996).

[11] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–478 (2014).

[12] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.* **98**, 140402 (2007).

[13] G. Chiribella. Perfect discrimination of no-signalling channels via quantum superposition of causal structures. *Phys. Rev. A* **86**, 040301 (2012).

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

[15] L. M. Procopio, A. Moqanaki, M. Araújo, F. Costa, Irati Alonso Calafell, Emma G. Dowd, D. R. Hamel, L. A. Rozema, Č. Brukner, and P. Walther. Experimental superposition of orders of quantum gates. *Nat. Commun.* **6**, 7913 (2015).

[16] K. Goswami, Jacquiline Romero, and A.G. White. Communicating via ignorance. arXiv: 1807.07383 [quant-ph] (2018).

Communication through coherent control of quantum channels

Alastair A. Abbott[1 2 *] Julian Wechs[2] Dominic Horsman[3] Mehdi Mhalla[3] Cyril Branciard[2]

[1] *Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland*
[2] *Univ. Grenoble Alpes, CNRS, Grenoble INP, Institut Néel, 38000 Grenoble, France*
[3] *Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG, 38000 Grenoble France*

Abstract. A surprising recent result showed that, if two depolarising channels are applied in a superposition of different orders in a "quantum switch", then information can nevertheless be transmitted through the channels [1]. We show that a similar effect can be obtained by simply coherently controlling between sending a system through one of two identical depolarising channels, a situation with no indefinite causal order. When quantum channels are controlled coherently in this way, however, we find that information about their implementation is accessible in the output of the joint control-target system, allowing two different implementations of the same channel to be differentiated.

Keywords: quantum channels, coherent control, quantum communication, quantum switch

The ability to create superpositions of quantum states opens up many advantages for communication and information processing that are inaccessible to classical mixtures of states, exemplified by their use in controlled logic gates (e.g., CNOT) in quantum computing [2]. Recently, it has been shown that a coherent quantum control system can be used to even put the causal ordering of quantum channels into superposition, thus rendering it "indefinite", in the so-called "quantum switch" [3]. Surprisingly, when certain zero-capacity channels are placed in a quantum switch the resulting switched channels still allow information to be transmitted, something impossible if their causal ordering is fixed or controlled classically [1].

Motivated by the quantum switch, we revisit here the notion of coherent control of arbitrary quantum channels—something that has in the generally been considered problematic or, at best, subtle [4–7]—by exploiting a control system to determine which channel is used to transmit a state rather than the order in which two communication channels are used. We show here that it allows the counter-intuitive communication advantage of the switch mentioned above to be reproduced in the absence of any "causal indefiniteness": when each channel is maximally noisy, information can nonetheless be transmitted through the coherently multiplexed communication channels.

When controlled coherently in this way we find that—in contrast to the quantum switch [1, 3]—the action of the "global" multiplexed channel depends not only the descriptions of the individual channels as completely positive trace-preserving (CPTP) maps but also on more fine-grained information about their realisations. This includes, but goes beyond, relative phase information, highlighting the subtleties involved in describing "controlled channels": indeed as we will see, without extra information on the specific channel implementation the problem is in fact ill-defined.

The preprint paper associated to this abstract is available on the arXiv [8].

*alastair.abbott@unige.ch

1 Communication through the "depolarising quantum switch"

The quantum switch is a process comprising a coherent control qubit, a d-dimensional target system, and a pair of "black box" operations that, taken individually, implement some CPTP maps—so-called "quantum channels"—$\mathcal{C}_0$ and $\mathcal{C}_1$ on their input systems [3]. If the control qubit is in the state $|0\rangle^c$, then first $\mathcal{C}_0$ then $\mathcal{C}_1$ is applied to the target system, while if it is in the state $|1\rangle^c$ then the operations are in the opposite order. Initialising the control in the state $|+\rangle^c = \frac{1}{\sqrt{2}}(|0\rangle^c + |1\rangle^c)$ therefore applies the operations in a superposition of the two orders. Since, in this case, one cannot say that either operation is definitely applied before another, the quantum switch is said to exhibit indefinite causal order [3, 9].

In [1], it was observed that, if the CPTP maps $\mathcal{C}_i$ are taken to be fully depolarising channels $\mathcal{N}_i$ (which map any initial target state ρ^t_{in} to the maximally mixed state $\frac{\mathbb{1}^t}{d}$), then the switch (with the initial state of the control qubit fixed to $|+\rangle^c$) implements a global channel $\mathcal{S}[\mathcal{N}_0, \mathcal{N}_1]$ mapping ρ^t_{in} to the joint control-target state

$$\rho^{ct}_{\text{out}} = \frac{\mathbb{1}^c}{2} \otimes \frac{\mathbb{1}^t}{d} + \frac{1}{2}\left[|0\rangle\langle 1|^c + |1\rangle\langle 0|^c\right] \otimes \frac{1}{d^2}\rho^t_{\text{in}}\,, \qquad (1)$$

which is *not* $\frac{\mathbb{1}^t}{d}$ but instead retains some dependence on ρ^t_{in}. Thus, information can propagate through the "depolarising quantum switch" despite this being impossible for the channels $\mathcal{N}_0$, $\mathcal{N}_1$, $\mathcal{N}_1 \circ \mathcal{N}_0$, and $\mathcal{N}_0 \circ \mathcal{N}_1$ individually.

2 Communication through coherently-controlled depolarising channels

In a standard interferometric implementation of the quantum switch, the target system is routed to the switched operations, which here correspond to communication channels, via some beamsplitters [10–16]. In this contribution, we consider instead the state of the joint control-target system after traversing only half of such

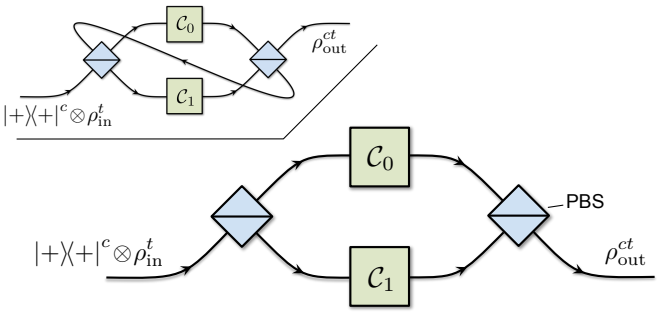


Figure 1: The inset shows a typical photonic implementation of the quantum switch [3, 17], in which the control qubit is encoded in the polarisation of a photon which is routed by polarising beamsplitters (PBS), and the target system is encoded in some internal degree of freedom of the photon (as e.g. in Refs. [13, 14]). Here we consider only the "first half" of the quantum switch process (main figure). This implements a coherent control between the two boxes implementing $\mathcal{C}_0$ and $\mathcal{C}_1$.

a quantum switch; that is, after the target system has passed, in a superposition, through the communication channels only a single time. This situation, a possible implementation of which is shown in Fig. 1, amounts to coherently controlling between applying the operations implementing $\mathcal{C}_0$ or $\mathcal{C}_1$ to the target system. By preparing the control qubit in the state $|+\rangle^c$, a "superposition" of the two operations is thus applied.

Let us consider, as in [1], the situation where the two operations implement fully depolarising channels ($\mathcal{C}_i = \mathcal{N}_i$) and, as done there, consider first the concrete case of a qubit target system ($d = 2$) where these channels are realised by randomising over a set of d^2 orthogonal unitary operators $\{U_i\}_{i=0}^{d^2-1}$. For each channel, one then indeed has $\mathcal{N}_{0/1}(\rho^t_{\text{in}}) = \frac{1}{d^2}\sum_i U_i \rho^t_{\text{in}} U_i^\dagger = \frac{\mathbb{1}^t}{d}$.

For each random choice of unitary operators (U_i, U_j), the control-target system therefore undergoes the unitary evolution $|0\rangle\langle 0|^c \otimes U_i + |1\rangle\langle 1|^c \otimes U_j$. If the control is initially in the state $|+\rangle^c$ and the target system is in some state $|\psi_{\text{in}}\rangle^t$, the joint system thus evolves to the state

$$|\Phi_{ij}\rangle^{ct} = \frac{1}{\sqrt{2}}\left(|0\rangle^c \otimes U_i |\psi_{\text{in}}\rangle^t + |1\rangle^c \otimes U_j |\psi_{\text{in}}\rangle^t\right). \quad (2)$$

Averaging over all choices of (U_i, U_j) one finds that the output state is

$$\begin{aligned}\rho^{ct}_{\text{out}} =& \frac{1}{d^4}\sum_{i,j} |\Phi_{ij}\rangle\langle\Phi_{ij}|^{ct} \\ =& \frac{\mathbb{1}^c}{2} \otimes \frac{\mathbb{1}^t}{d} + \frac{1}{2}\left[|0\rangle\langle 1|^c + |1\rangle\langle 0|^c\right] \otimes T\rho^t_{\text{in}}T^\dagger \end{aligned} \quad (3)$$

where $T := \frac{1}{d^2}\sum_i U_i$ and $\rho^t_{\text{in}} := |\psi_{\text{in}}\rangle\langle\psi_{\text{in}}|^t$. By linearity, Eq. (3) also holds for arbitrary ρ^t_{in}, and the setup thus gives rise to the global channel $\mathcal{M}$ mapping $\rho^t_{\text{in}} \to \rho^{ct}_{\text{out}}$.

It is immediately clear that ρ^{ct}_{out} depends in general on ρ^t_{in}, and thus some information can be transmitted through the setup. If, on the other hand, one classically controls which channel is applied to the input, no information can be transmitted. Thus, the global channel $\mathcal{M}$ arising from coherently controlling between $\mathcal{N}_0$ and $\mathcal{N}_1$ provides a communication advantage over classical control, mirroring that found using the quantum switch in [1]. In the example above, however, there is no indefinite causal order and yet the effect remains, contradicting any possible intuition that it should be attributed to causal indefiniteness.

Moreover, we present a lower bound on the amount of classical information that can be transmitted by a single use of the global channel $\mathcal{M}$ [8]. We find that significantly more information can be transmitted by this setup than with the full depolarising quantum switch [1] (e.g., for a qubit target, $\frac{1}{2}\log_2\frac{5}{4} \approx 0.16$ bits versus $-\frac{3}{8} - \frac{5}{8}\log_2\frac{5}{8} \approx 0.05$ bits with the depolarising quantum switch).

3 Implementation dependence

The approach employed above of randomising over unitary channels is not, however, the only way to implement a fully depolarising channel. In general, a quantum channel $\mathcal{C}$ is defined as a CPTP map, and can be described in terms of a (non-unique) set of Kraus operators $\{K_i\}_i$ satisfying $\sum_i K_i^\dagger K_i = \mathbb{1}$ [18]. However, if the channels $\mathcal{C}_0$ and $\mathcal{C}_1$ are not unitary (or described as a randomisation over unitary channels) it is *a priori* unclear how to determine the global channel mapping $\rho^t_{\text{in}} \to \rho^{ct}_{\text{out}}$ from the Kraus operators of $\mathcal{C}_0$ and $\mathcal{C}_1$.

One possible approach to doing so is to "purify" the channels via (independent) Stinespring dilations [19]. Any channel $\mathcal{C}$ with Kraus operators $\{K_i\}_i$ can indeed be extended to a unitary operation by introducing an environment in an initial state $|\varepsilon\rangle^e$ and considering the operation that acts on the system under consideration and the environment as $|\psi_{\text{in}}\rangle^t \otimes |\varepsilon\rangle^e \to \sum_i K_i |\psi_{\text{in}}\rangle^t \otimes |i\rangle^e := |\Phi_{\text{out}}\rangle^{te}$. After tracing out the environment, one recovers $\text{Tr}_e |\Phi_{\text{out}}\rangle\langle\Phi_{\text{out}}|^{te} = \mathcal{C}(|\psi_{\text{in}}\rangle\langle\psi_{\text{in}}|^t)$.

In the setup of Fig. 1 where the channels $\mathcal{C}_0$ and $\mathcal{C}_1$ have Kraus operators $\{K_i\}_i$ and $\{L_j\}_j$, respectively, one may therefore purify the channels by introducing two, initially uncorrelated, environments with initial states $|\varepsilon_0\rangle^{e_0}$ and $|\varepsilon_1\rangle^{e_1}$. Under these controlled, purified channels, the combined control-target-environments state evolves unitarily as

$$\begin{aligned}&|+\rangle^c \otimes |\psi_{\text{in}}\rangle^t \otimes |\varepsilon_0\rangle^{e_0} \otimes |\varepsilon_1\rangle^{e_1} \\ &\to \frac{1}{\sqrt{2}}|0\rangle^c \otimes \sum_i K_i |\psi_{\text{in}}\rangle^t \otimes |i\rangle^{e_0} \otimes |\varepsilon_1\rangle^{e_1} \\ &\quad + \frac{1}{\sqrt{2}}|1\rangle^c \otimes \sum_j L_j |\psi_{\text{in}}\rangle^t \otimes |\varepsilon_0\rangle^{e_0} \otimes |j\rangle^{e_1}. \end{aligned} \quad (4)$$

After tracing out the environments, the resulting joint control-target state ρ^{ct}_{out} is found to be

$$\begin{aligned}\rho^{ct}_{\text{out}} =& \frac{1}{2}\left[|0\rangle\langle 0|^c \otimes \mathcal{C}_0(\rho^t_{\text{in}}) + |1\rangle\langle 1|^c \otimes \mathcal{C}_1(\rho^t_{\text{in}})\right] \\ &+ \frac{1}{2}\left[|0\rangle\langle 1|^c \otimes T_0\rho^t_{\text{in}}T_1^\dagger + |1\rangle\langle 0|^c \otimes T_1\rho^t_{\text{in}}T_0^\dagger\right] \end{aligned} \quad (5)$$

with $T_0 := \sum_i \langle\varepsilon_0|i\rangle K_i$ and $T_1 := \sum_j \langle\varepsilon_1|j\rangle L_j$.

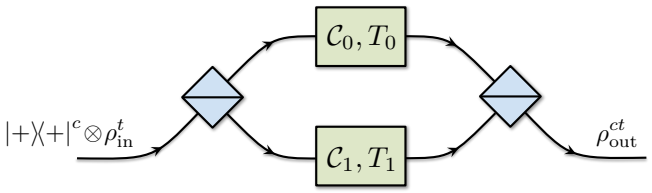


Figure 2: A corrected version of Fig. 1 in which the description of the two operations inside the interferometer, implementing the channels $\mathcal{C}_0$ and $\mathcal{C}_1$ on their respective subspaces, have been supplemented by the transformation matrices T_0 and T_1 needed to fully specify ρ^{ct}_{out}.

The output state (3) is recovered by taking $K_i = \frac{1}{d}U_i$, $L_j = \frac{1}{d}U_j$, and the initial states of the environment to be $|\varepsilon_0\rangle^{e_0} = \sum_{i=0}^{d^2-1} \frac{1}{d} |i\rangle^{e_0}$, $|\varepsilon_1\rangle^{e_1} = \sum_{j=0}^{d^2-1} \frac{1}{d} |j\rangle^{e_1}$. However, it is clear that a different choice of orthogonal unitary operations or, indeed, any other set of Kraus operators for depolarising channels would generally lead to a different output state in Eq. (5).

The crucial observation here is thus that ρ^{ct}_{out} depends on the implementation of the channels $\mathcal{C}_0$ and $\mathcal{C}_1$ [20, 21]. The interferometric circuit in Fig. 1 is therefore not fully defined by the channels $\mathcal{C}_0$ and $\mathcal{C}_1$, or the Kraus operators chosen to represent them. This may appear surprising given that, in the usual paradigm, quantum channels are understood to be fully characterised by their (non-unique) Kraus representation [2, 18, 22]. However, one should note that such a description of a channel is unchanged under addition of any global phase. On the other hand, any such "global" phase applied by one of the channels in Fig. 1 is only applied to the corresponding arm of the interferometer and therefore, in the overall controlled circuit, becomes a "relative" phase with physical significance. In the case where the channels $\mathcal{C}_0$ and $\mathcal{C}_1$ are unitary, the fact that Fig. 1 is only defined up to such a phase on the unitaries is well known [23, 24].

What we see here, however, is that the output of the interferometric circuit depends not only on any relative phases between (the Kraus operators of) the two channels, but also on a more detailed description of the implementation of the channels. More precisely, one requires some additional information encoded in the matrices T_0, T_1 introduced in Eq. (5) in order to fully specify the global channel $\mathcal{M}[\mathcal{C}_0, T_0, \mathcal{C}_1, T_1] : \rho^t_{\text{in}} \to \rho^{ct}_{\text{out}}$ induced by the circuit; see Fig. 2. We call these the "transformation matrices" of the channel implementations. In the description above in terms of a Stinespring dilation, these depend not only on the set of Kraus operators used to decompose the channel, but also on how these are combined (with coefficients that depend on the environment states) to define $T_0 := \sum_i \langle\varepsilon_0|i\rangle K_i$ and $T_1 := \sum_j \langle\varepsilon_1|j\rangle L_j$.

We characterise completely the transformation matrices T obtainable from some realisation of any given channel $\mathcal{C}$, by deriving a general constraint expressed in terms of the Choi representations [25] of $\mathcal{C}$ and T [8]. For a d-dimensional fully depolarising channel, for instance, this constraint simplifies to $\text{Tr}[T^\dagger T] \leq \frac{1}{d}$. Under this constraint, applied to both T_0 and T_1, Eq. (5) characterises all possible output states that one can obtain from the setup of Fig. 2, for any implementation of the channels $\mathcal{C}_0, \mathcal{C}_1 = \mathcal{N}$.

4 Distinguishing different implementations of coherently-controlled channels

The dependence of the output of the circuit of Fig. 2 on the implementation of the channels means that it is also possible to differentiate between two distinct implementations of the same quantum channel with different transformation matrices.

Consider the case where the channel $\mathcal{C}_0$ has a single, fixed implementation with a transformation matrix T_0, while the channel $\mathcal{C}_1$ can have two different possible implementations, with $T_1 \neq T_1'$. The global channels $\mathcal{M}_{T_1} := \mathcal{M}[\mathcal{C}_0, T_0, \mathcal{C}_1, T_1]$ and $\mathcal{M}_{T_1'} := \mathcal{M}[\mathcal{C}_0, T_0, \mathcal{C}_1, T_1']$ thus differ in general. If T_1 and T_1' are equally probable, then the maximal probability of successfully distinguishing the two channels—and thereby the two implementations of $\mathcal{C}_1$—is $\frac{1}{2}(1 + \mathcal{D}(\mathcal{M}_{T_1}, \mathcal{M}_{T_1'}))$, where $\mathcal{D}(\mathcal{M}_{T_1}, \mathcal{M}_{T_1'}) := \frac{1}{2}\|\mathcal{M}_{T_1} - \mathcal{M}_{T_1'}\|_\diamond$ is the diamond-norm distance between the two global channels [26]. We show that [8]

$$\mathcal{D}(\mathcal{M}_{T_1}, \mathcal{M}_{T_1'}) \leq \frac{1}{2}\left\|T_1 - T_1'\right\|_2 \tag{6}$$

(where $\|\cdot\|_2$ is the spectral norm), and that this upper bound can be reached with $\mathcal{C}_0 = \mathcal{I}$, $T_0 = \mathbb{1}$, in which case it is obtained by taking the input state $\rho^t_{\text{in}} = |\psi_{\text{in}}\rangle\langle\psi_{\text{in}}|$ maximising $\langle\psi_{\text{in}}| (T_1 - T_1')^\dagger (T_1 - T_1') |\psi_{\text{in}}\rangle$. One then discriminates the channels by performing optimal state discrimination between the corresponding output states ρ^{ct}_{out} and $\rho^{ct\,\prime}_{\text{out}}$ of the two global channels.

For two different implementations of a depolarising channel $\mathcal{C}_1 = \mathcal{N}$ with the transformation matrices $T_1^{(\prime)} = \pm\frac{1}{\sqrt{d}} |0\rangle\langle 0|$ one has $\frac{1}{2}\left\|T_1 - T_1'\right\|_2 = \frac{1}{\sqrt{d}}$, so that these two implementations of the depolarising channel can be distinguished with probability $\frac{1}{2}(1 + \frac{1}{\sqrt{d}})$. This turns out to be the optimal discrimination probability for any pair of implementations of $\mathcal{N}$ [8].

5 Conclusions

Our results show that coherent control of quantum channels is a powerful resource for communication through noisy channels [27], allowing classical information to be transmitted through completely depolarising channels and even quantum information through completely dephasing channels [8, 28, 29]. Our analysis illuminated the fact that the output of the circuit in Fig. 2 depends on the implementation of whatever channels are used, and the description of the channels as a CPTP maps must be supplemented by the "transformation matrices" T we introduced to fully describe their action. This "implementation dependence" stands in contrast to the usual paradigm of quantum channels as CPTP maps, opening the door for novel uses of coherent control as a tool for analysing channels.

References

[1] D. Ebler, S. Salek, and G. Chiribella, Enhanced communication with the assistance of indefinite causal order, Phys. Rev. Lett. **120**, 120502 (2018).

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, NY, USA, 2011).

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

[4] M. Araújo, A. Feix, F. Costa, and Č. Brukner, Quantum circuits cannot control unknown operations, New J. Phys. **16**, 093026 (2014).

[5] N. Friis, V. Dunjko, W. Dür, and H. J. Briegel, Implementing quantum control for unkown subroutines, Phys. Rev. A **89**, 030303(R) (2014).

[6] T. M. Rambo, J. B. Altepeter, P. Kumar, and G. M. D'Ariano, Functional quantum computing: An optical approach, Phys. Rev. A **93**, 052321 (2016).

[7] J. Thompson, K. Modi, V. Vedral, and M. Gu, Quantum plug n' play: modular computation in the quantum regime, New J. Phys. **20**, 013004 (2018).

[8] A. A. Abbott, J. Wechs, D. Horsman, M. Mhalla, and C. Branciard, Communication through coherent control of quantum channels (2018), arXiv:1810.09826 [quant-ph].

[9] O. Oreshkov, F. Costa, and Č. Brukner, Quantum correlations with no causal order, Nat. Commun. **3**, 1092 (2012).

[10] L. M. Procopio, A. Moqanaki, M. Araújo, F. Costa, Irati Alonso C., E. G. Dowd, D. R. Hamel, L. A. Rozema, Č. Brukner, and P. Walther, Experimental superposition of orders of quantum gates, Nat. Commun. **6**, 7913 (2015).

[11] G. Rubino, L. A. Rozema, A. Feix, M. Araújo, J. M. Zeuner, L. M. Procopio, Č. Brukner, and P. Walther, Experimental verification of an indefinite causal order, Sci. Adv. **3**, e1602589 (2017).

[12] G. Rubino, L. A. Rozema, F. Massa, M. Araújo, M. Zych, Č. Brukner, and P. Walther, Experimental entanglement of temporal orders (2017), arXiv:1712.06884 [quant-ph].

[13] K. Goswami, C. Giarmatzi, M. Kewming, F. Costa, C. Branciard, J. Romero, and A. G. White, Indefinite causal order in a quantum switch, Phys. Rev. Lett. **121**, 090503 (2018).

[14] K. Goswami, J. Romero, and A. G. White, Communicating via ignorance (2018), arXiv:1807.07383 [quant-ph].

[15] K. Wei, N. Tischler, S.-R. Zhao, Y.-H. Li, J. M. Arrazola, Y. Liu, W. Zhang, H. Li, L. You, Z. Wang, Y.-A. Chen, B. C. Sanders, Q. Zhang, G. J. Pryde, F. Xu, and J.-W. Pan, Experimental quantum switching for exponentially superior quantum communication complexity, Phys. Rev. Lett. **122**, 120504 (2019).

[16] Y. Guo, X.-M. Hu, Z.-B. Hou, H. Cao, J.-M. Cui, B.-H. Liu, Y.-F. Huang, C.-F. Li, and G.-C. Guo, Experimental investigating communication in a superposition of causal orders (2018), arXiv:1811.07526 [quant-ph].

[17] M. Araújo, F. Costa, and Č. Brukner, Computational Advantage from Quantum-Controlled Ordering of Gates, Phys. Rev. Lett. **113**, 250402 (2014).

[18] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013).

[19] W. F. Stinespring, Positive functions on c^*-algebras, Proc. Amer. Math. Soc. **6**, 211–216 (1955).

[20] J. Åberg, Subspace preservation, subspace locality, and gluing of completely positive maps, Ann. Phys. **313**, 326 – 367 (2004).

[21] D. K. L. Oi, Interference of quantum channels, Phys. Rev. Lett. **91**, 067902 (2003).

[22] K. Kraus, *States, Effects, and Operations: Fundamental Notions of Quantum Theory* (Springer-Verlag, Berlin Heidelberg, 1983).

[23] X.-Q. Zhou, P. Kalasuwan, T. C. Ralph, and J. L. O'Brien, Calculating unknown eigenvalues with a quantum algorithm, Nat. Photonics **7**, 223 (2013).

[24] A. Bisio, M. Dall'Arno, and P. Perinotti, Quantum conditional operations, Phys. Rev. A **94**, 022340 (2016).

[25] M.-D. Choi, Completely positive linear maps on complex matrices, Linear Algebra Appl. **10**, 285–290 (1975).

[26] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, 2018).

[27] N. Gisin, N. Linden, S. Massar, and S. Popescu, Error filtration and entanglement purification for quantum communication, Phys. Rev. A **72**, 012338 (2005).

[28] S. Salek, D. Ebler, and G. Chiribella, Quantum communication in a superposition of causal orders (2018), arXiv:1809.06655 [quant-ph].

[29] G. Chiribella, M. Banik, S. S. Bhattacharya, T. Guha, M. Alimuddin, A. Roy, S. Saha, S. Agrawal, and G. Kar, Indefinite causal order enables perfect quantum communication with zero capacity channel (2018), arXiv:1810.10457 [quant-ph].

Randomized Partial Decoupling Unifies One-Shot Quantum Channel Capacities

Eyuri Wakakuwa[1] * Yoshifumi Nakata[2 3 4]

[1] *Department of Communication Engineering and Informatics, Graduate School of Informatics and Engineering, The University of Electro-Communications, 182-8585, Japan*
[2] *Photon Science Center, Graduate School of Engineering, The University of Tokyo, 113-8656, Japan*
[3] *Yukawa Institute for Theoretical Physics, Kyoto university, 606-8502, Japan*
[4] *JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*

Abstract. We analyze a task in which classical and quantum messages are communicated via a noisy quantum channel, assisted with shared entanglement. We derive a one-shot capacity region in terms of the smooth conditional entropies. The direct and converse bounds for various communication tasks are obtained as corollaries, both for one-shot and asymptotic scenario. The proof is based on the *randomized partial decoupling theorem*, which is a generalization of the decoupling theorem and may be of independent interest. Thereby we provide a unified decoupling approach to the one-shot quantum channel coding, by fully incorporating classical communication, quantum communication and entanglement.

Keywords: one-shot information theory, decoupling, quantum channel coding, smooth entropy

1 Background

The major goals of quantum communication theory is to investigate the ultimate capacity of a noisy quantum channel for transmitting classical and quantum information, and to analyze the maximum amount of pure entanglement or secrecy that can be extracted from a mixed quantum states [1]. In an asymptotic scenario of infinitely many copies and vanishingly small error, Ref. [2] provided a unified approach for the two goals. This result was subsequently developed into quantum state merging [3] and the fully quantum Slepian-Wolf (FQSW) protocol [4]. Quite remarkably, various coding theorems including quantum capacity theorems are obtained by reduction from FQSW [4]. These results provided a unified picture for various quantum communication tasks, referred to as the protocol family [4, 5].

The concept of decoupling plays a crucial role in the above analyses of quantum protocols. Decoupling refers to the fact that we may destroy correlation between two quantum systems by applying an operation on one of the two subsystems. The decoupling approach simplifies many problems of our interest, particularly when combined with the fact that any purification of a mixed quantum state is convertible to another reversibly [6]. This enables us to prove the existence of a decoder for quantum communication without explicitly constructing it.

*e.wakakuwa@gmail.com

The decoupling approach to quantum protocols has been generalized to the one-shot scenario. Ref. [7] proved one of the most general formulations of decoupling, which is referred to as the *decoupling theorem*. The decoupling theorem provides necessary and sufficient conditions for an operation to decouple a quantum state with high precision, in terms of smooth min- and max- entropies of the operation and the state. In the same way as in the asymptotic scenario, various coding theorems can be obtained by reduction from the decoupling theorem in the one-shot scenario [8]. Furthermore, due to the fully quantum asymptotic equipartition property [9], the results also lead to reconstruction of the existing results in an asymptotic scenario.

There is, however, a limitation in the decoupling approach, in that it does not incorporate classical communication tasks. Although Ref. [10] addressed classical communication by a decoupling-like approach based on the *dequantizing theorem*, it does not fully incorporate a general scenario, in which classical and quantum messages are simultaneously transmitted, possibly with the assistance of shared entanglement. For addressing this scenario by the existing decoupling methods, it is necessary to apply the decoupling theorem and the dequantizing theorem separately for the two sources (see also Refs. [11] for a different approach based on the convex splitting). In this sense, the unified approach to quantum communication based on decoupling has not been fully completed.

2 Our Contribution

In this paper, we propose a unified decoupling approach that can incorporate classical communication, quantum communication and entanglement simultaneously. I.e., we consider a task in which classical and quantum messages are transmitted via a noisy quantum channel with the assistance of shared entanglement. This task was analyzed in [12] for an asymptotic scenario, whereas we consider the one-shot scenario based on the decoupling approach. The main result is that we derive the one-shot capacity region for this task. The bounds are simply represented in terms of the amount of shared entanglement, the lengths of classical and quantum messages to be transmitted, and the smooth conditional entropy of the channel. The direct and converse bounds for various communication tasks are obtained as corollaries, both for one-shot and asymptotic scenario. Thereby we complete the decoupling approach for quantum channel coding.

The proof is based on the *randomized partial decoupling theorem* [13], which is a generalization of the decoupling theorem and may be of independent interest. Here, we consider a scenario in which a bipartite quantum state on system AR is subject to a unitary operation on A, followed by the action of a quantum channel (CP map). The subsystem is decomposed into a direct-sum form, and the unitary is chosen at random from the set of unitaries that are block-diagonal under the decomposition. Along the similar line as [7], we analyze how close the final state is, on average over the unitaries, to the averaged final state. We derive upper and lower bounds on the average distance between the final state and the averaged one. The bounds are represented simply in terms of smooth conditional entropies of the initial state and the channel. The existing results on one-shot decoupling [7] and dequantization [10] are obtained from this result as corollaries (see Section III D in [13] for the details).

3 One-Shot Capacity Region

We consider a scenario in which Alice transmits classical and quantum messages simultaneously through a noisy quantum channel assisted with shared entantlement. We assume that, initially, Bob has no side information about the messages. We denote by c and q the numbers of classical and quantum bits that are to be transmitted. Let S_c, R_c and S_r, R_r be quantum systems of dimension 2^c and 2^q, respectively. The source is modeled by a state $\Phi'^{SR}_{c,q} = \frac{1}{2^c}\sum_{j=1}^{2^c} |j\rangle\langle j|^{S_c} \otimes |j\rangle\langle j|^{R_c} \otimes |\Phi_{2^q}\rangle\langle\Phi_{2^q}|^{S_rR_r}$, where Φ_{2^q} is the maximally entangled state with the Schmidt rank 2^q. The available resources are a noisy quantum channel $\mathcal{N}^{C\to D}$ and a pure entangled state $\Phi_{2^e}^{F_AF_B}$ shared in advance. The dimension of A is not necessarily the same as the dimension of the input space C of the channel.

The first main result of this submission is that we derive the one-shot capacity region for this scenario. The direct and converse parts are separately represented by the following two theorems:

Theorem 1 (direct part) *Consider a source state defined by* $\Phi'^{SR}_{c,q} = \frac{1}{2^c}\sum_{j=1}^{2^c} |j\rangle\langle j|^{S_c} \otimes |j\rangle\langle j|^{R_c} \otimes |\Phi_{2^q}\rangle\langle\Phi_{2^q}|^{S_rR_r}$ *and a resource state* $\Phi_{2^e}^{F_AF_B}$. *Let* $\mathcal{N}^{C\to D}$ *be a quantum channel, and let* A_r *be a quantum system such that* $\dim A_r \geq 2^{q+e}$. *For any* $J \geq 2^c$, *there exists an encoding CPTP map* $\mathcal{E}^{SF_A\to C}$ *and a decoding CPTP map* $\mathcal{D}^{DF_B\to S}$ *such that*

$$\left\| \mathcal{D}\circ\mathcal{N}\circ\mathcal{E}(\Phi'^{SR}_{c,q}\otimes\Phi_{2^e}^{F_AF_B}) - \Phi'^{SR}_{c,q} \right\|_1 \leq 2\sqrt{2}\cdot\sqrt[4]{\delta},$$

if there exists a normalized state in the form of $\rho^{AC} = \frac{1}{J}\sum_{j=1}^{J} |j\rangle\langle j|^{A_c} \otimes |\rho_j\rangle\langle\rho_j|^{A_rCC'}$ *that satisfies the following inequalities:*

$$\begin{aligned}
c+q+e &\leq -H_{\max}^{\delta/4}(A_cA_r|CC')_\rho + \log(J-1) + g(\delta),\\
q+e &\leq -H_{\max}^{\delta/4}(A_r|CC'A_c)_\rho + g(\delta),\\
c+q-e &\leq -H_{\max}^{\delta/4}(A_cA_r|D)_{\mathcal{N}(\rho)} + \log(J-1) + g(\delta),\\
q-e &\leq -H_{\max}^{\delta/4}(A_r|DA_c)_{\mathcal{N}(\rho)} + g(\delta),
\end{aligned}$$

where $g(\delta) := \log(4\delta^2)$.

Theorem 2 (converse part) *Consider the same setting as in Theorem 1, and suppose that there exists an encoding CPTP map* $\mathcal{E}^{SF_A\to C}$, *and a decoding CPTP map* $\mathcal{D}^{DF_B\to S}$ *such that* $\|\mathcal{D}\circ\mathcal{N}\circ\mathcal{E}(\Phi'^{SR}_{c,q}\otimes\Phi_{2^e}^{F_AF_B}) - \Phi'^{SR}_{c,q}\|_1 \leq \delta$. *Then, for any* $J \geq 2^c$, *there exists a state in the form of* $\rho^{ACC'} = \frac{1}{J}\sum_{j=1}^{J} |j\rangle\langle j|^{A_c} \otimes |\rho_j\rangle\langle\rho_j|^{A_rCC'}$, *such that for any* $\iota \in (0,1]$ *and* $\epsilon > 0$, *it holds that*

$$\begin{aligned}
c+q+e &\leq -H_{\max}^{\epsilon+2\lambda}(A_cA_r|CC')_\rho + \log J - \log\iota + f(\epsilon),\\
q+e &\leq -H_{\max}^{\epsilon+2\lambda'}(A_r|CC'A_c)_\rho - \log\iota + f(\epsilon),\\
c+q-e &\leq -H_{\max}^{\lambda}(A_cA_r|D)_{\mathcal{N}(\rho)} + \log J - \log\iota,\\
q-e &\leq -H_{\max}^{\lambda'}(A_r|DA_c)_{\mathcal{N}(\rho)} - \log\iota,
\end{aligned}$$

where $f(\epsilon) := -\log(1-\sqrt{1-\epsilon^2})$. *The smoothing parameters* λ *and* λ' *are functions of* δ *and* ι *that vanishes in the limit of* $\delta, \iota \to 0$.

4 Randomized Partial Decoupling

As a tool for proving Theorem 1 and 2, we introduce a task that we call *randomized partial decoupling*, which is a generalization of decoupling and may be of independent interest. For the details and proofs, please see the paper by the same authors [13].

Randomized partial decoupling is a task in which a bipartite quantum state Ψ^{AR} is transformed by a unitary operation on A and then is subject to the action of a quantum channel (linear CP map) $\mathcal{T}^{A\to E}$. We assume that the Hilbert space $\mathcal{H}^A$ is isomorphic to a tensor product Hilbert space $\mathcal{H}^{A_c}\otimes\mathcal{H}^{A_r}$, i.e., $A\cong A_cA_r$, where $\mathcal{H}^{A_c}$ is a J-dimensional Hilbert space with a fixed orthonormal basis $\{|j\rangle\}_{j=1}^J$.

We consider a random unitary U on system A in the form of $U:=\sum_{j=1}^J |j\rangle\langle j|^{A_c}\otimes U_j^{A_r}$, where $U_j\sim \mathsf{H}_j$ for each j, and H_j is the Haar measure on the unitary group on $\mathcal{H}^{A_r}$. We also introduce a unitary $G_\sigma:=\sum_{j=1}^J |\sigma(j)\rangle\langle j|^{A_c}\otimes I^{A_r}$ for a permutation σ on $[1,\cdots,J]$ that is chosen according to the uniform distribution. Our concern is how close the final state $\mathcal{T}^{A\to E}\circ\mathcal{G}_\sigma^A\circ\mathcal{U}^A(\Psi^{AR})$ is, on average, to the averaged final state $\mathcal{T}^{A\to E}\circ\mathcal{G}_\sigma^A(\Psi_{\rm av}^{AR})$, for typical choices of the permutation σ where $\Psi_{\rm av}^{AR}:=\mathbb{E}_{U\sim\mathsf{H}_\times}[\mathcal{U}^A(\Psi^{AR})]$. For the simplicity of analysis, we assume that Ψ^{AR} is *classically coherent* [10] in AR.

The following theorem is the direct part of the randomized partial decoupling theorem, and provides an upper bound on the average distance between $\mathcal{T}^{A\to E}\circ\mathcal{G}_\sigma^A\circ\mathcal{U}^A(\Psi^{AR})$ and $\mathcal{T}^{A\to E}\circ\mathcal{G}_\sigma^A(\Psi_{\rm av}^{AR})$.

Theorem 3 *(Theorem 3 in [13]) Let U and G_σ be random unitaries defined as above, and fix arbitrary $\epsilon,\mu\geq 0$. Consider a subnormalized state Ψ^{AR} that is classically coherent in AR. Let $\mathcal{T}^{A\to E}$ be a linear CP map with the complementary channel $\mathcal{T}^{A\to C}$. It holds that*

$$\mathbb{E}_{\sigma,U}\left[\left\|\mathcal{T}^{A\to E}\circ\mathcal{G}_\sigma^A\circ\mathcal{U}^A(\Psi^{AR})-\mathcal{T}^{A\to E}\circ\mathcal{G}_\sigma^A(\Psi_{\rm av}^{AR})\right\|_1\right]$$
$$\leq (J-1)^{-1/2}\cdot 2^{-\frac{1}{2}H_I}+2^{-\frac{1}{2}H_{II}}+4(\epsilon+\mu+\epsilon\mu),$$

where $\Psi_{\rm av}^{AR}:=\mathbb{E}_{U\sim\mathsf{H}_\times}[\mathcal{U}^A(\Psi^{AR})]$ and the exponents H_I and H_{II} are given by

$$H_I=H_{\min}^{\epsilon}(A|R)_\Psi-H_{\max}^{\mu}(A|C)_{\mathcal{C}(\tau)},$$
$$H_{II}=H_{\min}^{\epsilon}(A|R)_{\mathcal{C}(\Psi)}-H_{\max}^{\mu}(A_r|CA_c)_{\mathcal{C}(\tau)}. \quad (1)$$

Here, $\mathcal{C}$ is the completely dephasing operation on A_c with respect to the basis $\{|j\rangle\}_{j=1}^J$, and τ is the Choi-Jamiolkowski state of $\mathcal{T}^{A\to C}$.

The converse bound for randomized partial decoupling is stated by the following theorem.

Theorem 4 *(Theorem 4 in [13]) Let $|\Psi\rangle^{ABR}$ be a purification of a normalized state $\Psi^{AR}\in\mathcal{S}_=(\mathcal{H}^{AR})$, which is classically coherent in AR. Let $\mathcal{T}^{A\to E}$ be a CP map with the complementary channel $\mathcal{T}^{A\to C}$, such that $\mathrm{Tr}[\mathcal{T}^{A\to E}(\Psi^{AR})]=1$. Suppose that, for $\delta>0$, there exists a normalized state in the form of*

$$\Omega^{ER}:=\sum_{j=1}^J p_j\varsigma_j^E\otimes\Psi_j^{R_r}\otimes|j\rangle\langle j|^{R_c}, \quad (2)$$

such that $\|\mathcal{T}^{A\to E}(\Psi^{AR})-\Omega^{ER}\|_1\leq\delta$. Then, for any $\upsilon\in[0,1/2)$ and $\iota\in(0,1]$, it holds that

$$H_{\min}^{\lambda}(A|R)_\Psi-H_{\min}^{\upsilon}(BR|C)_{\mathcal{T}\circ\mathcal{C}(\Psi)}+\log J\geq\log\iota,$$
$$H_{\min}^{\lambda'}(A|R)_{\mathcal{C}(\Psi)}-H_{\min}^{\upsilon}(BR_r|CR_c)_{\mathcal{T}\circ\mathcal{C}(\Psi)}$$
$$\geq\log\iota+\log(1-2\upsilon),$$

where $\mathcal{C}$ is the completely dephasing channel on A_c. The smoothing parameters λ and λ' are functions of ι, υ and δ that vanishes in the limit of $\iota,\upsilon,\delta\to 0$.

References

[1] M. Wilde, *Quantum Information Theory*, Cambridge University Press (2013)

[2] I. Devetak and A. Winter, *Phys. Rev. Lett.* 93, 080501 (2004)

[3] M. Horodecki et al., *Comm. Math. Phys.* 269, 107 (2007)

[4] A. Abeyesinghe et al., *Proc. R. Soc. A* 465, 2537 (2009)

[5] I. Devetak et al., *Phys. Rev. Lett.* 93, 230504 (2004)

[6] A. Uhlmann, *Rep. Math. Phys.* 9, 273 (1976)

[7] F. Dupuis et al., *Comm. Math. Phys.* 328, 251 (2014)

[8] F. Dupuis, e-print arXiv:1004.1641 (2010)

[9] M. Tomamichel et al., *IEEE Trans. Inf. Theory* 55, 5840 (2009)

[10] F. Dupuis et al., *IEEE Trans. Inf. Theory* 60, 1562 (2014)

[11] F. Salek et al., arXiv:1809.07104 (2018)

[12] M.-H. Hsieh and M. Wilde, *IEEE Trans. Inf. Theory* 56, 4682 (2010)

[13] E. Wakakuwa and Y. Nakata, arXiv:1903.05796 (2019)

Capacity of Quantum Private Information Retrieval with Multiple Servers

Seunghoan Song[1] * Masahito Hayashi[1 2 3] †

[1] *Graduate School of Mathematics, Nagoya University*
[2] *Centre for Quantum Technologies, National University of Singapore*
[3] *Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology*

Abstract. We study the capacity of quantum private information retrieval (QPIR) with multiple servers. In the QPIR problem with multiple servers, a user retrieves a classical file by downloading quantum systems from multiple servers each of which containing the whole classical file set, without revealing the identity of the retrieved file to any individual server. The QPIR capacity is defined as the maximum rate of the file size over the whole dimension of the downloaded quantum systems. When the preexisting entanglement among servers are assumed, we prove that the QPIR capacity with multiple servers is 1 regardless of the number of servers and files. We propose a rate-one protocol which can be implemented by using only two servers. This capacity-achieving protocol outperforms its classical counterpart in the sense of the capacity, server secrecy, and upload cost. The strong converse bound is derived concisely without using any secrecy condition. We also prove that the capacity of symmetric multi-round QPIR with coded databases is 1.

A full version of this paper is accessible at: `https://arxiv.org/pdf/1903.10209.pdf`.

Keywords: private information retrieval, quantum private information retrieval, oblivious transfer

1 Introduction

Introduced in the seminal paper by Chor *et al.* [1], private information retrieval (PIR) finds efficient methods to download a file from non-communicating servers each of which containing the whole classical file set, without revealing the identity of the downloaded file to each server. This problem is trivially solved by requesting all files to the servers, but this method is inefficient. Finding an efficient method is the goal of this problem and it has been extensively studied in many papers [2–5]. Moreover, the papers [6–10] studied quantum PIR (QPIR) problem where the user downloads quantum systems, instead of classical bits, in order to retrieve a classical file from the servers.

In classical PIR studies, the paper [11] started the discussion of capacities for PIR problems with multiple servers. The PIR capacity is defined by the maximum rate of the file size over the download size. The upload cost, i.e., the total size of the queries, is neglected since it does not scale with the file size, which is allowed to go infinity. For the PIR with n non-communicating servers each containing the whole set of f files, the paper [11] showed that the capacity is $(1-1/\mathsf{n})/(1-(1/\mathsf{n})^{\mathsf{f}})$. Moreover, the paper [12] proposed a capacity-achieving protocol whose upload cost and file size are minimum in a general class of PIR protocols. Furthermore, after [11], several PIR capacities have been studied under different problem settings. Symmetric PIR is the PIR with server secrecy that the user obtains no more information than the target file, and the capacity of symmetric PIR is $1-\mathsf{n}^{-1}$ [13]. Another extension is the PIR with coded databases [16–18], where the set of files is coded and distributed to the servers, whereas the PIR in [11] assumes that the file set is replicated to all servers. The capacity of PIR with files coded by (n,k) maximum distance separable code is $(1-\mathsf{k}/\mathsf{n})/(1-(\mathsf{k}/\mathsf{n})^{\mathsf{f}})$ [16]. Multi-round PIR has also been studied in [19] and the capacity was proved to be the same as the PIR capacity derived in [11].

Table 1: Capacities of classical and quantum PIRs

	Classical PIR Capacity	Quantum PIR Capacity
PIR	$\frac{1-\mathsf{n}^{-1}}{1-\mathsf{n}^{-\mathsf{f}}}$ [11]	1 §
Symmetric PIR	$1-\mathsf{n}^{-1}$ [13] †	1 §
PIR with coded databases	$\frac{1-\mathsf{k}/\mathsf{n}}{1-(\mathsf{k}/\mathsf{n})^{\mathsf{f}}}$ [16] ‡	1 §
Multi-round PIR	$\frac{1-\mathsf{n}^{-1}}{1-\mathsf{n}^{-\mathsf{f}}}$ [19]	1

∗ n, f: the numbers of servers and files, respectively.
† Shared randomness among servers is necessary.
‡ Files are coded by (n,k) maximum distance separable code.
§ Capacities are derived by strong converse.

On the other hand, the QPIR problem is rarely treated with multiple servers and there is no study on the capacity of the QPIR problem. Though the paper [7] treated the QPIR problem with multiple servers, the paper [7] evaluated the communication complexity which is the sum of upload and download costs required to retrieve one bit file, instead of the capacity.

In the paper, as quantum extensions of the classical PIR capacities [11,13,16,19], we show that the capacities of QPIR, symmetric QPIR, QPIR with coded databases, and multi-round QPIR are 1 even when there are multiple servers. First, we derive the QPIR capacity when a user retrieves a file secretly from n non-communicating servers containing the whole set of f files by downloading quantum states under the assumption that an entan-

*m17021a@math.nagoya-u.ac.jp
†masahito@math.nagoya-u.ac.jp

gled state is shared previously among all servers. We define the security of the QPIR protocol with three parameters: the retrieval error probability, the user secrecy that the identity of the querying file is unknown to any individual server, and the server secrecy that the user obtains no more information than the target file. As a main result, we show that the QPIR capacity is 1 regardless of whether it is of exact/asymptotic security and with/without the restriction that the upload cost is negligible to the download cost. We propose a rate-one QPIR protocol with perfect security and finite upload cost. Even for any QPIR protocol with no secrecy, no upload constraint, and any error probability less than 1, we propose the converse bound is 1. Since our protocol is a special case of the QPIR with coded databases and our converse bound is also directly applicable to the QPIR with coded databases, our result also proves that the QPIR capacity with coded databases is 1. Moreover, we show that the capacity of symmetric multi-round QPIR with coded databases is 1 by proving a weak converse bound such that the multi-round QPIR rate is upper bounded by 1 when the error probability is asymptotically zero.

It should be noted that our QPIR protocol can be considered as a distributed version of oblivious transfer (OT) [20, 21]. OT is defined as the symmetric PIR with one server and therefore, symmetric PIR with multiple servers can be considered as a distributed version of OT. OT is an important cryptographic protocol because the free uses of OT protocol constructs an arbitrary secure multiparty computation [22, 23]. Unfortunately, the symmetric classical PIR cannot be constructed without secret shared randomness among servers [24]. On the other hand, the paper [7] showed that the two-way quantum communication between the servers and the user enables the symmetric PIR without secret shared randomness. Our result extends the result [7] so that even for the case of classical upload, quantum download, and previously shared entanglement among the servers, the symmetric PIR can be constructed without secret shared randomness. Note that if quantum upload is allowed to our model, the assumption of shared entanglement is not necessary because the user can upload an entangled state to all servers.

2 QPIR Protocol and Main Theorem

In this section, we formally define the QPIR protocol and its capacity, and presents a main theorem of the paper.

2.1 Formal definition of QPIR protocol

The QPIR with multiple servers (hereinafter QPIR) is described as follows. Consider a user and non-communicating n servers $\mathtt{serv}_1, \ldots, \mathtt{serv}_\mathsf{n}$ each of which containing the whole set of uniformly and independently distributed f files $W_1, \ldots, W_\mathsf{f} \in \{0, \ldots, \mathsf{m}-1\}$ for integers $\mathsf{n}, \mathsf{f}, \mathsf{m} \geq 2$. Each server $\mathtt{serv}_t$ possesses a quantum system $\tilde{\mathcal{A}}_t$ and the n servers share an entangled state $\rho_{\rm prev} \in \mathcal{S}(\bigotimes_{i=1}^{\mathsf{n}} \tilde{\mathcal{A}}_i)$ in the beginning. The user chooses

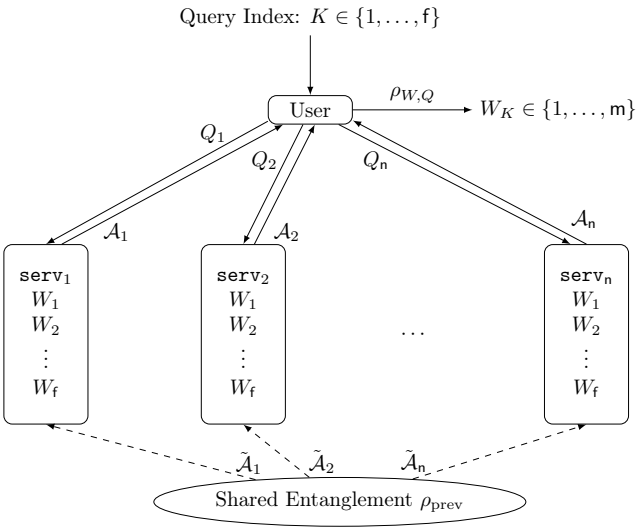


Figure 1: Quantum private information retrieval protocol with multiple servers. The composite system of the servers is initialized to an entangled state $\rho_{\rm perv}$.

the query index K in order to retrieve the K-th file W_K, where the distribution of K is uniform and independent of the file W_i for any $i \in \{1, \ldots, \mathsf{f}\}$.

In order to retrieve the K-th file W_K, the user chooses a random variable $R_{\rm user}$ in a set $\mathcal{R}_{\rm user}$ and encodes the queries for retrieving W_K by user encoder $\mathsf{Enc}_{\rm user}$:

$$\mathsf{Enc}_{\rm user}(K, R_{\rm user}) = (Q_1, \ldots, Q_\mathsf{n}) \in \mathcal{Q}_1 \times \cdots \times \mathcal{Q}_\mathsf{n},$$

where $\mathcal{Q}_t$ is the set of query symbols to the t-th server for any $t \in \{1, \ldots, \mathsf{n}\}$. The n queries $Q_1, \ldots, Q_\mathsf{n}$ are sent to the servers $\mathtt{serv}_1, \ldots, \mathtt{serv}_\mathsf{n}$, respectively. After receiving the t-th query Q_t, each server $\mathtt{serv}_t$ applies a trace-preserving completely positive (TP-CP) linear map Λ_t from $\tilde{\mathcal{A}}_t$ to $\mathcal{A}_t$ depending on $Q_t, W_1, \ldots, W_\mathsf{f}$ and sends the quantum system $\mathcal{A}_t$ to the user. With server encoder $\mathsf{Enc}_{\mathtt{serv}_t}$, the map Λ_t is written as

$$\Lambda_t = \mathsf{Enc}_{\mathtt{serv}_t}(Q_t, W_1, \ldots, W_\mathsf{f}),$$

and the received state of the user is written as

$$\rho_{W,Q} := \Lambda_1 \otimes \cdots \otimes \Lambda_\mathsf{n}(\rho_{\rm prev}) \in \mathcal{S}\left(\bigotimes_{i=1}^{\mathsf{n}} \mathcal{A}_i\right), \quad (1)$$

where $W := (W_1, \ldots, W_\mathsf{f})$ and $Q := (Q_1, \ldots, Q_\mathsf{n})$. Next, the user retrieves the file W_K by a decoder which is defined depending on K, Q as a Positive Operator-Valued Measure (POVM) $\mathsf{Dec}(K, Q) := \{\mathsf{Y}_M\}_{M=0}^{\mathsf{m}}$. The protocol outputs the measurement outcome $M \in \{1, \ldots, \mathsf{m}\}$ and if $M = \mathsf{m}$, it is considered as retrieval failure.

2.1.1 Protocol

When the numbers n and f of servers and files are fixed, a QPIR protocol of file size m is formulated by the 4-tuple $\Psi_{\rm QPIR}^{(\mathsf{m})} := (\rho_{\rm prev}, \mathsf{Enc}_{\rm user}, \mathsf{Enc}_{\rm serv}, \mathsf{Dec})$ of the previously shared entangled state $\rho_{\rm prev}$ among servers, the user encoder $\mathsf{Enc}_{\rm user}$, the collection of the server encoders $\mathsf{Enc}_{\rm serv} := (\mathsf{Enc}_{\mathtt{serv}_1}, \ldots, \mathsf{Enc}_{\mathtt{serv}_\mathsf{n}})$, and the decoder Dec.

2.1.2 Security

A QPIR protocol has two kinds of security parameters, the error probability and secrecy parameters. The error probability of the protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}$ is written as

$$P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) := \Pr_{W,K,Q}[M \neq W_K].$$

The secrecy parameters are defined as follows. For any $t \in \{1,\dots,\mathsf{n}\}$, let $\mathfrak{user}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ and $\mathfrak{serv}_t(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})$ be the information of the user and the server $\mathtt{serv}_t$ at the end of the protocol, respectively. We define the server secrecy parameter and the user secrecy parameter by

$$S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) := I(W_{K^c}; \mathfrak{user}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})|K), \tag{2}$$

$$S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) := \max_{t\in\{1,\dots,\mathsf{n}\}} I(K; \mathfrak{serv}_t(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})), \tag{3}$$

where $I(\cdot;\cdot|\cdot)$ denotes the conditional mutual information and $W_{K^c} := (W_1,\dots,W_{K-1},W_{K+1},\dots,W_{\mathsf{f}})$. If $S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = 0$, the files other than W_K are independent of the user information. Similarly, if $S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) = 0$, the query index K is independent of any individual server information.

2.1.3 Costs, rate, and capacity

Given the QPIR protocol $\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}$, the upload cost, download cost, and rate are defined by

$$U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) := \prod_{i=1}^{\mathsf{n}} |\mathcal{Q}_i|, \quad D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) := \prod_{i=1}^{\mathsf{n}} \dim \mathcal{A}_i,$$

$$R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})}) := \frac{\log \mathsf{m}}{\log D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m})})}.$$

The QPIR capacity is defined with constraints on the security parameters and upload cost. *The asymptotic security-constrained capacity* and *the exact security-constrained capacity* are defined with error constraint $\alpha \in [0,1)$, server secrecy constraint $\beta \in [0,\infty]$, user secrecy constraint $\gamma \in [0,\infty]$, and upload constraint $\theta \in [0,\infty]$ by

$$C_{\mathrm{asymp}}^{\alpha,\beta,\gamma,\theta} := \sup_{\substack{\{\mathsf{m}_\ell\}_{\ell=1}^\infty,\\ \{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^\infty}} \left\{ \liminf_{\ell\to\infty} R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \;\middle|\; \limsup_{\ell\to\infty} P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \alpha,\ \limsup_{\ell\to\infty} S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \beta, \right.$$
$$\left. \limsup_{\ell\to\infty} S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \gamma,\ \limsup_{\ell\to\infty} \frac{\log U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})}{\log D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})} \le \theta \right\},$$

$$C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta} := \sup_{\substack{\{\mathsf{m}_\ell\}_{\ell=1}^\infty,\\ \{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^\infty}} \left\{ \liminf_{\ell\to\infty} R(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \;\middle|\; P_{\mathrm{err}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \alpha,\ S_{\mathrm{serv}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \beta, \right.$$
$$\left. S_{\mathrm{user}}(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}) \le \gamma,\ \limsup_{\ell\to\infty} \frac{\log U(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})}{\log D(\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)})} \le \theta \right\},$$

where the supremum is taken for sequences $\{\mathsf{m}_\ell\}_{\ell=1}^\infty$ such that $\lim_{\ell\to\infty}\mathsf{m}_\ell = \infty$ and sequences $\{\Psi_{\mathrm{QPIR}}^{(\mathsf{m}_\ell)}\}_{\ell=1}^\infty$ of QPIR protocols. It is trivial from the definition that for any $\alpha \in [0,1)$, $\theta \in [0,\infty]$, $\beta \in [0,\infty]$, and $\gamma \in [0,\infty]$,

$$C_{\mathrm{exact}}^{0,0,0,0} \le C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta} \le C_{\mathrm{asymp}}^{\alpha,\beta,\gamma,\theta} \le C_{\mathrm{asymp}}^{\alpha,\infty,\infty,\infty}. \tag{4}$$

2.2 Main Result

The main theorem of this paper is given as follows.

Theorem 2.1 *For any $\alpha \in [0,1)$ and $\beta,\gamma,\theta \in [0,\infty]$, the capacity of the quantum private information retrieval with f files and $\mathsf{n} \ge 2$ servers sharing preexisting entanglement is*

$$C_{\mathrm{exact}}^{\alpha,\beta,\gamma,\theta} = C_{\mathrm{asymp}}^{\alpha,\beta,\gamma,\theta} = 1.$$

Proof. From [30, Sections 3 and 4], we proved $C_{\mathrm{exact}}^{0,0,0,0} \ge 1$ and $C_{\mathrm{asymp}}^{\alpha,\infty,\infty,\infty} \le 1$ for any $\alpha \in [0,1)$, respectively. Then, the inequality (4) implies Theorem 2.1. □

Note that the capacity does not depend on the number of files f and the number of servers n. This contrasts to the classical PIR capacity [11] which is strictly increasing for f and n. Moreover, the capacity does not depend on the security constraints, i.e., there is no trade-off between the capacity and the security constraints. Furthermore, the theorem implies that the symmetric QPIR capacity is 1.

Moreover, the following theorem presents the capacity for symmetric multi-round QPIR with coded databases.

Theorem 2.2 *For any positive integer r, the symmetric r-round QPIR capacity with coded databases when there are f files and $\mathsf{n} \ge 2$ servers sharing preexisting entanglement is* 1.

Acknowledgments

SS is grateful to Hsuan-Yin Lin for helpful discussions and comments. SS is supported by Rotary Yoneyama Memorial Master Course Scholarship (YM). MH is 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] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," *Journal of*

the ACM, 45(6):965-981, 1998. Earlier version in FOCS'95.

[2] C. Cachin, S. Micali, and M. Stadler, "Computationally Private Information Retrieval with Polylogarithmic Communication," in *Advances in Cryptology - EUROCRYPT '99,* pp. 402-414, 1999.

[3] H. Lipmaa, "First CPIR Protocol with Data-Dependent Computation," in *Proceedings of the 12th International Conference on Information Security and Cryptology,* pp. 193-210, 2010.

[4] A. Beimel and Y. Stahl, "Robust information-theoretic private information retrieval," in *Proceedings of the 3rd International Conference on Security in Communication Networks (SCN'02)*, pp. 326-341, 2003.

[5] C. Devet, I. Goldberg, and N. Heninger, "Optimally Robust Private Information Retrieval," in *21st USENIX Security Symposium*, August 2012.

[6] I. Kerenidis and R. de Wolf. "Exponential lower bound for 2-query locally decodable codes via a quantum argument," In Proceedings of 35th ACM STOC, pp. 106-115, 2003.

[7] I. Kerenidis and R. de Wolf, "Quantum symmetrically-private information retrieval," *Information Processing Letters*, vol. 90, pp. 109-114, 2004.

[8] L. Olejnik, "Secure quantum private information retrieval using phase-encoded queries," *Physical Review A* 84, 022313, 2011.

[9] Ä. Baumeler and A. Broadbent, "Quantum Private Information Retrieval has linear communication complexity," *Journal of Cryptology*, vol. 28, issue 1, pp. 161-175, 2015.

[10] F. Le Gall, "Quantum Private Information Retrieval with Sublinear Communication Complexity," arXiv:1107.5881, 2011.

[11] H. Sun and S. Jafar, "The Capacity of Private Information Retrieval," *IEEE Transactions on Information Theory*, vol. 63, no. 7, 2017.

[12] C. Tian, H. Sun, and J. Chen, "Capacity-Achieving Private Information Retrieval Codes with Optimal Message Size and Upload Cost," arXiv:1808.07536.

[13] H. Sun and S. Jafar, "The Capacity of Symmetric Private Information Retrieval," 2016 IEEE Globecom Workshops (GC Wkshps), Washington, DC, 2016, pp. 1-5.

[14] R. Freij-Hollanti, O. W. Gnilke, C. Hollanti, and D. A. Karpuk, "Private information retrieval from coded databases with colluding servers," *SIAM J. Appl. Algebra Geometry*, vol. 1, no. 1, pp. 647-664, 2017.

[15] H. Sun and S. Jafar, "The Capacity of Robust Private Information Retrieval with Colluding Databases," *IEEE Transactions on Information Theory* vol. 64, no. 4, 2018.

[16] K. Banawan and S. Ulukus, "The Capacity of Private Information Retrieval from Coded Databases," *IEEE Transactions on Information Theory*, vol. 64, no. 3, 2018.

[17] S. Kumar, H.-Y. Lin, E. Rosnes, and A. Graell i Amat, "Achieving maximum distance separable private information retrieval capacity with linear codes," arXiv:1712.03898v3 [cs.IT]. [Online].

[18] H.-Y. Lin, S. Kumar, E. Rosnes, and A. Graell i Amat, "An MDS-PIR capacity-achieving protocol for distributed storage using non-MDS linear codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Vail, CO, USA, Jun. 17-22, 2018.

[19] H. Sun and S. A. Jafar, "Multiround Private Information Retrieval: Capacity and Storage Overhead," *IEEE Transactions on Information Theory*, vol. 64, no. 8, pp. 5743-5754, 2018.

[20] M. O. Rabin, "How to exchange secrets with oblivious transfer," *Technical Report TR-81*, Harvard University, 1981.

[21] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Communications of the ACM*, vol. 28, no. 6, pp. 637–647, 1985.

[22] J. Kilian, "Founding crytpography on oblivious transfer," *Proc. 1988 ACM Annual Symposium on Theory of Computing*, p. 20.

[23] Y. Ishai, M. Prabhakaran, and A. Sahai, "Founding Cryptography on Oblivious Transfer - Efficiently," CRYPTO, pp. 572-591, 2008.

[24] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin. "Protecting data privacy in private information retrieval schemes," *Journal of Computer and Systems Sciences*, 60(3):592–629, 2000. Earlier version in STOC 98.

[25] M. Hayashi, Quantum Information Theory: Mathematical Foundation, Graduate Texts in Physics, Springer, 2017.

[26] D. Ding, Y. Quek, P. W. Shor, M. M. Wilde "Entropy Bound for the Classical Capacity of a Quantum Channel Assisted by Classical Feedback," arXiv:1902.02490v1, 2019.

[27] S. Song and M. Hayashi, "Capacity of Quantum Private Information Retrieval with Multiple Servers," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2019 (*arXiv:1903.10209v1 [quant-ph]*).

Resource theories of quantum channels and the universal role of resource erasure

(Full version arxiv:1904.04201)

Zi-Wen Liu[1 2 *] Andreas Winter[3 †]

[1] *Perimeter Institute for Theoretical Physics*
[2] *Center for Theoretical Physics, MIT*
[3] *Universitat Autònoma de Barcelona*

Abstract. We initiate the systematic study of resource theories of quantum channels, i.e. of the dynamics that quantum systems undergo by completely positive maps, *in abstracto*: Resources are in principle all maps from one quantum system to another, but some maps are deemed *free*. The free maps are supposed to satisfy certain axioms, among them closure under tensor products, under composition and freeness of the identity map (the latter two say that the free maps form a monoid). The free maps act on the resources simply by tensor product and composition. This generalizes the much-studied resource theories of quantum states, and abolishes the distinction between resources (states) and the free maps, which act on the former, leaving only maps, divided into resource-full and resource-free ones.

We discuss the axiomatic framework of quantifying channel resources, and show two general methods of constructing resource monotones of channels. Furthermore, we show that under mild regularity conditions, each resource theory of quantum channels has a distinguished monotone, the *robustness* (and its smoothed version), generalizing the analogous concept in resource theories of states. We give an operational interpretation of the log-robustness as the amount of heat dissipation (randomness) required for resource erasure by random reversible free maps, valid in broad classes of resource theories of quantum channels. Finally, we remark on several key issues concerning the asymptotic theory.

Keywords: Quantum channels, resource theory

The paradigm of resource theories has been applied successfully to capture the essence of what is valuable, and how to measure its value, in scenarios where certain objects and transformations are considered relatively "easy" compared to others. In resource theories this is idealized by considering some objects and transformations free, meaning they may be invoked unlimitedly in any situation. Specifically, resource theories of quantum states, i.e. where the objects are states of quantum systems undergoing (free) quantum channels, have proved to be extremely successful in characterizing various quantum and other features of quantum states (see [1] for a recent survey), such as entanglement, coherence, thermal non-equilibrium, asymmetry (related to conserved quantities by Noether's theorem), magic states, etc. The structure of resource theories can be characterized in much more abstract ways, for instance, in terms of category theory [2, 3], or for more general GPT objects.

In this work, rather than going all the way to these abstract structures, we will explore a more modest, but for quantum mechanics highly important, extension, namely from quantum states to quantum channels represented by completely positive maps as the objects of the resource theory. There are a number of strong motivations for doing so, including but not restricted to the following few. On the one hand, quantum channels or processes can represent dynamical resources which, as opposed to static state resources, play natural roles i many physical scenarios. For example, certain quantum channels can be used to efficiently transmit quantum information, and certain thermodynamic processes can be implemented to do work. Therefore, the resource theory approach for quantum channels is of great practical interest. On the other hand, due to the more complicated mathematical structure of quantum channels, the associated resource theory framework can be highly nontrivial and interesting from a mathematical point of view. In particular, as will be discussed in more depth later, several key aspects of the resource theory approach such as resource composition and transformation become more subtle than the traditional state theory. Furthermore, the application of resource theory approach to quantum channels augments and advances the study of this core area of quantum information, and of course the understanding of this extended resource theory scheme could greatly benefit from the profound literature of e.g. quantum channel coding and capacities. Our programme is not entirely new, in fact it has been done, at least in part, for certain concrete quantum resource theories: for instance for a good part of quantum Shannon theory [4, 5], bipartite entanglement [6], athermality [7, 8, 9], and recently for the resource theory of coherence [10, 11] and magic [12, 13]. However, a general framework of channel resource theories is still elusive. This work aims at initiating the systematic study of resource theories of quantum channels by discussing key aspects of the general framework, as summarized in the following. The full paper also contains detailed discussions of several illustrative examples to solidify the general scheme.

We first define the axioms and elements of channel resource theories in a rigorous manner. Resources are in principle all maps from one quantum system to another,

*zliu1@perimeterinstitute.ca
†andreas.winter@uab.cat

but some maps are deemed free. The free maps are supposed to satisfy certain axioms, among them closure under tensor products, under composition and freeness of the identity map (the latter two say that the free maps form a monoid). The free maps act on the resources simply by tensor product and composition. This generalizes the much-studied resource theories of quantum states, and abolishes their distinction between resources (states), on which free maps act, leaving only maps, divided into resource-full and resource-free ones. The resource transformation is defined by channel simulation with free pre- and post-processings. However, we would like to highlight that the mathematical structure and dynamical feature of quantum channels lead to some subtleties and fundamental differences with the state/static resource theories, in particular concerning the conversion and composition of resources. We discuss these fundamental features of channel theories in more depth in the full paper.

We show two general methods how to lift resource monotones from states to operations, namely i) the generating-power type measures given by $g(\mathcal{N}) = \max\{\omega(\mathcal{N}\otimes \mathrm{id}(\rho)) - \omega(\rho)\}$, where ω is a resource monotone of states and the maximization can run over free states or all states; ii) the distance-type measures given by $d(\mathcal{N}) = \min_{\mathcal{M}\in F} D(\mathcal{N},\mathcal{M})$ where D is some distance defined on channels (e.g. diamond norm) and F is set of free channels. We show that these general measures satisfy the lifted monotonicity conditions under the axioms of our framework, and are therefore sensible resource measures of channels in general.

In particular, we show that under mild regularity conditions, each resource theory of quantum channels has a distinguished class of monotones, the *robustness* and *log-robustness* (and their smoothed versions), generalizing the analogous concept in resource theories of states: $R(\mathcal{N}) = \min\{s \geq 0 : \frac{1}{1+s}\mathcal{N} + \frac{s}{1+s}\mathcal{N}' \in F\}$ and $LR(\mathcal{N}) = \log(1 + R(\mathcal{N}))$. In doing so we generalize the notion of max-relative entropy to cp maps:

$$D_{\max}(\mathcal{N}\|\mathcal{M}) := \log \min\{\lambda : \mathcal{N} \leq \lambda\mathcal{M}\}, \qquad (1)$$

where the inequality sign refers to the complete-positivity order between superoperators, meaning that the difference between r.h.s. and l.h.s. is completely positive. Smoothing is defined by optimizing over ϵ-ball of diamond norm. It can be verified that $LR^\epsilon(\mathcal{N}) = \min_{\mathcal{M}\in F} D^\epsilon_{\max}(\mathcal{N}\|\mathcal{M})$. We give a universal operational interpretation of the resource log-robustness as the amount of heat dissipation required for the task of one-shot resource erasure by random reversible free maps, valid in broad classes of resource theories of quantum channels.

Theorem 1. *For a channel $\mathcal{N} : A \longrightarrow B$ in a resource theory with free states $\mathbf{F}$ satisfying a few axioms of free resources (see full paper), define an* ϵ-resource-destruction process *to be any free channel $\mathcal{F} \in \mathbf{F}(A' \longrightarrow B')$ together with an ensemble of pairs of free reversible channels (i.e. unitary conjugations) $\{p_i, \mathcal{U}_i^{AA'}, \mathcal{V}_i^{BB'}\}_{i=1}^k$, such that*

$$\frac{1}{2}\left\|\sum_{i=1}^k p_i \mathcal{V}_i \circ (\mathcal{N}\otimes\mathcal{F})\circ\mathcal{U}_i - \mathcal{M}\right\|_\diamond \leq \epsilon,$$

for some free channel $\mathcal{M} \in (AA' \longrightarrow BB')$. Let $\mathsf{COST}^\epsilon(\mathcal{N})$ be the minimum $\log k$ such that an ϵ-resource-destruction process exists. Then for any $0 < \eta < \epsilon < 1$,

$$LR^{\mu\delta}(\mathcal{N}) + \log\left(1 - \frac{1}{\mu}\right) \leq \mathsf{COST}^\epsilon(\mathcal{N}) \leq LR^{\epsilon-\eta}(\mathcal{N}) + 2\log\frac{1}{\eta} - 1, \qquad (2)$$

where $\delta = \sqrt{\epsilon(2-\epsilon)}$ and $\mu > 1$. If the sets of free channels F are convex, then the lower bound can be improved to $\mathsf{COST}^\epsilon(\mathcal{N}) \geq LR^\delta(\mathcal{N})$.

Technically, the proof of achievability is based on an abstract version of the "convex-split lemma" [14], extended from its original domain of quantum states to ordered vector spaces with base norms; this includes in particular the set of cptp maps with the diamond norm. The optimality bound for quantum channels is based on the Uhlmann's theorem for the completely bounded fidelity.

Lastly, we would like to remark on the asymptotic theory where one is given an infinite number of i.i.d. instances of channel resources. This leads to several open problems of importance and interest to channel resource theory and information theory in general. In particular, we describe the problem of the asymptotic limit of the smooth resource log-robustness of channels (which carries operational meaning in terms of resource erasure and channel simulation cost of coherence [11] in the one-shot regime), with discussions of partial progress and examples. A key step is the asymptotic equipartition property (AEP) of the aforementioned channel's max-relative entropy, whose final form is unclear at the moment besides some straightforward lower bounds. Moreover, this problem is key to the study of asymptotic reversibility (meaning that cost equals yield) of channel resource theories. For example, for the resource theory of coherence for channels under maximal free operations MIO [11], the simulation cost is given by the asymptotic smooth log-robustness. It is unclear whether it equals the generating capacity (which is given by a complete coherence generating power) [10], which indicates reversibility. Either case seems very interesting: it could be that the reversibility holds, which seems highly nontrivial to show and may lead to important advances in the understanding of channel theories; or that the reversibility fails (even when the set of free channels is maximal, which guarantees reversibility for state theories), which would be a peculiar feature of the channel theory.

References

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

[2] Bob Coecke, Tobias Fritz, and Robert W. Spekkens. A mathematical theory of resources. *Information*

and Computation, 250:59–86, 2016. arXiv[quant-ph]:1409.5531.

[3] Tobias Fritz. Resource convertibility and ordered commutative monoids. *Mathematical Structures in Computer Science*, 27(6):850–938, 2017.

[4] Igor Devetak, Aram W. Harrow, and Andreas Winter. A resource framework for quantum shannon theory. *IEEE Transactions on Information Theory*, 54(10):4587–4618, Oct 2008.

[5] Charles H. Bennett, Igor Devetak, Aram W. Harrow, Peter W. Shor, and Andreas Winter. The quantum reverse shannon theorem and resource tradeoffs for simulating quantum channels. *IEEE Transactions on Information Theory*, 60(5):2926–2959, May 2014.

[6] Charles H. Bennett, Aram W. Harrow, Debbie W. Leung, and John A. Smolin. On the capacities of bipartite hamiltonians and unitary gates. *IEEE Transactions on Information Theory*, 49(8):1895–1911, Aug 2003.

[7] Miguel Navascués and Luis Pedro García-Pintos. Nonthermal quantum channels as a thermodynamical resource. *Physical Review Letters*, 115:010405, Jul 2015.

[8] Philippe Faist and Renato Renner. Fundamental work cost of quantum processes. *Physical Review X*, 8:021011, 2018. arXiv[quant-ph]:1709.00506.

[9] Philippe Faist, Mario Berta, and Fernando Brandão. Thermodynamic capacity of quantum processes. *Phys. Rev. Lett.*, 122:200601, May 2019.

[10] Khaled Ben Dana, María García Díaz, Mohamed Mejatty, and Andreas Winter. Resource theory of coherence: Beyond states. *Physical Review A*, 95:062327, Jun 2017.

[11] María García Díaz, Kun Fang, Xin Wang, Matteo Rosati, Michalis Skontiniotis, John Calsamiglia, and Andreas Winter. Using and reusing coherence to realize quantum processes. *Quantum*, 2:100, 2018. arXiv[quant-ph]:1805.04045.

[12] Xin Wang, Mark M. Wilde, and Yuan Su. Quantifying the magic of quantum channels. *arXiv e-prints*, page arXiv:1903.04483, Mar 2019.

[13] James R. Seddon and Earl Campbell. Quantifying magic for multi-qubit operations. *arXiv e-prints*, page arXiv:1901.03322, Jan 2019.

[14] Anurag Anshu, Vamsi Krishna Devabathini, and Rahul Jain. Quantum message compression with applications. *Physical Review Letters*, 119:120506, 2017. arXiv[quant-ph]:1410.3031.

Efficient verification of bosonic quantum channels via benchmarking

Ya-Dong Wu[1] * Barry C. Sanders[1 2 3] †

[1] *Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*
[2] *Program in Quantum Information Science, Canadian Institute for Advanced Research, Toronto, Ontario M5G 1M1, Canada*
[3] *Shanghai Branch, National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Shanghai 201315, People's Republic of China*

Abstract. We aim to devise feasible, efficient verification schemes for bosonic channels. To this end, we construct an average-fidelity witness that yields a tight lower bound for average fidelity plus a general framework for verifying optimal quantum channels. For both multi-mode unitary Gaussian channels and single-mode amplification channels, we present experimentally feasible average-fidelity witnesses and reliable verification schemes, for which sample complexity scales polynomially with respect to all channel specification parameters. Our verification scheme provides an approach to benchmark the performance of bosonic channels on a set of Gaussian-distributed coherent states by employing only two-mode squeezed vacuum states and local homodyne detections. Our results demonstrate how to perform feasible tests of quantum components designed for continuous-variable quantum information processing.

Keywords: verification, bosonic channels, average-fidelity witness, Gaussian quantum information

1 Introduction

Progress in optical quantum computing [19, 2, 27] demands efficient schemes to verify performance of optical quantum processes, which would serve as components and devices for the quantum system. Characterization by quantum process tomography [7, 23, 9, 1, 21, 15, 25] could serve as a means for gathering sufficient assessment data to be used for verification, but, unfortunately, quantum process tomography is inefficient. Partial characterization methods, such as direct fidelity estimation [11, 8] and randomized benchmark [17, 18, 30, 24], although requiring less sampling overhead, are not readily adapted to bosonic channels, due to non-compactness of phase space and that Gaussian unitary operations do not form an exact unitary 2-design [35], respectively. Our aim is to devise efficient and experimentally feasible verification schemes for bosonic channels.

Quantum-state verification is widely studied [3, 13, 29, 12, 22, 22, 34, 28]. Reliable and efficient verification schemes [3] for bosonic Gaussian pure states have been adapted to benchmarking continuous-variable (CV) quantum gates [10]. Although experimentally appealing, this adaption of recent verification schemes [3, 14] only estimates average fidelity over a finite-dimensional subspace chosen by selecting a finite set of coherent states. This subspace selection cannot assess quantum-channel performance over the entire infinite-dimensional Hilbert space $\mathscr{H}$.

On the other hand, an alternative quantum-process benchmark approach benchmarks the average fidelity of bosonic quantum processes over all coherent states by preparing a two-mode squeezed vacuum state and measuring a single observable [4]. However, this scheme [4] is challenged by experimental limitations: online squeezing [33, 20], and quantum memories [16, 26]. Here we combine the favourable features of the state verification approach [3] and the unified quantum-benchmark approach [4] to develop our verification schemes for bosonic channels.

We formulate quantum-channel verification as an adversarial game between a technology-limited verifier and an untrusted, powerful prover who has significant but bounded quantum technology. Our average-fidelity witness issues a certificate that contains a tight lower bound of the average fidelity of the quantum channel. We develop a general framework for verification of optimal quantum channels, and, as examples of this framework, we present reliable and experimentally feasible verification schemes for both multi-mode Gaussian unitary channels and single-mode amplification channels. Both schemes can be implemented by preparing two-mode squeezed vacuum states and applying local homodyne detections, and the sample complexities for both two schemes scale polynomially with all channel-specification parameters. Thus, our results provide experimentally feasible tests of quantum components in bosonic quantum systems.

2 Definitions and framework

This section presents the general framework of verification of an optimal quantum channel, and the mathematical definitions of completeness and soundness as well as average-fidelity witness.

A verifier provides a prover with the classical description of the input ensemble $\{(p_x, \rho_x); x \in X\}$ as well as the output-target-state set $\{|\phi_x\rangle\langle\phi_x|; x \in X\}$, and the prover sends independent and identical copies of quantum channels, $\mathcal{E}_{\rm p}$, to the verifier. The verifier needs to decide whether to accept $\mathcal{E}_{\rm p}$ as an optimal quantum channel in terms of average fidelity

$$\bar{F}_{\mathcal{E}_{\rm p}} = \sum_{x\in X} p_x \langle\phi_x| \mathcal{E}_{\rm p}(\rho_x) |\phi_x\rangle , \qquad (1)$$

*yadong.wu@ucalgary.ca
†sandersb@ucalgary.ca

or reject it. A reliable quantum-channel verification protocol is defined as follows.

Definition 1 *An optimal-quantum-channel verification, with respect to threshold average fidelity* $0 < \bar{F}_t < \sup_{\mathcal{E}} \bar{F}_{\mathcal{E}}$ *and maximal failure probability* δ*, satisfies*

1. *completeness: if* $\bar{F}_{\mathcal{E}_{\mathrm{p}}} = \sup_{\mathcal{E}} \bar{F}_{\mathcal{E}}$*, then the verifier accepts with probability no less than* $1-\delta$*;*
2. *soundness: if* $\bar{F}_{\mathcal{E}_{\mathrm{p}}} \leq \bar{F}_t$*, then the verifier rejects with probability no less than* $1-\delta$*.*

Rather than sampling different inputs ρ_x, our verification protocol requires only one input state $|\Psi\rangle_{\mathrm{AR}}$ and measurement of one observable $W_{\mathrm{A}'\mathrm{R}}$, by adding a reference system R, where A and A$'$ denote channel input and channel output, respectively. The observable $W_{\mathrm{A}'\mathrm{R}}$ is an average-fidelity witness, which yields a tight lower bound of the average fidelity.

Definition 2 *An observable* $W_{\mathrm{A}'\mathrm{R}}$ *is an average-fidelity witness for* $\bar{F}_{\mathcal{E}}$ *on the state* $\mathcal{E}\otimes\mathcal{I}\left(|\Psi\rangle\langle\Psi|_{\mathrm{AR}}\right)$ *if*

$$\omega(\mathcal{E}) \coloneqq \mathrm{tr}\left[W_{\mathrm{A}'\mathrm{R}}\mathcal{E}\otimes\mathcal{I}\left(|\Psi\rangle\langle\Psi|_{\mathrm{AR}}\right)\right] \tag{2}$$

satisfies

$$1.\ \omega(\mathcal{E}) = \bar{F}_{\mathcal{E}} \Longleftrightarrow \bar{F}_{\mathcal{E}} = \sup_{\mathcal{C}} \bar{F}_{\mathcal{C}}; \tag{3}$$

$$2.\ \forall \mathcal{E}, \omega(\mathcal{E}) \leq \bar{F}_{\mathcal{E}}. \tag{4}$$

Our general quantum-channel verification scheme is: 1. prepare an entangled state $|\Psi\rangle_{\mathrm{AR}}$, and send system A of $|\Psi\rangle_{\mathrm{AR}}$ through $\mathcal{E}_p$; 2. apply local measurements on A' and R of $\mathcal{E}_p\otimes\mathcal{I}(|\Psi\rangle\langle\Psi|_{\mathrm{AR}})$, respectively, to estimate the mean value $\omega(\mathcal{E}_p)$; 3. repeat the above procedure, and obtain an estimate $\omega(\mathcal{E}_{\mathrm{p}})^*$; 4. if $\omega(\mathcal{E}_{\mathrm{p}})^* \geq \bar{F}_{\mathrm{t}} + \epsilon$, where ϵ is an estimation error bound, accept $\mathcal{E}_p$; otherwise, reject it.

3 Verification of bosonic channels

In this section, we present two verification protocols, one for multi-mode Gaussian unitary channels, the other for single-mode Gaussian amplification channels. Both protocols require only the preparation of two-mode squeezed vacuum states and the application of local homodyne detections. The sample complexities scale polynomially with respect to all channel-specification parameters. In both protocols, we devise experimentally feasible average-fidelity witnesses, the mean values of which, can be sampled by local homodyne detections.

3.1 Verification of multi-mode Gaussian unitary channels

Here we investigate a verification protocol for m-mode Gaussian unitary channel

$$\mathcal{U}_{\boldsymbol{S},\boldsymbol{d}}(\rho) = U_{\boldsymbol{S},\boldsymbol{d}}\rho U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger}, \tag{5}$$

where $\boldsymbol{S}\in \mathrm{Sp}(2m,\mathbb{R})$ and $\boldsymbol{d}\in\mathbb{R}^{2m}$ determine an affine mapping on phase space yielded by $U_{\boldsymbol{S},\boldsymbol{d}}$, in terms of average fidelity

$$\bar{F}(\mathcal{E},\mathcal{U}_{\boldsymbol{S},\boldsymbol{d}}) \coloneqq \int \frac{\mathrm{d}^{2m}\boldsymbol{\alpha}}{\pi^m}\lambda^m \mathrm{e}^{-\lambda|\boldsymbol{\alpha}|^2}\langle\boldsymbol{\alpha}|U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger}\mathcal{E}(|\boldsymbol{\alpha}\rangle\langle\boldsymbol{\alpha}|)U_{\boldsymbol{S},\boldsymbol{d}}|\boldsymbol{\alpha}\rangle, \tag{6}$$

where $|\boldsymbol{\alpha}\rangle \coloneqq |\alpha_1\rangle\otimes|\alpha_2\rangle\otimes\cdots\otimes|\alpha_m\rangle$, $\boldsymbol{\alpha}\coloneqq(\alpha_1,\alpha_2,\ldots,\alpha_m)\in\mathbb{C}^{\otimes m}$ is a tensor product of m coherent states, and $\lambda>0$. The verification scheme is shown in Fig. 1.

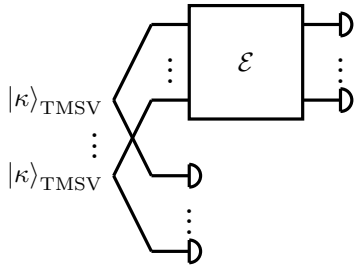


Figure 1: Our verification scheme for a multi-mode Gaussian unitary channel. Each $|\kappa\rangle_{\mathrm{TMSV}}$ denotes a two-mode squeezed vacuum state with squeezing parameter $\kappa = \mathrm{arctanh}\,\frac{1}{\sqrt{\lambda+1}}$. One mode of each $|\kappa\rangle_{\mathrm{TMSV}}$ goes through a multi-mode unknown bosonic quantum channel, denoted by $\mathcal{E}$ and represented by a square. Homodyne detections, represented by semicircles, are applied at each output mode of $\mathcal{E}$ and the other mode of each $|\kappa\rangle_{\mathrm{TMSV}}$.

Now we devise an average-fidelity witness for the average fidelity in Eq. (6).

Theorem 3 *The observable*

$$W_{U_{\boldsymbol{S},\boldsymbol{d}}} \coloneqq \mathbb{1} - \frac{\lambda}{\lambda+1}U_{\boldsymbol{S},\boldsymbol{d}}\otimes\mathbb{1}\left(\sum_{i=1}^{m} S_\kappa \hat{n}_i \otimes \mathbb{1} S_\kappa^{\dagger}\right)U_{\boldsymbol{S},\boldsymbol{d}}^{\dagger}\otimes\mathbb{1}, \tag{7}$$

where

$$S_\kappa \coloneqq \exp\frac{\kappa}{2}\left(\hat{a}_{\mathrm{A}'}\hat{a}_{\mathrm{R}} + \hat{a}_{\mathrm{A}'}^{\dagger}\hat{a}_{\mathrm{R}}^{\dagger}\right), \tag{8}$$

is an average-fidelity witness for $\bar{F}(\mathcal{E},\mathcal{U}_{\boldsymbol{S},\boldsymbol{d}})$ *on* $\mathcal{E}\otimes\mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)$.

To show Theorem 3, we need Lemmas 4 and 5.

Lemma 4 *To satisfy*

$$\int\frac{d^2\alpha}{\pi}\lambda\mathrm{e}^{-\lambda|\alpha|^2}\langle g\alpha|\,\mathcal{E}(|\alpha\rangle\langle\alpha|)\,|g\alpha\rangle = tr\left[O_{\mathrm{A}'\mathrm{R}}\mathcal{E}\otimes\mathcal{I}(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}})\right], \tag{9}$$

where $g>0$*, when* $g\leq\sqrt{\lambda+1}$*,*

$$O_{\mathrm{A}'\mathrm{R}} = S_\theta(G_\theta\otimes\mathbb{1})S_\theta^{\dagger}, \tag{10}$$

where

$$G_\theta = \sum_{n=0}^{\infty}\tanh^{2n}\theta\,|n\rangle\langle n|,\ \theta = \mathrm{arctanh}\,\frac{g}{\sqrt{\lambda+1}}; \tag{11}$$

when $g > \sqrt{\lambda+1}$,

$$O_{\mathrm{A'R}} = \tanh^2\theta' S_{\theta'}(\mathbb{1}\otimes G_{\theta'})S_{\theta'}^\dagger,\ \theta' = \operatorname{arctanh}\frac{\sqrt{\lambda+1}}{g}. \tag{12}$$

To devise an experimentally feasible verification scheme, we find lower bounds of the observables in Lemma 4 using the lemma below.

Lemma 5 *For any* $\theta > 0$, $m \in \mathbb{N}^+$,

$$G_\theta^{\otimes m} \geq \mathbb{1} - \frac{\sum_{i=1}^m \hat{n}_i}{\cosh^2\theta}. \tag{13}$$

Combining Lemma 5 with Lemma 4, we obtain the observable in Eq. (7).

The expectation value of the average-fidelity witness

$$\omega_{U_{\boldsymbol{S},\boldsymbol{d}}}(\mathcal{E}_{\mathrm{p}}) \coloneqq \mathrm{tr}\left[W_{U_{\boldsymbol{S},\boldsymbol{d}}}\mathcal{E}_{\mathrm{p}}\otimes\mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}^{\otimes m}\right)\right] \tag{14}$$

is a linear combination of the mean values and the covariances of quadrature operators (see Eq. (85) in ref. ([31])). To sample the mean values and the covariances of quadrature operators, the verifier only needs local homodyne detections. All the measurements can be accomplished by $m+5$ measurement settings. To assure a reliable certificate, the protocol requires

$$O\left(\frac{m^5\|\boldsymbol{S}\|_\infty^4\left(\|\boldsymbol{d}\|^2\sigma_1^2 + m\sigma_2^2\right)}{\varepsilon^2\ln(1/(1-\delta))}\right) \tag{15}$$

copies of $\mathcal{E}_{\mathrm{p}}$, where σ_1 and σ_2 are the upper bounds of variance of the measurement-outcome distribution of any single-mode quadrature operator and any products of two quadrature operators, respectively.

3.2 Verification of single-mode amplification channels

We investigate a verification protocol for Gaussian amplification channels in terms of average fidelity

$$\bar{F}_g(\mathcal{E}) = \int\frac{\mathrm{d}^2\alpha}{\pi}\lambda\mathrm{e}^{-\lambda|\alpha|^2}\langle g\alpha|\,\mathcal{E}(|\alpha\rangle\langle\alpha|)\,|g\alpha\rangle, \tag{16}$$

where $g > \lambda+1$ is the amplification gain. The maximum average fidelity in Eq. (16) can be achieved by a Gaussian amplification channel using two-mode squeezing [6]. We devise an average-fidelity witness in the following theorem.

Theorem 6 *The observable*

$$\frac{\lambda+1}{g^2}\left(\mathbb{1} - \frac{g^2-\lambda-1}{g^2}S_{\theta'}\mathbb{1}\otimes\hat{n}S_{\theta'}^\dagger\right) \tag{17}$$

is an average-fidelity witness for $\bar{F}_g(\mathcal{E})$ *on* $\mathcal{E}\otimes\mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}\right)$.

Theorem 6 can also be obtained from Lemmas 4 and 5.

The expectation value of the average-fidelity witness

$$\omega_{\mathrm{amp}}(\mathcal{E}_{\mathrm{p}}) \coloneqq \mathrm{tr}\left[W_{\mathrm{amp}}\mathcal{E}_{\mathrm{p}}\otimes\mathcal{I}\left(|\kappa\rangle\langle\kappa|_{\mathrm{TMSV}}\right)\right] \tag{18}$$

is a linear combination of quadrature covariances (see Eq. (97) in ref. ([31])). The mean value of the average-fidelity witness can be estimated by sampling the covariances of the quadrature operators using homodyne detections. The measurement scheme is similar to the one for verification of multi-mode Gaussian unitary channels. This verification protocol requires

$$O\left(\frac{g^6\sigma_2^2}{\varepsilon^2\ln(1/(1-\delta))}\right) \tag{19}$$

copies of $\mathcal{E}_p$ to obtain a reliable certificate.

4 Discussion and conclusion

We have presented a general verification framework for an optimal quantum channel by unifying the favourable features of quantum-state verification [3] and quantum-process benchmarking [4]. To develop our quantum-channel-verification framework, standard fidelity witness for quantum states has been generalized to an average fidelity witness for quantum channels per Definition 2. Rather than sampling a set of input states, our quantum-channel verification protocols require only one certain entangled input state and local measurements of an average-fidelity witness. Our verification protocols satisfy both completeness and soundness conditions per Definition 1, hence are reliable quantum-channel verification schemes.

We have presented the applications of our framework for the verification of two types of CPTP maps: multi-mode Gaussian unitary channels and single-mode amplification channels. We devise average-fidelity witnesses for these two types of quantum channels in Theorems 3 and Theorem 6, respectively, by truncating a thermal-state density operator in Lemma 5. The sample complexities scale polynomially with respect to number of modes m, maximum squeezing $\|\boldsymbol{S}\|_\infty$, phase-space displacement $\|\boldsymbol{d}\|$, and amplification gain g. Our measurement procedure comprises only local homodyne detections and is much simpler than the related work [4], as neither online two-mode squeezing nor quantum memories are required.

Different from quantum process tomography, our verification protocol's benchmark is average fidelity over an infinite set of gaussian-distributed coherent states. Our experimental setting uses only two-mode squeezed vacuum states and homodyne detections, which are feasible using current technology. Owing to extensive usage of Gaussian unitary operations, like squeezing, in continuous-variable quantum information processing and the remarkable utilization of amplification channels in quantum communication [5, 32], our verification protocols are important for testing components in continuous-variable quantum computing and quantum communication.

5 Acknowledgments

We thank Si-Hui Tan, Nana Liu and Yunlong Xiao for their valuable discussions and acknowledge funding from NSERC.

For the technical version of this work, please refer to arXiv:1904.10682.

References

[1] J. B. Altepeter, D. Branning, E. Jeffrey, T. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen, and A. G. White. Ancilla-assisted quantum process tomography. *Phys. Rev. Lett.*, 90(19):193601, 2003.

[2] U. L. Andersen, J. S. Neergaard-Nielsen, P. Van Loock, and A. Furusawa. Hybrid discrete- and continuous-variable quantum information. *Nat. Phys.*, 11(9):713, 2015.

[3] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert. Reliable quantum certification of photonic state preparations. *Nat. Commun.*, 6:8498, 2015.

[4] G. Bai and G. Chiribella. Test one to test many: a unified approach to quantum benchmarks. *Phys. Rev. Lett.*, 120(15):150502, 2018.

[5] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. *Phys. Rev. A*, 86:012327, Jul 2012.

[6] G. Chiribella and J. Xie. Optimal design and quantum benchmarks for coherent state amplifiers. *Phys. Rev. Lett.*, 110(21):213602, 2013.

[7] I. L. Chuang and M. A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.*, 44(11-12):2455–2467, 1997.

[8] M. P. da Silva, O. Landon-Cardinal, and D. Poulin. Practical characterization of quantum devices without tomography. *Phys. Rev. Lett.*, 107(21):210404, 2011.

[9] G. D'Ariano and P. L. Presti. Quantum tomography for measuring experimentally the matrix elements of an arbitrary quantum operation. *Phys. Rev. Lett.*, 86(19):4195, 2001.

[10] R. Farias and L. Aolita. Average channel-fidelity witnesses for benchmarking continuous-variable gates. *arXiv:1812.01968*, 2018.

[11] S. T. Flammia and Y.-K. Liu. Direct fidelity estimation from few pauli measurements. *Phys. Rev. Lett.*, 106(23):230501, 2011.

[12] M. Gluza, M. Kliesch, J. Eisert, and L. Aolita. Fidelity witnesses for fermionic quantum simulations. *Phys. Rev. Lett.*, 120(19):190501, 2018.

[13] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert. Direct certification of a class of quantum simulations. *Quant. Sci. Tech.*, 2(1):015004, 2017.

[14] N. Liu, T. F. Demarie, S.-H. Tan, L. Aolita, and J. F. Fitzsimons. Client-friendly continuous-variable blind and verifiable quantum computing. *arXiv:1806.09137*, 2018.

[15] M. Lobino, D. Korystov, C. Kupchak, E. Figueroa, B. C. Sanders, and A. Lvovsky. Complete characterization of quantum-optical processes. *Science*, 322(5901):563–566, 2008.

[16] A. I. Lvovsky, B. C. Sanders, and W. Tittel. Optical quantum memory. *Nat. photonics*, 3(12):706, 2009.

[17] E. Magesan, J. M. Gambetta, and J. Emerson. Scalable and robust randomized benchmarking of quantum processes. *Phys. Rev. Lett.*, 106(18):180504, 2011.

[18] E. Magesan, J. M. Gambetta, and J. Emerson. Characterizing quantum gates via randomized benchmarking. *Phys. Rev. A*, 85(4):042311, 2012.

[19] G. Masada, K. Miyata, A. Politi, T. Hashimoto, J. L. O'Brien, and A. Furusawa. Continuous-variable entanglement on a chip. *Nat. Photonics*, 9(5):316, 2015.

[20] Y. Miwa, J.-i. Yoshikawa, N. Iwata, M. Endo, P. Marek, R. Filip, P. van Loock, and A. Furusawa. Exploring a new regime for processing optical qubits: squeezing and unsqueezing single photons. *Phys. Rev. Lett.*, 113(1):013601, 2014.

[21] J. L. O'Brien, G. Pryde, A. Gilchrist, D. James, N. K. Langford, T. Ralph, and A. White. Quantum process tomography of a controlled-not gate. *Phys. Rev. Lett.*, 93(8):080502, 2004.

[22] S. Pallister, N. Linden, and A. Montanaro. Optimal verification of entangled states with local measurements. *Phys. Rev. Lett.*, 120(17):170502, 2018.

[23] J. Poyatos, J. I. Cirac, and P. Zoller. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Lett.*, 78(2):390, 1997.

[24] T. Proctor, K. Rudinger, K. Young, M. Sarovar, and R. Blume-Kohout. What randomized benchmarking actually measures. *Phys. Rev. Lett.*, 119(13):130502, 2017.

[25] S. Rahimi-Keshari, A. Scherer, A. Mann, A. T. Rezakhani, A. Lvovsky, and B. C. Sanders. Quantum process tomography with coherent states. *New J. Phys.*, 13(1):013006, 2011.

[26] E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussieres, M. George, R. Ricken, W. Sohler, and W. Tittel. Broadband waveguide quantum memory for entangled photons. *Nature*, 469(7331):512, 2011.

[27] S. Takeda and A. Furusawa. Universal quantum computing with measurement-induced continuous-variable gate sequence in a loop-based architecture. *Phys. Rev. Lett.*, 119(12):120504, 2017.

[28] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons. Resource-efficient verification of quantum computing using serfling's bound. *Npj Quantum Inf.*, 5(1):27, 2019.

[29] Y. Takeuchi and T. Morimae. Verification of many-qubit states. *Phys. Rev. X*, 8(2):021060, 2018.

[30] J. J. Wallman and S. T. Flammia. Randomized benchmarking with confidence. *New J. Phys.*, 16(10):103032, 2014.

[31] Y.-D. Wu and B. C. Sanders. Efficient verification of bosonic quantum channels via benchmarking. *arXiv:1904.10682*, 2019.

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

[33] J.-i. Yoshikawa, T. Hayashi, T. Akiyama, N. Takei, A. Huck, U. L. Andersen, and A. Furusawa. Demonstration of deterministic and high fidelity squeezing of quantum information. *Phys. Rev. A*, 76(6):060301, 2007.

[34] H. Zhu and M. Hayashi. Efficient verification of hypergraph states. *arXiv:1806.05565*, 2018.

[35] Q. Zhuang, T. Schuster, B. Yoshida, and N. Y. Yao. Scrambling and complexity in phase space. *Phys. Rev. A*, 99:062334, 2019.

Resource theory of asymmetric distinguishability

Xin Wang[1] Mark M. Wilde[2]

[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. This paper systematically develops the resource theory of asymmetric distinguishability, as initiated roughly a decade ago [K. Matsumoto, arXiv:1006.0302 (2010)]. The key constituents of this resource theory are quantum boxes, consisting of a pair of quantum states, which can be manipulated for free by means of an arbitrary quantum channel. We introduce bits of asymmetric distinguishability as the basic currency in this resource theory, and we prove that it is a reversible resource theory in the asymptotic limit, with the quantum relative entropy being the fundamental rate of resource interconversion. The distillable distinguishability is the optimal rate at which a quantum box consisting of independent and identically distributed (i.i.d.) states can be converted to bits of asymmetric distinguishability, and the distinguishability cost is the optimal rate for the reverse transformation. Both of these quantities are equal to the quantum relative entropy. The exact one-shot distillable distinguishability is equal to the Petz–Rényi relative entropy of order zero, and the exact one-shot distinguishability cost is equal to the max-relative entropy. Generalizing these results, the approximate one-shot distillable distinguishability is equal to the hypothesis testing relative entropy, and the approximate one-shot distinguishability cost is equal to the smooth max-relative entropy. As a notable application of the former results, we prove that the optimal rate of asymptotic conversion from a pair of i.i.d. quantum states to another pair of i.i.d. quantum states is fully characterized by the ratio of their quantum relative entropies.

1 Introduction

Distinguishability plays a central role in all sciences. That is, the ability to distinguish one possibility from another is what allows us to discover new scientific laws and make predictions of future possibilities. In the process of scientific discovery, we form a hypothesis based on conjecture, which is to be tested against a conventional or null hypothesis by repeated trials or experiments. With sufficient statistical evidence, one can determine which hypothesis should be rejected in favor of the other. If the null hypothesis is accepted, one can form alternative hypotheses to test against the null hypothesis in future experiments.

What is essential in this approach is the ability to perform repeated trials. Repetition allows for increasing the distinguishability between the two hypotheses. A natural question in this context is to determine how many trials are required to reach a given conclusion. If the two different hypotheses are relatively distinguishable, then fewer trials are required to decide between the possibilities. In this sense, distinguishability can be understood as a *resource*, because it limits the amount of effort that we need to invest in order to make decisions.

One of the fundamental settings in which distinguishability can be studied in a mathematically rigorous manner is statistical hypothesis testing. The basic setup is that one draws a sample x from one of two probability distributions $p \equiv \{p(x)\}_{x\in\mathcal{X}}$ or $q \equiv \{q(x)\}_{x\in\mathcal{X}}$, with common alphabet $\mathcal{X}$, with the goal being to decide from which distribution the sample x has been drawn. Let p be the null hypothesis and q the alternative. A Type I error occurs if one decides q when the distribution being sampled from is in fact p, and a Type II error occurs if one decides p when the distribution being sampled from is in fact q. The goal of asymmetric hypothesis testing is to minimize the probability of a Type II error, subject to an upper bound constraint on the probability of committing a Type I error.

In the scientific spirit of repeated experiments, we can modify the above scenario to allow for independent and identically distributed (i.i.d.) samples from either the distribution p or q. One of the fundamental results of asymptotic hypothesis testing is that, with a sufficiently large number of samples, it becomes possible to meet any upper bound constraint on the Type I error probability while having the Type II error probability decaying exponentially fast with the number of samples, with the optimal error exponent being given by the relative entropy [1, 2]:

$$D(p\|q) = \sum_{x\in\mathcal{X}} p(x)\log_2[p(x)/q(x)]. \tag{1}$$

That is, there exists a sequence of schemes that can achieve this error exponent for the Type II error probability while making the Type I error probability arbitrary small in the limit of a large number of samples. Meanwhile, the strong converse property holds: any sequence of schemes that has a fixed constraint on the Type I error probability is such that its Type II error probability cannot decay any faster than the exponent $D(p\|q)$. This gives a fundamental operational meaning to the relative entropy and represents one core link between hypothesis testing and information theory [3], the latter being the fundamental mathematical theory of communication [4].

Another perspective on the above process of decision making in hypothesis testing, the *resource-theoretic perspective* [5, 6] not commonly adopted in the literature on the topic, is that it is a process by which we *distill* distinguishability from the original distributions into a more standard form. That is, we can think of the distributions p and q being presented as a black box $\{p, q\}$. Given a sample $x \in \mathcal{X}$, we can perform a common transformation $\mathcal{T} : \mathcal{X} \to \{0, 1\}$ that outputs a single bit, "0" to decide p and "1" to decide q. The common transformation $\mathcal{T}$ can even be stochastic. In this way, one transforms

The detailed version is attached.

the initial box to a final box as

$$\{p, q\} \underset{\to}{\mathcal{T}} \{p_f, q_f\}, \tag{2}$$

where $p_f \equiv \{p_f(y)\}_{y\in\{0,1\}}$ and $q_f \equiv \{q_f(y)\}_{y\in\{0,1\}}$ are binary distributions. Then the probability of a Type I error is $p_f(1)$, and the probability of a Type II error is $q_f(0)$. Since the goal is to extract or distill as much distinguishability as possible, we would like for $q_f(0)$ to be as small as possible given a constraint $\varepsilon \in [0, 1]$ on $p_f(1)$ (i.e., $p_f(1) \leq \varepsilon$).

Once we have adopted this resource-theoretic approach to distinguishability, it is natural to consider two other questions, the first of which is the question of the *reverse process* [5, 6]. That is, we would like to start from initial binary distributions $p_i \equiv \{p_i(y)\}_{y\in\{0,1\}}$ and $q_i \equiv \{q_i(y)\}_{y\in\{0,1\}}$ having as little distinguishability as possible, and act on their samples with a common transformation $\mathcal{R} : \{0, 1\} \to \mathcal{X}$ in order to produce the distributions $p \equiv \{p(x)\}_{x\in\mathcal{X}}$ and $q \equiv \{q(x)\}_{x\in\mathcal{X}}$, while allowing for a slight error when reproducing p. That is, we would like to perform the *dilution* transformation

$$\{p_i, q_i\} \underset{\to}{\mathcal{R}} \{\tilde{p}, q\}, \tag{3}$$

where $\tilde{p} \equiv \{\tilde{p}(x)\}_{x\in\mathcal{X}}$ is a distribution satisfying $d(p, \tilde{p}) \leq \varepsilon$, for some suitable metric d of statistical distinguishability. In this way, we characterize the distinguishability of p and q in terms of the least distinguishable distributions p_i and q_i that can be diluted to prepare or simulate p and q, respectively. This dilution question is motivated by related questions in the theory of quantum entanglement [7].

The second, more general question is regarding the existence of a common transformation $\mathcal{T} : \mathcal{X} \to \mathcal{Z}$ that converts initial distributions p and q into final distributions $r \equiv \{r(z)\}_{z\in\mathcal{Z}}$ and $t \equiv \{t(z)\}_{z\in\mathcal{Z}}$:

$$\{p, q\} \underset{\to}{\mathcal{T}} \{\tilde{r}, t\}, \tag{4}$$

where $\tilde{r} \equiv \{\tilde{r}(z)\}_{z\in\mathcal{Z}}$ is a distribution satisfying $d(r, \tilde{r}) \leq \varepsilon$. One can then ask about the rate or efficiency at which it is possible to convert a pair of i.i.d. distributions to another pair of i.i.d. distributions.

This resource-theoretic approach to distinguishability offers a unique and powerful perspective on statistical hypothesis testing and distinguishability, similar to the perspective brought about by the seminal work on the resource theory of quantum entanglement [7], which has in turn inspired a flurry of activity on resource theories in quantum information and beyond [8]. Although the reverse process in (3) may seem nonsensical at first glance (why would one want to dilute fresh water to salt water? [9]), it plays a fundamental role in characterizing distinguishability as a resource, as well as for addressing the general question posed in (4). It is also natural from a thermodynamic or physical perspective to consider reversibility and cyclicity of processes. Another application for the reverse process is in understanding the minimal resources required for simulation in various quantum resource theories [8].

2 Main results

The main goal of this work is to develop systematically the resource-theoretic perspective on distinguishability, which was initiated in [5, 6]. More precisely, the theory developed here is a *resource theory of asymmetric distinguishability*, given that approximation is allowed for the first distribution in all of the distillation, dilution, and general transformation tasks mentioned above. The theory that we develop applies in the more general setting of *quantum* distinguishability, as it did in [5, 6], in particular when the distributions p and q are replaced by quantum states ρ and σ, respectively, and the common transformations allowed on a quantum box $\{\rho, \sigma\}$ are quantum channels.

Resource theory of asymmetric distinguishability— We begin by establishing the basics of the resource theory of asymmetric distinguishability. The basic object to manipulate in the resource theory of asymmetric distinguishability is the following "box":

$$\{\rho, \sigma\}, \tag{5}$$

where ρ and σ are quantum states acting on the same Hilbert space. The interpretation of the box $\{\rho, \sigma\}$ is that it corresponds to two different experiments or scenarios. In the first, the state ρ is prepared, and in the second, the state σ is prepared. The box is handed to another party, who is not aware of which experiment is being conducted. One basic manipulation in this resource theory is to transform this box into another box by means of any quantum physical operation $\mathcal{N}$, as allowed by quantum mechanics. Such physical operations are mathematically described by completely positive, trace-preserving (CPTP) maps and are known as quantum channels. By acting on the box $\{\rho, \sigma\}$ with the common quantum channel $\mathcal{N}$, one obtains the transformed box $\{\mathcal{N}(\rho), \mathcal{N}(\sigma)\}$. Observe that it is not necessary to know which experiment is being conducted in order to perform this transformation; one can easily perform it regardless of whether ρ or σ was prepared. For this reason, all quantum channels are allowed for free in this resource theory, so that the transformation $\{\rho, \sigma\} \underset{\to}{\mathcal{N}} \{\mathcal{N}(\rho), \mathcal{N}(\sigma)\}$ is allowed for free.

We then introduce the fundamental unit or currency of this resource theory, dubbed "bits of asymmetric distinguishability. To be specific, we introduce the following basic unit of currency or fiducial box

$$\{|0\rangle\langle 0|, \pi\}, \tag{6}$$

where $\pi := \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ is the maximally mixed qubit state. This represents one bit of asymmetric distinguishability, while the box $\{|0\rangle\langle 0|^{\otimes m}, \pi^{\otimes m}\}$ represents m bits of asymmetric distinguishability, which is a more powerful resource. Then the distinguishability distillation and dilution tasks amount to distilling bits of asymmetric distinguishability from a box $\{\rho, \sigma\}$ and diluting bits of asymmetric distinguishability to a box $\{\rho, \sigma\}$, respectively.

Exact one-shot distinguishability distillation and dilution—In the resource theory of asymmetric distinguishability, the goal of *exact distinguishability distillation* is to process a general box $\{\rho, \sigma\}$ with an arbitrary quantum channel in order to distill as many bits of asymmetric distinguishability as possible. Mathematically, we can phrase this task as the following optimization problem: $D_d^0(\{\rho, \sigma\}) := \log_2 \sup_{\mathcal{P}\in\text{CPTP}} \{M : \mathcal{P}(\rho) = |0\rangle\langle 0|,\ \mathcal{P}(\sigma) = \pi_M\}$, where the choice of D_d in $D_d^0(\{\rho, \sigma\})$ stands for *distillable distinguishability*, the "0" in $D_d^0(\{\rho, \sigma\})$ indicates that we do not

allow any error, CPTP denotes the set of CPTP maps (quantum channels), and $\pi_M := \frac{1}{M}|0\rangle\langle 0| + \left(1 - \frac{1}{M}\right)|1\rangle\langle 1|$. On the other hand, The goal of *exact distinguishability dilution* is the opposite: process as few bits of asymmetric distinguishability as possible, using free operations, in order to generate the box $\{\rho, \sigma\}$. Mathematically, we can phrase this task as the following optimization problem: $D_c^0(\{\rho,\sigma\}) := \log_2 \inf_{\mathcal{P}\in\text{CPTP}} \{M : \mathcal{P}(|0\rangle\langle 0|) = \rho,\ \mathcal{P}(\pi_M) = \sigma\}$.

We formally define the exact one-shot distinguishability distillation and dilution tasks, and we prove that the optimal number of bits of asymmetric distinguishability that can be distilled from a box $\{\rho, \sigma\}$ is equal to the Petz–Rényi relative entropy of order zero [10, 11] ,

$$D_d^0(\{\rho,\sigma\}) = D_0(\rho\|\sigma), \tag{7}$$

while the optimal number of bits of asymmetric distinguishability that can be diluted to a box $\{\rho, \sigma\}$ is equal to the max-relative entropy [11] ,

$$D_c^0(\{\rho,\sigma\}) = D_{\max}(\rho\|\sigma), \tag{8}$$

giving both of these quantities fundamental operational interpretations in the resource theory of asymmetric distinguishability. The operational interpretation of the Petz–Rényi relative entropy of order zero in the resource theory of asymmetric distinguishability suggests that it should indeed be known as the "min-relative entropy," as it was originally dubbed in [11].

Approximate one-shot distinguishability distillation and dilution—The goal of *ε-approximate distinguishability distillation* is to distill as many ε-approximate bits of asymmetric distinguishability from a given box $\{\rho, \sigma\}$. Mathematically, it corresponds to the following optimization $\varepsilon \in [0, 1]$:

$$D_d^\varepsilon(\{\rho,\sigma\}) := \log_2 \sup_{\mathcal{P}\in\text{CPTP}} \{M : \mathcal{P}(\rho) \approx_\varepsilon |0\rangle\langle 0|,\ \mathcal{P}(\sigma) = \pi_M\}. \tag{9}$$

Moreover, we can also generalize the distinguishability dilution task to the approximate case. In this case, we define the *ε-approximate distinguishability cost* of the box $\{\rho, \sigma\}$ to be the least number of ideal bits of asymmetric distinguishability that are needed to generate the box $\{\rho_\varepsilon, \sigma\}$, where $\rho_\varepsilon \approx_\varepsilon \rho$. This notion of approximate distinguishability cost is fully operational and the precise definition of the ε-approximate distinguishability cost of the box $\{\rho, \sigma\}$ is as follows:

$$D_c^\varepsilon(\{\rho,\sigma\}) := \log_2 \inf_{\mathcal{P}\in\text{CPTP}} \{M : \mathcal{P}(|0\rangle\langle 0|) \approx_\varepsilon \rho,\ \mathcal{P}(\pi_M) = \sigma\}. \tag{10}$$

We prove that the optimal number of bits of asymmetric distinguishability that can be distilled from a box $\{\rho, \sigma\}$ is equal to the hypothesis testing relative entropy [12, 13]

$$D_d^\varepsilon(\{\rho,\sigma\}) = D_H^\varepsilon(\rho\|\sigma), \tag{11}$$

where $D_H^\varepsilon(\rho\|\sigma)$ is the hypothesis testing relative entropy [12, 13]. Thus, the equality in (11) assigns to the hypothesis testing relative entropy an operational meaning as the ε-approximate distillable distinguishability of the box $\{\rho, \sigma\}$. This operational interpretation is directly linked to the role of $D_H^\varepsilon(\rho\|\sigma)$ in quantum hypothesis testing [14, 15, 16, 17, 13, 18].

On the other hand, we show that the optimal number of bits of asymmetric distinguishability that can be diluted to a box $\{\rho, \sigma\}$ is equal to the smooth max-relative entropy [11]

$$D_c^\varepsilon(\{\rho,\sigma\}) = D_{\max}^\varepsilon(\rho\|\sigma), \tag{12}$$

where $D_{\max}^\varepsilon(\rho\|\sigma)$ is the smooth max-relative entropy [11], defined as $D_{\max}^\varepsilon(\rho\|\sigma) := \inf_{\widetilde{\rho}:\frac{1}{2}\|\widetilde{\rho}-\rho\|_1\leq\varepsilon} D_{\max}(\widetilde{\rho}\|\sigma)$. Thus, the equality in (12) assigns to the smooth max-relative entropy a fundamental operational meaning as the ε-approximate distinguishability cost of the box $\{\rho, \sigma\}$.

We further prove that the optimization problems corresponding to one-shot distinguishability distillation and dilution, as well as the optimization corresponding to the quantum generalization of the transformation problem considered in (4), are characterized by semi-definite programs.

Asymptotic distillable distinguishability and distinguishability cost—We further reconsider the i.i.d. case of a box $\{\rho^{\otimes n}, \sigma^{\otimes n}\}$ in the context of approximate distillation and dilution. Notably, we prove that the resource theory is reversible in this setting, with the optimal rate of distillation or dilution equal to the quantum relative entropy.

Recall that the quantum relative entropy $D(\rho\|\sigma)$ is defined as [19] $D(\rho\|\sigma) := \text{Tr}[\rho\,(\log_2\rho - \log_2\sigma)]$, if $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$ and $D(\rho\|\sigma) = \infty$ otherwise. By defining the asymptotic distillable distinguishability and asymptotic distinguishability cost of the box $\{\rho, \sigma\}$ as follows:

$$D_d(\{\rho,\sigma\}) := \lim_{\varepsilon\to 0}\lim_{n\to\infty} \frac{1}{n} D_d^\varepsilon(\{\rho^{\otimes n}, \sigma^{\otimes n}\}), \tag{13}$$

$$D_c(\{\rho,\sigma\}) := \lim_{\varepsilon\to 0}\lim_{n\to\infty} \frac{1}{n} D_c^\varepsilon(\{\rho^{\otimes n}, \sigma^{\otimes n}\}), \tag{14}$$

respectively, we conclude from the quantum Stein's lemma [14, 15] and the asymptotic equipartition property for the smooth max-relative entropy [20] that

$$D_d(\{\rho,\sigma\}) = D_c(\{\rho,\sigma\}) = D(\rho\|\sigma), \tag{15}$$

thus demonstrating the fundamental operational interpretation of the quantum relative entropy in the resource theory of asymmetric distinguishability. As a consequence of the fundamental equality in (15), we conclude that the resource theory of asymmetric distinguishability is reversible in the asymptotic setting.

The implication of this result is that the rate or efficiency at which a pair of i.i.d. quantum states can be converted to another pair of i.i.d. quantum states is fully characterized by the ratio of their quantum relative entropies. Specifically, an (n, m, ε) box transformation protocol for the boxes $\{\rho, \sigma\}$ and $\{\tau, \omega\}$ consists of a channel $\mathcal{N}^{(n)}$ such that $\mathcal{N}^{(n)}(\rho^{\otimes n}) \approx_\varepsilon \tau^{\otimes m}$ and $\mathcal{N}^{(n)}(\sigma^{\otimes n}) = \omega^{\otimes m}$. A rate R is *achievable* if for all $\varepsilon \in (0, 1]$, $\delta > 0$, and sufficiently large n, there exists an $(n, n[R-\delta], \varepsilon)$ box transformation protocol. The optimal box transformation rate $R(\{\rho, \sigma\} \to \{\tau, \omega\})$ is then equal to the supremum of all achievable rates.

We further prove that the following fundamental equality for the resource theory of asymmetric distinguishability:

$$R(\{\rho,\sigma\} \to \{\tau,\omega\}) = \frac{D(\rho\|\sigma)}{D(\tau\|\omega)}, \tag{16}$$

indicating that the quantum relative entropy plays a central role as the optimal conversion rate between boxes. We note that the equality in (16) was established independently in [21].

References

[1] Charles Stein. Information and comparison of experiments.

[2] Herman Chernoff. Large-sample theory: Parametric case. *The Annals of Mathematical Statistics*, 27(1):1–22, March 1956.

[3] Richard Blahut. Hypothesis testing and information theory. *IEEE Transactions on Information Theory*, 20(4):405–417, July 1974.

[4] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.

[5] Keiji Matsumoto. Reverse test and characterization of quantum relative entropy. October 2010. arXiv:1010.1030.

[6] Keiji Matsumoto. Reverse test and characterization of quantum relative entropy. In *The Second Nagoya Winter Workshop on Quantum Information, Measurement, and Foundations*, 2011. Slides available at https://sites.google.com/site/nww2011/home/talks-slides/matsumoto.pdf.

[7] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, November 1996. arXiv:quant-ph/9604024.

[8] Eric Chitambar and Gilad Gour. Quantum resource theories. *Reviews of Modern Physics*, 91(2):025001, April 2019. arXiv:1806.06107.

[9] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Transactions on Information Theory*, 48(10):2637–2655, October 2002. arXiv:quant-ph/0106052.

[10] Dénes Petz. Quasi-entropies for finite quantum systems. *Reports in Mathematical Physics*, 23:57–65, 1986.

[11] Nilanjana Datta. Min- and max-relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826, June 2009. arXiv:0803.2770.

[12] Francesco Buscemi and Nilanjana Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56(3):1447–1460, March 2010. arXiv:0902.0158.

[13] Ligong Wang and Renato Renner. One-shot classical-quantum capacity and hypothesis testing. *Physical Review Letters*, 108(20):200501, May 2012. arXiv:1007.5456.

[14] Fumio Hiai and Dénes Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Communications in Mathematical Physics*, 143(1):99–114, December 1991.

[15] Tomohiro Ogawa and Hiroshi Nagaoka. Strong converse and Stein's lemma in quantum hypothesis testing. *IEEE Transactions on Information Theory*, 46(7):2428–2433, November 2000. arXiv:quant-ph/9906090.

[16] Masahito Hayashi. Hypothesis testing approach to quantum information theory. In *COE Symposium on Quantum Information Theory*, pages 15–16, Kyoto, Japan, 2003.

[17] Masahito Hayashi. Hypothesis testing approach to quantum information theory. In *1st Asia-Pacific Conference on Quantum Information Science*, National Cheng Kung University, Tainan, Taiwan, 2004.

[18] Masahito Hayashi. Role of hypothesis testing in quantum information theory. In *Asian Conference on Quantum Information Science (AQIS 17)*, National University of Singapore, Singapore, September 2017. arXiv:1709.07701.

[19] Hisaharu Umegaki. Conditional expectations in an operator algebra IV (entropy and information). *Kodai Mathematical Seminar Reports*, 14(2):59–85, 1962.

[20] Marco Tomamichel, Roger Colbeck, and Renato Renner. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory*, 55(12):5840–5847, December 2009. arXiv:0811.1221.

[21] Francesco Buscemi, David Sutter, and Marco Tomamichel. Manuscript in preparation. May 2019.

Two-stage Estimation for Quantum Detector Tomography

Yuanlong Wang[1] * Shota Yokoyama[2,4] † Daoyi Dong[2] ‡ Ian R. Petersen[3] §
Elanor H. Huntington[3,4] ¶ Hidehiro Yonezawa[2,4] ‖

[1]*Centre for Quantum Dynamics, Griffith University, Brisbane QLD 4111, Australia*
[2] *School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2600, Australia*
[3] *Research School of Engineering, Australian National University, Canberra, ACT 2601, Australia*
[4]*Centre for Quantum Computation and Communication Technology, Australian Research Council, Canberra, ACT 2600, Australia*

Abstract. Quantum detector tomography is a fundamental technique for calibrating quantum devices and performing quantum engineering tasks. In this abstract, a novel quantum detector tomography method is proposed. First, a series of different probe states are used to generate measurement data. Then, using constrained linear regression estimation, a stage-1 estimation of the detector is obtained. Finally, the positive semidefinite requirement is added to guarantee a physical stage-2 estimation. This Two-stage Estimation (TSE) method has computational complexity $O(nd^2M)$, where n is the number of d-dimensional detector matrices and M is the number of different probe states each with some copies. We establish an upper bound for the tomography error. We perform simulation and a quantum optical experiment to testify the effectiveness of the TSE method.

Keywords: Quantum system, quantum detector tomography, two-stage estimation, computational complexity

1 Introduction

Measurement, on a quantum entity or using a quantum object, is the connection between the classical (non-quantum) world and the quantum domain, and plays a fundamental role in investigating and controlling a quantum system [1]-[3]. For example, quantum computation can be performed through a series of appropriate measurements in certain schemes [4]. In quantum communication, measurement is a vital part of quantum key distribution [5]. In quantum metrology, adaptive measurement can achieve the Heisenberg limit in phase estimation [6].

Since quantum measurement can be viewed as a class of quantum resource, its investigation and characterization is fundamentally important. Quantum detector tomography is a technique to characterize quantum measurement devices [7]-[8], and paves the way for other estimation tasks like quantum state tomography [9]-[13], Hamiltonian identification [14]-[17] and quantum process tomography [18]-[20].

The investigation of protocols for quantum detector tomography dates back to [21], where the Maximum Likelihood Estimation (MLE) method is employed to reconstruct an unknown POVM detector. As one of the most widely recognized methods [9, 22], MLE can preserve the positivity and completeness of the detector, but it is difficult to characterize the error and computational complexity. In [23, 24], phase-insensitive (non-diagonal) detector tomography was modelled as a convex quadratic optimization problem and an efficient numerical solution was obtained, and then was developed in [25] and [26] to recursively solve it.

In this abstract, we propose a novel quantum detector tomography protocol, which is applicable to both phase-insensitive and general phase-sensitive detectors. We first input a series of different states (probe states) to the detector, and then collect all the measurement data. The forthcoming algorithm mainly consists of two stages: in the first stage, we find a constrained least square estimate, which corresponds to a Hermitian estimate satisfying the completeness constraint. However, this estimate can be non-physical; i.e., the estimated detectors may have negative eigenvalues. Hence, in the second stage we further design a series of matrix transformations preserving the Hermitian and completeness constraint to find a physical approximation based on the result in the first stage, and thus obtain the final physical estimate. Our Two-stage Estimation (TSE) method has computational complexity $O(nd^2M)$, where n and d are the number and dimension of the detector matrices, respectively, and we have M different probe states with N copies in total. We further prove an error upper bound $O(\frac{d^5n^2}{N})$ on the condition that the probe states are optimal (if not optimal, the specific form of the bound is also given in [27]). This theoretical characterization of the speed and teh error is not common in other detector tomography methods. We perform numerical simulation to validate the theoretical analysis and compare our algorithm with MLE method. Finally, we slightly modify our method to cater to a practical experiment situation, and we perform quantum optical experiments using two-mode coherent states to testify the effectiveness of our method.

For the full version of this work, please refer to [27].

*yuanlong.wang.qc@gmail.com
†s.yokoyama@adfa.edu.au
‡daoyidong@gmail.com
§i.r.petersen@gmail.com
¶elanor.huntington@anu.edu.au
‖h.yonezawa@adfa.edu.au

2 Problem formulation

Suppose the true values of a set for a detector are $\{P_i\}_{i=1}^n$ such that $\sum_{i=1}^n P_i = I$ (*completeness requirement*) with each P_i being d-dimensional Hermitian and positive semidefinite. We design M different quantum states ρ_j (*probe states*, each with N/M copies) and record the measurement results $\hat{p}_{ij}$ as the estimate of $p_{ij} = \mathrm{Tr}(P_i\rho_j)$. We then aim to solve the following optimization problem:

Problem 1 *Given experimental data* $\{\hat{p}_{ij}\}$. *Solve* $\min_{\{\hat{P}_i\}} \sum_{i=1}^n \sum_{j=1}^M [\hat{p}_{ij} - \mathrm{Tr}(\hat{P}_i\rho_j)]^2$ *such that* $\sum_{i=1}^n \hat{P}_i = I$ *and* $\hat{P}_i \geq 0$ *for* $1 \leq i \leq n$.

3 General procedure

We now generalize the procedure of our TSE algorithm and analyze its computational complexity. We do not consider the time spent on experiments, since it depends on the experimental realization.

Step 1. Stage-1 Approximation. Choose certain matrix basis (e.g., Pauli matrices) to parameterize $\{P_i\}_{i=1}^n$ as a real vector. Also parameterize each ρ_j as a known real vector. Measurement thus establish a linear mapping between measurement data and the unknown detector vector. The completeness requirement is thus a linear constraint on the unknown vector, and using constrained linear regression one can obtain a Constrained Least Square (CLS) solution, which is then transformed as the stage-1 approximation (*CLS estimation*) $\{\hat{E}_i\}_{i=1}^n$. At this stage, each $\hat{E}_i$ is Hermitian and they sum to identity, but they may not all be positive semidefinite.

Step 2. Difference Decomposition. For each $\hat{E}_i$, analytically solve $\min ||\hat{G}_i||$ (Frobenius norm) s.t. $\hat{E}_i = \hat{F}_i - \hat{G}_i$, $\hat{G}_i \geq 0$ and $\hat{F}_i \geq 0$. In fact, in the diagonal basis the optimal $-\hat{G}_i$ is composed of the negative eigenvalues of $\hat{E}_i$, and $\hat{F}_i$ the positive eigenvalues.

Step 3. Stage-2 Approximation. From $I = \sum_i \hat{E}_i = \sum_i \hat{F}_i - \sum_i \hat{G}_i$, we have $I + \sum_i \hat{G}_i = \sum_i \hat{F}_i$. Since each $\hat{G}_i$ is positive semidefinite, we can decompose $I + \sum_i \hat{G}_i = \hat{C}\hat{U}\hat{U}^\dagger\hat{C}^\dagger$ where $\hat{U}$ is any unitary. By minimizing $||\hat{C}\hat{U} - I||$, we choose $\hat{U} = \sqrt{\hat{C}^\dagger\hat{C}}\hat{C}^{-1}$. We finally have $\sum_i \hat{U}^\dagger\hat{C}^{-1}\hat{F}_i\hat{C}^{-\dagger}\hat{U} = I$. The final estimate of the detector is thus $\hat{P}_i = \hat{U}^\dagger\hat{C}^{-1}\hat{F}_i\hat{C}^{-\dagger}\hat{U}$, which both are positive semidefinite and sum to identity.

Each of the above steps has closed-form analytical formula, hence the total computational complexity can be analyzed as $O(nd^2M)$. We further theoretically characterize the error as:

Theorem 1 *When the probe states are optimal, the final mean squared error (MSE) of our algorithm* $E(\sum_i ||\hat{P}_i - P_i||^2)$ *scales as* $O(\frac{d^5n^2}{N})$.

The "optimal" here means the probe states have enough diversity. For its specific meanings and the non-optimal version of Theorem 1, please refer to the full version [27].

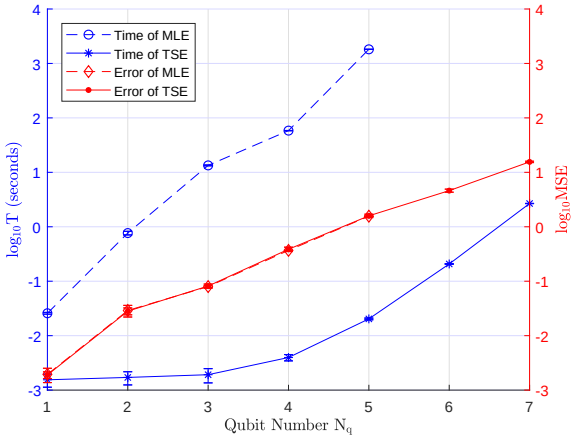


Figure 1: Comparison between our TSE algorithm with MLE for different qubit number N_q ($d = 2^{N_q}$).

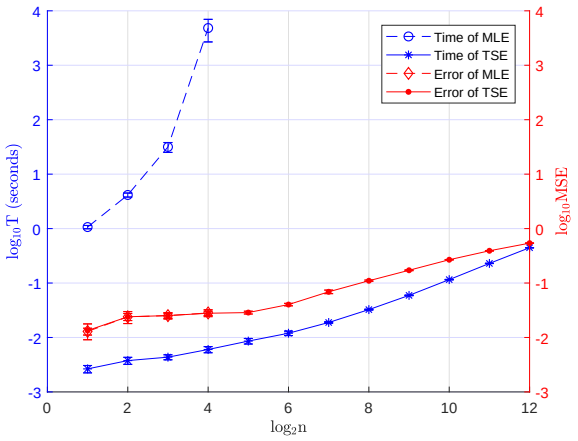


Figure 2: Comparison between our algorithm with MLE for different n number of matrices.

4 Optimization of the Coherent Probe States

The exact solutions of optimal photon-number states are already presented in the full version of Theorem 1 [27]. However, in practice coherent states are more commonly used. Then how to optimize them, w.r.t. the final estimation error? Since the detector to be estimated is usually unknown in practice, the optimization among all the possible probe states should be independent of the specific detector. An advantage of our TSE method is that an explicit error upper bound is presented (see [27]), which does not involve the specific form of the detector. In the full version we investigated the optimization of the coherent probe states (about their types and amplitudes).

5 Numerical Results

We compare our TSE method with the Maximum Likelihood Estimation (MLE) method [9] via two simulation examples. Note that the detector tomography method via a MLE is in essence a numerical searching algorithm and lacks a theoretical characterization of the computational complexity. For each detector, we first run our algorithm,

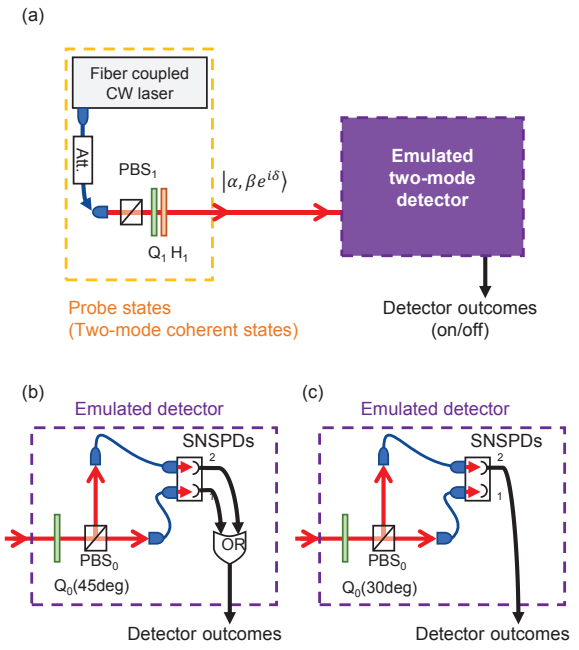


Figure 3: Experimental setup [28].

and then adjust the MLE method such that the averaged estimation error of MLE is within $[95\%, 105\%]$ of the error of our algorithm. In Fig. 1, we see that for $N_q \geq 4$ qubits our algorithm can be faster than MLE by over 4 orders of magnitude. Fig. 2 is the case when n increases, and we see the simulation performance of TSE matches the computational complexity analysis w.r.t. $T = O(n)$ very well for $n \geq 2^8$.

6 Experimental Results

Experimental setup and modified protocol: We briefly explain the entire experimental setup (as in Fig. 3(a)), which determines the structure of the detector to be estimated. More details about this setup can be found in [28].

In Fig. 3, the purple dashed box corresponds to the emulated quantum detector which works as two-mode inputs - one binary output detector. Two independent quantum modes are encoded within orthogonal polarization modes in one optical beam at the detector input. The two-mode quantum detector consists of two superconducting nanowire detectors (SNSPDs), a polarization beam splitter (PBS), a quarter wave plate (QWP), and a logical OR gate. The polarization of the input beam is first rotated by a QWP_0 with the azimuth angle of $45°$ (Fig. 3(b)), or $30°$ (Fig. 3(c)), respectively. Then the beam is split into two spatially separated beams via PBS_0, and they are injected into two SNSPDs through optical fibers. The photon counting signals from the two SNSPDs are sent to a logical OR gate, and the final detector output is obtained as on/off signal corresponding to POVMs of P_1 and P_0 ($P_0 + P_1 = I$). Fig. 3(b) and (c) are different specific settings to generate different emulated detectors.

This experimental setup leads to a special class of detectors. Specifically, we require them to be block diagonal (e.g., see [28]):

$$P_i = L_1^{(i)} \oplus L_2^{(i)} \oplus ... \oplus L_m^{(i)}, \tag{1}$$

where m is the number of different blocks and $L_j^{(i)} \geq 0$ is $d_j \times d_j$ dimensional, with $\sum_{j=1}^m d_j = d$. Hence, we need to modify our original TSE method to reconstruct $\{P_i\}$.

The block-diagonal requirement can be transformed as a second linear constraint, apart from the *completeness requirement*. Hence, constrained least square still works. Due to experiment imperfection, we add *Tikhonov regularization* [29] to the constrained linear regression estimation in Step 1 of TSE to reduce the estimation error. Then since the diagonal blocks of the detector are in essence decoupled with each other, we perform Step 2 and Step 3 on each block $L_j^{(i)}$ separately, to pull the stage-1 estimation to positive semidefiniteness.

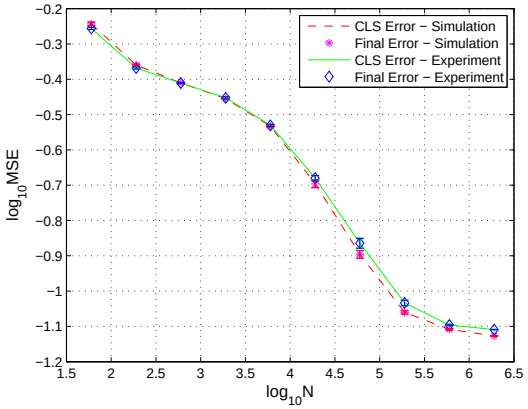


Figure 4: Experimental and simulation results.

Experimental result: We prepare 19 different two-mode coherent states

$$|\alpha, \beta e^{i\delta}\rangle = \exp[-\frac{1}{2}(\alpha^2 + \beta^2)] \sum_{j,k}^{\infty} \frac{\alpha^j \beta^k e^{ik\delta}}{\sqrt{j!k!}} |j, k\rangle$$

to perform the tomography experiment. The detector is 6×6 dimensional, and the result is as in Fig. 4, where we use the modified version TSE to reconstruct the detector from experimental data and also the simulated data as a comparison. We can see the experiment matches simulation result very well.

7 Conclusion

In this abstract, we have proposed a novel Two-stage Estimation (TSE) quantum detector tomography method. We analysed the computational complexity for our algorithm and established an upper bound for the estimation error. We discussed the optimization of the coherent probe states, and presented simulation results to illustrate the performance of our algorithm. Quantum optical experiments were performed and the results validated the effectiveness of our method.

References

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge, U.K.: Cambridge Univ. Press, 2000.

[2] H. M. Wiseman and G. J. Milburn, *Quantum Measurement and Control.* Cambridge, U.K.: Cambridge Univ. Press, 2009.

[3] M. Berta, J. M. Renes, and M. M. Wilde, "Identifying the information gain of a quantum measurement," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7987-8006, 2014.

[4] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Phys. Rev. Lett.*, vol. 86, no. 22, p. 5188, 2001.

[5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. P1, pp. 7-11, 2014.

[6] B. L. Higgins, D. W. Berry, S. D. Bartlett, H. M. Wiseman, and G. J. Pryde, "Entanglement-free Heisenberg-limited phase estimation," *Nature*, vol. 450, no. 7168, pp. 393-396, 2007.

[7] A. Luis and L. L. Sánchez-Soto, "Complete characterization of arbitrary quantum measurement processes," *Phys. Rev. Lett*, vol. 83, no. 18, p. 3573, 1999.

[8] G. M. D'Ariano, L. Maccone, and P. L. Presti, "Quantum calibration of measurement instrumentation," *Phys. Rev. Lett*, vol. 93, no. 25, p. 250407, 2004.

[9] M. Paris and J. Řeháček, *Quantum State Estimation*, vol. 649 of Lecture Notes in Physics, Springer, Berlin, 2004.

[10] B. Qi, Z. Hou, L. Li, D. Dong, G.-Y. Xiang, and G.-C. Guo, "Quantum state tomography via linear regression estimation," *Sci. Rep.*, vol. 3, no. 3496, 2013.

[11] M. Zorzi, F. Ticozzi, and A. Ferrante, "Minimum relative entropy for quantum estimation: Feasibility and general solution," *IEEE Trans. Inf. Theory*, vol. 60, no. 1, pp. 357-367, 2014.

[12] J. Haah, A. W. Harrow, Z. Ji, X. Wu, and N. Yu, "Sample-optimal tomography of quantum states," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 5628-5641, 2017.

[13] B. Qi, Z. Hou, Y. Wang, D. Dong, H.-S. Zhong, L. Li, G.-Y. Xiang, H. M. Wiseman, C.-F. Li and G.-C. Guo, "Adaptive quantum state tomography via linear regression estimation: Theory and two-qubit experiment," *npj Quantum Inform.*, vol. 3, no. 1, p. 19, 2017.

[14] D. Burgarth and K. Yuasa, "Quantum system identification," *Phys. Rev. Lett.*, vol. 108, no. 8, p. 080502, 2012.

[15] J. Zhang and M. Sarovar, "Quantum Hamiltonian identification from measurement time traces," *Phys. Rev. Lett.*, vol. 113, no. 8, p. 080401, 2014.

[16] Y. Wang, Q. Yin, D. Dong, B. Qi, I. R. Petersen, Z. Hou, H. Yonezawa, and G.-Y. Xiang, "Quantum gate identification: Error analysis, numerical results and optical experiment," *Automatica*, vol. 101, pp. 269-279, 2019.

[17] Y. Wang, D. Dong, B. Qi, J. Zhang, I. R. Petersen, and H. Yonezawa, "A quantum Hamiltonian identification algorithm: Computational complexity and error analysis," *IEEE Trans. Autom. Control*, vol. 63, no. 5, pp. 1388-1403, 2018.

[18] J. Fiurášek and Z. Hradil, "Maximum-likelihood estimation of quantum processes," *Phys. Rev. A*, vol. 63, no. 2, p. 020101, 2001.

[19] M. F. Sacchi, "Maximum-likelihood reconstruction of completely positive maps," *Phys. Rev. A*, vol. 63, no. 5, p. 054104, 2001.

[20] Z. Ji, G. Wang, R. Duan, Y. Feng, and M. Ying, "Parameter estimation of quantum channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5172-5185, 2008.

[21] J. Fiurášek, "Maximum-likelihood estimation of quantum measurement," *Phys. Rev. A*, vol. 64, no. 2, p. 024102, 2001.

[22] V. D'Auria, N. Lee, T. Amri, C. Fabre, and J. Laurat, "Quantum decoherence of single-photon counters," *Phys. Rev. Lett.*, vol. 107, no. 5, p. 050504, 2011.

[23] J. S. Lundeen, A. Feito, H. Coldenstrodt-Ronge, K. L. Pregnell, C. Silberhorn, T. C. Ralph, J. Eisert, M. B. Plenio, and I. A. Walmsley, "Tomography of quantum detectors," *Nat. Phys.* vol. 5, no. 1, p. 27, 2009.

[24] A. Feito, J. S. Lundeen, H. Coldenstrodt-Ronge, J. Eisert, M. B. Plenio, and I. A. Walmsley, "Measuring measurement: Theory and practice," *New J. Phys.*, vol. 11, no. 9, p. 093038, 2009.

[25] L. Zhang, H. B. Coldenstrodt-Ronge, A. Datta, G. Puentes, J. S. Lundeen, X.-M. Jin, B. J. Smith, M. B. Plenio, and I. A. Walmsley, "Mapping coherence in measurement via full quantum tomography of a hybrid optical detector," *Nat. Photon.*, vol. 6, no. 6, pp. 364-368, 2012.

[26] L. Zhang, A. Datta, H. B. Coldenstrodt-Ronge, X.-M. Jin, J. Eisert, M. B. Plenio, and I. A. Walmsley, "Recursive quantum detector tomography," *New J. Phys.*, vol. 14, no. 11, p. 115005, 2012.

[27] Y. Wang, S. Yokoyama, D. Dong, I. R. Petersen, E. H. Huntington, and H. Yonezawa, "Two-stage estimation for quantum detector tomography: Error analysis, numerical and experimental results," *arXiv preprint*, arXiv: 1905.05323, 2019.

[28] S. Yokoyama, N. D. Pozza, T. Serikawa, K. B. Kuntz, T. A. Wheatley, D. Dong, E. H. Huntington, and H. Yonezawa, "The quantum entanglement of measurement," *arXiv preprint*, quant-ph, arXiv: 1705.06441, 2017.

[29] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge, U.K.: Cambridge Univ. Press, 2004.

From quantum coherence to nonclassicality and metrological power

Kok Chuan Tan[1] * Hyukjoon Kwon[2] Tyler Volkoff[3] Hyunseok Jeong[1]

[1] *Department of Physics and Astronomy, Seoul National University, Seoul, 08826, Korea*
[2] *QOLS, Blackett Laboratory, Imperial College London, London SW7 2AZ, United Kingdom*
[3] *Department of Physics, Konkuk University, Seoul 05029, Korea*

Abstract. We consider the resource theory of nonclassicality for quantum light. Under this resource theory, we discuss two nonclassicality measures, one with a fundamental interpretation and another with an operational interpretation. The first of these measures is the amount of quantum coherence or superposition between the coherent states, thus relating nonclassicality in radiation fields to the superposition principle. The second measure is called the metrological power, which quantifies how sensitive a quantum state is to displacement operations. These examples demonstrate how the resource theory of nonclassicality can help to refine our understanding of nonclassicality in quantum systems of light and in what ways they may be useful.

Keywords: Coherence, Nonclassicality, Quantum Optics, Quantum Metrology

1 Introduction

One important aspect of the field of quantum information concerns the study of nonclassical quantum resources. Examples of quantum resources include notions of nonclassicality such as entanglement[1] and quantum coherence [2]. A quantum resource theory is a set of axioms and definitions which identifies a quantum resource of particular interest, and specifies certain ground rules that should reasonably be obeyed in order to qualify as resource measure.

Here, we consider the resource theory of nonclassicality based on the set of coherent states of light[3, 4](not to be confused with the notion of coherence for finite dimensional systems). The set of coherent states is denoted by $\{|\alpha\rangle\}$ and is a minimum uncertainty state which most closely resembles classical light. Every quantum state of light ρ permits a diagonal representation with respect to the set of coherent states of the form

$$\hat{\rho} = \int d^2\alpha P(\alpha) |\alpha\rangle \langle\alpha|.$$

The coefficient $P(\alpha)$ is called the Glauber-Sudarshan P-distribution [3]. The P-distribution always sums to 1 but may display negativities for some quantum states. A state is classical when it is expressible as a classical mixture of coherent states, i.e. when P corresponds to some classical probability distribution. Otherwise, we say that P displays negativities and the state is nonclassical.

We first discuss how a resource theory of nonclassical light may be formulated based on quantum linear optical operations. In such a resource theory, the nonclassicality in quantum systems of light are quantified via linear optical monotones — quantities that do not increase under linear optical operations. We then discuss 2 examples of such monotones: (i) the amount of coherent superposition among the set of coherent states, and (ii) the metrological power. The former has a fundamental interpretation in terms of the superposition principle, while the latter has operational significance in quantum metrology.

*bbtankc@gmail.com

2 Preliminaries

In this section, we will introduce some basic concepts surrounding the resource theory of nonclassicality in light, which was introduced in Ref. [4].

The essential idea is to quantify nonclassicality using linear optical monotones. Linear optical monotones are quantities that always decreases under linear optical maps, which are defined as any quantum operation expressible as some combination of displacement operations, beam splitters and phase shifters together with possible interations with a classical ancilla. A formal characterization is given below:

Define a general N-mode bosonic creation operator of the form $\hat{a}^\dagger_{\boldsymbol{\mu}} = \sum_{n=1}^N \mu_n \hat{a}^\dagger_n$ with complex values μ_n, and define $\boldsymbol{\mu} = (\mathrm{Re}[\mu_1], \mathrm{Im}[\mu_1], \mathrm{Re}[\mu_2], \mathrm{Im}[\mu_2], \cdots, \mathrm{Re}[\mu_N], \mathrm{Im}[\mu_N])^T$ to be a real $2N$-dimensional unit vector satisfying $||\boldsymbol{\mu}||^2 := \sum_{n=1}^N |\mu_n|^2 = 1$. A multi-mode linear optical unitary operation is any $\hat{U}_L$ which transforms $\hat{a}^\dagger_{\boldsymbol{\mu}}$ into $\hat{a}^\dagger_{\boldsymbol{\mu}'} + \bigoplus_{n=1}^N \alpha_n \mathbb{1}_n$, while satisfying the condition $||\boldsymbol{\mu}||^2 = ||\boldsymbol{\mu}'||^2$. Here, α_n is a complex number and $\mathbb{1}_n$ is the identity operator on the n-th mode.

Using the above definition of a linear optical unitary, a linear optical map is defined as:

$$\Phi_L(\hat{\rho}_A) = \mathrm{Tr}_E(\hat{U}_L \hat{\rho}_A \otimes \hat{\sigma}_E \hat{U}_L^\dagger),$$

where $\hat{\sigma}_E$ is a classical state.

In the resource theory of nonclassicality, we say that $\mathcal{N}$ is a nonclassicality measure if (i) $\mathcal{N}(\rho) > 0$ implies ρ is nonclassical, (ii) $\mathcal{N}(\rho) \geq \mathcal{N}[\Phi_L(\rho)]$, i.e. $\mathcal{N}$ is a linear optical monotone, and (iii) $\mathcal{N}$ is a convex function of state.

3 Coherence and nonclassicality

Here, we will discuss the connection between coherence in finite dimensional systems[5, 6] and nonclassicality in

quantum light. The presentation here will focus on pure states, which is sufficient for the discussion at hand. A more detailed discussion of the construction for mixed states may be found in Ref. [4].

The key complications that prevent nonclassicality in quantum light from being directly interpreted as coherences are: (i) coherence measures $\mathcal{C}$ typically apply only to finite dimensional systems, and (ii) coherence measures are defined with respect to a complete set of orthogonal set of basis vectors $\{|i\rangle\}$ while nonclassicality defined with respect to the set of coherent states $\{|\alpha\rangle\}$, which is overcomplete and not orthogonal.

These difficulties may be overcome via an orthogonalization procedure that is performed on the input state. This procedure essentially draws from the set of coherent states $\{|\alpha\rangle\}$ to set up an orthogonal basis. After the orthogonalization procedure, one may then apply any coherence measure of choice on the resulting state.

We now describe the orthogonalization procedure with respect to the coherent states in greater detail. We define $|\psi_i\rangle$ through the recursion relation

$$|\psi_i\rangle = |\psi_{i-1}\rangle - |\alpha_{i-1}\rangle \langle\alpha_{i-1}|\psi_{i-1}\rangle,$$

where the coherent state $|\alpha_i\rangle$ satisfies $\langle\alpha_i|\psi_i\rangle = \max_{\alpha'}\langle\alpha'|\psi_i\rangle$ and the initial state $|\psi_1\rangle = |\psi\rangle$ is some given pure quantum state of interest.

Given some finite series of vectors $\{|\alpha_i\rangle\}$ where $i = 1, \ldots, N$, we define the CNOT type unitary which performs the map $\hat{U}_{\alpha_i}|\alpha_i\rangle|0\rangle = |\alpha_i\rangle|\beta_i\rangle$ where $\{|\beta_i\rangle\}$ is an orthonormal set of vectors. From this, we construct a unitary map of the form $\hat{U} = \hat{U}\alpha_N \ldots \hat{U}_{\alpha_1}$ which results in the state $\hat{U}|\psi\rangle|0\rangle = \sum_i c_i'|\alpha_i'\rangle|\beta_i'\rangle$. Notice that the final state is written with respect to the now orthogonal set $\{|\alpha_i'\rangle|\beta_i'\rangle\}$. The states $|\alpha_i\rangle$, are drawn from the set of coherent states $\{|\alpha\rangle\}$, so the coefficients c_i' characterizes the coherence amongst the coherent states present in $|\psi\rangle$. $\hat{U}|\psi\rangle|0\rangle$ may be called the orthogonalized state.

One may now apply any preferred coherence measure $\mathcal{C}$ to the orthogonalized state. The resulting quantity $\mathcal{C}(\hat{U}|\psi\rangle|0\rangle)$ is referred to as the α-coherence [4]. It is possible to show that the α-coherence is a linear optical monotone, and therefore a nonclassicality measure under the resource theory of nonclassicality.

In Figure 1, we use the relative entropy of coherence as our coherence measure $\mathcal{C}$[6], and compare the α-coherence for cat states, Fock states, and vacuum squeezed states. All these states are well known nonclassical optical states. We see that as the amount of squeezing increases for the squeezed state, the α-coherence increases. As the number of photons in the Fock state increases, so too does the α-coherence. For the cat states, we see that the α-coherence tends towards a steady value for increasing α. Similar features appear in some other nonclassicality indicators[7]. This supports the idea that α-coherence is a valid quantifier of nonclassicality in quantum optical systems.

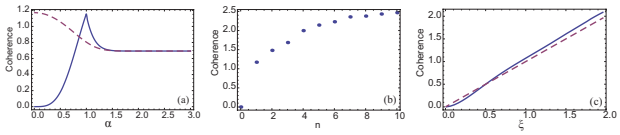


Figure 1: A comparison of α-coherence for some quantum optical states. (a) Even(solid line) and odd(dotted line) cat states $|\alpha\rangle \pm |-\alpha\rangle$, (b) Fock states $|n\rangle$, and (c) squeezed vacuum states $S(\xi)|0\rangle$ are compared.

4 Metrological power as a nonclassicality measure

While the α-coherence is a reasonable quantifier of nonclassicality and provides a bridge between coherence and nonclassical light, it lacks a strong operational interpretation in terms of a useful task. In this section we will introduce the metrological power, and describe how it may be used to construct nonclassicality monotones with stronger operational interpretations.

The task we will be considering will be parameter estimation. For such tasks, the ultimate sensitivity of a quantum state to small changes in the parameter is quantified by the Quantum Fisher Information (QFI). With respect to some Hermitian operator $\hat{L}$ which generates the unitary time evolution, the QFI is given by the following expression:

$$I_F(\hat{\rho}, \hat{L}) = 2\sum_{i,j}\frac{(\lambda_i - \lambda_j)^2}{\lambda_i + \lambda_j}|\langle i|\hat{L}|j\rangle|^2,$$

where the eigenvalues and eigenstates of $\hat{\rho}$ are given by λ_i and $|i\rangle$, respectively.

We will consider the parameter estimation of θ for the unitary dynamic generated by the collective quadrature observable $\hat{X}_{\boldsymbol{\mu}} = \sum_{n=1}^{N}\left(\mu_n^*\hat{a}_n + \mu_n\hat{a}_n^\dagger\right)/\sqrt{2}$. Under this unitary dynamic, an initial quantum state $\hat{\rho}_0$ evolves according to

$$\hat{\rho}_{\theta,\boldsymbol{\mu}} = e^{-i\theta\hat{X}_{\boldsymbol{\mu}}}\hat{\rho}_0 e^{i\theta\hat{X}_{\boldsymbol{\mu}}}.$$

In this case, the Fisher information can be simplified and expressed in matrix form:

$$I_F(\hat{\rho}, \hat{X}_{\boldsymbol{\mu}}) = \boldsymbol{\mu}^T\boldsymbol{F}\boldsymbol{\mu},$$

where $\hat{X}^{(2n-1)} = (\hat{a}_n + \hat{a}_n^\dagger)/\sqrt{2}$ and $\hat{X}^{(2n)} = (\hat{a}_n - \hat{a}_n^\dagger)/(\sqrt{2}i)$ are the local canonical quadrature operators for the nth mode. $\boldsymbol{F}$ is called the QFI matrix, which is a real symmetric $2N \times 2N$ matrix with elements

$$F_{kl} = 2\sum_{i,j}\frac{(\lambda_i - \lambda_j)^2}{\lambda_i + \lambda_j}\langle i|\hat{X}^{(k)}|j\rangle\langle j|\hat{X}^{(l)}|i\rangle.$$

If we were to estimate the parameter θ by performing measurements on the state $\hat{\rho}_{\theta,\boldsymbol{\mu}}$, a tight bound for the variance of the estimator $(\Delta\theta)^2_{\boldsymbol{\mu}}$ is given by

$$(\Delta\theta)^2_{\boldsymbol{\mu}} \geq \frac{1}{I_F(\hat{\rho}_0, \hat{X}_{\boldsymbol{\mu}})} = \frac{1}{\boldsymbol{\mu}^T\boldsymbol{F}\boldsymbol{\mu}}, \tag{1}$$

which is called the quantum Cramér Rao bound [8]. For the purpose of parameter estimation, the goal is to maximize the Fisher information $I_F(\hat{\rho}_0, \hat{X}_{\boldsymbol{\mu}})$, which essentially quantifies the sensitivity of the state to a displacement operation in the direction $\boldsymbol{\mu}$ in phase space.

We now introduce the concept of metrological power. Let us consider first some pure state $|\psi\rangle$. For every pure state, we can consider the average Fisher information over all possible quadrature directions:

$$\mathcal{P}_{\text{mean}}(|\psi\rangle) := \frac{1}{2}\int_{\mathcal{S}} \frac{d^{2N}\boldsymbol{\mu}}{\text{Vol}(\mathcal{S})} I_F(|\psi\rangle, \hat{X}_{\boldsymbol{\mu}}), \tag{2}$$

where $d^{2N}\boldsymbol{\mu} = d^2\mu_1 d^2\mu_2 \cdots d^2\mu_N$ and $\text{Vol}(\mathcal{S}) = \int_{\mathcal{S}} d^{2N}\boldsymbol{\mu} = 2\pi^N/(N-1)!$. For pure states, the Fisher information is especially simple. It is just 4 times the variance of the observable $\hat{X}_{\boldsymbol{\mu}}$, i.e. $I_F(|\psi\rangle, \hat{X}_{\boldsymbol{\mu}}) = 4(\Delta \hat{X}_{\boldsymbol{\mu}})^2$.

Due to the uncertainty principle, when the input state $|\psi\rangle$ is a coherent state, or a product of coherent states (i.e. a multimode coherent state), then we are assured that in any quadrature direction, $I_F(|\psi\rangle, \hat{X}_{\boldsymbol{\mu}})$ does not exceed 2, which in turn implies that after we taking the average $\mathcal{P}_{\text{mean}}(|\psi\rangle)$ will never exceed 1 if $|\psi\rangle$ is classical, as coherent states are the only classical pure states. This motivates us to consider

$$\mathcal{C}(|\psi\rangle) := \mathcal{P}_{\text{mean}}(|\psi\rangle) - 1 \tag{3}$$

as a non-classality measure over pure states. To extend it to mixed states, we take the common procedure of taking the convex roof of $\mathcal{C}$:

$$\mathcal{Q}(\hat{\rho}) := \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i \mathcal{C}(|\psi_i\rangle), \tag{4}$$

where $\{p_i, |\psi_i\rangle\}$ is a pure state decomposition of $\hat{\rho}$ satisfying $\hat{\rho} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ with $p_i \geq 0$ and $|\psi_i\rangle$. It can then be shown that $\mathcal{Q}(\hat{\rho})$ is also a linear optical monotone and thus also belongs to the resource theory of nonclassicality in Ref. [4]. The quantity $\mathcal{Q}$ is called the *mean metrological power*. More details can be found in Ref. [9].

However, even though the quantity $\mathcal{Q}$ qualifies as a nonclassicality measure, it is still non-ideal as it is difficult to compute for mixed states due to the convex roof construction, and also because parameter estimation is more concerned with the maximum Fisher information rather than the average. Ultimately, this limits the usefulness of the measure $\mathcal{Q}$.

In order to circumvent this, one may consider a slightly weaker nonclassicality measure.

Let us consider the optimal Fisher information over all possible quadrature directions $\boldsymbol{\mu}$ instead. This results in the closed form formula

$$\mathcal{P}_{\text{opt}}(\hat{\rho}) := \frac{1}{2}\max_{\boldsymbol{\mu}\in\mathcal{S}} I_F(\hat{\rho}, \hat{X}_{\boldsymbol{\mu}}) = \frac{\lambda_{\max}(\boldsymbol{F})}{2}, \tag{5}$$

where $\mathcal{S} = \{\boldsymbol{\mu} | \sum_{n=1}^N |\mu_n|^2 = 1\}$ and $\lambda_{\max}(\boldsymbol{F})$ is the maximum eigenvalue of $\boldsymbol{F}$. Note that in this case, the quantity has a simple closed form expression for a general mixed state as well as pure states, which is already a significant improvement in practicality compared to the mean metrological power $\mathcal{Q}$. For our nonclassicality measure, we define the quantity

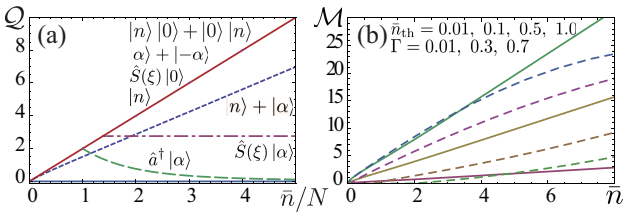


Figure 2: (a) Nonclassicality measure $\mathcal{Q}$ for a variety of nonclassical pure states. (b) Metrological power $\mathcal{M}$ for decohered cat states $\hat{\rho}_\Gamma$ (solid lines) and squeezed thermal states $\hat{S}(\xi)\hat{\tau}\hat{S}(\xi)$ (dashed lines).

$$\begin{aligned}\mathcal{M}(\hat{\rho}) &:= \mathcal{P}_{\text{opt}}(\hat{\rho}\otimes|0\rangle\langle 0|) - 1 \\ &= \max\{\mathcal{P}_{\text{opt}}(\hat{\rho}) - 1, 0\},\end{aligned} \tag{6}$$

where we have appended the vacuum state in the expression to ensure nonnegativity. It can then be verified that $\mathcal{M}$ satisfies the require monotonicity condition and is thus also a nonclassicality measure under the resource theory. We call $\mathcal{M}$ the *optimal metrological power*. On top of having a simple closed form expression for a general mixed state, it also has a direct operational interpretation as the maximum sensitivity of a state to a displacement operation. In fact, this operational significance can be greatly strengthened. It is known that when $\mathcal{M}(\hat{\rho}) > 0$, there always exists some linear optical optical unitary that allows it to beat a classical state in single parameter phase estimation tasks. The caveat is that while $\mathcal{Q}$ is able to detect all quantum states, and $\mathcal{M}$ can only detect most nonclassical states. This is discussed further in Ref. [9].

In Figure 2 we compare $\mathcal{Q}$ and $\mathcal{M}$ for various input states, including important states such as NOON states, Cat states and Squeezed states. In particular, as $\mathcal{M}$ is computable even for mixed states, we are able to compare the measures for the decohered cat states where $\hat{\rho}_\Gamma = N_\Gamma{}^{-1}[|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha| + \Gamma(|\alpha\rangle\langle-\alpha| + |-\alpha\rangle\langle\alpha|)]$, as well as the squeezed thermal states $\hat{S}(\xi)\hat{\tau}\hat{S}(\xi)$ where $\hat{\tau}$ is a thermal state and $\xi = 1$.

5 CONCLUSION

We introduced the resource theory of nonclassicality, which is based on linear optical maps and linear optical monotones. We then show how the amount the coherent superposition among the coherent states may be quantified and demonstrate that it is a nonclassicality measure under this resource theory. This provides a fundamental interpretation for the measure in terms of the superposition principle. We then construct another measure with a useful operational interpretation called the metrological power. The metrological power, which quantifies the sensitivity of a quantum state to displacement operations, may be used to construct nonclassicality measures with stronger operational interpretations. The ideas here are helpful for understanding the nature of nonclassicality in

light fields and why they are useful for many quantum processes.

References

[1] Horodecki, R., Horodecki, P., Horodecki, M. and Horodecki, K., "Quantum entanglement", Red. Mod. Phys. **81**, 865-942 (2009).

[2] Streltsov, A., Adesso, G., and Plenio, M. B., "Colloquium: Quantum coherence as a resource", Rev. Mod. Phys **89**, 041003 (2017).

[3] Titulaer, U. M. and Glauber, R. J., "Correlation functions for coherent fields," Phys. Rev. **140**, B676 (1965).

[4] Tan, K. C., Volkoff, T., Kwon, H. and Jeong, H., "Quantifying the Coherence between Coherent States," Phys. Rev. Lett. **119**, 190405 (2017).

[5] Aberg, J. "Quantifying superposition," arXiv:quant-ph/0612146 (2006).

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

[7] Sadeghi, P., Khademi, S. and Nasiri, S. , "Nonclassicality indicator for the real phase-space distribution functions," Phys. Rev. A **82**, 012102 (2010).

[8] Braunstein, S. L. and Caves, C. M., "Statistical distance and the geometry of quantum states," Phys. Rev. Lett. **72**, 3439 (1994).

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

One-Shot Detection Limits of Quantum Illumination with Discrete Signals

Man-Hong Yung[1 2 *] Fei Meng[1 3 †] Xiao-Ming Zhang[4] Ming-Jing Zhao[5 ‡]

[1] *Institute for Quantum Science and Engineering and Department of Physics, Southern University of Science and Technology, Shenzhen 518055, China*
[2] *Shenzhen Key Laboratory of Quantum Science and Engineering, Shenzhen, 518055, China*
[3] *Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong SAR, China*
[4] *Department of Physics, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong SAR, China*
[5] *School of Science, Beijing Information Science and Technology University, Beijing, 100192, China*

Abstract. To detect the presence of a stealth target, one may probe it with a single photon and analyze the reflected signals. The efficiency of such a conventional detection scheme can potentially be enhanced by the method of quantum illumination, where entanglement is exploited to break the classical limits. The question is, what is the optimal quantum state that allows us to achieve the detection limit with a minimal error? Here we address this question in a discrete model, and derived a complete and general set of analytic solutions for the whole parameter space. According to the minimal error for one-shot detection, the parameter space can be classified into three distinct regions, in the form of "phase diagrams" for both conventional and quantum illumination. Interestingly, whenever the reflectivity of the target is less than some critical values, all received signals become useless, which is true even if entangled resources are employed. However, there does exist a region where quantum illumination can provide advantages over conventional illumination; there, the optimal signal state is an entangled state with an entanglement spectrum inversely proportional to the spectrum of the environmental noise state and is, surprisingly, independent of the occurrence probability and the reflectivity of the object. These results not only impose physical limits in its application, but also analytically solved a class of channel discrimination problems.

Keywords: Quantum Illumination, Channel Discrimination, Analytic Solution.

Introduction— One of the most important tasks in quantum information science is to understand how physical procedures related to information processing can be improved by exploiting quantum resources such as entanglement. Apart from the well-established applications such as quantum computation, simulation, teleportation, metrology, etc., the area of quantum illumination [1, 2] is emerging as a promising and novel quantum method for increasing the sensitivity or resolution of target detection in a way that can go beyond the classical limits. The primary goal of quantum illumination is to detect the presence or absence of a target, with potentially a low reflectivity and in a highly-noisy background, by sending out an entangled signal and performing joint measurements. More specifically, the setup of quantum illumination consists of three parts: (i) a source emits a signal entangled with an idler system kept by an receiver; (ii) if a target exists, the receiver obtains the reflected part of the signal in addition to the background noise; otherwise, only the background noise can be received; (iii) the receiver perform a joint POVM measurement on the whole quantum system and infer from it the presence of the target.

An intriguing feature of quantum illumination is that it is highly robust against loss and decoherence; one can still gain quantum advantages, even if the signal is applied to entanglement-breaking channels [3]. As an important application, one can apply quantum illumination to secure quantum communication [4], where the sender encode a 0-or-1 message by controlling the presence or absence of an object and the receiver determine its presence by illuminating entangled photons; in this way, an eavesdropper who does not have access to another half of the entangled signal could virtually know nothing about the message communicated [4]. An experimental implementation [5] of the protocol above suggested that quantum illumination can provide a reduction up to five orders of magnitude in the bit-rate error against an eavesdropper attack.

Despite the progress achieved so far, quantum illumination lacks a foundational understanding on the ultimate limit of the quantum advantage. The existed literatures have not optimized the input signal for a better performance. Instead, the input signals are fixed and the problem is solved as an state discrimination problem. However, quantum illumination should be treated as a problem of channel discrimination [6]; the existence and absence of the object determines two different channels, whose inputs should be optimized such that their outputs can be discriminated better.

Quantum channel discrimination is generally a very hard computational problem where only a few analytic solutions have been discovered. In fact, quantum channel discrimination is generally a very hard computational problem [7]; it is complete for the quantum complexity class QIP (problems solvable by a quantum interactive proof system), which has been shown [8] to be equivalent to the complexity class PSPACE (problems solvable by classical computer with polynomial memory).

Here we show that, the problem of one-shot quantum illumination, for any given parameter regime and for signals with any finite dimension, can be solved *completely*

*yung@sustech.edu.cn
†mengf@mail.sustech.edu.cn
‡zhaomingjingde@126.com

with a compact analytic solution. More specifically, our main results include a derivation of an analytic expression for the minimized error probability for target detection in quantum illumination, where the minimization is over all possible POVM measurements and for all possible finite-dimensional (entangled) probe states. Furthermore, the optimal state we obtained depends only on the spectral information of the environment signal; in other words, the minimized error probability can always be achieved without even knowing the reflectivity and occurrence probability of the target.

On the other hand, researchers are trying to understand the resources that attribute to the advantages of quantum illumination, especially to explain its robustness. Quantum discord, a measure of non-classical correlation [9], was suggested [10, 11] to be the mechanism behind its robust advantage. However, these results are only applicable to quantum illumination with white noise. With our analytic solution for arbitrary noise spectrum, their results can be examined. Unfortunately, quantum discord cannot fully explain the performance gap between quantum and conventional illumination, when the noise is not completely mixed; one can show that there exist situations where the quantum discord of encoding defined in [10] is not equal to the quantum advantage. This imposes an interesting open problem of identifying the genuine mechanism behind the quantum advantage, and perhaps a new resource other than entanglement and discord can be found.

Model of one-shot quantum illumination— Our major contribution is the optimization of the input signal state and derivation of the ultimate performance of one-shot quantum illumination. As a first result stressing signal state optimization, we start with the one-shot scenario and restrict our analysis in single photon subspace for simplicity, similar as the framework Lloyd's used in the first paper of quantum illumination [1]. Recasting this optimization problem to channels for multiple photons such as those used in Tan *et al* [2], can lead to an essential performance improvement.

Within the single photon subspace, it is reasonable to assume that only finitely many modes can be resolved by the detector. Using the frequency basis for this single photon, we can assume that only d modes can be differentiated by the detector. Therefore, the states of a single photon can be described by a Hilbert space spanned by basis $\{|\theta_i\rangle\}_{i=1}^{d}$, where θ_i's are the frequencies that can be recognized by the detector. Different from the channel used by Lloyd [1], here the vacuum state is omitted. This is because the detector can wait until the first photon reaches in each run. Once one photon is detected, the detector refreshes itself for the next round detection, which makes sure that one and only one photon is detected each time.

For *conventional illumination*, a single photon probe state ρ is sent to detect the presence of a distant object. If the object is absent, only environmental noise can be detected. Existing literature simply approximate the thermal noise by white noise, where the noise intensity for any mode is the same. However, in general, the noise has nontrivial spectrum, with different intensity λ_i for different modes θ_i, which can be modeled by a density matrix $\rho_E = \sum_{i=1}^{d} \lambda_i |\theta_i\rangle\langle\theta_i|$. For convenience of analysis, we assume the noise spectrum $\lambda_1 \geqslant \lambda_2 ... \geqslant \lambda_d$ is decreasingly ordered. As shown later, this noise spectrum can be used to design optimal probing states and improve the detection performance. (i) if the target is absent, the probe signal ρ is completely lost; we can only receive the noisy state from the environment, which can be modeled by the following quantum channel,

$$\mathcal{E}_0(\rho) = \rho_E \ . \tag{1}$$

(ii) if the target is present, with probability η the probe photon is reflected, where η is its reflectivity. With probability $1-\eta$ the probe photon is absorbed, and only background noise can reach the detector. This process can be modeled by the following quantum channel:

$$\mathcal{E}_1(\rho) = \eta\rho + (1-\eta)\rho_E \ . \tag{2}$$

Then the detector measures the returned photon, telling us which state it is, and therefore the presence or absence of the object. To find the ultimate one-shot performance, one has to optimize the signal as well as the measurements, which makes it a channel discrimination problem [12].

For *quantum illumination*, besides the probe signal A, the agent also keeps an ancillary system B, which is entangled with the former. When the probe signal is sent, depending on the absence or presence of the target, it will undergo the evolution described by either $\mathcal{E}_0$ and $\mathcal{E}_1$, whereas the ancillary system B is kept unchanged.

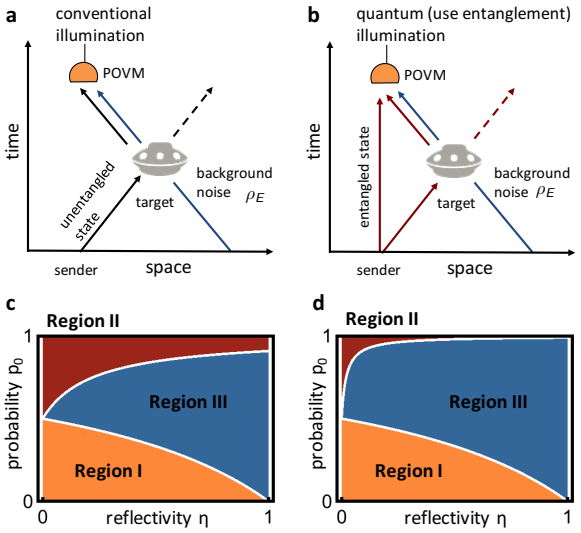


Figure 1: Conventional and quantum illumination. (a) In conventional illumination, a signal is sent to probe a target without the use of entanglement. (b) In quantum illumination, the signal is entangled, and a join POVM measurement is performed at the end to reduce the detection error. (c) The phase diagram for conventional illumination and (d) same diagram for quantum illumination.

Therefore, the composite system of the signal and ancilla is updated by the following quantum channel when the target is absent,

$$(\mathcal{E}_0 \otimes \mathcal{I})(\rho_{AB}) = \rho_E \otimes \rho_B \ , \tag{3}$$

where ρ_B is the reduced density state of the joint state ρ_{AB}, and when it is present,

$$(\mathcal{E}_1 \otimes \mathcal{I})(\rho_{AB}) = \eta\rho_{AB} + (1-\eta)\rho_E \otimes \rho_B \ . \tag{4}$$

Similar to conventional illumination, one has to optimize all possible signal-ancilla states and the joint measurements to find its ultimate performance.

Conclusions— In this work, we presented complete solutions to the problem of one-shot minimum-error discrimination for both conventional and quantum illuminations. We solved the optimization problem, and find out that the optimal probing state for the conventional illumination is $|\theta_d\rangle$, which is the photon precisely in the mode with minimal noise intensity λ_i. For quantum illumination, the optimal signal-ancilla state is an entangled state whose entanglement spectrum is inversely propositional to the noise intensity. Interestingly, the optimal probing states for both quantum and conventional illumination are independent of the reflectivity and the a prior probability of the target, but only depend on the properties of the noise.

The performance in terms of minimal error when probing with optimal signal, is divided into three regions, as shown in Fig.1. Region I are the same for both conventional and quantum illumination; the minimal error is a constant and does not depend on the reflectivity of the target, with the optimal strategy being simple guess. Region II is similar and the reflected signal is useless, but quantum illumination shrinks the boundary of region II. For region III, quantum illumination can yield a lower minimal error than conventional illumination.

Our results improves the performance of quantum illumination. Recasting our idea of signal state optimization to multiple photon domain [2] with arbitrary noise model could yield an essential performance improvement. Our result also provides a more general testbed for identifying the underlying mechanisms that lead to the robustness of quantum advantages.

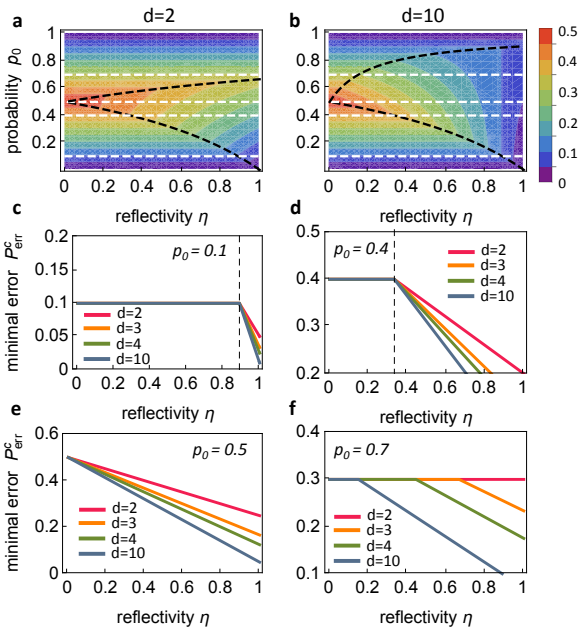


Figure 2: Behavior of conventional illumination in a completely-mixed environment $\rho_E = I/d$. (a) Color plot of the minimal-error $P^c_{\rm err}$ as a function of the occurence probability p_0 and reflectivity η for two-dimensional signals $d = 2$. (b) the same plot for $d = 10$. Explicit dependence of $P^c_{\rm err}$ as a function of η are shown in (c)-(f).

References

[1] S. Lloyd. Enhanced sensitivity of photodetection via quantum illumination. *Science*, 321(5895):1463–1465, 2008.

[2] S.-H. Tan, *et al.* Quantum Illumination with Gaussian States. *Phys. Rev. Lett.*, 101(25):253601, 2008.

[3] M. B. Ruskai. Qubit Entanglement Breaking Channels. *Rev. Math. Phys.*, 15(06):643–662, 2003.

[4] J. H. Shapiro. Defeating passive eavesdropping with quantum illumination. *Phys. Rev. A*, 80(2):22320, 2009.

[5] Z. Zhang, *et al.* Entanglement's Benefit Survives an Entanglement-Breaking Channel. *Phys. Rev. Lett.*, 111(1):10501, 2013.

[6] A. W. Harrow, *et al.* Adaptive versus nonadaptive strategies for quantum channel discrimination. *Phys. Rev. A*, 81(3), 2010.

[7] B. Rosgen and J. Watrous. On the Hardness of Distinguishing Mixed-State Quantum Computations. In *20th Annu. IEEE Conf. Comput. Complex.*, pages 344–354. IEEE, 2005.

[8] R. Jain, *et al.* QIP = PSPACE. *Commun. ACM*, 53(12):102, 2010.

[9] K. Modi, *et al.* The classical-quantum boundary for correlations: discord and related measures. *Rev. Mod. Phys.*, 84(4):1655, 2012.

[10] C. Weedbrook, *et al.* How discord underlies the noise resilience of quantum illumination. *New J. Phys.*, 18(4):43027, 2016.

[11] M. Bradshaw, *et al.* Overarching framework between Gaussian quantum discord and Gaussian quantum illumination. *Phys. Rev. A*, 95(2):022333, 2017.

[12] C. W. Helstrom. Quantum detection and estimation theory. *J. Stat. Phys.*, 1(2):231–252, 1969.

Parity-time-symmetric quantum walks

Peng Xue

Abstract. The study of non-Hermitian systems with parity-time (PT) symmetry is a rapidly developing frontier in recent years. Experimentally, PT-symmetric systems have been realized in classical optics by balancing gain and loss, which holds great promise for novel optical devices and networks. Here we report the first experimental realization of passive PT-symmetric quantum dynamics for single photons by temporally alternating photon losses in the quantum walk (QW) interferometers. The ability to impose PT symmetry allows us to realize and investigate Floquet topological phases driven by PT-symmetric QWs. We observe topological edge states between regions with different bulk topological properties and confirm the robustness of these edge states with respect to PT-symmetry-preserving perturbations and PT-symmetry-breaking static disorder. Our results pave the way for realizing quantum mechanical PT-synthetic devices and augur exciting possibilities for exploring topological properties of non-Hermitian systems using discrete-time QWs.

The Future of Computing in Silicon

Michelle Simmons

Abstract. Down-scaling has been the leading paradigm of the semiconductor industry since the invention of the first transistor in 1947. However miniaturization will soon reach the ultimate limit, set by the discreteness of matter, leading to intensified research in alternative approaches for creating logic devices. This talk will discuss the development of a radical new technology for creating atomic-scale devices which is opening a new frontier of research in electronics globally. We will introduce single atom transistors where we can measure both the charge and spin of individual dopants with unique capabilities in controlling the quantum world. To this end, we will discuss how we are now demonstrating atom by atom the best way to build a quantum computer a new type of computer that exploits the laws of physics at very small dimensions in order to provide an exponential speed up in computational processing power.

All sets of incompatible measurements give an advantage in quantum state discrimination

Paul Skrzypczyk[1] * Ivan Šupić[2] † Daniel Cavalcanti[3] ‡

[1]*H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol, BS8 1TL, United Kingdom*
[2]*Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland*
[3]*ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain*

Abstract. Some quantum measurements can not be performed simultaneously, *i.e.* they are incompatible. Here we show that every set of incompatible measurements provides an advantage over compatible ones in a suitably chosen quantum state discrimination task. This is proven by showing that the Robustness of Incompatibility, a quantifier of how much noise a set of measurements tolerates before becoming compatible, has an operational interpretation as the advantage in an optimally chosen discrimination task. We also show that if we take a resource-theory perspective of measurement incompatibility, then the guessing probability in discrimination tasks of this type forms a complete set of monotones that completely characterize the partial order in the resource theory. Finally, we make use of previously known relations between measurement incompatibility and Einstein-Podolsky-Rosen steering to also relate the later with quantum state discrimination.

In quantum mechanics, observables described by non-commuting operators satisfy an uncertainty relation, which implies that we can not acquire precise information about them simultaneously [1]. Commutation is well defined for sharp (von Neumann) measurements. However, a more refined notion of measurement incompatibility is needed for general measurements described by positive-operator-value-measures (POVMs) [2]. This is captured by the idea of joint measurability [17]. Suppose a set of measurements $\{\mathbb{M}_x\}_x$ labeled by $x = 1, \ldots, m$, each described by measurement operators $M_{a|x}$ ($M_{a|x} \geq 0$, $\sum_a M_{a|x} = \mathbb{1}\ \forall\ a, x$), where $a = 1, \ldots, o$ labels each of the measurement outcomes. This set is said to be jointly measurable (or compatible) if there exists a 'parent' measurement $\mathbb{G}$ with measurement operators G_λ, and conditional probability distributions $p(a|x,\lambda)$, such that

$$M_{a|x} = \sum_\lambda p(a|x,\lambda) G_\lambda \quad \forall\ a, x. \tag{1}$$

Otherwise the set is said to be incompatible. This definition can be interpreted as follows: if (1) holds, all measurements $\mathbb{M}_x$ can be performed jointly, by the implementation of the single measurement $\mathbb{G}$ and a probabilistic classical post-processing defined by the weights $p(a|x,\lambda)$.

Here we give an operational interpretation of measurement incompatibility in terms of quantum state discrimination: we show that a set of measurements is incompatible if and only if they provide an advantage over compatible ones in a quantum state discrimination (QSD) task with multiple ensembles of states. Moreover, we also show that the advantage of an optimally chosen QSD task is quantified exactly by the robustness of incompatibility of the set, a previously proposed quantifier of measurement incompatibility [10]. This result fits within a number of results recently obtained which have linked robustness-based quantifiers with advantages in suitably chosen discrimination games [19, 18, 21, 20, 16]

*paul.skrzypczyk@bristol.ac.uk
†ivan.supic@unige.ch
‡daniel.cavalcanti@icfo.eu

We consider the following two-party QSD task [8]: Bob can prepare different ensembles $\{\mathcal{E}_y\}_y$ ($y = 1, \ldots, n$) of quantum states $\mathcal{E}_y = \{\rho_{b|y}, q(b|y)\}_b$, for $b = 1, \ldots, p$. At each round of the protocol, Bob chooses one of the ensembles y with probability $q(y)$ and sends Alice his choice y, and the state prepared $\rho_{b|y}$, which occurs with probability $q(b|y)$. Upon receiving y and $\rho_{b|y}$, Alice's goal is to identify which state she was sent, *i.e.* to correctly identify b.

We will consider playing this game in two different scenarios. In the first scenario, Alice has access to a fixed set of incompatible measurements $\{\mathbb{M}_x\}_x$ in order to play. We consider the most general probabilistic strategies assuming that the only way Alice can interact with the system is through her fixed measuring device. In particular, we allow any strategy consisting of the following [1]: After receiving the state and the value of y, Alice makes use of a random variable μ to perform the measurement $\mathbb{M}_x$, with probability $p(x|y,\mu)$. After receiving outcome a she makes a guess of the value of b, according to $p(g|a,y,\mu)$. Optimizing over all strategies, we can quantify how well Alice does in this game by evaluating the average probability of correctly identifying b, i.e.

$$\begin{aligned} &P_g(\{\mathcal{E}_y\},\{\mathbb{M}_x\}) = \\ &= \max_{\mathcal{S}} \sum_{byaxg\mu} q(b,y)p(\mu)p(x|y,\mu)\,\mathrm{tr}[\rho_{b|y}M_{a|x}]p(g|a,y,\mu)\delta_{g,b} \end{aligned} \tag{2}$$

where the maximization is over strategies $\mathcal{S} = \{p(\mu), p(x|y,\mu), p(g|a,y,\mu)\}$, and we have written $q(b,y) = q(y)q(b|y)$.

We will contrast this to a scenario where in any given run of the game Alice can only perform a single measurement (al-

[1]Note that a more general class of strategies would allow for a pre-processing of the state also, i.e. the application of an arbitrary quantum instrument (collection of completely positive maps that sum to a trace-preserving channel). Here we do not give Alice such capabilities, but demand that the only Alice interact directly with the quantum system sent to her is through the measuring device corresponding to the incompatible measurements

though we will allow once again the possibility of using randomness to mix over different fixed measurements in different runs of the game). In particular, we consider measurements $\mathbb{G}_\nu = \{G_{a|\nu}\}_a$, and allow for the most general strategy using any such measurements. Crucially now, since Alice can only perform a single measurement, the side-information of y can only be used to implement a classical post-processing of this measurement. The net effect is equivalent to Alice only being able to perform a set of compatible measurements, those achieved by the 'parent' measurements $\mathbb{G}_\nu$. In this case the success probability is given by

$$P_g^{\mathrm{C}}(\{\mathcal{E}_y\}) = \max_{\mathcal{T}} \sum_{byav g} q(b,y)p(\nu)\,\mathrm{tr}[\rho_{b|y}G_{a|\nu}]p(g|a,y,\nu)\delta_{g,b} \tag{3}$$

where the maximization is over all strategies $\mathcal{T} = \{p(\nu), \mathbb{G}_\nu, p(g|a,y,\nu)\}$.

We are primarily interested in the *advantage* that is offered by a set of incompatible measurements $\{\mathbb{M}_x\}_x$ in any such QSD game. In particular, we are interested in the biggest relative increase in guessing probability that can be obtained by the set of measurements $\{\mathbb{M}_x\}_x$ compared to having access to only single measurements, among all possible ensembles, i.e.

$$\max_{\{\mathcal{E}_y\}} \frac{P_g(\{\mathcal{E}_y\},\{\mathbb{M}_x\})}{P_g^{\mathrm{C}}(\{\mathcal{E}_y\})} \tag{4}$$

As our main result we show that this quantity is completely characterised by the Robustness of Incompatibility (RoI) of the measurements $I_R(\{\mathbb{M}_x\})$ as

$$1 + I_R(\{\mathbb{M}_x\}) = \max_{\{\mathcal{E}_y\}} \frac{P_g(\{\mathcal{E}_y\},\{\mathbb{M}_x\})}{P_g^{\mathrm{C}}(\{\mathcal{E}_y\})}. \tag{5}$$

The Robustness of Incompability $I_R(\{\mathbb{M}_x\})$ is defined as the minimal amount of 'noise' that needs to be added to the set of measurements $\{\mathbb{M}_x\}_x$ before they become compatible [10]. Here, by 'noise', we mean that we mix the set of measurements with another, arbitrary, set of measurements $\{\mathbb{N}_x\}_x$, (of the same size, and with the same number of outcomes), in order to make the mixture compatible. Formally,

$$\begin{aligned} I_R(\{\mathbb{M}_x\}) = \min \quad & r \\ \text{s.t.} \quad & \frac{M_{a|x} + rN_{a|x}}{1+r} = \sum_\lambda p(a|x,\lambda)G_\lambda \\ & N_{a|x} \geq 0, \quad \sum_a N_{a|x} = \mathbb{1}, \\ & p(a|x,\lambda) \geq 0, \quad \sum_a p(a|x,\lambda) = 1, \\ & G_\lambda \geq 0, \quad \sum_\lambda G_\lambda = \mathbb{1} \end{aligned} \tag{6}$$

where the minimisation is over r, $\{\mathbb{N}_x\}_x$ (where $\mathbb{N}_x = \{N_{a|x}\}_a$), $\mathbb{G} = \{G_\lambda\}_\lambda$ and $\{p(a|x,\lambda)\}_{a,x,\lambda}$, and all constraints are understood to hold for all values of a, x, or λ, as appropriate.

The RoI has a number of desirable properties. It is (i) faithful ($I_R(\{\mathbb{M}_x\}) = 0$ if and only if the set of measurements $\{M_x\}_x$ is incompatible); (ii) convex and (iii) non-increasing under post-processing of the measurements. Due to (5), the properties (i) – (iii) are also satisfied by the advantage (4). In particular, due to (i), a set of measurements $\{\mathbb{M}_x\}_x$ provides an advantage over compatible measurements if and only if $I_R(\{\mathbb{M}_x\}) > 0$.

Another interesting consequence of (5) is that it gives an efficient way of computing the advantage (4). This is because the RoI can be shown to be expressed explicitly as the following semi-definite program (SDP):

$$\begin{aligned} 1 + I_R(\{\mathbb{M}_x\}) = \min_{s,\{\tilde{G}_{\mathbf{a}}\}} \quad & s \\ \text{s.t.} \quad & \sum_{\mathbf{a}} D_{\mathbf{a}}(a|x)\tilde{G}_{\mathbf{a}} \geq M_{a|x} \quad \sum_{\mathbf{a}} \tilde{G}_{\mathbf{a}} = s\mathbb{1}, \quad \tilde{G}_{\mathbf{a}} \geq 0 \end{aligned}$$

where $\mathbf{a} = \mathrm{a}_1\mathrm{a}_2\cdots\mathrm{a}_n$ is a string, which can be throught of as a list of 'results', one for each measurement, $D_{\mathbf{a}}(a|x) = \delta_{a,\mathrm{a}_x}$ are deterministic probability distributions, whereby $a = \mathrm{a}_x$ with certainty, and $\tilde{\mathbb{G}} = \{\tilde{G}_{\mathbf{a}}\}_{\mathbf{a}}$ is a super-normalised parent POVM. The derivation of this SDP formulation can be found in the appendix.

To summarise, the above shows that the RoI, which was introduced as a purely geometrical quantifier of incompatibility, in fact has an operational interpretation as the advantage that a set of measurements provides in an optimally chosen QSD game. Moreover, since the RoI is faithful, every set of incompatible measurements gives an advantage in at least one QSD task, and thus this task captures the utility of incompatible measurements. Finally, considering a resource theory of measurement incompatibility, one can show that the very same game is intimately related to the simulability of one set of measurements by another, providing (an infinite number of) criteria – often referred to as monotons – that collectively constitute necessary and sufficient conditions that must be met for one set of measurements to simulate another. This is similar to a number of other resource theories, where guessing probabilities in all discrimination games of a given type have also been shown to constitute complete criteria for transformations amount objects in the theory [15, 14, 16].

References

[1] H. P. Robertson, The Uncertainty Principle, Phys. Rev., 34, 1, 163–164. 1929

[2] , Kraus, K. and Bohm, A. and Dollard, J.D. and Wootters, W.H. States, effects, and operations: fundamental notions of quantum theory : lectures in mathematical physics at the University of Texas at Austin Lecture notes in physics, Springer - erlag, 1983

[3] Joint Measurability of Generalized Measurements Implies Classicality R. Uola, T. Moroder, O. Gühne, Phys. Rev. Lett. 113, 160403, 2014

[4] Joint Measurability, Einstein-Podolsky-Rosen Steering, and Bell Nonlocality M. T. Quintino, T. Vértesi, N. Brunner Phys. Rev. Lett. 113, 160403, 2014

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

[6] Quantitative relations between measurement incompatibility, quantum steering, and nonlocality D. Cavalcanti and P. Skrzypczyk, Phys. Rev. A, 93, 052112, 2016

[7] Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox H. M. Wiseman, S. J. Jones, A. C. Doherty, Phys. Rev. Lett. 98, 140402, 2007

[8] State discrimination with postmeasurement information and incompatibility of quantum measurements, C. Carmeli, T. Heinosaari, A. Toigo, Phys. Rev. A, 98, 012126, 2018

[9] Convex Optimization, S. Boyd and L. Vandenberghe, Cambridge University Press, 2004

[10] One-to-One Mapping between Steering and Joint Measurability Problems, R. Uola, C. Budroni, =. Gühne, J.-P. Pellonpää, Phys. Rev. Lett., 115, 230402, 2015

[11] Quantum Resource Theories, E. Chitambar and G. Gour, Rev. Mod. Phys. 91, 025001, 2019

[12] Negativity and steering: A stronger Peres conjecture, M. Pusey, Phys. Rev. A, 88, 032313, 2013

[13] Remote State Preparation, C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, W. K. Wootters, Phys. Rev. Lett., 87, 077902, 2001

[14] Quantum Majorization and a Complete Set of Entropic Conditions for Quantum Thermodynamics, G. Gour, D. Jennings, F. Buscemi, R. Duan, I. Marvian, Nature Comm., 9, 5352, 2018

[15] Degradable Channels, Less Noisy Channels, and Quantum Statistical Morphisms: An Equivalence Relation, F. Buscemi, Probl. Inf. Transm., 52, 201-203, 2016

[16] Robustness of Measurement, discrimination games and accessible information P. Skrzypczyk and N. Linden, Phys. Rev. Lett., 122, 140403, 2019

[17] An invitation to quantum incompatibility T. Heinosaari, T. Miyadera, M. Ziman, J. Phys. A: Math. Theor., 49, 123001, 2016

[18] Robustness of Coherence: An Operational and Observable Measure of Quantum Coherence, C. Napoli, T. R. Bromley, M. Ciancianruso, M. Piani, N. Johnson, G. Adesso, Phys. Rev. Lett., 116, 150502, 2016

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

[20] More Entanglement Implies Higher Performance in Tailored Channel Discrimination Tasks J. Bae, D. Chruściński, M. Piani, arXiv:1809.02082, 2018

[21] Operational Advantage of Quantum Resources in Subchannel Discrimination, R. Takagi, B. Regula, K. Bu, Z.-W, Liu, G. Adesso, arXiv:1809.01672, 2018

[22] One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering, C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, H. M. Wiseman, Phys. Rev. A, 85, 010301, 2012

Every entangled state provides an advantage in classical communication

Stefan Bäuml[1] * Andreas Winter[2 3] † Dong Yang[4 5] ‡

[1] *QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, Netherlands.*
[2] *Departament de Física, Grup d'Informació Quàntica, Universitat Autònoma de Barcelona,ES-08193 Bellaterra, Spain.*
[3] *ICREA - Institució Catalana de Recerca i Estudis Avançats, ES-08010 Barcelona, Spain.*
[4] *Department of Informatics, University of Bergen, 5020 Bergen, Norway.*
[5] *Laboratory for Quantum Information, China Jiliang University, Hangzhou, Zhejiang 310018, China.*

Abstract. We investigate whether for any entangled state there exists a quantum channel the classical capacity of which can be increased by providing the state as an additional resource. We show, for any entangled state, the existence of a quantum memory channel whose feedback-assisted classical capacity can be increased by using the state as a resource. Using a different channel construction, we also provide a sufficient entropic condition for an advantage in classical communication and thus provide an example of a state that is not distillable by means of one-way LOCC, but can provide an advantage in the classical communication.

Keywords: Classical Communication over Quantum Channel, Entanglement Assistance, Bound Entanglement

This submission is based on [1]. Since the early days of quantum information theory it is known that maximally entangled states can increase the rate of classical communication via a noiseless quantum channel using a fundamental protocol known as *superdense coding* [2]. One direction of research is to go beyond noiseless channels and study the classical communication capacity of general quantum channels, while still requiring pure entanglement assistance. In this setting, a capacity theorem has been derived [3]. Another direction is to consider noiseless channels assisted by noisy entanglement. It has been shown [4] that the advantage which a mixed state ρ_{AB} can provide is determined by the maximal *coherent information* available from ρ_{AB} by local operations on Alice's side. As the coherent information plays an important role in determining the advantage which entanglement can provide in dense coding, we believe it will be instructive to review another operational meaning of this quantity. It has been shown [5] that the coherent information $I(A\rangle B)_\rho$ provides a lower bound on the asymptotic rate at which ρ_{AB} can be distilled to maximal entanglement. Hence any state that is not one-way distillable will not be of any use in classical communication via a noiseless channel [4]. An example of a one-way undistillable state is the two-qubit Werner state $\frac{q}{3}P_{\text{sym}} + (1-q)P_{\text{anti}}$, with $q \geq 1/4$. Going further, there exists a huge class of states which cannot be distilled, even if two-way communication is available. Such states are known as *bound entangled* [6, 7]. The resource character of bound entangled states for various information theoretic tasks is still an active field of research.

In the present paper we combine the two research directions mentioned above. We investigate the scenario in which both the quantum channel and the assisting entanglement are noisy [8]. Apart from being the most realistic scenario experimentally, this doubly noisy scenario also poses an interesting open question concerning the resource character of states that are not one-way distillable, in particular bound entangled states. Namely, we are interested if, for any entangled state, there exists some quantum channel such that the state can provide an advantage in classical communication via the quantum channel. For states with positive coherent information this question has already been answered above; such states can yield an advantage in classical communication via the noiseless channel. However, for entangled states with vanishing or negative coherent information, in particular states which are only two-way distillable and bound entangled states, it is not known whether such channels exist. So, what we are looking for is a kind of activation effect, where the noise in the quantum channel is of such kind that classical communication can be improved by a given state which is noisy in a way that makes it useless for the noiseless channel, and probably most other channels. Let us also note that shared randomness as well separable states, which can be simulated by shared randomness cannot provide an advantage in classical communication [9].

In a first approach, we consider channels with finite memory, and communication schemes that allow for feedback after each channel use. We show that for each entangled state ρ, there exists a memory channel T^d such that its ρ-assisted feedback capacity, restricted to product encodings, is strictly larger than the unassisted feedback product capacity. Here we also assume that Alice does not store the feedback for future channel uses. The memory channel is of the form $T^d : A \otimes I \to I \otimes B$, with

$$T^d(\sigma_A \otimes |i\rangle\langle i|_I) = \begin{cases} |i\rangle\langle i|_I \otimes m_i(\sigma)_B & \text{even rounds} \\ \frac{1}{2}\mathrm{id}_I \otimes n_i^d(\sigma)_B & \text{odd rounds.} \end{cases} \quad (1)$$

The bit value i of I is initially in random value, which neither Alice nor Bob now. During each channel use, i

*s.m.g.bauml@tudelft.nl
†andreas.winter@uab.cat
‡dyang@cjlu.edu.cn

determines which of a pair of two channels $m_{0,1}$ (in odd rounds) or $n^d_{0,1}$ (in even rounds) is used. Thus the two channels become correlated. After each even round, I is randomized again. As channels $n^d_{0,1}$, which are used in even rounds, we choose qc-channels that are defined by

$$n^d_i(\sigma) = \sum_{k=1}^{d} |k\rangle\langle v^{(i)}_k|\sigma|v^{(i)}_k\rangle\langle k|, \tag{2}$$

where $d \in \mathbb{N}$ and $\mathcal{B}_i = \{|v^{(i)}_k\rangle\}$ are mutually unbiased bases (MUBs). If a message is encoded in basis $\mathcal{B}_i$, channel n^d_i can achieve a rate of $\log d$. If, on the other hand, the encoding is in basis $\mathcal{B}_{i\oplus 1}$, the message will be completely depolarized by n^d_i. If presented with a random mixture of $n^d_{0,1}$, Alice will a priori not know which of the MUBs to encode her message in. If feedback is allowed, however, the structure of (1) allows Alice and Bob to perform the following protocol: In every odd round, Alice sends some state that helps Bob to distinguish between channels $m_{0,1}$. The result (j) is then sent back to Alice, who, in the following even round, applies a unitary operation modifying the encoding. Intuitively, the achievable rate of communication of this protocol greatly depends the ability to distinguish channels m_0 and m_1, which is where the entanglement assistance comes in. Our main idea is to make use of the fact that any entangled state can provide an advantage in channel discrimination [10]. By choosing d large enough compared to the output dimension of the m_i, we can achieve a locking effect, where even the smallest advantage a weakly entangled state can provide in channel discrimination can be amplified.

The second approach we present in this paper is set in the usual framework of many independent channel uses and without feedback. Our main result in this section is an entropic condition on a given state ρ_{AB} and a given channel $M : A \to C$, which is sufficient for the existence of another channel $N : AD \to C$, the Holevo capacity of which can be increased by using ρ_{AB}. Namely, we require $S(C|B)_\omega < S_{\min}(M)$ $(*)$, where $\omega_{CB} = M \otimes \mathrm{id}\,(\rho_{AB})$ and $S_{\min}$ denotes the minimum output entropy. The channel N is constructed from M in a way which was introduced in [11] in order to show equivalence of additivity between the minimum output entropy and the Holevo capacity. If M is entanglement-breaking, so will be N, hence the Holevo quantity will equal the capacity. Using $(*)$ and the transpose depolarising channel [12] as M, we can show that the two-qubit Werner state can provide an advantage in the capacity for $q \leq 0.345$, i.e. for values where it is not one-way distillable, hence useless for dense coding [4]. As only entangled states can provide an advantage in the Holevo capacity, the condition $(*)$ with a suitable choice of M can also serve as an entropic entanglement witness for the state ρ_{AB}.

References

[1] Stefan Bäuml, Andreas Winter, and Dong Yang. Every entangled state provides an advantage in classical communication. *arXiv preprint arXiv:1810.11431*, 2018.

[2] Charles H Bennett and Stephen J Wiesner. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.

[3] Charles H Bennett, Peter W Shor, John A Smolin, and Ashish V Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. *Physical Review Letters*, 83(15):3081–3084, 1999.

[4] Michał Horodecki and Marco Piani. On quantum advantage in dense coding. *Journal of Physics A: Mathematical and Theoretical*, 45(10):105306, 2012.

[5] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society London A*, 461:207–235, 2005.

[6] Paweł Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physics Letters A*, 232(5):333–339, 1997.

[7] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed state entanglement and distillation: Is there a 'bound' entanglement in nature? *Physical Review Letters*, 80:5239–5242, 1998.

[8] Quntao Zhuang, Elton Yechao Zhu, and Peter W Shor. Additive classical capacity of quantum channels assisted by noisy entanglement. *Physical Review Letters*, 118(20):200503, 2017.

[9] Robert Prevedel, Yang Lu, William Matthews, Rainer Kaltenbaek, and Kevin J Resch. Entanglement-enhanced classical communication over a noisy classical channel. *Physical Review Letters*, 106(11):110505, 2011.

[10] Marco Piani and John Watrous. All entangled states are useful for channel discrimination. *Physical Review Letters*, 102(25):250501, 2009.

[11] Peter W Shor. Additivity of the classical capacity of entanglement-breaking quantum channels. *Journal of Mathematical Physics*, 43(9):4334–4340, 2002.

[12] Mark Fannes, Bart Haegeman, Milan Mosonyi, and Dimitri Vanpeteghem. Additivity of minimal entropy output for a class of covariant channels. *arXiv preprint quant-ph/0410195*, 2004.

The Heisenberg limit for laser coherence

S. N. Saadatmand[1] * T. J. Baker[1] † D. W. Berry[2] ‡ H. M. Wiseman[1] §

[1] *Centre for Quantum Dynamics, Griffith University, Nathan, Brisbane, QLD 4111, Australia*
[2] *Department of Physics and Astronomy, Macquarie University, Sydney, NSW 2109, Australia*

Abstract. To quantify quantum optical coherence requires both the particle- and wave-natures of light. For an ideal laser, it can be thought of as the number of photons emitted into the beam with the same phase. This number, $\mathfrak{C}$, for an ideal laser was thought to be on the order of the square of the photon number in the laser itself, $O(\mu^2)$. Here, assuming nothing about the laser operation, only some assumptions on the ideality of the laser, we find the ultimate (Heisenberg) limit: $\mathfrak{C} = O(\mu^4)$. Moreover, as a first, we employ a state-of-the-art quantum-information-theory tool, the matrix product states, to find a laser model that achieves this scaling.

Keywords: Laser Coherence, Quantum Optics, Matrix Product States

1 Introduction

Quantum theory underpins much modern technological development, and sets the ultimate limits to the performance of devices — the best conceivable performance towards which scientists and engineers can work under the constraint of a given resource (such as energy or power). In this context, a *quantum enhancement* exists when the ultimate limit, also known as a *Heisenberg limit*, scales better in terms of the resource than the *standard quantum limit* (SQL) [1]. The latter is also derived employing quantum theory, but using a set of 'standard' assumptions on how the device must work. The quadratic quantum enhancement found in static phase estimation [2, 3] is well known, and there are many other metrological examples [1, 4]. Here, by contrast, we prove that there can be a quadratic quantum enhancement in the *production* of a physical property of great importance for both classical and quantum technology: optical coherence.

A laser beam epitomises optical coherence in all its aspects, including a long coherence time. This time can be converted to a dimensionless measure of coherence, $\mathfrak{C}$, by multiplying by $\mathcal{N}$, the number of photons emitted per unit time. This gives, loosely speaking, the number of photons emitted consecutively that are mutually coherent. The quantum limit to the coherence time was famously studied by Schawlow and Townes over 60 years ago [5]. However, even more rigorous subsequent work [6] made assumptions not entailed by fundamental requirements such as local conservation of energy. In the 21st century, our ability to engineer and control quantum systems [7, 8] has changed our conception of what is practical. At the same time, our understanding of quantum processes has been deepened through theoretical and numerical quantum-information-theory techniques such as operational super-selection rules (SSRs) [9, 10], and matrix product states (MPSs) [11, 12, 13]. Hence it is plausible that the Schawlow–Townes limit, $\mathfrak{C}_{\rm SQL}^{\rm ideal} = O(\mu^2)$, to laser coherence is only a SQL, and that a Heisenberg limit can be proven to lie beyond it.

The central result of this paper is that the true ultimate limit, the Heisenberg limit, for a laser beam having properties akin to those of the ideal models, is $\mathfrak{C}_{\rm HL}^{\rm ideal} = \Theta(\mu^4)$. This quadratic improvement implies vastly better performance in the limit $\mu \gg 1$ which characterises most lasers. We prove the existence of a quadratic quantum enhancement in laser coherence creation by the following steps. First, we state our conditions on the laser and its beam. Second, we show analytically from these the upper bound of $\mathfrak{C} = O(\mu^4)$. Third, guided by our tensor-network description of such an ideal laser, we introduce a μ-parametrized family of laser models and show numerically that $\mathfrak{C} = \Theta(\mu^4)$. Fourth, we relay on some theoretical and numerical results to show that all conditions are satisfied in our tensor-network model. We conclude with a discussion of open questions.

2 Conditions defining an ideal laser

We formally consider the following conditions as defining an ideal laser assumptions, which are *sufficient* for deriving the Heisenberg limit to the coherence.

1. **One-dimensional beam.** The beam propagates away from the laser in a particular direction, at a constant speed, and has a single transverse mode and a single polarisation. Mathematically, at any time $T \in \mathbb{R}$, the beam is describable by a one-parameter quantum field $\hat{b}(t)$, satisfying $[\hat{b}(t), \hat{b}^\dagger(s)] = \delta(t-s)$, defined for $t \in (-\infty, T]$, such that $\hat{b}(t)$ is independent of T. The argument of $\hat{b}(t)$ is the time at which that infinitesimal part of the beam was created by the laser, and $\hat{b}^\dagger(t)\hat{b}(t)$ is the operator for photon flux (photons per unit time).

2. **Autochthonous phase.** The coherence of the beam proceeds only from the laser. That is, a phase shift imposed on the laser state at some time T will lead, in the future, to the same phase shift on the beam emitted after time T as well as on the laser state. The phase shift at time T on the laser (which may have been prepared by measurement on the beam generated prior to T) is described by the unitary transformation $\hat{U}_\zeta = \exp(-i\zeta\hat{n}_{\rm c})$.

*n.saadatmand@griffith.edu.au
†travis.baker@griffithuni.edu.au
‡dominic.berry@mq.edu.au
§h.wiseman@griffith.edu.au

The effect of this, at any time $T' > T$, on the state of the cavity plus the beam segment generated in the interval $(T, T']$, is described by the unitary transformation $\hat{U}'_\zeta = \exp(-i\zeta(\hat{n}_\mathrm{c} + \hat{n}'_\mathrm{b}))$, where $\hat{n}'_\mathrm{b} = \int_T^{T'} \hat{b}^\dagger(s)\hat{b}(s)ds$ is the photon number operator for the generated beam segment.

3. **Stationarity.** The statistics of the laser and beam are invariant under time translation, in the long-time limit. In particular, the mean of $\hat{n}_\mathrm{c}$ has a unique long-time limit, μ.

4. **Ideal Glauber$^{(1),(2)}$-coherence.** The stationary beam is close to an ideal laser beam [14, 15, 16, 6] — an eigenstate of $\hat{b}(t)$ of eigenvalue $\beta(t) = \sqrt{\mathcal{N}}e^{i\sqrt{\ell}W(t)}$, with $W(t)$ a Weiner process [16] — in the sense that the beam's first- and second-order Glauber coherence functions [17] well approximate those of the ideal beam. The first- and second-order Glauber coherence functions are defined as $G^{(1)}(s,t) = \langle \hat{b}^\dagger(s)\hat{b}(t)\rangle$, $G^{(2)}(s,s',t',t) = \langle \hat{b}^\dagger(s)\hat{b}^\dagger(s')\hat{b}(t')\hat{b}(t)\rangle$. $G^{(1)}$ yields the photon flux $\mathcal{N} = G^{(1)}(t,t)$, and the coherence $\mathfrak{C} = \max_\omega |\int_{-\infty}^{\infty} G^{(1)}(s,t)e^{-i\omega s}ds|$. The requirement on $G^{(1)}$ in this Condition is that the laser power spectrum is Lorentzian (or close to it) with linewidth $\ell \equiv 4\mathcal{N}/\mathfrak{C}$, while the requirement on $G^{(2)}$ implies that the photon statistics are Poissonian (or close to it).

3 Analytical derivation

Here, we only *sketch* the analytical proof of that the above Conditions lead to the upper bound $\mathfrak{C} = O(\mu^4)$. Consider a heterodyne measurement [18] of the laser beam in the interval $[t-\tau, t)$, where $\tau = \sqrt{3/(2\mathcal{N}\ell)}$ (this value is chosen to give the tightest bound, below). From the result, the observer can form an estimate, ϕ_F, of the phase of the laser beam at that time. Consider two methods by which a second, newly arrived, observer can estimate ϕ_F. The first method is by heterodyne measurement of the laser beam in the interval $(t, t+\tau]$. From Condition 4 we can show that the mean square error (MSE) for this estimate can attain $4\sqrt{8/(3\mathfrak{C})}$. The second method is by direct measurement on the laser cavity at time t. Now, Condition 2 ensures that information about ϕ_F can only be encoded in that quantity conjugate to $\hat{n}_\mathrm{c}$, which has mean μ from Condition 3. Using a result from Ref. [19], the MSE of any such estimate is bounded below by k/μ^2, where $k \approx 1.8936$. Condition 2 also implies that the first method accesses only that phase information stored in the cavity at time t. Thus the MSE from the first method cannot be smaller than that of the second, which cannot be smaller than k/μ^2. Hence,

$$\mathfrak{C}^{\mathrm{ideal}} \lesssim 11.90\mu^4. \tag{1}$$

4 The tensor network description

MPS methods are widely used in quantum information theory and condensed matter physics [13, 20], and have had some applications in quantum optics [21, 22], but have never been used to describe a laser beam, to the best of our knowledge. In particular, while Ref. [21] points out that a cavity quantum-electrodynamics system can be generally emulated using such a sequential process, the authors were not concerned with describing coherence generation (in the sense defined above) by a laser. Rather, they assumed external sources of coherence, *i.e.* lasers, driving their cavity QED system.

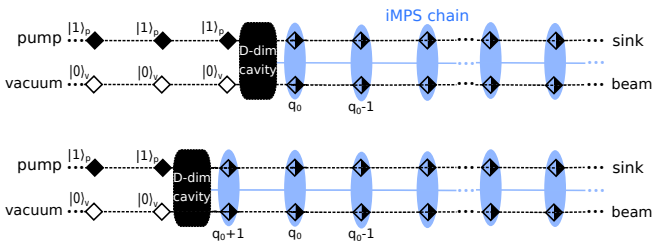


Figure 1: Conceptual diagram of our iMPS laser model containing five elements: the cavity (c), a pump, a vacuum input, the beam output (b), and a sink (s), all of which are essential for laser operation. We consider the sink and beam as a joint four-level system. The time evolution of the cavity (c) is governed by the generative interaction $\hat{V}_q = \sum_{j_{q+1},m,n} A^{[j_{q+1}]}_{mn} |j_{q+1}\rangle_\mathrm{o}|m\rangle_\mathrm{c}\langle n|$, which maps a D-dimensional vector space into a $4 \times D$-dimensional one.

Fig. 1 illustrates our MPS description of an ideal laser system. As pictured in the figure, we are interested in the *one-site unit-cell* infinite MPS (iMPS) that $\hat{V}$ eventually creates for arbitrary consecutive times $q_0\delta t$ and $(q_0+1)\delta$, where δt is an arbitrarily small time (connecting the discretized system to the continuum model). In terms of the A operators used above, the iMPS is given by

$$|\Psi_{\mathrm{iMPS}}\rangle = \sum_{\ldots,j_{q_0},j_{q_0-1},\ldots} \langle\Phi(q{=}+\infty)|_\mathrm{c} \cdots A^{[j_{q_0}]}_{(q_0)} \times A^{[j_{q_0-1}]}_{(q_0-1)} \cdots |\Phi(q{=}-\infty)\rangle_\mathrm{c} |\ldots, j_{q_0}, j_{q_0-1}, \ldots\rangle_\mathrm{o} \,, \tag{2}$$

where $|\Phi(q)\rangle_\mathrm{c}$ denotes the state of the cavity at integer time q. We suppose in the last step, $q = +\infty$, the cavity decouples from the output. Since there exists translational invariance in the outputs, we now drop the (q)-subscripts. The iMPS in Eq. (2) is fully equivalent to the tensor-network algorithm introduced in Ref. [23] when it reaches its fixed-point for the familiar reduced density matrix of the laser cavity, ρ^{ss}, i.e. $\sum_j \hat{A}^{[j]}\rho^{\mathrm{ss}}\hat{A}^{[j]\dagger} = \rho^{\mathrm{ss}}$. (Note also that the orthogonality of A-matrices are fixed due to the nature of the isometry and are heavily *sparse* due to photon number conservation.)

A-matrices relate to the laser's one-photon gain operator as $\hat{G} = A^{[0]}/\sqrt{\mathcal{N}\delta t}$ and to one-photon loss operator as $\hat{L} = A^{[3]}/\sqrt{\mathcal{N}\delta t}$. To obtain the ultimate limit to coherence, we do not assume linear damping ($L_n \propto \sqrt{n}$). Rather, guided by iMPS optimization of $\mathfrak{C}$, we define our family of models by the choices

$$\rho_n \propto \sin^4\left(\pi\frac{n+1}{D+1}\right), \; G_n = 1\,, \; L_n \in \mathbb{R}_+, \tag{3}$$

for which μ (Condition 3) equals $(D-1)/2$ and $\mathcal{N}$ (Condition 4) equals 1 (which simply sets a convenient time

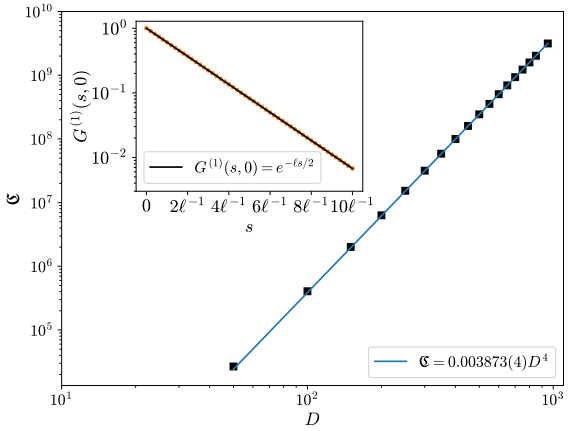


Figure 2: iMPS calculations (squares) of the beam coherence $\mathfrak{C}$ for our laser model as a function of dimension $D = 2\mu + 1$. The line is a fit $\mathfrak{C} \propto D^4$. Inset: numerical calculation of first-order Glauber coherence function $G^{(1)}(s, 0)$, which is indistinguishable from the ideal exponential decay (solid line).

unit). For our model, the coherence can be evaluated as $\mathfrak{C} = \int_{-\infty}^{\infty} G^{(1)}(s,t)ds = 2\mathrm{Tr}[\hat{L}^\dagger \mathcal{L}_+^{-1}(\hat{L}\rho_{\mathrm{ss}})]$, where $\mathcal{L}_+^{-1}$ is the inverse of $\mathcal{L}$ on its row space. We evaluate this for the above family of models, with D up to 1000. The data fit a power law $\mathfrak{C} \sim 0.0619(8)\mu^4$, as shown in Fig. 2.

We can show analytically that our model exactly satisfies Conditions 1–3, and we also showed numerically (not presented here) that Condition 4 is satisfied by our model for $\mu \gg 1$. Hence it shows that the scaling of the upper bound in our theorem is achievable, albeit with a far smaller coefficient than that in Eq. (1).

5 Conclusion

The Schawlow–Townes limit to laser coherence $\mathfrak{C}$ (the number of mutually coherent photons emitted in the beam) is only a standard quantum limit. Beyond it lies a Heisenberg limit which scales quadratically better in terms of μ (the number of excitations in the laser itself). For μ large this represents a vast improvement in laser coherence properties. We constructed a model that achieves this quantum enhancement in scaling, while retaining the same first- and second-order coherence properties as an ideal laser beam (a constant-intensity coherent state with a diffusing phase). It is the assumption of these coherence properties that allowed us to prove the Heisenberg limit $\mathfrak{C}_{\mathrm{HL}}^{\mathrm{ideal}} = O(\mu^4)$. It is thus natural to ask whether relaxing this assumption would enable an even higher scaling to be achieved. Preliminary results suggest that this is indeed the case. However, this remains to be investigated, along with many other fundamental and practical issues.

References

[1] V. Giovannetti, S. Lloyd, L. Maccone, *Science* **306**, 1330 (2004).

[2] C. M. Caves, *Phys. Rev. D* **23**, 1693 (1981).

[3] B. Yurke, S. L. McCall, J. R. Klauder, *Phys. Rev. A* **33**, 4033 (1986).

[4] D. Berry, M. Hall, H. Wiseman, *Phys. Rev. Lett.* **111**, 113601 (2013).

[5] A. L. Schawlow, C. H. Townes, *Phys. Rev.* **112**, 1940 (1958).

[6] H. M. Wiseman, *Phys. Rev. A* **60**, 4083 (1999).

[7] C. Sayrin, *et al.*, *Nature* **477**, 73 EP (2011).

[8] K. S. Chou, *et al.*, *Nature* **561**, 368 (2018).

[9] S. D. Bartlett, H. M. Wiseman, *Phys. Rev. Lett.* **91**, 097903 (2003).

[10] S. D. Bartlett, T. Rudolph, R. W. Spekkens, *Rev. Mod. Phys.* **79**, 555 (2007).

[11] I. Affleck, T. Kennedy, E. H. Lieb, H. Tasaki, *Phys. Rev. Lett.* **59**, 799 (1987).

[12] D. Perez-Garcia, F. Verstraete, M. M. Wolf, J. I. Cirac, *Quantum Info. Comput.* **7**, 401 (2007).

[13] U. Schollwock, *Annals of Physics* **326**, 96 (2011). January 2011 Special Issue.

[14] W. H. Louisell, *Quantum Statistical Properties of Radiation* (John Wiley & Sons, New York, 1973).

[15] M. Sargent, M. O. Scully, W. E. Lamb, eds., *Laser Physics* (Addison-Wesley, Reading Mass., 1974).

[16] H. Carmichael, *Statistical Methods in Quantum Optics 1* (Springer, 1999).

[17] R. J. Glauber, *Phys. Rev.* **130**, 2529 (1963).

[18] H. M. Wiseman, G. J. Milburn, *Quantum Measurement and Control* (Cambridge University Press, Cambridge, England, 2010).

[19] A. Bandilla, H. Paul, H. H. Ritze, *Quantum Optics: Journal of the European Optical Society Part B* **3**, 267 (1991).

[20] R. Orús, *Annals of Physics* **349**, 117 (2014).

[21] C. Schön, E. Solano, F. Verstraete, J. I. Cirac, M. M. Wolf, *Phys. Rev. Lett.* **95**, 110503 (2005).

[22] M. Jarzyna, R. Demkowicz-Dobrzanski, *Phys. Rev. Lett.* **110**, 400 (2013).

[23] I. P. McCulloch, *ArXiv e-prints* **0804.2509** (2008).

Experimental time-reversed adaptive Bell measurement towards all-photonic quantum repeaters

Rikizo Ikuta[1 2 *] Yasushi Hasegawa[1] Nobuyuki Matsuda[3] Kiyoshi Tamaki[4]
Hoi-Kwong Lo[5 6 7] Takashi Yamamoto[1 2] Koji Azuma[8 9] Nobuyuki Imoto[2]

[1] *Graduate School of Engineering Science, Osaka University, Japan*
[2] *Quantum Information and Quantum Biology Division, Institute for Open and Transdisciplinary Research Initiatives, Japan*
[3] *Department of Communications Engineering, Graduate School of Engineering, Tohoku University, Japan*
[4] *Graduate School of Science and Engineering for Research, University of Toyama, Japan*
[5] *Center for Quantum Information and Quantum Control (CQIQC), University of Toronto, Canada*
[6] *Department of Physics, University of Toronto, Canada*
[7] *The Edward S. Rogers Sr. Department of Electrical & Computer Engineering, University of Toronto, Canada*
[8] *NTT Basic Research Laboratories, NTT Corporation, Japan*
[9] *NTT Research Center for Theoretical Quantum Physics, NTT Corporation Japan*

Abstract. Quantum repeaters are indispensable for the quantum internet over the globe. The quantum repeaters had been believed to require matter-based quantum memories or qubits. Recently, this belief was disproved by a proposal of all-photonic quantum repeaters with no use of matter quantum memories and matter qubits. In this work, we demonstrated a proof-of-principle experiment of all-photonic time-reversed adaptive (TRA) Bell measurement for a key component of the all-photonic quantum repeaters.

This work has been published in Nature Communications [1], and the full version is available at https://www.nature.com/articles/s41467-018-08099-5.

Keywords: quantum repeater, quantum communication, Bell measurement

Quantum internet [2]—which is internet with an ability to transmit not only classical information but also quantum information—enables us to accomplish a variety of applications, such as quantum teleportation [3], quantum key distribution (QKD) [4, 5] and precise atomic clock synchronization [6], among arbitrary parties all over the world. For this, it is reasonable to utilize not only satellites [7, 8, 9] but also optical fiber networks that have been already installed in the world. An important building block for such a quantum internet against loss of photons in optical fibers is to utilize quantum repeaters [10, 11] over an optical fiber network. The quantum repeaters had been believed to require matter-based quantum systems for quantum memories or qubits. However, a theoretical proposal disproved this belief by showing all-photonic quantum repeaters with the use of no matter quantum memories and matter qubits[12]. Due to its all-optical nature, this scheme has several advantages compared to conventional quantum repeaters with matter quantum memories. For example, (1) the repetition rate could be as high as one wants, (2) the scheme could work at room temperature without cooling systems, and (3) the scheme does not need quantum interfaces for wavelength conversion of photons.

In this work [1], we demonstrated all-photonic time-reversed adaptive (TRA) Bell measurement as a proof-of-principle experiment for a key component of the all-photonic quantum repeaters. In the previous proposals [12, 13], a lot of single photons are required for implementing the TRA Bell measurement, but our experimental design dramatically reduces the number of the photons for an initial state for the TRA Bell measurement. In addition, it does not require large-scale optical switches and quantum nondemolition measurement [13], let alone quantum error correcting codes. The TRA Bell measurement is based on the concept of the 'time-reversal' in the proposal of all-photonic quantum repeaters and combination of a local delayed preparation of the Greenberger-Horne-Zeilinger (GHZ) state with utilization of the type-II fusion gate [14]. The conceptual experimental setup is shown in Fig. 1. The three-photon GHZ state in modes 1, 2 and 3 is initially prepared. The situation in the figure is that photons in modes A and B, which may be entangled with a distant node, are sent to the TRA Bell measurement system, and only the photon in mode A survives. Photon detection of the fusion gate for photon 1 disentangles the photon from the GHZ state, and the fusion gate for photon A and 2 teleports the quantum state of photon A to photon 3. If only the photon B reaches and photon A is lost, photon 2 is disentangled from the GHZ state and the quantum state of photon 1 is teleported to photon 3. An important feature is that the switch between connecting and disentangling is performed passively. We clearly observed that the quantum state of the survived single photon was teleported faithfully with no disturbance from the other lost photons. If the GHZ state is treated in a lossless manner, our TRA Bell measurement system could double the achievable distance of the QKD in principle. This means that it could have the same impact as the all-photonic intercity QKD [13].

*ikuta@mp.es.osaka-u.ac.jp

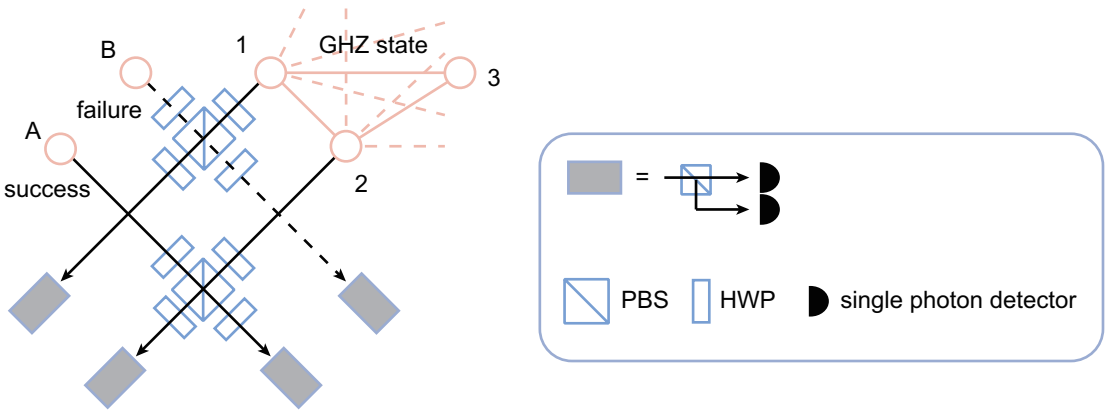


Figure 1: Our experimental setup of the all-photonic time-reversed adaptive Bell measurement for polarizing photons. The type-II fusion gate is composed of polarizing beamsplitters (PBSs), half-wave plate (HWP) and single photon detectors.

References

[1] Y. Hasegawa *et al.*, *Experimental time-reversed adaptive bell measurement towards all-photonic quantum repeaters*, Nature Communications **10**, 378 (2019).

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

[3] C. H. Bennett *et al.*, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895-1898 (1993).

[4] C. H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proc. IEEE Int. Conf. on Comp. Sys. and Signal Processing, 175-179 (Bangalore, India, 1984).

[5] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661-663 (1991).

[6] P. Kómór, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, M. D. Lukin, *A quantum network of clocks*, Nature Physics **10**, 582-587 (2014).

[7] J. Yin *et al.*, *Satellite-based entanglement distribution over 1200 kilometers*, Science **356**, 1140 (2017).

[8] S.-K. Liao *et al.*, *Satellite-to-ground quantum key distribution*, Nature **549**, 43 (2017).

[9] J.-G. Ren *et al.*, *Ground-to-satellite quantum teleportation*, Nature **549**, 70 (2017).

[10] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum repeaters: The role of imperfect local operations in quantum communication*, Physical Review Letters **81**, 5932 (1998).

[11] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, *Long-distance quantum communication with atomic ensembles and linear optics*, Nature **414**, 413 (2001).

[12] K. Azuma, K. Tamaki, and H.-K. Lo, *All-photonic quantum repeaters*, Nature communications **6**, 6787 (2015).

[13] K. Azuma, K. Tamaki, and W. J. Munro, *All-photonic intercity quantum key distribution*, Nature communications **6**, 10171 (2015).

[14] D. E. Browne and T. Rudolph, *Resource-efficient linear optical quantum computation*, Physical Review Letters **95**, 010501 (2005).

Observation of emergent momentum-time skyrmions in parity-time-symmetric non-unitary quench dynamics

Kunkun Wang[1 2] Xingze Qiu[3 4]
Lei Xiao[1 2] Xiang Zhan [1 2] Zhihao Bian [1 2] Barry C. Sanders [5 6 7] Wei Yi [3 4] * Peng Xue [1 2 5] †

[1] *Beijing Computational Science Research Center, Beijing 100084, China*
[2] *Department of Physics, Southeast University, Nanjing 211189, China*
[3] *CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*
[4] *CAS Center For Excellence in Quantum Information and Quantum Physics, Hefei 230026, China*
[5] *Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*
[6] *Program in Quantum Information Science, Canadian Institute for Advanced Research, Toronto, Ontario M5G 1Z8, Canada*
[7] *Shanghai Branch, National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Shanghai 201315, China*
[8] *State Key Laboratory of Precision Spectroscopy, East China Normal University, Shanghai 200062, China*

Abstract. Topology in quench dynamics gives rise to intriguing dynamic topological phenomena, which are intimately connected to the topology of static Hamiltonians yet challenging to probe experimentally. Here we theoretically characterize and experimentally detect momentum-time skyrmions in parity-time ($\mathcal{PT}$)-symmetric non-unitary quench dynamics in single-photon discrete-time quantum walks. The emergent skyrmion structures are protected by dynamic Chern numbers defined for the emergent two-dimensional momentum-time submanifolds, and are revealed through our experimental scheme enabling the construction of time-dependent non-Hermitian density matrices via direct measurements in position space. Our work experimentally reveals the interplay of $\mathcal{PT}$ symmetry and quench dynamics in inducing emergent topological structures, and highlights the application of discrete-time quantum walks for the study of dynamic topological phenomena.

Keywords: photonic quantum walk, parity-time-symmetric, skyrmions, quantum quench

1 Introduction

Topological phases feature a wealth of fascinating properties governed by the geometry of their ground-state wave functions at equilibrium, but topological phenomena also manifest as non-equilibrium quantum dynamics in driven-dissipative and Floquet systems, as well as in quench processes. Here we experimentally establish discrete-time photonic quantum walks (QWs) as one of the promising arena for engineering and detecting dynamic topological phenomena, among which, single photons, starting from their initial states, are subject to repeated unitary operations.

Here we theoretically characterize and experimentally detect dynamic skyrmion structures, a two-dimensional topological object, in $\mathcal{PT}$-symmetric one-dimensional QWs of single photons. In QW dynamics, dynamic skyrmions manifest themselves in the momentum-time spin texture of the time-evolved density matrix, and are protected by quantized dynamic Chern numbers in emergent momentum-time submanifolds. To detect dynamic skyrmions, we devise an experimental scheme where time-dependent momentum-space density matrices of spatially non-localized states are constructed based on a combination of interference-based measurements and projective measurements in position space. We confirm the emergence of dynamic skyrmion structures when QW dynamics correspond to quenches between distinct FTPs in the $\mathcal{PT}$-symmetry-unbroken regime, where the dynamics is coherent despite being non-unitary. By contrast, when the system is quenched into the $\mathcal{PT}$-symmetry-broken regime, skyrmions are absent in the momentum-time space, as the dynamics become incoherent. Our work unveils the fascinating relation between emergent topology and $\mathcal{PT}$-symmetric non-unitary dynamics, and opens up exploration of higher-dimensional dynamic topological structures using QWs.

2 Quench dynamics in $\mathcal{PT}$-symmetric QWs

We experimentally implement $\mathcal{PT}$-symmetric non-unitary QWs on a one-dimensional lattice L ($L \in \mathbb{Z}$) with single photons in the cascaded interferometric network illustrated in Fig. 1. The corresponding Floquet operator is [1]

$$U = R\left(\frac{\theta_1}{2}\right) SR\left(\frac{\theta_2}{2}\right) MR\left(\frac{\theta_2}{2}\right) SR\left(\frac{\theta_1}{2}\right), \qquad (1)$$

where $R(\theta)$ rotates coin states (encoded in the horizontal and vertical polarizations of single photons $|H\rangle$ and $|V\rangle$) by θ about the y-axis, and S moves the photon to neighbouring spatial modes depending on its polarization. The loss operator $M = \mathbb{1}_{\mathrm{w}} \otimes \left(|+\rangle\langle+| + \sqrt{1-p}\,|-\rangle\langle-|\right)$ enforces a partial measurement in the basis $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$ at each time step with a success probability $p \in [0, 1]$. Note that the non-unitary QW driven by U reduces to a unitary one $p = 0$.

*wyiz@ustc.edu.cn
†gnep.eux@gmail.com

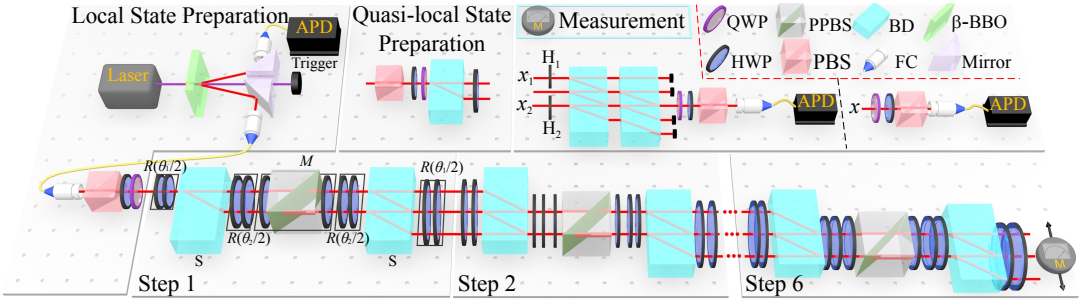


Figure 1: Experimental setup. Photons are generated via spontaneous parametric down conversion through a Type-I non-linear β-Barium-Borate (BBO) crystal. The single signal photon can be prepared in an arbitrary linear polarization state via a polarizing beam splitter (PBS) and wave plates. Conditional shift operation S and coin rotation R are realized by a beam displacer (BD) and two half-wave plates (HWPs), respectively. For non-unitary QWs, a sandwich-type HWP-PPBS-HWP setup is inserted to introduce non-unitarity, where PPBS is the partially polarizing beam splitters. The signal and heralding photons are detected by avalanche photodiodes (APDs).

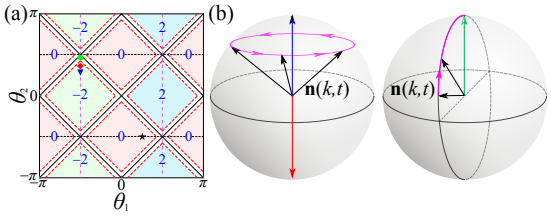


Figure 2: (a) Phase diagram for QWs governed by the Floquet operator U in Eq. (1), with the corresponding topological numbers ν as a function of coin parameters (θ_1, θ_2). (b) Schematic illustrations of the time evolution of $\mathbf{n}(k,t)$ on a Bloch sphere when E_k^{f} is real (left) and imaginary (right), respectively.

We define the quasienergy ϵ and eigenstate $|\psi\rangle$ as $U|\psi\rangle = \gamma^{-1}\mathrm{e}^{-i\epsilon}|\psi\rangle$, where $\gamma = (1-p)^{-\frac{1}{4}}$. U possesses passive $\mathcal{PT}$ symmetry with $\mathcal{PT}\gamma U\left(\mathcal{PT}\right)^{-1} = \gamma^{-1}U^{-1}$, where $\mathcal{PT} = \sum_x |-x\rangle\langle x| \otimes \sigma_3\mathcal{K}$, $\sigma_3 = |H\rangle\langle H| - |V\rangle\langle V|$, and $\mathcal{K}$ is the complex conjugation. U also features topological properties, characterized by winding numbers defined through the global Berry phase. We show the topological phase diagram of the system in Fig. 2(a), where distinct FTPs are marked by their corresponding winding numbers. The boundaries between $\mathcal{PT}$-symmetry-unbroken and -broken regimes are also shown in red-dashed lines, with $\mathcal{PT}$-symmetry-broken regimes surrounding topological phase boundaries.

To simulate quench dynamics, we initialize the walker photon in the eigenstate $|\psi^{\mathrm{i}}\rangle$ of a Floquet operator $U^{\mathrm{i}} = \mathrm{e}^{-iH_{\mathrm{eff}}^{\mathrm{i}}}$, characterized by coin parameters $(\theta_1^{\mathrm{i}}, \theta_2^{\mathrm{i}})$. The walker at the t-th time step is given by $|\psi(t)\rangle = \mathrm{e}^{-iH_{\mathrm{eff}}t}|\psi^{\mathrm{i}}\rangle$, such that the resulting QW can be identified as a sudden quench between $H_{\mathrm{eff}}^{\mathrm{i}}$ and H_{eff}. Adopting notations in typical quench dynamics, we denote U and H_{eff} as U^{f} and $H_{\mathrm{eff}}^{\mathrm{f}}$ in the following, characterized by coin parameters $(\theta_1^{\mathrm{f}}, \theta_2^{\mathrm{f}})$.

We denote pre- and post-quench Floquet operators in each k-sector as U_k^{i} and U_k^{f}, respectively, whose eigenstates are $|\psi_{k,\pm}^{\mathrm{i,f}}\rangle$. Quasienergies of $U_k^{\mathrm{i,f}}$ are denoted as $\epsilon_{k,\pm}^{\mathrm{i,f}}$, with $\epsilon_{k,\pm}^{\mathrm{i,f}} = \pm E_k^{\mathrm{i,f}}$.

By invoking the biorthogonal basis, the non-unitary time evolution of the system is captured by a non-Hermitian density matrix, which can be written as

$$\rho(k,t) = \frac{1}{2}\left[\tau_0 + \mathbf{n}(k,t)\cdot\boldsymbol{\tau}\right], \tag{2}$$

where $\mathbf{n}(k,t) = (n_1, n_2, n_3)$, $\boldsymbol{\tau} = (\tau_1, \tau_2, \tau_3)$, $\tau_i = \sum_{\mu,\nu=\pm} |\psi_{k,\mu}^{\mathrm{f}}\rangle\sigma_i^{\mu\nu}\langle\chi_{k,\nu}^{\mathrm{f}}|$ $(i = 0,1,2,3)$, and $\langle\chi_{k,\mu}^{\mathrm{f}}|$ $\left(|\psi_{k,\mu}^{\mathrm{f}}\rangle\right)$ is the left (right) eigenvector of U_k^{f}. Here, σ_0 is a 2×2 identity matrix, and σ_i $(i = 1,2,3)$ is the corresponding standard Pauli matrix.

As illustrated in Fig. 2(b), when E_k^{f} is real, $\mathbf{n}(k,t)$ rotates around poles of the Bloch sphere with a period $t_0 = \pi/E_k^{\mathrm{f}}$. Thus, momenta corresponding to poles of the Bloch sphere are identified as two different kinds of fixed points, where the density matrices do not evolve in time. In contrast, when E_k^{f} is imaginary, there are no fixed points in the dynamics, as $\mathbf{n}(k,t)$ asymptotically approaches the north pole in the long-time limit.

When U^{i} and U^{f} belong with distinct FTPs in the $\mathcal{PT}$-symmetry-unbroken regime, fixed points of different kinds necessarily emerge in pairs. Each momentum submanifold between a pair of distinct fixed points can be combined with the S^1 topology of the periodic time evolution to form an emergent S^2 momentum-time manifold, which can be mapped to the S^2 Bloch sphere of $\mathbf{n}(k,t)$. The Chern number characterizing such an $S^2 \to S^2$ mapping is finite and gives rise to intriguing skyrmion structures in the emergent momentum-time manifolds.

In our experiment, we perform projective measurements and interference-based measurements to construct the Hermitian density matrix $\rho'(k,t) = |\psi_k(t)\rangle\langle\psi_k(t)|$. This is achieved by writing $\rho'(k,t) = \frac{1}{2}\sum_{j=0}^{3}\sum_{x_1,x_2}\mathrm{e}^{-ik(x_1-x_2)}\langle\psi_{x_2}(t)|\sigma_j|\psi_{x_1}(t)\rangle\sigma_j$, where $|\psi_x(t)\rangle$ is the coin state on site x at the t-th time step. We experimentally measure $\langle\psi_{x_2}(t)|\sigma_j|\psi_{x_1}(t)\rangle$ $(j = 0,1,2,3)$ for each pair of positions x_1 and x_2 directly. We then calculate the non-Hermitian density matrix $\rho(k,t)$ from $\rho'(k,t)$ and determine $\mathbf{n}(k,t)$ through $\mathbf{n}(k,t) = \mathrm{Tr}\left[\rho(k,t)\boldsymbol{\tau}\right]$.

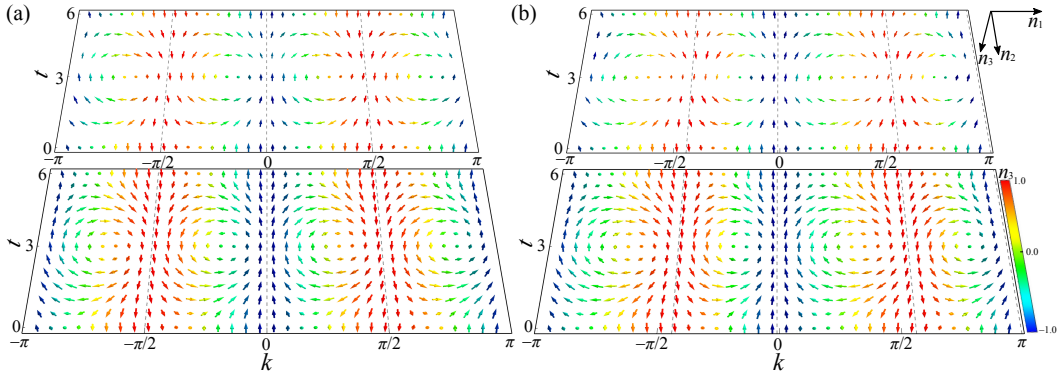


Figure 3: Experimental results of spin texture $\mathbf{n}(k,t)$. Experimental (upper layer) and theoretical results (lower layer) of spin texture $\mathbf{n}(k,t)$ in the momentum-time space for quench processes corresponding to unitary, and **(b)** non-uniatry, respectively. The spin textures are colored according to $n_3(k,t)$ and fixed points are indicated by dashed lines.

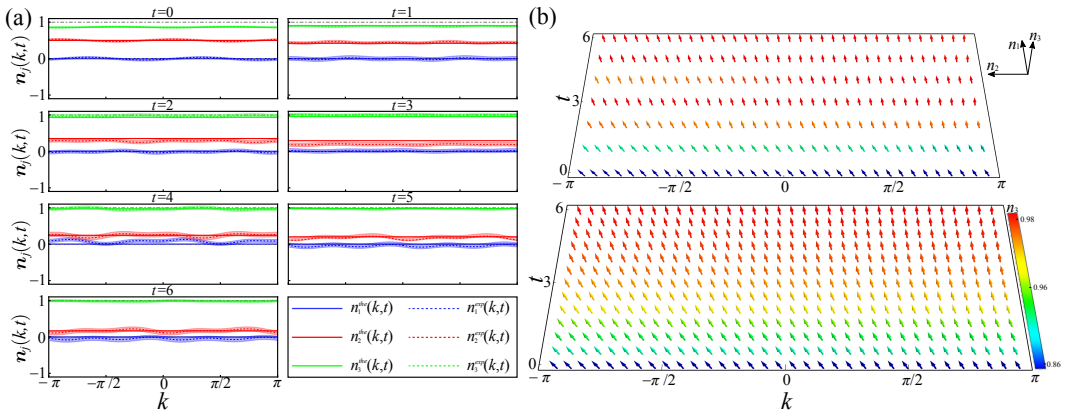


Figure 4: Experimental results for the $\mathcal{PT}$-symmetric broken QW dynamics. **(a)** Time-evolution and **(b)** spin textures of $\mathbf{n}(k,t)$ in momentum-time space. The quasi-energy spectrum associated with U^{f} is completely imaginary in this case.

3 Results

We first study fixed points and momentum-time skyrmions in the $\mathcal{PT}$-symmetry-unbroken regime. For comparison, we also experimentally characterize these quantities in unitary dynamics. We initialize the walker on a localized lattice site $|x=0\rangle$ and in the coin state $|\psi^{\mathrm{i}}_{-}\rangle_{\mathrm{c}}$. Importantly, $|\psi^{\mathrm{i}}_{k,-}\rangle = |\psi^{\mathrm{i}}_{-}\rangle_{\mathrm{c}}$ is an eigenstate of U^{i}_k for all k, with the corresponding $(\theta^{\mathrm{i}}_1, \theta^{\mathrm{i}}_2)$ on black dashed lines in Fig. 2(a). Without loss of generality, we choose $(\theta^{\mathrm{i}}_1 = \pi/4, \theta^{\mathrm{i}}_2 = -\pi/2)$ for both the unitary and non-unitary cases.

For the first case of study, we implement unitary QWs with $|\psi^{\mathrm{i}}_{-}\rangle_{\mathrm{c}} = (|H\rangle + i\,|V\rangle)/\sqrt{2}$ and $(\theta^{\mathrm{f}}_1 = -\pi/2, \theta^{\mathrm{f}}_2 = \pi/3)$, which simulate quench processes between FTPs with $\nu^{\mathrm{i}} = 0$ and $\nu^{\mathrm{f}} = -2$.

For the second case of study, we implement non-unitary QWs with $p = 0.36$, $|\psi^{\mathrm{i}}_{-}\rangle_{\mathrm{c}} = 0.7606\,|H\rangle + 0.6492i\,|V\rangle$, and $\left[\theta^{\mathrm{f}}_1 = -\pi/2, \theta^{\mathrm{f}}_2 = \arcsin(\frac{1}{\alpha}\cos\frac{\pi}{6})\right]$ (here $\alpha = \frac{\gamma}{2}(1+\sqrt{1-p})$). The post-quench FTP is in the $\mathcal{PT}$-symmetry unbroken regime with $\nu^{\mathrm{f}} = -2$.

Comparing Figs. 3(a) and (b), we see that dynamic skyrmion structures in the unitary and the $\mathcal{PT}$-symmetric non-unitary quench processes are qualitatively similar; albeit, in the non-unitary case, skyrmion structures are slightly deformed due to the shift of fixed points.

In the $\mathcal{PT}$-symmetric-symmetry-broken regime, we first initialize the walker on a localized lattice site in the coin state $(|H\rangle + |V\rangle)/\sqrt{2}$ and evolve it under U^{f} characterized by $(\theta^{\mathrm{f}}_1 = -\pi/2, \theta^{\mathrm{f}}_2 = \frac{1}{2}(\pi - \arccos\frac{1}{\alpha}))$, which has a completely imaginary quasienergy spectrum. As shown in Fig. 4(a), there is no periodical evolution in $\mathbf{n}(k,t)$ anymore. Instead, different components of $\mathbf{n}(k,t)$ slowly approach a steady state with $\mathbf{n} = (0,0,1)$ in the long-time limit. This is more clearly seen in momentum-time space shown in Fig. 4(b), where skyrmion structures are absent and vectors in all k-sectors tend to point out of the plane in the long-time limit.

References

[1] K. Wang, X. Qiu, L. Xiao, X. Zhan, Z. Bian, B. C. Sanders, W. Yi, and P. Xue Observation of emergent momentum-time skyrmions in parity-time-symmetric non-unitary quench dynamics *Nat. Commun.*, **10**, 2293, 2019.

A quantum cellular automaton for one-dimensional QED

Pablo Arrighi[1] * Cédric Bény[2] † Terry Farrelly[3] ‡

[1] *Aix-Marseille Univ., Université de Toulon, CNRS, LIS, Marseille and IXXI, Lyon, France.*
[2] *Department of Applied Mathematics, Hanyang University (ERICA), 55 Hanyangdaehak-ro, Ansan, Gyeonggi-do, 426-791, Korea.*
[3] *Institut für Theoretische Physik, Leibniz Universität Hannover, 30167 Hannover, Germany.*

Abstract. We propose a discrete spacetime formulation of quantum electrodynamics in one-dimension (the Schwinger model) in terms of quantum cellular automata, i.e. translationally-invariant local quantum circuits. These have exact gauge covariance and a maximum speed of information propagation. The continuum quantum field theory is recovered as a "convergent" sequence of quantum cellular automata, parameterized by the spacetime lattice spacing. This model provides a quantum simulation algorithm for the dynamics, and represents, to the best of our knowledge, a first complete QCA formulation of an interacting QFT.

Keywords: Quantum Cellular Automaton, Quantum Simulations, Schwinger Model, Quantum Field Theory

1 Introduction

Recently, a number of alternative descriptions of relativistic particles have emerged, which are attractively simple [1, 2, 3, 4, 5, 6]. These employ concepts from quantum information and quantum simulation to express the particles' dynamics directly as a circuit of local quantum gates. In the one-particle sector, these Quantum Walk models can simulate relativistic fermions propagating in $(3+1)$–dimensions, also in the presence of background electromagnetic and gravitational fields. In the two-particle sector, these interacting Quantum Walks models were shown to exhibit molecular binding. However, the many-particle sector of interacting quantum field theories (QFT) have so far remained unexplored by these discrete models.

In this work [7], we propose a discrete spacetime formulation of quantum electrodynamics (QED) in one dimension (the Schwinger model) [8], in terms of quantum cellular automata (QCA), which are essentially translationally invariant circuits of local quantum gates.

From a practical point of view, the QCA defines a quantum simulation algorithm for the dynamics of an interacting QFT (leaving aside the problems of state preparation and measurements [9], however). But, from a theoretical point of view it also constitutes a proof-of-principle showing that natively discrete formulations of an interacting QFT are possible and elegant. In this picture, the QFT is defined as a "convergent" sequence of QCA, parameterized by the spacetime lattice spacing—echoing the notions of continuum limit and renormalization.

In the paper, we discuss why we may hope to circumvent some of the technical issues of standard formulations of QFT this way. This includes problems coming from discrete space and continuous time formulations, such as the infinite speed of information propagation, and the fermion doubling problem, both of which do not occur in our formulation. In addition, standard formulations of interacting quantum field theories always need a form of discretization (usually in the form of a momentum cut-off) because there is no way of defining quantum theories which make sense in the continuum, unlike in classical field theory. Hence, rather than attempting a continuous formulation which fails and then having to renormalize it, it may be advantageous to start with a well-defined genuinely discrete one such as a QCA.

Because the formulation comes with a representation of scaling transformations (necessary to define the continuum limit), it is possible in principle to also obtain a representation of the Lorentz group as done in Refs. [10, 11, 12, 13].

Our construction is intuitive and requires little prerequisites. It leads to a simple, explanatory model of a QFT based on quantum information concepts. Given that QFT can be rather intricate, we believe this also constitutes an important pedagogical asset.

2 Quantum Cellular Automaton

Our QCA is defined by the circuit depicated in Figure 1. Each site of a one-dimensional lattice, with position $x = n\varepsilon$, $n \in \mathbb{Z}$, is associated with 2 qubits, or equivalently two fermionic (Dirac) modes.

Each mode can be occupied or empty, which corresponds to orthogonal states. The red wires represent "left-moving" modes, while the black wires represent "right-moving" modes (a terminology coming from the fact that, in the noninteracting and massless limit, the gates like W are just swaps).

The green wiggly lines represent an extra infinite-dimensional Hilbert space associated with each edge between two Fermionic site. This is the Hilbert space of the local electromagnetic modes, or gauge field. Because it involves infinite-dimensional Hilbert spaces, this model is not a standard QCA, but it is possible in principle to limit these Hilbert spaces to a finite basis.

*pablo.arrighi@univ-amu.fr
†cedric.beny@gmail.com
‡farreltc@tcd.ie

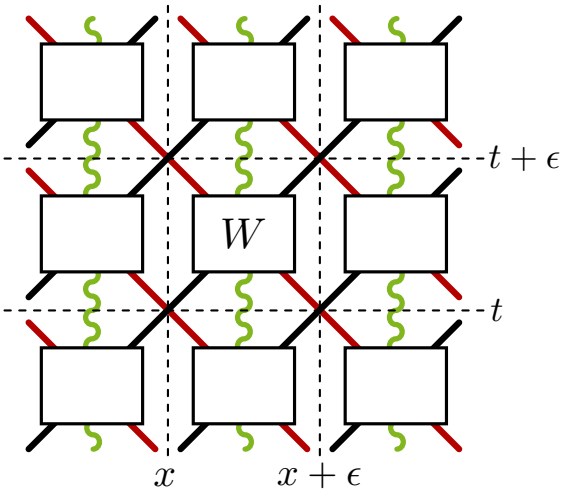


Figure 1: $(1+1)$–QED QCA structure. At $x+\varepsilon/2$ positions lies a wire carrying a state representing the gauge field. Its sole role is to count the Fermions passing by, and to undergo a phase accordingly: this phase triggers the interaction.

If we think of the modes simply as qubits, then each crossing between a red and a blue wire on the dashed line corresponds to a controlled-Z gate which multiplies the state by a minus sign only if both modes are occupied.

Each box represents the same unitary gate W. It takes as input a right-moving and a left-moving mode, as well as the electric field in between the two modes. Let us denote the input fermionic states as $|ij\rangle$, $i,j=0,1$. Similarly, let us denote the output states as $|ij\rangle$. We also use the discrete basis $|l\rangle$, $l\in\mathbb{Z}$ for the eigenstates of the electric field on each edge, with eigenvalues el, where e, where e is the charge of our fermions. Hence the electric field operator on a given edge is $E=eL$, where

$$L=\sum_{l\in\mathbb{Z}}|l\rangle\langle l|.$$

The gate W, which entirely specifies the dynamics of the theory, is defined by:

$$W=\Big(|00\rangle\langle 00|-|11\rangle\langle 11|+cV^\dagger|01\rangle\langle 10|+cV|10\rangle\langle 01| \\ -is|01\rangle\langle 01|-is|10\rangle\langle 10|\Big)e^{\frac{i}{2}\varepsilon^2e^2L^2},$$

where $c=\cos(m\varepsilon)$, $s=\sin(m\varepsilon)$, m being the "bare" mass of the fermions. The operator $V^\dagger$ increases the discrete value of the electric field by 1:

$$V^\dagger=\sum_{l\in\mathbb{Z}}|l+1\rangle\langle l|.$$

This gate can be intuitively interpreted as follows: the two fermions, when present, just pass past each other with amplitude $\cos(m\varepsilon)$, or change direction with amplitude $\sin(m\varepsilon)$. If there was no electric field, this would be the well known Dirac QCA, whose continuum limit is the the one-dimensional QFT representing free Dirac fermions of mass m [4, 14].

3 Gauge invarience

The operator V in the gates simply makes sure that the electric field to the right of a fermion is one step large than that of the left of a fermion. This is what makes the dynamic invariant under spatially local $U(1)$ *gauge transformations* as follows.

A gauge transformation corresponds to a choice of a different element $e^{i\phi(x)}$ of the group $U(1)$ at each vertex at a given time t, where $x=n\varepsilon$, $n\in\mathbb{Z}$.

These phases act on the Hilbert space of our system as follows: on the fermions at the point x, it maps $|nm\rangle$ to $e^{i(n+m)\phi(x)}$, where $n,m=0,1$. But it also maps the electric field states $|l\rangle$ in between sites x and $x+\varepsilon$ to $e^{-il(\phi(x+\varepsilon)-\phi(x))}|l\rangle$.

Hence, the state is gauge-invariant if the initial state is in the basis spanned by states which are tensor products of fermionic states $|nm\rangle$ and electric field states $|l\rangle$ such that those phases cancel out, i.e., reading from left to right, if the field value increases by 1 per fermion encountered.

The dynamical steps defined by W preserve the gauge invariance of the states by increasing (resp. decreasing) the electric field by one quantum everytime a fermion passes left (resp. right).

Instead of requiring gauge-invariance on the states, we can alternatively demand that we restrict observables to only gauge invariant ones. These form a quasilocal C*-algebra, of which the QCA step is an automorphism.

4 Continuum limit

For zero mass ($m=0$), the ε-dependence of our gates W is chosen such that, in conjunction also with strong assumptions on the states and observables, the QCA ought to converge for $\varepsilon\to 0$ to a quantum field theory: the (massless) Schwinger model.

This is possible because the massless Schwinger model is exactly solvable. For non-zero mass, however, it is likely not possible to find the exact dependence of the QCA on ε that is requires to converge to a smooth dynamics. Instead, one must expend the dynamics on powers of m around $m=0$, and find the dependence in ε for each order, a procedure known as *renormalization*.

In the zero mass case, in order to recover the standard Schwinger model, it is essential that we restrict the states to a specific Fock state which is spanned by creating a finite number of fermions on top of a special state $|\Omega\rangle$ called the vacuum. In order to preserve gauge-invariance, each fermion creation is associated with an increase in the electric field everywhere on the right side of it (local operators are recovered when considering only gauge-invariant even-order polynomials in those creation operators, as per the usual fermionic parity constraint).

These new creations operators are similar to those used in solving the Schwinger model in Ref. [8], and satisfy the usual fermionic anticommutation relations.

The vacuuum state $|\Omega\rangle$ that is required is not, as one might expect, the tensor product of the states $|00\rangle$ in the above notation (let's call it the computational vacuum).

Instead, $|\Omega\rangle$ corresponds to the vaccuum of the Dirac QFT, i.e, the so-called Dirac see, which is an infinite superposition of states with various occupation numbers.

It is most easily formulated as being the vaccuum for different fermions, whose creation amounts to the creation or annihilation of our original modes depending on the sign of their *momentum* (i.e., we are talking about the Fourier transform of the creation operators). It is these new fermions which correspond to the *electrons* and *positrons*.

In order to obtain a continuum limit, however, we need extra restrictions on the Fock states: there needs to be a momentum cutoff so that they are approximately constant at the level of the lattice spacing. In conjunction, we also need a momentum cutoff on observables, namely, they must be generated by "smeared" creations operators, i.e., linear combinations of the electron and positron creation operators with a wavefunction whose Fourier transform is also zero or rapidely decaying beyond a momentum cutoff.

With those assumptions, we provide a fairly detailed arguments (although not a proof) that the dynamics converge to the solution of the Schwinger model. Technically, we show how an appropriately smeared version of the fermions density converges to a field operator which evolves as a free boson of effective mass $e/\sqrt{\pi}$.

One may be surprised that the continuum limit is one involving bosons rather than a QFT of electrons and positrons, however, this is a peculiarity of the Schwinger model which comes from the fact that the model is *confined*: the energy of a pair of electron-positron increases with the distance between them. It is unclear to us whether a continuum limit could be formulated that lead to a more "microscopic" formulation of the QFT directly in terms of fermions.

References

[1] Sauro Succi and Roberto Benzi. Lattice boltzmann equation for quantum mechanics. *Physica D: Nonlinear Phenomena*, 69(3):327–332, 1993.

[2] I. Bialynicki-Birula. Weyl, Dirac, and Maxwell equations on a lattice as unitary cellular automata. *Phys. Rev. D.*, 49(12):6920–6927, 1994.

[3] David A Meyer. From quantum cellular automata to quantum lattice gases. *Journal of Statistical Physics*, 85(5-6):551–574, 1996.

[4] P. Arrighi, M. Forets, and V. Nesme. The Dirac equation as a Quantum Walk: higher-dimensions, convergence. Pre-print arXiv:1307.3524, 2013.

[5] Andre Ahlbrecht, Andrea Alberti, Dieter Meschede, Volkher B Scholz, Albert H Werner, and Reinhard F Werner. Molecular binding in interacting quantum walks. *New Journal of Physics*, 14(7):073050, 2012.

[6] Alessandro Bisio, Giacomo Mauro D'Ariano, Paolo Perinotti, and Alessandro Tosini. Thirring quantum cellular automaton. *Physical Review A*, 97(3):032132, 2018.

[7] Pablo Arrighi, Cédric Bény, and Terry Farrelly. A quantum cellular automaton for one-dimensional QED. *arXiv preprint arXiv:1903.07007*, 2019.

[8] Kirill Melnikov and Marvin Weinstein. Lattice schwinger model: Confinement, anomalies, chiral fermions, and all that. *Physical Review D*, 62(9):094504, 2000.

[9] S. P. Jordan, K. S. M. Lee, and J. Preskill. Quantum Algorithms for Fermionic Quantum Field Theories, 2014. arXiv:1404.7115v1.

[10] P. Arrighi and C. Patricot. A note on the correspondence between qubit quantum operations and special relativity. *Journal of Physics A: Mathematical and General*, 36(20):L287–L296, 2003.

[11] A. Bibeau-Delisle, A. Bisio, G. M. D'Ariano, P. Perinotti, and A. Tosini. Doubly special relativity from quantum cellular automata. *EPL (Europhysics Letters)*, 109(5):50003, 2015.

[12] Alessandro Bisio, Giacomo Mauro DAriano, and Paolo Perinotti. Quantum walks, weyl equation and the lorentz group. *Foundations of Physics*, 47(8):1065–1076, 2017.

[13] Fabrice Debbasch. Action principles for quantum automata and lorentz invariance of discrete time quantum walks. *arXiv preprint arXiv:1806.02313*, 2018.

[14] T. C. Farrelly. *Insights from Quantum Information into Fundamental Physics*. PhD thesis, University of Cambridge, 2015. arXiv:1708.08897.

Compression Protocols for Tensor Network States

Ge Bai [*1] Yuxiang Yang [2] [†] Giulio Chiribella [‡] [1] [3]

[1] *Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*
[2] *Institute for Theoretical Physics, ETH Zürich, Switzerland*
[3] *Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford, UK.*

Abstract. We construct compression protocols for parametric families of tensor network states. We start from exact protocols, constructed by partitioning the tensor network into constant and variable tensors, and by defining a suitable flow network in which the variable tensors are associated to the source and the physical systems are associated to the sink. Our protocols use a quantum memory of size determined by the minimum cut of the flow network, which is intuitively related to the flow of information from the variable tensors to the physical systems. We propose efficient algorithms to realise the compression protocols based on certain properties of tensor network states. For arbitrary tensor network states with given network topology and given edge dimensions, the memory usage of our protocols is optimal when all edge dimensions are powers of a given integer, and otherwise is optimal up to a multiplicative factor of at most $\log_2 3$. Applying the above technique, we show that arbitrary translationally invariant tensor network states of n identical systems can be compressed without errors into $O(\log n)$ memory qubits, which is the optimal scaling with n. Finally, we provide examples of approximate compression protocols for translationally invariant matrix product states, showing that states with finite correlation length can be compressed by operating on a small subset of the physical systems.

Keywords: Quantum data compression, tensor networks, matrix product states

Quantum data compression [1] is one of the pillars of quantum information theory. At the foundational level, it establishes the qubit as the basic unit of quantum information. At the more practical level, it provides a blueprint for the efficient transmission of quantum data in future quantum networks, with applications to distributed quantum computing [2] and quantum cloud computing [3].

The ultimate limit for compressing long sequences of independently prepared quantum states was established by Schumacher in the pure state case [1], and later extended to mixed states [4, 5, 6]. Universal compression protocols for the scenario where the average state of each system is unknown, except for an upper bound on its von Neumann entropy, were provided in Ref. [7]. In recent years, there has been an interest in developing compression protocols for identically prepared systems [8, 9, 10, 11, 12]. Such systems occur in a wide range of tasks from quantum tomography [13, 14] to quantum cloning [15, 16], estimation [17, 18], and machine learning [19]. Compression protocols for identically prepared systems, studied in Refs. [8, 9, 10, 11, 12], have found applications in quantum metrology [20] and inspired new results in quantum state estimation [21]. A basic instance of compression of identically prepared systems was demonstrated experimentally in Ref. [22].

Most of the compression protocols considered so far assume that the input systems are in a product state. However, many relevant scenarios involve correlated systems, whose state cannot be expressed as a tensor product of single-system states. The ability to store correlated states into a smaller amount of quantum bits is important for the simulation of many-body quantum systems. For example, it was shown that $O(\log n)$ [1] qubits are enough to simulate specific models of n-qubit many-body systems [23, 24, 25], and this result led to simulation of a 32-spin Ising chain using only 5 qubits [26]. In addition, many-body states can be used as probes in quantum metrology [27], and thus compression protocols for many-body states are useful to transmit such probes or to store them until they are measured.

In this paper we address the compression of tensor network states, a broad class that includes cluster states [28, 29], matrix product states (MPS) [30, 31, 32], projected entangled pair states (PEPS) [33, 34], tree tensor networks [35], and multi-scale entanglement renormalization ansatz (MERA) states [36]. Our first result involves translationally invariant MPSs [31], hereafter abbreviated as TIMPS. We show that a completely unknown TIMPS of n identical systems with given bond dimension can be compressed without errors into a number of logical qubits growing at most as $O(\log n)$. Our result enables a compressed simulation of various models of many-body quantum states, such as the one-dimensional Ising model [37] and the AKLT model [38]. The logarithmic scaling of the total memory is optimal, as the set of TIMPSs includes the set of all identically prepared states, for which the optimal compression protocol is known to require $\Omega(\log n)$ memory qubits, both for exact [10] and approximate protocols [11, 12]. The same result holds for states on higher dimensional lattices such as PEPSs: a generic translationally invariant n-particle state with a given bond dimension can be perfectly stored into $O(\log n)$ logical qubits. We then consider generic tensor network states without translational symmetry, but with the property that all tensors are constant, except for those on the boundary. For every subset of systems in the bulk, we show that our compression protocols satisfy an area law:

[*] baige@connect.hku.hk
[†] yangyu@phys.ethz.ch
[‡] giulio@cs.hku.hk

[1] Here and in the following $\log := \log_2$.

the number of logical qubits used to compress the systems in the chosen subset is proportional to the size of its boundary.

Our compression protocols are based on a general technique applicable to arbitrary tensor network states. The idea is to define a mapping from tensor networks to flow networks [39], namely networks with two distinguished vertices (the *source* and the *sink*) and with a non-negative number (the capacity) assigned to each edge. For a given parametric family of tensor network states, we first identify the *variable tensors*, that is, those that depend on the parameters specifying the states in the family. Then, we construct a flow network by associating the variable tensors with the source, and the physical systems to the sink. The capacity of an edge is defined as the logarithm of the dimension of the Hilbert space associated to that edge.

Our compression protocols use a number of qubits equal to the minimum cut in the network, defined as the minimum sum of the capacities of the edges crossing a partition of the network in two subsets, one containing the source, and the other containing the sink. This feature provides a graphical way to construct compression protocols, and motivates the search of tensor network representations with small values of the minimum cut.

Intuitively, the minimum cut is a bottleneck to the amount of information flowing from the free parameters to the physical systems, and therefore determines the compressibility of the parametric family. For the family of all tensor network states with given network topology and given edge dimensions, the number of memory qubits used by our protocol is minimum, provided that all the edge dimensions are powers of the same integer. For arbitrary edge dimensions, the amount of memory is optimal up to a multiplicative factor of at most $\log 3$, whose presence is due to the failure of the quantum version of the "max-flow min-cut theorem" [40].

We can efficiently realise the compression protocols on quantum computers under assumptions that hold for many tensor network states including TIMPS and MERA. We construct the algorithm using the universal quantum emulator [41], which simulates the encoding and decoding processes by consuming a polynomial number of input-output pairs.

We conclude the paper with a discussion of approximate compression protocols. Specifically, we consider the compression of MPSs with finite correlation length [31, 42] and with variable boundary conditions. We show that any such MPS can be approximately compressed by acting on a small number of systems near the boundaries. This allows us to cut and connect MPSs with local operations, which is convenient to measurement-based quantum computation (MBQC) [43, 44] using MPSs as resource states.

The full version of this paper can be found in [45].

References

[1] Benjamin Schumacher. Quantum coding. *Physical Review A*, 51(4):2738, 1995.

[2] Robert Beals, Stephen Brierley, Oliver Gray, Aram W Harrow, Samuel Kutin, Noah Linden, Dan Shepherd, and Mark Stather. Efficient distributed quantum computing. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 469(2153):20120686, 2013.

[3] Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph F Fitzsimons, Anton Zeilinger, and Philip Walther. Demonstration of blind quantum computing. *Science*, 335(6066):303–308, 2012.

[4] Hoi-Kwong Lo. Quantum coding theorem for mixed states. *Optics Communications*, 119(5-6):552–556, 1995.

[5] Michał Horodecki. Limits for compression of quantum information carried by ensembles of mixed states. *Physical Review A*, 57(5):3364, 1998.

[6] Howard Barnum, Carlton M Caves, Christopher A Fuchs, Richard Jozsa, and Benjamin Schumacher. On quantum coding for ensembles of mixed states. *Journal of Physics A: Mathematical and General*, 34(35):6767, 2001.

[7] Richard Jozsa, Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Universal quantum information compression. *Physical Review Letters*, 81(8):1714, 1998.

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

[9] Giulio Chiribella, Yuxiang Yang, and Cupjin Huang. Universal superreplication of unitary gates. *Physical Review Letters*, 114(12):120504, 2015.

[10] Yuxiang Yang, Giulio Chiribella, and Daniel Ebler. Efficient quantum compression for ensembles of identically prepared mixed states. *Physical Review Letters*, 116(8):080501, 2016.

[11] Yuxiang Yang, Giulio Chiribella, and Masahito Hayashi. Optimal compression for identically prepared qubit states. *Physical Review Letters*, 117(9):090502, 2016.

[12] Yuxiang Yang, Ge Bai, Giulio Chiribella, and Masahito Hayashi. Compression for quantum population coding. *IEEE Transactions on Information Theory*, 2018.

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

[14] G Mauro D'Ariano, Matteo GA Paris, and Massimiliano F Sacchi. Quantum tomography. *Advances in Imaging and Electron Physics*, 128:206–309, 2003.

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

[16] Dagmar Bruß, David P DiVincenzo, Artur Ekert, Christopher A Fuchs, Chiara Macchiavello,

and John A Smolin. Optimal universal and state-dependent quantum cloning. *Physical Review A*, 57(4):2368, 1998.

[17] Carl W Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969.

[18] Alexander S Holevo. *Probabilistic and statistical aspects of quantum theory*, volume 1. Springer Science & Business Media, 2011.

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

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

[21] Yuxiang Yang, Giulio Chiribella, and Masahito Hayashi. Attaining the ultimate precision limit in quantum state estimation. *arXiv preprint arXiv:1802.07587*, 2018.

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

[23] Barbara Kraus. Compressed quantum simulation of the ising model. *Physical Review Letters*, 107(25):250503, 2011.

[24] Walter León Boyajian, Valentin Murg, and Barbara Kraus. Compressed simulation of evolutions of the x y model. *Physical Review A*, 88(5):052329, 2013.

[25] Walter León Boyajian and Barbara Kraus. Compressed simulation of thermal and excited states of the one-dimensional x y model. *Physical Review A*, 92(3):032323, 2015.

[26] Zhaokai Li, Hui Zhou, Chenyong Ju, Hongwei Chen, Wenqiang Zheng, Dawei Lu, Xing Rong, Changkui Duan, Xinhua Peng, and Jiangfeng Du. Experimental realization of a compressed quantum simulation of a 32-spin ising chain. *Physical Review Letters*, 112(22):220501, 2014.

[27] Mathieu Beau and Adolfo del Campo. Nonlinear quantum metrology of many-body open systems. *Physical Review Letters*, 119(1):010403, 2017.

[28] Hans J Briegel and Robert Raussendorf. Persistent entanglement in arrays of interacting particles. *Physical Review Letters*, 86(5):910, 2001.

[29] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

[30] Mark Fannes, Bruno Nachtergaele, and Reinhard F Werner. Finitely correlated states on quantum spin chains. *Communications in Mathematical Physics*, 144(3):443–490, 1992.

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

[32] Frank Verstraete and J Ignacio Cirac. Matrix product states represent ground states faithfully. *Physical Review B*, 73(9):094423, 2006.

[33] Frank Verstraete and J Ignacio Cirac. Renormalization algorithms for quantum-many body systems in two and higher dimensions. *arXiv preprint cond-mat/0407066*, 2004.

[34] Frank Verstraete, Michael M Wolf, David Perez-Garcia, and J Ignacio Cirac. Criticality, the area law, and the computational power of projected entangled pair states. *Physical Review Letters*, 96(22):220601, 2006.

[35] Y-Y Shi, L-M Duan, and Guifre Vidal. Classical simulation of quantum many-body systems with a tree tensor network. *Physical review a*, 74(2):022320, 2006.

[36] Guifré Vidal. Class of quantum many-body states that can be efficiently simulated. *Physical Review Letters*, 101(11):110501, 2008.

[37] Ernst Ising. Beitrag zur theorie des ferromagnetismus. *Zeitschrift für Physik*, 31(1):253–258, 1925.

[38] Ian Affleck, Tom Kennedy, Elliott H Lieb, and Hal Tasaki. Rigorous results on valence-bond ground states in antiferromagnets. In *Condensed Matter Physics and Exactly Soluble Models*, pages 249–252. Springer, 2004.

[39] Lester Randolph Ford Jr and Delbert Ray Fulkerson. *Flows in networks*. Princeton university press, 2015.

[40] Shawn X Cui, Michael H Freedman, Or Sattath, Richard Stong, and Greg Minton. Quantum max-flow/min-cut. *Journal of Mathematical Physics*, 57(6):062206, 2016.

[41] Iman Marvian and Seth Lloyd. Universal quantum emulator. *arXiv preprint arXiv:1606.02734*, 2016.

[42] Michael M Wolf, Frank Verstraete, Matthew B Hastings, and J Ignacio Cirac. Area laws in quantum systems: mutual information and correlations. *Physical Review Letters*, 100(7):070502, 2008.

[43] Richard Jozsa. An introduction to measurement based quantum computation. *NATO Science Series, III: Computer and Systems Sciences. Quantum Information Processing-From Theory to Experiment*, 199:137–158, 2006.

[44] Daivd Gross, Jens Eisert, Norbert Schuch, and David Perez-Garcia. Measurement-based quantum computation beyond the one-way model. *Physical Review A*, 76(5):052315, 2007.

[45] Ge Bai, Yuxiang Yang, and Giulio Chiribella. Compression protocols for tensor network states. *arXiv preprint arXiv:1904.06772*, 2019.

Interfering future trajectories in experimental quantum-enhanced stochastic simulation

Farzad Ghafari[1] Nora Tischler[1] Carlo Di Franco[2] Jayne Thompson[3] Mile Gu[2 3] Geoff Pryde[1]

[1] *Centre for Quantum Dynamics, Griffith University, Brisbane, 4111, Australia*
[3] *Centre for Quantum Technologies, National University of Singapore, 117543, Singapore*
[2] *School of Physical and Mathematical Sciences, Nanyang Technological University, 639673, Singapore*

Abstract. Stochastic simulation plays an important role in quantitative science, enabling future predictions based on past observations. Here we report on systematic means to generate such models coherently, and its experimental realization using a photonic quantum information processor. A key feature of the processor is that it creates a quantum superposition of all possible future trajectories a stochastic system can evolve into. This superposition allows us to introduce, and demonstrate, the idea of comparing statistical futures of two classical processes via quantum interference. We demonstrate interference of two 16-dimensional quantum states, representing statistical futures of a given process, with a visibility of 0.96 ± 0.02.

Keywords: Quantum Optics, Quantum Information, Complexity Science, Quantum Models

Many of the most interesting phenomena are complex—whether in urban design, meteorology or financial prediction, the systems involved feature a vast array of interacting components. Predicting and simulating such systems often requires the use of a prohibitive amount of data, evincing a pressing need for more efficient tools in algorithmic modelling and simulation. Quantum technologies have shown the potential to dramatically reduce the amount of working memory required to simulate stochastic processes [1, 2]. A quantum device can replicate the system's conditional future behaviour, while storing less past information than provably optimal classical counterparts. The key to achieving a quantum memory advantage is maintaining coherence of the quantum memory during the simulation process. This advantage was first illustrated for simulating a particular stochastic process, where relevant past information was encoded within non-orthogonal polarisation states of a single photon [5]. The scheme, however, maintained quantum coherence over only a single simulation cycle. This limited the resulting simulator exhibited a memory advantage only when simulating a single time step.

In this talk, we first review recent results showing how unitary quantum circuits for generating future statistics of a stochastic process can be systematically designed – such that coherence is maintained at all stages of simulation [3]. We then introduce our recent experiments that realize such a quantum simulator using (time-bin) encoding in an optical system [4]. We illustrate how the resulting devices have the added benefit of being able to create a quantum superposition of all possible future trajectories of a stochastic process. We implement two such quantum simulations in parallel, simultaneously generating superpositions over the trajectories for each of two independent systems. Experimentally, this corresponds to using our quantum simulators to produce and control high-dimensional quantum states. These are interfered, allowing estimation of how well the corresponding statistical futures coincide.

Framework – A stochastic process describes a sequence of possible random variables X_t, where $t < 0$ can be considered the past and $t \geq 0$ the future. Any simulator that seeks to replicate correct conditional future statistics must retain relevant past information in some memory system. This involves a prescription for configuring its memory S in an appropriate state s for each possible observed past, such that systematic actions on S recover a sequence of future outputs that correctly sample desired conditional future statistics. The amount of past information stored in memory is quantified by the Shannon entropy of S. The minimal possible memory required, C_μ, is known as the statistical complexity and is an important measure of structure in complexity science [6, 7, 8, 9].

A quantum simulator can further reduce this memory by encoding relevant past information in non-orthogonal quantum states. In particular, we introduce methods to design quantum machines that generate future statistics using by sequential application of an appropriate unitary U with an sequence of blank ancilla (see Fig. 1). Each interaction corresponds to a time-step of the stochastic process, and entangles memory and tape. Measuring the ancilla after interaction then provides a sample of desired statistics at that time-step. This construction ensures that the memory advantage is maintained at all times during simulation. Moreover, if the tape is left unmeasured, it is automatically set to a quantum superposition of all possible conditional futures of the process.

Simulating Futures – Our experiment considers simulating a particular stochastic process known as the perturbed coin [1]. It consists of a binary random variable that represents the state of a possibly biased coin inside a box. At each time step, the box is perturbed, causing the coin to flip with some probability. The process is the defined by two parameters, l and m. l is the probability a coin in tails stays in tails. While m is similarly defined as

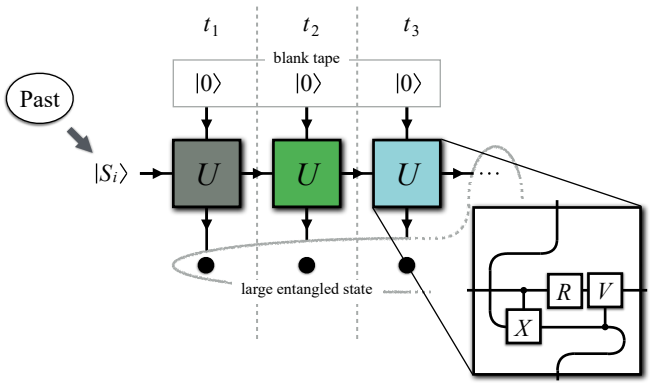


Figure 1: A unitary quantum simulator works by recording relevant past information about a process within some internal memory state. At each time step, the simulator interacts with the kth ancilla through the same unitary operator U. Measuring the ancilla samples the statistical distribution of the process, and at the same time the internal state of the simulator collapses into the correct memory state required for further simulation steps. If ancilla's are left unmeasured, the simulator instead generates a superposition of all possible conditional futures. In our experiment the simulates the perturbed coin, U has a specific gate sequence (as described by inset) while the quantum memory is a single qubit initialized in either $|S_0\rangle = \sqrt{l}|0\rangle + \sqrt{1-l}|1\rangle$ or $|S_1\rangle = \sqrt{1-m}|0\rangle + \sqrt{m}|1\rangle$, depending on initial state of the coin.

for when the coin is initially heads. The resulting state of the coin is then emitted as output. Repetition of this procedure generates a string of 0s and 1s, whose statistics define the perturbed coin process. The process has statistical complexity of $C_\mu = -q\log q - (1-q)\log(1-q)$, where q represents the proportion of time-steps the coin is in heads. The exact elementary gate decomposition for the associated U can be determined (see inset in Fig. 1).

We implement the memory system and multiple ancillas — here, corresponding to three time-steps — by encoding on a single photon. The ancillas, which can be read to obtain the classical outcomes of the process, are encoded in the arrival time of the photon, and the memory state of the simulator is encoded in its polarisation. Thus, for a simulation of M time steps, a 2^M-dimensional system corresponding to 2^M different photon arrival times replaces M distinct ancillary photons. Instead of measuring the classical outcome at each time step, our quantum information processor keeps the photon and builds up a superposition in a high-dimensional Hilbert space; in our case $M = 3$, and the output of the simulator is 16 dimensional (8 arrival time modes $\times$ 2 polarisation modes). The associated experimental setup is shown in Fig. 2. Here, one of the photons (the lower beam) is prepared in the appropriate initial a state ($|S_0\rangle$ or $|S_1\rangle$) depending on the past. It then passes through three sequential blocks, which represent the three time steps being simulated. In each block, the short and long paths correspond to outcomes 0 and 1,

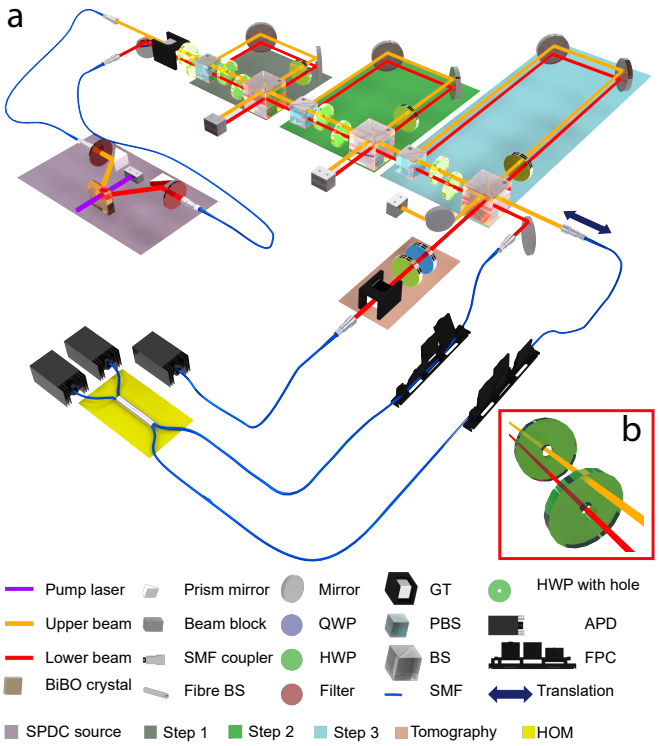


Figure 2: (**a**) Polarisation qubits from the two output beams of a spontaneous parametric down-conversion source are used as memory states for the simulation two separate and potentially different processes Π_1 (red) and Π_2. To implement the three-step simulation, three processor blocks are built (labelled Step 1, Step 2, and Step 3). In each step, path and arrival time modes are also employed to realise the relevant physical operation (see related publication [4]). The output of one of the simulators (lower beam) is used to perform the polarisation tomography for determining C_q. To measure the overlap of the future statistics of two processes, both photons are used, while the other outputs of the third beam splitter are interfered in a fibre BS (yellow box). (**b**) A close-up of two vertically-separated beams passing through two HWPs with holes, each of which only acts on one of the beams.

respectively. In this way, we obtain the probability distribution of the stochastic process as simulated by our quantum information processor, together with the final memory state of our simulator, which is needed for further simulation steps. Running this simulator, our statistical predictions agree with optimal predictions to a fidelity of at least 0.991 (detailed statistics in accompanying manuscript [4]).

The resulting memory cost C_q is shown in Fig. 3a, demonstrating that quantum processing can significant reduce the amount of past information needed for simulating a multi-step stochastic process. To guarantee that associated memory cost during this simulation does not increase, we require the internal dynamics to be close to (ideally, completely) unitary. We can verify via two-photon quantum interference. We use the complete setup

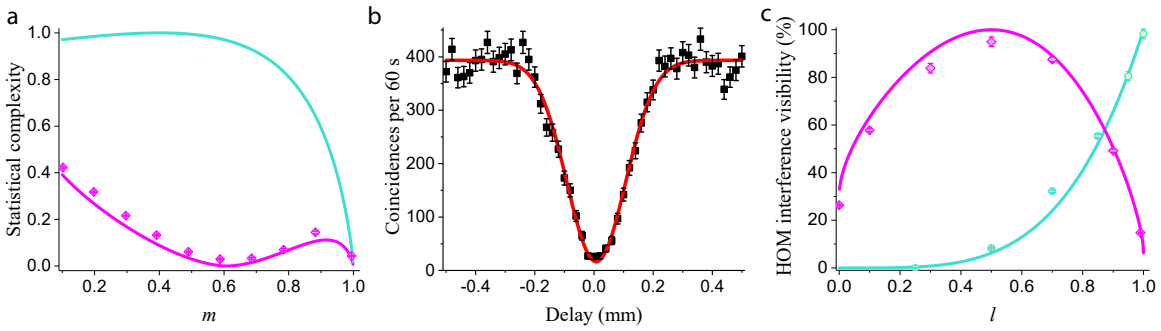


Figure 3: (**a**) The memory cost C_q of our quantum simulator as function of m, the probability the coin does not flip when in tails. The probability of remaining in heads l is fixed at 0.4. Experimental measurements of C_q (magenta dots) fit well with theory (magenta line), and is significantly lower than the classical limit C_μ (turquoise line). (**b**) Two-photon interference of a quantum simulator simulating two separate instances of the same stochastic process to verify that it maintains coherence. **c** Magenta and turquoise elements (points—experiment; curves—theory) show the comparison of the statistical futures from two different stochastic processes by two-photon interference visibility. In each case, one process (Π_1) is fixed, and the other process (Π_2) has fixed m but varying l, and both processes begun with the same past. Magenta represents interference of the output states of the simulators for Π_1 ($l = 0.5$, and $m = 0.5$) with Π_2 ($m = 0.5$, and l varying). Turquoise represents interference of the output states of the simulators for Π_1 ($l = 1.0$, and $m = 1.0$) with Π_2 ($m = 0.5$, and l varying). Uncertainties are so small that they are barely visible.

of Fig. 2, where the photon depicted by the orange path is now also goes through the apparatus. Both the photons pass independently through the three sequential blocks, with each experiencing nominally the same optical elements. If the coherence between the different time bins and polarisations exploited in our simulation is maintained, we expect a complete interference, or unit visibility. The result in Fig. 3b shows a visibility of 0.96 ± 0.02 for the case where the theoretical output states of the apparatus are uniform superpositions of all time bins and polarisations (which is the scenario where the highest discrepancy from the ideal visibility would be expected as it is most susceptible to imperfections). The high value obtained here indicates that our simulator is (almost) implementing a unitary operator, and the entropy of our system does not significantly increase throughout the simulation process.

Interfering Futures – Modifying this setup allows us to compare two different processes, Π_1 and Π_2. Clearly, one way to perform such a statistical comparison is to consider each process individually, and sample its outcomes to reconstruct the corresponding distribution. These two reconstructed distributions can then be compared. However, we notice that in our quantum simulation, all the information about the future statistics is already encoded in the state that exists in our apparatus. Thus, we do not need to collapse the superposition of possible outcomes by sampling, instead we can exploit this superposition for our task of comparing the future of processes. In particular, by simultaneously running quantum simulations of processes Π_1 and Π_2 in parallel and interfering the resulting output states, we can estimate the overlap of their future statistics.

In our experiment, we realise different processes by applying different operations to the two photons (red beam and orange beam) in the three blocks of the setup in Fig. 2. We fix one of the processes and change the other process gradually. As the parameters defining the processes become increasingly similar, the two output probability distributions overlap more. This is reflected in the experiment by a higher visibility value, showing how the comparison between two sets of future statistics can be evaluated via interference visibility. Results are shown in Fig. 3c, where the experimental values are close to theoretical predictions.

Discussion – Our multi-step photonic implementation of a stochastic simulation has verified the memory advantage available with quantum resources. We have demonstrated that it is possible to maintain this advantage at all stages of the simulation by preserving quantum coherence, as opposed to previous experiments [5, 10]. Furthermore, we showed that superpositions of statistical distributions of potential process futures can be interfered. Technologically, our results demonstrate yjay high- (here, 16-) dimensional quantum states can be encoded, manipulated in photonic temporal and polarisation modes with high fidelity [11, 12], and interfered with an extremely high visibility [13].

The time-bin encoding techniques in our experiment can be extended to other small or medium-scale simulations by expanding the number of time bins. For example, 10^8 time bin modes have been realized in the context of communication complexity [14]. However, the number of bins does not scale efficiently with the number of qubits, and thus very-large-scale simulations are not possible with this encoding. This is not a fundamental problem, as the concepts that we demonstrate can be equivalently implemented in any potential quantum processor. Meanwhile interfering future statistics has direct relation to other protocols, such as potential reduced communication complexity when comparing vectors quantum fingerprinting or image recognition [14, 15, 16].

References

[1] Gu, M., Wiesner, K., Rieper, E. & Vedral, V. Quantum mechanics can reduce the complexity of classical models. *Nat. Commun.* **3**, 762 (2012).

[2] Mahoney, J. R., Aghamohammadi, C. & Crutchfield, J. P. Occam's quantum strop: Synchronizing and compressing classical cryptic processes via a quantum channel. *Sci. Rep.* **6**, 20495 (2016).

[3] Binder, F. C., Thompson, J. & Gu, M. Practical unitary simulator for non-markovian complex processes. *Phys. Rev. Lett.* **120**, 240502 (2018).

[4] Ghafari, F., Tischler, N., Di Franco, C., Thompson, J. & Gu, M. Pryde, G. Interfering trajectories in experimental quantum-enhanced stochastic simulation. *Nat. Comms.* **10**, 1630 (2019).

[5] Palsson, M. S., Gu, M., Ho, J., Wiseman, H. M. & Pryde, G. J. Experimentally modeling stochastic processes with less memory by the use of a quantum processor. *Sci. Adv.* **3**, e1601302 (2017).

[6] Grassberger, P. Toward a quantitative theory of self-generated complexity. *Int. J. Theor. Phys.* **25**, 907–938 (1986).

[7] Crutchfield, J. P. & Young, K. Inferring statistical complexity. *Phys. Rev. Lett.* **63**, 105 (1989).

[8] Shalizi, C. R. & Crutchfield, J. P. Computational mechanics: Pattern and prediction, structure and simplicity. *J. Stat. Phys.* **104**, 817–879 (2001).

[9] Crutchfield, J. P., Ellison, C. J. & Mahoney, J. R. Time's barbed arrow: Irreversibility, crypticity, and stored information. *Phys. Rev. Lett.* **103**, 094101 (2009).

[10] Ghafari, F. *et al.* Observing the ambiguity of simplicity via quantum simulations of an ising spin chain. *Preprint at http://arxiv.org/abs/1711.03661* (2017).

[11] Franson, J. D. Bell inequality for position and time. *Phys. Rev. Lett.* **62**, 2205 (1989).

[12] Kwiat, P. G., Steinberg, A. M. & Chiao, R. Y. High-visibility interference in a Bell-inequality experiment for energy and time. *Phys. Rev. A* **47**, R2472 (1993).

[13] Zhang, Y. *et al.* Engineering two-photon high-dimensional states through quantum interference. *Sci. Adv.* **2**, e1501165 (2016).

[14] Xu, F. *et al.* Experimental quantum fingerprinting with weak coherent pulses. *Nat. Commun.* **6**, 8735 (2015).

[15] Kumar, N., Diamanti, E. & Kerenidis, I. Efficient quantum communications with coherent state fingerprints over multiple channels. *Phys. Rev. A* **95**, 032337 (2017).

[16] Shalev-Shwartz, S. & Ben-David, S. *Understanding machine learning: From theory to algorithms* (Cambridge University Press, 2014).

Open quantum systems are harder to track than open classical systems

Prahlad Warszawski[1] * Howard M. Wiseman[2] †

[1] *Centre of Excellence in Engineered Quantum Systems (Australian Research Council), School of Physics, The University of Sydney, Sydney, New South Wales 2006, Australia*
[2] *Centre for Quantum Computation and Communication Technology (Australian Research Council), Centre for Quantum Dynamics, Griffith University, Brisbane, Queensland 4111, Australia*

Abstract. For a Markovian open quantum system it is possible, by continuously monitoring the environment, to perfectly track the system (know its pure state) without altering the master equation. However, typically a positive-dimensional manifold of states in Hilbert space is explored, even for a finite D-dimensional system and, consequently, an infinite classical memory is required to track the state. Our paper concerns exceptional adaptive measurement schemes that result in the system stochastically jumping between a *finite* ensemble of states, K. We answer the long-standing open question of whether the minimum K is generically larger than D and thus establish that, indeed, open quantum systems are harder to track than open classical systems. See `arXiv:1905.10935.`

Keywords: Open quantum systems, quantum measurement, Schrödinger-HJW theorem, WV theorem

1 Introduction

Tracking an open quantum system requires measuring the environment to which the system is coupled. In this way, the experimentalist gains knowledge of the quantum trajectory [1] followed by the system of interest. For the case of perfect detector efficiency, no system information is lost into the environment and the system trajectory maps the path of a pure quantum state. It is of interest to ask, how much memory is required to track such a pure state trajectory? The answer is typically that an infinite memory is required, due to the fact that generic monitoring schemes will result in a continuous (or piece-wise continuous) quantum state trajectory that explores a non-zero dimensional manifold of pure states. Remarkably, this is not always the case: it has been shown [2–6] that, via the implementation of especially chosen system-dependent adaptive measurement schemes, quantum trajectories of some systems can be constrained to a finite number, K, of pure quantum states. This has profound consequences for the memory requirements of tracking an open quantum system, as a classical device with only K states (a 'finite state machine' [7]) is sufficient to follow the quantum evolution. In this paper, we will investigate the minimum ensemble size, $K_{\min}$, that is achievable, given complete freedom of measurement scheme. In particular, we compare and contrast $K_{\min}$ with the dimension, D, of the quantum system and so address some long-standing open questions of interest raised in Refs. [3, 4]. Note that an effectively classical system (which explores a finite ensemble of *orthogonal* pure states) will have $K_{\min} = D$.

The choice of monitoring of a generic open quantum system can have a profound effect upon its evolution. The system, by definition, is interacting with the environment and, for suitable initial conditions, becomes entangled with it. The measurement of the environment by an experimentalist effects 'quantum steering' [8] upon the system. In this paper we are concerned with the case of continuous Markovian dynamics induced by the bath, also known as quantum white noise (QWN) coupling; the system will then, *in the absence of measurement*, obey a Lindblad-form master equation (ME) for the density matrix [1]:

$$\dot{\rho} = \mathcal{L}\rho \equiv -i[\hat{H}_{\rm eff}\rho - \rho\hat{H}_{\rm eff}^\dagger] + \sum_{l=1}^{L} \hat{c}_l \rho \hat{c}_l^\dagger, \qquad (1)$$

where $\hat{H}_{\rm eff} \equiv \hat{H} - i\sum_l \hat{c}_l^\dagger \hat{c}_l/2$ and $\hat{H}$ is the Hermitian Hamiltonian.

The stochastic path followed by the state is known as a quantum trajectory, and different monitoring schemes will lead to different types of quantum trajectories [1, 9]. In fact, there are an infinite number of ways to measure the environment that maintains a pure quantum state for the system. Here, we are concerned with quantum jump trajectories, rather than diffusive trajectories, as the latter would rule out a finite ensemble of realised quantum states. However, in between the quantum jumps the experimentalist is continuously updating the system state in a non-trivial way, as the 'no-click' results also carry information, albeit an amount that scales with dt. This information affects the state even when it is a state of maximal information (i.e. pure), unlike the classical case, leading to smooth but non-unitary evolution between jumps. Thus, it is clear that the system generically explores a continuum of states in Hilbert space.

Whilst a non-zero dimensional manifold of states is therefore typically associated with continuous measurement, the Schrödinger-Hughston-Jozsa-Wootters (S-HJW) theorem [10–12], by contrast, gives physical meaning to any pure state ensemble representing a mixed state matrix (also called a density matrix) ρ. In particular, for finite $D = \mathrm{rank}(\rho)$, one may consider ensembles,

$$\rho = \sum_{k=1}^{K} \wp_k \left|\phi_k\right\rangle \left\langle\phi_k\right|, \qquad (2)$$

for any choice of K, provided that $D \leq K < \infty$. The S-HJW theorem states that if there exists physically a

*`prahladw@gmail.com`
†`h.wiseman@griffith.edu.au`

purification, in a higher dimensional Hilbert space, of a system in a mixed state ρ, then for any ensemble that represents ρ, there is a way to measure the environment(s) — that is, make measurements in the larger Hilbert space that act as the identity on the system Hilbert space — such as to collapse the system into one of the pure states $|\phi_k\rangle$ with the appropriate probability $\wp_k$. Note that in general these states are not mutually orthogonal, even for $K = D$, and this must be so for $K > D$.

The S-HJW theorem applies to a measurement on the environment at a particular time. If this is a time remote from the initial conditions, and the system obeys Eq. (1) with a unique stationary solution $\rho_{\rm ss}$ of rank D [13], then in Eq. (2), $\rho = \rho_{\rm ss}$. An obvious question is: can the finite ensembles representing $\rho_{\rm ss}$ allowed by the S-HJW theorem also pertain, at remote times, to continuous monitoring? To address this we make the additional assumption, mentioned above, that the ME has been derived from a QWN coupling. Then we can ask whether a given pure state ensemble can be realised continuously by the experimentalist via a carefully chosen measurement scheme. That is, is it possible, merely by obtaining information from the bath in the right way, to force a quantum system, obeying a given ME, to behave like a discrete classical system, in the sense of jumping between a given finite set of pure states? A theorem by Wiseman and Vaccaro [2] says that this question is equivalent to asking whether the following finite set of algebraic constraints can be satisfied

$$\forall k,\ \mathcal{L}\left|\phi_k\right\rangle\left\langle\phi_k\right| = \sum_{j=1}^{K} \kappa_{jk}\left(\left|\phi_j\right\rangle\left\langle\phi_j\right| - \left|\phi_k\right\rangle\left\langle\phi_k\right|\right) \qquad (3)$$

for some ensemble $\{(\wp_k,\, |\phi_k\rangle) : k\}$ of size K. The real-valued transition rates, $\kappa_{jk} \geq 0$, naturally determine the occupation probabilities $\wp_k$. A valid solution is known as a *physically realisable ensemble* (PRE) [2], because there exists some measurement procedure that will realize the ensemble in the sense described above, even if that procedure may by difficult to implement in practice. In particular, it is known that the measurement scheme required to achieve a PRE is generally adaptive in nature [3].

Most of the difficulty of our research program arises due to the system of non-linear constraints defined by Eq. (3) being difficult to solve, even numerically, when $D > 2$. The difficulty of this task becomes exponentially larger as the number of equations and variables increases. In fact, the problem is known to fall into the NP-complete complexity class [14]. This alone does not prohibit the constraints' solution; it just places low practical bounds on the system size that can be solved. Two major tools are used in order to aid our computational efforts to solve Eq. (3). The first is that of symmetry, as was recently introduced by the authors [6]. Secondly, we newly apply two powerful software packages (MAGMA [15] and PHCpack [16]) to PREs that respectively take advantage of Gröbner basis [17] and polynomial homotopy continuation [18] techniques.

It was shown in Ref. [2] that there are ensembles that represent $\rho_{\rm ss}$ but that are not PREs (this was referred to as the "preferred ensemble fact"). A fundamental question for open quantum systems is whether, for a given master equation, there exist *any* finite PREs. It was found in Ref. [3] that for $D = 2$ it always possible to find at least one $K = 2$ PRE. For $D > 2$, a heuristic argument, using free parameter and constraint counting, was made in Ref. [3] predicting that one can expect a PRE to exist if $K \geq (D-1)^2 + 1$. This separation from the classical case (where $K = D$ is necessary and sufficient) for $D > 2$ would indicate a profound difference between quantum and classical open systems. However, the heuristic argument of Ref. [3] was not tested against numerical evidence, and both the quantum–classical gap, and the very existence of finite quantum ensembles in general, remained conjectural. The question of whether ME symmetries can alter our expectations regarding the minimal size of PREs was treated in [6]. There it was found that a commonly employed invariant subspace symmetry can reduce the heuristic ensemble size to $K \geq \frac{1}{2}\left(D^2 - D + 2\right)$, which is still larger than D for $D > 2$. Here, we will further refine the heuristic arguments in order to take account of the number of decoherence channels, that is the number of Lindblad operators in Eq. (1).

In this paper we address the three most important open questions raised by Ref. [3]. We answer the first two definitively, and provide strong numerical evidence to support our conjectures regarding the third. The first question (Q1) is: *are there MEs for which the minimally sized PRE is larger than D?* The second question (Q2) is as follows: *is an ensemble size of $K = (D-1)^2+1$ always sufficient for a PRE to be found?* The third question (Q3) is: *does this refined form of the argument in Ref. [3] reliably predict whether PREs are feasible for a ME of a given form?*

2 Results

Our first result, being a refined heuristic for the existence of PREs taking into account L, will guide us when answering the proposed research questions. As mentioned, a heuristic is obtained by the counting of free parameters (describing the system state and the transition rates between them) and constraints (provided by Eq. (3)). By considering the dimension of the post-detection Hilbert space, which is constrained by L and D, it is possible to rule various graphs out as possibly representing PREs. Transcribing this to an algebraic constraint on the number of transition rates leads to

$$K_{\rm min} = (D-1)^2 + 1 + \mathbf{1}_{\{L<D-1\}} \times (2D - 2L - 1)\,, \quad (4)$$

where $\mathbf{1}_{\{A\}}$ is the indicator function, which is 1 if A is true and 0 otherwise. That is, if $L \geq D-1$ then we reproduce the minimum ensemble size suggested in Ref. [3]. But if $L < D-1$, the minimum ensemble size is larger by $2D - 2L - 1$, making it equal to $K_{\rm min} = D^2 - 2L + 1$. For all values of L, $K_{\rm min} \sim D^2$ and in the 'worst' case, of $L = 1$, we find $K_{\rm min} = D^2 - 1$ (for $D > 2$).

2.1 Q1: Are open quantum systems harder to track than open classical systems? (Yes)

In order to answer this central question in the affirmative, it needs to be proven that there exists a ME such that $K = D$ states are not sufficient for a PRE to be formed (Q1). This is because a classical system can always be tracked with $K = D$ states as the occupation (1 or 0) of each state could, in principle, always be known by monitoring the environment. It is also of interest to look for a generic difference in difficulty of tracking quantum and classical systems. That is, we ask whether $K = D$ is insufficient *in general*, for randomly drawn MEs. The computational algebraic technique we use is to obtain Hilbert Nullstellensatz certificates of infeasibility for examples of the polynomial system defining PREs. Specifically, our heuristic (Eq. (4)) suggests that the simplest case to look at is $D = K = 3$. By randomly generating some $D = 3$ MEs, we were able to obtain the necessary certificates and thus rule out $K = 3$ PREs for those MEs. Consequently, we have provided very strong evidence that generically open quantum systems harder to track than open classical systems.

2.2 Q2: is an ensemble size of $K = (D-1)^2 + 1$ always sufficient for a PRE to be found, as suggested in Ref. [3]? (No)

The heuristic of Eq. (4) suggests that when $L < D - 1$ more than $(D-1)^2 + 1$ PRE members are required. To *prove* this requires obtaining Hilbert Nullstellensatz for the relevant polynomial systems. The easiest case to tackle is $D = 3$, $L = 1$, for which Eq. (4) indicates $K_{\min} = 8$. The computational difficulty proved too great for $K = 6, 7$, but we were able to obtain Nullstellensätze for $K = 5$ ensembles for randomly generated MEs. Given that $(D-1)^2 + 1 = 5$ for $D = 3$, we have thus shown that $(D-1)^2 + 1$ ensemble members is not generically sufficient for a PRE to be found.

2.3 Q3: does our refined heuristic (Eq. (4)) reliably predict whether PREs are feasible for a ME of a given form? (Yes)

Q1 and Q2 were answerable via Nullstellensatz, however, Q3 requires actually finding some PREs. The completely generic case was too computationally difficult, so ME symmetries were introduced in order to reduce the number of constraints and parameters. The symmetry consequently changes the relationship between constraints and parameters and leads to the introduction of a new, but similar, heuristic. We take evidence supporting the new heuristic as also being evidence for the original heuristic, due to their similar derivation and nature. Our examination consisted of randomly drawing 240 symmetric $D = 3$ MEs spread over $L = 1, 2, 3$. The symmetry utilized was that real-valued density matrices stayed as real-valued under the ME evolution. The modified heuristic predicts that PREs are feasible for $K = 4$ when $L > 1$. By utilising the techniques of polynomial homotopy continuation [16, 19], $K = 4$ PREs were found for some of the $L = 3$ MEs, as predicted by the heuristic. $L = 2$ PREs were found once further symmetry was introduced, also consistent with our heuristic.

3 Discussion

In this paper, we have answered a number of open questions concerning PREs. Most importantly, we now state that open quantum systems are harder to track than open classical systems. That is, despite complete freedom given to the experimentalist, $D > 2$ quantum systems generically cannot form PREs with D members. Furthermore, for small L, the minimally sized ensemble is generically larger than that for larger L. Our investigations were guided by the formation of a new heuristic (modifying a previously existing one that did not consider L) describing when the existence of a PRE was feasible. All obtained results were consistent with this heuristic, giving us confidence in its most interesting feature: $K_{\min} \sim D^2$, implying a quadratic gap between the classical and quantum tracking problems.

It is perhaps appropriate to conclude with a different perspective on the significance of there being a gap between D and $K_{\min}$. This gap makes open quantum systems harder to track than open classical systems, as per our title, but also suggests that there is a resource associated with an open quantum system. Specifically, despite only having D internal states, we have shown that generically, for $D > 2$, a PRE can represent a finite classical hidden Markov model having $K > D$ states and therefore provide can a compression relative to the classical implementation [20]. It seems likely that this compression could be arbitrarily large as increasing K leads to a larger ratio of parameters to constraints. Similarly, for a stochastic process with a fixed number of states that can be mapped to a PRE, a lower internal entropy implementation is possible as the PRE is comprised, in general, of non-orthogonal states [21]. The relation between these complementary perspectives on open quantum systems is surely a fruitful topic for future research.

References

[1] H. M. Wiseman and G. J. Milburn. *Quantum measurement and control*. Cambridge University Press, 2010.

[2] H. M. Wiseman and J. A. Vaccaro. Inequivalence of pure state ensembles for open quantum systems: the preferred ensembles are those that are physically realizable. *Phys. Rev. Lett.*, 87(24):240402, 2001.

[3] R. I. Karasik and H. M. Wiseman. How many bits does it take to track an open quantum system? *Phys. Rev. Lett.*, 106(2):020406, 2011.

[4] R. I. Karasik and H. M. Wiseman. Tracking an open quantum system using a finite state machine: stability analysis. *Phys. Rev. A*, 84(5):052120, 2011.

[5] S. Daryanoosh, H. M. Wiseman, and T. Brandes. Stochastic feedback control of quantum transport to

realize a dynamical ensemble of two nonorthogonal pure states. *Phys. Rev. B*, 93(8):085127, 2016.

[6] P. Warszawski and H. M. Wiseman. Symmetries and physically realizable ensembles for open quantum systems. *New J. Phys.*, 21:053006, 2019.

[7] Arthur Gill et al. Introduction to the theory of finite-state machines. 1962.

[8] E. Schrödinger. Discussion of probability relations between separated systems. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 31, pages 555–563. Cambridge University Press, 1935.

[9] H. Carmichael. *An open systems approach to quantum optics: lectures presented at the Université Libre de Bruxelles, October 28 to November 4, 1991*, volume 18. Springer Science & Business Media, 2009.

[10] E. Schrödinger. Probability relations between separated systems. *Proc. Camb. Phil. Soc.*, 32:446, 1936.

[11] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Phys. Lett. A*, 183(1):14–18, 1993.

[12] K. A. Kirkpatrick. The Schrödinger-HJW theorem. *Found. Phys. Lett.*, 19(1):95, 2006.

[13] In the case that the rank of $\rho_{\rm ss}$ is less than D, then we can project the Lindblad ME onto a smaller dimensional subspace and redefine that as D.

[14] N. Courtois, A. Klimov, J. Patarin, and A. Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Advances in CryptologyEUROCRYPT 2000*, pages 392–407. Springer, 2000.

[15] W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system i: The user language. *J. Symb. Comput.*, 24(3):235–265, 1997.

[16] J. Verschelde. Algorithm 795: Phcpack: A general-purpose solver for polynomial systems by homotopy continuation. *ACM Transactions on Mathematical Software (TOMS)*, 25(2):251–276, 1999.

[17] D. A. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185. Springer Science & Business Media, 2006.

[18] T. Li. Numerical solution of multivariate polynomial systems by homotopy continuation methods. *Acta numerica*, 6:399–436, 1997.

[19] C. Hill, K. Lee, A. Leykin, T. Duff, A. Jensen, and J. Sommars. Solving polynomial systems via homotopy continuation and monodromy. *IMA J. Numer. Anal.*, 04 2018.

[20] A. Monras, A. Beige, and K. Wiesner. Hidden quantum Markov models and non-adaptive read-out of many-body states. *Appl. Math. and Comp. Sciences*, 3:93, 2011.

[21] M. Gu, K. Wiesner, E. Rieper, and V. Vedral. Quantum mechanics can reduce the complexity of classical models. *Nat. Commun.*, 3, Mar 2012.

Randomness expansion certified by quantum contextuality in a trapped ion system

Mark Um[1] * Qi Zhao[1] Junhua Zhang[2] Pengfei Wang[1] Ye Wang[3] Mu Qiao[1]
Hongyi Zhou[1] Xiongfeng Ma[1] † Kihwan Kim[1] ‡

[1] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, P. R. China*
[2] *Shenzhen Institute for Quantum Science and Engineering, and Department of Physics, Southern University of Science and Technology, Shenzhen 518055, P. R. China*
[3] *Department of Electrical and Computer Engineering, Duke University, Durham, NC 27708, USA*

Abstract. The randomness can be certified by observing the violation of quantum contextuality inequalities based on the Kochen-Specker theorem. In a single quantum system, one can test contextuality which significantly simplifies the experimental requirements to observe the violation comparing to the ones based on nonlocality tests. However, it is not yet resolved how to ensure compatibilities for sequential measurements that is required in contextuality tests. Here, we employ a modified Klyachko-Can-Binicioğlu-Shumovsky contextuality inequality, which can ease the strict compatibility requirement on measurements. On a trapped single $^{138}Ba^{+}$ ion system, we experimentally realize self-testing protocol of quantum random number expansion by observing violation of the contextuality inequality without the detection loopholes. We perform 1.29×10^8 trials of experiments and extract the randomness of 8.06×10^5 bits with a speed of 270 bits s^{-1}. Our demonstration paves the way for the practical high-speed spot-checking quantum random number expansion and other secure information processing applications.

Keywords: randomness expansion, quantum contextuality, self-testing, ion trap

1 Randomness expansion protocol certified by the KCBS inequality

In this work [1], in order to test contextuality, we employ the Klyachko-Can-Binicioğlu-Shumovsky (KCBS) inequality which uses five observables A_i taken ± 1 and shows that there is no hidden variables models in the smallest dimension $d = 3$. Based on the original KCBS inequality

$$\langle A_1A_2\rangle+\langle A_3A_2\rangle+\langle A_3A_4\rangle+\langle A_5A_4\rangle+\langle A_5A_1\rangle \geq -3, \quad (1)$$

where the five observables $A_1, A_2, \ldots, A_5$ are the projectors on the axes respectively. The maximal violation of the inequality (1) is achieved when five state vectors $\{|v_i\rangle\}$ form a regular pentagram as shown in Fig. 1(a). The connected axes $|v_i\rangle$ and $|v_{i+1}\rangle$ are orthogonal, representing compatibility of the corresponding observables A_i and A_{i+1}. $\langle A_iA_j\rangle$ denotes the expectation value of the observables in the time order of A_iA_j for the sequential measurements.

we use modified inequality [2, 3] to reveal quantum correlations without the requirement of the perfect compatibility on sequential measurements, all the imperfections in control and the disturbances from classical and quantum noise are characterized and compensated.

$$\begin{aligned}\langle\chi_{KCBS}\rangle = \langle A_1A_2\rangle + \langle A_3A_2\rangle + \langle A_3A_4\rangle \\ + \langle A_5A_4\rangle + \langle A_5A_1\rangle - \langle A_1A_1\rangle \geq -4 \\ -(\epsilon_{12} + \epsilon_{32} + \epsilon_{34} + \epsilon_{54} + \epsilon_{51} + \epsilon_{11}),\end{aligned} \quad (2)$$

where ϵ_{ij} describes the incompatibility between a same pair of observables A_i and A_j in different time orders, A_iA_j and A_jA_i:

$$\epsilon_{ij} = |\langle A_j|A_jA_i\rangle - \langle A_j|A_iA_j\rangle|. \quad (3)$$

We employ a spot-checking protocol [4] to achieve the first experimental demonstration of the strict randomness expansion with exponential gain. In this scenario, we can expand the randomness from the generated strings merely based on the experimental observed data that violate the modified KCBS inequality in a self-testing manner. According to the definition of Ref. [4], the score of the KCBS game is given by $g \in \{0, 1\}$. Thus, Eq. (2) can be rewritten in the form KCBS game G,

$$\begin{aligned}g_{KCBS} = -\frac{1}{6}(\langle A_1A_2\rangle + \langle A_3A_2\rangle + \langle A_3A_4\rangle + \langle A_5A_4\rangle \\ + \langle A_5A_1\rangle - \langle A_1A_1\rangle + \epsilon_{12} + \epsilon_{32} + \epsilon_{34} \\ +\epsilon_{54} + \epsilon_{51} + \epsilon_{11}).\end{aligned} \quad (4)$$

The classical winning probability is $\chi_g = 2/3$ while maximal quantum winning probability is $\chi'_g = (4\sqrt{5} - 4)/6 \approx 0.824$. The gap between χ_g and χ'_g enables randomness expansion. Our randomness expansion protocol is listed as follows:

- Choose a bit $t \in \{0, 1\}$ according to the Binomial distribution $(1 - q, q)$.
- If $t = 1$ ("game round"), the game G is played with our device and the output is recorded. Outputs of game rounds are additionally collected for checking.
- If $t = 0$ ("generation round"), $\{1, 2\}$ is given to our device and the output is recorded.

*ummark@gmail.com
†xma@tsinghua.edu.cn
‡kimkihwan@mail.tsinghua.edu.cn

- Steps 1-3 are repeated N times.
- Calculate the score g_{KCBS} from all game round outputs. If $g_{KCBS} < \chi_g$, then abort. Otherwise, move to to randomness extraction.

We note that we do not require the perfect compatibility. Instead, we assume approximate compatibility, which can be quantified by the terms of ϵ_{ij} and $\langle A_1 A_1 \rangle$ in (2). Due to those terms, the violation of the inequality of (2) is getting difficult if two sequential measurements are deviated from the perfect compatibility. However, in our scheme, two measurements in a context are performed on a single system, which makes it impossible to exclude the possibility that a malicious manufacturer sabotage the compatibility assumption by registering the setting and results of the first measurements and using them for the second measurements. Therefore, our protocol can not be viewed as a fully-device independent scenario. We need the trust of the device that the measurement settings are close enough to be compatible, but it is fine to have imperfections in the realization and disturbance from classical or quantum noisy environments since the amount of introduced incompatibilities are quantified. Our protocol is well fitted to a scenario of trusted but error-susceptible devices. Given these assumptions, the generated randomness is certified by only experimental statistics.

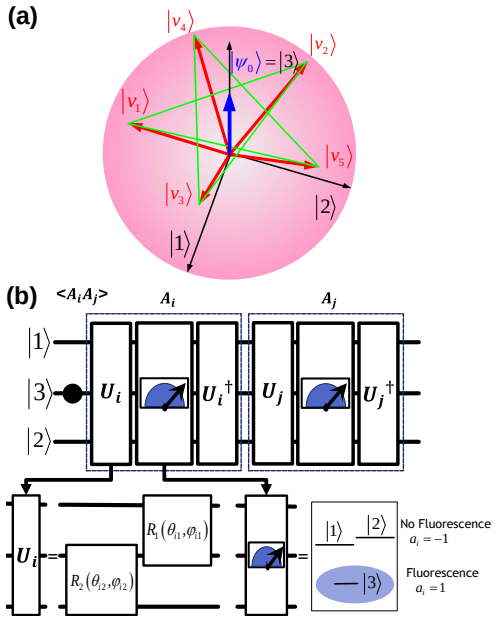


Figure 1: KCBS pentagram and experimental procedure. (a) Initial state and five axes which form a pentagram in d=3 space. (b) We first prepare initial $|3\rangle$ state, then perform two sequential measurements of A_i and A_j.

2 Experimental realization

Although the experimental violations of the KCBS inequality has been demonstrated using a single trapped $^{171}Yb^+$ ion [5], it is not possible to test the modified KCBS inequality (2) since when we observe fluorescence in the first measurement, the state is ruined and the second measurement is meaningless. In this work [1], we develop a single $^{138}Ba^+$ ion system to obtain full-correlation results from the sequential measurements. Our protocol fully closes detection loophole realizing in a qutrit system of the $^{138}Ba^+$ ion by taking advantage of its long-lived $^5D_{5/2}$ states that can be used for the coherent shelving of a quantum state during the sequential measurements. The basic operations are based on quadrupole transitions between $^6S_{1/2}$ and $^5D_{5/2}$ are coherently manipulated by a narrow-line laser with the wavelength of 1762 nm, which is stabilized to a high-finesse optical cavity. Fig. 2(a) shows the qutrit configuration in a $^{138}Ba^+$ ion.

Fig. 1(b) shows our sequential measurement configuration. Each sequential measurement contains a unitary rotation U_i, projective measurement, and an inverse unitary rotation $U_i^\dagger$. Each unitary rotation U_i is comprised of first $R_2(\theta_{2i}, \phi_{2i})$ then $R_1(\theta_{1i}, \phi_{1i})$. In projective measurement, we assign $a_i = 1(-1)$ if flourescence is (not) detected. At each game round, one of 11 measurement configurations $\{\{1,2\},\{2,1\},\{2,3\},\{3,2\},\{3,4\},\{4,3\},\{4,5\},\{5,4\},\{5,1\},\{1,5\},\{1,1\}\}$ is randomly selected. Note that each observable is included in at least two different contexts, when Alice and Bob receive i and j, they could not know the setting of the other. Pulse sequences of two measurements are independently generated by their own Direct Digital Synthesizer (DDS) and amplifiers, sent to the acousto-optic modulator (AOM) through independent paths, and finally applied to the ion on different time order. The experimental setup is shown in fig. 2(b).

3 Experimental results

We perform 1.29×10^8 trials of experiments and extract the randomness of 8.06×10^5 bits with the speed of 270 bits s^{-1}. The detailed experimental results of the measurements are summarized in Table 1. Our test probability is $q_{exp} = 10^{-4} \sim O((\log^3 N_{exp})/N_{exp})$, and the required amount of initial random seed is $O(\log^4 N_{exp})$ bits. The min-entropy of final randomness is 5.3×10^{-3} per bit, thus the output random bits is $\Theta(N_{exp})$, achieving exponential randomness expansion. All the experimental data is optimized by calculation based on test data shown in fig. 3. In real number, we get 6.88×10^5 bits of min-entropy which exceeds 2.35×10^5 bits of input randomness, resulting 4.52×10^5 net random bits, expansion rate per round is 3.5×10^{-3}.

References

[1] Mark Um, Qi Zhao, Junhua Zhang, Pengfei Wang, Ye Wang, Mu Qiao, Hongyi Zhou, Xiongfeng Ma, and Kihwan Kim Randomness expansion secured by quantum contextuality. *arXiv preprint arXiv:1902.00244v1*, 2019.

[2] Otfried Gühne, Matthias Kleinmann, Adan Cabello, Jan Åke Larsson, Gerhard Kirchmair, Florian Zähringer, Rene Gerritsma, and Christian F.

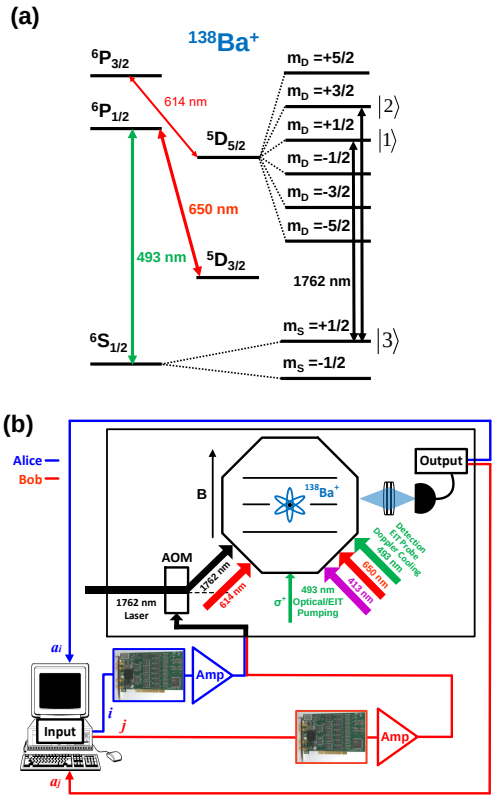


Figure 2: Experimental setup of the $^{138}Ba^{+}$ ion system. (a) The energy level diagram of a $^{138}Ba^{+}$ ion for a qutrit system, which is represented by two Zeeman sublevels $|m_D = +1/2\rangle \equiv |1\rangle$, $|m_D = +3/2\rangle \equiv |2\rangle$ in the $^5D_{5/2}$ manifold, and $|m_S = +1/2\rangle \equiv |3\rangle$ sublevel in the $^6S_{1/2}$ manifold. The 493 nm and 650 nm lasers are used for Doppler cooling, EIT cooling, optical pumping and detection. The 614 nm laser is used for depopulation of $^5D_{5/2}$ level to $^6S_{1/2}$ level. (b) The experimental setup of a trapped $^{138}Ba^{+}$ ion for testing KCBS inequality and for the spot checking random number expansion.

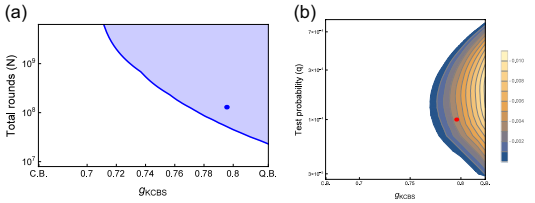


Figure 3: The relation of the score of KCBS game g_{KCBS}, number of total rounds N, test probability q, and randomness expansion rate with smoothing parameter $\delta = 10^{-2}$. (a) The minimum number of rounds to have net randomness depending on the score g_{KCBS}. The minimum N decreases as g_{KCBS} increases. We can get net randomness only within the shadow area. Our experimental $g_{KCBS} = 0.795$ and $N_{exp} = 1.29 \times 10^8$ are shown as the green circle. (b) Randomness expansion rate at different g_{KCBS} and q for our N_{exp}. Only with the combination of large enough g_{KCBS} and proper q can we obtain net randomness.

Table 1: Experimental results for different observables and compatibility terms for the KCBS inequality (2). Total game rounds are 1.2×10^4. The standard deviations of the final result are 0.015 and 0.023 for the single observables and correlations, respectively, 10^{-3} order for the compatibility terms, all as shown in the parenthesis. The standard deviation for the violation σ is 0.068 and our experimental data shows the violation of the extended inequality (2) with 11 σ.

$\{i,j\}$	$\langle A_i A_j \rangle$	$\langle A_i \rangle$	$\langle A_j \rangle$	ϵ_{ij}
{1,2}	**-0.768(23)**	0.082(15)	0.091(15)	**0.005(2)**
{2, 1}	-0.783(23)	0.096(15)	0.065(15)	0.017(4)
{2, 3}	-0.767(22)	0.098(14)	0.088(14)	0.033(5)
{3,2}	**-0.750(23)**	0.107(15)	0.098(15)	**0.009(3)**
{3,4}	**-0.773(23)**	0.084(15)	0.082(15)	**0.019(4)**
{4, 3}	-0.762(22)	0.122(14)	0.068(14)	0.000(0)
{4, 5}	-0.782(23)	0.095(15)	0.075(15)	0.014(3)
{5,4}	**-0.789(22)**	0.056(15)	0.094(15)	**0.025(4)**
{5,1}	**-0.773(22)**	0.100(14)	0.069(14)	**0.000(0)**
{1, 5}	-0.767(23)	0.109(15)	0.066(15)	0.007(2)
{1,1}	**0.977(21)**	0.106(15)	0.108(15)	**0.001(1)**
$g_{KCBS} = 4.772(68)/6 = 0.795(11)$				

Roos. Compatibility and noncontextuality for sequential measurements. *Phys. Rev. A.*, 81:022121, 2010.

[3] Jochen Szangolies, Matthias Kleinmann, and Otfried Gühne. Tests against noncontextual models with measurement disturbances. *Phys. Rev. A.*, 87:050101, 2013.

[4] Carl A. Miller and Yaoyun Shi. Universal security for randomness expansion from the spot-checking protocol. *Siam J. Comput.*, 46(4):1304–1335, 2017.

[5] Mark Um, Xiang Zhang, Junhua Zhang, Ye Wang, Shen Yangchao, D.-L. Deng, Lu-Ming Duan, and Kihwan Kim. Experimental certification of random numbers via quantum contextuality. *Sci. Rep.*, 3:1627, 2013.

Robust self-testing of quantum systems via non-contextuality inequalities

Kishor Bharti[1] * Maharshi Ray[1] † Antonios Varvitsiotis[2] ‡ Naqueeb Ahmad Warsi [1] §
Adán Cabello[3] ¶ Leong-Chuan Kwek[1 4 5 6] ‖

[1] *Centre for Quantum Technologies, National University of Singapore*
[2] *Department of Electrical and Computer Engineering, National University of Singapore*
[3] *Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*
[4] *MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, Singapore UMI 3654, Singapore*
[5] *Institute of Advanced Studies, Nanyang Technological University, Singapore 639673, Singapore*
[6] *National Institute of Education, Nanyang Technological University, Singapore 637616, Singapore*

Abstract. Characterising unknown quantum states and measurements is a fundamental problem in quantum information processing. In this manuscript, we provide a novel scheme to self-test local quantum systems using non-contextuality inequalities. Our work leverages the graph-theoretic framework for contextuality introduced by Cabello, Severini, and Winter, combined with tools from mathematical optimisation that guarantee the unicity of optimal solutions. As an application, we show that the celebrated Klyachko-Can-Binicioğlu-Shumovsky inequality and its generalisation to contextuality scenarios with odd n-cycle compatibility relations admit robust self-testing.

Keywords: Self-Testing, Contextuality, KCBS Inequality, Bell Nonlocality

1 Introduction

The deployment and analysis of mathematical models have been a crucial tool to advance our scientific understanding of the physical world. Nevertheless, complex mathematical models often admit a multitude of possible solutions, a phenomenon that can lead to ambiguity and erroneous predictions when the solution of the model is used to study some real-life problem. Models with no uniquely-identifiable solutions manifest themselves across most fields of science and mathematics, typical examples being the nonuniqueness of solutions to partial differential equations and the existence of multiple Nash equilibria in non-coopearative games. More pertinent to this work, the uniqueness of the ground state of a Hamiltonian is a problem with important engineering applications. Indeed, quantum annealing crucially relies on the uniqueness of the ground state of the underlying Hamiltonian, which is used to encode the solution of an optimization problem. From a practical standpoint, the noisy nature of the collected data governing the model selection process, suggests we should employ "robust" models, i.e., models that have a unique solution that is moreover stable under perturbations of the input data. Notwithstanding the ubiquitousness and importance of problems related to the unicity and robustness of the solutions of a given model, there is no general framework allowing to address these questions in a unified manner.

One of the most extensively used modeling tools in science and engineering is mathematical optimization. In this setting, the model is specified by a family of decision variables that satisfy certain feasibility constraints. The goal is then to find the value of the decision variables that maximizes an appropriate measure of performance. Undoubtedly, the most important optimization model is linear programming, where the decision variables are scalar variables subject to affine constraints. An equally important optimization model is semidefinite programming (SDP), constituting a wide generalization of linear programming with extensive modeling power and efficient algorithms for solving them. Unlike linear programs, the decision variables in a SDP are vectors, and the constraints are defined in terms of the inner products of the vectors. SDPs have many important applications in physics, e.g. in quantum foundations (Bell nonlocality, contextuality, steering) [10, 1, 2], quantum information theory (entanglement witnesses, tomography, quantum state discrimination) [3, 4, 5], quantum cryptography [7], and quantum complexity [8], just to mention a few. Most importantly, the aspect of SDPs that is crucial to this work is that they offer a general framework for studying uniqueness and robustness of model solutions.

In this manuscript, we employ the paradigm of identifiable robust models to characterize untrusted devices via contextuality. Contextuality refers to the impossibility of reproducing a set of probability distributions, each of them for a context (defined as a set of compatible and mutually nondisturbing observables), that share some marginal probabilities with a joint probability distribution in a single probability space. Quantum theory is an example of a contextual theory [6]. In this work we appropriately extend the paradigm of Bell self-testing to the framework of contextuality. In terms of techniques, our work leverages the well-known link between contextuality and semidefinite programming identified in the seminal work by Cabello, Severini, and Winter [1], combined with some less-known results concerning the unic-

*e0016779@u.nus.edu
†maharshi91@gmail.com
‡avarvits@gmail.com
§warsi.naqueeb@gmail.com
¶adan@us.es
‖cqtklc@gmail.com

ity and robustness of optimal solutions to semidefinite programs. Roughly speaking, we show that the nearness-of-optimality of the CSW semidefinite program bounds the distance in the SDP-solution space, which in turn translates into a bound on the distance from the ideal quantum realization. We believe that the tools employed in this paper will have value outside of the domain of contextuality, e.g., see [9] for a recent application in Bell nonlocality. Our results render new insights into the foundations of quantum contextuality and a proof-of-principle approach to characterize the underlying quantum states and measurements manifesting quantum contextuality via experimental statistics. We provide an innovative scheme to attest robust self-testing for any noncontextuality inequality and present a concrete illustration for the case of the generalized KCBS inequality, which is defined for any odd number of measurement events $n \geq 5$.

2 Background and Results (Informal)

We proceed to provide the non-technical version of our important results and the necessary background. The technical version of the same can be accessed via the arXiv link `https://arxiv.org/abs/1812.07265`. The contextual nature of a theory can be attested via the violation of certain linear inequalities, referred to as non-contextuality inequalities. The maximum quantum value of the linear expression for a non-contextuality inequality can be calculated using semidefinite programming. A semidefinite program (SDP) corresponds to optimizing a linear function over the cone of positive semidefinite matrices (of certain fixed size) intersected with an affine space. SDPs constitute one of the most important models of mathematical optimization due to their modeling power and the existence of efficient algorithms for solving them.

The relevance of SDPs to the study of contextuality is found in the works of Cabello, Severini and Winter, where the authors related contextuality with graph theory [1]. It was shown that the classical and quantum bounds on a non-contextuality inequality can be given by specific graph theoretic numbers. Moreover, it was shown that the quantum value of a non-contextuality inequality is given by a SDP. Concretely, the maximum quantum value is equal to

$$\begin{aligned} \max \ & \sum_{i=1}^{N} X_{ii} \\ \text{s.t. } & X_{ii} = X_{0i}, \ \forall i \in [N], \\ & X_{ij} = 0, \ i,j \in E, \\ & X_{00} = 1, \ X \in \mathcal{S}_+^{1+N}, \end{aligned} \tag{1}$$

which is a SDP known as the Lovász theta number of the graph $G = (V, E)$. Here $\mathcal{S}_+^{1+N}$ is a positive semidefinite matrix with $N+1$ rows (columns) and $[N] = \{1, 2, \cdots N\}$. The matrix X is referred to as a "Gram matrix" and can be used to get back the measurement settings (quantum projectors) and the quantum state leading to the quantum value.

Based on the tools provided in our technical manuscript (`https://arxiv.org/abs/1812.07265`), it can be established that "Given a non-contextuality inequality with the maximum quantum value B_q, if an experimental arrangement achieves this bound and the corresponding SDP optimization matrix "X" is unique then the underlying quantum state and measurements are unique up to an isometry ". In technical words, the non-contextuality inequality admits self testing. Moreover, the self-testing is guaranteed to be "robust".

Using the tools implemented in the last result, we also showed that the KCBS inequality and its generalizations admit robust self-testing.

3 Conclusions

In this work we introduced an appropriate extension of the notion of Bell self-testing to the framework of contextuality, where the noncontextuality assumption is not enforced via locality. In our main technical result, we identified a sufficient condition for showing that an arbitrary noncontextuality inequality is a robust self-test. As an application of our main theorem, we showed that the celebrated KCBS noncontextuality inequalities are robust self-tests. Our main theorem is not restricted to KCBS inequalities and can be used to self-test other noncontextuality inequalities, given they satisfy the necessary conditions; this will the be the topic of future investigations. Equally important, our proof techniques leverage a largely unnoticed connection between unicity problems in physics with uniqueness properties of optimization problems, which we believe will be of independent interest to the physics community.

References

[1] Adán Cabello, Simone Severini, and Andreas Winter. Graph-theoretic approach to quantum correlations. *Phys. Rev. Lett.*, 112(4):040401, 2014.

[2] Daniel Cavalcanti and Paul Skrzypczyk. Quantum steering: a review with focus on semidefinite programming. *Reports on Progress in Physics*, 80(2):024001, 2016.

[3] Andrew C Doherty, Pablo A Parrilo, and Federico M Spedalieri. Distinguishing separable and entangled states. *Physical Review Letters*, 88(18):187904, 2002.

[4] DS Gonçalves, C Lavor, MA Gomes-Ruggiero, AT Cesário, RO Vianna, and TO Maciel. Quantum state tomography with incomplete data: Maximum entropy and variational quantum tomography. *Physical Review A*, 87(5):052140, 2013.

[5] M Ježek, J Řeháček, and J Fiurášek. Finding optimal strategies for minimum-error quantum-state discrimination. *Physical Review A*, 65(6):060301, 2002.

[6] S. Kochen and E. P. Specker. The problem of hidden variales in quantum mechanics. *J. Math. Mech.*, 17:59–87, 1967.

[7] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications*, 2:238, 2011.

[8] Ben W Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every boolean function. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 544–551. IEEE, 2009.

[9] Le Phuc Thinh, Antonios Varvitsiotis, and Yu Cai. Structure of the set of quantum correlators via semidefinite programming. *arXiv preprint arXiv:1809.10886*, 2018.

[10] Jordi Tura, Remigiusz Augusiak, Ana Belén Sainz, Tamas Vértesi, Maciej Lewenstein, and Antonio Acín. Detecting nonlocality in many-body quantum states. *Science*, 344(6189):1256–1258, 2014.

Complementary Information Principle and Universal Uncertainty Regions

Yunlong Xiao[1 2 *] Kun Fang[3 †] Gilad Gour[1 2 ‡]

[1] *Department of Mathematics and Statistics, University of Calgary, Calgary, Alberta T2N 1N4, Canada*
[2] *Institute for Quantum Science and Technology, University of Calgary, Calgary, Alberta T2N 1N4, Canada*
[3] *Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge, CB3 0WA, UK*

Abstract. Uncertainty principle bounds the uncertainties about incompatible measurements, clearly setting quantum theory apart from the classical world. Its mathematical formulation, uncertainty relation, plays an irreplaceable role in quantum technologies. However, neither uncertainty principle nor uncertainty relation can fully describe the complementarity between quantum measurements. As an attempt to advance the efforts of complementarity in quantum theories, we formally propose a *complementary information principle*, significantly extending the one introduced by Heisenberg. First, we build a framework of black box testing consisting of pre- and post-testing with two incompatible measurements, introducing a rigorous mathematical expression of complementarity with definite information causality. Second, we provide majorization lower and upper bounds for the complementary information by utilizing the tool of semidefinite programming. In particular, we prove that our bounds are optimal under majorization due to the completeness of majorization lattice. Finally, as applications of our framework, we present a general method to outer-approximating all uncertainty regions and also establish fundamental limits for all qualified joint uncertainties.

Keywords: Complementary Information, Uncertainty Principle, Uncertainty Regions, Uncertainty Relations

1 Introduction

Backgrounds: Uncertainty principle unfolds a central mystery of quantum theory, namely *complementarity* [1]—a given physical attribute can only be revealed at the price of another complementary attribute being suppressed. As a more general concept, complementarity can also be exhibited through other "duality paradox", such as wave-particle duality. The arise of complementarity differentiates quantum theory from its classical counterpart, leading to a plethora of applications such as entanglement detection [3–6], Einstein-Podolsky-Rosen (EPR) steering detection [7–12] as well as quantum key distribution [13–15].

In recent developments, the study of uncertainty relations becomes a main approach to explore the complementarity of measurements. A series of efforts have been devoted to seeking the optimal bounds on uncertainty relations for given specific uncertainty measures, such as Shannon or Rényi entropies [16–40]. However, there is no doubt that the complete information of the physical attributes of incompatible measurements should be fully preserved in the set of their outcome probability vectors [41]. Inevitable losses of information will occur whenever we project a high dimensional probability vector to its one-dimensional entropic values. To have a full-scale understanding of complementarity between incompatible measurements and to be able to find more practical applications, it is of great importance to consider a more general framework, in which the complementary information remains undistorted.

Outline of results: In this work, we establish a new framework of *complementary information principle*, characterizing the trade-off between incompatible measurements with respect to their outcome probability vectors. Our main contributions can be outlined as follows:

1. We introduce the notion of marginal majorization and provide majorization lower and upper bounds for the complementary information between incompatible measurements by utilizing the tool of semidefinite programming. In particular, we prove that our bounds are optimal under majorization by using the completeness of majorization lattice.

2. We introduce the *universal uncertainty region* based on the complementary information principle and demonstrate its application to outer-approximating uncertainty regions with any given uncertainty measures in general [42], in contrast to previous developments which only restricted to specific uncertainty measures [43] or weak measures [44, 45]. The generality and efficiency of our approach make it suitable as a benchmark for the forthcoming research on uncertainty regions.

3. Finally, we discuss another application of our framework in bounding general forms of joint uncertainties. Our method works for all quantified joint uncertainty measures and provides strong supports for finding their fundamental limits.

The technical version of this work is attached after the extended abstract.

2 Details of Results

2.1 Complementary Information Principle

The basic task of black box testing is shown in Fig. 1. An unknown black box prepares two independent and identically distributed resources ρ, which are being tested by incompatible measurements M and N chronologically. Without loss of generality, we assume that the test with M (a.k.a. *pre-testing*) is performed first. After that, we do the test with N (a.k.a. *post-testing*). Each test is performed repeatedly, returning us an outcome probability distribution. Prior to the

*mathxiao123@gmail.com
†kf383@cam.ac.uk
‡gour@ucalgary.ca

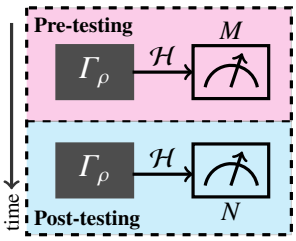


Figure 1: Diagram of black box testing. Two independent and identically distributed resources ρ is prepared by an unknown black box. After the preparation, two test with incompatible measurements M and N are being preformed chronologically.

test, the knowledge associated with the outcomes is the "uncertainty" of the measurement. Once the test is completed and its outcome is physically observed, this knowledge turns into our "information gain" of the same measurement. The following discussion will focus on the study of complementarity between the information gain from the pre-testing and the uncertainty of post-testing before it is actually performed. Suppose the outcome probability distribution from the pre-testing is given by $\mathbf{p}$. Since the post-testing will be performed over the same quantum state, its outcome is necessarily confined by the information gain $\mathbf{p}$ we obtained. We denote the set of all possible outcome $\mathbf{q}$ from the post-testing as $Q(M, N, \mathbf{p})$.

To exhibit the complementarity study quantitatively, we introduce the *right-majorization* $(\mathbf{p}_1, \mathbf{q}_1) \prec_R (\mathbf{p}_2, \mathbf{q}_2)$ if $\mathbf{p}_1 = \mathbf{p}_2$ and $\mathbf{q}_1 \prec \mathbf{q}_2$, interpreting that two sets of black box testing admit the same pre-testing outcome while the first post-testing outcome is more uncertain than the second one. The *left-majorization* can be similarly defined as $(\mathbf{p}_1, \mathbf{q}_1) \prec_L (\mathbf{p}_2, \mathbf{q}_2)$ if $\mathbf{q}_1 = \mathbf{q}_2$ and $\mathbf{p}_1 \prec \mathbf{p}_2$. Both $\prec_R$ and $\prec_L$ are called *marginal majorizations*, which is more informative than $\prec$ in our context.

Based on the notion of marginal majorizations, we are now in a position to quantify the complementarity. Due to the fact that a probability simplex with majorization forms a complete lattice [46, 47], then any possible $\mathbf{q} \in Q$ must be confined within two unique probability vectors $\boldsymbol{r}, \boldsymbol{t}$. The following theorems establish an explicit construction of the optimal choices of $\boldsymbol{r}$ and $\boldsymbol{t}$.

Theorem 1. *Let $M = \{|u_j\rangle\}_{j=1}^n$ and $N = \{|v_\ell\rangle\}_{\ell=1}^n$ be the measurements of pre- and post-testing respectively. If the outcome probability of M is given by $\mathbf{p} = (c_j)_{j=1}^n$, then any outcome probability $\mathbf{q}$ of N is bounded as $(\mathbf{p}, \boldsymbol{r}) \prec_R (\mathbf{p}, \mathbf{q}) \prec_R (\mathbf{p}, \boldsymbol{s})$ where $\boldsymbol{r}$ and $\boldsymbol{s}$ can be explicitly computed via semidefinite programs. Their explicit forms are given in the technical version attached.*

An intuitive understanding of this result can be illustrated in terms of Lorenz curves. Denote the Lorenz curve of $\mathbf{q}$ as $\mathcal{L}(\mathbf{q})$. Then the majorization relation $\boldsymbol{x} \prec \boldsymbol{y}$ can be geometrically interpreted as $\mathcal{L}(\boldsymbol{x})$ laying everywhere below $\mathcal{L}(\boldsymbol{y})$. To find the optimal $\boldsymbol{r}$ and $\boldsymbol{t}$ such that $\boldsymbol{r} \prec \mathbf{q} \prec \boldsymbol{t}$ for all $\mathbf{q} \in Q$ is equivalent to find the tightest Lorenz curves bounding $\mathcal{L}(\mathbf{q})$ from below and above for all $\mathbf{q} \in Q$, respectively. The lower bound $\boldsymbol{r}$ can be shown as optimal. To obtain the optimal upper bound, it suffices for us to perform an additional *flatness process* [48]. Denote $\boldsymbol{t}$ as the probability vector after performing the flatness process on $\boldsymbol{s}$. Then the bounds $\boldsymbol{r}$ and $\boldsymbol{t}$ can be ensured as optimal for the set Q under the order of majorization.

Theorem 2. *Based on the same settings in Theorem 1, for any probability vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ such that $\boldsymbol{x} \prec \mathbf{q} \prec \boldsymbol{y}$ for all $\mathbf{q} \in Q$, it holds $\boldsymbol{x} \prec \boldsymbol{r} \prec \mathbf{q} \prec \boldsymbol{t} \prec \boldsymbol{y}$.*

Our results inspire a new form of "information causality" [49]: the information that an observer can gain from a state in the past confines the uncertainty associated with the same state in the future. In other words, the physical attribute of the uncertainty associated with N can only be exhibited at the expense of information gained from M. One extreme case is that without any information gain from the pre-testing, our majorization bounds lead to the trivial result for the post-testing, i.e. $(1/n, 1/n, \ldots, 1/n) \prec \mathbf{q} \prec (1, 0, \ldots, 0)$. Another extreme case is Heisenberg's uncertainty principle, which corresponds to the situation where we obtain an outcome from pre-testing with certainty. That is, the outcome probability vector $\mathbf{p}$ has one entry equal to 1 and 0 otherwise. Calculation of our upper bound gives us $\mathbf{q} \prec \boldsymbol{t} \neq (1, 0, \ldots, 0)$ indicating the uncertainty of the measurement N. For this reason, our complementary information principle (Theorem 1) significantly extends the one by Heisenberg, providing a much more complete characterization of the complementarity between incompatible measurements.

2.2 Universal Uncertainty Regions

Since the pioneering work of Deutsch [16], much has been done in the direction of lower-bounding the joint uncertainties $f(\mathbf{p}(\rho)) + g(\mathbf{q}(\rho)) \geqslant b$, where $\mathbf{p}(\rho)$ and $\mathbf{q}(\rho)$ are outcome probability distributions of the pre- and post-testing on state ρ respectively, and f, g are valid uncertainty measures. In the case of *uncertainty region*

$$\mathcal{R}(f, g) := \bigcup_\rho \{ (f(\mathbf{p}(\rho)), g(\mathbf{q}(\rho))) \}, \tag{1}$$

the relation $f(\mathbf{p}(\rho)) + g(\mathbf{q}(\rho))$ is nothing but a strainght line with slope -1 in the coordinate plane of $(f(\mathbf{p}), g(\mathbf{q}))$, and its optimal lower bound $b = \min_\rho \{f(\mathbf{p}(\rho)) + g(\mathbf{q}(\rho))\}$ is then achieved at the tangent line to the bottom left of $\mathcal{R}(f, g)$ as shown in Fig. 2. Namely the description of uncertainty regions can be much more informative than uncertainty relations. However, no efficient method is known to characterize the region $\mathcal{R}(f, g)$ in general. As an application of the majorization bounds in Theorem 1 and 2, we can provide a general approach for outer-approximations.

Consider the statistics set $\mathcal{R} := \bigcup_\rho \{(\mathbf{p}(\rho), \mathbf{q}(\rho))\}$ in $\mathbb{R}^n \times \mathbb{R}^n$ by collecting all compatible pairs of pre- and post-testing outcome probabilities. Note that the set of all quantum states ρ can be divided into equivalent classes based on the outcome probability $\mathbf{p}$ of pre-testing. Then $\mathcal{R}$ can be fine-grained as

$$\mathcal{R} = \bigcup_{\mathbf{p} \in \mathsf{S}_n} \mathcal{R}_\mathbf{p}, \quad \text{with} \quad \mathcal{R}_\mathbf{p} := \{(\mathbf{p}, \mathbf{q}) : \mathbf{q} \in Q(M, N, \mathbf{p})\}, \tag{2}$$

where $\mathsf{S}_n := \{\boldsymbol{x} \in \mathbb{R}^n : \sum_i x_i = 1, x_i \geq 0, \forall i\}$ is the probability simplex of dimension n. For any fixed $\mathbf{p}$, the majorization bounds $\boldsymbol{r}$, $\boldsymbol{t}$ set a boundary for the set $Q(M, N, \mathbf{p})$. Thus we have the relaxation

$$\mathcal{R}_\mathbf{p} \subseteq \widetilde{\mathcal{R}}_\mathbf{p}, \quad \text{with} \quad \widetilde{\mathcal{R}}_\mathbf{p} := \{ (\mathbf{p}, \mathbf{q}) : \boldsymbol{r} \prec \mathbf{q} \prec \boldsymbol{t} \}. \tag{3}$$

As a consequence, by taking the union with respect to $\mathbf{p}$, we have the relaxation of the whole region,

$$\mathcal{R} \subseteq \widetilde{\mathcal{R}} \quad \text{with} \quad \widetilde{\mathcal{R}} := \bigcup_{\mathbf{p}\in \mathsf{S}_n} \widetilde{\mathcal{R}}_{\mathbf{p}}. \tag{4}$$

Finally, any uncertainty region $\mathcal{R}(f,g)$ can be retrieved by projecting $\mathcal{R}$ from $\mathbb{R}^n\times\mathbb{R}^n$ to $\mathbb{R}\times\mathbb{R}$ via the uncertainty measures f, g, and the projection of $\widetilde{\mathcal{R}}$ will give us an outer-approximation of $\mathcal{R}(f,g)$ accordingly. Since $\widetilde{\mathcal{R}}$ can be used to generate an approximation of uncertainty region with any measures, we thus name it a *universal uncertainty region*. We emphasize that this universal region $\widetilde{\mathcal{R}}$ as well as its projections can be explictly depicted by running $\mathbf{p}$ over the probability simplex, which is significantly more tractable than characterizing $\mathcal{R}$ by taking ρ over the set of all quantum states.

Theorem 3. *Let $M = \{|u_j\rangle\}_{j=1}^n$ and $N = \{|v_\ell\rangle\}_{\ell=1}^n$ be the measurements of pre- and post-testing respectively. For any uncertainty measures f for M and g for N, their uncertainty region is outer-approximated as $\mathcal{R}(f,g) \subseteq \widetilde{\mathcal{R}}(f,g)$ with $\widetilde{\mathcal{R}}(f,g) := \{(f(\mathbf{p}), g(\mathbf{q})) : (\mathbf{p},\mathbf{q}) \in \widetilde{\mathcal{R}}\}$. In particular, the outer-approximation is tight $\mathcal{R}(f,g) = \widetilde{\mathcal{R}}(f,g)$ when $n = 2$.*

Note that for any given pre-testing outcome probability $\mathbf{p}$, the majorization bounds $\boldsymbol{r}$ and $\boldsymbol{t}$ can be computed explicitly. Combining the Schur-concavity of the uncertainty measure g, the fine-grained outer-approximation can be simplified as

$$\widetilde{\mathcal{R}}_{\mathbf{p}}(f,g) = \{(f(\mathbf{p}), y) \mid g(\boldsymbol{t}) \leqslant y \leqslant g(\boldsymbol{r})\}. \tag{5}$$

By running $\mathbf{p}$ over the probability simplex, we can explicitly depict the whole region $\widetilde{\mathcal{R}}(f,g)$. A schematic diagram is given in Fig. 2, which legibly explains how our approximation method works. It is also worth mentioning that our results can also be easily generalized to multiple testings.

Due to the generality of our approach, the approximation is not guaranteed to work well for every uncertainty measures. But we should stress that our approximation can be computed explicitly and is valid for any eligible uncertainty measures, liberating us from specific forms of uncertainty relations. More importantly, this is the first efficient method to approximating uncertainty regions in general, which can be used as a benchmark for future works.

2.3 Fundamental Limits for Joint Uncertainties

As another illustration of the generality of our framework, we study the joint uncertainties given by the most general measure $\mathcal{J} : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ for a pair of probability vectors $(\mathbf{p},\mathbf{q}) \in \mathcal{R}$ [42]. Such a measure includes the usual forms $f(\mathbf{p}) + g(\mathbf{q})$, $f(\mathbf{p})g(\mathbf{q})$, $f(\mathbf{p}\otimes\mathbf{q})$ and $f(\mathbf{p}\oplus\mathbf{q})$ as special cases. To capture the essential properties of a measure of joint uncertainties, it has been argued in [42] that $\mathcal{J}$ should meet the following postulates : (i) Non-negativity: $\mathcal{J}(\mathbf{p},\mathbf{q}) \geqslant 0$; (ii) Monotonicity under randomly relabelling: $\mathcal{J}(D_1\mathbf{p}, D_2\mathbf{q}) \geqslant \mathcal{J}(\mathbf{p},\mathbf{q})$ for all doubly stochastic matrices D_1 and D_2. The characterization of the joint uncertainties $\mathcal{J}(\mathbf{p},\mathbf{q})$ is crucial in the study of quantum information and quantum measurements, leading to a plethora of applications [3–12]. In particular, any state-independent lower bound b of $\mathcal{J}(\mathbf{p},\mathbf{q})$ leads to a uncertainty relation $\mathcal{J}(\mathbf{p},\mathbf{q}) \geqslant b$ while any state-independent upper bound a of $\mathcal{J}(\mathbf{p},\mathbf{q})$ gives us a reverse uncertainty relation $a \geqslant \mathcal{J}(\mathbf{p},\mathbf{q})$. A natural question is to ask how to find a and b for joint uncertainties $\mathcal{J}(\mathbf{p},\mathbf{q})$ in general.

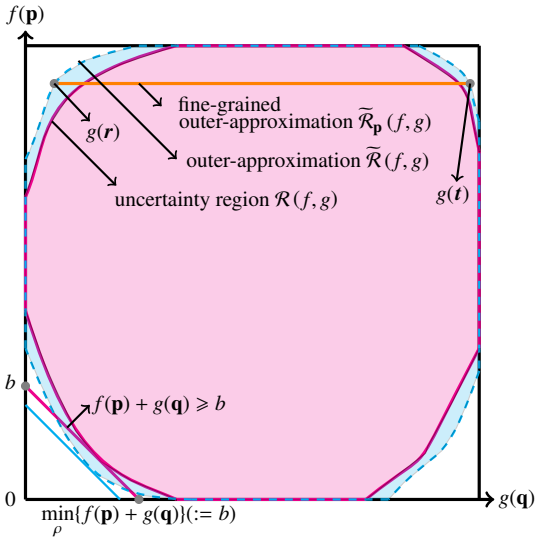


Figure 2: (color online) A schematic diagram depicts the uncertainty region $\mathcal{R}(f,g)$ (magenta) with its outer-approximation $\widetilde{\mathcal{R}}(f,g)$ (cyan), and the fined-grained outer-approximation $\widetilde{\mathcal{R}}_{\mathbf{p}}(f,g)$ (orange). The optimal uncertainty relations $f(\mathbf{p}) + g(\mathbf{q}) \geqslant \min_\rho\{f(\mathbf{p}) + g(\mathbf{q})\}$ is tangent to the left lower boundaries of $\mathcal{R}(f,g)$.

By associating *Hardy-Littlewood-Pólya theorem* [50], which states that two probability vectors $\boldsymbol{x} \prec \boldsymbol{y}$ if and only if $\boldsymbol{x} = D\boldsymbol{y}$ for some doubly stochastic matrix D, with our marginal majorization bounds from Theorem 1 and 2, we establish the state-independent bounds $a \geqslant \mathcal{J}(\mathbf{p},\mathbf{q}) \geqslant b$ with

$$\begin{aligned} a &:= \min\left\{\max_{\mathbf{p}\in\mathsf{S}_n} \mathcal{J}(\mathbf{p},\boldsymbol{r}), \max_{\mathbf{q}\in\mathsf{S}_n} \mathcal{J}(\boldsymbol{u},\mathbf{q})\right\}, \\ b &:= \max\left\{\min_{\mathbf{p}\in\mathsf{S}_n} \mathcal{J}(\mathbf{p},\boldsymbol{t}), \min_{\mathbf{q}\in\mathsf{S}_n} \mathcal{J}(\boldsymbol{v},\mathbf{q})\right\}. \end{aligned} \tag{6}$$

In particular, the bounds a and b are tight for the qubit case. More remarkably, our method works for all quantified joint uncertainty measures and provides strong supports for finding their fundamental limits.

References

[1] N. Bohr, The Quantum Postulate and the Recent Development of Atomic Theory, *Nature (London)* **121**, 580 (1928).

[2] M. J. W. Hall, Information Exclusion Principle for Complementary Observables, *Phys. Rev. Lett.* **74**, 3307 (1995).

[3] R. Horodecki and P. Horodecki, Quantum redundancies and local realism, *Phys. Lett. A* **194**, 147 (1994).

[4] V. Giovannetti, Separability conditions from entropic uncertainty relations, *Phys. Rev. A* **70**, 012102 (2004).

[5] O. Gühne and M. Lewenstein, Entropic uncertainty relations and entanglement, *Phys. Rev. A* **70**, 022316 (2004).

[6] O. Gühne and G. Tóth, Entanglement detection, *Phys. Rep* **474**, 1 (2009).

[7] Y. Xiao, Y. Xiang, Q. He, and B. C. Sanders, Quasi-Fine-Grained Uncertainty Relations, arXiv:1807.07829.

[8] A. Rutkowski, A. Buraczewski, P. Horodecki, and M Stobińska, Quantum steering inequality with tolerance for measurement-setting errors: Experimentally feasible signature of unbounded violation, *Phys. Rev. Lett.* **118**, 020402 (2017).

[9] A. Riccardi, C. Macchiavello, and L. Maccone, Multipartite steering inequalities based on entropic uncertainty relations, *Phys. Rev. A* **97**, 052307 (2018).

[10] A. C. S. Costa, R. Uola, and O. Gühne, Entropic Steering Criteria: Applications to Bipartite and Tripartite Systems, *Entropy* **20**, 763 (2018).

[11] A. C. S. Costa, R. Uola, and O. Gühne, Steering criteria from general entropic uncertainty relations, *Phys. Rev. A* **98**, 050104(R) (2018).

[12] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Quantum Steering, arXiv:1903.06663.

[13] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d-Level Systems, *Phys. Rev. Lett.* **88**, 127902 (2002).

[14] J. M. Renes and J.-C. Boileau, Conjectured Strong Complementary Information Tradeoff, *Phys. Rev. Lett.* **103**, 020402 (2009).

[15] R. Renner, Security of Quantum Key Distribution, *Ph.D. thesis* (ETH Zurich).

[16] D. Deutsch, Uncertainty in quantum measurements, *Phys. Rev. Lett.* **50**, 631 (1983).

[17] M. H. Partovi, Entropic formulation of uncertainty for quantum measurements, *Phys. Rev. Lett.* **50**, 1883 (1983).

[18] K. Kraus, Complementary observables and uncertainty relations, *Phys. Rev. D* **35**, 3070 (1987).

[19] H. Maassen and J. B. M. Uffink, Generalized entropic uncertainty relations, *Phys. Rev. Lett.* **60**, 1103 (1988).

[20] I. D. Ivanovic, An in equality for the sum of entropies of unbiased quantum measurements, *J. Phys. A* **25**, L363 (1992).

[21] J. Sánchez, Entropic uncertainty and certainty relations for complementary observables, *Phys. Lett. A* **173**, 233 (1993).

[22] M. A. Ballester and S. Wehner, Entropic uncertainty relations and locking: tight bounds for mutually unbiased bases, *Phys. Rev. A* **75**, 022319 (2007).

[23] S. Wu, S. Yu, and K. Mølmer, Entropic uncertainty relation for mutually unbiased bases, *Phys. Rev. A* **79**, 022104 (2009).

[24] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, The uncertainty principle in the presence of quantum memory, *Nature Phys.* **6**, 659 (2010).

[25] C.-F. Li, J.-S. Xu, X.-Y. Xu, K. Li, and G.-C. Guo, Experimental investigation of the entanglement-assisted entropic uncertainty principle, *Nat. Phys.* **7**, 752 (2011).

[26] R. Prevedel, D. R. Hamel, R. Colbeck, K. Fisher, and K. J. Resch, Experimental investigation of the uncertainty principle in the presence of quantum memory and its application to witnessing entanglement, *Nat. Phys.* **7**, 757 (2011).

[27] Y. Huang, Entropic uncertainty relations in multidimensional position and momentum spaces, *Phys. Rev. A* **83**, 052124 (2011).

[28] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, *Phys. Rev. Lett.* **106**, 110506 (2011).

[29] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, Uncertainty relations from simple entropic properties, *Phys. Rev. Lett.* **108**, 210405 (2012).

[30] P. J. Coles and M. Piani, Improved entropic uncertainty relations and information exclusion relations, *Phys. Rev. A* **89**, 022112 (2014).

[31] J. Kaniewski, M. Tomamichel, and S. Wehner, Entropic uncertainty from effective anticommutators, *Phys. Rev. A* **90**, 012332 (2014).

[32] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, Position-momentum uncertainty relations in the presence of quantum memory, *J. Math. Phys.* **55**, 122205 (2014).

[33] M. Berta, S. Wehner, and M. M. Wilde, Entropic uncertainty and measurement reversibility, *New J. Phys.* **18**, 073004 (2016).

[34] Y. Xiao, N. Jing, S.-M. Fei, T. Li, X. Li-Jost, T. Ma, and Z.-X. Wang, Strong entropic uncertainty relations for multiple measurements, *Phys. Rev. A* **93**, 042125 (2016).

[35] Y. Xiao, N. Jing, S.-M. Fei, and X. Li-Jost, Improved uncertainty relation in the presence of quantum memory, *J. Phys. A* **49**, 49LT01 (2016).

[36] Y. Xiao, N. Jing, and X. Li-Jost, Uncertainty under quantum measures and quantum memory, *Quantum Inf. Proc.* **16**, 104 (2017).

[37] J.-L. Huang, W.-C. Gan, Y. Xiao, F.-W. Shu, and M.-H. Yung, Holevo bound of entropic uncertainty in Schwarzschild spacetime, *Eur. Phys. J. C* **78**, 545 (2018).

[38] Z. Chen, Z. Ma, Y. Xiao, and S.-M. Fei, Improved quantum entropic uncertainty relations, *Phys. Rev. A* **98**, 042305 (2018).

[39] P. J. Coles, V. Katariya, S. Lloyd, I. Marvian, and M. M. Wilde, Entropic Energy-Time Uncertainty Relation, *Phys. Rev. Lett.* **122**, 100401 (2019).

[40] J.-L. Li and C.-F. Qiao, The Optimal Uncertainty Relation, arXiv:1902.00834.

[41] D. Saha, M. Oszmaniec, L. Czekaj, M. Horodecki, and R. Horodecki, Operational foundations for complementarity and uncertainty relations, arXiv:1809.03475.

[42] V. Narasimhachar, A. Poostindouz, and G. Gour, Uncertainty, joint uncertainty, and the quantum uncertainty principle, *New J. Phys.* **18** 033019 (2016).

[43] K. Abdelkhalek, R. Schwonnek, H. Maassen, F. Furrer, J. Duhme, P. Raynal, B.-G. Englert, and R. F. Werner, Optimality of entropic uncertainty relations, *Int. J. Quantum Inf.* **13**, 1550045 (2015).

[44] R. Schwonnek, L. Dammeier, and R. F. Werner, State-Independent Uncertainty Relations and Entanglement Detection in Noisy Systems, *Phys. Rev. Lett.* **119**, 170404 (2017).

[45] P. Busch and O. Reardon-Smith, On Quantum Uncertainty Relations and Uncertainty Regions, arXiv:1901.03695.

[46] R. B. Rapat, Majorization and singular values. III, *Linear Algebra Its Appl.* **145**, 59 (1991).

[47] G. M. Bosyk, G. Bellomo, F. Holik, H. Freytes, and G. Sergioli, Optimal common resource in majorization-based resource theories, arXiv:1902.01836.

[48] F. Cicalese and U. Vaccaro, Supermodularity and Subadditivity Properties of the Entropy on the Majorization Lattice, *IEEE Trans. Inf. Theory* **48**, 933 (2002).

[49] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Information causality as a physical principle, *Nature* **461**, 1101 (2009).

[50] G.H. Hardy, J. E. Littlewood, and G. Pólya, Some simple inequalities satisfied by convex functions, *Mess. Math.* **58**, 145 (1929).

The power of dephasing-covariant operations in the manipulation of quantum coherence

Bartosz Regula[1] Varun Narasimhachar[1] Francesco Buscemi[2] Mile Gu[1 3]

[1] *School of Physical and Mathematical Sciences, Nanyang Technological University, 637371, Singapore*
[2] *Graduate School of Informatics, Nagoya University, Chikusa-ku, 464-8601 Nagoya, Japan*
[3] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore*

Abstract. Although quantum coherence plays a fundamental role in enabling quantum advantages in technological applications, the operational rules governing its manipulation are still not very well understood. Here, we investigate the operational capabilities of the dephasing-covariant incoherent operations (DIO), the largest class of quantum channels which can neither create nor detect coherence, in efficiently manipulating quantum coherence as a resource. We first show that pure-state transformations under DIO are completely governed by majorization, establishing for the first time necessary and sufficient conditions for such transformations, and showing that DIO forms another class of operations in which majorization plays a vital role. We then propose an operationally-motivated extension of the set DIO, the input-dependent class ρ-DIO, and characterize its capabilities. We show that, although ρ-DIO cannot detect the coherence of input state ρ, they can distill more coherence than DIO. Curiously, the advantage disappears at the asymptotic level, where both sets of operations achieve the same performance, thus establishing ρ-DIO as a good operational substitute for DIO.

Keywords: Quantum coherence, Quantum resource theories, One-shot quantum information theory

1 Introduction

Quantum coherence, or superposition, is an intrinsic feature of quantum mechanics which underlies the advantages enabled by quantum information processing and quantum technologies [1]. The resource theory of quantum coherence [1–4] has found extensive use in the characterization of our ability to manipulate coherence efficiently within a rigorous theoretical framework, wherein the properties of a resource are investigated under a suitable set of allowed ("free") operations which reflect the constraints placed on the manipulation of the given resource [5, 6]. Despite many promising developments in the establishment of a comprehensive theory of coherence, the constraints on its manipulation are not clear [1, 7, 8] — in particular, no compelling set of physically-motivated assumptions managed to single out a unique class of free operations under which the operational features of coherence should be investigated, mirroring the fundamental role of local operations and classical communication in the resource theory of entanglement [9]. This has motivated the definition and characterization of a multitude of possible sets of free operations, and sparked efforts to compare their operational power [7, 8, 10–25].

Many proposed types of free operations stem from meaningful physical considerations: these include the physically incoherent operations [7], which only require the use of incoherent ancillary systems and incoherent measurements, making them very easily implementable; the strictly incoherent operations [4, 12], which allow for a similar implementation with an incoherent ancilla; or the genuinely incoherent operations [14], which preserve any incoherent state. However, these operations were found to be very limited in their operational capabilities [14, 26, 27], suggesting that any non-trivial and useful resource theory of coherence would require a larger set of allowed maps. It therefore remains to uncover the exact capabilities of different sets of operations, establishing the ultimate limits on our power to manipulate quantum coherence while bound by the resource-theoretic restrictions.

Out of the many choices of operations, the study of operations based on dephasing covariance has recently attracted significant attention due to their strong physical justification and considerable operational power [7, 8, 15, 18–20, 22, 23]. In this work, we characterize the operational capabilities of such **dephasing-covariant incoherent operations** (DIO) [7, 8], which constitute the largest class of channels which can neither create nor detect (use) coherence and can be considered to be inherently "classical" operations [23, 28]. We establish for the first time a complete description of pure-state transformations under these operations by relating them with the theory of majorization, revealing also an operational connection between DIO and various other classes of free operations. We then introduce an extension of the class DIO, the input-dependent ρ-DIO, and characterize its properties in coherence manipulation. We show in particular that it satisfies a curious property: even though ρ-DIO cannot detect the coherence of the state ρ, they can still *distill* more coherence from ρ than the class DIO; however, this advantage disappears in the asymptotic limit, where DIO again match the capabilities of ρ-DIO. Our results provide novel insight into the operational power of free operations in the manipulation of coherence, shedding light on the capabilities of dephasing-covariant channels in state transformations, and in particular suggest that ρ-DIO — a structurally simpler class of channels than DIO — can be employed as a substitute for DIO without sacrificing its physical relevance. The results provide insight into the structure of the physical constraints on coherence manipulation and establish new connections in the operational description of quantum coherence.

1.1 DIO and ρ-DIO

Quantum coherence is inherently a basis-dependent concept. We will therefore fix an orthonormal basis $\{|i\rangle\}_{i=1}^{d}$ which we deem incoherent, and use $\mathcal{I}$ to denote the set of all states diagonal (incoherent) in this basis. We will use $\Delta(\cdot) = \sum_i |i\rangle\langle i| \cdot |i\rangle\langle i|$ to denote the

completely dephasing channel in this basis.

The class of operations MIO is defined to consist of all maps which do not create coherence in the sense that $\sigma \in \mathcal{I} \Rightarrow \Lambda(\sigma) \in \mathcal{I}$. Due to their inability to create coherence, it can be regarded as the largest possible class of free operations. However, it satisfies some undesirable properties such as being able to increase the diagonal rank of a pure state [13]: a two-level superposition $\sum_{i=1}^{2} \psi_i |i\rangle$ can be mapped with MIO to a multi-level superposition $\sum_{i=1}^{3} \phi_i |i\rangle$, which could be regarded as effectively increasing the strength of the coherence contained in the state. To circumvent this problem, more restricted choices of operations can be defined. One such class are the precisely DIO, defined to be all maps which commute with the completely dephasing channel, i.e. $\Lambda \circ \Delta(\rho) = \Delta \circ \Lambda(\rho)\ \forall \rho$. The crucial difference between MIO and DIO is that DIO neither create nor *detect* coherence, in the sense that measurement statistics under any incoherent measurement remain unaffected by the DIO operation Λ: we have $\langle i|\Lambda(\rho)|i\rangle = \langle i|\Lambda(\Delta(\rho))|i\rangle$ for all i. These operations have previously been considered in various contexts [15, 28], and indeed they admit several interpretations. The operations DIO can be regarded as inherently classical [23, 28], as any classical (incoherent) observer is unable to distinguish $\Lambda(\rho)$ from $\Lambda \circ \Delta(\rho)$, and hence is unable to say whether the coherence of ρ has been employed in the process. The latter point shows that DIO can also be understood as the operations which do not use coherence [12], as the properties of the output system accessible to a classical observer are independent of the coherence of the input.

The ability to detect coherence is of particular importance in practical setups relying on quantum coherence, such as general interferometric experiments [12, 23, 29]. A general interferometric protocol can be understood as consisting of three separate parts: first, a state in superposition is created; second, path-dependent phases are encoded in the state with suitable unitary operations; and third, the information about the paths is extracted in a measurement. It is then explicit that the ability to create (in the first step) and detect (in the last step) coherence are crucial for any such setup to work, and indeed any operation which can neither create nor detect coherence is inherently free and cannot be used in such an experimental protocol.

However, consider now a scenario in which the input coherent state ρ of a protocol is known: the operations which cannot detect the coherence of the input state are then precisely those which satisfy $\Lambda \circ \Delta(\rho) = \Delta \circ \Lambda(\rho)$ for this choice of ρ, and indeed it is not necessary to impose dephasing-covariance for all quantum states if one is concerned with detecting the coherence of ρ specifically. This point of view motivates us to define the class of **ρ-dephasing covariant incoherent operations** (ρ-DIO), which we take to be the operations which commute with the dephasing channel Δ for a given input state ρ.

It is clear that a ρ-DIO map can in principle create or detect coherence when acting on an input state other than ρ. However, the definition of ρ-DIO is justified whenever one deals with an explicit protocol which transforms a fixed input state to some desired output. Two of such protocols form the foundations of the manipulation of coherence as a quantum resource: these are the tasks of *coherence distillation* [4, 19, 25], which aims to convert a given input state to a maximally coherent state, as well as *coherence dilution* [4, 18], which performs the opposite transformation of a maximally coherent input state to some desired state. The definition of ρ-DIO then motivates the question: can the operational capabilities of DIO be surpassed by operations which do not detect the coherence of ρ? To address this question, we first describe the transformations achievable under DIO, and later investigate whether ρ-DIO can outperform DIO.

2 Transformations under DIO

Although a fundamental and operationally meaningful choice of operations, the class DIO is relatively unexplored, and few of its properties are known. Other sets of operations are better understood: in particular, it is known that the transformations of pure states under the classes of incoherent operations (IO) [3] and strictly incoherent operations (SIO) [4, 12] are governed by majorization theory, in a similar way to the manipulation of pure-state entanglement under local operations and classical communication [30]. Precisely, one has that a pure-state transformation $|\psi\rangle = \sum_i \psi_i |i\rangle \to |\phi\rangle = \sum_i \phi_i |i\rangle$ is achievable under IO or SIO if and only if $\Delta(\psi) \prec \Delta(\phi)$ [13, 31, 32], i.e. if $\sum_{i=1}^{k} |\psi_i|^2 \leq \sum_{i=1}^{k} |\phi_i|^2\ \forall k \in \{1, \ldots, d\}$ where we assume that the coefficients of the states are arranged so that $|\psi_1| \geq \ldots \geq |\psi_d|$. Our first contribution is to extend this relation to the class DIO.

Theorem 1 *The deterministic pure-state transformation $\psi \to \phi$ is possible under DIO if and only if $\Delta(\psi) \prec \Delta(\phi)$.*

This establishes DIO as another class of operations in which pure-state transformations are fully governed by majorization theory, and reveals an operational equivalence between DIO, IO, and SIO in manipulating pure states. The equivalence is non-trivial: for example, there exist coherence monotones which can increase under DIO despite always decreasing under the action of SIO/IO [33].

The Theorem immediately lets us apply a plethora of results to coherence manipulation under DIO. For instance, the recent investigation of moderate-deviation interconversion rates under majorization in [34, 35] allows one to precisely characterize DIO transformations beyond the single-shot regime; similarly, a recent investigation of quantum coherence fluctuation relations [36] relies purely on the theory of majorization, and our result immediately establishes that the results can be directly applied to describe the fluctuations and battery-assisted transformations under DIO operations.

The result can also be extended to so-called heralded probabilistic transformations, where a state $|\psi\rangle$ is transformed to one of the states $\{|\phi_j\rangle\}$ with a corresponding probability p_j, and the information about the final state is encoded onto a classical flag register; one can show that this is possible under DIO if and only if $\Delta(\psi) \prec \sum_j p_j \Delta(\phi_j)$. This again establishes an equivalence between DIO, IO, and SIO in such transformations.

3 Coherence manipulation with ρ-DIO

The existence of a ρ-DIO transformation between states ρ and ω is equivalent to the existence of a quantum channel Λ such that $\Lambda(\rho) = \omega$ and $\Lambda(\Delta(\rho)) = \Lambda(\Delta(\omega))$. This has strong connections with the concept of relative majorization [37–39], and could perhaps suggest that majorization will also play a role in ρ-DIO transformations, making them no more powerful than DIO. We will show that this in fact not the case. To investigate this problem, we now focus on the fundamental tasks of distillation and dilution.

3.1 Distillation

The ε-error one-shot distillable coherence under the class ρ-DIO is defined to be the maximal size of the maximally coherent state $|\Psi_m\rangle = \sum_i \frac{1}{\sqrt{m}} |i\rangle$ achievable under a single ρ-DIO transformation; formally, we have

$$C^{(1),\varepsilon}_{d,\rho\text{-DIO}}(\rho) \coloneqq \log \max \left\{ m \,\middle|\, \max_{\Lambda \in \rho\text{-DIO}} F(\Lambda(\rho), \Psi_m) \geq 1-\varepsilon \right\}.$$

Our first result exactly characterizes this quantity in terms of the hypothesis testing relative entropy D^{ε}_H [40]

$$D^{\varepsilon}_H(\rho||X) \coloneqq -\log \min\{\operatorname{Tr} MX \mid 0 \leq M \leq \mathbb{1}, 1 - \operatorname{Tr} M\rho \leq \varepsilon\}.$$

In particular, we have the following.

Theorem 2 *The one-shot distillable coherence under ρ-DIO for any input state ρ is given by*

$$C^{(1),\varepsilon}_{d,\rho\text{-DIO}}(\rho) = \lfloor D^{\varepsilon}_H(\rho \| \Delta(\rho)) \rfloor_{\log}, \text{ where } \lfloor x \rfloor_{\log} = \log \lfloor 2^x \rfloor.$$

This explicitly shows a very intuitive property of the class of operations ρ-DIO: the more distinguishable a state ρ is from its dephased version $\Delta(\rho)$, the more coherence we can extract from it using ρ-DIO.

Of particular importance will be the case $\varepsilon = 0$, that is, exact deterministic distillation of coherence. In particular, combining the results of Thm. 1 and 2, we have the following.

Corollary 3 *A pure state $|\psi\rangle = \sum_i \psi_i |i\rangle$ can be deterministically transformed to $|\Psi_m\rangle$ under DIO iff*

$$\max_i |\psi_i|^2 \leq \frac{1}{m}, \tag{1}$$

while the transformation is possible under ψ-DIO iff

$$\langle \psi | \Delta(\psi) | \psi \rangle = \sum_i |\psi_i|^4 \leq \frac{1}{m}. \tag{2}$$

The above allows us to easily construct examples of states such that, even though $|\psi\rangle \to \Psi_m$ is impossible under DIO, the transformation can be achieved by ψ-DIO. Consider for example the state $|\psi\rangle \coloneqq \left(\sqrt{\frac{5}{8}}, \sqrt{\frac{3}{16}}, \sqrt{\frac{3}{16}}\right)^T$, for which it can be verified that $\Delta(\Psi_2) \not\succ \Delta(\psi)$, which means the transformation $|\psi\rangle \to |\Psi_2\rangle$ is impossible by DIO (and in fact by all MIO [19]). However, we easily compute $\sum_i |\psi_i|^4 = \frac{59}{128} < \frac{1}{2}$ and so $C^{(1),0}_{d,\psi\text{-DIO}}(\psi) = 1$ and hence one coherence bit Ψ_2 can be distilled exactly. This explicitly shows an operational advantage provided by the operations ρ-DIO over DIO in state transformations and in particular in coherence distillation. Such an advantage is rather surprising: to any classical observer, the distillation protocol is indistinguishable from a classical operation, yet it can distill more coherence than even the powerful class MIO.

However, consider now the many-copy scenario in which we have access to multiple copies of the given state ρ and perform joint quantum operations on the composite system $\rho^{\otimes n}$. In the asymptotic independent and identically distributed (i.i.d.) limit, one can then define the distillable coherence under ρ-DIO as

$$C^{\infty}_{d,\rho\text{-DIO}}(\rho) = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} C^{(1),\varepsilon}_{d,\rho^{\otimes n}\text{-DIO}}(\rho^{\otimes n}). \tag{3}$$

A simple application of Thm. 1 together with the quantum Stein's lemma [41, 42] reveals that we have in fact $C^{\infty}_{d,\rho\text{-DIO}}(\rho) = S(\rho \| \Delta(\rho))$, that is, the relative entropy of coherence $S(\rho\|\Delta(\rho))$ characterizes the asymptotic rate of coherence distillation under ρ-DIO. But it is known already that under DIO we also have $C^{\infty}_{d,DIO}(\rho) = S(\rho\|\Delta(\rho))$ [19, 20], which means that ρ-DIO do not perform any better than DIO in the asymptotic limit. Taking into consideration the operational gap between the operations DIO and ρ-DIO in single-shot transformations, the asymptotic result can be quite surprising, since it effectively shows that the advantage provided by ρ-DIO over DIO will be relatively minor and will disappear completely at the asymptotic level.

3.2 Dilution

Consider the case when one wants to transform a maximally coherent state Ψ_m into a general state ρ, using a Ψ_m-DIO protocol. The one-shot coherence cost is given by

$$C^{(1),\varepsilon}_{c,\Psi_m\text{-DIO}}(\rho) \coloneqq \log \min \left\{ m \,\middle|\, \max_{\Lambda \in \Psi_m\text{-DIO}} F(\Lambda(\Psi_m), \rho) \geq 1-\varepsilon \right\}.$$

To characterize this quantity, we will consider the coherence monotone [13]

$$R_\Delta(\omega) \coloneqq \min \left\{ \lambda \;\middle|\; \frac{\omega + \lambda\sigma}{1+\lambda} \in \mathcal{I},\ \sigma \in \mathbb{D},\ \Delta(\sigma) = \Delta(\rho) \right\}.$$

It is easy to verify that $\mathcal{R}_\Delta(\Lambda(\omega)) \leq R_\Delta(\omega)$ for any ω-DIO operation Λ. Using this quantity, we have the following.

Theorem 4 *The one-shot coherence cost under Ψ_m-DIO operations is given by* $C^{(1),\varepsilon}_{c,\Psi_m\text{-DIO}}(\rho) = \left\lceil \log \min \left\{ R_\Delta(\omega) + 1 \;\middle|\; \omega \in \mathbb{D},\ F(\rho,\omega) \geq 1-\varepsilon \right\} \right\rceil_{\log}$.

Interestingly, combining the above with the results obtained previously for DIO [18], we have that

$$C^{(1),\varepsilon}_{c,DIO}(\rho) = C^{(1),\varepsilon}_{c,\Psi_m\text{-DIO}}(\rho); \tag{4}$$

that is, the operations Ψ_m-DIO provide no advantage over DIO whatsoever. Combining this with the fact that the asymptotic coherence cost under DIO is given exactly by $S(\rho\|\Delta(\rho))$ [20], we have that the relative entropy between ρ and $\Delta(\rho)$ completely characterises the asymptotic transformations under ρ-DIO.

The monotone R_Δ can in fact characterize state transformations under ρ-DIO which go beyond coherence distillation and dilution; in particular, we have that if $R_\Delta(\omega) + 1 \leq 1/\operatorname{Tr}\rho\Delta(\rho)$, then there exists a ρ-DIO map such that $\Lambda(\rho) = \omega$. Several other conditions characterizing general transformations under ρ-DIO can be obtained in a similar way.

References

[1] A. Streltsov, G. Adesso, and M. B. Plenio, "Quantum coherence as a resource", Rev. Mod. Phys. **89**, 041003 (2017).

[2] J. Aberg, "Quantifying Superposition", (2006), arXiv:quant-ph/0612146.

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

[4] A. Winter and D. Yang, "Operational resource theory of coherence", Phys. Rev. Lett. **116**, 120404 (2016).

[5] M. Horodecki and J. Oppenheim, "(Quantumness in the context of) Resource theories", Int. J. Mod. Phys. B **27**, 1345019 (2012).

[6] E. Chitambar and G. Gour, "Quantum Resource Theories", (2018), arXiv:1806.06107.

[7] E. Chitambar and G. Gour, "Critical examination of incoherent operations and a physically consistent resource theory of quantum coherence", Phys. Rev. Lett. **117**, 030401 (2016).

[8] I. Marvian and R. W. Spekkens, "How to quantify coherence: Distinguishing speakable and unspeakable notions", Phys. Rev. A **94**, 052324 (2016).

[9] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement", Rev. Mod. Phys. **81**, 865–942 (2009).

[10] S. Du, Z. Bai, and X. Qi, "Coherence Measures and Optimal Conversion for Coherent States", Quantum Inf Comput **15**, 1307–1316 (2015).

[11] X. Yuan, H. Zhou, Z. Cao, and X. Ma, "Intrinsic randomness as a measure of quantum coherence", Phys. Rev. A **92**, 022124 (2015).

[12] B. Yadin, J. Ma, D. Girolami, M. Gu, and V. Vedral, "Quantum Processes Which Do Not Use Coherence", Phys. Rev. X **6**, 041028 (2016).

[13] E. Chitambar and G. Gour, "Comparison of incoherent operations and measures of coherence", Phys. Rev. A **94**, 052336 (2016).

[14] J. I. de Vicente and A. Streltsov, "Genuine quantum coherence", J. Phys. A: Math. Theor. **50**, 045301 (2017).

[15] Z.-W. Liu, X. Hu, and S. Lloyd, "Resource Destroying Maps", Phys. Rev. Lett. **118**, 060502 (2017).

[16] H. Zhu, M. Hayashi, and L. Chen, "Coherence and entanglement measures based on Rényi relative entropies", J. Phys. A: Math. Theor. **50**, 475303 (2017).

[17] A. Streltsov, S. Rana, P. Boes, and J. Eisert, "Structure of the Resource Theory of Quantum Coherence", Phys. Rev. Lett. **119**, 140402 (2017).

[18] Q. Zhao, Y. Liu, X. Yuan, E. Chitambar, and X. Ma, "One-Shot Coherence Dilution", Phys. Rev. Lett. **120**, 070403 (2018).

[19] B. Regula, K. Fang, X. Wang, and G. Adesso, "One-Shot Coherence Distillation", Phys. Rev. Lett. **121**, 010401 (2018).

[20] E. Chitambar, "Dephasing-covariant operations enable asymptotic reversibility of quantum resources", Phys. Rev. A **97**, 050301 (2018).

[21] D. Egloff, J. M. Matera, T. Theurer, and M. B. Plenio, "Of Local Operations and Physical Wires", Phys. Rev. X **8**, 031005 (2018).

[22] K. Fang, X. Wang, L. Lami, B. Regula, and G. Adesso, "Probabilistic Distillation of Quantum Coherence", Phys. Rev. Lett. **121**, 070404 (2018).

[23] T. Theurer, D. Egloff, L. Zhang, and M. B. Plenio, "Quantifying the Coherence of Operations", (2018), arXiv:1806.07332.

[24] B. Regula, L. Lami, and A. Streltsov, "Nonasymptotic assisted distillation of quantum coherence", Phys. Rev. A **98**, 052329 (2018).

[25] Q. Zhao, Y. Liu, X. Yuan, E. Chitambar, and A. Winter, "One-Shot Coherence Distillation: The Full Story", (2018), arXiv:1808.01885.

[26] L. Lami, B. Regula, and G. Adesso, "Generic Bound Coherence under Strictly Incoherent Operations", Phys. Rev. Lett. **122**, 150402 (2019).

[27] L. Lami, "Completing the Grand Tour of asymptotic quantum coherence manipulation", ArXiv190202427 Math-Ph Physicsquant-Ph (2019), arXiv:1902 . 02427 [math-ph, physics:quant-ph].

[28] S. Meznaric, S. R. Clark, and A. Datta, "Quantifying the Nonclassicality of Operations", Phys. Rev. Lett. **110**, 070502 (2013).

[29] T. Biswas, M. García Díaz, and A. Winter, "Interferometric visibility and coherence", Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **473**, 20170170 (2017).

[30] M. A. Nielsen, "Conditions for a Class of Entanglement Transformations", Phys. Rev. Lett. **83**, 436–439 (1999).

[31] S. Du, Z. Bai, and Y. Guo, "Conditions for coherence transformations under incoherent operations", Phys. Rev. A **91**, 052120 (2015).

[32] H. Zhu, Z. Ma, Z. Cao, S.-M. Fei, and V. Vedral, "Operational one-to-one mapping between coherence and entanglement measures", Phys. Rev. A **96**, 032316 (2017).

[33] K. Bu and C. Xiong, "A note on cohering power and de-cohering power", Quant. Inf. Comput. **13**, 1206 (2017), arXiv:1604.06524.

[34] K. Korzekwa, C. T. Chubb, and M. Tomamichel, "Avoiding Irreversibility: Engineering Resonant Conversions of Quantum Resources", Phys. Rev. Lett. **122**, 110403 (2019).

[35] C. T. Chubb, M. Tomamichel, and K. Korzekwa, "Moderate deviation analysis of majorization-based resource interconversion", Phys. Rev. A **99**, 032332 (2019).

[36] B. Morris and G. Adesso, "Quantum coherence fluctuation relations", J. Phys. A: Math. Theor. **51**, 414007 (2018).

[37] F. Buscemi, "Comparison of Quantum Statistical Models: Equivalent Conditions for Sufficiency", Commun. Math. Phys. **310**, 625–647 (2012).

[38] F. Buscemi and G. Gour, "Quantum relative Lorenz curves", Phys. Rev. A **95**, 012110 (2017).

[39] J. M. Renes, "Relative submajorization and its use in quantum resource theories", Journal of Mathematical Physics **57**, 122202 (2016).

[40] M. Tomamichel and M. Hayashi, "A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks", IEEE Trans. Inf. Theory **59**, 7693–7710 (2013).

[41] T. Ogawa and H. Nagaoka, "Strong converse and Stein's lemma in quantum hypothesis testing", IEEE Trans. Inf. Theory **46**, 2428–2433 (2000).

[42] T. Ogawa and M. Hayashi, "On error exponents in quantum hypothesis testing", IEEE Trans. Inf. Theory **50**, 1368–1372 (2004).

Accuracy enhancing protocols for quantum clocks

Yuxiang Yang, Lennart Baumgärtner, Ralph Silva, and Renato Renner
Institute for Theoretical Physics, ETH Zürich, Switzerland

The accuracy of the time information generated by clocks can be enhanced by allowing them to communicate with each other. Here we consider a basic scenario where a quantum clock receives a low-accuracy time signal as input and ask whether it can generate an output of higher accuracy. We propose protocols that, using a clock with a d-dimensional state space, achieve an accuracy enhancement by a factor d (in the limit of large d). If no feedback on the input signal is allowed, this enhancement is temporary. Conversely, with feedback, the accuracy enhancement can be retained for longer. The protocols may be used to synchronise clocks in a network and define a time scale that is more accurate than what can be achieved by non-interacting clocks.

For the full article, see arXiv:1905.09707.

That progress in quantum technologies is commonly accompanied by progress in high-precision time-keeping, as witnessed again recently [1, 13, 14], is not a coincidence. There are indeed fundamental reasons why the use of quantum phenomena enables more accurate time measurements than purely classical means [2, 9]. One of these reasons is of information-theoretic nature — a quantum clock with a d-dimensional state space can hold $\log_2 d$ qubits of information about time, whereas a corresponding classical clock only holds $\log_2 d$ classical bits.

From the viewpoint of information theory, it is natural to study clocks both individually and in scenarios where multiple clocks can communicate with each other and hence exchange information about time. This is practically relevant, since networks of clocks are commonly used to define a time scale that is more reliable than what any individual clock could achieve.[1] Furthermore, it is known that the accuracy of frequency measurements can be enhanced with correlated quantum systems [2, 9]. In future networks of quantum clocks, this fact may be exploited to define a highly accurate global time scale [11].

Here we study a basic task that a clock may carry out within such a communication scenario: the enhancement of time information (see Fig. 1). More precisely, we consider a setup where one clock, the *Enhancing Clock (EC)*, receives information from another clock about what time it is. Combining this input with internal information, the EC is supposed to output more accurate information about what time it is. For this, it may also send feedback to the clock that generates the input. We note that, while this scenario merely involves two clocks, it serves as a building block for larger clock networks.

The concept of enhancing time information also plays a crucial role for operating individual high-precision clocks, such as atomic clocks [4, 13, 14]. In a caesium clock, for instance, one may regard the gas of caesium atoms as the EC, which receives an input, in the form of a microwave signal, from an electronic oscillator (e.g., a crystal oscillator), and also feedbacks to this oscillator. Radio clocks also fall into this scheme. They receive time signals sporadically (e.g., once an hour), which they use in combination with an internal quartz crystal to output a continuous time signal.

As already noted, the ability of clocks to generate accurate time information is related to their size, measured in terms of the dimension d of their state space — the larger d is, the more accurate the clock can be [17, 19]. In this work we show that this is also the case for the task of enhancing time information. Specifically, we propose protocols which allow an EC of size d to enhance the accuracy of an input signal up to a factor of d. These protocols make use of the effect that quantum systems can evolve in a reversible fashion without any dissipation, allowing them to outperform basic classical protocols.

Quantifying Accuracy — For our purposes, a clock is a quantum system that autonomously emits information about time. We suppose that this time information comes in the form of *ticks*, which subdivide time into

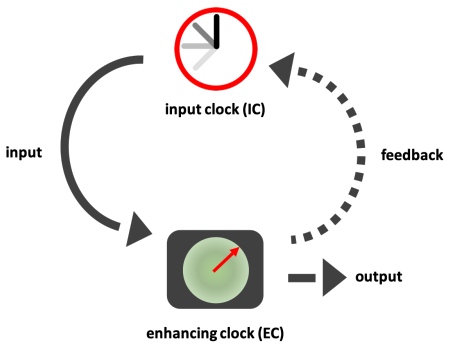


FIG. 1. **Accuracy enhancement.** The enhancing clock (EC) receives a clock signal from an input clock (IC) and produces an enhanced clock signal as output. The performance of the protocol can be further improved when feedback on the input clock is allowed.

[1] The International Atomic Time, which serves as a basis for the Coordinated Universal Time (UTC), is defined as an average of the reading of approximately 400 atomic clocks, with a weighting that depends on the measured stability of the individual clocks.

intervals [17].[2]

To motivate the definition that follows for an accuracy measure operationally, we note that the ticks emitted by a clock can be used to time-tag events. The tick that is generated before all the others is taken as a starting point, and we therefore refer to it as the 0-th tick. If an event occurred before the j-th tick, we tag it with "$j-1$", and if it occurs after, we tag it with "j". For a perfect clock, whose ticks occur at fixed times, this tagging is deterministic and, in this sense, unambiguous. This is no longer the case for an imperfect clock, where the exact emission time T_j of the j-th tick can be random. Nevertheless, we may define a $(1-\epsilon)$-confidence interval C_j of time for each tick j, demanding that C_j contains T_j except with a fixed probability $\epsilon > 0$. Whenever an event lies either before or after the interval C_j, the distinction between tag "$j-1$" and "j" would still be unambiguous with confidence at least $1-\epsilon$. Only events that occur within the interval C_j would be more likely to be classified erroneously.

Following this idea, we may introduce a family of *inaccuracy measures*, $\Sigma_j(\epsilon)$, parameterised by $\epsilon \in [0,1]$ and $j \in \mathbb{N}$. Roughly, Σ_j can be interpreted as the fraction of events for which the time tag "j" may be ambiguous, i.e., events that lie within the interval C_j, among all events that occur between the $(j-1)$-th and the j-th tick.

Definition 1 (Inaccuracy)**.** *For any desired* confidence level $1-\epsilon$*, the* ϵ-inaccuracy of the j-th tick *is defined as*

$$\Sigma_j(\epsilon) := \inf_{\substack{\mathsf{C}_j=[\mu-\frac{\sigma}{2},\mu+\frac{\sigma}{2}] \\ \Pr[T_j \notin \mathsf{C}_j] \leq \epsilon}} \frac{\sigma}{\mu/j} \ , \tag{1}$$

where the infimum ranges over intervals C_j *with any width* σ *and centre* μ *that contain the time* T_j *of the* j*-th tick with probability at least* $1-\epsilon$*.*

An important special case is that of an *i.i.d.* clock, where the time durations between ticks, i.e., the differences $T_j - T_{j-1}$, are *independent and identically distributed* for all $j \in \mathbb{N}$. The behaviour of an i.i.d. clock is thus fully defined by the distribution of the first tick. One can use the Hoeffding inequality to bound the inaccuracy of later ticks from the first, in particular for those distributions of T_1 that have bounded tails (e.g. sub-Gaussian).

Stable quantum clocks — Given an input clock signal, the goal of accuracy enhancement is to produce an output signal with as small inaccuracy as possible, using an enhancing clock (EC) as in Fig. 1. To model the EC, we extend the concept of autonomous clocks developed in [7, 8, 17, 18], which produce signals without an external time reference. An autonomous clock is characterised by two key ingredients: a finite-dimensional clock system (which can be either classical or quantum) that evolves continuously in time and a detector that *constantly* measures the clock system and produces ticks [17, 19]. In what follows, we will usually operate the clock as a *reset* clock as in [19], i.e., it shall admit the same state, called the *reset state*, after each tick.

We assume that the EC is an autonomous quantum clock equipped with a switch that determines whether the detector is on or off. In the first case, the dynamics of the clock, $\mathcal{D}_{\text{tick}}$, corresponds to that of the autonomous clock as defined in [17], i.e., the clock state is constantly measured and ticks can be produced. In the second case, the dynamics, $\mathcal{D}_{\text{no-tick}}$, corresponds to unitary evolution, i.e., the clock evolves periodically without any dissipation.

Our protocols for accuracy enhancement work for those clocks such as the *Quasi-Ideal Clocks* [18] which fulfil a *stability criterion*, which is a condition placed on a family of clocks of increasing dimension d. Details may be found in the arXiv version. In summary, one can imagine that a clock satisfying this criterion has a "hand" moving on a dial, with the detector located at one point. The criterion then demands that the clock ticks if and only if the hand is close the detector regardless of (a) how long the hand was evolving under $\mathcal{D}_{\text{no-tick}}$ and (b) where the hand started, as long as it did not start too closely to the detector.

The stability criterion is independent of the input signal and can be applied to any autonomous quantum clock. In particular, it is satisfied by Quasi-Ideal Clocks [18, 19]. These are the most accurate autonomous clocks for which analytical upper bounds on the inaccuracy have been calculated [18, 19]. Specifically, a Quasi-Ideal Clock of dimension d achieves a first-tick inaccuracy of $O(d^{-1+\nu})$ for any positive ν and for any confidence level $1-\epsilon < 1$ in the limit of large d.

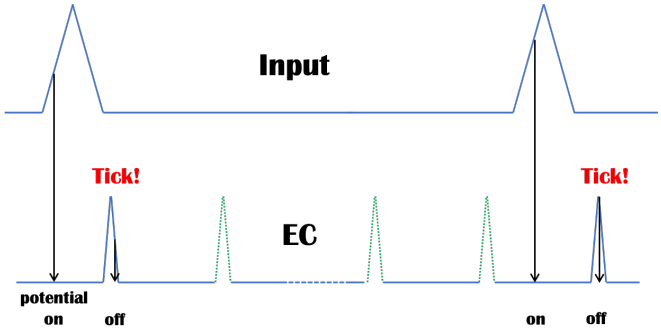
The accuracy enhancement protocol — This protocol requires a quantum EC satisfying the stability criterion discussed above. When we write that the clock is set to $(\Psi, \mathcal{D})$, we mean that the clock state is set to Ψ and the switch that controls the dynamics is set to $\mathcal{D} \in \{\mathcal{D}_{\text{tick}}, \mathcal{D}_{\text{no-tick}}\}$.

Protocol 1 Accuracy enhancement without feedback by controlling the EC's switch.

(Initialization) On receiving the first input tick, reset the EC to $(\Psi_0, \mathcal{D}_{\text{tick}})$.
1: **loop**
2: Wait for an EC tick.
3: Produce an output tick and set the EC to $(\Psi_0, \mathcal{D}_{\text{no-tick}})$.
4: Wait for an input tick.
5: Set the EC's dynamics to $\mathcal{D}_{\text{tick}}$.
6: **end loop**

See Fig. 2 for a visual explanation of this protocol. One sees there that the input signal uncertainty must

[2] Note that is conceptually distinct from the treatment of clocks in the context of metrology, which is common in the literature (see, for instance, Refs. [3, 10, 11]). A discussion on the same may be found in the full text.



(a)

FIG. 2. **Tick patterns of the input signal and the enhancing clock (EC) in Protocol 1.** The pikes mark intervals within which ticks occur with high probability. Here the protocol succeeds in generating accurate ticks, indicated in the lower half of the figure. The ticks of the input signal, which are shown in the upper half of the figure, are used to turn on the detector of the EC. The green dotted pikes correspond to ticks of the EC that are suppressed when it evolves unitarily.

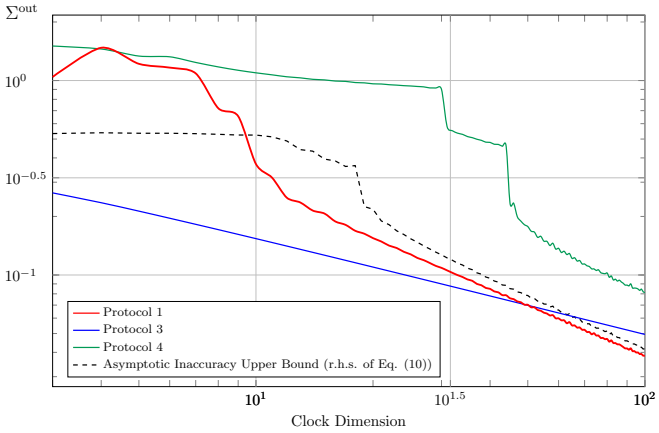


FIG. 3. **Numerical results for the performance of different accuracy enhancing protocols.** The graph shows the inaccuracy $\Sigma^{\text{out}} = \Sigma^{\text{out}}(\epsilon_0)$ for various protocols (Protocol 3 is described in the arXiv version). The input is assumed to be i.i.d. and box-shaped with $\Sigma^{\text{in}}(\epsilon) \approx 0.33$ and $\epsilon = 0.01$. The horizontal axis shows the dimension d of the EC in logarithmic scale. The confidence on the output is chosen to be the same as the one on the input, i.e. $\epsilon_0 = 0.01$. For both Protocol 1 and 4 the scaling is approximately proportional to d^{-1}, but the accuracy of the latter is worse. This may be compared to a basic protocol that simply bunches d ticks of the input signal together to one output tick (Protocol 3), whose inaccuracy scales like $d^{-\frac{1}{2}}$. The dotted line represents the asymptotic upper bound on the output inaccuracy, Eq. (2) (evaluated for an EC with tail probability $\epsilon^{\text{EC}_d} = 0.001$), which is seen to be close to tight already above $d \sim 20$.

fall within a single period of the EC. From this it can be argued that the minimal inaccuracy of the output signal (for the first tick) is approximately the product of the inaccuracies of the input signal and the EC. More precisely, for Quasi-Ideal Clocks of dimension d we are able to prove the following attainable enhancement,

Theorem 1. *Let the input clock be i.i.d. and such that* $\Sigma^{\text{in}}(\epsilon) < 2/3$*, and let the EC be a Quasi-Ideal Clock. Then, for any* $\epsilon_0 > \epsilon$*, for* $j < 2/(3\Sigma^{\text{in}}(\epsilon))$*, and for large enough* d*, the inaccuracy of the* j*-th output tick of Protocol 1 satisfies*

$$\Sigma_j^{\text{out}}(\epsilon_j) \leq \frac{5j^2}{3} \cdot \frac{\Sigma^{\text{in}}(\epsilon)}{d^{1-\nu}}. \tag{2}$$

This is a temporary enhancement, since the inaccuracy increases quadratically with the number of ticks. However, this can be eliminated if feedback on the input signal is allowed, by modifying step (3) of the above protocol to also include a reset to the initial state of the input clock.

Comparison to non-quantum protocols — The protocol is dependent upon the unitary evolution of the EC under $\mathcal{D}_{\text{no-tick}}$. We now present a protocol that does not require switching between different dynamics, and would work even for classical ECs. We find that accuracy enhancement is possible, but less than Protocol 1.

Protocol 4 Accuracy enhancement without controlling the dynamics of the enhancing clock.

1: **loop**
2: Wait for an input tick.
3: Wait for an EC tick.
4: Produce an output tick.
5: **end loop**

See Fig. 3 for a comparison of the performance of Protocols 1, 4 and another protocol detailed in the full text that also does not use switching dynamics.

Our protocols can be used as a subroutine of a highly accurate clock consisting of a macroscopic oscillator producing clock signals and a quantum system that further improves their accuracy. They may also be employed in a network setting to establish a common clock signal for multiple, and possible distant, nodes, which is crucial for various applications [5, 6, 12, 15]. Although each node may be equipped with a clock, these clocks suffer from random drifts as they produce more and more ticks without synchronisation. Our accuracy enhancing protocols, especially the one without feedback, fit this task well.

The task considered in this work can be regarded as signal processing [16], where an input signal is processed by a special-purpose system. The difference between the particular task of clock signal processing as considered here and general signal processing is that, in the former, no time reference other than the input signal is available. Common operations in signal processing, like time shifts, are therefore prohibited, which makes the task harder. Our work represents a first concrete step towards a theory of time signal processing by harnessing quantum mechanics.

[1] B. Bloom, T. Nicholson, J. Williams, S. Campbell, M. Bishof, X. Zhang, W. Zhang, S. Bromley, and J. Ye. An optical lattice clock with accuracy and stability at the 10- 18 level. *Nature*, 506(7486):71, 2014.

[2] J. J. . Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen. Optimal frequency measurements with maximally correlated states. *Phys. Rev. A*, 54:R4649–R4652, Dec 1996.

[3] V. Bužek, R. Derka, and S. Massar. Optimal quantum clocks. *Physical Review Letters*, 82(10):2207, 1999.

[4] A. Derevianko and H. Katori. Colloquium: Physics of optical lattice clocks. *Reviews of Modern Physics*, 83(2):331, 2011.

[5] J. Elson and D. Estrin. *Time synchronization for wireless sensor networks*. IEEE, 2001.

[6] J. Elson, L. Girod, and D. Estrin. Fine-grained network time synchronization using reference broadcasts. *ACM SIGOPS Operating Systems Review*, 36(SI):147–163, 2002.

[7] P. Erker. The quantum hourglass: approaching time measurement with quantum information theory. Master's thesis, ETH Zürich, 2014.

[8] P. Erker, M. T. Mitchison, R. Silva, M. P. Woods, N. Brunner, and M. Huber. Autonomous quantum clocks: does thermodynamics limit our ability to measure time? *Physical Review X*, 7(3):031022, 2017.

[9] S. F. Huelga, C. Macchiavello, T. Pellizzari, A. K. Ekert, M. B. Plenio, and J. I. Cirac. Improvement of frequency standards with quantum entanglement. *Phys. Rev. Lett.*, 79:3865–3868, Nov 1997.

[10] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams. Quantum clock synchronization based on shared prior entanglement. *Physical Review Letters*, 85(9):2010, 2000.

[11] P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin. A quantum network of clocks. *Nature Physics*, 10(8):582, 2014.

[12] L. Lamport. Time, clocks, and the ordering of events in a distributed system. *Communications of the ACM*, 21(7):558–565, 1978.

[13] A. D. Ludlow, M. M. Boyd, J. Ye, E. Peik, and P. O. Schmidt. Optical atomic clocks. *Reviews of Modern Physics*, 87(2):637, 2015.

[14] A. D. Ludlow, W. F. McGrew, X. Zhang, D. Nicolodi, R. J. Fasano, S. A. Schaffer, R. C. Brown, R. W. Fox, N. Hinkley, T. H. Yoon, and K. Beloy. Optical frequency measurements at 1×10^{-18} uncertainty with Ytterbium optical lattice clocks. In *2018 Conference on Precision Electromagnetic Measurements (CPEM 2018)*, pages 1–2, 2018.

[15] D. L. Mills. Internet time synchronization: the network time protocol. *IEEE Transactions on Communications*, 39(10):1482–1493, 1991.

[16] A. V. Oppenheim, A. S. Willsky, and S. H. Nawab. *Signals &Amp; Systems (2Nd Ed.)*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1996.

[17] S. Ranković, Y.-C. Liang, and R. Renner. Quantum clocks and their synchronisation - the alternate ticks game. *arXiv:1506.01373*, 2015.

[18] M. P. Woods, R. Silva, and J. Oppenheim. Autonomous quantum machines and finite-sized clocks. *Annales Henri Poincaré*, 20(1), 2019.

[19] M. P. Woods, R. Silva, G. Pütz, S. Stupar, and R. Renner. Quantum clocks are more accurate than classical ones. *arXiv:1806.00491*, 2018.

Noise-induced amplification: Parametric amplifiers cannot simulate all phase-preserving linear amplifiers

A. Chia[1] * M. Hajdušek[1] R. Nair[2 3] R. Fazio[1 4] L. C. Kwek[1] V. Vedral[1 5]

[1] *Centre for Quantum Technologies, National University of Singapore.*
[2] *School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.*
[3] *Complexity Institute, Nanyang Technological University, Singapore.*
[4] *ICTP, Strada Costiera, Trieste, Italy.*
[5] *Department of Physics, University of Oxford, UK.*

Abstract. A deterministic quantum linear amplifier must add noise to its input. Here we show how an amplifier, while being linear and phase-preserving, overturns the following two important and widely accepted beliefs in the literature: (i) Noise added internally by the amplifier is purely deleterious, the sole purpose of which is to impose quantum theory. (ii) A phase-preserving linear amplifier, no matter how it is physically realised, can be simulated by a parametric amplifier [C. M. Caves *et al.*, Phys. Rev. A **86**, 063802 (2012)].

Keywords: linear amplifiers, quantum noise, quantum optics

Linear amplification has long been an integral part of quantum measurements whereby a weak signal is amplified to a detectable level [1, 2]. In more recent times, due to advances in quantum optics and quantum information, linear amplifiers are also seen as a facilitating component of many useful tasks such as state discrimination [3], quantum feedback [4], metrology [5], and entanglement distillation [6, 7].

Quantum mechanics commands any linear amplifier to add noise to its input [8]. Such noisy amplification of a single bosonic input can be modelled by a linear differential equation for its amplitude (annihilation operator) of the form

$$\frac{d}{dt}\,\hat{a}(t) = \kappa\,\hat{a}(t) + \hat{f}(t)\;, \tag{1}$$

where κ is the amplification rate (a positive real number), and $\hat{f}(t)$ represents noise added by the amplifier (or internal noise). Generally $\hat{f}(t)$ is assumed to be a zero-mean Markov process. It is due to amplifier degrees of freedom. The time-dependent solution $\hat{a}(t)$ to (1) — often at a designated time instant — is defined as the output of the amplifier corresponding to the input $\hat{a}(0)$. The ultimate performance of a linear amplifier is thus determined by the least amount of noise that it must add consistent with quantum theory. Such quantum-limited performance of linear amplifiers had been studied as early as the 1960s for phase-preserving amplifiers [9, 10]. These results were later unified, and further generalised to phase-sensitive amplifiers by Caves [11].

It is a long held belief that amplifier-added noise is nothing but mere nuisance. This view has motivated noise-reduction methods in linear amplifiers [12, 13, 14], or methods which evade it altogether by trading the amplifier's deterministic operation for noiseless gain [15, 16, 17]. It should not come as a surprise that amplifier-added noise is viewed as something purely negative since it has not been shown to behave otherwise in all known examples of linear amplifiers to date. In fact, the ubiquity of such added noise in linear amplifiers has led Caves *et al.* to argue that any phase-preserving linear amplifier, no matter how it is realised, is equivalent to a parametric amplifier (paramp) [18]. An implicit caveat for this to be true, as we will show, is that the added noise be independent of the signal (though it may not be obvious how other kinds of noise would arise). In other words, conventional wisdom regards the amplifier noise to be only additive [19], neglecting the possibility that it may also be multiplicative or otherwise.

In this work[1], we show how multiplicative noise may arise in phase-preserving linear amplifiers and that this has two very important implications for the theory of linear amplifiers: (i) Such noise serves to impose quantum mechanics on the amplifier and *simultaneously* amplify an input signal. This is in stark contrast to the conventional view that the sole function of added noise is to enforce quantum theory. (ii) It violates the equivalence of phase-preserving linear amplifiers to the paramp model claimed in Ref. [18]. To the best of our knowledge, this is the first time that a phase-preserving linear amplifier has been shown to fall outside the scope of the paramp. This finding advances the current understanding of linear amplifiers, showing that a complete theory of noise in phase-preserving amplifiers remains to be found.

A further implication of our result is that the paramp cannot be programmed to emulate an arbitrary linear phase-preserving amplifier. Programmability is a concept in quantum information which captures the idea that one can "reconfigure" parts of a quantum device in order to simulate another quantum device insofar as their outputs are concerned (see Sec. 3 for a precise definition of programmability) [21]. The main result of Ref. [18] may then be restated in (quantum) information theoretic terms as conjecturing that a paramp can be programmed to out-

*photonicboy@gmail.com

[1] See arXiv:1903.09370 (https://arxiv.org/abs/1903.09370).

put a state identical to the state outputted by any linear phase-preserving amplifier (which is shown to be incorrect in Sec. 2 and is the sense in which "simulate" is used in our paper title).

1 Noise-induced amplification

If we demand that amplification be linear and the result of noise alone, then the average of the added noise can no longer be zero because linear amplification requires the average amplitude $\langle\hat{a}\rangle$ to satisfy $d\langle\hat{a}\rangle/dt = \gamma\,\langle\hat{a}\rangle$ with γ being positive (and real if it is to be phase preserving [11, 18]). We show that this is possible when

$$\frac{d}{dt}\,\hat{a}(t) = \hat{a}^\dagger(t)\,\hat{w}(t)\;. \tag{2}$$

That is, it is possible to choose a noise process $\hat{w}(t)$ that ensures $[\hat{a}(t), \hat{a}^\dagger(t)] = \hat{1}$ for all t, and simultaneously satisfies the requirement for amplification

$$\left\langle \hat{a}^\dagger(t)\,\hat{w}(t)\right\rangle = \gamma\,\left\langle \hat{a}(t)\right\rangle\;, \tag{3}$$

where $\gamma \geq 0$. Unlike the 'signal-plus-noise' model of (1), the noise in (2) is multiplicative but otherwise $\hat{w}(t)$ itself may be treated as zero-mean and Markovian, just like $\hat{f}(t)$ in (1). We refer to (2) and (3) as noise-induced amplification ("noisi amplification"), and to the amplifier as a "noisiamp". The amplitude gain of the noisiamp is $g(t) = \langle\hat{a}(t)\rangle/\langle\hat{a}(0)\rangle = \exp(\gamma\,t)$.

The model of (2) and (3) can be realised by using a gain medium that mediates two-photon interactions. An effective model for this is an interaction Hamiltonian that couples a single bosonic mode (representing the signal) to a collection of two-level atoms via two-photon exchanges in the rotating-wave approximation. One can show, that such an interaction Hamiltonian within the Born–Markov approximation leads to (2) on setting the excited-state and ground-state atomic populations equal. The operator $\hat{w}(t)$ is then realised by a weighted sum over the Pauli lowering operators for each atom (the weights being coupling constants). The detailed derivation of (2) and (3) is left to Ref. [20]. In Ref. [20] we have also found the underlying atom-photon interactions responsible for noisi amplification [shown in Fig. 1(b), where it is contrasted to a model of (1) realised using atom-photon interactions]. This explains, in physical terms, how an inherently nonlinear interaction (i.e. a two-photon process) can result in linear amplification which is usually associated with one-photon processes.

Noisi amplification can be understood as classical correlation between the internal noise source of the amplifier and the signal that is being amplified. This is the essential content of (3). Though such equations are not typically encountered in the amplifier literature, it is certainly allowed within the Born–Markov framework. The important point to note here is that the Markov approximation does not treat $\hat{w}(t)$ as truly white. All that is required is for $\hat{w}(t)$ to have a small but nonzero correlation time, otherwise (3) would be zero and there would be no amplification. In other words, if there is no correlation between the noise and signal, there is no amplification.

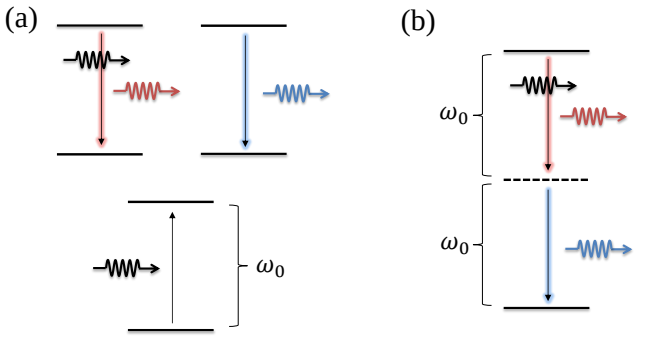


Figure 1: (a) Fundamental atom-photon interactions which realise the linear amplifier of (1). The amplifier derives its gain from population inversion in the atoms. Photons emitted spontaneously contribute to noise and are shown in blue while stimulated ones contribute to the signal and are in red (with the original signal photon shown in black). (b) Elementary atom-photon interaction responsible for the linear gain of the noisiamp in (2): A two-photon emission with one of the emitted photons being stimulated and one spontaneous via an intermediate virtual level. See Ref. [20] for a more complete description.

2 Inequivalence to the paramp

A paramp has two inputs, $\hat{a}$ and $\hat{b}$. The input mode $\hat{a}$ represents the signal amplitude to be amplified and acts on Hilbert space $\mathbb{H}_{\rm A}$. Mode $\hat{b}$ is an ancillary system acting on $\mathbb{H}_{\rm B}$ and whose initial state is σ. If we assume the signal mode to be prepared in an initial state $\rho(0)$, then the paramp output in the Schrödinger picture is defined by

$$\rho(t) = \mathcal{E}(t)\,\rho(0) = {\rm Tr}_{\rm B}\left[\hat{S}(t)\,\rho(0)\otimes\sigma\,\hat{S}^\dagger(t)\right]\;. \tag{4}$$

Here ${\rm Tr}_{\rm B}$ denotes a partial trace over $\mathbb{H}_{\rm B}$ and $\hat{S}(t) = \exp[\kappa\,(\hat{a}\,\hat{b} - \hat{a}^\dagger\hat{b}^\dagger)\,t]$ where $\kappa \geq 0$ (see also Fig. 2). In Ref. [18], it was asserted that any phase-preserving linear amplifier, no matter how it is physically realised, is always equivalent to the paramp for some (κ, t) (which determines its amplitude gain), and a physical choice of σ, thus leading to a complete classification of such amplifiers. We have analysed in Ref. [20] the phase properties of the noisiamp to show that it satisfies all the assumptions required in Ref. [18] to fall under the ambit of the paramp model. We now show that, despite this, the noisiamp is irreproducible by a paramp as illustrated in Fig. 2.

For the paramp to be equivalent to the noisiamp, it is necessary that moments of the output $\hat{a}(t)$ from the paramp be identical to the moments of $\hat{a}(t)$ from the noisiamp for an arbitrary input state $\rho(0)$ sent into both types of amplifiers. Now we show that this cannot be satisfied by considering the output amplitude and photon number corresponding to both types of amplifiers. For

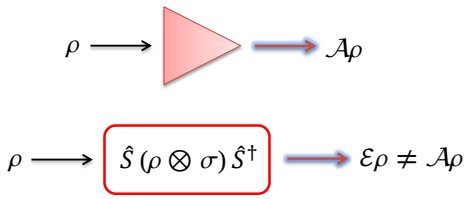


Figure 2: Top: An arbitrary phase-preserving linear amplifier described by the map $\mathcal{A}$. The input is shown in black while the output (the amplified signal) is shown in red. The added noise due to the internal physics of the amplifier is shown as the blurry blue outline on the output. Bottom: Paramp model—Ref. [18] argues that regardless of the amplifier's internal physics, they may all be thought of as a two-mode squeezing operation with an appropriately chosen $\hat{S}$ and σ. The noisiamp of this paper is a counterexample to this.

the noisiamp they are [20]

$$\langle \hat{a}(t) \rangle = g \langle \hat{a}(0) \rangle \, , \tag{5}$$

$$\langle \hat{n}(t) \rangle = g^4 \langle \hat{n}(0) \rangle + \frac{g^4 - 1}{2} \, . \tag{6}$$

The same quantities for the paramp are

$$\langle \hat{a}(t) \rangle = G \langle \hat{a}(0) \rangle + \sqrt{G^2 - 1} \, \langle \hat{b}(0) \rangle \, , \tag{7}$$

$$\langle \hat{n}(t) \rangle = G^2 \langle \hat{n}(0) \rangle + \left(G^2 - 1 \right) \langle \hat{b}(0) \, \hat{b}^\dagger(0) \rangle \, . \tag{8}$$

where $G = \cosh(\kappa \, t)$. Note that all initial moments for the ancillary mode are taken with respect to σ while those for the signal mode are taken with respect to $\rho(0)$. By linearity one must choose, $\langle \hat{b}(0) \rangle = 0$ for the paramp. To ensure the two amplifiers give identical $\langle \hat{a}(t) \rangle$ we must also set $G = g$. Now consider an input signal prepared in some state, say ρ_1 with average photon number $\langle \hat{n}(0) \rangle_1$. It is necessary that the noisiamp output the same photon number as the paramp corresponding to this input, i.e.

$$g^4 \langle \hat{n}(0) \rangle_1 + \frac{g^4 - 1}{2} = g^2 \langle \hat{n}(0) \rangle_1 + \langle \hat{b}(0) \, \hat{b}^\dagger(0) \rangle \, . \tag{9}$$

Similarly we may consider another input state ρ_2 with a different average photon number $\langle \hat{n}(0) \rangle_2$. The same requirement leads to

$$g^4 \langle \hat{n}(0) \rangle_2 + \frac{g^4 - 1}{2} = g^2 \langle \hat{n}(0) \rangle_2 + \langle \hat{b}(0) \, \hat{b}^\dagger(0) \rangle \, . \tag{10}$$

Subtracting (10) from (9) we get

$$g^4 \left[\langle \hat{n}(0) \rangle_1 - \langle \hat{n}(0) \rangle_2 \right] = g^2 \left[\langle \hat{n}(0) \rangle_1 - \langle \hat{n}(0) \rangle_2 \right] \, . \tag{11}$$

Equation (11) clearly cannot be satisfied unless $g = 1 = G$ (which means no amplification). Thus, the paramp cannot be a universal model for all phase-preserving linear amplifiers. Note that it is the difference in how $\langle \hat{n}(t) \rangle$ scales with g in the two types of amplifiers that makes the paramp and noisiamp inequivalent. The noisiamp is the first counterexample known to date that violates the conjecture of Ref. [18]. A second counterexample is given in Ref. [20].

3 Programmability

Interestingly the claimed universality of the paramp model of Ref. [18] can be understood in terms of the concept of programmability defined for a set of maps [21]. A family of completely-positive maps $\{\Phi_k\}_k$ acting on $\rho \in \mathbb{H}_\mathrm{S}$ is defined to be programmable if and only if there exist a set of states $\{\sigma_k\}_k$ ($\sigma_k \in \mathbb{H}_\mathrm{B}$) and a fixed unitary $\hat{U}$ (independent of k) acting on $\mathbb{H}_\mathrm{S} \otimes \mathbb{H}_\mathrm{B}$ such that

$$\Phi_k \rho = \mathrm{Tr}_\mathrm{B}[\hat{U}(\rho \otimes \sigma_k)\hat{U}^\dagger] \, . \tag{12}$$

If we let $\{\Phi_k\}_k$ describe the set of phase-preserving linear amplifiers with a common gain, then we see that Ref. [18] may be understood as claiming $\{\Phi_k\}_k$ to be programmable by a paramp i.e. with $\hat{U} = \hat{S}$ [two-mode squeezing with a fixed $\kappa \, t$, defined underneath (4)]. We have thus shown that there are in fact some phase-preserving linear amplifiers (namely ones with multiplicative noise) that a paramp cannot be programmed to simulate.

References

[1] C. M. Caves, K. S. Thorne, R. W. P. Drever, V. D. Sandberg, and M. Zimmermann. On the measurement of a weak classical force coupled to a quantum-mechanical oscillator. I. Issues of principle. Rev. Mod. Phys. **52**, 341 (1980).

[2] A. A. Clerk, M. H. Devoret, S. M. Girvin, F. Marquardt and R. J. Schoelkopf. Introduction to quantum noise, measurement, and amplification. Rev. Mod. Phys. **82**, 1155 (2010).

[3] A. Zavatta, J. Fiurášek, and M. Bellini. A high-fidelity noiseless amplifier for quantum light states. Nat. Photon. **5**, 52 (2010).

[4] R. Vijay, C. Macklin, D. H. Slichter, S. J. Weber, K. W. Murch, R. Naik, A. N. Korotkov, and I. Siddiqi. Stabilizing Rabi oscillations in a superconducting qubit using quantum feedback. Nature **490**, 77 (2012)

[5] F. Hudelist, J. Kong, C. Liu, J. Jing, Z. Y. Ou, and W. Zhang. Quantum metrology with parametric amplifier-based photon correlation interferometers. Nat. Comm. **5**, 3049 (2014).

[6] T. C. Ralph and A. P. Lund. Nondeterministic noiseless linear amplification of quantum systems. In *Proceedings of the 9th International Conference on Quantum Communication Measurement and Computing, (A. Lvovsky Ed.)*, 155, (AIP, 2009).

[7] G. Y. Xiang, T. C. Ralph and N. Walk and G. J. Pryde. Heralded noiseless linear amplification and distillation of entanglement. Nat. Photon. **4**, 316 (2010).

[8] S. Stenholm. The theory of quantum amplifiers. Physica Scripta, **T12**, 56 (1986).

[9] H. A. Haus and J. A. Mullen. Quantum noise in linear amplifiers. Phys. Rev. **62**, 2407 (1962).

[10] H. Heffner. The fundamental noise limit of linear amplifiers. Proc. IRE **50**, 1604 (1962).

[11] C. M. Caves. Quantum limits on noise in linear amplifiers. Phys. Rev. D **26**, 1817 (1982).

[12] G. J. Milburn, M. L. Steyn-Ross, and D. F. Walls. Linear amplifiers with phase-sensitive noise. Phys. Rev. A **35**, 4443 (1987).

[13] Z. Y. Ou, S. F. Pereira, and H. J. Kimble. Quantum noise reduction in optical amplification. Phys. Rev. Lett. **70**, 3239 (1993).

[14] J. Kong, F. Hudelist, Z. Y. Ou, and W. Zhang. Cancellation of internal quantum noise of an amplifier by quantum correlation. Phys. Rev. Lett. **111**, 033608 (2013).

[15] J. Combes, N. Walk, A. P. Lund, T. C. Ralph, and C. M. Caves. Models of reduced-noise, probabilistic linear amplifiers. Phys. Rev. A **93**, 052310 (2016).

[16] R. Blandino, M. Barbieri, P. Grangier, and R. Tualle-Brouri. Heralded noiseless linear amplification and quantum channels. Phys. Rev. A **91**, 062305 (2015).

[17] J. Ho, A. Boston, M. Palsson, and G. J. Pryde. Experimental noiseless linear amplification using weak measurements. New J. Phys. **18**, 093026 (2016).

[18] C. M. Caves, J. Combes, Z. Jiang, and S. Pandey. Quantum limits on phase-preserving linear amplifiers. Phys. Rev. A **86**, 063802 (2012).

[19] K. Jacobs, *Stochastic Processes for Physicists: Understanding Noisy Systems*, (Cambridge University Press, 2010).

[20] A. Chia, M. Hajdušek, R. Nair, R. Fazio, L. C. Kwek, and V. Vedral. Noise-induced amplification: Parametric amplifiers cannot simulate all phase-preserving linear amplifiers. arXiv:1903.09370.

[21] M. Hillery, M. Ziman, and V. Bužek. Implementation of quantum maps by programmable processors. Phys. Rev. A **66**, 042302 (2002).

Coherence time of single qubit, scalable global gate and quantum error mitigation with trapped ions

Kihwan Kim[1] *

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

Abstract.

In this talk, I discuss our experimental developments for the quantum computation with trapped ions. The performance of a physical quantum device can be evaluated by the three criteria, which are the coherence time of a qubit, the fidelity of a logical gate, and number of qubits involved in coherent operations.

We have demonstrated the coherence time of a single $^{171}Yb^{+}$ ion-qubit over 600 s with sympathetic cooling by a $^{138}Ba^{+}$ ion and optimized dynamical decoupling-pulses in an ambient magnetic field condition [1]. Recently, we experimentally investigate the limiting factors and enhance the coherence time to more than twice. We find that ambient magnetic-field noise and phase noise of the local oscillator are main sources for decoherence. To suppress field fluctuation, we enclose our vacuum system with a two-layer μ-metal magnetic-shielding and use a permanent magnets to produce stable field. In this way, we observe the coherence time of field-sensitive qubit is increased to more than 30 ms. For the reference of the local oscillator, we use a crystal oscillator, which has one order of magnitude smaller Allan deviation than our previous Rb clock at 1 s. With such improvements, we observe the enhancement for the coherence time of clock state of $^{171}Yb^{+}$ ion.

We also have developed a five-qubit programmable system and realized a global quantum gate. A quantum algorithm can be decomposed into a sequence consisting of single qubit and 2-qubit entangling gates. To optimize the decomposition and achieve more efficient construction of the quantum circuit, we can replace multiple 2-qubit gates with a single global entangling gate. Here, we propose and implement a scalable scheme to realize the global entangling gates on multiple $^{171}Yb^{+}$ ion qubits by coupling to multiple motional modes through external fields. Such global gates require simultaneously decoupling of multiple motional modes and balancing of the coupling strengths for all the qubit-pairs at the gate time. To satisfy the complicated requirements, we develop a trapped-ion system with fully-independent control capability on each ion, and experimentally realize the global entangling gates. As examples, we utilize them to prepare the Greenberger-Horne-Zeilinger (GHZ) states in a single entangling operation, and successfully show the genuine multi-partite entanglements up to four qubits with the state fidelities over 93.4 % [2].

For the improvements of logic gate fidelities, we apply a scheme of quantum error mitigation based on probabilistic error cancellation [3], which requires no additional qubit resources different from the scheme of quantum error correction. We benchmark the performance of the protocol of the probabilistic error cancellation in our trapped-ion system. We clearly observe that effective gate fidelities exceed physical fidelities. The error rates are effectively reduced from $(1.10 \pm 0.12) \times 10^{-3}$ to $(1.44 \pm 5.28) \times 10^{-5}$ and from $(0.99 \pm 0.06) \times 10^{-2}$ to $(0.96 \pm 0.10) \times 10^{-3}$ for single- and two-qubit gates, respectively [4]. We believe our demonstration opens up the possibility of implementing high-fidelity computations on a near-term noisy quantum device.

References

[1] Ye Wang, Mark Um, Junhua Zhang, Shuoming An, Ming Lyu, Jing-Ning Zhang, L.-M. Duan, Dahyun Yum, and Kihwan Kim. Single-qubit quantum memory exceeding ten-minute coherence time. *Nature Photon.*, 11(10): 646, 2017.

[2] Yao Lu, Shuaining Zhang, Kuan Zhang, Wentao Chen, Jialiang Zhang, Jing-Ning Zhang and Kihwan Kim Global entangling gates on arbitrary ion qubits. *arXiv:1901.03508*, 2019. Accepted to Nature.

[3] Y. Li, S. C. Benjamin, Efficient Variational Quantum Simulator Incorporating Active Error Minimization *Phys. Rev. X*, 7:021050, 2017.

[4] Shuaining Zhang, Yao Lu, Kuan Zhang, Wentao Chen, Ying Li, Jing-Ning Zhang, and Kihwan Kim Error-Mitigated Quantum Gates Exceeding Physical Fidelities in a Trapped-Ion System *arXiv:1905.10135*, 2019.

*kimkihwan@mail.tsinghua.edu.cn