Asian
Quantum
Information
Science Conference **2023**

Abstract Booklet

TALKS

August 28 - September 1, 2023

Venue: KIAS, Seoul, Korea

Hosted by KIAS (Korea Institute for Advanced Study)

Program Committee

Divesh Aggarwal (National University of Singapore)
Hiroo Azuma (National Institute of Informatics)
Koji Azuma (NTT Basic Research Laboratories)
Joonwoo Bae (Korea Advanced Institute of Science and Technology)
Konrad Banaszek (University of Warsaw)
Jeongho Bang (Electronics and Telecommunications Research Institute)
Salman Beigi (Institute for Research in Fundamental Sciences)
Anthony Brady (University of Arizona)
Taeyoung Choi (Ewha Womans University)
Eleni Diamanti (CNRS / Sorbonne Université)
Dawei Ding (Alibaba)
Kun Fang (Baidu Research)
Hartmut Haeffner (University of California, Berkeley)
Sang-Wook Han (Korea Institute of Science and Technology)
Zoe Holmes (École Polytechnique Fédérale de Lausanne)
Karol Horodecki (University of Gdansk)
Zixin Huang (Macquarie University)
Joonsuk Huh (Sungkyunkwan University)
Aeysha Khalique (National University of Sciences and Technology, Pakistan)
Jehyung Kim (Ulsan National Institute of Science & Technology)
Junki Kim (Sungkyunkwan University)
Yong-Su Kim (Korea Institute of Science and Technology)
Yosep Kim (Korea Institute of Science and Technology)
Hyukjoon Kwon (Korea Institute for Advanced Study)
Felix Leditzky (University of Illinois Urbana-Champaign)
Changhyoup Lee (Korea Research Institute of Standards and Science)
Donghun Lee (Korea University)
Seung-Woo Lee (Korea Institute of Science and Technology, Co-Chair)
Anthony Leverrier (INRIA Paris)
Hyang-Tag Lim (Korea Institute of Science and Technology)
Jin-Guo Liu (Hong Kong University of Science and Technology – GuangZhou)
Chao-Yang Lu (University of Science and Technology of China)
Xiongfeng Ma (Tsinghua University)
Prabha Mandayam (Indian Institute of Technology Madras)
Hemant Mishra (Cornell University)
Yoshifumi Nakata (Kyoto University)
Hui Khoon Ng (Yale-NUS College / National University of Singapore)
Chinmay Nirkhe (IBM)
Harumichi Nishimura (Nagoya University)
Irina Novikova (College of William and Mary)
Daniel Kyungdeock Park (Yonsei University)
Hee Su Park (Korea Research Institute of Standards and Science)

Young-Sik Ra (Korea Advanced Institute of Science and Technology)
Marina Radulaski (University of California Davis)
Bartosz Regula (RIKEN)
Hoon Ryu— (Korea Institute of Science and Technology Information)
Junghee Ryu (Korea Institute of Science and Technology Information)
Ilya Sinayskiy (University of KwaZulu-Natal)
Young-Ik Sohn (Korea Advanced Institute of Science and Technology)
Ryuji Takagi (Nanyang Technological University)
Masahiro Takeoka (Keio University)
Ting Rei Tan (University of Sydney)
Seiichiro Tani (NTT Communication Science Laboratories)
Geza Toth (University of the Basque Country / Wigner Research Centre for Physics)
Vilasini Venkatesh (ETH Zurich)
Qisheng Wang (Nagoya University)
Xin Wang (Hong Kong University of Science and Technology – Guangzhou)
Mark M. Wilde (Cornell University, Chair)
Feihu Xu (University of Science and Technology of China)
Naoki Yamamoto (Keio University)
Xiao Yuan (Peking University)
Bei Zeng (Hong Kong University of Science and Technology)
Qi Zhao (University of Hong Kong)
Hongyi Zhou (Tsinghua University)
You Zhou (Fudan University)

Steering Committee

Charles Bennett (IBM)
Jozef Gruska (Masaryk University)
Guang-Can Guo (University of Science and Technology of China)
Hiroshi Imai (University of Tokyo, ex-Chair)
Richard Jozsa (University of Cambridge)
Jaewan Kim (Korea Institute for Advanced Study, Chair)
Shigeru Yamashita (Ritsumeikan, Secretary)

Organizing Committee

Jaewan Kim (Korea Institute for Advanced Study, Chair)
Soojoon Lee (Kyung Hee University)
Seung-Woo Lee (Korea Institute of Science and Technology)
Eunok Bae (Korea Institute for Advanced Study)
Minki Hhan (Korea Institute for Advanced Study)
Hyukjoon Kwon (Korea Institute for Advanced Study)
Youngrong Lim (Korea Institute for Advanced Study)
Ki Hyuk Yee (Korea Institute for Advanced Study)
Jieun Jeong (Korea Institute for Advanced Study, Secretary)

PROGRAM

Oral Presentations

August 28, 2023 (Mon.)

[Tutorial]

[Long Talks]

[Regular Talks (Parallel session A)]

[Regular Talks (Parallel session B)]

[Invited Talk]

August 29, 2023 (Tue.)

[Invited Talk]

[Long Talks]

[Regular Talks (Parallel session A)]

[Regular Talks (Parallel session B)]

[Invited Talk]

August 30, 2023 (Wed.)

[Invited Talk]

[Regular Talks (Parallel session A)]

[Regular Talks (Parallel session B)]

August 31, 2023 (Thur.)

[Invited Talk]

[Long Talks]

[Regular Talks (Parallel session A)]

[Regular Talks (Parallel session B)]

September 1, 2023 (Fri.)

[Invited Talk]

[Long Talks]

[Regular Talks (Parallel session A)]

[Regular Talks (Parallel session B)]

[Regular Talks (Parallel session A)]

[Regular Talks (Parallel session B)]

Quantum Entanglement, Bell's Theorem, Quantum Information Science

Marek Zukowski[1]

[1]*ICTQT, University of Gdansk*

Abstract. Quantum mechanics gives probabilistic predictions. Its predictions seem paradoxical. It was discovered twice in 1925. By Heisenberg, at the Helgoland island, and by Schroedinger half a year later in Alps. It almost immediately met an opposition. Einstein fully recognized it as a practical tool but criticized its non-deterministic nature. The Einstein-Bohr debate begun.

The talk will cover the developments which led to the 2022 Nobel prize in physics, the recipients of which closed the debate of the two 1922 Nobel Laureates. Brief resume on the EPR-paradox, Bell's comment on that. Clauser's better Bell inequalities, proposal of an experiment, and the first experiment. Aspect masterpiece versions of Clauser experiments. The mood of the times. Reemergence of interest in Bell-type photon correlations. Loopholes in experiments. Down-conversion as the work horse in optical Bell experiments. G-H-Zeilinger correlations. Entanglement swapping as the path to observable multiphoton entanglement/interference. Birth of quantum information science. Innsbruck teleportation experiment. 2015-2017 loophole free Bell experiments.

On the way I shall discuss various misinterpretations of all that, and present some less known approaches to Bell's Theorem, and important quantum optical conditions which allow to observe and control multi-photon interference.

[MZ is supported by the ICTQT IRAP (MAB) project of FNP, co-financed by structural funds of the EU.]

Quantum Complexity for Discrete Logarithms and Related Problems (Extended Abstract)

Minki Hhan[1] * Takashi Yamakawa[2 3] † Aaram Yun[4] ‡

[1] *Quantum Universe Center, Korea Institute for Advanced Study, Seoul 02455, Korea*
[2] *Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto 606-8502, Japan*
[3] *NTT Social Informatics Laboratories, Tokyo 180-8585, Japan*
[4] *Department of Cyber Security, Ewha Womans University, Seoul 03760, Korea*

Abstract. This paper studies the quantum computational complexity of the discrete logarithm and related group-theoretic problems in the context of "generic algorithms"—that is, algorithms that do not exploit any properties of the group encoding.

We prove that any generic quantum discrete logarithm algorithm for the underlying group $\mathcal{G}$ must make $\Omega(\log|\mathcal{G}|)$ depth of group operation queries. This shows that Shor's algorithm that makes $O(\log|\mathcal{G}|)$ group operations is asymptotically optimal among the generic quantum algorithms, even considering parallel algorithms. Furthermore, we extend this result to the generic hybrid quantum-classical algorithms and the bounded-size quantum memory setting, showing that variants of Shor's discrete logarithm algorithm are essentially optimal in each setting.

Keywords: Shor's algorithm, Lower bound, Discrete Logarithm

1 Introduction

The discrete logarithm (DL) problem and related problems have long been fundamental cryptographic primitives in the pre-quantum world [3, 10]. The emergence of quantum computing has drastically altered the landscape of cryptography in the post-quantum world. Shor's algorithm [29] has demonstrated that the DL problem (and integer factoring) can be solved in quantum polynomial time, rendering many cryptographic protocols that rely on the DL problem insecure against full-fledged quantum computers.

Algorithmic optimizations for quantum algorithms solving the DL problem have shown significant progress [21, 22, 11, 27, 14], and a recent estimation of Gidney and Ekerå [12] predicted that a single practical DL instance could be solved in few hours under some plausible physical assumptions. However, the base algorithm of these circuit optimizations is essentially the same as Shor's original one or its near variants [16, 7, 6, 5]. In other words, the complexity of the quantum DL algorithms is still dominated by $O(\log|\mathcal{G}|)$ group operations for the underlying group $\mathcal{G}$, just like in the original Shor's algorithm. As such, no asymptotic improvements have been made since the original algorithm.

This state of affairs raises an important question:

Can we solve the discrete logarithm asymptotically better than Shor's algorithm?

There are several potential approaches to addressing this question. In an extreme case, a direct quantum algorithm with better asymptotic complexity may suddenly appear. Alternatively, a hybrid classical-quantum algorithm could take advantage of the potentially massive power of classical computation with a favorable classical-quantum tradeoff. Another interesting avenue of exploration is a shallow quantum circuit that exploits parallelism, making quantum depth another important measure of complexity.[1]

To the best of our knowledge, there is no known lower bound, in terms of either time complexity or depth, for the quantum complexity of the DL problem.

2 Our Result

In this paper, we study the hardness of the discrete logarithm problem and related problems by considering a natural class of quantum algorithms referred to as generic algorithms. A generic quantum algorithm is an algorithm that does not take advantage of the special properties of the encodings of group elements. Instead, these algorithms only use group operations only in a black-box manner, potentially in superposition.

We formally establish the quantum generic group model (QGGM) by restricting that access to group elements is provided through the group oracle. The QGGM resembles the classical generic group model (GGM) [30, 20] proposed for arguing the security of group-theoretic cryptographic problems in classical settings. As in the classical GGM, the main complexity measure in the QGGM is the number of group operation queries. In addition, we are also concerned with the *depth* of group operation queries to study the power of near-term quantum computers.

*minkihhan@kias.ac.kr
†takashi.yamakawa.ga@hco.ntt.co.jp
‡aaramyun@ewha.ac.kr

[1] Cleve and Watrous [2] showed a lower bound on the depth for the quantum Fourier transform, which is a crucial step of Shor's algorithm. However, there might exist a completely different quantum algorithm that does not rely on the quantum Fourier transform. For example, the phase estimation-based DL algorithm [17] can be done without the quantum Fourier transform.

2.1 Lower bound in the fully quantum setting

Our first result states that no generic quantum algorithm in the QGGM can solve the DL problem much faster than Shor's original algorithm, even with parallel group operations. Precisely, we show the following theorem.

Theorem 1 *For a prime-order cyclic group $\mathcal{G}$, any generic quantum algorithm solving the DL problem over $\mathcal{G}$ must make queries of depth $\Omega(\log|\mathcal{G}|)$.*

To establish this theorem, for any generic quantum DL algorithm A, we construct a generic DL algorithm B in the *classical* GGM that perfectly simulates the output of A. Although the classical simulation may require unbounded time for precise simulation, its query complexity is only exponentially larger than that of A. It is known that a generic DL algorithm in the classical GGM must make $\Omega(|\mathcal{G}|^{1/2})$ classical group operation queries even if the algorithm is allowed to run in unbounded time [30, 20]. Combined with the above simulation with an exponential blowup, we obtain the desired result. We also establish the similar hardness of other group-theoretic problems, such as CDH and DDH using this simulation. We note that the naïve version of Shor's algorithm[2] has the matching group operation complexity to the lower bound in Theorem 1.

2.2 Hybrid quantum-classical algorithms

The above result may initially seem sufficient to refute our main question. However, this is not the case because this lower bound only considers purely quantum algorithms. We observe that some simple (combination of) folklore hybrid quantum-classical algorithms can do better than the purely quantum bound, exploiting classical computation to perform most group operations.

These hybrid algorithms consist of two phases: They first compute multiple group elements using $O(\mathrm{polylog}\,|\mathcal{G}|)$ classical group operation queries and store them as precomputed data. Then, they implement Shor's algorithm using the stored group elements using $O(\log|\mathcal{G}|/\log\log|\mathcal{G}|)$ quantum group operations and $O(\log\log|\mathcal{G}|)$ quantum query depth[3].

We complement these algorithms by proving the matching lower bounds. We formalize a model for generic hybrid quantum-classical algorithms that captures the above algorithms and more general class of algorithms. In the model, we allow an algorithm to make both classical and quantum group operation queries with the restriction that it is *forced to measure* all the registers whenever its quantum query number or depth count exceeds a certain threshold. It is supposed to capture hybrids of classical and quantum computers with limited coherence time. Note that we do not consider noises in our model whereas actual near-term quantum computers are likely to be noisy. Since our main results are the lower bounds, this just makes our results stronger.

[2]We describe Shor's algorithm in the QGGM in the full version of our paper for completeness.

[3]We describe the hybrid algorithms in the full version.

The following theorem states the limitations of the generic hybrid algorithms, showing that the above hybrid algorithms are indeed optimal with respect to both query number and depth.

Theorem 2 (Informal) *For a prime-order cyclic group $\mathcal{G}$, any generic hybrid quantum-classical algorithm solving the DL problem with $O(\mathrm{poly}\log|\mathcal{G}|)$ total queries (including both classical and quantum) must make $\Omega(\log|\mathcal{G}|/\log\log|\mathcal{G}|)$ quantum queries of depth $\Omega(\log\log|\mathcal{G}|)$ between some two consecutive forced measurements.*

More generally, any generic hybrid DL algorithm with Q total queries must make $\Omega(\log|\mathcal{G}|/\log Q)$ quantum queries of depth $\Omega(\log\log|\mathcal{G}|-\log\log Q)$ between some two consecutive forced measurements.

2.3 Quantum memory-bounded algorithms

Quantumly processable memory is an expensive resource, either quantum memory that can store quantum states or quantum random accessible (classical) memory (qRAM) that stores classical data but can be accessed coherently.[4] While the original Shor's algorithm only uses quantum memory that stores a single group element, the hybrid algorithms make use of relatively large quantum memory or large qRAM. This motivates the question of whether quantumly processable memory is necessary even for a mild speed-up of Shor's algorithm.

We prove that it is indeed necessary. The following theorem asserts such a lower bound.

Theorem 3 *For a prime-order cyclic $\mathcal{G}$, any generic hybrid algorithm solving the DL problem with quantum memory that can store t group elements and no qRAM must make either $\Omega(\sqrt{|\mathcal{G}|})$ classical or quantum group operation queries in total or $\Omega(\log|\mathcal{G}|/\log t)$ quantum group operation queries between some two consecutive forced measurements.*[5]

More generally, any generic hybrid DL algorithm with quantum memory that can store t group elements and qRAM that can store r group elements must make either $\Omega(\sqrt{|\mathcal{G}|})$ group operation queries in total or $\Omega(\log|\mathcal{G}|/\log(tr))$ quantum group operation queries between some two consecutive forced measurements.

In particular, the above theorem means that classical queries cannot reduce the number of quantum queries beyond $\Omega(\log|\mathcal{G}|/\log t)$, or just $\Omega(\log|\mathcal{G}|)$ when $t=O(1)$. We have algorithms that match the above lower bounds: Baby-step giant-step algorithm makes $O(\sqrt{|\mathcal{G}|})$ classical group operations, and the hybrid algorithm with quantum memory that can store t group elements and no qRAM makes $\Omega(\log|\mathcal{G}|/\log t)$ quantum queries.

[4]Formally, it enables one to realize a unitary $|i\rangle\otimes|0\rangle\mapsto|i\rangle\otimes|x_i\rangle$ for a classical data $(x_i)_i$.

[5]This gives a depth lower bound of $\Omega(\log|\mathcal{G}|/t\log t)$ as an immediate corollary as an algorithm can make at most t queries in one parallel query in this setting.

2.4 The multiple DL problem

The multiple discrete logarithm problem asks to solve multiple instances of the DL problem with the same underlying group simultaneously. When m DL instances are given, this problem is written by m-MDL. This problem is important in the context of the standard curves in elliptic curve cryptography, where only a few curves are recommended as standard. In the classical setting, Kuhn and Struik [18] suggested an $O(\sqrt{m|\mathcal{G}|})$ generic algorithm for the m-MDL problem, and Yun [33] proved the matching lower bound.

We present a generic quantum MDL algorithm using the results in vectorial addition chain [24], slightly faster than Shor's algorithm. When m is a moderate size[6], our algorithm solves the m-MDL problem using $O(m \log |\mathcal{G}| / \log(m \log |\mathcal{G}|))$ group operations. This gives an amortized group operation complexity of $O(\log |\mathcal{G}| / \log m)$ per DL instance.

Regarding Theorem 1, the complexity of the m-MDL problem is lower than solving each instance individually. It is related to the quantum annoying property [32, 4] suggested in the context of password-authenticated key exchange (PAKE), which roughly means that quantum algorithms must solve a DLP for each password guess of PAKE. Our algorithm shows that the strongest form of quantum annoying cannot hold.

3 Discussion

Tight complexity. Our lower bounds show asymptotically tight group operation complexity, but the constant factor has room for improvement. In the formal theorems, the concrete quantum query bounds are $0.25 \log |\mathcal{G}| + O(1)$ (or depth) in the fully quantum case and $0.5 \log |\mathcal{G}| + O(1)$ for the memory-bounded hybrid case with $t = r = 1$. Shor's DL algorithm and early variants [21, 17] make quantum and classical group operations $2 \log |\mathcal{G}|$ times each, having a gap in the constant factor. The later hybrid quantum-classical algorithms [16, 5, 6, 7] narrow down this gap to about $(1 + c) \log |\mathcal{G}|$ group operations before the forced measurement for some small c (depending on the algorithms) with appropriate classical pre- and post-processing. The constant gap still exists besides the number of subroutine calls. Filling this gap is of practical interest.

We may ask if a small number of quantum group operations could reduce the classical group operation queries. Our theorem says that if a generic hybrid algorithm makes one quantum group operation, then it should make $\Omega(|\mathcal{G}|^{0.25})$ classical group operations. This does not rule out a hybrid DL algorithm with $|\mathcal{G}|^{0.25}$ classical group operations and one quantum group operation, leaving a gap between the algorithm.

The quantum complexity of the composite-order DL problem is also unknown. We also do not know how to use the composite order either in constructing algorithms or proving lower bounds. The lower bound or better algorithm for the MDL problem is also unknown.

[6] Loosely speaking, $m = \text{polylog}|\mathcal{G}|$ works.

Generic vs. non-generic algorithms. While the group-theoretic algorithms discussed above can be viewed as generic algorithms, some variants leverage specific encoding structures [25, 15, 28, 27, 14] for theoretic or practical purposes, most of which are for speeding up the group operation in a non-black-box manner. In particular, Høyer and Spalek [15] showed that the DL problem on $\mathbb{Z}_N$ can be solved by a hybrid quantum-classical algorithm with a constant quantum depth if we allow for unbounded fan-out gates.[7] This overcomes our quantum depth lower bound using the non-generic method.[8]

This circumstance is reminiscent of the classical GGM, where some non-generic algorithms, such as index calculus, show better efficiency than generic algorithms by exploiting the integer encoding of group elements. Still, the classical GGM has been used as a meaningful model for arguing the hardness of group-theoretic problems, especially for the general elliptic curves. Thus, we believe that lower bounds in the QGGM are at least as meaningful as those in classical GGM. Moreover, to the best of our knowledge, all non-generic quantum algorithms for the DL problem are circuit optimization of (variants of) Shor's algorithm, which is generic. In contrast, non-generic classical algorithms start from fundamentally different ideas. This fact gives us more motivation to study the limitations of generic quantum algorithms.

Relation to the hidden subgroup problems. This paper suggests the number of (quantum) group operations as a complexity measure for studying the DL and related problems. We believe this is an important conceptual contribution. The usual complexity in this context is the query complexity to the relevant function f that instantiates the hidden subgroup problem (HSP). For the DL problem, this query complexity is 1 and the lower bound regarding f is pointless, suggesting that the new complexity measure is essential.

The known HSP algorithms [13, 8, 19, 9] can be considered as generic algorithms by extending our QGGM for general groups. In terms of the query complexity to the oracle function, proving a meaningful lower bound is unlikely because [9] showed that $O(\log^4 |\mathcal{G}|)$ queries suffice for the HSP over an arbitrary group. Contrary to the query complexity, the group operation complexity of [9] is exponentially large.

One may wonder if the group operation complexity provides an interesting lower bound of the HSP for some nonabelian groups. The answer is elusive with this paper's tools. The *dihedral group* case, a crucial case connected to the lattice-based [26] and isogeny-based cryptography [23, 1], has a negative answer to this question, as the algorithm of Ettinger and Høyer [8] only makes a polynomial number of group operations.

[7] It does not contradict the depth lower bound of the quantum Fourier transform [2], which assumes that each gate acts on a constant number of qubits.

[8] For example, they use that multiplication of many elements of $\mathbb{Z}_N$ can be done in $\mathbf{TC}_0$, i.e., computed by a constant depth classical circuit with threshold gates [31]. Also, note that using fan-out gates does not affect the query depth in the QGGM.

References

[1] A. M. Childs, D. Jao, and V. Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.*, 8(1):1–29, 2014.

[2] R. Cleve and J. Watrous. Fast parallel circuits for the quantum Fourier transform. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 526–536. IEEE, 2000.

[3] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, 1976.

[4] E. Eaton and D. Stebila. The "quantum annoying" property of password-authenticated key exchange protocols. In J. H. Cheon and J. Tillich, editors, *Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20-22, 2021, Proceedings*, volume 12841 of *Lecture Notes in Computer Science*, pages 154–173. Springer, 2021.

[5] M. Ekerå. Revisiting Shor's quantum algorithm for computing general discrete logarithms. *arXiv preprint arXiv:1905.09084*, 2019.

[6] M. Ekerå. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. *J. Math. Cryptol.*, 15(1):359–407, 2021.

[7] M. Ekerå and J. Håstad. Quantum algorithms for computing short discrete logarithms and factoring RSA integers. In T. Lange and T. Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings*, volume 10346 of *Lecture Notes in Computer Science*, pages 347–363. Springer, 2017.

[8] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. *Adv. Appl. Math.*, 25(3):239–251, 2000.

[9] M. Ettinger, P. Høyer, and E. Knill. The quantum query complexity of the hidden subgroup problem is polynomial. *Inf. Process. Lett.*, 91(1):43–48, 2004.

[10] T. E. Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory*, 31(4):469–472, 1985.

[11] C. Gidney. Windowed quantum arithmetic. *arXiv preprint arXiv:1905.07682*, 2019.

[12] C. Gidney and M. Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433, 2021.

[13] S. Hallgren, A. Russell, and A. Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. In F. F. Yao and E. M. Luks, editors, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*, pages 627–635. ACM, 2000.

[14] T. Häner, S. Jaques, M. Naehrig, M. Roetteler, and M. Soeken. Improved quantum circuits for elliptic curve discrete logarithms. In J. Ding and J. Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings*, volume 12100 of *Lecture Notes in Computer Science*, pages 425–444. Springer, 2020.

[15] P. Høyer and R. Spalek. Quantum fan-out is powerful. *Theory Comput.*, 1(1):81–103, 2005.

[16] B. S. K. Jr. A quantum "magic box" for the discrete logarithm problem. Cryptology ePrint Archive, Paper 2017/745, 2017. `http://eprint.iacr.org/2017/745`.

[17] A. Y. Kitaev. Quantum measurements and the abelian stabilizer problem. *Electron. Colloquium Comput. Complex.*, TR96-003, 1996.

[18] F. Kuhn and R. Struik. Random walks revisited: Extensions of Pollard's Rho algorithm for computing multiple discrete logarithms. In S. Vaudenay and A. M. Youssef, editors, *Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001, Revised Papers*, volume 2259 of *Lecture Notes in Computer Science*, pages 212–229. Springer, 2001.

[19] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005.

[20] U. M. Maurer. Abstract models of computation in cryptography. In N. P. Smart, editor, *Cryptography and Coding, 10th IMA International Conference, Cirencester, UK, December 19-21, 2005, Proceedings*, volume 3796 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2005.

[21] M. Mosca and A. Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. In C. P. Williams, editor, *Quantum Computing and Quantum Communications, First NASA International Conference, QCQC'98, Palm Springs, California, USA, February 17-20, 1998, Selected Papers*, volume 1509 of *Lecture Notes in Computer Science*, pages 174–188. Springer, 1998.

[22] A. Pavlidis and D. Gizopoulos. Fast quantum modular exponentiation architecture for Shor's factoring algorithm. *Quantum Inf. Comput.*, 14(7-8):649–682, 2014.

[23] C. Peikert. He gives c-sieves on the CSIDH. In A. Canteaut and Y. Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May*

10-14, 2020, Proceedings, Part II, volume 12106 of *Lecture Notes in Computer Science*, pages 463–492. Springer, 2020.

[24] N. Pippenger. On the evaluation of powers and monomials. *SIAM Journal on Computing*, 9(2):230–250, 1980.

[25] J. Proos and C. Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Inf. Comput.*, 3(4):317–344, 2003.

[26] O. Regev. Quantum computation and lattice problems. *SIAM J. Comput.*, 33(3):738–760, 2004.

[27] M. Roetteler, M. Naehrig, K. M. Svore, and K. E. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In T. Takagi and T. Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 241–270. Springer, 2017.

[28] M. Rötteler and R. Steinwandt. A quantum circuit to find discrete logarithms on ordinary binary elliptic curves in depth $O(\log^2 n)$. *Quantum Inf. Comput.*, 14(9-10):888–900, 2014.

[29] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[30] V. Shoup. Lower bounds for discrete logarithms and related problems. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 256–266. Springer, 1997.

[31] K. Siu, J. Bruck, T. Kailath, and T. Hofmeister. Depth efficient neural networks for division and related problems. *IEEE Trans. Inf. Theory*, 39(3):946–956, 1993.

[32] S. Thomas. Re: [Cfrg] proposed PAKE selection process. CFRG Mailing list, June 2019.

[33] A. Yun. Generic hardness of the multiple discrete logarithm problem. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 817–836. Springer, 2015.

Quantum Computing Quantum Monte Carlo

Yukun Zhang[1 2] Yifei Huang[3] Jinzhao Sun [4 5] Dingshun Lv [3 *] Xiao Yuan [1 2 †]

[1] *Center on Frontiers of Computing Studies, Peking University, Beijing 100871, China*
[2] *School of Computer Science, Peking University, Beijing 100871, China*
[3] *ByteDance Ltd., Zhonghang Plaza, No. 43, North 3rd Ring West Road, Haidian District, Beijing, China*
[4] *Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom*
[5] *Quantum Advantage Research, Beijing 100080, China*

Abstract. We propose a hybrid quantum-classical algorithm that integrates quantum computing and quantum Monte Carlo (QMC) methods for understanding many-body quantum systems. Our algorithm mitigates the sign problem in QMC through the use of non-stoquasticity indicator (NSI) and its upper bounds. We leverage quantum computing to decrease NSIs and enhance the expressivity of shallow quantum circuits. We validate the method with numerical tests on the N_2 molecule and the Hubbard model. This approach opens possibilities for solving practical problems using intermediate-scale and early-fault tolerant quantum computers, with applications in chemistry, condensed matter physics, materials, and high energy physics.

Keywords: quantum many-body systems, sign problem, quantum Monte Carlo

1 Introduction

In recent years, tremendous efforts have been put into finding the find ground (excited) eigenstates and eigenenergies of a quantum many-body system [6, 8, 17, 28]. Among various methods, projector QMC has drawn great attention and has been widely exploited to study chemistry and condensed matter physics problems. The projector QMC algorithms realize the imaginary time evolution (ITE) process in a statistical way. The insight is that one can represent quantum states by an effective superposition of classical basis states that are dubbed as "walkers", and evolve the distribution of the walkers through a sampling process upon enforcing the ITE operator. Therefore, the whole process manages to circumvent the ITE operator's non-unitarity. However, the QMC algorithms suffer from the sign problem [25], which is statistical fluctuation caused by the vanishing partition function $Z = \mathrm{Tr}(e^{-\beta H})$. On the other hand, with the development of quantum hardware, it is intriguing to wonder if near-term quantum devices are able to provide classically-inaccessible results for the ground-state problem. While many recent works have shown the potential applicability of quantum computing using NISQ devices [1, 2, 7, 10, 20], whether they are sufficiently powerful (extensive and accurate) to solve practical problems better than their classical counterpart still remains open.

Here we introduce a hybrid approach that integrates quantum Monte Carlo and quantum computing, leveraging their complementary strengths in representing and processing quantum states while mitigating their weaknesses of exponentially small average signs and hardware limitations. The sign problem comes from the non-stoqusticity [5] of the Hamiltonian. We first introduce the non-stoquaticity indicator (NSI) which is a generic formula for measuring the seriousness of the sign problem and a low-computational-cost upper bound for the NSI. For easing the sign problem, the general way is to perform a similar transformation [13] that preserves the spectrum of the Hamiltonian. However, a general transformation could scramble the operator, which renders the Hamiltonian highly non-local. To this end, we propose the quantum version of the full configuration interaction quantum Monte Carlo (FCIQMC) [4, 9], which we call the QC-FCIQMC algorithms. Compare to its classical counterpart, our protocol leverages quantum circuits to effectively perform the similarity transformation of the QMC basis, but still remains efficient. By computing the upper bound for the NSI for different quantum systems, we see the seriousness of the sign problem drop by several orders of magnitudes in aiding our methods.

*lvdingshun@bytedance.com
†xiaoyuan@pku.edu.cn

2 Sign problem and its indicators

The sign problem manifests when computing the expectation value of observable with the final-round walkers as we normalize the wave function in the chosen basis. To see this, let us consider a similar scenario—the thermal state $e^{-\beta H}/Z$ with $Z = \mathrm{Tr}[e^{-\beta H}]$, and the expectation of observable A is $\langle A\rangle = \mathrm{Tr}[Ae^{-\beta H}]/Z$. In the following, we consider a general walker basis (orthonormal states) $\{|\phi_i\rangle\}$. Denote $G = \alpha I - H$ with $\alpha = \max_i H_{ii}$, and we expand the expectation estimation formula in a path-integral form by inserting bases in the trace

$$\begin{aligned}\langle A\rangle &= \frac{\mathrm{Tr}[Ae^{-\beta H}]}{\mathrm{Tr}[e^{-\beta H}]} = \frac{\mathrm{Tr}[Ae^{\beta G}]}{\mathrm{Tr}[e^{\beta G}]} \\ &= \frac{\sum_{k=0}^{\infty}\frac{\beta^k}{k!}\sum_{i_0,i_1,\dots i_k} A_{i_0 i_1}G_{i_1 i_2}\cdots G_{i_k i_0}}{\sum_{k=0}^{\infty}\frac{\beta^k}{k!}\sum_{i_1,i_2\dots i_k} G_{i_1 i_2}G_{i_2 i_3}\cdots G_{i_k i_1}} \\ &= \frac{\sum_{k=0}^{\infty}\frac{\beta^k}{k!}\sum_{i_0,i_1,\dots i_k}\frac{A_{i_0 i_1}|G_{i_1 i_2}\cdots G_{i_k i_0}|s_{i_1\cdots i_k,i_0}}{\sum_{i_1,i_2\dots i_k}|G_{i_1 i_2}\cdots G_{i_k i_0}|}}{\sum_{k=0}^{\infty}\frac{\beta^k}{k!}\sum_{i_1,i_2\dots i_k}\frac{|G_{i_1 i_2}G_{i_2 i_3}\cdots G_{i_k i_1}|s_{i_1\cdots i_k,i_1}}{\sum_{i_1,i_2\dots i_k}|G_{i_1 i_2}\cdots G_{i_k i_1}|}} = \frac{\langle As\rangle}{\langle s\rangle},\end{aligned} \tag{1}$$

where denote $M_{ij} := \langle\phi_i|M|\phi_j\rangle$ for any operator M, and extract the sign of $G_{i_1 i_2}G_{i_2 i_3}\cdots G_{i_k i_1}$ as $s_{i_1\cdots i_k,i_1}$. Ac-

cording to Troyer [25], a system presents the sign problem whenever the path integral in Eq. (1) contains negative paths. "Stoquastic" [5] or "bonsonic" Hamiltonians are known to be sign-problem-free. Specifically, a Hamiltonian is "stoquastic" when all its off-diagonal terms (in the walker basis) are non-positive. Thus, every element of G is positive in this case, and so are the expanded terms of $\mathrm{Tr}[e^{\beta G}]$. This suggests that the sign problem is basis-dependent. In general cases, due to both positive and negative paths being involved, the standard way for Monte Carlo simulation is to sample according to the absolute value of each path as the second line in Eq. (1). However, it is shown that the average sign $\langle s\rangle$ vanishes exponentially compared to its "bosonic" form [25], so as the requiring number of walkers to counterbalance the variance.

To quantify the sign problem of Hamiltonian H, we separate it by $H = H_+ + H_-$ with nonzero elements $(H_-)_{ij} = H_{ij}$ ($[i = j]$ *or* $[i \neq j$ *and* $H_{ij} < 0]$) and $(H_+)_{ij} = H_{ij}$ $[i \neq j$ *and* $H_{ij} > 0]$. The bosonic form [25] of H is $\tilde{H} = H_- - H_+$, which is stoquastic and hence has no sign problem. The non-stoquasticity indicator (NSI) is defined by

$$S(H) = \frac{\mathrm{Tr}[e^{-\beta\tilde{H}}] - \mathrm{Tr}[e^{-\beta H}]}{\mathrm{Tr}[e^{-\beta H}]} = \frac{1}{\langle s\rangle - 1}. \tag{2}$$

As discussed above, the sign problem indicates an exponentially small average sign $\langle s\rangle = e^{-\beta\Delta f}$ with Δf being the free energy difference between H and $\tilde{H}$. Thus $S(H)$ also exponentially increases with $\beta\Delta f$. However, it is in general hard to evaluate Δf. Here, we provide an upper bound of $S(H)$ with more explicit dependence on the matrix element of the Hamiltonian $H_\pm$.

Theorem 1 *The non-stoquasticity indicator is upper-bounded by* $S(H) \leq 2e^{\beta\|(\alpha - H_-)\|_{L_1}} \sinh(\beta\|H_+\|_{L_1})$, *where we define the matrix norm as* $\|M\|_{L_1} := \sum_{i,j} |M_{ij}|$ *for matrix* M.

A stoquastic Hamiltonian has $H_+ = 0$, which indicates $S(H) = 0$ and hence no sign problem. In general, a smaller $\|H_+\|_{L_1}$ also corresponds to a less serious sign problem, which is consistent with recent works [13, 15, 16, 24].

Meanwhile, when we focus on the imaginary time evolution of a specific initial state, say ϕ_0, with time $\tau = \beta/2$, we can similarly define the NSI as

$$S(H, \phi_0) = \frac{\langle\phi_0|e^{-\beta\tilde{H}}|\phi_0\rangle - \langle\phi_0|e^{-\beta H}|\phi_0\rangle}{\langle\phi_0|e^{-\beta H}|\phi_0\rangle}. \tag{3}$$

Again, $S(H, \phi_0)$ measures the sign problem and is related to the average sign. We provide an upper bound of $S(H, \phi_0)$ as a function of ϕ_0 and $H_\pm$.

Theorem 2 *The non-stoquasticity indicator is upper-bounded by* $S(H, \psi_0) = \mathcal{O}\left(\|\Pi_\perp H |\phi_0\rangle\|\right)$, *where* $\|\,|v\rangle\,\| = \sqrt{\langle v|\,v\rangle}$ *and* $\Pi_\perp = I - |\phi_0\rangle\langle\phi_0|$.

Here, we have ignored the dependence on other matrix elements of H. We can see that apart from small H_+, a good initial state that is close to an eigenstate of H can also alleviate the sign problem.

3 QC-FCIQMC algorithm

We now introduce our hybrid algorithm using a quantum computer to mitigate the sign problem of QMC. The basic idea is to replace the simple walker states $\{|i\rangle\}$ with states $\{|\phi_i\rangle\}$ prepared by quantum circuits $|\phi_i\rangle = U|i\rangle$. This is equivalent to considering walkers $\{|i\rangle\}$ with a similarity transformed Hamiltonian $U^\dagger H U$. We may use a quantum computer to find U that approximately diagonalizes H [18, 19], where the off-diagonal part $U^\dagger H U$ is suppressed. Furthermore, according to Theorem 2, we may not even need to diagonalize H, but just find an approximate ground state, which is a much simpler task and requires even shallower circuits [11, 12, 22, 23, 27]. Our algorithm requires VQAs such as VQE with an even shorter circuit but still runs QMC with eased sign problems. In particular, as one can see in our numerical results in Fig. 1 (c), for the ground state of the nitrogen molecule, we manage to boost the results of VQE at different circuit depths much closer to the exact energy with the help of QMC. Meanwhile, as we increase the circuit depth according to the capability of the quantum devices, the severity of the sign problem of the traditional FCIQMC is suppressed exponentially as shown by our numerical results in Fig. 1 (d), and we expect this trend to continue for many more layers. Therefore, our work hints at a new direction toward practical quantum advantage.

Now we introduce the methodology of our algorithm. Suppose we already find the unitary U using either approximate Hamiltonian diagonalization [18, 19] or VQE [11, 12, 22, 23, 27], and replace $|i\rangle$ with $|\phi_i\rangle = U|i\rangle$, the wavefunction is expanded as $|\psi(\tau)\rangle = \sum_i \widetilde{c}_i(\tau)|\phi_i\rangle$ and the coefficients $\widetilde{c}_i(\tau)$ follow the imaginary time evolution as

$$\frac{\mathrm{d}\widetilde{c}_i(\tau)}{\mathrm{d}\tau} = -\sum_j (H_{ij} - S\delta_{ij})\widetilde{c}_j(\tau), \tag{4}$$

with $H_{ij} = \langle\phi_i|H|\phi_j\rangle$ and an adjustable energy shift S. Now, we need to propagate the (quantum) walkers to effectively realize the imaginary time evolution. FCIQMC realizes the ITE of the state as $|\psi(\tau)\rangle \propto e^{-(H-S)\tau}|\psi(0)\rangle$ with time $\tau > 0$ and certain parameter S by walkers of weights ± 1. The algorithm is designed such that the population $N_i(\tau)$ by summing up all of the weights of walkers at configuration i is proportional to the corresponding amplitude $c_i(\tau)$ following the imaginary time dynamics. Incorporate the new walker states generated from VQE to FCIQMC, we first initialize $N_i(\tau)$ number of the walker $|\phi_i\rangle$ at time $\tau = 0$; then, for small time $\Delta\tau$, we repeatedly update each walker $|\phi_i\rangle$ through (1) spawning — spawn a child walker $|\phi_j\rangle$ ($j \neq i$) with probability $|H_{ji}|\Delta\tau$ with the same sign as walker $|\phi_i\rangle$ multiplied by $-H_{ji}/|H_{ji}|$; (2) Death or cloning — the walker $|\phi_i\rangle$ dies with probability $(H_{ii} - S)\Delta\tau$ (if $H_{ii} - S > 0$) and clones itself with probability $|(H_{ii} - S)|\Delta\tau$ otherwise; (3) Annihilation — annihilate same walker pairs with opposite signs. Here, a major challenge is how to realize the spawning process, i.e., to propagate walker $|\phi_i\rangle$ to $|\phi_j\rangle$ with probability $|H_{ji}|\Delta\tau$. In conventional

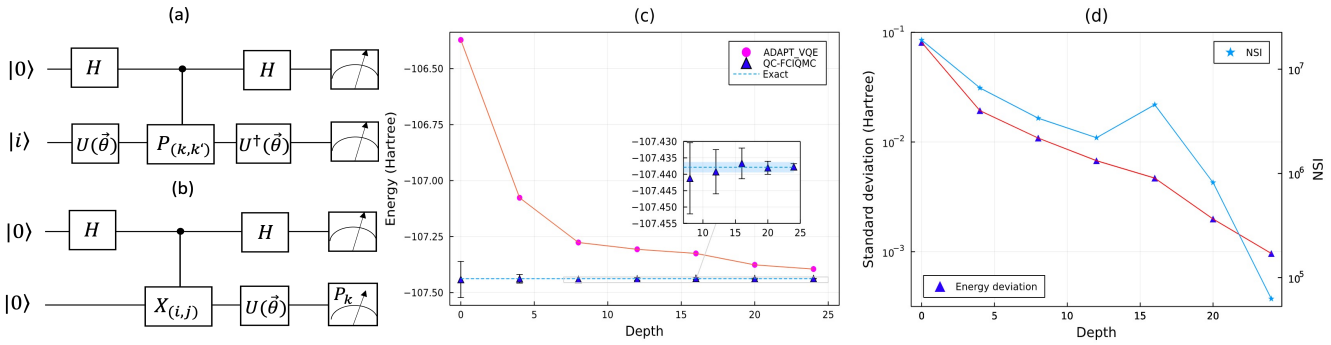


Figure 1: (a) Quantum circuits for evaluating $|H_{ji}|^2$. (b) Circuit for evaluating the real part of H_{ji}. (c) ADAPT-VQE energies and QC-FCIQMC energies with standard deviations for different depths of ADAPT-VQE. (d) Standard deviations from (a) as well as the non-stoquastic indicator with $\beta = 10^{-1}$.

FCIQMC, this is possible since there is only a polynomial number of nonzero H_{ji} for (classical) walkers $\{|i\rangle\}$. However, for (quantum) walkers $|\phi_i\rangle$, there might be an exponential number of nonzero H_{ji}, so naively, we may need to measure all H_{ji} to realize the spawning process, which is formidable.

Here we introduce an efficient way to realize the spawning process. To evaluate the probability $|H_{ji}|\Delta\tau$, we note that $|H_{ji}|^2 = \langle i|U^\dagger HU\Pi_j U^\dagger HU|i\rangle$ with $\Pi_j = |j\rangle\langle j|$. Suppose the Hamiltonian is expanded as $H = \sum_k h_k P_k$ with coefficients h_k and Pauli operators P_k, then $|H_{ji}|^2 = \sum_{kk'} h_k h_{k'} p^i_{kk'}(j)$ with $p^i_{kk'}(j) = \mathrm{Re}\langle i|U^\dagger P_k U\Pi_j U^\dagger P_{k'} U|i\rangle$ satisfying $\sum_j |p^i_{kk'}(j)| \leq 1$. For fixed i, k, k', we can use the quantum circuit in Fig. 1(a) to measure $p^i_{kk'}(j)$ for all j and hence obtain $|H_{ji}|$ up to a desired accuracy. We usually get a small number of nonzero $|H_{ji}|$. Then we can apply the quantum circuit in Fig. 1(b) to further estimate the sign (phase) of H_{ji}. Note that the quantum circuits for estimating $|H_{ji}|$ and its sign only introduce one ancillary qubit and at most doubles the unitary U (apart from a few gates independent of U). Meanwhile, H_{ji} only needs to be measured once and information could be re-used.

After implementing the evolution (with initial walkers ϕ_0), we can get the energy by the mixed energy evaluation $E(\tau) = E_0 + \sum_{i\neq 0} \langle\phi_i| H |\phi_0\rangle \frac{\mathrm{sign}(i) N_i(\tau)}{N_0(\tau)}$, where $E_0 = \langle\phi_0|H|\phi_0\rangle$, and $N_i(\tau)$ and $\mathrm{sign}(i)$ are the number and sign of walker ϕ_i, respectively, at time τ. Suppose ϕ_0 is obtained by running VQE, then our method effectively introduces corrections from all other ϕ_i by implementing QMC. Note that our protocol is capable of evaluating any observable as long as it can be expressed succinctly in the Pauli basis.

4 Discussion

In this work, we propose a hybrid QC-QMC method. We derive upper bounds to NSIs, which guide the discovery and testing of the effectiveness of the method. The QC-FCIQMC algorithm also relies on a nontrivial efficient realization of the spawning process, which otherwise requires exponential resources. We benchmark the algorithm for N_2 and the Hubbard model, and the results show notable improvements over the single use of QC or FCIQMC.

There are several interesting future directions. First, the derived bounds for NSIs could be exploited to find other basis rotations as a classical means to mitigate the sign problem. Besies, our algorithm is compatible with current and near-term quantum hardware, and therefore its detailed resource analysis, error mitigation, and experimental realization also deserve future work. One could also explore the use of the VQE basis and our circuit construction for the deterministic selected-CI variants of FCIQMC [3, 14, 21, 26].

References

[1] Ehud Altman, Kenneth R. Brown, Giuseppe Carleo, Lincoln D. Carr, Eugene Demler, Cheng Chin, Brian DeMarco, Sophia E. Economou, Mark A. Eriksson, Kai-Mei C. Fu, Markus Greiner, Kaden R.A. Hazzard, Randall G. Hulet, Alicia J. Kollár, Benjamin L. Lev, Mikhail D. Lukin, Ruichao Ma, Xiao Mi, Shashank Misra, Christopher Monroe, Kater Murch, Zaira Nazario, Kang-Kuen Ni, Andrew C. Potter, Pedram Roushan, Mark Saffman, Monika Schleier-Smith, Irfan Siddiqi, Raymond Simmonds, Meenakshi Singh, I.B. Spielman, Kristan Temme, David S. Weiss, Jelena Vučković, Vladan Vuletić, Jun Ye, and Martin Zwierlein. Quantum simulators: Architectures and opportunities. *PRX Quantum*, 2:017003, Feb 2021. doi: 10.1103/PRXQuantum.2.017003. URL `https://link.aps.org/doi/10.1103/PRXQuantum.2.01700`

[2] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S. Kottmann, Tim Menke, Wai-Keong Mok, Sukin Sim, Leong-Chuan Kwek, and Alán Aspuru-Guzik. Noisy intermediate-scale quantum algorithms. *Rev. Mod. Phys.*, 94:015004, Feb 2022. doi: 10.1103/RevModPhys.94.015004. URL `https://link.aps.org/doi/10.1103/RevModPhys.94.0150`

[3] NS Blunt, Simon D Smart, JAF Kersten, JS Spencer, George H Booth, and Ali Alavi. Semi-stochastic full configuration interaction quantum monte carlo: Developments and application. *The Journal of chemical physics*, 142(18):184107, 2015.

[4] George H Booth, Alex JW Thom, and Ali Alavi. Fermion monte carlo without fixed nodes: A game of life, death, and annihilation in slater determinant space. *The Journal of chemical physics*, 131 (5):054106, 2009.

[5] Sergey Bravyi, David P Divincenzo, Roberto I Oliveira, and Barbara M Terhal. The complexity of stoquastic local hamiltonian problems. *arXiv preprint quant-ph/0606140*, 2006.

[6] Yudong Cao, Jonathan Romero, Jonathan P Olson, Matthias Degroote, Peter D Johnson, Mária Kieferová, Ian D Kivlichan, Tim Menke, Borja Peropadre, Nicolas PD Sawaya, et al. Quantum chemistry in the age of quantum computing. *Chemical reviews*, 119(19):10856–10915, 2019.

[7] Marco Cerezo, Alexander Poremba, Lukasz Cincio, and Patrick J Coles. Variational quantum fidelity estimation. *Quantum*, 4:248, 2020.

[8] Garnet Kin-Lic Chan and Sandeep Sharma. The density matrix renormalization group in quantum chemistry. *Annual review of physical chemistry*, 62 (1):465–481, 2011.

[9] Deidre Cleland, George H Booth, and Ali Alavi. Communications: Survival of the fittest: Accelerating convergence in full configuration-interaction quantum monte carlo. *The Journal of chemical physics*, 132(4):041103, 2010.

[10] Suguru Endo, Zhenyu Cai, Simon C. Benjamin, and Xiao Yuan. Hybrid quantum-classical algorithms and quantum error mitigation. *Journal of the Physical Society of Japan*, 90(3):032001, 2021. doi: 10.7566/JPSJ.90.032001. URL https://doi.org/10.7566/JPSJ.90.032001.

[11] Yi Fan, Changsu Cao, Xusheng Xu, Zhenyu Li, Dingshun Lv, and Man-Hong Yung. Circuit-depth reduction of unitary-coupled-cluster ansatz by energy sorting. *arXiv preprint arXiv:2106.15210*, 2021.

[12] Harper R Grimsley, Sophia E Economou, Edwin Barnes, and Nicholas J Mayhall. An adaptive variational algorithm for exact molecular simulations on a quantum computer. *Nature comm.*, 10(1): 1–9, 2019. doi: 10.1038/s41467-018-07090-4. URL https://www.nature.com/articles/s41467-019-10988-2.

[13] Dominik Hangleiter, Ingo Roth, Daniel Nagaj, and Jens Eisert. Easing the monte carlo sign problem. *Science advances*, 6(33):eabb8341, 2020.

[14] Adam A Holmes, Norm M Tubman, and CJ Umrigar. Heat-bath configuration interaction: An efficient selected configuration interaction algorithm inspired by heat-bath sampling. *Journal of chemical theory and computation*, 12(8):3674–3680, 2016.

[15] Joel Klassen, Milad Marvian, Stephen Piddock, Marios Ioannou, Itay Hen, and Barbara M. Terhal. Hardness and ease of curing the sign problem for two-local qubit hamiltonians. *SIAM Journal on Computing*, 49(6):1332–1362, 2020. doi: 10.1137/19M1287511. URL https://doi.org/10.1137/19M1287511.

[16] Ryan Levy and Bryan K. Clark. Mitigating the sign problem through basis rotations. *Phys. Rev. Lett.*, 126:216401, May 2021. doi: 10.1103/PhysRevLett.126.216401. URL https://link.aps.org/doi/10.1103/PhysRevLett.126.21

[17] Sam McArdle, Suguru Endo, Alan Aspuru-Guzik, Simon C Benjamin, and Xiao Yuan. Quantum computational chemistry. *Reviews of Modern Physics*, 92(1):015003, 2020. URL https://doi.org/10.1103/RevModPhys.92.015003.

[18] Ken M. Nakanishi, Kosuke Mitarai, and Keisuke Fujii. Subspace-search variational quantum eigensolver for excited states. *Phys. Rev. Research*, 1:033062, Oct 2019. doi: 10.1103/PhysRevResearch.1.033062. URL https://link.aps.org/doi/10.1103/PhysRevResearch.1.

[19] Robert M. Parrish, Edward G. Hohenstein, Peter L. McMahon, and Todd J. Martínez. Quantum computation of electronic transitions using a variational quantum eigensolver. *Phys. Rev. Lett.*, 122:230401, Jun 2019. doi: 10.1103/PhysRevLett.122.230401. URL https://link.aps.org/doi/10.1103/PhysRevLett.122.23

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

[21] Jeffrey B Schriber and Francesco A Evangelista. Communication: An adaptive configuration interaction approach for strongly correlated electrons with tunable accuracy. *The Journal of chemical physics*, 144(16):161106, 2016.

[22] Ho Lun Tang, VO Shkolnikov, George S Barron, Harper R Grimsley, Nicholas J Mayhall, Edwin Barnes, and Sophia E Economou. qubit-adapt-vqe: An adaptive algorithm for constructing hardware-efficient ansatze on a quantum processor. *arXiv preprint arXiv:1911.10205*, 2019.

[23] Ho Lun Tang, VO Shkolnikov, George S Barron, Harper R Grimsley, Nicholas J Mayhall, Edwin Barnes, and Sophia E Economou. qubit-adapt-vqe: An adaptive algorithm for constructing hardware-efficient ansätze on a quantum processor. *PRX Quantum*, 2(2):020310, 2021.

[24] Giacomo Torlai, Juan Carrasquilla, Matthew T. Fishman, Roger G. Melko, and Matthew P. A. Fisher. Wave-function positivization via automatic differentiation. *Phys. Rev. Research*, 2:032060, Sep 2020. doi: 10.1103/PhysRevResearch.2.032060. URL `https://link.aps.org/doi/10.1103/PhysRevResearch.2.032060`.

[25] Matthias Troyer and Uwe-Jens Wiese. Computational complexity and fundamental limitations to fermionic quantum monte carlo simulations. *Physical review letters*, 94(17):170201, 2005.

[26] Norm M Tubman, Joonho Lee, Tyler Y Takeshita, Martin Head-Gordon, and K Birgitta Whaley. A deterministic alternative to the full configuration interaction quantum monte carlo method. *The Journal of chemical physics*, 145(4):044112, 2016.

[27] Zi-Jian Zhang, Thi Ha Kyaw, Jakob Kottmann, Matthias Degroote, and Alan Aspuru-Guzik. Mutual information-assisted adaptive variational quantum eigensolver. *Quantum Science and Technology*, 2021. URL `http://iopscience.iop.org/article/10.1088/2058-9565/abdca4`.

[28] Bo-Xiao Zheng, Chia-Min Chung, Philippe Corboz, Georg Ehlers, Ming-Pu Qin, Reinhard M Noack, Hao Shi, Steven R White, Shiwei Zhang, and Garnet Kin-Lic Chan. Stripe order in the underdoped region of the two-dimensional hubbard model. *Science*, 358 (6367):1155–1160, 2017.

Quantum advantage in temporally flat measurement-based quantum computation

Michael de Oliveira[1 2 *] Luis S. Barbosa[1 2 †] Ernesto F.Galvão[1 ‡]

[1] *International Iberian Nanotechnology Laboratory*
[2] *University of Minho*

Abstract. Several classes of quantum circuits have been shown to provide a quantum computational advantage under certain assumptions. The study of ever more restricted classes of quantum circuits capable of quantum advantage is motivated by possible simplifications in experimental demonstrations. In this paper we study the efficiency of measurement-based quantum computation with a completely flat temporal ordering of measurements. We propose new constructions for the deterministic computation of arbitrary Boolean functions, drawing on correlations present in multi-qubit Greenberger, Horne, and Zeilinger (GHZ) states. We characterize the necessary measurement complexity using the Clifford hierarchy, and also generally decrease the number of qubits needed with respect to previous constructions. In particular, we identify a family of Boolean functions for which deterministic evaluation using non-adaptive MBQC is possible, featuring quantum advantage in width and number of gates with respect to classical circuits.

Keywords: Measurement-based Quantum computing, Non-local games, Circuit Complexity, Boolean analysis.

1 Introduction

One of the primary motivations for studying quantum information and computation, along with the search for practical advantage, is to clarify the longstanding question of what generates the classical-quantum separation with respect to information processing power [1]. Phenomena such as non-locality and contextuality have been identified as possible sources of quantum computational advantage [2, 3, 4], among others [5, 6, 7]. It appears that no single phenomenon can be associated with all forms of quantum information processing advantage, so it is important to identify and study quantum advantage in different models and regimes.

In this pursuit, the measurement-based quantum computation (MBQC) model, first presented by Raussendorf and Briegel in [8] as a sequence of adaptively selected single-qubit measurements on a highly entangled quantum state, is a natural setting to study quantum-to-classical separations. In particular, it allows for demonstrations that specific structures of non-local correlations between qubits are necessary for universal quantum computation [9]. Nevertheless, a temporal structure for the measurements is simultaneously imposed to achieve universality [10, 11, 12]. This means statically selected measurements are not computationally expressive enough to implement arbitrary quantum algorithms, even with access to highly correlated resource states. A judicious choice of side classical computation and control is essential for universality in the MBQC model.

The importance of time structure in measurement-based quantum computation is not fully understood. For instance, it is conjectured that classical computers cannot efficiently simulate instantaneous quantum polynomial (IQP) circuits [13], despite the fact that these circuits of commuting gates have no temporal structure, and can be implemented without adaptive measurements in MBQC [14]. These results have motivated the study of temporally flat computation for demonstrations of quantum advantage [15, 16, 17]. Despite having an output distribution that is hard to simulate classically, no practical application for IQP circuits has been found. Even for quantum circuits with temporal order, constant improvements in classical simulation techniques contribute to enlarging the classes of circuits that are classically efficiently simulable [18].

In this paper, we study non-adaptive MBQC computations, which lack temporal structure for the measurement operators, enabling simpler realizations across various quantum computing platforms. For instance, in photonic quantum computations, adaptive measurements generate high photon losses [19]. Furthermore, we focus our interest on exploring the potential use of this model in decision problems, which are well-known for their multitude of applications, contrasting with the difficult-to-simulate probability distributions previously studied [20, 21].

2 Our results

For temporally unstructured MBQC computations, we propose new constructions that synthesize quantum circuits for the deterministic evaluation of Boolean functions. These constructions reduce the number of qubits required in the GHZ resource states used, especially for the case of symmetric Boolean functions. We also improve the circuit synthesis process, removing an exponential scaling of previous constructions on the degree of the Boolean function [22, 23]. Regarding the complexity of the single-qubit measurements, we also characterize the maximum level of the Clifford hierarchy required for deterministic Boolean function evaluation.

*michael.oliveira@inl.int
†lsb@di.uminho.pt
‡ernesto.galvao@inl.int

This paper was uploaded to arxiv (https://arxiv.org/abs/2212.03668) and submitted to the Quantum journal.

Theorem 1 *(Informal) Any Boolean function f can be evaluated deterministically in the non-adaptive MBQC model using measurement operators of the* $\mathsf{deg}(f)$*-level of the Clifford hierarchy.*

This result describes a measure of complexity for the evaluation of Boolean functions in the model while defining the type of measurement operators (Figure 1) necessary to maximally violate a multipartite Bell inequality with dichotomic observables and outcomes [24]. Furthermore, this strengthens the idea that the degree of a Boolean function that can be computed with certain given quantum resources introduces a hierarchy for quantum correlations, connecting measures of computational complexity with measures of non-classicality beyond the binary characterization, as suggested in [23].

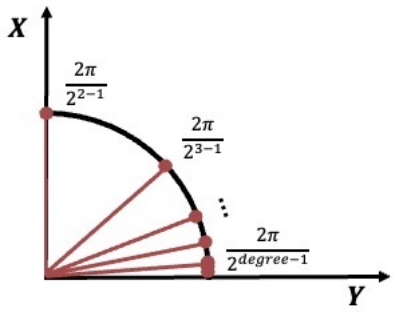


Figure 1: Representation of the required precision of the angles, which characterize the measurement operators, concerning the degree of the Boolean function being computed.

We translate the abstract description of the quantum circuits obtained from the constructions into specific circuits based on a fixed gate set. We also characterize how the solutions produced by the constructions are related to various circuit complexity measures. This enables us to prove a quantum classical separation on the circuit level for computations of a specific class of Boolean functions with degree two.

Theorem 2 *(Informal) Any classical circuit with unary and binary Boolean operators with single fan out computes symmetric Boolean functions f with* $\mathsf{deg}(f) = 2$ *with* $\Theta(n * \log_2(n))$ *gates and circuit width. In contrast, realizations of the non-adaptive MBQC model compute these functions with* $\Theta(n)$ *gates and circuit width.*

The proof compares these quantum circuits with the length of the classical Boolean formulas, which describe classical circuits without a memory. The comparison is indeed very strong in the sense that the quantum circuit also does not use any memory (see Figure 2 for a pictorial representation of this subclass of circuits). Interestingly, this result also has an interpretation in terms of Bell inequalities. In particular, the evaluation of the specific family of Boolean functions for which we identify quantum advantage corresponds to maximal violations of generalized Svetlichny inequalities [25]. Therefore, a maximal violation of these inequalities starting from a specific size implies a corresponding circuit separation. More precisely, any quantum state that can be prepared and measured with linearly bounded quantum circuits that violate these inequalities maximally implies a corresponding circuit separation.

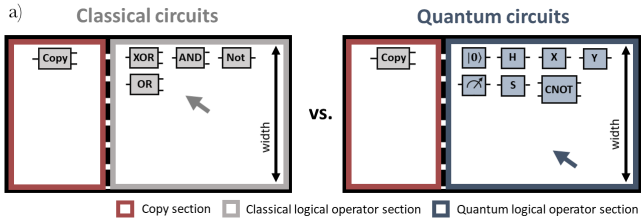


Figure 2: Illustration of the circuit classes for which we prove a separation in Theorem 2.

Finally, we extend the previous analysis to higher degree symmetric Boolean functions, and conjecture that these have no advantage with respect to classical circuits.

Conjecture 1 *(Informal) Symmetric Boolean functions f with* $\mathsf{deg}(f) \geq 3$ *evaluated within the non-adaptive MBQC model do not entail circuits with better scalings than classical circuits with unary and binary Boolean operators with single fan out.*

This conjecture is based on several independent results. The first one is the exponential lower bound proven in [24] for the general AND function, which is symmetric and has an instance for any possible degree. Then, we conjecture and provide support with a finite number of instances that the symmetric Boolean functions require quantum states whose size scales at a greater rate than the corresponding number of classical bits required in the optimal classical circuits for the same computations. Furthermore, we show that with the Clifford+T gate set the necessary measurement operators cannot be synthesized exactly, and always need to be approximated. In contrast, there is no difficulty in computing the same function deterministically with classical circuits. This illustrates some of the restrictions resulting from the imposed flat temporal order.

3 Related work

Non-local games. Computations within the non-adaptive MBQC model were proven to have a one-to-one correspondence to multi-party Bell inequalities with dichotomic observables and outcomes [24]. Therefore, the classical and the quantum bounds determined in previous works for this type of Bell inequalities immediately translate to computational efficiencies of the respective functions in the non-adaptive MBQC model [26]. For the quantum bounds, we obtain the maximal efficiency that can be obtained from quantum resources to compute the respective Boolean functions, and equivalently, the same happens for classical bounds. From this relation, we can compare our work with a large spectrum of results and

techniques on the optimal strategies for non-local games [26, 27, 28].

Quantum circuits. A breakthrough result by Bravyi, Gosset, and König [29] shows that a specific relation problem can be solved in constant depth with a quantum circuit, while requiring logarithmic depth in a classical computer [29]. Our main result demonstrates that the quantum advantage does prevail, respective to the number of gates, if we use the circuit that computes this relation to solve the equivalent decision problem (see Figure 3) [1].

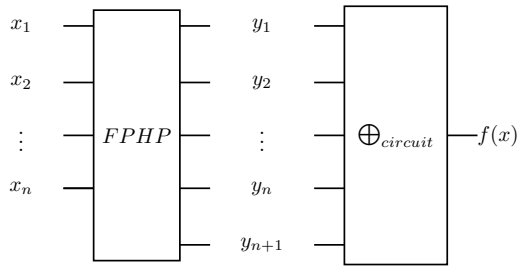


Figure 3: The quantum circuits used in Theorem 2, composed by the circuits used in [29] to solve a particular relation problem, and additional quantum pre-processing and classical post-processing.

From another perspective, the quantum advantage for the decision problem we identified can be described in terms of the number of gates and the width of the circuits. Interestingly, in [30], the authors prove an advantage using the same symmetric Boolean function of degree two that we address here. The advantage regarding the equivalent classical model is established by fixing the computational space and showing that these computations can be computed with higher efficiency on a quantum device (IBM's quantum computer). Consequently, our result can be interpreted as the computation of the same function without any width restriction. Additionally, for the classes of symmetric Boolean functions we studied here, quantum advantages were demonstrated in the branching programs setting in [31], and sampling problems in [32, 33].

4 Conclusions

We investigated the problem of evaluating deterministically Boolean functions in the non-adaptive MBQC computational model, providing new constructions, and a more precise understanding of the instructions for each stage of the model, using the discrete Fourier series decomposition of the algebraic normal forms of the functions as the main techniques. We characterized the complexity of two resources in this model: the number of required qubits in a GHZ state, and the required level of the Clifford hierarchy for single-qubit measurements. Regarding the number of qubits in a GHZ state, we lowered the upper bound for the number of qubits required to evaluate the entire set of symmetric Boolean functions and conjectured a lower bound for this same set, assuming symmetries between the instructions of the process. Regarding the complexity of the measurements required, we proved an upper bound on the level of the Clifford hierarchy. In particular, this bound is proven to be tight to the boundary identified in [23], which limits the degree of the Boolean functions that a set of operators can evaluate. In the end, we translated the examined non-adaptive MBQC evaluations to possible circuit realizations. This translation motivated our main result demonstrating a circuit separation for a family of degree two symmetric Boolean functions. For higher-degree functions, although these functions have not shown any prospect for advantage under the non-adaptive MBQC model, they guide the way to other computational models with potential advantages. Also, they can solve non-local games for which classical circuit analogs fail. Therefore, non-adaptive MBQC computations could still be exciting for studying non-locality and contextuality.

[1] Importantly, our separation indicates that for equivalent subclasses of QNC^1 and NC^1 circuits, there is a difference between quantum and classical circuits concerning the minimal size necessary to compute the identified functions, thus moving the discussion beyond the confines of constant depth circuits we mention.

References

[1] Scott Aaronson, DeVon Ingram, and William Kretschmer. The acrobatics of bqp. *arXiv preprint arXiv:2111.10409*, 2021.

[2] Richard Jozsa and Noah Linden. On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 459(2036):2011–2032, 2003.

[3] Mark Howard, Joel Wallman, Victor Veitch, and Joseph Emerson. Contextuality supplies the 'magic' for quantum computation. *Nature*, 510(7505):351–355, 2014.

[4] Juan Bermejo-Vega, Nicolas Delfosse, Dan E Browne, Cihan Okay, and Robert Raussendorf. Contextuality as a resource for models of quantum computation with qubits. *Physical review letters*, 119(12):120505, 2017.

[5] Ernesto F Galvão. Discrete Wigner functions and quantum computational speedup. *Phys. Rev. A*, 71(4):042302, apr 2005.

[6] A Mari and J Eisert. Positive Wigner Functions Render Classical Simulation of Quantum Computation Efficient. *Phys. Rev. Lett.*, 109(23):230503, dec 2012.

[7] Lov K Grover. The advantages of superposition. *Science*, 280:228, feb 1998.

[8] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, may 2001.

[9] Maarten Van den Nest, Akimasa Miyake, Wolfgang Dür, and Hans J Briegel. Universal resources for measurement-based quantum computation. *Physical review letters*, 97(15):150504, 2006.

[10] Janet Anders and Dan E. Browne. Computational power of correlations. *Phys. Rev. Lett.*, 102:050502, Feb 2009.

[11] Vincent Danos and Elham Kashefi. Determinism in the one-way model. *Phys. Rev. A*, 74(5):052310, nov 2006.

[12] Daniel E Browne, Elham Kashefi, Mehdi Mhalla, and Simon Perdrix. Generalized flow and determinism in measurement-based quantum computation. *New Journal of Physics*, 9(8):250, aug 2007.

[13] Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Average-Case Complexity Versus Approximate Simulation of Commuting Quantum Computations. *Phys. Rev. Lett.*, 117(8):080501, aug 2016.

[14] Matty J Hoban, Joel J Wallman, Hussain Anwar, Naïri Usher, Robert Raussendorf, and Dan E Browne. Measurement-based classical computation. *Physical review letters*, 112(14):140505, 2014.

[15] Michael J Bremner, Ashley Montanaro, and Dan J Shepherd. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *Quantum*, 1:8, 2017.

[16] Leonardo Novo, Juani Bermejo-Vega, and Raúl García-Patrón. Quantum advantage from energy measurements of many-body quantum systems. *Quantum*, 5:465, jun 2021.

[17] Masahito Hayashi and Yuki Takeuchi. Verifying commuting quantum computations via fidelity estimation of weighted graph states. *New Journal of Physics*, 21(9):93060, sep 2019.

[18] Julien Codsi and John van de Wetering. Classically Simulating Quantum Supremacy IQP Circuits through a Random Graph Approach. *arXiv e-prints*, page arXiv:2212.08609, December 2022.

[19] S. Takeda and A. Furusawa. Toward large-scale fault-tolerant universal photonic quantum computing. *APL Photonics*, 4(6), 06 2019. 060902.

[20] Juan Bermejo-Vega, Dominik Hangleiter, Martin Schwarz, Robert Raussendorf, and Jens Eisert. Architectures for Quantum Simulation Showing a Quantum Speedup. *Phys. Rev. X*, 8(2):021010, apr 2018.

[21] Jacob Miller, Stephen Sanders, and Akimasa Miyake. Quantum supremacy in constant-time measurement-based computation: A unified architecture for sampling and verification. *Phys. Rev. A*, 96:062320, Dec 2017.

[22] Ryuhei Mori. Periodic Fourier representation of Boolean functions. *Quantum Info. Comput.*, 19(5–6):392–412, may 2019.

[23] Markus Frembs, Sam Roberts, Earl T Campbell, and Stephen D Bartlett. Hierarchies of resources for measurement-based quantum computation. *arXiv preprint arXiv:2203.09965*, 2022.

[24] Matty J Hoban, Earl T Campbell, Klearchos Loukopoulos, and Dan E Browne. Non-adaptive measurement-based quantum computation and multi-party Bell inequalities. *New Journal of Physics*, 13(2):23014, feb 2011.

[25] Daniel Collins, Nicolas Gisin, Sandu Popescu, David Roberts, and Valerio Scarani. Bell-Type Inequalities to Detect True n-Body Nonseparability. *Phys. Rev. Lett.*, 88(17):170405, apr 2002.

[26] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86(2):419–478, apr 2014.

[27] Dmitrijs Kravčenko. *Quantum Games, Quantum States, Their Properties and Applications*. PhD thesis, Latvijas Universitāte, 2013.

[28] William Slofstra. Lower bounds on the entanglement needed to play XOR non-local games. *Journal of Mathematical Physics*, 52(10):102202, 2011.

[29] Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.

[30] Dmitri Maslov, Jin-Sung Kim, Sergey Bravyi, Theodore J Yoder, and Sarah Sheldon. Quantum advantage for computations with limited space. *Nature Physics*, 17(8):894–897, 2021.

[31] Farid Ablayev, Aida Gainutdinova, Marek Karpinski, Cristopher Moore, and Christopher Pollett. On the computational power of probabilistic and quantum branching program. *Information and Computation*, 203(2):145–162, 2005.

[32] Natalie Parham. On the Power and Limitations of Shallow Quantum Circuits. Master's thesis, University of Waterloo, 2022.

[33] Adam Bene Watts and Natalie Parham. Unconditional Quantum Advantage for Sampling with Shallow Circuits. *arXiv e-prints arXiv:2301.00995*, 2023.

Trapped-ion quantum simulations for condensed-phase chemical dynamics: seeking a quantum advantage

Mingyu Kang[1 2 *] Hanggai Nuomin[3] Sutirtha N. Chowdhury[3] Jonathon L. Yuly[4]
Ke Sun[1 2] Jacob Whitlow[1 5] Jesús Valdiviezo[6] Zhendian Zhang[3] Peng Zhang[3]
David N. Beratan[2 3 8 †] Kenneth R. Brown[1 2 3 5 ‡]

[1] *Duke Quantum Center, Duke University, Durham, NC, USA*
[2] *Department of Physics, Duke University, Durham, NC, USA*
[3] *Department of Chemistry, Duke University, Durham, NC, USA*
[4] *Lewis-Sigler Institute for Integrative Genomics, Princeton University, Princeton, NJ, USA*
[5] *Department of Electrical and Computer Engineering, Duke University, Durham, NC, USA*
[6] *Kenneth S. Pitzer Theory Center, University of California, Berkeley, CA, USA*
[7] *Department of Chemistry, University of California, Berkeley, CA, USA*
[8] *Department of Biochemistry, Duke University, Durham, NC, USA*

Abstract. Simulating the quantum dynamics of molecules in the condensed phase represents a long-standing challenge in chemistry. Trapped-ion systems may serve as a platform for the analog-quantum simulation of chemical dynamics that is beyond the reach of current classical-digital simulation. To identify a "quantum advantage", performance analysis of both classical-digital algorithms and analog-quantum simulation on noisy hardware is needed. Here, we make this comparison for the simulation of model molecular Hamiltonians that possess linear vibronic coupling, comparing the accuracy and computational cost. Further, we identify dynamical regimes where classical-digital simulations seem to have the weakest performance compared to analog-quantum simulations.

Keywords: quantum simulation, molecular dynamics, trapped ion

This extended abstract is based on the work in Ref. [1].

1 Introduction

One of the ubiquitous challenges in quantum chemistry is to describe the time-evolving dynamics of molecules, often in the condensed phase. The highest accuracy is achieved using the full quantum theory, but the computational cost grows exponentially with system size for the most reliable descriptions. As such, high-accuracy simulations of even modest-sized molecules (tens of atoms) are challenging, even on the world's finest supercomputers [2]. The most common approach to addressing quantum problems on classical computers is to use approximations. While many practical approximations are available, there is generally a trade-off between accuracy and computational cost.

It was suggested that quantum computers/simulators might provide an advantage over classical-digital simulation for problems faced in quantum chemistry, since quantum properties may be best explored using computational resources that, themselves, are intrinsically quantum mechanical [3]. This Perspective motivates the search for a quantum advantage in the area of molecular quantum dynamics [4]. Advances in understanding the physical underpinnings of photosynthesis [5, 6] and protein function [7, 8] could result from advances in quantum computing and simulations.

Finding quantum advantages requires making detailed comparisons between the strengths and weaknesses of classical-digital and quantum simulation methods. Finding opportunities where the performance of quantum simulations may surpass those of classical-digital methods is anticipated to be challenging, as over 80 years of progress in quantum calculations using classical-digital computers must be confronted by an emerging quantum-simulation technology.

We focus our attention on analog quantum simulation using trapped-ion systems. Trapped ions have excellent coherence of their internal states and allow high-fidelity state preparation, manipulation, and measurement [9]. As well, significant progress has been made to control the external degrees of freedom for trapped ions, namely their motional modes [10, 11, 12]. The internal and external states of trapped ions can be mapped onto the electronic and nuclear degrees of freedom of molecular Hamiltonians [13, 14, 15]. This makes trapped-ion systems natural candidates for analog quantum simulators of quantum molecular dynamics. The weakness of analog quantum simulation is its inaccuracy, especially as noise is intrinsic to the computing hardware.

2 Test match: classical-digital vs. analog trapped-ion simulations

We first consider simulating quantum molecular dynamics using linear vibronic coupling models (LVCMs). This class of models is approximate, and real molecules exhibit rich anharmonicities and nonlinear interactions that are beyond the reach of these simple models (see the Outlook section below). A LVCM includes M elec-

*mingyu.kang@duke.edu
†david.beratan@duke.edu
‡ken.brown@duke.edu

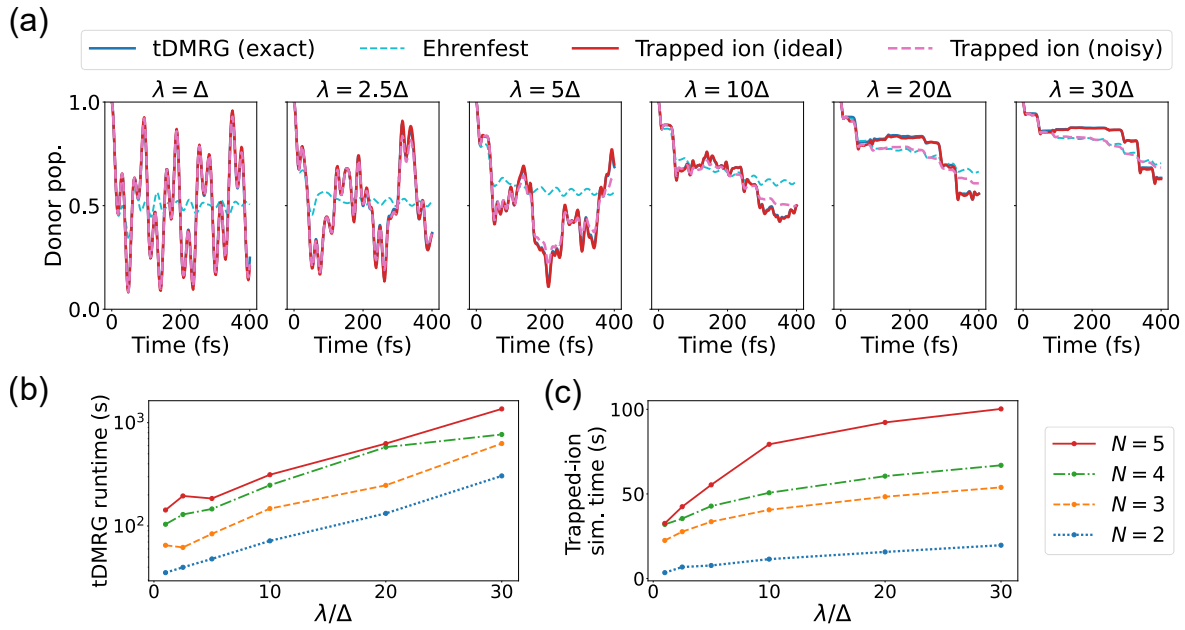


Figure 1: Comparison of classical (tDMRG and Ehrenfest) and quantum (trapped ion) methods for simulating the model Hamiltonian (1). $\Delta = 0.08679$ eV, $\nu_k = [0.08679 + 0.01240(k-1)/(N-1)]$ eV for $k = 1,..N$, where N is the number of bath modes. For the trapped-ion method, we assume using $\lceil N/2 \rceil$-ion chain to generate N radial motional modes. (a) Evolution of the donor population, for the indicated reorganization energy values (λ) and $N = 2$, simulated using various methods. For the curves labeled "Trapped ion", we numerically simulate the evolution of a trapped-ion simulator system. The ideal case assumes no decoherence, and the noisy case assumes state-of-art noise parameters, such as the motional heating rate and the coherence times of motional modes and lasers that characterize their dephasing rates. In all panels, the blue and red solid curves overlap. (b) Computational run time for the tDMRG method, with various values of λ/Δ and N. See Ref. [16] for details of the method (the start-geometry algorithm). The singular value decomposition threshold is set to 10^{-4}. Computational run time for the Ehrenfest method is negligible compared to the tDMRG method. (c) Estimated experimental time for the trapped-ion simulation, with various values of λ/Δ and N. We assume 40 equally-spaced time steps and 100 simulation runs per time step, in order to produce accurate estimates of the average donor population from the binary result of each measurement. The time spent for cooling and state preparation, which precedes each simulation, and measurement, which follows each simulation, is not included.

tronic states and N harmonic bath modes, where the bath modes represent the degrees of freedom in the intra/intermolecular vibrations and/or the vibrations of solvents. Each electronic state and the linear coupling between electronic states is often coupled linearly to the bath degrees of freedom.

The time-dependent density-matrix renormalization group (tDMRG) method [17] is an example of *numerically exact* classical-digital simulation method that can describe the dynamics of the LVCM up to a controllable error, which can be made arbitrarily small if infinite computing resources are used. The Ehrenfest method [18] is an example of *approximate* classical-digital simulation method that relies on a physical or mathematical simplification of the Hamiltonian dynamics.

Analog trapped-ion simulations can efficiently simulate the LVCM dynamics. Specifically, each term in the LVCM can be mapped to one of, or a combination of, the three native operations in trapped-ion systems: single-qubit rotation, spin-dependent force, and Mølmer-Sørensen (MS) [19] interaction (see Ref. [1] for details). Then, the evolution with respect to the full LVCM can be tracked using Trotterization [20].

Figure 1a compares the predicted performance of the analog trapped-ion simulation with two classical-digital algorithms, tDMRG and Ehrenfest, in simulating the electronic-state population dynamics of a simple LVCM. The Hamiltonian, consisting of two electronic states (donor $|D\rangle$ and acceptor $|A\rangle$) and N bath modes, is

$$\hat{H} = \frac{\Delta}{2}\left(|D\rangle\langle A| + |A\rangle\langle D|\right) + \sum_{k=1}^{N}\left[\kappa\left(|D\rangle\langle D| - |A\rangle\langle A|\right)\left(\hat{a}_k + \hat{a}_k^\dagger\right) + \nu_k \hat{a}_k^\dagger \hat{a}_k\right], \quad (1)$$

where Δ is the coupling between the two electronic states, ν_k is the energy (frequency) of the k-th bath mode, and κ is the state-dependent coupling between the states and each mode. The reorganization energy λ of the system is given by $\lambda = \kappa^2 \sum_{k=1}^{N} \frac{1}{\nu_k}$. Typical reorganization energies range from a few Δ to hundreds of Δ [21, 22]. We assume that the vibrational modes have high frequencies compared to the room temperature (times $k_B/\hbar$), such

that the average phonon number is much smaller than 1 for the initial state of each bath mode.

For all λ values examined, the populations calculated using the tDMRG and the numerical simulation of the ideal trapped-ion simulation without noise match perfectly. Indeed, both methods capture the quantum dynamics with high accuracy. The Ehrenfest method does not describe the strong population oscillations for smaller values of λ, as the effects of quantum coherence are ignored. The Ehrenfest simulations perform better when the system-bath coupling is very strong ($\lambda \gtrsim 20\Delta$), as the bath oscillators become highly excited and behave nearly classically.

For $\lambda \lesssim 5\Delta$, the populations calculated by the numerical simulation of the noisy trapped-ion simulation closely matches the ideal simulation and the tDMRG analysis, capturing many fine details of the population dynamics. However, for larger λ values, the experimental time approaches the timescale of the noise due to longer operations, so the population curve deviates from the ideal simulation. Interestingly, when λ is very large ($\gtrsim 20\Delta$), the populations of the noisy trapped-ion simulation approach those of the Ehrenfest calculations.

Figure 1b and c show the run time of the tDMRG simulation and the experimental time for the trapped-ion simulation, with various λ and N values. The run time of the tDMRG simulation increases exponentially with the value of λ. This shows that a model Hamiltonian, even as simple as (1), carries a fairly large computational cost when the entanglement between the molecular components is large. For more complicated LVCMs, where multiple electronic states are strongly coupled to each other and to many vibrational modes, the computation becomes intractable when the entanglement is large. For example, if the Hamiltonian cannot be transformed into a one-dimensional topology, the tDMRG method is inefficient even for systems with moderately large reorganization energy compared to the electronic coupling strength.

The experimental time of the trapped-ion simulations is only $\mathcal{O}(\kappa) = \mathcal{O}(\lambda^{1/2})$. This indicates that trapped ions can simulate strongly entangled dynamics rather efficiently. We expect similar scaling of experimental time to hold for simulations of more complicated models that involve MS interactions.

Combining (i) the comparison between Fig. 1b and c and (ii) the observation that noisy trapped-ion simulation and Ehrenfest calculation results match for very large λ values, we expect that trapped-ion simulations may have advantages over classical-digital methods, in terms of both computational cost and accuracy, for an *intermediate* regime of reorganization energy compared to the electronic coupling and energy gap.

3 Outlook: beyond the LVCM

The LVCM is simple, as (i) it contains only a finite number of vibrational modes that are (ii) harmonic and (iii) only linearly coupled to the electronic states. As a consequence of these simplifications, the LVCM may fail to capture several key aspects of real molecular systems.

Aside from these limitations, models beyond the LVCM might provide a compelling target to achieve quantum advantage in simulating molecular dynamics, as the LVCM is a favorable framework for classical-digital simulation. There are fundamental reasons to suggest that the approximations used in quantum-classical [23] or semiclassical [24, 25] analysis are particularly effective for dynamics generated by the LVCM. Thus, building quantum simulators for models beyond the LVCM may lead to a more immediate quantum advantage.

There are at least three ways to go beyond the LVCM to describe molecular systems more realistically, and these strategies can make classical-digital simulation methods less tractable. First, dissipation of the bath modes may be added. Second, the coupling between electronic states and bath modes may be of higher order, and the bath modes may be anharmonic.

The dissipation of bath modes can be simulated by trapped ions using sympathetic laser cooling or heating, which may require trapping two kinds of ions [4, 26, 27]. Alternatively, averaging over many instances of random stochastic operations, which does not require trapping two kinds of ions, can simulate a limited regime of dissipation [28].

The higher-order coupling and anharmonicity can be simulated by trapped ions using interactions that are resonant to higher-order sidebands, as demonstrated in recent experiments [29, 30, 31, 32, 33]. The challenge is that the higher-order sideband interactions are typically order(s) of magnitude weaker than the first-order interaction, so larger laser power and/or longer coherence times of the experimental system may be required.

4 Conclusion

In order to identify quantum advantages in simulating molecular quantum dynamics, it is essential to understand the capabilities of both classical-digital algorithms and analog quantum simulations on noisy devices. Using a simplified model Hamiltonian based on linear vibronic couplings, we suggest that analog trapped-ion simulations may have an advantage over classical-digital algorithms, in terms of accuracy and computational cost, in an intermediate regime of coupling strength between the electronic states and bath modes. LVCMs with complex connectivity between the electronic states and bath modes, or models where the bath modes are themselves dissipative, are of particular interest. Quantum advantages may also be achieved in models with nonlinear system-bath couplings and anharmonic bath modes, features that semiclassical or quantum-classical approximations struggle to treat accurately.

This Perspective is intended to inspire collaboration between the communities of quantum-chemical theory and analog quantum simulation. Analog quantum simulation may serve as a catalyst for advancing our understanding of complex chemical dynamics, and may allow studying elements of molecular realism that remain inaccessible with current classical-digital simulation approaches.

References

[1] M. Kang, K. T. Liu, S. N. Chowdhury, J. L. Yuly, K. Sun, J. Whitlow, J. Valdiviezo, Z. Zhang, P. Zhang, D. N. Beratan, and K. R. Brown, "Trapped-ion quantum simulations for condensed-phase chemical dynamics: seeking a quantum advantage," *arXiv:2305.03156*, 2023.

[2] H. R. Larsson, H. Zhai, C. J. Umrigar, and G. K.-L. Chan, "The chromium dimer: closing a chapter of quantum chemistry," *J. Am. Chem. Soc.*, vol. 144, no. 35, pp. 15932–15937, 2022.

[3] J. I. Cirac and P. Zoller, "Goals and opportunities in quantum simulation," *Nature physics*, vol. 8, no. 4, pp. 264–266, 2012.

[4] R. J. MacDonell, C. E. Dickerson, C. J. Birch, A. Kumar, C. L. Edmunds, M. J. Biercuk, C. Hempel, and I. Kassal, "Analog quantum simulation of chemical dynamics," *Chemical Science*, vol. 12, no. 28, pp. 9794–9805, 2021.

[5] L. Wang, M. A. Allodi, and G. S. Engel, "Quantum coherences reveal excited-state dynamics in biophysical systems," *Nature Reviews Chemistry*, vol. 3, no. 8, pp. 477–490, 2019.

[6] J. Cao, R. J. Cogdell, D. F. Coker, H.-G. Duan, J. Hauer, U. Kleinekathöfer, T. L. Jansen, T. Mančal, R. D. Miller, J. P. Ogilvie, *et al.*, "Quantum biology revisited," *Science Advances*, vol. 6, no. 14, p. eaaz4888, 2020.

[7] S. Hammes-Schiffer and A. V. Soudackov, "Proton-coupled electron transfer in solution, proteins, and electrochemistry," *The Journal of Physical Chemistry B*, vol. 112, no. 45, pp. 14108–14123, 2008.

[8] S. Hammes-Schiffer, "Proton-coupled electron transfer: Moving together and charging forward," *Journal of the American Chemical Society*, vol. 137, no. 28, pp. 8860–8871, 2015.

[9] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, "Trapped-ion quantum computing: Progress and challenges," *Applied Physics Reviews*, vol. 6, no. 2, p. 021314, 2019.

[10] M. Um, J. Zhang, D. Lv, Y. Lu, S. An, J.-N. Zhang, H. Nha, M. Kim, and K. Kim, "Phonon arithmetic in a trapped ion system," *Nature communications*, vol. 7, no. 1, pp. 1–7, 2016.

[11] J. Zhang, M. Um, D. Lv, J.-N. Zhang, L.-M. Duan, and K. Kim, "NOON states of nine quantized vibrations in two radial modes of a trapped ion," *Physical review letters*, vol. 121, no. 16, p. 160502, 2018.

[12] Z. Jia, Y. Wang, B. Zhang, J. Whitlow, C. Fang, J. Kim, and K. R. Brown, "Determination of multimode motional quantum states in a trapped ion system," *Physical Review Letters*, vol. 129, no. 10, p. 103602, 2022.

[13] D. J. Gorman, B. Hemmerling, E. Megidish, S. A. Moeller, P. Schindler, M. Sarovar, and H. Haeffner, "Engineering vibrationally assisted energy transfer in a trapped-ion quantum simulator," *Physical Review X*, vol. 8, no. 1, p. 011038, 2018.

[14] J. Whitlow, Z. Jia, Y. Wang, C. Fang, J. Kim, and K. R. Brown, "Simulating conical intersections with trapped ions," *arXiv:2211.07319*, 2022.

[15] C. H. Valahu, V. C. Olaya-Agudelo, R. J. MacDonell, T. Navickas, A. D. Rao, M. J. Millican, J. B. Pérez-Sánchez, J. Yuen-Zhou, M. J. Biercuk, C. Hempel, *et al.*, "Direct observation of geometric phase in dynamics around a conical intersection," *arXiv:2211.07320*, 2022.

[16] K. T. Liu, D. N. Beratan, and P. Zhang, "Improving the efficiency of open-quantum-system simulations using matrix product states in the interaction picture," *Physical Review A*, vol. 105, no. 3, p. 032406, 2022.

[17] S. R. White and A. E. Feiguin, "Real-time evolution using the density matrix renormalization group," *Physical review letters*, vol. 93, no. 7, p. 076401, 2004.

[18] P. Ehrenfest, "Bemerkung über die angenäherte gültigkeit der klassischen mechanik innerhalb der quantenmechanik," *Zeitschrift fuer Physik*, vol. 45, p. 455–457, 1927.

[19] K. Mølmer and A. Sørensen, "Multiparticle entanglement of hot trapped ions," *Physical Review Letters*, vol. 82, no. 9, p. 1835, 1999.

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. USA: Cambridge University Press, 10th ed., 2011.

[21] A. Ishizaki and G. R. Fleming, "Theoretical examination of quantum coherence in a photosynthetic system at physiological temperature," *Proc. Natl. Acad. Sci. U.S.A.*, vol. 106, no. 41, pp. 17255–17260, 2009.

[22] A. Nitzan, *Chemical dynamics in condensed phases: relaxation, transfer and reactions in condensed molecular systems*. Oxford university press, 2006.

[23] R. Kapral, "Quantum dynamics in open quantum-classical systems," *Journal of Physics: Condensed Matter*, vol. 27, no. 7, p. 073201, 2015.

[24] M. Thoss and H. Wang, "Semiclassical description of molecular dynamics based on initial-value representation methods," *Annu. Rev. Phys. Chem*, vol. 55, p. 299, 2004.

[25] M. K. Lee, P. Huo, and D. F. Coker, "Semiclassical path integral dynamics: Photosynthetic energy transfer with realistic environment interactions,"

Annu. Rev. Phys. Chem., vol. 67, no. 1, pp. 639–668, 2016.

[26] A. Lemmer, C. Cormick, D. Tamascelli, T. Schaetz, S. F. Huelga, and M. B. Plenio, "A trapped-ion simulator for spin-boson models with structured environments," *New Journal of Physics*, vol. 20, no. 7, p. 073002, 2018.

[27] F. Schlawin, M. Gessner, A. Buchleitner, T. Schätz, and S. S. Skourtis, "Continuously parametrized quantum simulation of molecular electron-transfer reactions," *PRX Quantum*, vol. 2, no. 1, p. 010314, 2021.

[28] A. Chenu, M. Beau, J. Cao, and A. del Campo, "Quantum simulation of generic many-body open system dynamics using classical noise," *Physical review letters*, vol. 118, no. 14, p. 140403, 2017.

[29] K. Marshall and D. F. James, "Linear mode-mixing of phonons with trapped ions," *Applied Physics B*, vol. 123, no. 1, p. 26, 2017.

[30] Y. Shen, Y. Lu, K. Zhang, J. Zhang, S. Zhang, J. Huh, and K. Kim, "Quantum optical emulation of molecular vibronic spectroscopy using a trapped-ion device," *Chemical science*, vol. 9, no. 4, pp. 836–840, 2018.

[31] H. Gan, G. Maslennikov, K.-W. Tseng, C. Nguyen, and D. Matsukevich, "Hybrid quantum computing with conditional beam splitter gate in trapped ion system," *Physical review letters*, vol. 124, no. 17, p. 170502, 2020.

[32] C.-H. Nguyen, K.-W. Tseng, G. Maslennikov, H. Gan, and D. Matsukevich, "Experimental swap test of infinite dimensional quantum states," *arXiv:2103.10219*, 2021.

[33] W. Chen, Y. Lu, S. Zhang, K. Zhang, G. Huang, M. Qiao, X. Su, J. Zhang, J.-N. Zhang, L. Banchi, *et al.*, "Scalable and programmable phononic network with trapped ions," *Nature Physics*, pp. 1–7, 2023.

Implementing quantum dimensionality reduction for non-Markovian stochastic simulation

Kang-Da Wu[1 2] Chengran Yang [*3] Ren-Dong He[1 2] Mile Gu[4 3 5 †]
Guo-Yong Xiang[1 2 6 ‡] Chuan-Feng Li[1 2 6] Guang-Can Guo[1 2 6] Thomas J. Elliott[7 8 9 §]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, People's Republic of China*
[2]*CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, 230026, People's Republic of China*
[3]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*
[4]*Nanyang Quantum Hub, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, Singapore*
[5]*MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, Singapore 117543, Singapore*
[6]*Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, People's Republic of China*
[7]*Department of Physics & Astronomy, University of Manchester, Manchester M13 9PL, United Kingdom*
[8]*Department of Mathematics, University of Manchester, Manchester M13 9PL, United Kingdom*
[9]*Department of Mathematics, Imperial College London, London SW7 2AZ, United Kingdom*

Abstract. Stochastic modelling enables us to understand and predict the behaviour of complex systems. Yet, accurate models of highly non-Markovian processes must track copious amounts of information about past observations, bearing high memory cost. Quantum technologies offer a promising route to mitigating this cost. We implement quantum models with a single qubit of memory using a photonic setup, and show that they can simulate a family of non-Markovian processes to higher precision than possible with any classical model of the same memory dimension. This heralds a key step towards applying quantum technologies in complex systems modelling.

Keywords: Quantum information, non-Markovianity, photonics, stochastic processes, complex systems

We are surrounded by complex processes at all scales. Faced with such rich complexity, we turn to stochastic modelling to predict the future behaviour of these processes. Often, these future behaviours – and thus our predictions – are based not only on what we can observe about the current state of the process, but also its past: they are *non-Markovian*. To simulate such processes, our models must have a memory to store information about the past. Storing all past observations comes with a prohibitively-large memory cost, forcing a more parsimonious approach to be adopted whereby we seek to distil the useful information from the past observations, and store only this. Yet, when processes are highly non-Markovian, we must typically retain information about observations far into the past, which still bears high memory costs. This leads to a bottleneck, where we trade-off reductions in the amount of past information stored against a loss in predictive accuracy.

Quantum technologies can offer a significant advantage in this endeavour, even when modelling processes with purely classical dynamics. They can be used to encode past information into quantum states to push memory costs below classical limits [1, 2]. This advantage can be particularly pronounced for highly non-Markovian processes where the separation between quantum and classical memory costs can grow without bound [3, 4, 5].

[*]yangchengran92@gmail.com
[†]mgu@quantumcomplexity.org
[‡]gyxiang@ustc.edu.cn
[§]physics@tjelliott.net

Here, we experimentally realise quantum models for a family of non-Markovian stochastic processes within a photonic system. This family of processes has a tunable parameter that controls their effective memory length, and the memory dimension of the minimal classical model grows with the value of this parameter. Our quantum models can simulate any process within the family with only a single qubit of memory. Moreover, we show that even with the experimental noise in our implementation, our models are more accurate than any distorted classical compression to a single bit of memory. Our work thus presents a key step towards demonstrating the scalability and robustness of such quantum memory advantages.

Framework and Theory. Stochastic processes consist of a series of (possibly correlated) random events occurring in sequence. We consider discrete-time stochastic processes [7], such that events occur at regular timesteps. The sequence of events can be partitioned into a past $\overleftarrow{x}$ detailing events that have already happened, and a future $\overrightarrow{x}$ containing those yet to occur. Stochastic modelling then consists of sequentially drawing samples of future events from the process given the observed past.

This requires a model that can sample from the conditional form of the process' distribution, using a memory that stores relevant information from past observations. An (impractical) brute force approach would require the model to store the full sequence of past observations. A more effective model consists of an encoding function that maps from the set of pasts to a set of memory states $\{s_j\}$, and an evolution procedure that produces

the next output (drawn according to the conditional distribution) and updates the memory state accordingly [8]. See manuscript for the full exposition.

A natural way to quantify the memory cost is in terms of the requisite size (i.e., dimension):

Definition: (Memory Cost) *The memory cost D of a model is given by the logarithm of the memory dimension, i.e., $D := \log_2 \dim(\{s_j\})$.*

The number of (qu)bits required by the model's memory system corresponds to the ceiling of this quantity. For classical models, where the memory states must all be orthogonal, the memory cost is simply given by the (logarithm of the) number of memory states, i.e., $D = \log_2 |\{s_j\}|$. Moreover, when statistically-exact sampling of the future is required, a systematic prescription for encoding the memory states with provably minimal classical memory cost D_μ is known [9, 10].

Renewal processes [11] represent a particularly apt class of stochastic process for studying the impact of non-Markovianity in stochastic modelling. They generalise Poisson processes to time-dependent decay rates. In discrete-time, families of renewal processes with tunable lengths of memory effects can be constructed, providing a means of exploring how memory costs change as non-Markovianity is increased [4, 12]. Renewal processes consist of a series of 'tick' events (labelled "1"), stochastically spaced in time; in discrete-time, timesteps where no tick occurs are denoted "0". The time between each consecutive pair of events is drawn from the same distribution. Thus, a discrete-time renewal process is fully characterised by a *survival distribution* $\Phi(n)$, codifying the probability that two consecutive tick events are at least n timesteps apart.

In this work we consider a family of renewal processes with a periodically modulated decay (PMD) rate, which we refer to as PMD processes. Their survival probability takes the form $\Phi(n) = \Gamma^n(1 - V\sin^2(n\theta))$, where $\theta := \pi/N$. Here, Γ represents the base decay factor (i.e., the probability that the process survives to the next timestep in the absence of modulation), V the strength of the modulation, and $N \in \mathbb{N}$ the period length.

For a general renewal process, the minimal memory states are synonymous with the number of timesteps since a tick event last occurred [12, 13], as the conditional distribution for the number of timesteps until next tick is unique for each n. However, due to the symmetry of PMD processes the conditional distribution repeats every N steps, and so the states group according to the value of $n \mod N$. Correspondingly, the minimal classical memory cost for statistically-exact modelling of a PMD process is $D_\mu = \log_2 N$.

Quantum models can push memory costs below classical limits [1, 2, 14] by encoding relevant past information into a set of quantum memory states (i.e., $\{s_j\} \to \{|\sigma_j\rangle\}$). By coupling the quantum memory system with an ancilla probe (initialised in a 'blank' state $|0\rangle$) at each timestep, the output statistics can be imprinted onto the probe state. See manuscript for details.

The memory cost of a quantum model is given by the (logarithm of the) span of its memory states: $D_q = \log_2(\dim(\{|\sigma_j\rangle\}))$. Thus, when these quantum memory states are linearly dependent, D_q is less than the corresponding classical cost [2, 3, 4]. Linear dependence is central to quantum memory advantage: a quantum model will still require 2^{D_μ} different memory states $\{|\sigma_j\rangle\}$ in one-to-one correspondence with the classical states, but when they are linearly dependent (such that they span a Hilbert space of dimension $2^{D_q} < 2^{D_\mu}$), a quantum memory advantage is achieved.

Result (Theory): *For any PMD process, we can construct a statistically-exact quantum model with memory cost $D_q \leq 1$.*

See manuscript for proof of this statement. That is, a statistically-exact quantum model can be constructed for any PMD process that requires only a single qubit memory. Crucially, this holds for any value of N, and so while the classical memory cost will diverge with increasing N, the quantum memory cost remains bounded. The quantum memory advantage $D_\mu - D_q$ is thus scalable. In the manuscript, we prescribe an explicit construction of such a quantum model for any given PMD process.

Experimental Implementation. We implement these memory-efficient quantum models of PMD processes using a quantum photonic setup. We outline the setup here, with full details given in the manuscript. The polarisation of a photon is used for the memory qubit, and the ancilla(e) are encoded in its path degree of freedom.

An initial state preparation module is able to initialise the memory qubit in an arbitrary pure state, together with an initial vacuum state of the ancilla. This allows us to initialise the model in the state $|\sigma_j\rangle|0\rangle$ for any of the memory states $\{|\sigma_j\rangle\}$. Following this is the the simulation module – the key part of the model – where the photon undergoes an evolution to produce the outputs and updated memory state. At each timestep the photon passes through a series of optical components that displaces the beam such that the path corresponds to the outputs $\{0, 1\}$, and the polarisation is conditionally rotated into the subsequent memory state for the next timestep. Finally, a state tomography module enables us to validate the performance of the model. By detecting the final path of the photon the output statistics of the model are manifest. Further, through tomographic reconstruction of the final polarisation of the photon (conditional for each initial state and set of outputs) we are able to verify the integrity of the final memory state, which could in principle instead been used to produce the outputs for further timesteps.

Our implementation runs the model for $L = 2$ timesteps. This is sufficient to witness the effect of memory preserved across timesteps; the conditional distribution of the second output given the first changes based on the initial memory state, indicating that information contained within this initial state is propagated across the simulation – i.e., that there is a persistent memory. We modelled multiple PMD processes with base decay factor Γ ranging from 0.49 to 0.64, period N from 3 to 8, and modulation strength $V = 0.4$.

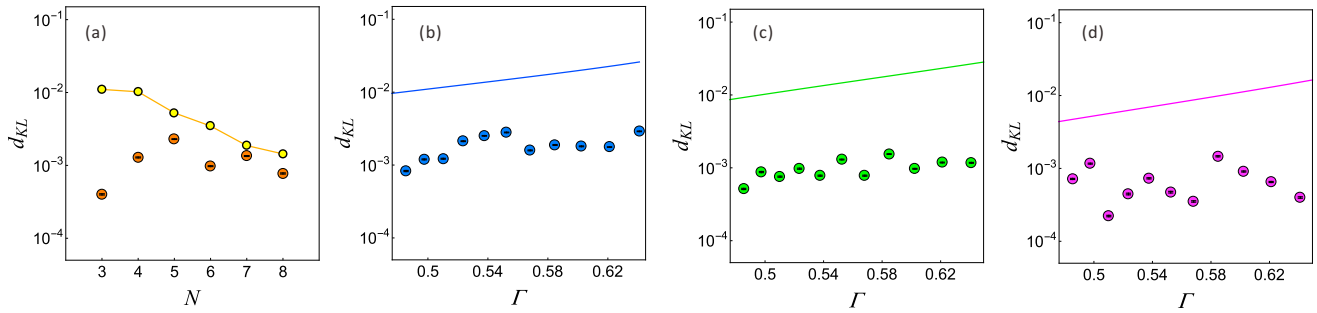


Figure 1: **Distortion of single (qu)bit memory models**. (a) KL divergence d_{KL} of experimentally-obtained statistics from our quantum models (orange) and lower bound on divergence of single bit distorted classical models (yellow) for $N = [3..8]$, $\Gamma = 0.5$, and $V = 0.4$. (b-d) Analogous plots for $N = 3$ (b), $N = 4$ (c), and $N = 5$ (d) with varying Γ. Disks show quantum model distortion, solid lines the lower bound distortion of single bit classical models.

Experimental Results. We first verify that the output statistics produced by our model are faithful to the process. Outputs are determined by measurement of the final path of the photon, each corresponding to one of the four possible outputs for two timesteps of the process $\{00, 01, 10, 11\}$. For each of parameter ranges detailed above, and for each of the initial memory states $\{|\sigma_j\rangle\}$ we obtain $\mathrm{O}(10^6)$ coincidence events, each corresponding to a single simulation run. We use these to reconstruct the probability distributions $\tilde{P}(x_0x_1|s_j)$. We quantify the distortion of the statistics using the Kullbach-Liebler (KL) divergence [15] between experimentally-reconstructed and exact theoretical distributions (see maniscript). We find that the normalised (per symbol) KL divergence d_{KL} yielded a distortion below 10^{-2} bits for all parameters simulated by our models.

Given this statistical distortion due to experimental imperfections, it would be disingenuous to consider only the memory cost of statistically-exact classical models. In order to provide a fair comparison we compare the accuracy we achieve to that of the least-distorted classical models with the same memory cost $D = 1$ (i.e., one bit). Specifically, we establish a lower bound on the smallest distortion (according to the KL divergence) that can be achieved by classical models with a single bit of memory (see manuscript). This bound is plot together with the distortion of our quantum models in Fig. 1, where we can see that our quantum models in all cases have a smaller distortion. That is, even accounting for the experimental imperfections of current quantum technologies, our quantum models of PMD processes achieve a greater accuracy than is possible with any classical model of the same memory size. Note that the distortion in the classical models here is fundamental due to the constraints on the memory size, while for the quantum case the distortion is purely due to imperfect experimental realisation.

We also verify the integrity of the final memory state at the end of our simulations. While we run our models for $L = 2$ timesteps, in principle they can be run for an arbitrarily-many timesteps given sufficient optical components as the simulation updates the memory state at each step. This continuation requires that the final memory state output by the model (i.e., the polarisation of the photon) is faithful. By tomographic reconstruction of the photon polarisation we can evaluate the infidelity of the final memory state $\tilde{\rho}$: $I(\tilde{\rho}) = 1 - \langle\sigma_k|\tilde{\rho}|\sigma_k\rangle$, where $|\sigma_k\rangle$ is the requisite final memory state given the initial state and outputs. We find that reconstructed final states are highly faithful to their corresponding requisite states (across all parameters simulated, a maximum infidelity of 0.0212 was obtained), suggesting that our simulation could be run for several more timesteps before the onset of significant degradation in the statistics.

Discussion. We report the first experimental implementation of quantum simulators of non-Markovian stochastic processes exhibiting memory advantages over optimal classical counterparts. We modelled a family of stochastic processes that have a tunable memory length, theoretically possessing a scalable quantum advantage. This advantage is robust to experimental noise introduced by our implementation, shown via comparison with bounds on the smallest noise achievable with classical models of the same memory cost.

The photonic setup in which we have implemented our quantum models is well-suited to the task at hand. As the circuit is fixed, the optical components can be finely calibrated in advance to achieve much smaller errors than typical of current universal quantum processors. Furthermore, our setup can readily be modified to simulate other non-Markovian stochastic processes; by adjusting only single-qubit unitaries acting on photon polarisation our setup can implement single-qubit-memory quantum models (exact if possible, approximate otherwise [5]) of *any* renewal process.

A further advantage of our quantum models is that the outputs are not measured until the final step, up until which the output system is in a weighted superposition of the possible output strings [16]. This quantum sample ('*q-sample*') state can be used as an input to quantum algorithms for e.g., quantum-enhanced stochastic analysis [17] with potential applications in financial modelling [18, 19]. Quantum models of stochastic processes have also been shown to exhibit other advantages over classical models that can be explored, such as reduced thermal dissipation [20, 21].

References

[1] M. Gu, K. Wiesner, E. Rieper, and V. Vedral, Quantum mechanics can reduce the complexity of classical models, Nature Communications **3**, 762 (2012).

[2] Q. Liu, T. J. Elliott, F. C. Binder, C. Di Franco, and M. Gu, Optimal stochastic modeling with unitary quantum dynamics, Physical Review A **99**, 062110 (2019).

[3] J. Thompson, A. J. P. Garner, J. R. Mahoney, J. P. Crutchfield, V. Vedral, and M. Gu, Causal asymmetry in a quantum world, Physical Review X **8**, 031013 (2018).

[4] T. J. Elliott, C. Yang, F. C. Binder, A. J. P. Garner, J. Thompson, and M. Gu, Extreme dimensionality reduction with quantum modeling, Physical Review Letters **125**, 260501 (2020).

[5] T. J. Elliott, Quantum coarse graining for extreme dimension reduction in modeling stochastic temporal dynamics, PRX Quantum **2**, 020342 (2021).

[6] F. Ghafari, N. Tischler, J. Thompson, M. Gu, L. K. Shalm, V. B. Verma, S. W. Nam, R. B. Patel, H. M. Wiseman, and G. J. Pryde, Dimensional quantum memory advantage in the simulation of stochastic processes, Physical Review X **9**, 041013 (2019).

[7] A. Khintchine, Korrelationstheorie der stationären stochastischen Prozesse, Mathematische Annalen **109**, 604 (1934).

[8] J. P. Crutchfield, Between order and chaos, Nature Physics **8**, 17 (2012).

[9] J. P. Crutchfield and K. Young, Inferring statistical complexity, Physical Review Letters **63**, 105 (1989).

[10] C. R. Shalizi and J. P. Crutchfield, Computational mechanics: Pattern and prediction, structure and simplicity, Journal of Statistical Physics **104**, 817 (2001).

[11] W. L. Smith, Renewal theory and its ramifications, Journal of the Royal Statistical Society: Series B (Methodological) **20**, 243 (1958).

[12] S. E. Marzen and J. P. Crutchfield, Informational and causal architecture of discrete-time renewal processes, Entropy **17**, 4891 (2015).

[13] T. J. Elliott and M. Gu, Superior memory efficiency of quantum devices for the simulation of continuous-time stochastic processes, npj Quantum Information **4**, 18 (2018).

[14] S. P. Loomis and J. P. Crutchfield, Strong and weak optimizations in classical and quantum models of stochastic processes, Journal of Statistical Physics **176**, 1317 (2019).

[15] T. M. Cover and J. A. Thomas, *Elements of information theory* (John Wiley & Sons, 2012).

[16] F. Ghafari, N. Tischler, C. Di Franco, J. Thompson, M. Gu, and G. J. Pryde, Interfering trajectories in experimental quantum-enhanced stochastic simulation, Nature Communications **10**, 1 (2019).

[17] C. Blank, D. K. Park, and F. Petruccione, Quantum-enhanced analysis of discrete stochastic processes, npj Quantum Information **7**, 1 (2021).

[18] S. Woerner and D. J. Egger, Quantum risk analysis, npj Quantum Information **5**, 1 (2019).

[19] N. Stamatopoulos, D. J. Egger, Y. Sun, C. Zoufal, R. Iten, N. Shen, and S. Woerner, Option pricing using quantum computers, Quantum **4**, 291 (2020).

[20] S. P. Loomis and J. P. Crutchfield, Thermal efficiency of quantum memory compression, Physical Review Letters **125**, 020601 (2020).

[21] T. J. Elliott, Memory compression and thermal efficiency of quantum implementations of nondeterministic hidden Markov models, Physical Review A **103**, 052615 (2021).

[22] M. P. Woods, R. Silva, G. Pütz, S. Stupar, and R. Renner, Quantum clocks are more accurate than classical ones, PRX Quantum **3**, 010319 (2022).

[23] Y. Yang and R. Renner, Ultimate limit on time signal generation, arXiv:2004.07857 (2020).

[24] C. Budroni, G. Vitagliano, and M. P. Woods, Ticking-clock performance enhanced by nonclassical temporal correlations, Physical Review Research **3**, 033051 (2021).

[25] Z. Li, H. Zhang, and H. Zhu, Implementation of generalized measurements on a qudit via quantum walks, Phys. Rev. A **99**, 062342 (2019).

[26] T. J. Elliott, M. Gu, A. J. Garner, and J. Thompson, Quantum adaptive agents with efficient long-term memories, Physical Review X **12**, 011007 (2022).

[27] G. D. Paparo, V. Dunjko, A. Makmal, M. A. Martin-Delgado, and H. J. Briegel, Quantum speedup for active learning agents, Physical Review X **4**, 031002 (2014).

[28] V. Dunjko and H. J. Briegel, Machine learning & artificial intelligence in the quantum domain: a review of recent progress, Reports on Progress in Physics **81**, 074001 (2018).

[29] S. Milz and K. Modi, Quantum stochastic processes and quantum non-Markovian phenomena, PRX Quantum **2**, 030201 (2021).

[30] P. Taranto, F. A. Pollock, S. Milz, M. Tomamichel, and K. Modi, Quantum Markov order, Physical Review Letters **122**, 140401 (2019).

[31] P. Taranto, S. Milz, F. A. Pollock, and K. Modi, Structure of quantum stochastic processes with finite Markov order, Physical Review A **99**, 042108 (2019).

[32] C. Aghamohammadi, S. P. Loomis, J. R. Mahoney, and J. P. Crutchfield, Extreme quantum memory advantage for rare-event sampling, Physical Review X **8**, 011025 (2018).

[33] C. K. Hong and L. Mandel, Experimental realization of a localized one-photon state, Phys. Rev. Lett. **56**, 58 (1986).

[34] Z. Hou, J.-F. Tang, J. Shang, H. Zhu, J. Li, Y. Yuan, K.-D. Wu, G.-Y. Xiang, C.-F. Li, and G.-C. Guo, Deterministic realization of collective measurements via photonic quantum walks, Nature Communications **9**, 1 (2018).

[35] Y.-Y. Zhao, N.-K. Yu, P. Kurzyński, G.-Y. Xiang, C.-F. Li, and G.-C. Guo, Experimental realization of generalized qubit measurements based on quantum walks, Phys. Rev. A **91**, 042101 (2015).

[36] P. Xue, R. Zhang, H. Qin, X. Zhan, Z. H. Bian, J. Li, and B. C. Sanders, Experimental quantum-walk revival with a time-dependent coin, Phys. Rev. Lett. **114**, 140502 (2015).

[37] N. Tishby, F. C. Pereira, and W. Bialek, The information bottleneck method, arXiv:physics/0004057 (2000).

[38] C. Yang, A. Garner, F. Liu, N. Tischler, J. Thompson, M.-H. Yung, M. Gu, and O. Dahlsten, Provable superior accuracy in machine learned quantum models, arXiv:2105.14434 (2021).

Efficient Learning of Continuous-Variable Quantum States

Ya-Dong Wu[1] Giulio Chiribella[1 2 3 *] Nana Liu[4 5 6 †]

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

[2] *Department of Computer Science, Parks Road, Oxford, OX1 3QD, UK*

[3] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*

[4] *Institute of Natural Sciences, Shanghai Jiao Tong University, Shanghai 200240, China*

[5] *Ministry of Education, Key Laboratory in Scientific and Engineering Computing, Shanghai Jiao Tong University, Shanghai 200240, China*

[6] *University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai 200240, China*

Abstract. The characterization of continuous-variable quantum states is crucial for applications in quantum communication, sensing, and computing. However, a full characterization of multimode quantum states requires a number of experiments that grows exponentially with the number of modes. Here we propose an alternative approach where the goal is not to reconstruct the full quantum state, but rather to estimate its characteristic function at a given set of points. For multimode states with reflection symmetry, we show that the characteristic function at M points can be estimated using only $O(\log M)$ copies of the state, independently of the number of modes. The number of copies can be further reduced to a constant when the characteristic function is known to be positive, as in the case of squeezed vacuum states. In these cases, the estimation is achieved by an experimentally friendly setup.

Keywords: continuous variable, shadow tomography, quantum state characterization

1 Introduction

Continuous-variable (CV) quantum systems [1, 2] are an important platform for quantum computing, simulation, sensing and communication. A large body of work has been devoted to the characterization of CV quantum states, exploring a variety of techniques including quantum tomography [3, 4], quantum compressed sensing [5], quantum fidelity estimation [6], detection of nonclassicality [7], certification of quantum states [8, 9, 10, 11] and CV classical shadow tomography [12, 13, 14]. Recently, classical machine learning techniques have been applied to the characterization of CV states [15, 16, 17, 18, 19, 20, 21].

The full characterization of a multimode quantum state generally requires measurements on an exponential number of copies of the state, and therefore becomes unfeasible when the number of modes is large. Here, we explore an alternative approach, where the goal is not to completely characterize the state, but rather to estimate its characteristic function at a finite number of points. Having an estimate of the characteristic function is important for estimating physical properties, such as amount of nonclassicality [7], non-Gaussianity [16, 22], or the fidelity with a given target state [6]. The characteristic function is also important in the study of quantum information scrambling in phase space [23], and its estimation is often used as the first step in experimental schemes of CV state tomography [24, 25, 26].

2 Background

To get around the exponential complexity of quantum state tomography, Huang *et al.* proposed classical shadow tomography [27], which has been recently extended to CV quantum states [12, 13, 14]. When used to estimate the expectation values of any of all 4^n Pauli observables on an n-qubit state, however, classical shadow tomography still requires an exponential number of measurements. To provide an efficient estimate of all Pauli observables, a quantum strategy using global measurements on multiple copies was then shown [28]. In the following we will establish an analogue result for CV systems, with the crucial difference that instead of estimating the expectation values of an arbitrary set of observables, we will estimate the values of the characteristic function at an arbitrary set of phase space points.

Consider a k-mode quantum system, described by the Hilbert space $\mathcal{H}^{\otimes k}$ where each $\mathcal{H}$ is an infinite-dimensional Hilbert space. A multimode displacement operator is s unitary operator of the form $D(\boldsymbol{\alpha}) = \mathrm{e}^{\boldsymbol{\alpha}\hat{\boldsymbol{a}}^\dagger - \bar{\boldsymbol{\alpha}}\hat{\boldsymbol{a}}}$, where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k) \in \mathbb{C}^k$, $\hat{\boldsymbol{a}} = (\hat{a}_1, \ldots, \hat{a}_k)^\top$, $\hat{\boldsymbol{a}}^\dagger = (\hat{a}_1^\dagger, \ldots, \hat{a}_k^\dagger)^\top$, $\hat{a}_j$ and $\hat{a}_j^\dagger$ are the annihilation and creation operators for j-th mode, and satisfy the canonical communication relations $\left[\hat{a}_j, \hat{a}_l^\dagger\right] = \delta_{jl}$ for every j and l.

The characteristic function of a quantum state ρ is defined as $C_\rho(\boldsymbol{\alpha}) := \mathrm{tr}[D(-\mathrm{i}\boldsymbol{\alpha})\rho]$ [29]. It fully characterizes the quantum state ρ, which can be reconstructed with the tomographic formula $\rho = 1/\pi^k \int_{\mathbb{C}^k} d^{2k}\boldsymbol{\alpha}\, C_\rho(\boldsymbol{\alpha})\, D(i\boldsymbol{\alpha})$. The Wigner function, often used to represent CV states, can be obtained from the characteristic function via a Fourier transform in phase space [30, 29, 31].

A simple way to estimate the characteristic function at a specific point $\boldsymbol{\alpha}$ is to subject each mode j to a homodyne measurement, *i.e.* a projective measurement of the quadrature operator $Q_{\alpha_j} := (\alpha_j\, \hat{a}_j^\dagger + \overline{\alpha}_j\, \hat{a}_j)/|\sqrt{2}\alpha_j|$. From the value of the measurement outcome q_j, one can

*giulio@cs.hku.hk

†nana.liu@quantumlah.org

then evaluate the empirical average of the exponential $\exp[-i\sum_{j=1}^{k} q_j\,|\sqrt{2}\alpha_j|]$, which provides an estimate of the characteristic function when averaged over many repetitions of the measurement procedure. This approach is commonly used in quantum state tomography due to its ease of implementation [4]. On the other hand, it has the obvious limitation that the sample complexity grows linearly with the number of points where the characteristic function is evaluated. In the following, we provide an exponentially more efficient method.

3 Efficient estimation of the characteristic function

Our method applies to quantum states with *reflection symmetry*, that is, quantum states ρ for which there exists a $k\times k$ unitary matrix U such that $C_\rho(\overline{\boldsymbol{\alpha}}) = C_\rho(\boldsymbol{\alpha}U)$ for every vector of displacements $\boldsymbol{\alpha}$. In the single-mode case, quantum states with reflection symmetry include important classes of states such as Gaussian states with zero mean values, Fock states, Gottesman-Kitaev-Preskill (GKP) states [32], Schrödinger cat states [33] and binomial code states [34].

Our main result is the following theorem, which provides a method for estimating the characteristic function of a multimode state with reflection symmetry. The sample complexity of our estimation strategy is independent of the number of modes, and logarithmic in the number of evaluation points.

Theorem 1 *For every k-mode state ρ with reflection symmetry, the values of the characteristic function $C_\rho(\boldsymbol{\alpha})$ at M given points $\{\boldsymbol{\alpha}_i\}_{i=1}^M$ can be accurately estimated using $O(\log M)$ copies, independently of k. Specifically, $O(1/\epsilon^4\log(M/\delta))$ copies are sufficient to produce an estimate $\widehat{C_\rho(\boldsymbol{\alpha})}$ that satisfies the condition* $\mathsf{Prob}\left(\max_i \left|\widehat{C_\rho(\boldsymbol{\alpha}_i)} - C_\rho(\boldsymbol{\alpha}_i)\right| > \epsilon\right) < \delta$ *for any fixed $\epsilon>0$ and $\delta>0$.*

The theorem is based on two techniques, which are interesting in their own right. The first technique allows one to estimate the product $C_\rho(\boldsymbol{\alpha})C_\rho(\overline{\boldsymbol{\alpha}})$ for an arbitrary CV state ρ, without any assumption of reflection symmetry. The measurements used in the estimation are experimentally friendly, requiring only beamsplitters and homodyne detections. The sample complexity of this strategy is constant in the number of modes, and depends only on the chosen error threshold:

Lemma 2 *For every k-mode state ρ, $O(\log(1/\delta)/\epsilon^2)$ copies of ρ are sufficient to produce an estimate $\widehat{C_\rho(\boldsymbol{\alpha})C_\rho(\bar{\boldsymbol{\alpha}})}$ that satisfies the condition* $\mathsf{Prob}\left(\left|\widehat{C_\rho(\boldsymbol{\alpha})C_\rho(\bar{\boldsymbol{\alpha}})} - C_\rho(\boldsymbol{\alpha})C_\rho(\bar{\boldsymbol{\alpha}})\right| > \epsilon\right) < \delta\,, \forall \alpha\in\mathbb{C}^k$. *The protocol and its sample complexity are independent of $\boldsymbol{\alpha}$.*

In the single-mode case, the joint measurement is achieved by a simple setup, illustrated in Fig. 1(a): The product state $\rho\otimes\rho$ goes through a balanced beam splitter

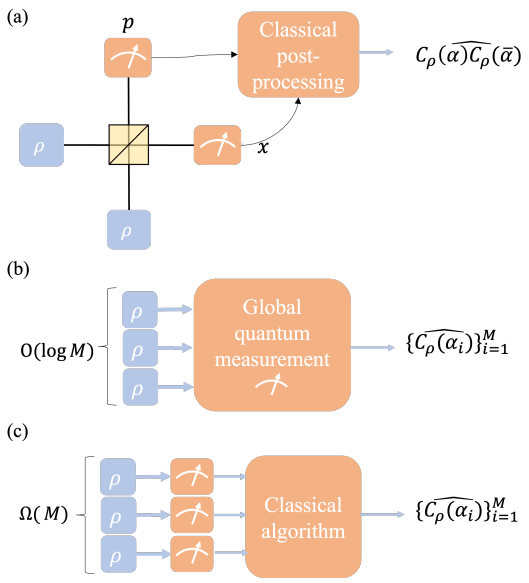


Figure 1: (a) estimation of $C_\rho(\alpha)C_\rho(\overline{\alpha})$ using a balanced beam splitter and two homodyne measurements. (b) estimation of the characteristic function at M phase-space points using global measurements, and (c) conventional scenarios using single-copy measurements.

followed by two homodyne detections on the two ouput modes, measuring on the spectral resolutions of the the position operator $\hat{x} := (\hat{a}+\hat{a}^\dagger)/\sqrt{2}$ and the momentum operator $\hat{p} := (\hat{a}-\hat{a}^\dagger)/(\sqrt{2}\mathrm{i})$, respectively. Denoting the two measurement outcomes by x and p respectively, we have

$$\langle D(-\mathrm{i}\alpha)\otimes D(-\mathrm{i}\bar{\alpha})\rangle_{\rho\otimes\rho} = \mathbb{E}\left[\mathrm{e}^{-2\mathrm{i}(\mathrm{Re}(\alpha)x+\mathrm{Im}(\alpha)p)}\right]\,, \quad (1)$$

where $\mathbb{E}$ denotes the expectation value over all possible pairs (x,p) of measurement outcomes obtained in the experiment.

For states with reflection symmetry, the estimation of the product $C_\rho(\boldsymbol{\alpha})C_\rho(\bar{\boldsymbol{\alpha}})$ is equivalent to the estimation of the square of the characteristic function $C_\rho(\boldsymbol{\alpha})^2$. This fact is evident for states satisfying the condition $C_\rho(\bar{\boldsymbol{\alpha}}) = C_\rho(\boldsymbol{\alpha})$. For characteristic functions with reflection symmetry, the result in Lemma 2 can be used to estimate the purity $\mathrm{tr}(\rho^2) = 1/\pi^{2k}\int_{\mathbb{C}^k} d^{2k}\boldsymbol{\alpha}|C_\rho(\boldsymbol{\alpha})^2|$. Lemma 2 has another important implication: if we know that the characteristic function of the state is has reflection symmetry, and, in addition, is positive, then we can estimate its value at M phase points with a *constant* number of copies, independent of k and M.

Corollary 3 *For every k-mode state ρ with reflection symmetry and positive characteristic function, the values of the characteristic function at M given points can be estimated from $O(\log(1/\delta)/\epsilon^2)$ copies using only beamsplitters and homodyne measurements.*

This result can be used to estimate the characteristic function of squeezed vacuum states with known phase, both in the single-mode and in the multimode scenario.

Let us consider now the general case where the characteristic function can take arbitrary complex values. In

this case, the square $C_\rho(\boldsymbol{\alpha})^2$ determines the value of the characteristic function up to a sign. The second technique used in the derivation of Theorem 1 is a method for identifying the correct sign of the characteristic function.

Lemma 4 *Let ρ be a k-mode CV state and let $\{\boldsymbol{\alpha}_i\}_{i=1}^L$ be a set of phase space points satisfying the condition $|C_\rho(\boldsymbol{\alpha_i})| > \epsilon$ for every $i \in \{1,\dots,L\}$. Then, the signs of all $C_\rho(\boldsymbol{\alpha_i})$ can be estimated from $O(1/\epsilon^2 \log(L/\delta))$ copies of ρ with probability of error at most δ.*

Combining Lemma 2 and Lemma 4, we then obtain Theorem 1. To estimate the characteristic function up to error ϵ, we first estimate its square $C_\rho(\boldsymbol{\alpha})^2$ up to error $O(\epsilon^2)$, using the technique provided by Lemma 2. This step requires $O(\log(1/\delta)/\epsilon^4)$ copies of the state ρ. We then check whether the modulus of the estimate is close to zero for the M values of interest. If $\left|\widehat{C_\rho(\boldsymbol{\alpha}_i)^2}\right|$ is less than $4\epsilon^2/9$, we set the estimate of the characteristic function to zero, namely $\widehat{C_\rho(\boldsymbol{\alpha}_i)} = 0$. Otherwise, we can estimate the sign of the characteristic function. By Lemma 4, this step consumes $O(\epsilon^{-2}\log(M/\delta))$.

4 Comparison with conventional scenarios

Theorem 1 shows that the characteristic function at M points can be accurately estimated using global measurements on $O(\log M)$ copies of the state, as illustrated in Figure 1(b). This setting is different from that of conventional scenarios in which each copy of the state undergoes an individual measurement [Figure 1(c)] Consider for example the naive conventional scenario in which each copy is used to estimate the value of the characteristic function value at one specific point. Intuitively, estimating M different values in this naive setting will require a number of samples growing linearly in M, no matter what kind of classical post-processing is done on the experimental data. This intuition can be made rigorous using the results of Ref. [28] on the complexity of learning point functions. This result can be summarized in the following proposition.

Proposition 5 *For every reflection symmetric CV state, the sample complexity of the estimation of the characteristic function at M points up to a constant error with high probability is at least $\Omega(M)$ using individual measurements in the naive scenario.*

Our method also exhibits advantages over classical shadow tomography. When used for estimating a set of observables over a k-mode CV state, existing methods of classical shadow tomography using homodyne measurements [13, 14] have a sample complexity growing exponentially with k, in contrast with the sample complexity of our method, which is independent of k. Moreover, classical shadow tomography approaches require a truncation, either in Fock space or the phase space, which is not necessary in our method for estimation of point values of a state characteristic function.

5 Application: estimation of CV observables

Our method for estimating the characteristic function can be used to estimate the expectation value of a variety of CV observables. In general, the expectation value of a k-mode observable O on a state ρ is given by the tomographic formula $\mathrm{tr}[O\,\rho] = \int \mathrm{d}^{2k}\boldsymbol{\alpha}\, C_\rho(\boldsymbol{\alpha})\, C_O(-\boldsymbol{\alpha})/\pi^k$, with $C_0(\boldsymbol{\alpha}) := \mathrm{tr}[O\,D(-i\boldsymbol{\alpha})]$ [31]. Now, suppose that the observable satisfies the condition $|\int_{\boldsymbol{\alpha}\notin\mathcal{A}} \mathrm{d}^{2k}\boldsymbol{\alpha}\, C_\rho(\boldsymbol{\alpha})\, C_O(-\boldsymbol{\alpha})| < \epsilon/2$ for some $\epsilon > 0$ and some compact region $\mathcal{A} \subset \mathbb{C}^k$. For example, this condition is satisfied if $C_O(\boldsymbol{\alpha})$ decays exponentially with $|\boldsymbol{\alpha}|$, as it happens *e.g.* when O is the fidelity with a k-mode coherent state and the region $\mathcal{A}$ is large compared to the amplitude of such state. In this case, an estimate of the expectation value of O can be obtained by randomly sampling M points inside $\mathcal{A}$ and by estimating the characteristic function of ρ at these points. In the Supplemental Material, we show that picking $M = 16\sigma_M^2|\mathcal{A}|^2/\epsilon^2$, where $\sigma_M^2 := \frac{1}{M-1}\sum_{i=1}^M \left(\widehat{C_\rho(\alpha_i)}C_O(-\alpha_i) - \frac{1}{M}\sum_{i=1}^M \widehat{C_\rho(\alpha_i)}C_O(-\alpha_i)\right)^2$ and $|\mathcal{A}|$ is the volume of $\mathcal{A}$, and estimating the characteristic function with error $\tilde{\epsilon} = \epsilon/(4|\mathcal{A}|)$ guarantees an accurate estimate of $\mathrm{tr}[O\rho]$.

Corollary 6 *The expectation value of a k-mode observable O on a state ρ can be estimated using $O\left(|\mathcal{A}|^4/\epsilon^4 \log(|\mathcal{A}|^2/(\epsilon^2\delta))\right)$ copies of ρ and the estimate $o := \frac{|\mathcal{A}|}{\pi^2 M}\sum_{i=1}^M \widehat{C_\rho(\boldsymbol{\alpha}_i)}C_O(\boldsymbol{\alpha}_i)$ satisfies the condition $\mathsf{Prob}\left(|o - \mathrm{tr}(\rho O)| \gtrsim \epsilon\right) < \delta$, where $\sim$ comes from the approximation of estimation error of Monte Carlo integration.*

Note also that the same randomly sampled points can be used for multiple observables O, provided that all observables have a small contribution outside the region $\mathcal{A}$. Hence, the sample complexity of the estimation depends on the region $\mathcal{A}$, and is independent of the number of observables.

6 Conclusions

We have shown that the characteristic function of a multimode state with reflection symmetry can be estimated at M points using $O(\log M)$ copies of the state, independently of the number of modes. This contrasts with the naive conventional scenario, where $\Omega(M)$ copies of ρ are required. For states with positive characteristic function, such as squeezed vacuum states, the sample complexity can be further reduced to a constant, independent of the number of points and on the number of modes. In this case, the estimation is achieved by an experimentally-friendly setup that uses only beamsplitters and homodyne measurements.

A full technical version of this work can be found via the link https://arxiv.org/abs/2303.05097.

References

[1] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, pp. 513–577, Jun 2005.

[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, pp. 621–669, May 2012.

[3] G. M. D'Ariano, M. G. Paris, and M. F. Sacchi, "Quantum tomography," *Advances in Imaging and Electron Physics*, vol. 128, pp. 206–309, 2003.

[4] A. I. Lvovsky and M. G. Raymer, "Continuous-variable optical quantum-state tomography," *Rev. Mod. Phys.*, vol. 81, pp. 299–332, Mar 2009.

[5] M. Ohliger, V. Nesme, D. Gross, Y.-K. Liu, and J. Eisert, "Continuous-variable quantum compressed sensing," *arXiv preprint arXiv:1111.0853*, 2011.

[6] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, "Practical characterization of quantum devices without tomography," *Phys. Rev. Lett.*, vol. 107, p. 210404, Nov 2011.

[7] A. Mari, K. Kieling, B. M. Nielsen, E. S. Polzik, and J. Eisert, "Directly estimating nonclassicality," *Phys. Rev. Lett.*, vol. 106, p. 010403, Jan 2011.

[8] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, "Reliable quantum certification of photonic state preparations," *Nat. Commun.*, vol. 6, no. 8498, pp. 1–8, 2015.

[9] Y.-D. Wu, G. Bai, G. Chiribella, and N. Liu, "Efficient verification of continuous-variable quantum states and devices without assuming identical and independent operations," *Phys. Rev. Lett.*, vol. 126, p. 240503, Jun 2021.

[10] U. Chabaud, G. Roeland, M. Walschaers, F. Grosshans, V. Parigi, D. Markham, and N. Treps, "Certification of non-gaussian states with operational measurements," *PRX Quantum*, vol. 2, p. 020333, Jun 2021.

[11] Y.-D. Wu, "Reliable quantum certification of bosonic code preparations," *arXiv preprint arXiv:2211.16777*, 2022.

[12] J. T. Iosue, K. Sharma, M. J. Gullans, and V. V. Albert, "Continuous-variable quantum state designs: theory and applications," *arXiv preprint arXiv:2211.05127*, 2022.

[13] S. Gandhari, V. Albert, J. Taylor, and M. Gullans, "Shadow tomography of continuous-variable quantum systems," *arXiv preprint arXiv:2211.05149*, 2022.

[14] S. Becker, N. Datta, L. Lami, and C. Rouzé, "Classical shadow tomography for continuous variables quantum systems," *arXiv preprint arXiv:2211.07578*, 2022.

[15] E. S. Tiunov, V. Tiunova, A. E. Ulanov, A. Lvovsky, and A. K. Fedorov, "Experimental quantum homodyne tomography via machine learning," *Optica*, vol. 7, no. 5, pp. 448–454, 2020.

[16] V. Cimini, M. Barbieri, N. Treps, M. Walschaers, and V. Parigi, "Neural networks for detecting multimode wigner negativity," *Phys. Rev. Lett.*, vol. 125, p. 160504, Oct 2020.

[17] S. Ahmed, C. Sánchez Muñoz, F. Nori, and A. F. Kockum, "Quantum state tomography with conditional generative adversarial networks," *Phys. Rev. Lett.*, vol. 127, p. 140502, Sep 2021.

[18] S. Ahmed, C. Sánchez Muñoz, F. Nori, and A. F. Kockum, "Classification and reconstruction of optical quantum states with deep neural networks," *Phys. Rev. Res.*, vol. 3, p. 033278, Sep 2021.

[19] H.-Y. Hsieh, Y.-R. Chen, H.-C. Wu, H. L. Chen, J. Ning, Y.-C. Huang, C.-M. Wu, and R.-K. Lee, "Extract the degradation information in squeezed states with machine learning," *Phys. Rev. Lett.*, vol. 128, p. 073604, Feb 2022.

[20] Y. Zhu, Y.-D. Wu, G. Bai, D.-S. Wang, Y. Wang, and G. Chiribella, "Flexible learning of quantum states with generative query neural networks," *Nat. Commun.*, vol. 13, p. 6222, 2022.

[21] Y.-D. Wu, Y. Zhu, G. Bai, Y. Wang, and G. Chiribella, "A data-driven approach to quantum cross-platform verification," *arXiv:2211.01668*, 2022.

[22] M. Walschaers, "Non-gaussian quantum states and where to find them," *PRX Quantum*, vol. 2, p. 030204, Sep 2021.

[23] Q. Zhuang, T. Schuster, B. Yoshida, and N. Y. Yao, "Scrambling and complexity in phase space," *Phys. Rev. A*, vol. 99, p. 062334, Jun 2019.

[24] C. Flühmann and J. P. Home, "Direct characteristic-function tomography of quantum states of the trapped-ion motional oscillator," *Phys. Rev. Lett.*, vol. 125, p. 043602, Jul 2020.

[25] P. Campagne-Ibarcq, A. Eickbusch, S. Touzard, E. Zalys-Geller, N. E. Frattini, V. V. Sivak, P. Reinhold, S. Puri, S. Shankar, R. J. Schoelkopf, *et al.*, "Quantum error correction of a qubit encoded in grid states of an oscillator," *Nature*, vol. 584, no. 7821, pp. 368–372, 2020.

[26] A. Eickbusch, V. Sivak, A. Z. Ding, S. S. Elder, S. R. Jha, J. Venkatraman, B. Royer, S. Girvin, R. J. Schoelkopf, and M. H. Devoret, "Fast universal control of an oscillator with weak dispersive coupling to

a qubit," *Nature Phys.*, vol. 18, no. 12, pp. 1464–1469, 2022.

[27] H.-Y. Huang, R. Kueng, and J. Preskill, "Predicting many properties of a quantum system from very few measurements," *Nat. Phys.*, vol. 16, no. 10, pp. 1050–1057, 2020.

[28] H.-Y. Huang, R. Kueng, and J. Preskill, "Information-theoretic bounds on quantum advantage in machine learning," *Phys. Rev. Lett.*, vol. 126, p. 190505, May 2021.

[29] U. Leonhardt, *Measuring the quantum state of light*, vol. 22. Cambridge university press, 1997.

[30] M. O. Scully, M. S. Zubairy, *et al.*, *Quantum Optics*. Cambridge University Press, 1997.

[31] A. Serafini, *Quantum continuous variables: a primer of theoretical methods*. CRC press, 2017.

[32] D. Gottesman, A. Kitaev, and J. Preskill, "Encoding a qubit in an oscillator," *Phys. Rev. A*, vol. 64, p. 012310, Jun 2001.

[33] M. Mirrahimi, Z. Leghtas, V. V. Albert, S. Touzard, R. J. Schoelkopf, L. Jiang, and M. H. Devoret, "Dynamically protected cat-qubits: a new paradigm for universal quantum computation," *New J. Phys.*, vol. 16, no. 4, p. 045014, 2014.

[34] M. H. Michael, M. Silveri, R. T. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin, "New class of quantum error-correcting codes for a bosonic mode," *Phys. Rev. X*, vol. 6, p. 031006, Jul 2016.

Tensor network algorithm for simulating experimental Gaussian boson sampling

Changhun Oh[1 *] Minzhao Liu[2 3] Yuri Alexeev[3 4 5] Bill Fefferman[4] Liang Jiang[1]

[1] *Pritzker School of Molecular Engineering, The University of Chicago, Chicago, Illinois 60637, USA*
[2] *Department of Physics, The University of Chicago, Chicago, Illinois 60637, USA*
[3] *Computational Science Division, Argonne National Laboratory, Lemont, Illinois 60439, USA*
[4] *Department of Computer Science, The University of Chicago, Chicago, Illinois 60637, USA*
[5] *Chicago Quantum Exchange, Chicago, Illinois 60637, USA*

Abstract. Gaussian boson sampling is a sampling task that has been used to experimentally demonstrate quantum computational advantage. While a common critical weakness of the current Gaussian boson sampling experiments is a large amount of photon loss, they are claimed to be hard to classically simulate with the best-known classical algorithm even under the loss. In this work, we present a novel classical algorithm that simulates Gaussian boson sampling and whose complexity can be significantly reduced when the photon loss rate is large. The key observation is that due to the large photon loss, the actual quantum resources are much smaller and thermal photons generated by photon loss are dominant and that a tensor network method can take advantage of such a property. Using the proposed algorithm we simulate the largest Gaussian boson sampling experiments in about 10 minutes, which was claimed to take 10^{10} years.

Keywords: Quantum computational advantage, Gaussian boson sampling, Algorithm

1 Introduction

Over the last few years, we have seen the first experimental claims of quantum computational advantages using random circuit sampling [1, 2, 3] and Gaussian boson sampling [4, 5, 6], which are proven to be hard under plausible conjectures. Quantum advantage demonstration is not only a crucial step toward practical quantum advantage but also a fundamental milestone as evidence of violation of the extended Church-Turing thesis. An important feature that characterizes the current quantum experiments is uncorrected noise. Since the quantum advantage demonstration has been implemented by noisy quantum devices, it is imperative to understand the effect of noise on the complexity of the experiments.

Especially for Gaussian boson sampling, the main source of noise is photon loss. Even though the state-of-the-art Gaussian boson sampling has 0.5 to 0.7 loss rate in the circuits, the experiments claimed that their experiments cannot be simulated using classical algorithms in a reasonable time, based on the best-known classical algorithm [7]. A caveat is that many classical algorithms simulating Gaussian boson sampling, including the best-known classical algorithm, do not take advantage of such a large amount of loss. Therefore, understanding the complexity of the current experiments requires us to develop a classical algorithm that fully takes advantage of the effect of loss.

In this work, we present a novel classical algorithm that simulates the state-of-the-art Gaussian boson sampling in a much more efficient way than the existing algorithms by exploiting the effect of loss. The presented algorithm is particularly efficient when a loss rate is large, which is the case for the current Gaussian boson sampling experiments. The algorithm first separates the actual quantum resources of the output state of Gaussian boson sampling from the classical resources. More specifically, due to photon loss, many of photons from input squeezed states become thermalized, so they do not contribute to the exponential complexity; this property has not been employed in the existing classical algorithms in an efficient way to the best of our knowledge. Here, the quantum resources are described again by a Gaussian boson sampling circuit with a much smaller photon number, while the classical part can be described by a Gaussian random displacement channel (see Fig. 1). Our strategy is to simulate the quantum part by using the matrix product state (MPS), which is particularly useful method for a system that has a slight entanglement [8]. Then since the additional classical part can be implemented by local operations, which does not increase entanglement, we can efficiently apply and sample. Using the proposed algorithm, we simulate the largest Gaussian boson sampling experiments so far, which claimed that it would take 10^{10} years using the largest supercompter, in about 10 minutes.

2 Results

2.1 New classical algorithm for simulating Gaussian boson sampling

We now present a decomposition of Gaussian boson sampling's output state, which is a crucial first step for our classical algorithm. As mentioned before, our strategy is to decompose the output state into the quantum part and the classical part. To do that, we decompose the output Gaussian state's covariance matrix into two parts as $V = V_p + W$, where V_p represents the covariance matrix of a pure Gaussian state and $W \geq 0$. Here, clearly, the covariance matrix V_p can be interpreted as a pure quantum resource because it is composed of pure

*changhun@uchicago.edu

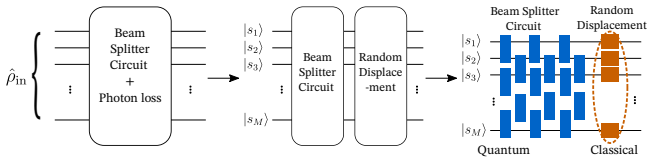


Figure 1: (a) Gaussian boson sampling circuit with photon loss with Gaussian input state $\hat{\rho}_{\rm in}$, which is, in the standard setup, the product of squeezed vacuum states. Using the decomposition introduced in the main text, we decompose the output state as pure squeezed states input followed by a beam splitter network and Gaussian random displacement channel. Note that the random displacement follows a Gaussian distribution which is generally correlated over different modes.

squeezed states and beam splitters. On the other hand, the positive semidefinite matrix W can be interpreted as a Gaussian random displacement because the initial covariance matrix V can be obtained by applying Gaussian random displacement characterized by the classical covariance matrix W to the pure Gaussian state of its covariance matrix V_p. Since any pure Gaussian state with the zero mean vector can be written as squeezed vacuum states followed by a beam splitter network, we can always decompose the output state of Gaussian boson sampling with photon loss as Fig. 1. More specifically, for multimode Gaussian state's covariance matrix V, we can implement the procedure by using semidefinite programming under the constraint:

$$\min_{V_p} \mathrm{Tr}[V_p] \text{ with } V - V_p \geq 0,\ V_p \geq i\Omega, \tag{1}$$

where the second constraint is to guarantee that V_p represents a proper physical Gaussian state's covariance matrix.

We now simulate the quantum part by using the matrix product states (MPS). The MPS is a method of writing a quantum state as a product of matrices:

$$|\psi\rangle = \sum_{n_1,\cdots,n_M=0}^{d-1} \sum_{\alpha_1,\cdots,\alpha_{M-1}=0}^{\chi-1} \Gamma^{[1]n_1}_{\alpha_1} \lambda^{[1]}_{\alpha_1} \Gamma^{[2]n_2}_{\alpha_1\alpha_2} \lambda^{[2]}_{\alpha_2} \times \cdots \lambda^{[M-1]}_{\alpha_{M-1}} \Gamma^{[M]n_M}_{\alpha_{M-1}} |n_1,\cdots,n_M\rangle, \tag{2}$$

where d is the dimension of a local Hilbert space and χ is the bond dimension. Here, the bond dimension χ determines the accuracy of the approximation and the computational cost. We provide a new method of constructing an MPS of a Gaussian state. The idea is based on Ref. [8] with using the fact that a marginal state of a Gaussian state is still a Gaussian state and that a Gaussian state can be easily diagonalized by Williamson decomposition. After constructing the MPS of an output Gaussian state, the remaining part is to apply random displacement and perform a photon-number measurement. A crucial fact to use the MPS is that a random displacement and photon-number measurement are local operations, which do not increase entanglement. As a result, this step is efficient as long as the MPS construction is efficient.

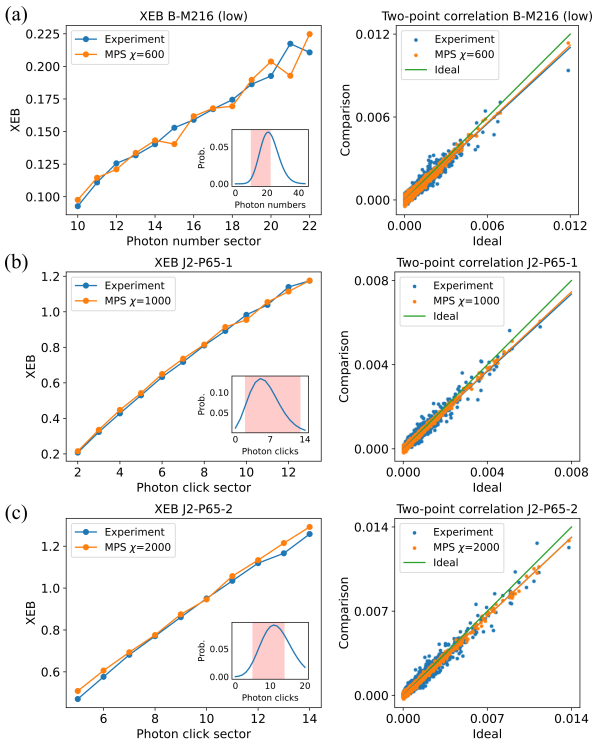


Figure 2: XEB and two-point correlation function for (a) Borealis $M = 216$ (low), (b) Jiuzhang2.0's P65-1 with $M = 144$, and (c) Jiuzhang2.0's P65-2 with $M = 144$. It clearly shows that our sampler attains comparable scores for different benchmarks.

2.2 Asymptotic behavior of running time

We study the asymptotic behavior of running time of our algorithm by investigating how the entanglement entropy scales as system size and loss rate. Here, we parameterize the loss rate as $\eta = O(K^\beta)$, where K is the number of squeezed states and $0 \leq \beta \leq 1$ In particular, we show that when $\beta < 1/2$, our proposed MPS algorithm takes polynomial time in the number of squeezed states K and the accuracy $1/\epsilon$. On the other hand, when $\beta > 1/2$, we show that the MPS algorithm starts to take superpolynomial time in the parameters. While it recovers the existing results, it has a significant advantage over other classical algorithms in that our algorithm can efficiently improve the accuracy by increasing the running time.

2.3 Simulation of the state-of-the-art Gaussian boson sampling

We finally simulate the state-of-the-art Gaussian boson sampling experiments by using the proposed classical algorithm. We first simulate the intermediate-scale experiments and verify that our algorithm outperforms the experiments by using the cross-entropy benchmarking (XEB) and the two-point correlation method, which is shown in Fig. 2. We show that for both benchmarkings, our choices of bond dimension χ render comparable scores.

For the largest Gaussian boson sampling experiments, which were claimed in the quantum computational ad-

vantage regime, we choose the bond dimension $\chi = 10000$ and demonstrate that the two-point correlation functions of the MPS simulator recover more precisely than the experiments, which is presented in Fig. 3. We also verify that our MPS sampler can reproduce even higher-order correlations better than the experiments. Therefore, all the benchmarkings that were employed for demonstrating quantum computational advantage from experiments can be outperformed by our new algorithm. Using the simulation, we also observe that the connectivity of the beam-splitter circuit is another important factor that changes the running time of our algorithm. It can be understood by the fact that MPS's cost is determined by the entanglement, which gets larger as the circuit is deeper. We emphasize that the experiments in Refs. [4, 5, 6] claimed that for the hardest sample they experimentally attained the largest supercomputer would take $10^9 - 10^{10}$ years using the best-known classical algorithm. However, our classical sampler only takes less than 10 minutes using the number of GPUs which is the same as the number of modes. Therefore, it indicates that we have strong evidence that our classical sampler implemented in a reasonable time can outperform the existing Gaussian boson sampling experiments and that to achieve a quantum advantage, the experiments have to improve the transmission rate, or the number of squeezers, or the noise parameters.

3 Discussion

In summary, we have proposed a novel classical algorithm that can simulate the state-of-the-art Gaussian boson sampling experiments in a reasonable time using a classical computer. Our new classical algorithm significantly pushes the boundary of quantum computational advantages. In addition, our algorithm enables us to capture the main quantum resources in lossy Gaussian boson sampling, which will guide future Gaussian boson sampling experiments to demonstrate the quantum advantage. One possible way to make our algorithm inefficient is to scale up the number of input squeezed states instead of increasing the squeezing parameters. Another obvious way is to improve the transmission rate. From the simulation, we also observe that circuit connectivity is an important factor that decides the complexity because it determines the entanglement of the output state. Therefore, future experiments need to the connectivity sufficiently large so the output state has a large amount of entanglement.

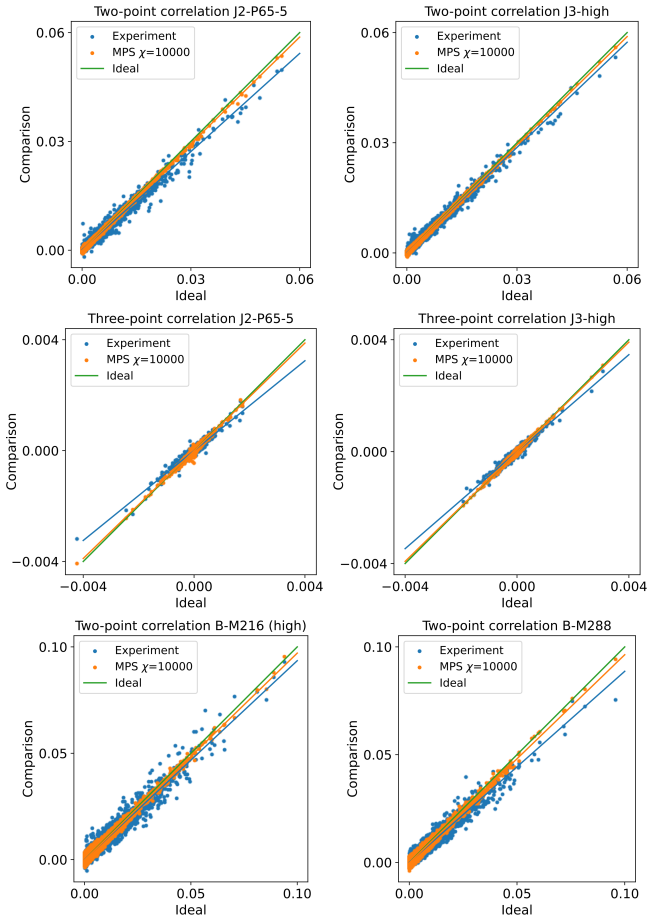


Figure 3: XEB and two-point, three-point correlation functions of experiments and our MPS sampler for Jiuzhang2.0's P65-5 with $M = 144$, Jiuzhang3.0's high with $M = 144$, Borealis $M = 216$ (high) and $M = 288$.

References

[1] Frank Arute et al. Quantum supremacy using a programmable superconducting processor. Nature 574, 505 (2019).

[2] Yulin Wu et al. Strong quantum computational advantage using a superconducting quantum processor. Phys. Rev. Lett. 127, 180501 (2021).

[3] A. Morvan et al. Phase transition in Random Circuit Sampling arXiv:2304.11119

[4] Han-Sen Zhong et al. Phase-programmable Gaussian boson sampling using stimulated squeezed light Phys. Rev. Lett. 127, 180502 (2021).

[5] Lars S. Madsen et al. Quantum computational advantage with a programmable photonic processor Nature 606, 75 (2022).

[6] Yu-Hao Deng et al. Gaussian Boson Sampling with Pseudo-Photon-Number Resolving Detectors and Quantum Computational Advantage. arXiv:2304.12240.

[7] Jacob FF Bulmer et al. The boundary for quantum advantage in Gaussian boson sampling. Science advances 8.4 (2022): eabl9236.

[8] G. Vidal. Efficient classical simulation of slightly entangled quantum computations. Phys. Rev. Lett. 91, 147902 (2003).

Deep quantum neural networks form Gaussian processes

Diego García-Martín[1] * Martín Larocca[2 3] † M. Cerezo[1] ‡

[1] *Information Sciences, Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
[2] *Theoretical Division, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA*
[3] *Center for Nonlinear Studies, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA*

Abstract. It is well known that certain artificial neural networks converge to Gaussian processes in the limit of large number of neurons per hidden layer. In this work we prove an analogous result for Quantum Neural Networks (QNNs). Namely, we show that the outputs of certain models based on Haar random unitary or orthogonal QNNs converge to Gaussian processes in the limit of large Hilbert space dimension. Our theorems imply that the concentration of measure phenomenon in Haar random QNNs is much worse than previously thought, as we prove that expectation values and gradients concentrate exponentially in the Hilbert space dimension.

Keywords: Quantum computing, quantum machine learning, random quantum circuits

1 Introduction

Neural Networks (NNs) have revolutionized the fields of Machine Learning (ML) and artificial intelligence. Their tremendous success across many fields of research in a wide variety of applications [1, 2] is certainly astonishing. While much of this success has come through heuristics, the past few decades have witnessed a significant increase in our theoretical understanding of their inner workings. One of the most interesting results regarding NNs is that fully-connected models with a single hidden layer converge to Gaussian Processes (GPs) in the limit of large number of hidden neurons, when the parameters are initialized from independent and identically distributed (i.i.d.) priors [3]. More recently, it has been shown that i.i.d.-initialized, fully-connected, multi-layer NNs also converge to GPs in the infinite-width limit [4]. Furthermore, other architectures, such as convolutional NNs [5], transformers [6] or recurrent NNs [7] are also GPs under certain assumptions. More than just a mathematical curiosity, the correspondence between NNs and GPs opened up the possibility of performing exact Bayesian inference for regression and learning tasks using wide NNs [3].

With the advent of quantum computers, there has been an enormous interest in merging quantum computing with ML, leading to the thriving field of Quantum Machine Learning (QML) [8, 9]. Rapid progress has been made in this field, largely fueled by the hope that QML may provide a quantum advantage in the near-term for some practically-relevant problems.

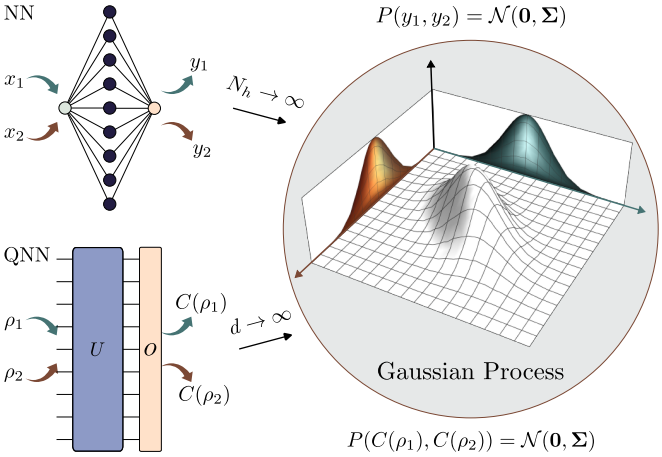


Figure 1: **Schematic of our main results.** It is well known that certain classical NNs with N_h neurons per hidden layer become GPs when $N_h \to \infty$. That is, given inputs x_1 and x_2, and corresponding outputs y_1 and y_2, then the joint probability $P(y_1, y_2)$ is a multivariate Gaussian $\mathcal{N}(\vec{0}, \vec{\Sigma})$. In this work, we show that a similar result holds under certain conditions for deep QNNs in the limit of large Hilbert space dimension, $d \to \infty$. Now, given quantum states ρ_1 and ρ_2, $C(\rho) = \text{Tr}[U\rho U^\dagger O]$ is such that $P(C(\rho_1), C(\rho_2)) = \mathcal{N}(\vec{0}, \vec{\Sigma})$.

In this work, we contribute to the QML body of knowledge by proving that under certain conditions, the outputs of deep Quantum Neural Networks (QNNs) – i.e., parametrized quantum circuits acting on input states drawn from a training set– converge to GPs in the limit of large Hilbert space dimension (see Fig. 1). Our results are derived for

*dgarciamartin@lanl.gov
†larocca@lanl.gov
‡cerezo@lanl.gov

QNNs that are Haar random over the unitary and orthogonal groups. Unlike the classical case, where the proof of the emergence of GPs stems from the central limit theorem, the situation becomes more intricate in the quantum setting as the entries of the QNN are not independent – the rows and columns of a unitary matrix are constrained to be mutually orthonormal. Hence, our proof strategy boils down to showing that each moment of the QNN's output distribution converges to that of a multivariate Gaussian. In addition, we show that in contrast to classical NNs, the Bayesian distribution of the QNN is inefficient for predicting the model's outputs. We then use our results to provide a precise characterization of the concentration of measure phenomenon in deep random quantum circuits [10, 11]. Here, our theorems indicate that the expectation values, as well as the gradients, of Haar random processes concentrate exponentially faster than reported in previous barren plateau studies [10, 11]. Finally, we discuss how our results can be leveraged to study QNNs that are not fully Haar random but instead form t-designs, which constitutes a much more practical assumption [12, 13, 14].

2 Main results

We consider a setting where one is given repeated access to a dataset $\mathscr{D}$ containing pure quantum states $\{\rho_i\}_i$ on a d-dimensional Hilbert space. We will make no assumptions regarding the origin of these states, as they can correspond to classical data encoded in quantum states [29, 30], or quantum data obtained from some quantum mechanical process [31, 32]. Then, we assume that the states are sent through a deep QNN, denoted U. While in general U can be parametrized by some set of trainable parameters θ, we leave such dependence implicit for the ease of notation. At the output of the circuit one measures the expectation value of a traceless Hermitian operator taken from a set $\mathscr{O} = \{O_j\}_j$ such that $\mathrm{Tr}[O_j O_{j'}] = d\delta_{j,j'}$ and $O_j^2 = 1$, for all j, j' (e.g., Pauli strings). We denote the QNN outputs as

$$C_j(\rho_i) = Tr[U\rho_i U^\dagger O_j]\,. \tag{1}$$

Then, we collect these quantities over some set of states from $\mathscr{D}$ and some set of measurements from O in a vector

$$\mathscr{C} = (C_j(\rho_i), ..., C_{j'}(\rho_{i'}), \dots)\,. \tag{2}$$

What we show in this work is that, in the large-d limit, $\mathscr{C}$ converges to a GP when the QNN unitaries

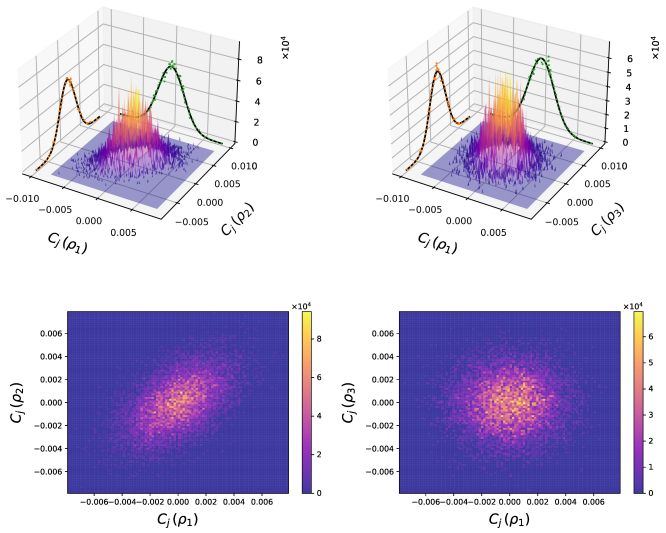


Figure 2: **Two-dimensional GPs.** We plot the joint probability density function, as well as its scaled marginals, for the measurement outcomes at the output of a unitary Haar random QNN acting on $n = 18$ qubits. The measured observable is $O_j = Z_1$, where Z_1 denotes the Pauli z operator on the first qubit. Moreover, the input states are: $\rho_1 = |0\rangle\langle 0|^{\otimes n}$ and $\rho_2 = |\mathrm{GHZ}\rangle\langle \mathrm{GHZ}|$ with $|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$, for the left panel; ρ_1 and $\rho_3 = |\Psi\rangle\langle\Psi|$ with $|\Psi\rangle = \frac{1}{\sqrt{d}}|0\rangle^{\otimes n} + \sqrt{1-\frac{1}{d}}|1\rangle^{\otimes n}$ for the right panel. In both cases we took 10^4 samples.

U are sampled according to the Haar measure on the degree-d unitary $\mathbb{U}(d)$ or orthogonal $\mathbb{O}(d)$ groups (see Fig. 1). Moreover, we assume that when the circuit is sampled from $\mathbb{O}(d)$, the states in $\mathscr{D}$ and the measurement operators in $\mathscr{O}$ are real valued.

We prove convergence to GPs in three different regimes (Theorems 1,2 and 3 in our manuscript, linked below), depending on the overlaps between input states in the training set $\mathscr{D}$. Namely, i) when the overlaps are such that $\mathrm{Tr}[\rho_i, \rho_{i'}] \in \Omega(\mathrm{poly}(\log(d)))$ for all i, i', ii) when $\mathrm{Tr}[\rho_i, \rho_{i'}] = \frac{1}{d}$ for all i, i', and iii) when $\mathrm{Tr}[\rho_i, \rho_{i'}] = 0$ for all i, i'. We remark that in each of these different regimes, the variables in the GP show positive, null and negative correlations respectively (see Fig. 2).

There are several corollaries that stem from our main results. A first corollary is

Corollary 1 *Let $C_j(\rho_i)$ be the expectation value of a Haar random QNN as in Eq. (1). Then, for any $\rho_i \in \mathscr{D}$ and $O_j \in \mathscr{O}$, we have*

$$P(C_j(\rho_i)) = \mathcal{N}(0, \sigma^2)\,, \tag{3}$$

where $\sigma^2 = \frac{1}{d}, \frac{2}{d}$ for $\mathbb{U}(d)$ and $\mathbb{O}(d)$.

This result shows that when a single state from $\mathscr{D}$ is sent through the QNN, and a single operator from $\mathscr{O}$ is measured, the outcomes follow a Gaussian distribution with a variance that vanishes inversely proportional with the Hilbert space dimension (see Fig. 3).

A second corollary that we can prove is the following,

Corollary 2 *Let $C_j(\rho_i)$ be the expectation value of a Haar random QNN as in Eq. (1). Assuming that there exists a parametrized gate in U of the form $e^{-i\theta H}$ for some Pauli operator H, then*

$$P(|C_j(\rho_i)| \geq c),\ P(|\partial_\theta C_j(\rho_i)| \geq c) \in \mathcal{O}\left(\frac{1}{ce^{dc^2}\sqrt{d}}\right).$$

Corollary 2 indicates that the QNN outputs, and their gradients, actually concentrate with a probability which vanishes exponentially with d. In an n-qubit system, where $d = 2^n$, then $P(|C_j(\rho_i)| \geq c)$ and $P(|\partial_\theta C_j(\rho_i)| \geq c)$ are doubly exponentially vanishing with n. The tightness of our bound arises from the fact that Chebyshev's inequality is loose for highly narrow Gaussian distributions. Corollary 2 also implies that the narrow gorge region of the landscape [15], i.e., the fraction of non-concentrated $C_j(\rho_i)$ values, also decreases exponentially with d.

Another theorem that we prove in our work is the following,

Theorem 4 *Consider a GP obtained from a Haar random QNN. Given the set of observations $(y(\rho_1), \ldots, y(\rho_m))$ obtained from $N \in \mathcal{O}(\text{poly}(\log(d)))$ measurements, then the predictive distribution of the GP is trivial:*

$$P(C_j(\rho_{m+1})|C_j(\rho_1), \ldots, C_j(\rho_m)) = P(C_j(\rho_{m+1})) = \mathcal{N}(0, \sigma^2),$$

where σ^2 is given by Corollary 1.

Here, the observations are $y(\rho_i) = C_j(\rho_i) + \varepsilon_i$, where the statistical noise terms ε_i (arising from finite sampling) are independently drawn from the same zero-mean Gaussian distribution. Theorem 4 shows that by spending only a poly-logarithmic-in-d number of measurements , one cannot use Bayesian statistical theory to learn any information about new outcomes given previous ones.

3 Conclusions and Outlook

In this manuscript we have shown that under certain conditions, the output distribution of deep Haar random QNNs converges to a Gaussian process in the limit of large Hilbert space dimension. While this result had been conjectured in [17], a formal proof was still lacking. We remark that although our result mirrors its classical counterpart –that certain classical NNs form GPs–, there exist nuances that differentiate our findings from the classical case. For instance, we need to make assumptions on the states processed by the QNN, as well as on the measurement operator. Moreover, some of these assumptions are unavoidable, as Haar random QNNs will not necessarily always converge to a GP. As an example, we have that if O_i is a projector onto a computational basis state, then one recovers a Porter-Thomas distribution [16]. Ultimately, these subtleties arise because the entries of unitary matrices are not independent. In contrast, classical NNs are not subject to this constraint.

It is worth noting that our theorems have further implications beyond those discussed here. We envision that our methods and results will be useful in more general settings where Haar random unitaries / t-designs are considered, such as quantum information scramblers and black holes [18, 20, 19], many-body physics [21], quantum decouplers and quantum error correction [22].

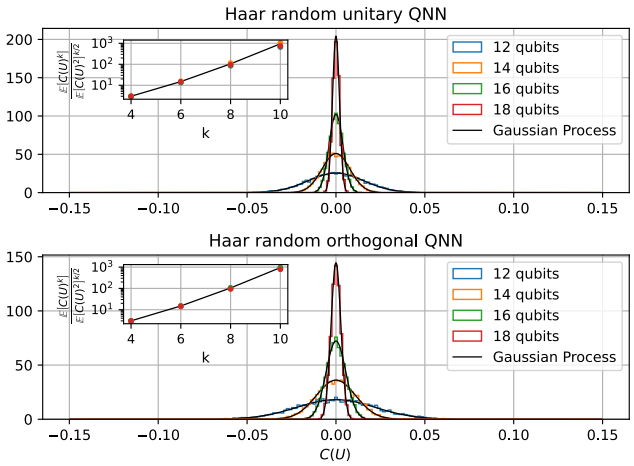


Figure 3: **Probability density function for $C_j(\rho_i)$, for Haar random QNNs and different problem sizes.** We consider unitary and orthogonal QNNs with n-qubits, and we take $\rho_i = |0\rangle\langle 0|^{\otimes n}$, and $O_j = Z_1$. The colored histograms are built from 10^4 samples in each case, and the solid black lines represent the corresponding Gaussian distributions $\mathcal{N}\left(0, \sigma^2\right)$, where σ^2 is given in Corollary 1. The insets show the numerical versus predicted value of $\mathbb{E}[C_j(\rho_i)^k]/\mathbb{E}[C_j(\rho_i)^2]^{k/2}$. For a Gaussian distribution with zero mean, such quotient is $\frac{k!}{2^{k/2}(k/2)!}$ (solid black line).

Link to the manuscript

https://arxiv.org/abs/2305.09957

References

[1] L. Alzubaidi, J. Zhang, A. J. Humaidi, A. Al-Dujaili, Y. Duan, O. Al-Shamma, J. Santamaría, M. A. Fadhel, M. Al-Amidie, and L. Farhan. Review of deep learning: Concepts, cnn architectures, challenges, applications, future directions. *Journal of big Data* 8:1, 2021.

[2] D. Khurana, A. Koli, K. Khatter, and S. Singh. Natural language processing: State of the art, current trends and challenges. *Multimedia tools and applications*, 82:3713, 2023.

[3] R. M. Neal. Priors for infinite networks. *Bayesian learning for neural networks*, 29, 1996.

[4] J. Lee, Y. Bahri, R. Novak, S. S. Schoenholz, J. Pennington, and J. Sohl-Dickstein. Deep neural networks as gaussian processes. arXiv:1711.00165, 2017.

[5] R. Novak, L. Xiao, Y. Bahri, J. Lee, G. Yang, D. A. Abolafia, J. Pennington, and J. Sohl-dickstein. Bayesian deep convolutional networks with many channels are gaussian processes. In *International Conference on Learning Representations*, 2019.

[6] J. Hron, Y. Bahri, J. Sohl-Dickstein, and R. Novak. Infinite attention: Nngp and ntk for deep attention networks. In *International Conference on Machine Learning*, pages 4376–4386, 2020.

[7] G. Yang. Wide feedforward or recurrent neural networks of any architecture are gaussian processes. *Advances in Neural Information Processing Systems*, 32, 2019.

[8] M. Cerezo, G. Verdon, H.-Y. Huang, L. Cincio, and P. J. Coles. Challenges and opportunities in quantum machine learning. *Nature Computational Science*, 2:567–576, 2022.

[9] M. Cerezo, A. Arrasmith, R. Babbush, S. C. Benjamin, S. Endo, K. Fujii, J. R. McClean, K. Mitarai, X. Yuan, L. Cincio, and P. J. Coles. Variational quantum algorithms. *Nature Reviews Physics*, 3:625–644, 2021.

[10] J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, and H. Neven. Barren plateaus in quantum neural network training landscapes. *Nature Communications*, 9:1, 2018.

[11] M. Cerezo, A. Sone, T. Volkoff, L. Cincio, and P. J. Coles. Cost function dependent barren plateaus in shallow parametrized quantum circuits. *Nature Communications*, 12:1, 2021.

[12] A. W. Harrow and R. A. Low. Random quantum circuits are approximate 2-designs. *Communications in Mathematical Physics*, 291:257, 2009.

[13] A. Harrow and S. Mehraban. Approximate unitary t-designs by short random quantum circuits using nearest-neighbor and long-range gates. arXiv:1809.06957, 2018.

[14] J. Haferkamp. Random quantum circuits are approximate unitary t-designs in depth $\mathcal{O}(nt^{5+o(1)})$. arXiv:2203.16571, 2022.

[15] A. Arrasmith, Z. Holmes, M. Cerezo, and P. J. Coles. Equivalence of quantum barren plateaus to cost concentration and narrow gorges. *Quantum Science and Technology*, 7:045015, 2022.

[16] C. E. Porter and R. G. Thomas. Fluctuations of nuclear reaction widths. *Physical Review*, 104:483, 1956.

[17] J. Liu, F. Tacchino, J. R. Glick, L. Jiang, and A. Mezzacapo. Representation learning via quantum neural tangent kernels. arXiv:2111.04225, 2021.

[18] P. Hayden and J. Preskill. Black holes as mirrors: quantum information in random subsystems. *Journal of High Energy Physics*, 9:120, 2007.

[19] Z. Holmes, A. Arrasmith, B. Yan, P. J. Coles, A. Albrecht, and A. T. Sornborger. Barren plateaus preclude learning scramblers. *Physical Review Letters*, 126:190501, 2021.

[20] S. F. Oliviero, L. Leone, S. Lloyd, and A. Hamma. Black hole complexity, unscrambling, and stabilizer thermal machines, arXiv:2212.11337, 2022.

[21] A. Nahum, S. Vijay, and J. Haah. Operator spreading in random unitary circuits. *Physical Review X*, 8:021014, 2018.

[22] W. Brown and O. Fawzi. Decoupling with random quantum circuits. *Communications in mathematical physics*, 340:867, 2015.

Exponential quantum speedup in simulating coupled classical oscillators

Ryan Babbush[1]

[1]*Google Quantum AI*

Abstract. We present a quantum algorithm for simulating the classical dynamics of 2^n coupled oscillators (e.g., 2^n masses coupled by springs). Our approach leverages a mapping between the Schrodinger equation and Newton's equation for harmonic potentials such that the amplitudes of the evolved quantum state encode the momenta and displacements of the classical oscillators. When individual masses and spring constants can be efficiently queried, and when the initial state can be efficiently prepared, the complexity of our quantum algorithm is polynomial in n, almost linear in the evolution time, and sublinear in the sparsity. As an example application, we apply our quantum algorithm to efficiently estimate the kinetic energy of an oscillator at any time. We show that any classical algorithm solving this same problem is inefficient and must make $2^{\Omega(n)}$ queries to the oracle and, when the oracles are instantiated by efficient quantum circuits, the problem is BQP-complete. Thus, our approach solves a potentially practical application with an exponential speedup over classical computers. Finally, we show that under similar conditions our approach can efficiently simulate more general classical harmonic systems with 2^n modes. This talk is based on the paper arXiv:2303.13012.

Recent progress in scaling quantum error mitigation toward useful quantum computing

Youngseok Kim [*1] Andrew Eddins [*2] Sajant Anand[3] Ken Xuan Wei[1]
Ewout van den Berg[1] Sami Rosenblatt[1] Hasan Nayfeh[1] Yantao Wu[5]
Michael Zaletel[3 4] Kristan Temme[1] Abhinav Kandala[1]

[1] *IBM Quantum, IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA*
[2] *IBM Quantum, MIT-IBM Watson AI Lab, Cambridge, MA, 02142, USA*
[3] *Dept. of Physics, University of California, Berkeley, CA 94720, USA*
[4] *Material Sciences Division, Lawrence Berkeley National Laboratory, Berkeley, CA 94720, USA*
[5] *RIKEN iTHEMS, Wako, Saitama 351-0198, Japan*

Abstract. Quantum error mitigation enables access to accurate expectation values even on existing, noisy quantum computers. Establishing the applicability of these techniques at scales beyond those accessible to brute force classical methods is a crucial step toward probing a computational advantage with near-term noisy quantum computers. Here, we experimentally demonstrate the efficacy of an error mitigation technique, zero-noise extrapolation, for exactly verifiable Clifford quantum circuits using up to 127 qubits. The accuracy of the mitigated expectation values is greatly enhanced by novel advances in the coherence of large-scale superconducting quantum processors, and the ability to controllably scale noise at this scale. These experiments demonstrate an important tool for the realization of near-term quantum applications in a pre-fault tolerant era.

Keywords: quantum error mitigation, zero noise extrapolation, IBM hardware, experiment

1 Motivation

While exciting demonstrations of quantum error correction have been made for recent years [1, 2, 3, 4], numerous challenges remain to establish logical qubits at a scale capable of tackling useful problems. This motivates a search for near-term applications utilizing noisy quantum computers. Recent development in error mitigation techniques such as zero-noise extrapolation (ZNE) [5, 6] have led to greatly improved accuracy of experimentally measured observables. In this work, we further extend ZNE, and improve its performance at scale by accurately characterizing the device noise and manipulating it.

2 Summary of our results

We primarily focus on establishing the reliability of the hardware and methods at sufficient scale, as an important first step before finding advantageous applications that fit the demonstrated circuit volume. Here, we provide an evidence that we are producing accurate expectation values at a scale beyond direct diagonalization. This is in itself particularly valuable since the majority of near-term quantum algorithms reduce to the estimation of expectation values.

Our benchmark circuit is the Trotterized time evolution of a 2D transverse-field Ising spin lattice, sharing the topology of the qubit processor. Specifically, we consider time dynamics of the Hamiltonian,

$$H = -J \sum_{\langle i,j \rangle} Z_i Z_j + h \sum_i X_i, \qquad (1)$$

where $J > 0$ is the coupling of nearest neighbor spins and h is the global transverse field.

Despite advances in coherence and gate calibration, the measured expectation values are biased from their noise-free values by noise over the duration of the circuit. We therefore rely on ZNE to combine results from multiple configurations of a noisy circuit to obtain an improved estimate of an observable of interest, at an increased sampling cost. ZNE requires the controlled amplification of the intrinsic hardware noise by a known gain factor G in order to extrapolate to the ideal $G = 0$ result. ZNE has been widely adopted in part because amplification methods based on pulse stretching [7, 5] or subcircuit repetition [8, 9, 10] permit relatively simple implementations, though these often rely on certain simplifying assumptions about the device noise. Pulse stretching, for instance, has enabled estimates of expectation values for 26-qubit circuits at a level competitive with certain tensor-network calculations [6]. However, the ability to learn and controllably amplify noise over a large device can enable significant reductions in the bias of the extrapolated estimators. This is precisely where the Pauli-Lindblad noise model comes into play. Given the success of Pauli-Lindblad noise learning in recent experiments, we follow the characterization procedure in [11] to obtain such a noise model for each CNOT layer. Applying random Pauli twirls [12, 13, 14, 15, 16] to each layer of noisy two-qubit gates simplifies the overall noise in that layer, on average, to a Pauli channel. The noise characterization then provides a decomposition of the obtained Pauli channel as a set of local Pauli generators. Based on the obtained noise model, we can amplify the noise for ZNE by stochastic insertion of Pauli gates. Errors inserted with appropriate probabilities effectively realize a second copy of the original Pauli channel. By tuning the sampling probabilities, we enable precise, arbitrary

[*] These authors contributed equally to this work

scaling of the noise gain desired for extrapolation.

The above mentioned error scaling technique allows us to deploy ZNE for a superconducting quantum processor with 127 qubits to run quantum circuits with up to 60 layers of 2-qubit gates comprising a total of 2,880 CNOT gates. First, we verify that the resulting expectation values for local observables agree with the ideal values for a set of Clifford circuits permitting direct classical evaluation. We then evaluate the utility of running these circuits, by turning to circuit regimes and observables where classical simulation becomes challenging, and compare to the results from state-of-the-art approximate classical methods.

3 Conclusion

In conclusion, the observation that even noisy quantum processors at a scale beyond 100 qubits and significant circuit depth are able to produce reliable expectation values provides us with strong evidence that there is a path to useful quantum computation prior to the advent of full fault tolerance. We have now reached reliability at a scale where one will be able to verify proposals that utilize noise limited quantum circuits, and explore new approaches to determine which can provide optimal utility of noisy quantum computers.

References

[1] Neereja Sundaresan, Theodore J. Yoder, Youngseok Kim, Muyuan Li, Edward H. Chen, Grace Harper, Ted Thorbeck, Andrew W. Cross, Antonio D. Córcoles, and Maika Takita. Demonstrating multi-round subsystem quantum error correction using matching and maximum likelihood decoders. *Nature Communications*, 14(1):2852, 2023.

[2] Rajeev Acharya, Igor Aleiner, Richard Allen, Trond I. Andersen, Markus Ansmann, Frank Arute, Kunal Arya, Abraham Asfaw, Juan Atalaya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Joao Basso, Andreas Bengtsson, Sergio Boixo, Gina Bortoli, Alexandre Bourassa, Jenna Bovaird, Leon Brill, Michael Broughton, Bob B. Buckley, David A. Buell, Tim Burger, Brian Burkett, Nicholas Bushnell, Yu Chen, Zijun Chen, Ben Chiaro, Josh Cogan, Roberto Collins, Paul Conner, William Courtney, Alexander L. Crook, Ben Curtin, Dripto M. Debroy, Alexander Del Toro Barba, Sean Demura, Andrew Dunsworth, Daniel Eppens, Catherine Erickson, Lara Faoro, Edward Farhi, Reza Fatemi, Leslie Flores Burgos, Ebrahim Forati, Austin G. Fowler, Brooks Foxen, William Giang, Craig Gidney, Dar Gilboa, Marissa Giustina, Alejandro Grajales Dau, Jonathan A. Gross, Steve Habegger, Michael C. Hamilton, Matthew P. Harrigan, Sean D. Harrington, Oscar Higgott, Jeremy Hilton, Markus Hoffmann, Sabrina Hong, Trent Huang, Ashley Huff, William J. Huggins, Lev B. Ioffe, Sergei V. Isakov, Justin Iveland, Evan Jeffrey, Zhang Jiang, Cody Jones, Pavol Juhas, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Tanuj Khattar, Mostafa Khezri, Mária Kieferová, Seon Kim, Alexei Kitaev, Paul V. Klimov, Andrey R. Klots, Alexander N. Korotkov, Fedor Kostritsa, John Mark Kreikebaum, David Landhuis, Pavel Laptev, Kim-Ming Lau, Lily Laws, Joonho Lee, Kenny Lee, Brian J. Lester, Alexander Lill, Wayne Liu, Aditya Locharla, Erik Lucero, Fionn D. Malone, Jeffrey Marshall, Orion Martin, Jarrod R. McClean, Trevor McCourt, Matt McEwen, Anthony Megrant, Bernardo Meurer Costa, Xiao Mi, Kevin C. Miao, Masoud Mohseni, Shirin Montazeri, Alexis Morvan, Emily Mount, Wojciech Mruczkiewicz, Ofer Naaman, Matthew Neeley, Charles Neill, Ani Nersisyan, Hartmut Neven, Michael Newman, Jiun How Ng, Anthony Nguyen, Murray Nguyen, Murphy Yuezhen Niu, Thomas E. O'Brien, Alex Opremcak, John Platt, Andre Petukhov, Rebecca Potter, Leonid P. Pryadko, Chris Quintana, Pedram Roushan, Nicholas C. Rubin, Negar Saei, Daniel Sank, Kannan Sankaragomathi, Kevin J. Satzinger, Henry F. Schurkus, Christopher Schuster, Michael J. Shearn, Aaron Shorter, Vladimir Shvarts, Jindra Skruzny, Vadim Smelyanskiy, W. Clarke Smith, George Sterling, Doug Strain, Marco Szalay, Alfredo Torres, Guifre Vidal, Benjamin Villalonga, Catherine Vollgraff Heidweiller, Theodore White, Cheng Xing, Z. Jamie Yao, Ping Yeh, Juhwan Yoo, Grayson Young, Adam Zalcman, Yaxing Zhang, Ningfeng Zhu, and Google Quantum AI. Suppressing quantum errors by scaling a surface code logical qubit. *Nature*, 614(7949):676–681, 2023.

[3] J. F. Marques, B. M. Varbanov, M. S. Moreira, H. Ali, N. Muthusubramanian, C. Zachariadis, F. Battistel, M. Beekman, N. Haider, W. Vlothuizen, A. Bruno, B. M. Terhal, and L. DiCarlo. Logical-qubit operations in an error-detecting surface code. *Nature Physics*, 18(1):80–86, 2022.

[4] Sebastian Krinner, Nathan Lacroix, Ants Remm, Agustin Di Paolo, Elie Genois, Catherine Leroux, Christoph Hellings, Stefania Lazar, Francois Swiadek, Johannes Herrmann, Graham J. Norris, Christian Kraglund Andersen, Markus Müller, Alexandre Blais, Christopher Eichler, and Andreas Wallraff. Realizing repeated quantum error correction in a distance-three surface code. *Nature*, 605(7911):669–674, 2022.

[5] Abhinav Kandala, Kristan Temme, Antonio D. Córcoles, Antonio Mezzacapo, Jerry M. Chow, and Jay M. Gambetta. Error mitigation extends the computational reach of a noisy quantum processor. *Nature*, 567:491, Mar 2019.

[6] Youngseok Kim, Christopher J. Wood, Theodore J. Yoder, Seth T. Merkel, Jay M. Gambetta, Kristan Temme, and Abhinav Kandala. Scalable error mitigation for noisy quantum circuits produces competitive expectation values. *Nature Physics*, feb 2023.

[7] Kristan Temme, Sergey Bravyi, and Jay M. Gambetta. Error mitigation for short-depth quantum circuits. *Phys. Rev. Lett.*, 119:180509, Nov 2017.

[8] E. F. Dumitrescu, A. J. McCaskey, G. Hagen, G. R. Jansen, T. D. Morris, T. Papenbrock, R. C. Pooser, D. J. Dean, and P. Lougovski. Cloud quantum computing of an atomic nucleus. *Phys. Rev. Lett.*, 120:210501, May 2018.

[9] Andre He, Benjamin Nachman, Wibe A. de Jong, and Christian W. Bauer. Zero-noise extrapolation for quantum-gate error mitigation with identity insertions. *Phys. Rev. A*, 102:012426, Jul 2020.

[10] Tudor Giurgica-Tiron, Yousef Hindy, Ryan LaRose, Andrea Mari, and William J. Zeng. Digital zero noise extrapolation for quantum error mitigation. In *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pages 306–316, 2020.

[11] Ewout van den Berg, Zlatko K. Minev, Abhinav Kandala, and Kristan Temme. Probabilistic error cancellation with sparse pauli-lindblad models on noisy quantum processors. *Nature Physics*, May 2023.

[12] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722–725, Jan 1996.

[13] E. Knill. Fault-tolerant postselected quantum computation: Threshold analysis, 2004.

[14] O. Kern, G. Alber, and D. L. Shepelyansky. Quantum error correction of coherent errors by randomization. *The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics*, 32:153–156, Jan 2005.

[15] Michael R. Geller and Zhongyuan Zhou. Efficient error models for fault-tolerant architectures and the pauli twirling approximation. *Phys. Rev. A*, 88:012314, Jul 2013.

[16] Joel J. Wallman and Joseph Emerson. Noise tailoring for scalable quantum computation via randomized compiling. *Phys. Rev. A*, 94:052325, Nov 2016.

Estimate distillable entanglement and quantum capacity by squeezing useless entanglement

Chengkai Zhu[1] Chenghong Zhu[1] Xin Wang[1]

[1] *Institute for Quantum Computing, Baidu Research, Beijing 100193, China*

Abstract. We propose methods for evaluating the distillable entanglement and the quantum capacity by squeezing out useless entanglement within a state or a quantum channel. We first consider a general resource measure called the reverse divergence of resources to quantify the minimum divergence between a target state and the set of free states. We then introduce the reverse max-relative entropy of entanglement and apply it to establish efficiently computable upper bounds on the distillable entanglement. We also extend the reverse divergence of resources to quantum channels and derive upper bounds on the quantum capacity. Our method has practical applications for purifying maximally entangled states under practical noises, such as depolarizing and amplitude damping noises, leading to improvements in estimating the one-way distillable entanglement. Our bounds also offer useful benchmarks for evaluating the quantum capacities of qubit quantum channels of interest, including the Pauli channels and the random mixed unitary channels. Note: A technical version of this work is attached.

Keywords: Distillable entanglement, quantum capacity, quantum resources, extendibility.

Background. In quantum entanglement theory, the golden resource is usually assumed to be ideal copies of the maximally entangled states. In a practical scenario, noises inevitably occur in quantum states, resulting in some mixed entangled states. This naturally raises the question of how to obtain the maximally entangled states from a source of less entangled states using well-motivated operations, known as the *entanglement distillation*.

One fundamental measure for characterizing the entanglement distillation is the *one-way distillable entanglement* [1], denoted by $E_{D,\rightarrow}$. It captures the highest rate at which one can obtain the maximally entangled states from less entangled states by one-way local operations and classical communication (LOCC):

$$E_{D,\rightarrow}(\rho_{AB}) = \sup\{r : \lim_{n\to\infty} [\inf_{\Lambda} \|\Lambda(\rho_{AB}^{\otimes n}) - \Phi(2^{rn})\|_1] = 0\},$$

where Λ ranges over one-way LOCC operations and $\Phi(d) = 1/d \sum_{i,j=1}^{d} |ii\rangle\langle jj|$ is the standard $d\otimes d$ maximally entangled state. Likewise, the *two-way distillable entanglement* $E_{D,\leftrightarrow}(\rho_{AB})$ is defined by the supremum over all achievable rates under two-way LOCC. We have for all bipartite states ρ_{AB} that $E_{D,\rightarrow}(\rho_{AB}) \leq E_{D,\leftrightarrow}(\rho_{AB})$. Notably, the distillable entanglement is closely connected to the fundamental notion of *quantum capacity* in quantum communication tasks [2], which is central to quantum Shannon theory. Consider modeling the noise in transmitting quantum information from Alice to Bob as a quantum channel $\mathcal{N}_{A\to B}$. The quantum capacity $Q(\mathcal{N}_{A\to B})$ is the maximal achievable rate at which Alice can reliably transmit quantum information to Bob by asymptotically many uses of the channel.

Despite many efforts that have been made in the past two decades, computing $E_{D,\rightarrow}(\cdot)$ and $Q(\cdot)$ still generally remains a challenging task. Therefore, numerous studies try to estimate them by deriving lower and upper bounds (see, e.g., [1, 3–8] for the distillable entanglement, e.g., [9–12] for the quantum capacity). For the distillable entanglement, a well-known lower bound dubbed *Hashing bound* is established by Devetak and Winter [1]. Considering upper bounds, the Rains bound [3] is arguably the best-known efficiently computable bound for the two-way distillable entanglement of general states. Recent works [6, 8] utilize the techniques of finding upper bounds by constructing meaningful extended states. For quantum capacity, many useful upper bounds for general quantum channels are studied for benchmarking arbitrary quantum noise [13–20]. Useful upper bounds are also developed to help us better understand quantum communication via specific channels [8, 10–12, 21–23].

In specific, due to the regularization in the characterizations of $E_{D,\rightarrow}(\cdot)$ and $Q(\cdot)$, one main strategy to establish efficiently computable upper bounds on them is to develop single-letter formulae. For example, a common approach is to decompose a state (resp. a quantum channel) into degradable parts and anti-degradable parts [11], or use approximate degradability (anti-degradability) [14]. Another recent fruitful technique called flag extension optimization [8, 10, 12] relies on finding a degradable extension of the state or the quantum channel. However, the performance of these methods is limited by the absence of a good decomposition strategy. It is unknown how to partition a general state or quantum channel to add flags or how to construct a proper and meaningful convex decomposition on them. Thus, the flag extension optimization is only effective for the states and channels with symmetry or known structures.

Overview of Results. This work aims to derive upper bounds for the distillable entanglement of a general state and the quantum capacity of a noisy channel. To achieve this, we explore a family of resource measures known as the "reverse divergence of resources" and introduce multiple variants within this framework. In particular, we establish the following:

- We introduce **reverse max-relative entropy of entanglement** for quantum states, which can be efficiently computed via semidefinite programming (SDP) [24] and has applications for estimating the

distillable entanglement.

- We introduce **reverse max-relative entropy of anti-degradability** for quantum channels, which can be efficiently computed via SDP and applied to bound the quantum capacity.
- We investigate the **distillation** of the maximally entangled states under practical noises. We show that the bound obtained by the reverse max-relative entropy of entanglement outperforms other known computable bounds for general states in a high-noise region, including the Rains bound and the anti-degradability continuity bounds.
- We study the **quantum capacity** of qubit channels. The upper bound offered by the reverse max-relative entropy of anti-degradability provides an alternative interpretation of the no-cloning bound of the Pauli channel [21], and notably outperforms the continuity bounds on random unital qubit channels.

Main Methods. In this paper, we mainly study a measure called *reverse max-relative entropy of resources*,

$$\mathcal{R}_{\max,\mathcal{F}}(\rho_{AB}) := \min_{\tau\in\mathcal{F}} D_{\max}(\tau_{AB}||\rho_{AB}), \tag{1}$$

where $\mathcal{F}$ is some set of free states, $D_{\max}$ is the *max-relative entropy* [25] of ρ with respect to σ: $D_{\max}(\rho||\sigma) = \inf\{\lambda \in \mathbb{R} : \rho \leq 2^{\lambda}\sigma\}$. This measure can be efficiently computed via SDP in many cases and gives the closest free state $\tau_{AB} \in \mathcal{F}$ to ρ_{AB}, w.r.t. the max-relative entropy. In fact, $\mathcal{R}_{\max,\mathcal{F}}(\rho_{AB})$ is closely related to the *weight of resource* $W(\rho_{AB})$ [26–29] and the *free component* $\Gamma(\rho_{AB})$ [30], both of which have fruitful properties and applications [31–33], as follows

$$2^{-\mathcal{R}_{\max,\mathcal{F}}(\rho_{AB})} = 1 - W(\rho_{AB}) = \Gamma(\rho_{AB}). \tag{2}$$

We note that each part of Eq. (2) quantifies the largest weight where a free state can take in a convex decomposition of ρ_{AB}. When moving on to operational tasks that the free state can be ignored, what is left in a convex decomposition becomes our main concern. Optimization of the weight in the decomposition can be visualized as *squeezing out* all free parts of the given state. Thus, we further introduce the *$\mathcal{F}$-squeezed state* of ρ_{AB} as follows.

Definition 1 *For a bipartite quantum state ρ_{AB} and a free state set $\mathcal{F}$, if $\mathcal{R}_{\max,\mathcal{F}}(\rho_{AB})$ is non-zero, the $\mathcal{F}$-squeezed state of ρ_{AB} is defined by*

$$\omega_{AB} = \frac{\rho_{AB} - 2^{-\mathcal{R}_{\max,\mathcal{F}}(\rho_{AB})}\cdot\tau_{AB}}{1 - 2^{-\mathcal{R}_{\max,\mathcal{F}}(\rho_{AB})}}, \tag{3}$$

where τ_{AB} is the closest free state to ρ_{AB} in terms of the max-relative entropy, i.e., the optimal solution in Eq. (1). If $\mathcal{R}_{\max,\mathcal{F}}(\rho_{AB}) = 0$, the $\mathcal{F}$-squeezed state of ρ_{AB} is itself.

Next, we illustrate the applications of $\mathcal{R}_{\max,\mathcal{F}}(\rho_{AB})$ and the concept of squeezing in determining upper bounds for the distillable entanglement and quantum capacity.

Distillable Entanglement. Our first contribution is to introduce the *reverse max-relative entropy of unextendible entanglement*:

$$\mathcal{R}_{\max,\mathrm{ADG}}(\rho_{AB}) := \min_{\tau\in\mathrm{ADG}} D_{\max}(\tau_{AB}||\rho_{AB}), \tag{4}$$

where ADG is the set of all anti-degradable (extendible) states. Combined with the idea of entanglement of formation, we apply $\mathcal{R}_{\max,\mathrm{ADG}}(\rho_{AB})$ to establish an upper bound on the one-way distillable entanglement of an arbitrary state ρ_{AB} as shown in Theorem 2.

Theorem 2 *For any bipartite state ρ_{AB}, it satisfies*

$$E_{D,\rightarrow}(\rho_{AB}) \leq E^{u}_{\mathrm{rev}}(\rho_{AB}) := [1-2^{-\mathcal{R}_{\max,\mathrm{ADG}}(\rho_{AB})}]\cdot E_F(\omega_{AB}),$$

where ω_{AB} is the ADG*-squeezed state of ρ_{AB}, $E_F(\cdot)$ is the entanglement of formation.*

Thanks to the essential convexity of $E_{D,\rightarrow}(\cdot)$ on decomposing a state into degradable and anti-degradable parts, the main insight of our method is to squeeze out as much of the *free or useless* part, the anti-degradable state here, as possible. We note $\mathcal{R}_{\max,\mathrm{ADG}}(\rho_{AB})$ can be efficiently computed via SDP and $E_F(\omega_{AB})$ has a trivial upper bound as $E_F(\omega_{AB}) \leq \sum_i \lambda_i S(B)_{\psi_i}$ where $S(B)_{\psi_i}$ is the von Neumann entropy of $|\psi_i\rangle$. Then we obtain an efficiently computable bound as Corollary 3.

Corollary 3 *For any bipartite state ρ_{AB}, it satisfies*

$$\begin{aligned} E_{D,\rightarrow}(\rho_{AB}) &\leq \hat{E}^{u}_{\mathrm{rev}}(\rho_{AB}) \\ &:= [1-2^{-\mathcal{R}_{\max,\mathrm{ADG}}(\rho_{AB})}]\cdot\sum\lambda_i S(B)_{\psi_i}, \end{aligned}$$

where $\omega_{AB} = \sum_i \lambda_i|\psi_i\rangle\langle\psi_i|$ is the spectral decomposition of the ADG-squeezed state ω_{AB} of ρ_{AB}.

Also, after choosing the free states to be the states with positive partial transpose (PPT), we introduce the *reverse max-relative entropy of NPT entanglement*:

$$\mathcal{R}_{\max,\mathrm{PPT}}(\rho_{AB}) := \min_{\tau\in\mathrm{PPT}} D_{\max}(\tau_{AB}||\rho_{AB}). \tag{5}$$

This helps to give an upper bound on the two-way distillable entanglement as Theorem 4.

Theorem 4 *For any bipartite state ρ_{AB}, it satisfies*

$$E_{D,\leftrightarrow}(\rho_{AB}) \leq E^{npt}_{\mathrm{rev}}(\rho_{AB}) := [1-2^{-\mathcal{R}_{\max,\mathrm{PPT}}(\rho_{AB})}]\cdot E_F(\omega_{AB}),$$

where ω_{AB} is the PPT-squeezed state of ρ_{AB}.

It also follows an easily computable relaxation $\hat{E}^{npt}_{\mathrm{rev}}(\cdot)$ as that in Corollary 3. Remarkably, for the example states illustrated in [6], our bound tightens the approximation of the upper bound $E_{\mathrm{MP}}(\cdot)$ presented in [6].

Quantum Capacity. Our second contribution is to introduce the *reverse max-relative entropy of anti-degradability* for a quantum channel $\mathcal{N}_{A\rightarrow B}$:

$$\widetilde{\mathcal{R}}_{\max,\mathrm{ADG}}(\mathcal{N}_{A\rightarrow B}) := \min_{\mathcal{N}'_{A\rightarrow B}\in\mathcal{C}_{\mathrm{ADG}}} D_{\max}(\mathcal{N}'||\mathcal{N}), \tag{6}$$

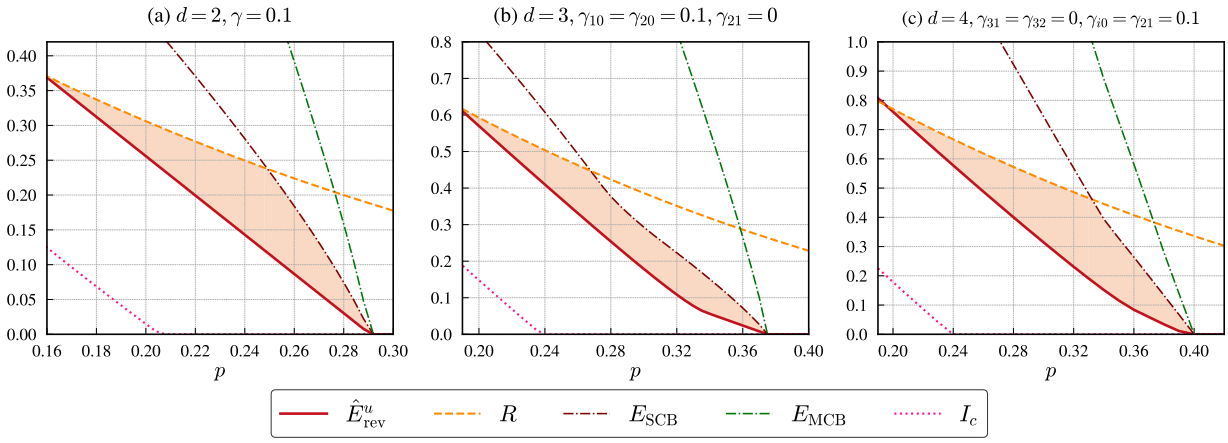


Figure 1: **Upper bounds on the one-way distillable entanglement of less entangled states.** The x-axis represents the change of the depolarizing noise p. The state's coherent information I_c provides a lower bound. R is the Rains bound. $\hat{E}^u_{\text{rev}}$ is the upper bound derived in Corollary 3. E_{SCB} and E_{MCB} are continuity bounds that can be found in the full version. It shows that $\hat{E}^u_{\text{rev}}$ outperforms all other upper bounds on these less entangled states.

where $\mathcal{C}_{\text{ADG}}$ is the set of all anti-degradable channels and the max-relative entropy of $\mathcal{N}'_{A\to B}$ with respect to $\mathcal{N}_{A\to B}$ is given by $D_{\max}(\mathcal{N}'_{A\to B}||\mathcal{N}_{A\to B}) := \inf\{\lambda\in\mathbb{R} : J^{\mathcal{N}'}_{AB} \leq 2^{\lambda} J^{\mathcal{N}}_{AB}\}$. We then introduce the ADG-*squeezed channel* of $\mathcal{N}_{A\to B}$ in Definition 5 and use these ideas to derive an upper bound on the quantum capacity in Theorem 6.

Definition 5 *For a quantum channel $\mathcal{N}_{A\to B}$ and the anti-degradable channel set $\mathcal{C}_{\text{ADG}}$, if $\widetilde{\mathcal{R}}_{\max,\text{ADG}}(\mathcal{N})$ is non-zero, the* ADG*-squeezed channel of $\mathcal{N}_{A\to B}$ is defined by*

$$\mathcal{S}_{A\to B} = \frac{\mathcal{N}_{A\to B} - 2^{-\widetilde{\mathcal{R}}_{\max,\text{ADG}}(\mathcal{N})}\cdot\mathcal{N}'_{A\to B}}{1-2^{-\widetilde{\mathcal{R}}_{\max,\text{ADG}}(\mathcal{N})}} \tag{7}$$

where $\mathcal{N}'_{A\to B}$ is the closest anti-degradable channel to $\mathcal{N}_{A\to B}$ in terms of the max-relative entropy, i.e., the optimal solution in Eq. (6). If $\widetilde{\mathcal{R}}_{\max,\text{ADG}}(\mathcal{N})$ is zero, the ADG*-squeezed channel of $\mathcal{N}_{A\to B}$ is itself.*

Theorem 6 *Given a quantum channel $\mathcal{N}_{A\to B}$, if it has an ADG-squeezed channel $\mathcal{S}_{A\to B}$, we denote $\widehat{\mathcal{S}}_{A\to BB'}$ as an extended channel of $\mathcal{S}_{A\to B}$ such that $\text{Tr}_{B'}[\widehat{\mathcal{S}}_{A\to BB'}(\rho_A)] = \mathcal{S}_{A\to B}(\rho_A), \forall\rho_A\in\mathcal{D}(\mathcal{H}_A)$. Then it satisfies*

$$\begin{aligned} Q(\mathcal{N}) \leq Q_{\text{sqz}}(\mathcal{N}) := [1-2^{-\widetilde{\mathcal{R}}_{\max,\text{ADG}}(\mathcal{N})}]\cdot \\ \min\left\{Q^{(1)}(\widehat{\mathcal{S}})|\ \widehat{\mathcal{S}}_{A\to BB'} \text{ is degradable}\right\}, \end{aligned} \tag{8}$$

where the minimization is over all possible extended channels of $S_{A\to B}$. If there is no such a degradable $\widehat{\mathcal{S}}_{A\to BB'}$ exists, the value of this bound is set to be infinity.

Notably, $\widetilde{\mathcal{R}}_{\max,\text{ADG}}(\mathcal{N})$ can be efficiently computed via SDP. For qubit quantum channels, we prove that the ADG-squeezed channel is always degradable. As a result, we obtain an efficiently computable upper bound on the quantum capacity of qubit channels as shown in the full version.

Applications to cases of interest. Our third contribution involves examining specific examples of various less entangled states and qubit channels. We demonstrate the advantages of our bounds in evaluating the distillable entanglement and the quantum capacity, compared with previous computable bounds. First, suppose Alice and Bob are sharing pairs of maximally entangled states affected by bi-local noisy channels, i.e.,

$$\rho_{A'B'} = \mathcal{N}_{A\to A'}\otimes\mathcal{N}_{B\to B'}(\Phi_{AB}). \tag{9}$$

With regard to the amplitude damping channel and the depolarizing channel acting on Alice and Bob respectively, our bound outperforms the Rains bound [3] and different continuity bounds in a high-noise region in different dimensional systems, as shown in Fig. 1.

For the quantum capacity of noisy channels, we compare the performance of our method with some best-known computable bounds, e.g., the continuity bound in Theorem [34] and the bound $\hat{R}_\alpha$ [20] generalized from the max-Rain information [17], using the mixed unitary channel $\mathcal{U}_{A\to B}(\cdot)$ as $\mathcal{U}(\rho) = \sum_{i=0}^{k} p_i U_i\rho U_i^\dagger$, where $\sum_{i=0}^{k} p_i = 1$ and U_i are unitary operators on a qubit system. For many instances, our bound can outperform the continuity bound of anti-degradability and achieve comparable results to $\hat{R}_\alpha$ shown in the full version.

In particular, a qubit Pauli channel $\Lambda(\cdot)$ is defined as $\Lambda(\rho) = p_0\rho + p_1 X\rho X + p_2 Y\rho Y + p_3 Z\rho Z$, where X, Y, Z are the Pauli operators and $\sum_{i=0}^{3} p_i = 1$ are probability parameters. Our method can recover the no-cloning bound [21] on the quantum capacity of qubit Pauli channels. Moreover, recent work [35] studies the capacities of a subclass of Pauli channels called the *covariant Pauli channel*, where the parameters are set $p_1 = p_2$ with $p_0+2p_1+p_3 = 1$, i.e., $\Lambda_{\text{cov}}(\rho) = p_0\rho + p_1(X\rho X + Y\rho Y) + p_3 Z\rho Z$. We compare our bound with the upper bounds given in [35], as well as the previous computable bounds shown in the full version Part.IV. It can be seen that our bound, coinciding with the no-cloning bound, outperforms other bounds in certain regions, and thus can better characterize the quantum capacity of $\Lambda_{\text{cov}}(\cdot)$ when it is in proximity to being anti-degradable.

References

[1] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, jan 2005. ISSN 1364-5021. doi: 10.1098/rspa.2004.1372. URL http://arxiv.org/abs/quant-ph/0306078%0Ahttp://dx.doi.org/10.1098/rspa.2004.1372https://royalsocietypublishing.org/doi/10.1098/rspa.2004.1372.

[2] Satvik Singh and Nilanjana Datta. Fully undistillable quantum states are separable. *arXiv preprint arXiv:2207.05193*, 2022.

[3] Eric M. Rains. A semidefinite program for distillable entanglement. *IEEE Transactions on Information Theory*, 47(7):2921–2933, aug 2000. ISSN 00189448. doi: 10.1109/18.959270.

[4] Xin Wang and Runyao Duan. Improved semidefinite programming upper bound on distillable entanglement. *Physical Review A*, 94(5):050301, nov 2016. ISSN 2469-9926. doi: 10.1103/PhysRevA.94.050301.

[5] Masahito Hayashi. *Quantum Information*. Number 1. Springer, 2006. ISBN 3540302654. doi: 10.1007/s13398-014-0173-7.2.

[6] Felix Leditzky, Nilanjana Datta, and Graeme Smith. Useful states and entanglement distillation. *IEEE Transactions on Information Theory*, 64(7):4689–4708, jan 2017. ISSN 0018-9448. doi: 10.1109/TIT.2017.2776907.

[7] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter. Extendibility Limits the Performance of Quantum Processors. *Physical Review Letters*, 123(7):070502, aug 2019. ISSN 0031-9007. doi: 10.1103/PhysRevLett.123.070502.

[8] Xin Wang. Pursuing the Fundamental Limits for Quantum Communication. *IEEE Transactions on Information Theory*, 67(7):4524–4532, jul 2021. ISSN 0018-9448. doi: 10.1109/TIT.2021.3068818.

[9] Yingkai Ouyang. Channel covariance, twirling, contraction, and some upper bounds on the quantum capacity. *Quantum Information and Computation*, 14(11-12):917–936, jun 2011. doi: 10.26421/QIC17.11-12.

[10] Farzad Kianvash, Marco Fanizza, and Vittorio Giovannetti. Bounding the quantum capacity with flagged extensions. *Quantum*, 6:647, feb 2022. ISSN 2521-327X. doi: 10.22331/q-2022-02-09-647. URL https://quantum-journal.org/papers/q-2022-02-09-647/.

[11] Michael M Wolf and David Pérez-Garcia. Quantum capacities of channels with small environment. *Physical Review A*, 75(1):012303, jan 2007. ISSN 1050-2947. doi: 10.1103/PhysRevA.75.012303.

[12] Marco Fanizza, Farzad Kianvash, and Vittorio Giovannetti. Quantum Flags and New Bounds on the Quantum Capacity of the Depolarizing Channel. *Physical Review Letters*, 125(2):020503, jul 2020. ISSN 0031-9007. doi: 10.1103/PhysRevLett.125.020503.

[13] A. Holevo and R. Werner. Evaluating capacities of bosonic Gaussian channels. *Physical Review A*, 63 (3):032312, feb 2001. ISSN 1050-2947. doi: 10.1103/PhysRevA.63.032312.

[14] David Sutter, Volkher B Scholz, Andreas Winter, and Renato Renner. Approximate Degradable Quantum Channels. *IEEE Transactions on Information Theory*, 63(12):7832–7844, dec 2014. ISSN 0018-9448. doi: 10.1109/TIT.2017.2754268.

[15] Alexander Müller-Hermes, David Reeb, and Michael M Wolf. Positivity of linear maps under tensor powers. *Journal of Mathematical Physics*, 57(1):015202, jan 2016. ISSN 0022-2488. doi: 10.1063/1.4927070. URL http://aip.scitation.org/doi/10.1063/1.4927070.

[16] Xin Wang and Runyao Duan. A semidefinite programming upper bound of quantum capacity. In *2016 IEEE International Symposium on Information Theory (ISIT)*, volume 2016-Augus, pages 1690–1694. IEEE, jul 2016. ISBN 978-1-5090-1806-2. doi: 10.1109/ISIT.2016.7541587.

[17] Xin Wang, Kun Fang, and Runyao Duan. Semidefinite Programming Converse Bounds for Quantum Communication. *IEEE Transactions on Information Theory*, 65(4):2583–2592, apr 2019. ISSN 0018-9448. doi: 10.1109/TIT.2018.2874031. URL https://ieeexplore.ieee.org/document/8482492/.

[18] Robert Pisarczyk, Zhikuan Zhao, Yingkai Ouyang, Vlatko Vedral, and Joseph F. Fitzsimons. Causal Limit on Quantum Communication. *Physical Review Letters*, 123(15):150502, oct 2019. ISSN 0031-9007. doi: 10.1103/PhysRevLett.123.150502.

[19] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8:15043, apr 2017. ISSN 2041-1723. doi: 10.1038/ncomms15043.

[20] Kun Fang and Hamza Fawzi. Geometric Renyi Divergence and its Applications in Quantum Channel Capacities. *arXiv:1909.05758*, sep 2019.

[21] Nicolas J Cerf. Pauli Cloning of a Quantum Bit. *Physical Review Letters*, 84(19):4497–4500, may 2000. ISSN 0031-9007. doi: 10.1103/PhysRevLett.84.4497.

[22] Graeme Smith, John A. Smolin, and Andreas Winter. The Quantum Capacity With Symmetric

Side Channels. *IEEE Transactions on Information Theory*, 54(9):4208–4217, sep 2008. ISSN 0018-9448. doi: 10.1109/TIT.2008.928269. URL http://ieeexplore.ieee.org/document/4608993/.

[23] Li Gao, Marius Junge, and Nicholas LaRacuente. Capacity bounds via operator space methods. *Journal of Mathematical Physics*, 59(12):122202, dec 2018. ISSN 0022-2488. doi: 10.1063/1.5058692.

[24] Lieven Vandenberghe and Stephen Boyd. Semidefinite Programming. *SIAM Review*, 38(1):49–95, mar 1996. ISSN 0036-1445. doi: 10.1137/1038003.

[25] Nilanjana Datta. Min- and max-relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826, jun 2009. doi: 10.1109/tit.2009.2018325.

[26] Avshalom C. Elitzur, Sandu Popescu, and Daniel Rohrlich. Quantum nonlocality for each pair in an ensemble. *Physics Letters A*, 162(1):25–28, 1992. ISSN 0375-9601. doi: https://doi.org/10.1016/0375-9601(92)90952-I. URL https://www.sciencedirect.com/science/article/pii/037596019290952I.

[27] Maciej Lewenstein and Anna Sanpera. Separability and entanglement of composite quantum systems. *Phys. Rev. Lett.*, 80:2261–2264, Mar 1998. doi: 10.1103/PhysRevLett.80.2261. URL https://link.aps.org/doi/10.1103/PhysRevLett.80.2261.

[28] Andrés F. Ducuara and Paul Skrzypczyk. Operational Interpretation of Weight-Based Resource Quantifiers in Convex Quantum Resource Theories. *Physical Review Letters*, 125(11):110401, sep 2020. ISSN 0031-9007. doi: 10.1103/PhysRevLett.125.110401. URL https://link.aps.org/doi/10.1103/PhysRevLett.125.110401.

[29] Roope Uola, Tom Bullock, Tristan Kraft, Juha-Pekka Pellonpää, and Nicolas Brunner. All Quantum Resources Provide an Advantage in Exclusion Tasks. *Physical Review Letters*, 125(11):110402, sep 2020. ISSN 0031-9007. doi: 10.1103/PhysRevLett.125.110402. URL https://link.aps.org/doi/10.1103/PhysRevLett.125.110402.

[30] Kun Fang and Zi-Wen Liu. No-Go Theorems for Quantum Resource Purification: New Approach and Channel Theory. *PRX Quantum*, 3(1):010337, mar 2022. ISSN 2691-3399. doi: 10.1103/PRXQuantum.3.010337. URL https://link.aps.org/doi/10.1103/PRXQuantum.3.010337.

[31] Bartosz Regula and Ryuji Takagi. Fundamental limitations on distillation of quantum channel resources. *Nature Communications*, 12(1), jul 2021. doi: 10.1038/s41467-021-24699-0. URL https://doi.org/10.1038%2Fs41467-021-24699-0.

[32] Bartosz Regula, Ludovico Lami, and Mark M Wilde. Overcoming entropic limitations on asymptotic state transformations through probabilistic protocols. *arXiv preprint arXiv:2209.03362*, 2022.

[33] Bartosz Regula, Ludovico Lami, and Mark M Wilde. Postselected quantum hypothesis testing. *arXiv preprint arXiv:2209.10550*, 2022.

[34] David Sutter, Volkher B. Scholz, Andreas Winter, and Renato Renner. Approximate degradable quantum channels. *IEEE Transactions on Information Theory*, 63(12):7832–7844, dec 2017. doi: 10.1109/tit.2017.2754268.

[35] Abbas Poshtvan and Vahid Karimipour. Capacities of the covariant pauli channel. *Physical Review A*, 106(6):062408, 2022. doi: 10.1103/physreva.106.062408. URL https://doi.org/10.1103%2Fphysreva.106.062408.

Limitations and optimizations of quantum computing in the presence of resource constraints

Marco Fellous-Asiani[1] Jing Hao Chai[2 1] Robert S. Whitney[3] Alexia Auffèves[2]
Hui Khoon Ng[4 2 5 *]

[1] *Institut Néel, France*
[2] *Centre for Quantum Technologies, National University of Singapore, Singapore*
[3] *Laboratoire de Physique et Modélisation des Milieux Condensés, Université Grenoble Alpes and CNRS, France*
[4] *Yale-NUS College, Singapore*
[5] *MajuLab, International Joint Research Unit UMI 3654, CNRS, UCA-SU-NUS-NTU, Singapore*

Abstract. Fault-tolerant quantum computing is the only known route to bring our present-day small and noisy devices to large-scale ones capable of accurate computation for useful problems. In current experiments, however, physical resource constraints (e.g., energy, space, bandwidth, etc.) place significant limitations in the attainable computational accuracy. In a series of two papers [1, 2], we discuss the performance of quantum computers in the presence of resource constraints, and demonstrate how to make the best use of available resources to achieve a target accuracy. Our study highlights the power of a full-stack, user-to-experimenter, analysis that accounts for all physical and computational elements that enter a large-scale quantum computer.

Keywords: Fault-tolerant quantum computing, full-stack quantum computers, implementations

1 Introduction

With the advent of small-scale quantum computing devices from companies like IBM, and the myriad software and hardware quantum startups, the interest in realising quantum computers is at an all-time high. While we hope for small quantum advantages in NISQ-era devices, the central question is still "how do we make our quantum computers more powerful?" The answer is, of course, to have larger quantum computers. But larger also usually means noisier, with more fragile quantum components that can go wrong, leading to more computational errors. The standard way out of this conundrum is fault-tolerant quantum computation (FTQC), the only known route to scaling up quantum computers while keeping errors in check.

FTQC schemes have been known since the early days of the field, and remain an active field of research, especially with the more recent discussions of experimentally feasible surface codes. Underlying all FTQC schemes are basic assumptions about the nature of the quantum devices and the noise afflicting them. Many of these assumptions, laid down long before experimental devices came about, were based on general physical expectations not specific to any one implementation. As we learn more about the shape of quantum computers to come, it is important to re-visit those assumptions, to update them to properly describe real devices, so that the schemes remain relevant to our progress towards large-scale, useful quantum computers.

FTQC tells us, for a fixed problem size, how to improve computational accuracy by increasing the number of physical qubits and gates—and hence the physical size or scale of the quantum computer—spent on implementing the computation. Every known FTQC scheme relies on quantum error correction (QEC) to remove errors, using more and more powerful codes to remove more and more errors, accompanied by a prescription to avoid uncontrolled spread of errors as the computer grows. One key assumption is that the physical error probability (or more generally, the strength) η—the maximum probability that an error occurs in a physical qubit or gate—remains constant as the computer scales up in size. If η grows as the computer grows, we cannot expect to keep up with the rapid accumulation of errors.

Unfortunately, the growth of η with scale is observed in current quantum devices. For example, in ion-trap experiments, the gate fidelity drops rapidly if more and more ions are put into the same trap; this is the motivation behind the push for networked ion traps and flying qubits to communicate between traps (see, for example, [3]). Another example is provided by qubits that are coherently controlled, by resonantly addressing their transition. Here a limit on the total available driving power results in lower gate fidelity, if many gates have to be done simultaneously [4]. This effect can also occur simply because qubit transition frequencies are too close for the available physical separation: Qubits may be placed closer together as we scale up, giving rise to greater cross-talk between qubits when doing individual gates [5]. All these are, of course, indicators of how certain aspects of current technology are not yet fully scalable, but such practical difficulties are likely to remain in near- to middle-term devices.

This reality of the growth of physical error probability as the computer scales up in size brings into complex interplay two parts of building a quantum computer: On the one side, we have the computational accuracy we want to achieve; on the other side, we have the effects of noise and our attempts, using limited resources, to control it. With constrained resources, we find a limit to

*huikhoon.ng@nus.edu.sg

the attainable computational accuracy even if we make use of FTQC procedures that promises arbitrarily accurate computation but only if physical error probability remains scale-independent. Our Paper [1] examines this limitation in various contexts, from toy models to more realistic cross-talk situations. On the flip side, with the recognition that we need only achieve some target accuracy for some given algorithm we want to run on the quantum computer, we can instead talk about minimizing the physical resource cost—e.g., number of physical qubits used, the total energy usage, physical volume, etc.—to achieve the desired computation. Our Paper [2] discusses this optimization angle using a full-stack superconducting quantum computer as the illustrative example. We refer the reader to the full articles for further details. Below, we highlight some of the lessons learned.

2 Some highlights

The toy model defined in Paper [1], though simple, already brings out the qualitative nature of the limits to computational accuracy in the presence of physical error probability that grows with scale, or "scale-dependent noise" for short. Making use of the concrete FTQC scheme of Aliferis et al. [6], built by concatenating the 7-qubit quantum error correcting code, we show how the standard quantum accuracy threshold theorem—a cornerstone result that says that arbitrarily accurate quantum computation is attainable by scaling up the size of the physical computer once the noise is below a threshold level—no longer holds. Fig. 1 depicts the typical situation: **As the computer scales up** (quantified here by the concatenation level k in the fault tolerance scheme)**, rather than having the accuracy of the computer** (quantified here by the error per logical gate operation) **increase monotonically without limit as in standard fault tolerance, scale-dependent noise results in a turnaround of the computational accuracy after reaching a maximum, or, equivalently, a minimum error.**

With the violation of a basic assumption of fault tolerance theory, that the standard threshold theorem fails should come as no surprise. What is startling is how early its failure can set in, and how easily such conditions can arise in real experiments. In one of our examples (see Sec. IVA in Paper [1]), for error correction to even be useful, we require a condition on the physical error probability that is 10^5 smaller than the usual fault-tolerance threshold condition. This highlights the areas of current weakness that demand further study, if we want to continue on the road to genuinely useful quantum computers.

The close link between computational accuracy and our attempts to control noise by investing more physical resources offers the possibility of estimating and optimizing the resource use, to attain a specific target computational accuracy for a given algorithm. This is what is done in our Paper [2], using superconducting qubit devices as the central example. One of the tasks we examine is to optimize the power cost to crack the RSA public-key cryptographic system using Shor's factoring algorithm. Such an analysis requires **a complete model of the full-stack quantum computer protected by fault-tolerant quantum error correction**, necessarily drawing on a wide range of expertise on computational-theoretical knowledge to physical-experimental details. Figure 2 illustrates the level of detailed description of the physical and FTQC pieces used in our analysis. Our optimization is able to give the experimental settings, including operating temperatures and attenuation levels for the different classical and quantum physical layers, that minimize the power cost. We discuss this for the 7-qubit FTQC scheme of [6] as well as for the currently popular surface-code approach. In addition, **we observe surprising behaviors that could not have easily been predicted without a direct computational-physical link as we have used here**, including regimes of energetic advantage for quantum computers without a speed advantage over classical computers; see Fig. 3. In some cases, the optimization of the computer design can reduce the power bill by orders of magnitude.

Our analysis can be applied to a wide array of quantum computing platforms. The conclusions provide better clarity on areas of practical constraints that can affect computational accuracy, and give design guidance to experimentalists striving towards resource-efficient quantum devices.

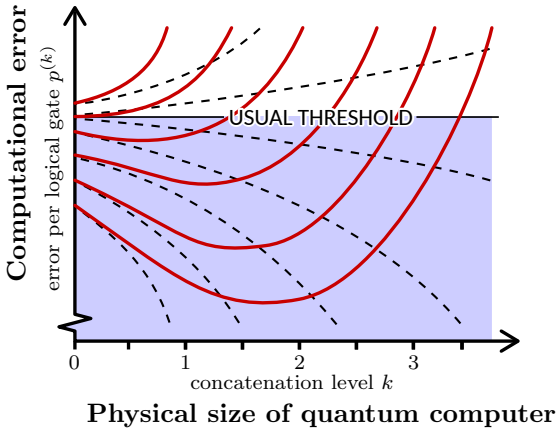


Figure 1: (Taken from Fig. 3 of Paper [1].) A schematic diagram depicting the conventional situation (black dotted lines) where the physical error probability η is independent of the physical size—quantified by the "concatenation level k" of the 7-qubit FTQC scheme—of the computer, and our current consideration where η grows with k (red solid lines, each for a different value of $p^{(0)} \equiv \eta$). If η is scale-independent, standard fault tolerance analysis says that the error per logical gate $p^{(k)}$—quantifying the computational accuracy—can be brought as close to 0 as desired by increasing k, provided one starts below the threshold (solid horizontal line) at $k = 0$. If η depends on k, even if one starts below the threshold, $p^{(k)}$ eventually turns around for large enough k; $p^{(k)}$ cannot reach 0, there is a maximum concatenation level, and further increase in k only increases the logical error.

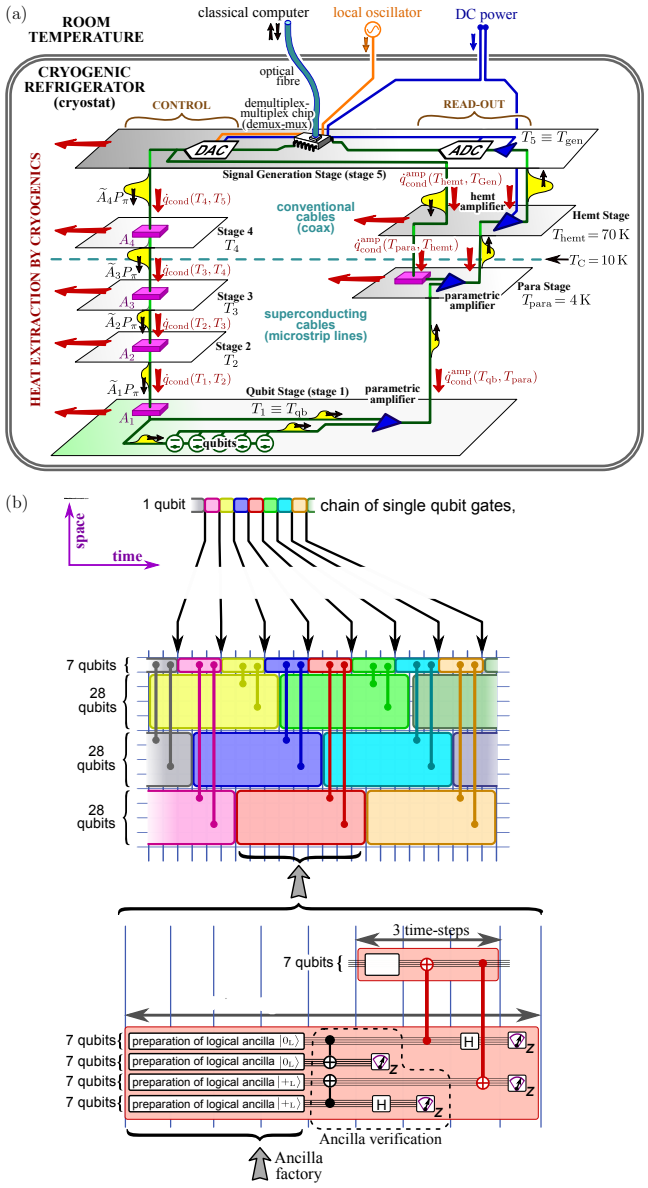


Figure 2: (Taken from Figs. 8 & 9 of Paper [2].) The full-stack quantum computing system considered in our work: (a) shows the physical system, including the classical electronics and cryogenic stages in addition to the quantum layer at the bottom; (b) shows the 7-qubit-code concatenated FTQC scheme. The comprehensive analysis in our work requires a detailed model of every aspect of the quantum computing system. Such an analysis yields results that cannot be easily deduced from more simplistic modeling that neglects the close ties between the physical and algorithmic aspects. We consider mainly the 7-qubit code FTQC scheme of Ref. [6] due to its theoretical simplicity; however, we also discuss the situation of the currently popular surface-code scheme. See full details in Paper [2].

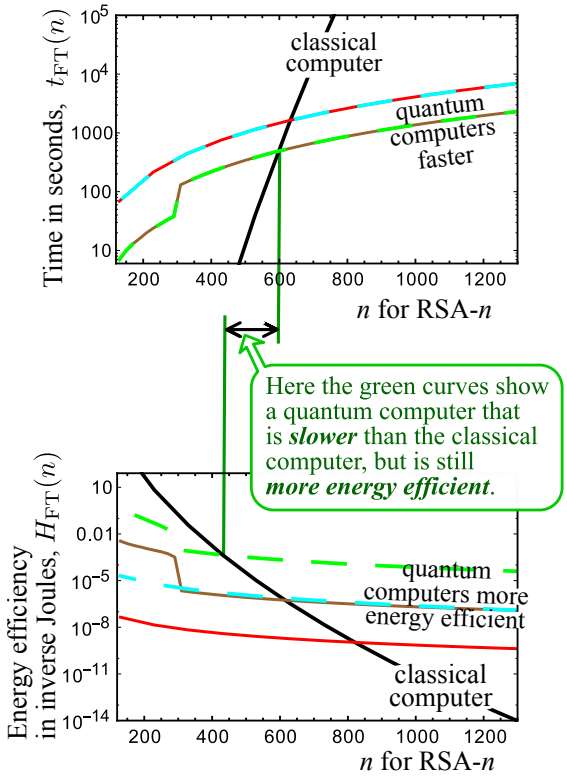


Figure 3: (Taken from Fig. 11 of Paper [2].) Comparing classical and quantum computing for cracking the RSA cryptographic system for different key sizes n. We find the perhaps surprising result that there is a region with a quantum *energetic* advantage without a speed advantage; see figure. This is a distinct quantum advantage from the usual quantum "supremacy" tagline where one expects an energetic advantage because the quantum computer is able to complete the calculation in a significantly shorter time. See full details in Paper [2].

References

[1] Marco Fellous-Asiani, Jing Hao Chai, Robert S. Whitney, Alexia Auffèves, and Hui Khoon Ng. Limitations in quantum computing from resource constraints. *PRX Quantum*, 2:040335, Nov 2021.

[2] Marco Fellous-Asiani, Jing Hao Chai, Yvain Thonnart, Hui Khoon Ng, Robert S. Whitney, and Alexia Auffèves. Optimizing resource efficiencies for scalable full-stack quantum computers. arXiv:2209.05469, 2022.

[3] C. Monroe and J. Kim. Scaling the ion trap quantum processor. *Science*, 339(6124):1164–1169, 2013.

[4] J. Ikonen, Salmilehto, J., and M. Möttönen. Energy-efficient quantum computing. *npj Quantum Inf*, 3:17, 2017.

[5] Frank Arute, Kunal Arya, Ryan Babbush, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[6] Panos Aliferis, Daniel Gottesman, and John Preskill. Quantum accuracy threshold for concatenated distance-3 codes. *Quantum Info. Comput.*, 6(2):97–165, Mar 2006.

Extended Abstract: Thermodynamic Signatures of Genuinely Multipartite Entanglement

Samgeeth Puliyil,[1] Manik Banik,[2] and Mir Alimuddin[2]

[1]*School of Physics, IISER Thiruvananthapuram, Vithura, Kerala 695551, India.*

[2]*Department of Theoretical Sciences, S.N. Bose National Center for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India.*

Theory of bipartite entanglement shares profound similarities with thermodynamics. In this letter we extend this connection to multipartite quantum systems where entanglement appears in different forms with genuine entanglement being the most exotic one. We propose thermodynamic quantities that capture signature of genuineness in multipartite entangled states. Instead of entropy, these quantities are defined in terms of energy – particularly the difference between global and local extractable works (ergotropies) that can be stored in quantum batteries. Some of these quantities suffice as faithful measures of genuineness and to some extent distinguish different classes of genuinely entangled states. Along with scrutinizing properties of these measures we compare them with the other existing genuine measures, and argue that they can serve the purpose in a better sense. Furthermore, generality of our approach allows to define suitable functions of ergotropies capturing the signature of k-nonseparability that characterizes qualitatively different manifestations of entanglement in multipartite systems.

Journal Reference: Phys. Rev. Lett. **129**, 070601 (2022)

Introduction.– Like the second law of thermodynamics that prohibits complete conversion of heat (disordered form of energy) to work (ordered form of energy) in a cyclic process, the theory of entanglement is also governed by a no-go that forbids creation of entanglement among spatially separated quantum systems under local operations and classical communication (LOCC). This qualitative analogy goes even deeper – in accordance with the thermodynamic reversibility, the inter-conversion among pure bipartite entangled states is reversible under LOCC in asymptotic limit [1–3]. Furthermore, the rate of inter-conversion is quantitatively determined by von Neumann entropy, which has direct relation with the thermodynamic entropy [4–7]. For such states, the von Neumann entropy of the reduced marginal, in fact, serves as the unique quantifier (measure) of entanglement [3]. Although the reversibility of entanglement theory breaks down for mixed states [8–11], it does not cancel the analogy between entanglement theory and thermodynamics; rather, it acts as a constitutive element [9]. In this letter we ask the question how far the analogy between thermodynamics and entanglement theory can go when multipartite systems are considered. This question is quite pertinent, since for such systems classification of quantum states becomes much richer as compared to the separable vs entangled dichotomy of bipartite scenario. Depending on how different subsystems are correlated with each other, qualitatively different classes of entangled states are possible when more than two subsystems are involved. Among these, the most exotic one is the genuinely entangled state that first ap-

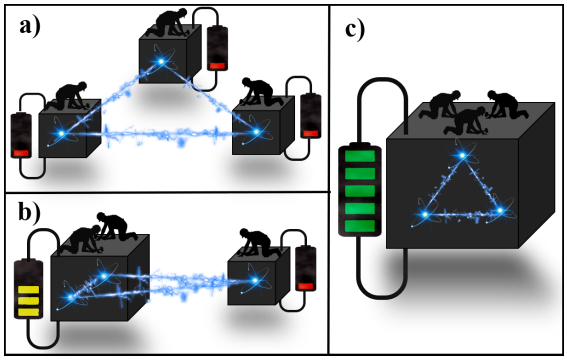


FIG. 1: Different amount of ergotropic works can be extracted from a multipartite entangled quantum state: (a) local ergotropic work $W_e^{A|B|C} \equiv W_e^l$, (b) biseparable ergotropic work $W_e^{X|X^{\mathsf{C}}}$, with $X \in \{A, B, C\}$, and (c) global ergotropic work W_e^g. In general, $W_e^l \leq W_e^{X|X^{\mathsf{C}}} \leq W_e^g$, where strict inequalities hold for genuinely entangled states.

pears in the seminal Greenberger–Horne–Zeilinger (GHZ) Version of the Bell test [12, 13]. Subsequently, it has been shown that genuinely entangled states can also be of different types [14–16]. Identification, characterization, and quantification of genuine entanglement are of practical relevance, as they find several applications [17–25], and accordingly different quantifiers have been suggested [26–32]. In this letter, we propose thermodynamic quantities that capture signature of genuineness in multipartite states. Unlike the bipartite pure states, where entanglement is captured through entropic quantity, our proposed measures are defined in terms of internal energy of the system. In particular, the *ergotropic gap* – difference between the extractable works from a composite system under global and local unitary operations, respectively – plays a crucial role to define these measures. We show that, suitably defined functions of this quantity – minimum ergotropic gap, average ergotropic gap, ergotropic fill, and ergotropic volume – can serve as good measures of genuineness for multipartite systems. In fact, one can come up with measures that capture the notion of k-separability for arbitrary multipartite systems [33]. Apart from theoretical curiosity these measures are of special interest as there are several proposals for quantum batteries to store ergotropic work [34–40]. By comparing strengths and weaknesses of these newly proposed measures with the other existing genuine measures, we show that the ergotropic measures show superiority.

Ergotropy and genuine entanglement.– Ergotrpic work (W_e) defines how much work can be extracted from an isolated system[41–43]. For the multipartite system different scenarios can be constructed for the ergotropic work extraction (See fig 1). Now we can define various measure of entanglement (fully separable, ni-separable, genuine) in terms of ergotropic work difference. Here I will very shortly introduce those quantities:

A. Fully separable entanglement measure: A n-partite fully separable measure is defined by the global ergotropic work and completely local ergotropic work *i.e.,* $\Delta^{(n)}_{A_1|\cdots|A_n} = W_e^g - W_e^{A_1|\cdots|A_n}$.

B. K-separble entanglement measure: To capture the notion of k-nonseparability here we propose the

concept of k-separable ergotropic gap $\Delta^{(k)}_{X_1|\cdots|X_k} := W_e^g - W_e^{X_1|\cdots|X_k}$, where $W_e^{X_1|\cdots|X_k}$ denotes the ergotropic works when n different parties are partitioned as $X_1|\cdots|X_k$.

C. Genuine entanglement measure: (i) *Minimum ergotropic gap* $\left(\Delta^G_{\min}\right)$:- It is defined as the minimum among all possible bi-separable ergotropic gaps, *i.e.,* for $|\psi\rangle_{A_1\cdots A_n} \in \bigotimes_{i=1}^n \mathbb{C}^{d_i}$ $\Delta^G_{\min}(|\psi\rangle) := \min\left\{\Delta^{(2)}_{X|X^{\mathsf{C}}}(|\psi\rangle)\right\}$, where minimization is over all possible bipartitions $\{X|X^{\mathsf{C}}\}$ of the parties.

(ii) Genuine average ergotropic gap $\left(\Delta^G_{\text{avg}}\right)$:- The following quantity is also a genuine measure, $\Delta^G_{\text{avg}}(|\psi\rangle) := \frac{\Theta\left(\prod_X \Delta^{(2)}_{X|X^{\mathsf{C}}}(|\psi\rangle)\right)}{2^{(n-1)}-1} \sum_X \Delta^{(2)}_{X|X^{\mathsf{C}}}(|\psi\rangle)$, where X ranges over all possible bipartitions ($2^{(n-1)}-1$ in number for n-party system) and $\Theta(Z) = 0$ for $Z = 0$ else $\Theta(Z) = 1$.

(iii) *Ergotropic fill* $\left(\Delta^G_F\right)$:- Motivated by the genuine measure of 'concurrence fill' recently introduced for three-qubit systems [32], we can define ergotropic fill for such systems as follows,

$$\Delta^G_F(|\psi\rangle) := \frac{1}{\sqrt{3}}\left[\left(\sum_X \Delta^{(2)}_{X|X^{\mathsf{C}}}\right)^2 - 2\left(\sum_X \left(\Delta^{(2)}_{X|X^{\mathsf{C}}}\right)^2\right)\right]^{\frac{1}{2}},$$

where $X \in \{A, B, C\}$.

(iv) *Ergotropic volume* $\left(\Delta^G_V\right)$:- For an n-party state $|\psi\rangle_{A_1\cdots A_n} \in \otimes_{i=1}^n \mathbb{C}^{d_i}$ we can define the normalized volume Δ^G_V of N-edged hyper-cuboid with sides $\Delta^{(2)}_{X|X^{\mathsf{C}}}(|\psi\rangle)$ as a genuine measure of entanglement, *i.e.*, $\Delta^G_V(|\psi\rangle) := \left(\prod_{X=1}^N \Delta^{(2)}_{X|X^{\mathsf{C}}}(|\psi\rangle)\right)^{\frac{1}{N}}$; $N = 2^{(n-1)} - 1$.

In our letter, we have discussed the LOCC monotonicity of genuine measures (i), (ii) and (iv) as well as compare them with the existing measures. Most importantly, with addition we state their physical meaning.

Discussion.– Genuine entanglement represents prototypical features of multipartite quantum systems. Apart from their foundational importance [12] they find several applications [17–25] and also they are crucial for the emerging technology of quantum internet [44, 45]. Here we have proposed several measures of genuine entanglement based on thermodynamic quantities. The correspondence between thermodynamics and entanglement theory is not new as information theory makes a link between bipartite entanglementment and thermodynamics through the abstract concept of entropy. Importantly, the connection established between genuine entanglement and thermodynamics in this work is much direct as it does not invoke entropy, rather it is based on internal energies or ergotropic works of the system. Ergotropic work being an experimentally measurable quantity, even under ambient conditions, makes this connection more interesting. In particular, we have introduced four different measures for genuine entanglement among which ergotropic volume has been inferred to perform better than other three as well as the previously existing measures. Importantly, ergotropic volume also captures a physical meaning up-to some degree while still maintaining the integrity as a genuine multipartite entanglement measure without any ad-hoc conditions. Furthermore, we have shown that based on ergotropic quantities it is also possible to define measures of k-nonseparability that signifies qualitatively different manifestations of entanglement for multipartite systems. As for future, possible

experimental realisations of the proposed measures would be quite interesting. It would be instructive to explore the multi-qubit systems, more particularly three-qubit system, first. Another possible study would be to see how the ergotropic gap decreases when more and more restrictions are imposed on the collaboration among the parties, as this would give an idea whether or not the cost of coming together pays off significant increment in work extraction. It would also be interesting to capture the signature of *entanglement depth* [46] of an multipartite state through the ergotropic approach explored in this letter. Finally, it would also be interesting to see how our approach can be generalized to study other forms of correlation in mutipartite systems, a closely related study recently made for bipartite systems in Ref.[47].

[1] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[2] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[3] V. Vedral and E. Kashefi, Phys. Rev. Lett. **89**, 037903 (2002).

[4] S. Popescu and D. Rohrlich, Phys. Rev. A **56**, R3319 (1997).

[5] P. Horodecki, R. Horodecki, and M. Horodecki, arXiv:quant-ph/9805072 (1998).

[6] V. Vedral, AIP Conf. Proc. **643**, 41 (2002).

[7] M. Weilemann, L. Kraemer, P. Faist, and R. Renner, Phys. Rev. Lett. **117**, 260601 (2016).

[8] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[9] M. Horodecki, J. Oppenheim, and R. Horodecki, Phys. Rev. Lett. **89**, 240403 (2002).

[10] G. Vidal, W. Dür, and J. I. Cirac, Phys. Rev. Lett. **89**, 027901 (2002).

[11] L. Lami and B. Regula, arXiv:2111.02438 (2021).

[12] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Quantum Theory, and Conceptions of the Universe , 69 (1989).

[13] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[14] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).

[15] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach, Phys. Rev. Lett. **85**, 1560 (2000).

[16] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde, Phys. Rev. A **65**, 052112 (2002).

[17] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[18] D. Leibfried, M. D. Barrett, T. Schaetz, J. Britton, J. Chiaverini, W. M. Itano, J. D. Jost, C. Langer, and D. J. Wineland, Science **304**, 1476 (2004).

[19] V. Giovannetti, S. Lloyd, and L. Maccone, Science **306**, 1330 (2004).

[20] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, and J.-W. Pan, Nature **430**, 54 (2004).

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

[22] S. Agrawal, S. Halder, and M. Banik, Phys. Rev. A **99**, 032335 (2019).

[23] S. Rout, A. G. Maity, A. Mukherjee, S. Halder, and M. Banik, Phys. Rev. A **100**, 032321 (2019).

[24] S. Rout, A. G. Maity, A. Mukherjee, S. Halder, and M. Banik, Phys. Rev. A **104**, 052433 (2021).

[25] S. S. Bhattacharya, A. G. Maity, T. Guha, G. Chiribella, and M. Banik, PRX Quantum **2**, 020350 (2021).

[26] A. R. R. Carvalho, F. Mintert, and A. Buchleitner, Phys. Rev. Lett. **93**, 230501 (2004).

[27] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[28] A. Miyake, Phys. Rev. A **67**, 012108 (2003).

[29] A. Osterloh and J. Siewert, Phys. Rev. A **72**, 012337 (2005).

[30] A. Sen(De) and U. Sen, Phys. Rev. A **81**, 012308 (2010).

[31] B. Jungnitsch, T. Moroder, and O. Gühne, Phys. Rev. Lett. **106**, 190502 (2011).

[32] S. Xie and J. H. Eberly, Phys. Rev. Lett. **127**, 040403 (2021).

[33] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[34] G. M. Andolina, M. Keck, A. Mari, M. Campisi, V. Giovannetti, and M. Polini, Phys. Rev. Lett. **122**, 047702 (2019).

[35] D. Rossini, G. M. Andolina, D. Rosa, M. Carrega, and M. Polini, Phys. Rev. Lett. **125**, 236402 (2020).

[36] J. Monsel, M. Fellous-Asiani, B. Huard, and A. Auffèves, Phys. Rev. Lett. **124**, 130601 (2020).

[37] E. S. *et al.*, Nature Nanotechnology **15**, 656 (2020).

[38] T. Opatrný, A. Misra, and G. Kurizki, Phys. Rev. Lett. **127**, 040602 (2021).

[39] J. Joshi and T. S. Mahesh, arXiv:2112.15437 (2021), 10.48550/ARXIV.2112.15437.

[40] C. Cruz, M. F. Anka, M. S. Reis, R. Bachelard, and A. C. Santos, Quantum Sci. Technol. **7**, 025020 (2022).

[41] A. E. Allahverdyan, R. Balian, and T. M. Nieuwenhuizen, EPL **67**, 565 (2004).

[42] W. Pusz and S. L. Woronowicz, Commun. Math. Phys **58**, 273 (1978).

[43] A. Lenard, J. Stat. Phys **19**, 575 (1978).

[44] H. J. Kimble, Nature **453**, 1023 (2008).

[45] S. Wehner, D. Elkouss, and R. Hanson, Science **362**, 303 (2018).

[46] A. S. Sørensen and K. Mølmer, Phys. Rev. Lett. **86**, 4431 (2001).

[47] G. Francica, Phys. Rev. E **105**, L052101 (2022).

An Optimal Oracle Separation of Classical and Quantum Hybrid Schemes

Atsuya Hasegawa[1] * François Le Gall[2] †

[1] *Graduate School of Information Science and Technology, The University of Tokyo, Japan*
[2] *Graduate School of Mathematics, Nagoya University, Japan*

Abstract. Recently, Chia, Chung and Lai (JACM 2023) and Coudron and Menda (STOC 2020) have shown that there exists an oracle $\mathcal{O}$ such that $\mathsf{BQP}^{\mathcal{O}} \neq (\mathsf{BPP}^{\mathsf{BQNC}})^{\mathcal{O}} \cup (\mathsf{BQNC}^{\mathsf{BPP}})^{\mathcal{O}}$. In fact, Chia et al. proved a stronger statement: for any depth parameter d, there exists an oracle that separates quantum depth d and $2d+1$, when polynomial-time classical computation is allowed. This implies that relative to an oracle, doubling quantum depth gives classical and quantum hybrid schemes more computational power.

In this paper, we show that for any depth parameter d, there exists an oracle that separates quantum depth d and $d+1$, when polynomial-time classical computation is allowed. This gives an optimal oracle separation of classical and quantum hybrid schemes. To prove our result, we consider d-Bijective Shuffling Simon's Problem (which is a variant of d-Shuffling Simon's Problem considered by Chia et al.) and an oracle inspired by an "in-place" permutation oracle.

Keywords: small-depth quantum circuit, hybrid quantum computer, oracle separation

1 Introduction

Background. In recent years, the development of quantum computers has been very active (see, e.g., [1] for information about current quantum computers) and "quantum supremacy" has been claimed [8, 20]. However, it is still difficult to implement large-depth quantum circuits with current quantum technology since such quantum devices are subjective to noise and have short coherent time. One potential way to extract the computational powers of such quantum devices is to consider a hybrid scheme combining them with classical computers. For example, variational quantum algorithms are considered in such a scheme to obtain quantum advantage (see [9] for a survey).

Therefore, understanding the capabilities and limits of this hybrid approach is an essential topic in quantum computation. As one of the most notable results, Cleve and Watrous [13] showed the quantum Fourier transformation can be implemented by combining logarithmic-depth quantum circuits with a classical polynomial-time algorithm. With the possibility to implement Shor's algorithm in such a hybrid scheme and the developments of measurement-based quantum computation, Jozsa [17] conjectured that "Any quantum polynomial-time algorithm can be implemented with only $O(\log n)$ quantum depth interspersed with polynomial-time algorithm classical computations". This can be formalized as $\mathsf{BQP} = \mathsf{BQNC}^{\mathsf{BPP}}$. On the other hand, Aaronson [3, 4, 5] conjectured "there exists an oracle separation between BQP and $\mathsf{BPP}^{\mathsf{BQNC}}$". $\mathsf{BPP}^{\mathsf{BQNC}}$ is a complexity class recognized by a polynomial classical scheme which has access to poly-logarithmic depth quantum circuits. $\mathsf{BQNC}^{\mathsf{BPP}}$ and $\mathsf{BPP}^{\mathsf{BQNC}}$ are sets of problems recognized by two natural and seemingly incomparable models of hybrid classical and quantum computation.

Recent works by Chia, Chung and Lai [10] and Coudron and Menda [14] proved Aaronson's conjecture and refuted Jozsa's conjecture in a relativized setting. Interestingly, computational problems and oracles they considered were completely different. Coudron and Menda [14] considered, as an oracle problem, the Welded Tree Problem which exhibits a difference between quantum walks and classical random walks: this problem can be solved efficiently by a quantum algorithm [12] but, in the classical setting, exponential queries are required [12, 16]. To prove a lower bound of classical and quantum hybrid schemes, Coudron and Menda introduced "Information Bottleneck" to simulate classical and quantum hybrid schemes with fewer classical queries. They showed if we assume the hybrid schemes solve the problem, we reach a contradiction with the lower bound of classical queries from [16].

Chia, Chung and Lai [10] considered d-Shuffling Simon's Problem, which is a variant of Simon's Problem [18]. Since Simon's Problem can be solved with a constant-depth quantum circuit with classical post-processing, we cannot prove the hardness for classical and quantum hybrid schemes. To devise a harder problem, they combine Simon's function with sequential random permutations: for a Simon's function f, they consider random one-to-one functions $f_0, ..., f_{d-1}$ and two-to-one function f_d such that $f = f_d \circ \cdots \circ f_0$. They also hide the domains of the functions in larger domains and apply the idea of the Oneway-to-Hiding (O2H) lemma [6, 19] to prove the hardness. In fact, they proved a stronger statement below.

Theorem 1 ([10]) *For any $d \in \mathbb{N}$, there exists an oracle $\mathcal{O}$ such that*

$$(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}} \cup (\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}} \neq (\mathsf{BQNC}_{2d+1}^{\mathsf{BPP}})^{\mathcal{O}} \cap (\mathsf{BPP}^{\mathsf{BQNC}_{2d+1}})^{\mathcal{O}}.$$

*atsuyahasegawa@is.s.u-tokyo.ac.jp
†legall@math.nagoya-u.ac.jp

Description of our result. In this paper, we improve Theorem 1 above and show the following result.

Theorem 2 *For any $d \in \mathbb{N}$, there exists an oracle $\mathcal{O}$ such that*

$$(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}} \cup (\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}} \neq (\mathsf{BQNC}_{d+1}^{\mathsf{BPP}})^{\mathcal{O}} \cap (\mathsf{BPP}^{\mathsf{BQNC}_{d+1}})^{\mathcal{O}}$$

Our result implies that, relative to an oracle, increasing the quantum depth even by *one* gives the hybrid schemes more computational power and it cannot be traded by combining polynomial-time classical processing.

In Theorem 2, quantum circuits consisting of any 1- and 2-qubit gates are considered. Indeed, we give an algorithm by $d+1$-depth quantum circuits consisting only of $\{H, CNOT\}$ with classical processing for the upper bound (this is also the case for Theorem 1 but not mentioned in [10]). Therefore we also prove that, even if we are allowed to use quantum circuits consisting of a restricted gate set contains $\{H, CNOT\}$ such as Clifford circuits, adding even one quantum depth gives the two hybrid schemes more computational power relative to an oracle.

Outline of our approach. Chia et al. gave the upper bound $(\mathsf{BQNC}_{2d+1}^{\mathsf{BPP}})^{\mathcal{O}} \cap (\mathsf{BPP}^{\mathsf{BQNC}_{2d+1}})^{\mathcal{O}}$ for d-Shuffling Simon's Problem by an algorithm inspired by the Simon's algorithm. Since they considered a standard oracle, $U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$, it is required to erase the information of past queries and it takes d-quantum depth. To eliminate the d-quantum depth, we propose an idea to consider an "in-place" permutation oracle [2, 15] acts as $U_f |x\rangle = |f(x)\rangle$. However, when f is a Simon's function, f_d on a restricted domain is also a two-to-one function and there is no unitary operator U_{f_d} such that $U_{f_d} |x\rangle = |f_d(x)\rangle$. Therefore, in this paper, we consider another function η and make the function bijective. We name the problem d-Bijective Shuffling Simon's Problem and show an upper bound $(\mathsf{BQNC}_{d+1}^{\mathsf{BPP}})^{\mathcal{O}} \cap (\mathsf{BPP}^{\mathsf{BQNC}_{d+1}})^{\mathcal{O}}$. The other obstacle is, for f_d and the shadows to prove the lower bounds, how to define a unitary operator that includes mappings to $\perp$ (a constant with no information). Note that this is because there exists no unitary operator $U_\perp$ such that $U_\perp |x\rangle = |\perp\rangle$. In this paper, we give a solution by keeping values on domains and considering "flags" on ancilla qubits. Finally we carefully tailor the Oneway-to-Hiding lemma in our quantum oracle setting and show that the similar proofs of the lower bounds also follow as [10].

The main contribution of our work is to define the d-Bijective Shuffling Simon's Problem and give the upper bound with quantum depth $d+1$. The proof of the lower bound is very similar to [10] except the Oneway-to-Hiding lemma, which has to be adapted to the quantum oracle of this paper. We are grateful to Nai-Hui Chia for discussions about this, and in particular for clarifying that all steps in the lower bound from [10] remain true for our new oracle as well, with the exception of this Oneway-to-Hiding lemma.

Related work. Arora, Gheorghiu and Singh [7] proved oracle separations of $(\mathsf{BQNC}_d^{\mathsf{BPP}})^{\mathcal{O}}$ and $(\mathsf{BPP}^{\mathsf{BQNC}_d})^{\mathcal{O}}$ with respect to each other. As corollaries, they obtained sharper separations than [10] for each scheme. For the quantum-classical scheme, they proved an oracle separation between quantum depth d and $d+1$ if the Hadamard measurements are allowed in every layer. In our result, we only need to measure qubits in the Hadamard basis in the last layer. For the classical-quantum scheme, they proved a separation between quantum depth d and $d+5$ relative to what they call a stochastic oracle (which is non-unitary). Our separation is between quantum depth d and $d+1$ relative to a unitary oracle.

In an independent work [11], Chia and Hung have also shown how to reduce the gap from d versus $2d+1$ to d versus $d+1$ by techniques similar to ours (they consider an oracle inspired by an "in-place" permutation oracle and manage to make the final function one-to-one). They also instantiate the oracle separation to construct a protocol such that a classical verifier can check if a prover has a quantum depth of at least $d+1$.

References

[1] `https://en.wikipedia.org/wiki/List_of_quantum_processors`.

[2] Scott Aaronson. Quantum lower bound for the collision problem. In *Proceedings of the 34th ACM Symposium on Theory of Computing (STOC 2002)*, pages 635–642, 2002.

[3] Scott Aaronson. Ten semi-grand challenges for quantum computing theory, 2005.

[4] Scott Aaronson. BQP and the polynomial hierarchy. In *Proceedings of the 42nd ACM Symposium on Theory of Computing (STOC 2010)*, pages 141–150, 2010.

[5] Scott Aaronson. Projects aplenty, 2011.

[6] Andris Ambainis, Mike Hamburg, and Dominique Unruh. Quantum security proofs using semi-classical oracles. In *Advances in Cryptology – CRYPTO 2019*, volume 11693 of *Lecture Notes in Computer Science*, pages 269–295. Springer, 2019.

[7] Atul Singh Arora, Alexandru Gheorghiu, and Uttam Singh. Oracle separations of hybrid quantum-classical circuits. *arXiv:2201.01904*, 2022.

[8] Frank Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[9] Marco Cerezo et al. Variational quantum algorithms. *Nature Reviews Physics*, 3(9):625–644, 2021.

[10] Nai-Hui Chia, Kai-Min Chung, and Ching-Yi Lai. On the Need for Large Quantum Depth. *Journal of the ACM*, 70(1):1–38, 2023.

[11] Nai-Hui Chia and Shih-Han Hung. Classical verification of quantum depth. *arXiv:2205.04656*, 2022.

[12] Andrew M Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A Spielman. Exponential algorithmic speedup by a quantum walk. In *Proceedings of the 35th ACM Symposium on Theory of Computing (STOC 2003)*, pages 59–68, 2003.

[13] Richard Cleve and John Watrous. Fast parallel circuits for the quantum Fourier transform. In *Proceedings 41st IEEE Annual Symposium on Foundations of Computer Science (FOCS 2000)*, pages 526–536, 2000.

[14] Matthew Coudron and Sanketh Menda. Computations with greater Quantum depth are strictly more powerful (relative to an oracle). In *Proceedings of the 52nd ACM Symposium on Theory of Computing (STOC 2020)*, pages 889–901, 2020.

[15] Bill Fefferman and Shelby Kimmel. Quantum vs. Classical Proofs and Subset Verification. In *Proceedings of 43rd International Symposium on Mathematical Foundations of Computer Science (MFCS 2018)*, pages 22:1–22:23, 2018.

[16] Stephen A Fenner and Yong Zhang. A note on the classical lower bound for a quantum walk algorithm. *arXiv:quant-ph/0312230*, 2003.

[17] Richard Jozsa. An introduction to measurement based quantum computation. *arXiv:quant-ph/0508124*, 2005.

[18] Daniel R. Simon. On the power of quantum computation. In *Proceedings of 35th IEEE Annual Symposium on Foundations of Computer Science (FOCS 1994)*, pages 116–123, 1994.

[19] Dominique Unruh. Revocable Quantum Timed-Release Encryption. *Journal of the ACM*, 62(6):1–76, 2015.

[20] Han-Sen Zhong et al. Quantum computational advantage using photons. *Science*, 370:1460–1463, 2020.

Quantum Search with Noisy Oracle

Ansis Rosmanis[1] *

[1] *Graduate School of Mathematics, Nagoya University*
Building B, Furocho, Chikusa Ward, Nagoya, Aichi, 464-0813, Japan

Abstract. We consider quantum search algorithms that have access to a noisy oracle that, for every oracle call, with probability $p > 0$ completely depolarizes the query registers, while otherwise working properly. Previous results had not ruled out quantum $\mathrm{O}(\sqrt{n})$-query algorithms in this setting, even for constant p. We show that for all $p \in [1/\sqrt{n}, 1 - \Omega(1)]$, the quantum noisy-query complexity of the unstructured search is $\Omega(np)$, which is tight up to logarithmic factors. The same bound holds for the dephasing noise and even when, for every oracle call, the algorithm is provided with a flag indicating whether the noise has occurred.

Keywords: query algorithms, noisy oracle, unstructured search

Extended Abstract

Unstructured search is one of the most studied computational tasks in quantum computing, in part due to Grover algorithm performing this task quadratically faster than any classical algorithm [Gro96]. Even before Grover presented his algorithm, Bennett, Bernstein, Brassard, and Vazirani showed that quadratic quantum speedups is the best one can hope for [BBBV97]. More formally, these works showed that finding a marked element among n elements has the bounded-error quantum query complexity $\Theta(\sqrt{n})$.

Since then, many subsequent works have shed more light on the problem. Zalka showed that quadratic speedups do not survive parallelization [Zal99]. In the same work, it was shown that Grover's algorithm is the very best algorithm for the problem and that not even constant additive gains can be made in quantum query complexity over it (see also [DH09] for an alternative proof). Recent works also investigated hybrid quantum-classical algorithm that can access the oracle both in a quantum, coherent manner as well as in a classical, non-coherent manner, and showed that sublinear number of classical queries cannot substantially speed up the quantum search [Ros22, HLS22]. Yet, multiple important questions regarding unstructured search remain open.

In this work we focus on search with faulty oracles. That is, we consider models of quantum query algorithms where the algorithm itself is faultless, but the interaction with the oracle can suffer from certain faults. Regev and Schiff [RS08] considered a scenario where the oracle is neglectful and, independently for each oracle call, with some constant probability p it forgets to apply the unitary query operator O_f, instead simply applying the identity operator I. Regev and Schiff showed that, in such a scenario, $\Omega(n)$ queries are required to perform search.

The faults of the neglectful oracle can be considered as a certain type of noise: since $I = O_f O_f^*$, we can think of O_f^* as the noise $\mathscr{N}$ that (with probability p) occurs after the faultless oracle call. This noise, O_f^*, is however arguably rather artificial and non-local. Instead, in this work, we consider dephasing and depolarizing noise. Here, after the faultless oracle call, independently for each oracle call, with probability p the query register gets projected to the computational basis (dephasing noise) or replaced by the maximally mixed state, effectively erasing the registers (depolarizing noise).

While these noise models are seemingly much harsher than the one considered by Regev and Schiff, for them, quadratic speedups by quantum algorithms were not ruled out even for constant p. The proof technique in [RS08] relied on the fact that, when there are no marked elements, one has $O_f^* = I$, and hence there are no faults and the overall computation remains pure. In the case of the dephasing noise, however, the overall state of the system will become mixed whenever we attempt to access the oracle in a superposition, and, in the case of the depolarizing noise, it will always become mixed.

Results. In this work we show that the dephasing and the depolarizing oracle faults indeed thwart quantum speedups. More precisely, we consider the model of quantum query algorithms where, after each oracle call, with probability $p > 0$ we apply noise $\mathscr{N}$, which is either the completely dephasing or the completely depolarizing channel, then the quantum query complexity of finding a marked element, assuming there exists one, has the query complexity query complexity $\Omega(np)$.

Theorem 1 *For noise probability $p > 0$, the ϵ-error quantum noisy-query complexity of the unstructured search is at least $np(1-\epsilon)/65 - 1$.*

When $p \geq 1/\sqrt{n}$, the lower bound $\Omega(np)$ is tight up to logarithmic factors [CCHL22] (for the completely depolarizing channel, additionally assuming $1 - p = \Omega(1)$). For $p = o(1/\sqrt{n})$, one expects to be able to run the entire Grover's algorithm before the first occurrence of the noise.

The lower bound holds even when for every oracle call the algorithm is provided with the flag bit indicating whether or not the noise occurred. Hence, this extra bit of information does not help the algorithm to overcome effects of noise. Let us note that, in the fault model considered by Regev and Schiff, having such an a bit would

*rosmanis@math.nagoya-u.ac.jp

restore the quadratic speedups achieved by Grover's algorithm.

Techniques. The aforementioned flag bit plays an additional role in our proof. Namely, because of it, it is sufficient to prove the result only for the dephasing noise. Indeed, if there were faster algorithms for the depolarizing noise, those algorithms could be transformed into algorithms for the dephasing noise of the same query complexity. In particular, whenever the flag bit received by the algorithm indicates that the dephasing noise has occurred, the algorithm can depolarize all query registers, in effect simulating the depolarizing noise.

The dephasing noise, in turn, has a close connection to the classical oracle calls considered in works on hybrid quantum-classical search algorithms in [Ros22, HLS22]. Indeed, the faultless quantum oracle call followed by a completely dephasing noise is exactly the same as the classical oracle call considered in those works. The difference being that, unlike in the hybrid algorithm scenario, now the algorithm has no control over when this effectively-classical oracle call will happen, every oracle call being classical with probability p.

For the noisy oracle scenario considered in this work, proof techniques by Hamoudi, Liu, and Sinha [HLS22], which allow one to deal with mixed-state computation, are more useful than the ones in [Ros22], which stay closer to the approach in [RS08]. In addition to being inspired by techniques in [HLS22], we also draw inspiration from the quantum lower bound for search in [Ros21]. Both of these works, in turn, are inspired by Zhandry's compressed oracle approach [Zha19]. While [HLS22] builds upon [Zha19] by showing how to simultaneously handle both classical and quantum queries, [Ros21] shows how to avoid compression-decompression steps and thus allows handling scenarios where the output of the oracle on one input may depend on that on another input (as is the case when searching for a unique marked element).

Similarly to the adversary bound [Amb02] and many of its variants, we introduce the truth-table register, which contains the full description of the function f computed by the oracle. This register then controls actions of the oracle O_f. Furthermore, similarly to [HLS22], we also introduce what we call the "record" registers that purify the overall system. We then use the joint state of the truth-table and record registers, which are the registers not directly accessible by the algorithm, to define a certain metric that measures the progress of the computation. More precisely, similarly to [HLS22], we decompose the entire memory space (including that of the algorithm) into three parts as $\mathcal{H}^{\mathfrak{A}} \oplus \mathcal{H}^{\mathfrak{B}} \oplus \mathcal{H}^{\mathfrak{C}}$, where $\mathcal{H}^{\mathfrak{C}}$ essentially corresponds to the scenario where the classical oracle has succeeded (that is, the dephasing noise has collapsed the query input register to a marked input x), $\mathcal{H}^{\mathfrak{B}}$ corresponds to the space orthogonal to $\mathcal{H}^{\mathfrak{C}}$ where the quantum oracle has found a marked input, and $\mathcal{H}^{\mathfrak{A}}$ corresponds to the space where no substantial progress has been made. All three spaces are invariant under linear operations on the algorithm registers alone. Initially, all the probability weight is on the subspace $\mathcal{H}^{\mathfrak{A}}$, but, in order for the algorithm to succeed, this probability weight has to be transferred to $\mathcal{H}^{\mathfrak{B}} \oplus \mathcal{H}^{\mathfrak{C}}$.

Departing from previous proof techniques, now we have to go further and decompose the space $\mathcal{H}^{\mathfrak{B}}$ as $\mathcal{H}^{\mathfrak{B},act} \oplus \mathcal{H}^{\mathfrak{B},pas}$, where, this time, the "active" subspace $\mathcal{H}^{\mathfrak{B},act}$ and the "passive" subspace $\mathcal{H}^{\mathfrak{B},pas}$ are not invariant under linear operations on the algorithm registers. The active subspace $\mathcal{H}^{\mathfrak{B},act}$ is the subspace of $\mathcal{H}^{\mathfrak{B}}$ to which the probability weight from $\mathcal{H}^{\mathcal{A}}$ can be partially transferred, and the subspace which would be used by a noiseless execution of Grover's algorithm. Unfortunately, however, $\mathcal{H}^{\mathfrak{B},act}$ is also the subspace affected by the noise. On the other hand, the passive subspace $\mathcal{H}^{\mathfrak{B},pas}$ can be used to shield the quantum memory from noise, yet this shielding thwarts the progress of the computation. So, we show that, in this case, you can't have your cake and eat it too; namely, we show that you cannot simultaneously both progress the computation and avert its corruption by noise. As a result, we show the tight bound $\Omega(np)$ as given in Theorem 1.

Related work on noisy search. In a recent and independent work [CCHL22], Chen, Cotler, Huang, and Li formulated the computational class of noisy intermediate-scale quantum (NISQ) computation, where all qubits are affected by the depolarizing noise of rate p. Among other results, they showed that in such a scenario a noisy quantum algorithm cannot perform quantum search faster than in time $\tilde{\Theta}(np)$, also providing a matching upper bound. While their upper bound carries over to our model, our lower bound is stronger then theirs in various aspects. First, for us only the oracle registers and only just after oracle calls are affected by noise. Second, our results also work for the dephasing noise. Third, our lower bound applies even when the algorithm gets informed whenever the noise occurs. And, finally, we also get rid of logarithmic factors in the complexity.

Technical version. For technical details of the computational model and the proof of the main theorem, Theorem 1, refer to Appendices A–E.

References

[Amb02] Andris Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[CCHL22] Sitan Chen, Jordan Cotler, Hsin-Yuan Huang, and Jerry Li. The complexity of NISQ. arXiv:2210.07234 [quant-ph], 2022. https://arxiv.org/abs/2210.07234.

[DH09] Cătălin Dohotaru and Peter Høyer. Exact quantum lower bound for Grover's problem. *Quantum Information and Computation*, 9(5):533–540, 2009.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. of 28th ACM Symposium on Theory of Computing*, pages 212–219, 1996.

[HLS22] Yassine Hamoudi, Qipeng Liu, and Makrand Sinha. Quantum-classical tradeoffs in the random oracle model. arXiv:2211.12954 [quant-ph], 2022. https://arxiv.org/abs/2211.12954.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[Ros21] Ansis Rosmanis. Tight bounds for inverting permutations via compressed oracle arguments. arXiv:2103.08975 [quant-ph], 2021. https://arxiv.org/abs/2103.08975.

[Ros22] Ansis Rosmanis. Hybrid quantum-classical search algorithms. arXiv:2202.11443 [quant-ph], 2022. https://arxiv.org/abs/2202.11443.

[RS08] Oded Regev and Liron Schiff. Impossibility of a quantum speed-up with a faulty oracle. In *Automata, Languages and Programming*, pages 773–781. Springer Berlin Heidelberg, 2008.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[Zal99] Christof Zalka. Grover's quantum searching algorithm is optimal. *Phys. Rev. A*, 60:2746–2751, 1999.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In *Advances in Cryptology – CRYPTO 2019*, pages 239–268. Springer, 2019.

A Model of Computation

We assume that the reader is familiar with basic concepts of quantum computation. For introductory texts, see, for example [NC00, Wat18].

In this section we define query algorithms for a rather general computational problem, and we focus on unstructured search in Section B.

A.1 Quantum memory

The memory of a quantum algorithm is organized in registers. Each register is associated with some finite set S and a complex Euclidean space of dimension $|S|$, denoted $\mathbb{C}^S$. The standard basis of this space is some fixed orthonormal basis whose vectors are uniquely labeled by the elements of S, and we write it as $\{|s\rangle : s \in S\}$. The pure states of the register are denoted by (column) unit vectors in $\mathbb{C}^S$. A qubit is a register associated with the set $\{0,1\}$, and multiple qubits can be grouped together into a larger register. We will also occasionally associate a qubit with the set $\{\mathfrak{q},\mathfrak{c}\}$, where $\mathfrak{q} := 0$ and $\mathfrak{c} := 1$ are flags with $\mathfrak{c}$ indicating that the noise has occurred and thus the oracle call is classical in nature, and $\mathfrak{q}$ indicating no noise and the oracle call being quantum in nature.

We may also write a pure state $|\psi\rangle$ as its corresponding density operator $|\psi\rangle\langle\psi|$. The quantum memory can also be in a mixed-state, in which case its corresponding density operator is a convex combination over pure states $|\psi\rangle\langle\psi|$.

We use capital letters $\mathsf{A},\mathsf{Q},\mathsf{R},\mathsf{T},\mathsf{W}$ in sans serif font to denote registers, and we might add them as subscripts to operators to highlight on which registers these operators act.

The memory of a quantum algorithm typically consists of multiple registers, and the state of the entire memory is a density operator on the tensor product of the Euclidean spaces corresponding to each register. The evolution of quantum memory is governed by completely-positive trace-preserving (CPTP) maps, also known as quantum channels, an evolution governed by unitary operators being a special case. When an operator or a CPTP map acts as the identity on some registers, we typically omit those registers from the notation.

A.2 Oracle calls

Let us here introduce various forms of the quantum oracle and notation pertaining to it. Let $[n] := \{1,2,\ldots,n\}$ here and throughout the text.

We consider algorithms that have oracle access to a function $f\colon [n] \to \{0,1\}$. We call such algorithms *query algorithms*, and we refer to each oracle access to f by using terms an "oracle call" and a "query" interchangeably.

As we will discuss in more detail in Section A.3, the algorithm registers A will consist of the query register Q and the workspace register W. When considering oracles with flag qubits, each oracle call will grow the workspace register by a qubit.

Noiseless oracle. The oracle call acts on the *query* register $\mathsf{Q} = \mathsf{Q_i}\mathsf{Q_o}$, which is composed of two subregisters: the *query-input* register $\mathsf{Q_i}$ corresponding to the set $[n]$ and the *query-output* register $\mathsf{Q_o}$ corresponding to $\{0,1\}$.[1] The oracle call to f is the unitary

$$\begin{aligned} O_f &:= \sum_{x\in[n]}\sum_{y\in\{0,1\}} (-1)^{f(x)\cdot y}|x,y\rangle\langle x,y| \\ &= I_{2n} - 2\sum_{x\in f^{-1}(1)} |x,1\rangle\langle x,1|, \end{aligned}$$

[1] The query-input register and the query-output registers are also commonly referred to as, respectively, the index and the target register.

which is sometimes referred to as the *phase* oracle, as opposed to the *standard* oracle

$$O_f^{\text{std}} := \sum_{x\in[n]} \sum_{y\in\{0,1\}} |x, y \oplus f(x)\rangle\langle x, y|.$$

The two oracles are equivalent up to a basis change of the query-output register.[2] We denote the CPTP map corresponding to O_f by $\mathscr{O}_f$.

Noisy oracles. We will define noisy oracles as CPTP maps on the query register Q as the composition of the noiseless oracle call $\mathscr{O}_f$ followed by a probabilistic, non-unitary noise $\mathscr{N}_p$. For ρ a linear operator on Q, we define the *completely* depolarizing noise (of $\mathsf{Q_i Q_o}$) as the CPTP map

$$\mathscr{N}_1^{polar}\colon \rho \mapsto \operatorname{Tr}[\rho]\, I_{\mathsf{Q}}/(2n)$$

and the *completely* dephasing noise (of $\mathsf{Q_i}$) as the CPTP map

$$\mathscr{N}_1^{phase}\colon \rho \mapsto \sum_{x\in[n]} \big(|x\rangle\langle x| \otimes I_{\mathsf{Q_o}}\big)\rho\big(|x\rangle\langle x| \otimes I_{\mathsf{Q_o}}\big).$$

Note that we have chosen to define the completely dephasing noise so as not to affect the query-output register. This will turn out to be without loss of generality because we will have an access to the flag qubits indicating whether the noise has occurred and thus we will be able to purposely dephase $\mathsf{Q_o}$ whenever $\mathsf{Q_i}$ dephases.

We omit superscripts *polar* and *phase* from $\mathscr{N}_1$ when we make general statements addressing both types of noise or, starting Section A.3, when we only consider the dephasing noise. The subscript 1 in $\mathscr{N}_1$ indicates that the noise happens with probability 1. More generally, for both noise models and for a probability $p \in [0, 1]$, we define $\mathscr{N}_p := (1-p)\mathscr{I} + p\mathscr{N}_1$, where $\mathscr{I}$ is the identity map. That is, $\mathscr{N}_p$ as a CPTP map that maps ρ to $(1-p)\rho + p\mathscr{N}_1(\rho)$. We might drop the subscript p from $\mathscr{N}_p$ when it is clear from the context, especially when making informal statements.

We define the noisy oracle call as the CPTP map $\mathscr{N}_p \circ \mathscr{O}_f = \mathscr{O}_f \circ \mathscr{N}_p$, where $\circ$ denotes the composition of maps.

Oracles with flag bits. Let us now introduce noisy oracles that signal whether or not the noise has occurred. This signal is in a form of a *flag* (qu)bit that the oracle call adds to the workspace of the algorithm. After the oracle call, the algorithm is then permitted to do whatever it pleases with this additional qubit, including, to ignore it, as if it were not even received. We will refer to this new qubit register, which extends the workspace, as W_+. Hence, we can formalize *signaling probabilistic noise* as a CPTP map that maps from Q to QW_+ that acts on linear operators ρ on Q as

$$\widetilde{\mathscr{N}_p}\colon \rho \mapsto (1-p)\rho \otimes |\mathfrak{q}\rangle\langle\mathfrak{q}| + p\mathscr{N}_1(\rho) \otimes |\mathfrak{c}\rangle\langle\mathfrak{c}|.$$

[2] The basis choice for the query-output register could play a role when one talks about dephasing that qubit as the dephasing noise is basis-specific. However, in this work we already show the hardness of the case when the dephasing noise affects only the query-input register. That, together with flag qubits indicating the presence of noise, will also imply hardness for stronger noise models.

Consider a CPTP map $\mathscr{D}$ acting on QW_+ that first measures qubit W_+ with respect to basis $\{|\mathfrak{q}\rangle, |\mathfrak{c}\rangle\}$ and, if the measurement yields $\mathfrak{c}$, it then applies the completely depolarizing noise $\mathscr{N}_1^{polar}$ on Q. We have $\widetilde{\mathscr{N}_p^{polar}} = \mathscr{D} \circ \widetilde{\mathscr{N}_p^{phase}}$. Since the algorithm can implement $\mathscr{D}$ without any queries, any hardness results that we show for noise-signaling oracles with dephasing noise will carry over to oracles with depolarizing noise (see also footnote 2).

We define the noise-signaling noisy oracle call as the CPTP map from Q to QW_+ as the composition $\mathscr{O}_{f,p} := \widetilde{\mathscr{N}_p} \circ \mathscr{O}_f$. From now on, we will only consider the noise-signaling noisy oracle corresponding to the dephasing noise, and, for brevity, we will simply refer to it as the noisy oracle.

A.3 Quantum noisy-query algorithms

Now that we have introduced the oracle, let us formalize the query algorithm with noisy oracles, and describe its operation.

We divide the memory of the algorithm into two registers: one is the query register Q and the other is the *workspace* register W that we assume to consist of some number of qubits. As we have described above, every call to the noisy oracle $\mathscr{O}_{f,p}$ introduces an extra qubit, which we incorporate into the workspace register. We call the joint register $\mathsf{A} = \mathsf{QW}$ the *algorithm register* (or *registers*).

A quantum noisy-query algorithm is specified by four components: (1) the number of quantum queries, (2) the initial state of the algorithm, (3) input-independent unitary operators that govern the evolution of the quantum system between oracle calls, and (4) the final measurement. Let us describe these components in detail.

1. We denote the number of queries by τ and we enumerate oracle calls from 1 to τ.

2. Let initially the workspace register W consist of ℓ qubits, therefore the entire initial memory corresponds to a $2n2^{\ell}$-dimensional Euclidean space. The initial state of the algorithm is an input-independent pure state $|\psi^0\rangle$ in this space; the first oracle call is performed directly on this state.

3. Each noisy oracle call expands the workspace register by a qubit. The evolution between oracle calls and after the last call is given by input-independent unitary operators $U_1, \ldots, U_\tau$, where the dimension of U_t is $2n2^{\ell+t}$.

4. Given some finite set $\mathcal{A}$ of answers, the final measurement is given by a set $\{\Pi_a\colon a \in \mathcal{A}\}$, where each Π_a is an orthogonal projector of dimension $2n2^{\ell+\tau}$ and $\sum_a \Pi_a = I$.

The execution of the algorithm starts in the initial state $|\psi^0\rangle$, and then alternates between oracle calls and input-independent unitaries as follows. Iteratively, for $t = 1, 2, \ldots, \tau$, the algorithm first performs an oracle call $\mathscr{O}_{f,p}$, and then applies unitary U_t. Finally, the algorithm

performs the measurement according to $\{\Pi_a \colon a \in \mathcal{A}\}$, returning the measurement outcome a as an answer. We say that the algorithm is *successful* if a is a correct answer for f, and we say that it *fails* otherwise.

B Purifying the Computation

From now on, let us focus on the problem of unstructured search. Here we will introduce registers that will purify the overall computation, those extra registers being a part of the overall lower bound framework.

For a function $f \colon [n] \to \{0,1\}$, we call an input $x \in [n]$ *marked* if $f(x) = 1$. The goal of the unstructured search is, given an oracle access to f, to find a marked input x, assuming there exists one.

Intuitively, the hardest instances of the problem are functions f that have exactly one marked input, and we will only consider such functions. Namely, let $f_x \colon [n] \to \{0,1\}$ be the function for which x is the unique marked input, that is,

$$f_x(x') = \begin{cases} 1 & \text{if } x' = x, \\ 0 & \text{if } x' \in [n] \setminus \{x\}. \end{cases}$$

Note that the noiseless oracle corresponding to f_x is $O_{f_x} = I_{2n} - 2|x,1\rangle\langle x,1|$.

Let us consider a scenario where we are given a noisy oracle access to the function f_x being chosen uniformly at random from the set of functions $\mathcal{F} := \{f_1, \dots, f_n\}$. Our goal is to find x.

Without loss of generality, let the query-input register $\mathsf{Q_i}$ be also used by the algorithm to return the answer, and thus let $\{\Pi_x := |x\rangle\langle x| \colon x \in [n]\}$ be the final measurement. Hence, if $\rho_{x,t}$ is the final state of the computation with oracle access to f_x, then average success probability q_{succ} is given by

$$q_{succ} = \frac{1}{n} \sum_{x \in [n]} \mathrm{Tr}[(\Pi_x \otimes I_{\mathsf{Q_o W}})\rho_{x,t}].$$

B.1 Environment registers

The overall quantum system will consist of three sets of registers. In addition to the registers Q and W used by the algorithm, we introduce two additional registers, which we describe below.

Truth register. The *truth* register T corresponds to the set of functions $\mathcal{F}$. One can think of each its basis state $|f\rangle$ containing the full truth table of f.[3]

At the beginning of the computation, we initialize the register T as the uniform superposition $|u\rangle := \sum_{x \in [n]} |f_x\rangle/\sqrt{n}$, and we can think of this register as effectively purifying the random choice of $f_x \in \mathcal{F}$.

Record register. The *record* register R will start empty, then the subregister R_1 will be appended to it by the first oracle call, R_2 by the second oracle call, and so on. For every $t \in \{1, \dots, \tau\}$, the register R_t corresponds to the set $\mathfrak{R} := \{\perp, 1, 2, \dots, n\} = [n] \cup \{\perp\}$, where $\perp$ indicates the absence of noise in t-th oracle call,[4] while, $x \in [n]$ indicates that the dephasing has occurred and the query-input register has been dephased to the basis state $|x\rangle$. In effect, the register R_t will purify the action of non-unitary, noisy oracle call number t.

After t oracle calls, the register R corresponds to the set $\mathfrak{R}^t$, and we think about its contents as strings $R = r_1 r_2 \dots r_t$ of length t, which we call *records*. As per standard notation, let $\mathfrak{R}^* := \bigcup_t \mathfrak{R}^t$ be the set of all records.

For a record $R = r_1 \dots r_t \in \mathfrak{R}^*$, we say that an input $x \in [n]$ appears in R if $r_t = x$ for some t, and let $R_{\mathrm{in}} \subset [n]$ be the set of all inputs appearing in R; note that here we ignore the symbol $\perp$. Also note that, for $R \in \mathfrak{R}^t$, we have $|R_{\mathrm{in}}| \le t$. For conciseness, let $n_R := n - |R_{\mathrm{in}}| = |[n] \setminus R_{\mathrm{in}}|$, which will be approximately n because we will mostly consider $R \in \mathfrak{R}^t$ with $t \ll n$.

For a record $R = r_1 \dots r_t \in \mathfrak{R}^t$ and a symbol $r \in \mathfrak{R}$, let $R \wr r$ denote the record obtained by appending r to R. That is, $R \wr r = r_1 \dots r_t r \in \mathfrak{R}^{t+1}$. We have $(R \wr \perp)_{\mathrm{in}} = R_{\mathrm{in}}$ and $(R \wr x)_{\mathrm{in}} = R_{\mathrm{in}} \cup \{x\}$ for $x \in [n]$.

B.2 Extended oracles

We define the extended noisy oracle call as a linear isometry

$$O_p := \sum_{f_z \in \mathcal{F}} |f_z\rangle\langle f_z| \otimes \Big(\big(\sqrt{1-p} I_{\mathsf{Q_i}} \otimes |\mathfrak{q}, \perp\rangle + \sqrt{p} \sum_{x \in [n]} |x\rangle\langle x| \otimes |\mathfrak{c}, x\rangle \big) \otimes I_{\mathsf{Q_o}} \Big) O_{f_z},$$

where the states $|\mathfrak{q}, \perp\rangle$ and $|\mathfrak{c}, x\rangle$ are on registers $\mathsf{W}_+\mathsf{R}_t$. Here, the subscript of the register R_t indicates that we implicitly think of O_p as t-th oracle call. While O_p acts as the identity on earlier record subregisters $\mathsf{R}_1 \dots \mathsf{R}_{t-1}$, it is sometimes useful to reintroduce them—and thus the whole record register R—in the notation when expressing O_p. So, we can write t-th extended noisy oracle call as

$$O_p = \sum_{f_z \in \mathcal{F}} |f_z\rangle\langle f_z| \otimes \sum_{R \in \mathfrak{R}^t} \Big(\big(\sqrt{1-p} I_{\mathsf{Q_i}} \otimes |\mathfrak{q}, R \wr \perp\rangle\langle R| + \sqrt{p} \sum_{x \in [n]} |x\rangle\langle x| \otimes |\mathfrak{c}, R \wr x\rangle\langle R| \big) \otimes I_{\mathsf{Q_o}} \Big) O_{f_z},$$

It will be useful to separate the noiseless and the noisy components of O_p, and express it as $O_p = \sqrt{1-p} O_Q + \sqrt{p} O_C$, where

$$O_Q := O_0 = \sum_f |f\rangle\langle f| \otimes O_f \otimes |\mathfrak{q}, \perp\rangle,$$

$$O_C := O_1 = \sum_f |f\rangle\langle f| \otimes \sum_{x \in [n]} |x\rangle\langle x| \otimes \sum_{y \in \{0,1\}} (-1)^{f(x) \cdot y} |y\rangle\langle y| \otimes |\mathfrak{c}, x\rangle$$

[3] In similar lower bound techniques, this register is called the oracle register, the adversary register, and the function register.

[4] The state $|\perp\rangle$ corresponding to the label $\perp \in \mathfrak{R}$ is unrelated to an equally-denoted state in Zhandry's work on the compressed oracle [Zha19].

are linear isometries with orthogonal images. The latter one, O_C, exhibits close similarity to the classical oracle considered in works [Ros22, HLS22] on hybrid quantum-classical query algorithms, except that it permits the query-output register to remain in a superposition. For that reason, we may refer to O_C as the *classical oracle* and to O_Q as the *quantum oracle*.

B.3 Extended computation

Now let us consider how the algorithm extends to entire space of registers TAR, and describe its execution. The execution of the *extended algorithm* starts in the initial state $|\phi_0\rangle := |u\rangle \otimes |\psi^0\rangle$, which is also the state of the overall system just before the first oracle call. Recall that we start the computation with empty record. That is, initially, the register R corresponds to one-dimensional Euclidean space (i.e., zero qubits).

Then, similarly as before, the computation alternates between extended noisy oracle calls on TQR and input-independent unitaries on QW as follows. Iteratively, for $t = 1, 2, \ldots, \tau$, the algorithm first performs an oracle call O_p, and then applies unitary U_t. For $t \in \{1, \ldots, \tau - 1\}$, let $|\phi_t\rangle$ be the state of the overall system just before $(t+1)$-th oracle call and let $|\phi_\tau\rangle$ be the final state of the system. These states can be recursively expressed as $|\phi_t\rangle = U_t O_p |\phi_{t-1}\rangle$ for all $t \in \{1, \ldots, \tau\}$.

Finally, on state $|\phi_\tau\rangle$, the algorithm measures registers T and $\mathsf{Q_i}$, obtaining a function f_z and an input x, and the algorithm is successful if and only if x is a marked input for f_z, that is, $x = z$. Accordingly, let us define the projector on successful outcomes as $\Pi_{succ} := \sum_{x\in[n]} |f_x, x\rangle\langle f_x, x|$, which acts on registers $\mathsf{TQ_i}$. We have $q_{succ} = \|\Pi_{succ}|\phi_\tau\rangle\|^2$.

C Progress Measure

Let us decompose the whole joint space of registers TAR in three subspaces corresponding to the scenarios where, informally, 1) the query-input register has been dephased to a marked input, 2) the query-input register has not been dephased to the marked input, but the quantum oracle has found the marked input, and 3) no progress has been made. When considering queries, we will further decompose the second subspace.

C.1 Progress-defining subspaces

Let us consider the n-dimensional space corresponding to the register T, that is, the space spanned by $|f_x\rangle$. Recall the uniform superposition $|u\rangle = \sum_{x\in[n]} |f_x\rangle/\sqrt{n}$, and note that the initial state of the truth register is $|u\rangle$. Also recall the notation $n_R = n - |R_{\mathrm{in}}|$. Let us define the unit vector

$$|\psi_{R_{\mathrm{in}}}\rangle := \sum_{x\in[n]\setminus R_{\mathrm{in}}} |f_x\rangle/\sqrt{n_R},$$

for which we have

$$\langle f_x|\psi_{R_{\mathrm{in}}}\rangle = \begin{cases} 1/\sqrt{n_R} & \text{if } x \in [n] \setminus R_{\mathrm{in}}, \\ 0 & \text{if } x \in R_{\mathrm{in}}. \end{cases} \tag{1}$$

In turn, let us define projectors

$$\Pi_t^{\mathfrak{C}} := \sum_{R\in\mathfrak{R}^t} \sum_{z\in R_{\mathrm{in}}} |f_z\rangle\langle f_z| \otimes |R\rangle\langle R|,$$

$$\Pi_t^{\mathfrak{B}} := \sum_{R\in\mathfrak{R}^t} \Big(\sum_{z\in[n]\setminus R_{\mathrm{in}}} |f_z\rangle\langle f_z| - |\psi_{R_{\mathrm{in}}}\rangle\langle\psi_{R_{\mathrm{in}}}| \Big) \otimes |R\rangle\langle R|,$$

$$\Pi_t^{\mathfrak{A}} := \sum_{R\in\mathfrak{R}^t} |\psi_{R_{\mathrm{in}}}\rangle\langle\psi_{R_{\mathrm{in}}}| \otimes |R\rangle\langle R|$$

on registers TR, which act as the identity on the algorithm registers A. We denote the spaces corresponding to these projectors, that is, their images, by $\mathcal{H}_t^{\mathfrak{C}}, \mathcal{H}_t^{\mathfrak{B}}, \mathcal{H}_t^{\mathfrak{A}}$, respectively. We might drop the subscript t when it is clear from the context.

Similarly to [HLS22], we define the *progress measure* as

$$\Psi_t := \|\Pi_t^{\mathfrak{C}}|\phi_t\rangle\|^2 + 4\|\Pi_t^{\mathfrak{B}}|\phi_t\rangle\|^2,$$

which is essentially an upper bound on the provisional success probability of the algorithm after t oracle calls (see the second claim of Lemma 2). We elaborate on the choice for the scalar 4 in front of $\|\Pi_t^{\mathfrak{B}}|\phi_t\rangle\|^2$ in Remark 1.

C.2 Proof of main theorem

Here we state Lemma 2 and show how it easily leads to Theorem 1. Then, the rest of the paper is devoted to proving the lemma, its first two claims being relatively easy to show.

Lemma 2 *We have*

$$\Psi_0 = 0, \tag{2a}$$

$$q_{succ} \le \Psi_\tau + \frac{2}{n-\tau}, \tag{2b}$$

$$\Psi_{t+1} - \Psi_t \le \frac{64}{p(n-t-1)}. \tag{2c}$$

Proof. (Theorem 1 given Lemma 2). From Lemma 2, we see that the success probability q_{succ} is at most

$$\frac{2}{n-\tau} + \frac{64}{p}\sum_{t=1}^{\tau} \frac{1}{n-t} \le \frac{2}{n-\tau} + \frac{64\tau}{p(n-\tau)} = \frac{2p+64\tau}{p(n-\tau)}$$

Since we want the success probability to be at least $1-\epsilon$, we thus get

$$\tau \ge \frac{p(n(1-\epsilon)-2)}{64+p(1-\epsilon)} \ge \frac{pn(1-\epsilon)}{65} - 1.$$

□

Now it is left to prove Lemma 2. Its first claim is trivial, because initially the record is empty and for the empty record we have $|\psi_\emptyset\rangle = |u\rangle$, which is the initial state of the truth register.

Let us now prove the second claim of the lemma, while the proof of the final claim is much more involved, and we leave it to Sections D and E.

Proof. (The second claim of Lemma 2). To prove the second claim of Lemma 2, recall $\Pi_{succ} = \sum_{z\in[n]} |f_z\rangle\langle f_z| \otimes$

$|z\rangle\langle z|$. It can be easily seen that Π_{succ} commutes with both $\Pi_\tau^{\mathfrak{C}}$ and $\Pi_\tau^{\mathfrak{B}} + \Pi_\tau^{\mathfrak{A}}$ (see Claim 1 below), and hence

$$\begin{aligned} q_{succ} &= \|\Pi_{succ}\Pi_\tau^{\mathfrak{C}}|\phi_\tau\rangle\|^2 + \|\Pi_{succ}(\Pi_\tau^{\mathfrak{B}} + \Pi_\tau^{\mathfrak{A}})|\phi_\tau\rangle\|^2 \\ &\le \|\Pi_\tau^{\mathfrak{C}}|\phi_\tau\rangle\|^2 + \big(\|\Pi_\tau^{\mathfrak{B}}|\phi_\tau\rangle\| + \|\Pi_{succ}\Pi_\tau^{\mathfrak{A}}\|\big)^2 \\ &\le \|\Pi_\tau^{\mathfrak{C}}|\phi_\tau\rangle\|^2 + 2\|\Pi_\tau^{\mathfrak{B}}|\phi_\tau\rangle\|^2 + 2\|\Pi_{succ}\Pi_\tau^{\mathfrak{A}}\|^2 \\ &\le \Psi_\tau + 2\|\Pi_{succ}\Pi_\tau^{\mathfrak{A}}\|^2, \end{aligned}$$

where for the first inequality we have used $\|\Pi_{succ}\| = 1$ and $\||\phi_\tau\rangle\| = 1$. To conclude, we have

$$\|\Pi_{succ}\Pi_\tau^{\mathfrak{A}}\| = \max_{\substack{R\in\mathfrak{R}^\tau \\ z\in[n]}} \||f_z\rangle\langle f_z|\psi_{R_{\mathrm{in}}}\rangle\langle\psi_{R_{\mathrm{in}}}|\| = 1/\sqrt{n-\tau}.$$

□

D Transitions Among Progress-defining Subspaces

Here we first decompose $\mathcal{H}_t^{\mathfrak{B}}$ as $\mathcal{H}_t^{\mathfrak{B},act} \oplus \mathcal{H}_t^{\mathfrak{B},pas}$, and then we provide various claims that will serve as basis of proving Lemma 2.

D.1 Active and passive intermediate subspaces

It is important to note that the progress measure Ψ_t is not affected by any operations on the algorithm registers alone, in particular, unitaries U_t. That is because $\Pi_t^{\mathfrak{C}}$, $\Pi_t^{\mathfrak{B}}$, $\Pi_t^{\mathfrak{A}}$ all act as the identity on the algorithm registers. However, when analyzing how Ψ_t evolves under oracle calls, it is useful to decompose $\Pi_t^{\mathfrak{B}}$ further, this decomposition involving query input register as well.

For $R \in \mathfrak{R}^*$ and $x \in [n] \setminus R_{\mathrm{in}}$, let us define the approximation of $|f_x\rangle$ with respect to R as the unit vector

$$\begin{aligned} |\tilde{f}_{x,R}\rangle &:= \sqrt{\frac{n_R - 1}{n_R}}|f_x\rangle - \frac{1}{\sqrt{n_R(n_R-1)}} \sum_{\substack{x'\in[n]\setminus R_{\mathrm{in}} \\ x'\neq x}} |f_{x'}\rangle \\ &= \frac{\sqrt{n_R}|f_x\rangle - |\psi_{R_{\mathrm{in}}}\rangle}{\sqrt{n_R - 1}}. \end{aligned}$$

We note that $\langle\psi_{R_{\mathrm{in}}}|\tilde{f}_{x,R}\rangle = 0$. Also note that $|\tilde{f}_{x,R}\rangle$ is the same for all R with the same R_{in}.

For every t, let us decompose

$$\Pi_{\mathsf{TR}}^{\mathfrak{B}} \otimes I_{\mathsf{Q_i}} = \Pi_{\mathsf{TRQ_i}}^{\mathfrak{B},act} + \Pi_{\mathsf{FEQ_i}}^{\mathfrak{B},pas},$$

where

$$\Pi_t^{\mathfrak{B},act} := \sum_{R\in\mathfrak{R}_0^t} \sum_{x\in[n]\setminus R_{\mathrm{in}}} |\tilde{f}_{x,R}, R, x\rangle\langle\tilde{f}_{x,R}, R, x|.$$

We call the subspace $\mathcal{H}_t^{\mathfrak{B},act}$ corresponding to $\Pi_t^{\mathfrak{B},act}$ the *active subspace* and the subspace $\mathcal{H}_t^{\mathfrak{B},pas}$ corresponding to $\Pi_t^{\mathfrak{B},pas}$ the *passive subspace*.

D.2 Non-alterability of the record

Claim 1 *$\Pi^{\mathfrak{C}}$ and $\Pi^{\mathfrak{B}} + \Pi^{\mathfrak{A}}$ both commute with $|f_z\rangle\langle f_z|$ for every z. Moreover, $O_Q\Pi_t^{\mathfrak{C}} = \Pi_{t+1}^{\mathfrak{C}}O_Q$. We also have that the images of $\Pi_{t+1}^{\mathfrak{C}}O_C\Pi_t^{\mathfrak{C}}$ and $\Pi_{t+1}^{\mathfrak{C}}O_C(\Pi_t^{\mathfrak{B}} + \Pi_t^{\mathfrak{A}})$ are orthogonal. We also have $O_p\Pi_t^{\mathfrak{C}} = \Pi_{t+1}^{\mathfrak{C}}O_p\Pi_t^{\mathfrak{C}}$.*

Proof. By direct inspection, $\Pi^{\mathfrak{C}}$ clearly commutes with $|f_z\rangle\langle f_z|$, and thus so does $I - \Pi^{\mathfrak{C}} = \Pi^{\mathfrak{B}} + \Pi^{\mathfrak{A}}$. Since O_Q appends $\perp$ to the record, yet $R_{\mathrm{in}} = (R \wr \perp)_{\mathrm{in}}$, we have

$$\begin{aligned} O_Q\Pi_t^{\mathfrak{C}} &= \sum_{R\in\mathfrak{R}^t}\sum_{z\in R_{\mathrm{in}}} O_Q\big(|f_z\rangle\langle f_z| \otimes |R\rangle\langle R|\big) \\ &= \sum_{R\in\mathfrak{R}^t}\sum_{z\in R_{\mathrm{in}}} |f_z\rangle\langle f_z| \otimes O_{f_z} \otimes |\mathfrak{q}, R\wr\perp\rangle\langle R| \\ &= \sum_{\substack{R'\in\mathfrak{R}^{t+1} \\ R'_{t+1}=\perp}}\sum_{z\in R'_{\mathrm{in}}} O_Q\big(|f_z\rangle\langle f_z| \otimes |R'\rangle\langle R'|\big)O_Q \\ &= \Pi_{t+1}^{\mathfrak{C}}O_Q. \end{aligned}$$

where we have used that $\langle R'|O_Q = 0$ whenever the last entry of the record R' is not $\perp$.

If we look at the truth T and the record R registers of the image of $\Pi_t^{\mathfrak{B}} + \Pi_t^{\mathfrak{A}}$, it is spanned by vectors in form $|f_z, R\rangle$, where $R \in \mathfrak{R}^t$ and $z \in [n] \setminus R_{\mathrm{in}}$. Hence, the image of $\Pi_{t+1}^{\mathfrak{C}}O_C(\Pi_t^{\mathfrak{B}} + \Pi_t^{\mathfrak{A}})$ restricted to those registers is spanned by vectors form $|f_z, R\wr z\rangle$ where $R \in \mathfrak{R}^t$ and $z \in [n]\setminus R_{\mathrm{in}}$. On the other hand, the image of $\Pi_t^{\mathfrak{C}}$ restricted to TR is spanned by vectors in form $|f_z, R\rangle$, where $R \in \mathfrak{R}^t$ and $z \in R_{\mathrm{in}}$. Hence, the image of $\Pi_{t+1}^{\mathfrak{C}}O_C\Pi_t^{\mathfrak{C}}$ restricted to TR is spanned by vectors in form $|f_z, R\wr x\rangle$ where $R \in \mathfrak{R}^t$, $z \in R_{\mathrm{in}}$, and $x \in [n]$.

Because $|f_z\rangle\langle f_z|$ commutes with O_C and because the oracle appends some symbol $r \in \mathfrak{R}$ to the record, we have

$$\begin{aligned} O_C\Pi_t^{\mathfrak{C}} &= \sum_{R\in\mathfrak{R}^t}\sum_{z\in R_{\mathrm{in}}} O_C\big(|f_z\rangle\langle f_z| \otimes |R\rangle\langle R|\big) \\ &= \sum_{R\in\mathfrak{R}^t}\sum_{z\in R_{\mathrm{in}}}\sum_{r\in\mathfrak{R}} \big(|f_z\rangle\langle f_z| \otimes |R\wr r\rangle\langle R\wr r|\big) \\ &\qquad O_C\big(|f_z\rangle\langle f_z| \otimes |R\rangle\langle R|\big). \end{aligned}$$

For every $x \in [n]$, we clearly have $(R\wr x)_{\mathrm{in}} = R_{\mathrm{in}} \cup \{x\} \supseteq R_{\mathrm{in}}$. Thus, for $R \in \mathfrak{R}^t$, $z \in R_{\mathrm{in}}$, and $x \in [n]$, we have

$$\Pi_{t+1}^{\mathfrak{C}}\big(|f_z\rangle\langle f_z| \otimes |R\wr x\rangle\langle R\wr x|\big) = |f_z\rangle\langle f_z| \otimes |R\wr x\rangle\langle R\wr x|$$

concluding the proof. □

D.3 The action of O_Q and O_C on the active subspace

Claim 2 *We have $\Pi_{t+1}^{\mathfrak{B}}O_Q\Pi_t^{\mathfrak{B},act} = \Pi_{t+1}^{\mathfrak{B},act}O_Q\Pi_t^{\mathfrak{B},act}$ and $\Pi_{t+1}^{\mathfrak{B}}O_Q\Pi_t^{\mathfrak{B},pas} = \Pi_{t+1}^{\mathfrak{B},pas}O_Q\Pi_t^{\mathfrak{B},pas}$. We have $O_C\Pi_t^{\mathfrak{B},act} = (\Pi_{t+1}^{\mathfrak{C}} + \Pi_{t+1}^{\mathfrak{A}})O_C\Pi_t^{\mathfrak{B},act}$.*

Proof. The space $\mathcal{H}_t^{\mathfrak{B},act}$ is spanned by vectors in form $|\tilde{f}_{x,R}, x, y, R\rangle$ (here we ignore the content of workspace registers), on which the oracle O_Q acts as $O_Q|\tilde{f}_{x,R}, x, 0, R\rangle = |\tilde{f}_{x,R}, x, 0, R\rangle$, and

$$\begin{aligned} &O_Q|\tilde{f}_{x,R}, x, 1, R\rangle \\ &= \Big(-\sqrt{\frac{n_R-1}{n_R}}|f_x\rangle - \frac{1}{\sqrt{n_R(n_R-1)}}\sum_{\substack{x'\in[n]\setminus R_{\mathrm{in}} \\ x'\neq x}}|f_{x'}\rangle\Big) \\ &\qquad\qquad |x, 1, R\wr\perp, \mathfrak{q}\rangle \\ &= \Big(-\frac{n_R-2}{n_R}|\tilde{f}_{x,R}\rangle - \frac{2\sqrt{n_R-1}}{n_R}|\psi_{R_{\mathrm{in}}}\rangle\Big)|x, 1, R\wr\perp, \mathfrak{q}\rangle. \end{aligned}$$

Opening the parenthesis, the former vector is in $\mathcal{H}^{\mathfrak{B},act}_{t+1}$ while the latter is in $\mathcal{H}^{\mathfrak{A}}_{t+1}$. This shows that $\Pi^{\mathfrak{B}}_{t+1}O_Q\Pi^{\mathfrak{B},act}_t = \Pi^{\mathfrak{B},act}_{t+1}O_Q\Pi^{\mathfrak{B},act}_t$.

Note that O_Q is essentially its own inverse (aside from it adding $|\perp\rangle$ to the record and $|\mathfrak{q}\rangle$ to the workspace). So, for $|\zeta_{t+1}\rangle$ the state right after tth oracle call, we have $\langle\zeta_{t+1}|O_Q = 0$ whenever the last flag subregister W_+ is not $\langle\mathfrak{q}|$ or the last record subregister R_{t+1} is not $\langle\perp|$. If they are, however, similarly as above, we get

$$\begin{aligned}
&\langle\tilde{f}_{x,R},x,0,R\wr\perp,\mathfrak{q}|O_Q = \langle\tilde{f}_{x,R},x,0,R|,\\
&\langle\tilde{f}_{x,R},x,1,R\wr\perp,\mathfrak{q}|O_Q\\
&\quad= \Big(-\frac{n_R-2}{n_R}\langle\tilde{f}_{x,R}| - \frac{2\sqrt{n_R-1}}{n_R}\langle\psi_R|\Big)\langle x,1,R|.
\end{aligned}$$

Hence, we also have $\Pi^{\mathfrak{B},act}_{t+1}O_Q\Pi^{\mathfrak{B}}_t = \Pi^{\mathfrak{B},act}_{t+1}O_Q\Pi^{\mathfrak{B},act}_t$, which means that $\Pi^{\mathfrak{B}}_{t+1}O_Q\Pi^{\mathfrak{B},pas}_t = \Pi^{\mathfrak{B},pas}_{t+1}O_Q\Pi^{\mathfrak{B},pas}_t$.

Now, let us consider $O_C\Pi^{\mathfrak{B},act}_t$. For $R\in\mathfrak{R}^*$ and $x\in[n]\setminus R_{\mathrm{in}}$. We have

$$\begin{aligned}
&O_C|\tilde{f}_{x,R},x,y,R\rangle\\
&=\sqrt{\frac{n_R-1}{n_R}}O_C|f_x,x,y,R\rangle\\
&\qquad\qquad-\frac{1}{\sqrt{n_R(n_R-1)}}\sum_{\substack{x'\in[n]\setminus R_{\mathrm{in}}\\x'\neq x}}O_C|f_{x'},x,y,R\rangle\\
&=(-1)^y\sqrt{\frac{n_R-1}{n_R}}|f_x,x,y,R\wr x\rangle\\
&\qquad\qquad-\frac{1}{\sqrt{n_R(n_R-1)}}\sum_{\substack{x'\in[n]\setminus R_{\mathrm{in}}\\x'\neq x}}|f_{x'},x,y,R\wr x\rangle\\
&=(-1)^y\sqrt{\frac{n_R-1}{n_R}}|f_x,x,y,R\wr x\rangle\\
&\qquad\qquad-\frac{1}{\sqrt{n_R}}|\psi_{(R\wr x)_{\mathrm{in}}}\rangle|x,y,R\wr x\rangle.
\end{aligned}$$

The former vector is in $\mathcal{H}^{\mathfrak{C}}_{t+1}$, while the latter is in $\mathcal{H}^{\mathfrak{A}}_{t+1}$. □

D.4 Escaping the no-progress subspace

Claim 3 *We have* $\Pi^{\mathfrak{B}}_{t+1}O_Q\Pi^{\mathfrak{A}}_t = \Pi^{\mathfrak{B},act}_{t+1}O_Q\Pi^{\mathfrak{A}}_t$, *and its norm is* $2\frac{\sqrt{n-t-1}}{n-t}$.

Proof. We can see that

$$\begin{aligned}
&\Pi^{\mathfrak{B}}_{t+1}O_Q\Pi^{\mathfrak{A}}_t\\
&=\Big(\sum_{R'\in\mathfrak{R}^{t+1}}\Big(\sum_{z\in[n]\setminus R'_{\mathrm{in}}}|f_z\rangle\langle f_z| - |\psi_{R'_{\mathrm{in}}}\rangle\langle\psi_{R'_{\mathrm{in}}}|\Big)\otimes|R'\rangle\langle R'|\Big)\\
&\qquad\cdot\Big(\Big(I_{\mathsf{TQ}}-2\sum_{x\in[n]}|f_x,x,1\rangle\langle f_x,x,1|\Big)\otimes|\mathfrak{q},\perp\rangle\Big)\\
&\qquad\cdot\Big(\sum_{R\in\mathfrak{R}^t}|\psi_{R_{\mathrm{in}}}\rangle\langle\psi_{R_{\mathrm{in}}}|\otimes|R\rangle\langle R|\Big)\\
&=-2\sum_{R\in\mathfrak{R}^t}\sum_{x\in[n]}\Big(\Big(\sum_{z\in[n]\setminus R_{\mathrm{in}}}|f_z\rangle\langle f_z| - |\psi_{R_{\mathrm{in}}}\rangle\langle\psi_{R_{\mathrm{in}}}|\Big)\\
&\qquad\qquad|f_x\rangle\langle f_x||\psi_{R_{\mathrm{in}}}\rangle\langle\psi_{R_{\mathrm{in}}}|\Big)\\
&\qquad\qquad\otimes|x,1\rangle\langle x,1|\otimes|\mathfrak{q}\rangle\otimes|R\wr\perp\rangle\langle R|,
\end{aligned}$$

where we have used $(R\wr\perp)_{\mathrm{in}} = R_{\mathrm{in}}$. Because of (1), we have

$$\begin{aligned}
&\Pi^{\mathfrak{B}}_{t+1}O_Q\Pi^{\mathfrak{A}}_t\\
&=-2\sum_{R\in\mathfrak{R}^t}\sum_{x\in[n]\setminus R_{\mathrm{in}}}\frac{|f_x\rangle-|\psi_{R_{\mathrm{in}}}\rangle/\sqrt{n_R}}{\sqrt{n_R}}\langle\psi_{R_{\mathrm{in}}}|\\
&\qquad\qquad\otimes|x,1\rangle\langle x,1|\otimes|\mathfrak{q}\rangle\otimes|R\wr\perp\rangle\langle R|\\
&=-2\sum_{R\in\mathfrak{R}^t}\sum_{x\in[n]\setminus R_{\mathrm{in}}}\frac{\sqrt{n_R-1}|\tilde{f}_{x,R}\rangle}{n_R}\langle\psi_{R_{\mathrm{in}}}|\\
&\qquad\qquad\otimes|x,1\rangle\langle x,1|\otimes|\mathfrak{q}\rangle\otimes|R\wr\perp\rangle\langle R|,
\end{aligned}$$

whose image is in $\mathcal{H}^{\mathfrak{B},act}_{t+1}$. Since the terms corresponding to distinct x and R are orthogonal,

$$\|\Pi^{\mathfrak{B}}_{t+1}O_Q\Pi^{\mathfrak{A}}_t\| = \max_{R\in\mathfrak{R}^t}2\frac{\sqrt{n_R-1}}{n_R} = 2\frac{\sqrt{n-t-1}}{n-t}.$$

□

Claim 4 *We have* $\Pi^{\mathfrak{B}}_{t+1}O_C\Pi^{\mathfrak{A}}_t = 0$ *and* $\|\Pi^{\mathfrak{C}}_{t+1}O_C\Pi^{\mathfrak{A}}_t\|^2 = 1/(n-t)$.

Proof. We can write $O_C\Pi^{\mathfrak{A}}_t$ as the summation

$$\begin{aligned}
O_C\Pi^{\mathfrak{A}}_t =&\Big(\sum_{\substack{x,z\in[n]\\y\in\{0,1\}}}(-1)^{y\cdot\delta_{x,y}}|f_z,x,y\rangle\langle f_z,x,y|\otimes|x\rangle\otimes|\mathfrak{c}\rangle\Big)\\
&\qquad\Big(\sum_{R\in\mathfrak{R}^t}|\psi_{R_{\mathrm{in}}}\rangle\langle\psi_{R_{\mathrm{in}}}|\otimes|R\rangle\langle R|\Big)\\
=&M'+M''
\end{aligned}$$

where M' corresponds to all terms in the summation such that $z\neq x$, and M'' to those with $z=x$. For both, we use (1) to evaluate $\langle f_x|\psi_{R_{\mathrm{in}}}\rangle$, and let $I_{\mathsf{Q}_\circ} = |0\rangle\langle 0|+|1\rangle\langle 1|$

and $Z_{\mathsf{Q}_\circ} = |0\rangle\langle 0| - |1\rangle\langle 1|$ below. We have,

$$\begin{aligned} M' = &\sum_{R\in\mathfrak{R}^t} \sum_{z\in[n]\setminus R_{\text{in}}} \sum_{\substack{x\in[n]\\ x\neq z}} \frac{|f_z\rangle\langle\psi_{R_{\text{in}}}|}{\sqrt{n_R}} \otimes |R\wr x\rangle\langle R| \\ &\otimes |x\rangle\langle x| \otimes I_{\mathsf{Q}_\circ} \otimes |\mathfrak{c}\rangle \\ = &\sum_{R\in\mathfrak{R}^t} \sum_{x\in[n]} \Bigg(\sum_{\substack{z\in[n]\setminus R_{\text{in}}\\ z\neq x}} \frac{|f_z\rangle}{\sqrt{n_R}} |R\wr x\rangle \Bigg) \langle\psi_{R_{\text{in}}}|\langle R| \\ &\otimes |x\rangle\langle x| \otimes I_{\mathsf{Q}_\circ} \otimes |\mathfrak{c}\rangle \\ = &\sum_{R\in\mathfrak{R}^t} \sum_{x\in[n]} \left(\sqrt{\frac{n_{R\wr x}}{n_R}} |\psi_{(R\wr x)_{\text{in}}}\rangle |R\wr x\rangle \right) \langle\psi_{R_{\text{in}}}|\langle R| \\ &\otimes |x\rangle\langle x| \otimes I_{\mathsf{Q}_\circ} \otimes |\mathfrak{c}\rangle, \end{aligned}$$

whose image is in $\mathcal{H}^{\mathfrak{A}}_{t+1}$. We have

$$\begin{aligned} M'' = &\sum_{R\in\mathfrak{R}^t} \sum_{z\in[n]\setminus R_{\text{in}}} \frac{|f_z\rangle\langle\psi_{R_{\text{in}}}|}{\sqrt{n_R}} \otimes |R\wr z\rangle\langle R| \\ &\otimes |z\rangle\langle z| \otimes Z_{\mathsf{Q}_\circ} \otimes |\mathfrak{c}\rangle, \end{aligned}$$

whose image is in $\mathcal{H}^{\mathfrak{C}}_{t+1}$. Since the terms corresponding to distinct z and R are orthogonal, $\|M''\| = \max_{R\in\mathfrak{R}^t} 1/\sqrt{n_R} = 1/\sqrt{n-t}$. □

E Bounding Increase in Progress

Now we combine Claims 1–4 to show the following lemma, which bounds the size of overlaps on spaces $\mathcal{H}^{\mathfrak{B}}_{t+1}$ and $\mathcal{H}^{\mathfrak{C}}_{t+1}$ after the quantum and the classical oracle calls, given the size of overlaps on $\mathcal{H}^{\mathfrak{B},act}_t$, $\mathcal{H}^{\mathfrak{B},pas}_t$, and $\mathcal{H}^{\mathfrak{C}}_t$ before those oracle calls. We then use this lemma to conclude the proof of Lemma 2.

Lemma 3 *Let $|\phi\rangle := |\phi_t\rangle$ be the state of the whole system just before $(t+1)$th oracle call. We have*

$$\|\Pi^{\mathfrak{B}}_{t+1} O_Q |\phi\rangle\|^2 \le \left(\|\Pi^{\mathfrak{B},act}_t |\phi\rangle\| + \frac{2}{\sqrt{n-t-1}} \right)^2 + \|\Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2, \tag{3a}$$

$$\|\Pi^{\mathfrak{B}}_{t+1} O_C |\phi\rangle\|^2 \le \|\Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2 - \|\Pi^{\mathfrak{C}}_{t+1} O_C \Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2, \tag{3b}$$

$$\|\Pi^{\mathfrak{C}}_{t+1} O_Q |\phi\rangle\|^2 = \|\Pi^{\mathfrak{C}}_t |\phi\rangle\|^2, \tag{3c}$$

$$\|\Pi^{\mathfrak{C}}_{t+1} O_C |\phi\rangle\|^2 \le \|\Pi^{\mathfrak{C}}_t |\phi\rangle\|^2 + 3\|\Pi^{\mathfrak{B},act}_t |\phi\rangle\|^2 + 3\|\Pi^{\mathfrak{C}}_{t+1} O_C \Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2 + \frac{3}{n-t-1}. \tag{3d}$$

Proof. Towards (3a), first note that $\Pi^{\mathfrak{B}}_{t+1} O_Q \Pi^{\mathfrak{C}}_t = 0$ due to Claim 1. Then, by Claims 2 and 3, we have

$$\Pi^{\mathfrak{B}}_{t+1} O_Q = \Pi^{\mathfrak{B},act}_{t+1} O_Q \Pi^{\mathfrak{B},act}_t + \Pi^{\mathfrak{B},pas}_{t+1} O_Q \Pi^{\mathfrak{B},pas}_t + \Pi^{\mathfrak{B},act}_{t+1} O_Q \Pi^{\mathfrak{A}}_t.$$

Because $\Pi^{\mathfrak{B},act}_{t+1}$ and $\Pi^{\mathfrak{B},pas}_{t+1}$ have orthogonal images, we therefore have

$$\begin{aligned} \|\Pi^{\mathfrak{B}}_{t+1} O_Q |\phi\rangle\|^2 =& \|\Pi^{\mathfrak{B},act}_{t+1} O_Q \Pi^{\mathfrak{B},act}_t |\phi\rangle + \Pi^{\mathfrak{B},act}_{t+1} O_Q \Pi^{\mathfrak{A}}_t |\phi\rangle\|^2 \\ &+ \|\Pi^{\mathfrak{B},pas}_{t+1} O_Q \Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2 \\ \le& \left(\|\Pi^{\mathfrak{B},act}_t |\phi\rangle\| + \|\Pi^{\mathfrak{B},act}_{t+1} O_Q \Pi^{\mathfrak{A}}_t |\phi\rangle\| \right)^2 \\ &+ \|\Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2, \end{aligned}$$

and the inequality (3a) follows due to $\|\Pi^{\mathfrak{B},act}_{t+1} O_Q \Pi^{\mathfrak{A}}_t\| < \frac{2}{\sqrt{n-t-1}}$, as given by Claim 3.

Towards (3b), we have $\Pi^{\mathfrak{B}}_{t+1} O_C \Pi^{\mathfrak{C}}_t = 0$ by Claim 1, $\Pi^{\mathfrak{B}}_{t+1} O_C \Pi^{\mathfrak{B},act}_t = 0$ by Claim 2, and $\Pi^{\mathfrak{B}}_{t+1} O_C \Pi^{\mathfrak{A}}_t = 0$ by Claim 4. Hence, $\Pi^{\mathfrak{B}}_{t+1} O_C = \Pi^{\mathfrak{B}}_{t+1} O_C \Pi^{\mathfrak{B},pas}_t$, and the inequality (3b) follows from

$$\begin{aligned} &\|\Pi^{\mathfrak{B}}_{t+1} O_C \Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2 \\ &= \|(\Pi^{\mathfrak{C}}_{t+1} + \Pi^{\mathfrak{B}}_{t+1}) O_C \Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2 - \|\Pi^{\mathfrak{C}}_{t+1} O_C \Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2 \\ &\le \|\Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2 - \|\Pi^{\mathfrak{C}}_{t+1} O_C \Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2. \end{aligned}$$

The equality (3c) follows immediately from Claim 1. Towards (3d), recall Claim 1 stating that $\Pi^{\mathfrak{C}}_{t+1} O_C \Pi^{\mathfrak{C}}_t = O_C \Pi^{\mathfrak{C}}_t$ and that its image is orthogonal to that of $\Pi^{\mathfrak{C}}_{t+1} O_C (\Pi^{\mathfrak{B}}_t + \Pi^{\mathfrak{A}}_t)$. Hence,

$$\begin{aligned} &\|\Pi^{\mathfrak{C}}_{t+1} O_C |\phi\rangle\|^2 \\ &= \|\Pi^{\mathfrak{C}}_t |\phi\rangle\|^2 + \|\Pi^{\mathfrak{C}}_{t+1} O_C (\Pi^{\mathfrak{B},act}_t + \Pi^{\mathfrak{B},pas}_t + \Pi^{\mathfrak{A}}_t) |\phi\rangle\|^2 \\ &\le \|\Pi^{\mathfrak{C}}_t |\phi\rangle\|^2 + 3\|\Pi^{\mathfrak{B},act}_t |\phi\rangle\|^2 + 3\|\Pi^{\mathfrak{C}}_{t+1} O_C \Pi^{\mathfrak{B},pas}_t |\phi\rangle\|^2 \\ &\quad + 3 \underbrace{\|\Pi^{\mathfrak{C}}_{t+1} O_C \Pi^{\mathfrak{A}}_t\|^2}_{=\frac{1}{n-t} < \frac{1}{n-t-1}}, \end{aligned} \tag{4}$$

where the equality under the brace is due to Claim 4. □

Remark 1 *Consider the last three squares of norms on the left hand side of (4), namely, $a := \|\Pi^{\mathfrak{B},act}_t |\phi_t\rangle\|^2$, $b := \|\Pi^{\mathfrak{C}}_{t+1} O_C \Pi^{\mathfrak{B},pas}_t |\phi_t\rangle\|^2$, and $c := \|\Pi^{\mathfrak{C}}_{t+1} O_C \Pi^{\mathfrak{A}}_t\|^2$, and also consider $d := \|\Pi^{\mathfrak{B}}_t |\phi_t\rangle\|^2$ appearing in the definition of the progress measure Ψ_t. As we will see below, when proving the final claim of Lemma 2, we need that the scalar in front of d in the definition of Ψ_t must be both at least as large as the scalar in front of b in (4) and strictly larger than the scalar in front of a in (4). While currently those scalars are 4, 3, and 3, respectively, we could have taken them to be $2+\alpha$, $2+\alpha$, and $2+\alpha/2$ for any $\alpha > 0$. That is because we could have used in (4) the fact that*

$$(a+b+c)^2 \le (2+\alpha/2)a^2 + (2+\alpha)b^2 + (1+3/\alpha)c^2.$$

We have chosen the scalar 4 instead of $2+\alpha$ in the definition of Ψ_t for sake of simplicity.

Proof. (The final claim of Lemma 2). For conciseness, let $n_t := n - t - 1$. Note that $\Pi^{\mathfrak{B}}_{t+1} O_Q$, $\Pi^{\mathfrak{B}}_{t+1} O_C$, $\Pi^{\mathfrak{C}}_{t+1} O_Q$, $\Pi^{\mathfrak{C}}_{t+1} O_C$ have orthogonal images. Hence, by Lemma 3

and the fact that U_{t+1} commutes with both $\Pi^{\mathfrak{C}}_{t+1}$ and $\Pi^{\mathfrak{B}}_{t+1}$, we have

$$\begin{aligned}\Psi_{t+1} &= \|\Pi^{\mathfrak{C}}_{t+1}U_{t+1}O_p|\phi_t\rangle\|^2 + 4\|\Pi^{\mathfrak{B}}_{t+1}U_{t+1}O_p|\phi_t\rangle\|^2 \\ &\le \|\Pi^{\mathfrak{C}}_{t}|\phi_t\rangle\|^2 + 3p\|\Pi^{\mathfrak{B},act}_{t}|\phi_t\rangle\|^2 \\ &\quad + 3p\|\Pi^{\mathfrak{C}}_{t+1}O_C\Pi^{\mathfrak{B},pas}_{t}|\phi_t\rangle\|^2 + \frac{3p}{n_t} \\ &\quad + 4(1-p)\Big(\|\Pi^{\mathfrak{B},act}_{t}|\phi_t\rangle\| + \frac{2}{\sqrt{n_t}}\Big)^2 \\ &\quad + 4\|\Pi^{\mathfrak{B},pas}_{t}|\phi_t\rangle\|^2 - 4p\|\Pi^{\mathfrak{C}}_{t+1}O_C\Pi^{\mathfrak{B},pas}_{t}|\phi_t\rangle\|^2.\end{aligned}$$

Here we observe that the sum of the two terms having $\|\Pi^{\mathfrak{C}}_{t+1}O_C\Pi^{\mathfrak{B},pas}_{t}|\phi_t\rangle\|^2$ is non-positive, and thus can be omitted (in Remark 1, this concerns the scaling of b and d). Moreover, note that

$$\|\Pi^{\mathfrak{C}}_{t}|\phi_t\rangle\|^2 + 4\|\Pi^{\mathfrak{B},pas}_{t}|\phi_t\rangle\|^2 = \Psi_t - 4\|\Pi^{\mathfrak{B},act}_{t}|\phi_t\rangle\|^2,$$

therefore we have

$$\begin{aligned}\Psi_{t-1} - \Psi_t &\le \frac{3p}{n_t} - (4-3p)\|\Pi^{\mathfrak{B},act}_{t}|\phi_t\rangle\|^2 \\ &\quad + 4(1-p)\Big(\|\Pi^{\mathfrak{B},act}_{t}|\phi_t\rangle\| + \frac{2}{\sqrt{n_t}}\Big)^2 \\ &= \frac{64-112p+51p^2}{pn_t} \\ &\quad - p\bigg(\|\Pi^{\mathfrak{B},act}_{t}|\phi_t\rangle\| - \frac{8(1-p)}{p\sqrt{n_t}}\bigg)^2 \\ &\le \frac{64}{pn_t}.\end{aligned}$$

(In above, we used that $-(4-3p)+4(1-p)$ is strictly negative, which, in Remark 1, concerns the scaling of a and d.) □

Acknowledgements

The author would like to thank Yassine Hamoudi, François Le Gall, Han-Hsuan Lin, and Qisheng Wang for fruitful and insightful discussions. The author was supported by JSPS KAKENHI Grant No. JP20H05966 and MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant No. JPMXS0120319794.

Divide-and-conquer verification method for noisy intermediate-scale quantum computation

Yuki Takeuchi[1] Yasuhiro Takahashi[2] Tomoyuki Morimae[3] Seiichiro Tani[1]

[1]*NTT Communication Science Laboratories, NTT Corporation, Japan*
[2]*Faculty of Informatics, Gunma University, Japan*
[3]*Yukawa Institute for Theoretical Physics, Kyoto University, Japan*

Abstract. Several noisy intermediate-scale quantum computations can be regarded as logarithmic-depth quantum circuits on a sparse quantum computing chip. In this presentation, we propose a method to efficiently verify such noisy intermediate-scale quantum computation. Although the direct fidelity estimation requires $O(2^n)$ copies of an n-qubit output state on average, our method requires only $O(D^3 2^{12D})$ copies even in the worst case, where $D = O(\log n)$ is the denseness of the ideal output state. We also perform a proof-of-principle experiment of our method by using IBM's cloud quantum computing platform. The detail is given in the full paper [1].

Keywords: Verification of quantum computation, Noisy intermediate-scale quantum computation, Planar separator theorem

1 Background

Universal quantum computers are expected to efficiently solve several hard problems that are intractable for classical counterparts. However, to exploit their full potential, quantum error correction (QEC) is necessary. For current technologies, QEC is highly demanding because it requires precise state preparations, quantum operations, and measurements. That is why the potential of quantum computation without QEC is being actively explored. Such non-fault-tolerant quantum computation is called noisy intermediate-scale quantum (NISQ) computation [2], and several NISQ algorithms have already been proposed [3, 4, 5].

Although several error mitigation techniques have been proposed [6, 7, 8, 9], NISQ computation should be finished in at most logarithmic time due to the lack of fault-tolerance. Note that when an error occurs with a constant probability in each time step, logarithmic-depth quantum circuits succeed with a probability of the inverse of a polynomial. Furthermore, some current quantum computing chips are sparse in the sense that they can be separated into two parts by removing a small number of connections between two qubits. For example, IBM's 53-qubit chip [10, 11] in Fig. 1 can be separated into two parts ($0-27$ and $28-52$) by removing only two connections between the 21st and 28th qubits and between the 25th and 29th qubits. In short, several NISQ computations can be regarded as shallow (i.e., at most logarithmic-depth) quantum circuits on a sparse chip, and we focus on such NISQ computations.

Since the performance of NISQ computations is strongly affected by noise, it is necessary to efficiently check whether a given NISQ computer works as expected. This task is known as the verification of quantum computation. Although various efficient verification methods [12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28] have been proposed so far, they all assume (fault-tolerant) universal quantum computations. Particularly, some of these methods [12, 13, 14, 16, 17, 19, 22, 23, 26, 28] are based on measurement-based quantum computation (MBQC) [29], which consumes at least one qubit to apply a single elementary quantum gate. Therefore, MBQC requires more qubits than the quantum circuit model. Since the number of available qubits is limited in NISQ computations, the MBQC is inadequate for it. The method of Fitzsimons *et al.* [18] requires a prover (i.e., a quantum computer to be verified) to generate a Feynman-Kitaev history state whose generation seems to be hard for NISQ computations. Other methods [21, 24, 25, 27] require the prover to compute classical functions in a superposition, where the functions are constructed from the learning-with-errors problem [30]. This task also seems to be beyond the capability of NISQ computations. Furthermore, since NISQ computers are expected to be used to solve several problems such as optimizations, classifications, and simulations of materials, a verification method should be developed for

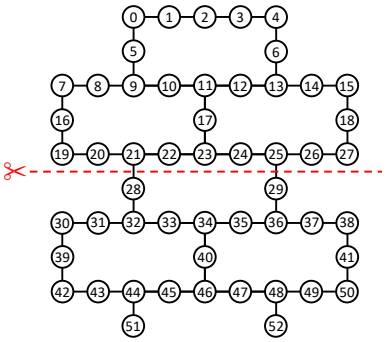


Figure 1: The connectivity of qubits within the IBM Rochester 53-qubit chip. Two-qubit operations can be directly applied on only pairs of two qubits connected by a line. This chip can be separated into two parts ($0-27$ and $28-52$) by removing only two connections between the 21st and 28th qubits and between the 25th and 29th qubits.

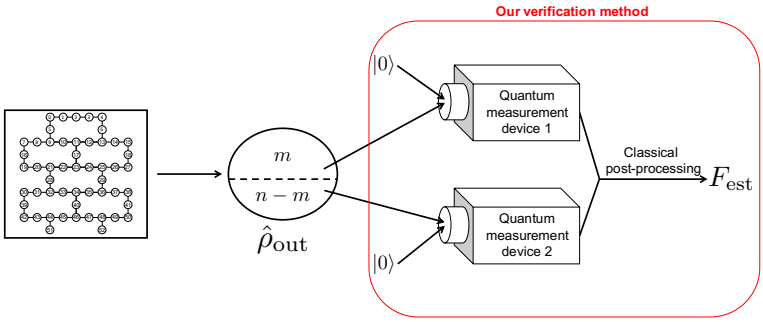


Figure 2: Diagram of our verification method. The n-qubit quantum state $\hat{\rho}_{\rm out}$ is the output from a sparse chip. m and other $n-m$ qubits of $\hat{\rho}_{\rm out}$ are measured by noisy quantum measurement devices 1 and 2 with an ancillary qubit $|0\rangle$, respectively. Our method repeats these procedures polynomially many times. Then by classically post-processing all measurement outcomes, we obtain an estimate $F_{\rm est}$ of the fidelity $\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$. Although we depict the quantum measurement devices 1 and 2 as different devices for simplicity, they can be treated as a single $(m+1)$-qubit device by sequentially measuring m and the other $n-m$ qubits of $\hat{\rho}_{\rm out}$.

general problems other than decision problems, which can be answered by YES or NO. It is highly nontrivial whether an n-qubit NISQ computer can be efficiently verified by using a quantum measurement device that is strictly smaller than n qubits.

2 Our result

Let $|\psi_t\rangle$ be any n-qubit pure state generated from an ideal logarithmic-depth quantum circuit on a sparse chip. We propose an efficient method to estimate the fidelity between $|\psi_t\rangle$ and the actual state $\hat{\rho}_{\rm out}$ generated from an actual NISQ computer. Our method needs a $(m+1)$-qubit measurement device, where $n/2+1 \leq m+1 < n$. Since our method estimates the fidelity between the actual and ideal quantum states, it can be used for any problems beyond decision problems. Our method is constructed as follows (see also Fig. 2): first, we obtain an upper bound on the diamond norms between the ideal quantum operations achieved in the $(m+1)$-qubit measurement device and its actual ones. Our method works even if the $(m+1)$-qubit measurement device is somewhat noisy, i.e., the upper bound is non-zero but sufficiently small. Then we measure m qubits of $\hat{\rho}_{\rm out}$ and an ancillary qubit $|0\rangle$ by using the noisy $(m+1)$-qubit operators. The remaining $n-m$ qubits of $\hat{\rho}_{\rm out}$ are also similarly measured with another ancillary qubit $|0\rangle$, where $n-m \leq m$. We repeat these procedures by generating a polynomial number of copies of $\hat{\rho}_{\rm out}$. Finally, by classically post-processing all measurement outcomes, we estimate the fidelity $\langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle$. Since we divide $\hat{\rho}_{\rm out}$ into two parts and measure each of them separately, our verification method can be considered as a divide-and-conquer method. Its detailed procedure is given in our full paper [1].

The efficiency of our verification method can be summarized as the following theorem:

Theorem 1 *Let $|\psi_t\rangle \equiv U|0^n\rangle$ be an n-qubit pure state generated from an ideal logarithmic-depth quantum circuit on a sparse chip, where U consists of a polynomial number of CZ gates and single-qubit quantum gates. Suppose that n qubits are divided into m and $(n-m)$ qubits, where $n/2 \leq m$, $m = \Theta(n)$, and $n-m = \Theta(n)$, such that the number of CZ gates between them is $D = O(\log n)$. We assume that the diamond norm between any ideal and actual $(m+1)$-qubit gates is upper bounded by $\epsilon/4^{D+2}$. Then for any n-qubit state $\hat{\rho}_{\rm out}$, our method outputs $F_{\rm est}$ such that with probability of at least $1-\delta$, $|F_{\rm est} - \langle\psi_t|\hat{\rho}_{\rm out}|\psi_t\rangle| \leq \epsilon$, by performing $(m+1)$-qubit measurements on*

$$O\left(\frac{2^{12D}}{\epsilon^6}\left(D+\log\frac{1}{\delta\epsilon^4}\right)^3\right)$$

copies of $\hat{\rho}_{\rm out}$, where $0 < \epsilon, \delta < 1$.

The proof of this theorem and experimental evaluation of our protocol with IBM's cloud quantum computing platform are given in our full paper [1].

3 Comparisons to existing methods

Our verification method is superior to existing methods in terms of the number of required copies, which we call the sample complexity. The sample complexity of our method is $O(D^3 2^{12D})$ that is a polynomial in n for NISQ computations because $D = O(\log n)$. As an existing fidelity estimation method, the quantum state tomography [31, 32, 33] can estimate the fidelity by reconstructing the matrix representation of $\hat{\rho}_{\rm out}$. Since any n-qubit state can be identified using $O(4^n)$ complex numbers, the quantum state tomography requires at least the same number of copies of $\hat{\rho}_{\rm out}$. To improve the efficiency, Flammia and Liu proposed a direct fidelity estimation method that estimates the fidelity without reconstructing $\hat{\rho}_{\rm out}$ [34]. Their method requires $O(2^n)$ copies of $\hat{\rho}_{\rm out}$ on average. Although their method improved on the quantum state tomography in terms of the number of required copies, the number is still exponential in n. On the other hand, as mentioned above, our method requires only a polynomial number of copies even in the worst case.

So far, we have assumed that the quantum computing chip $\mathcal{C}$ is sparse. Our method is superior to the direct fidelity estimation method [34] even when $\mathcal{C}$ is not

sparse but is a planar graph with a constant maximum degree. Since the graphs underlying almost all current physical chips are planar ones with constant maximum degrees, this assumption is quite natural. For example, the geometry of Google's Sycamore 53-qubit chip [35] is a planar graph with the maximum degree four, although it is not sparse. As a consequence of the planar separator theorem [36, 37], D is $O(\sqrt{n}\log n)$ for logarithmic-depth quantum circuits on any planar graph with a constant maximum degree. Therefore, the sample complexity of our method is $2^{O(\sqrt{n}\log n)}$, which is less than the sample complexity $O(2^n)$ of the direct fidelity estimation method.

Prior to our work, as far as we know, only two types of verification methods were developed for NISQ computers [38, 39, 40, 41]. Our method can estimate the fidelity between ideal and actual output states, unlike the methods in Refs. [38, 40], which can estimate the total variation distance between an actual output probability distribution and the ideal one. In this sense, our method is superior to theirs. Note that theirs can also be used to estimate lower and upper bounds on the probability that the target quantum circuit is afflicted by errors. By using the upper bound, a lower bound on the fidelity can be obtained, which may be loose. The methods in Refs. [39, 41] achieve both verifiability and the security, i.e., they enable us to securely and verifiably delegate quantum computing to a remote server even if the server's quantum computer is noisy. Its error robustness is promising. However, their method is based on the MBQC, which seems to be inadequate for NISQ computers as we have mentioned, whereas our method is not.

Efficient verification methods have already been proposed for several quantum states such as graph states [13, 28, 22], hypergraph states [17, 19, 26], weighted graph states [23], and Dicke states [42]. Since these previous methods are tailored for the specific classes of states, they cannot be used for our purpose. Our method can efficiently estimate the fidelity for any pure state generated by shallow quantum circuits on a sparse chip.

References

[1] Y. Takeuchi, Y. Takahashi, T. Morimae, and S. Tani. Divide-and-conquer verification method for noisy intermediate-scale quantum computation. Quantum, 6:758, 2022.

[2] J. Preskill. Quantum Computing in the NISQ era and beyond. Quantum, 2:79, 2018.

[3] 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. Nat. Commun., 5:4213, 2014.

[4] E. Farhi, J. Goldstone, and S. Gutmann. A Quantum Approximate Optimization Algorithm. 1411.4028, 2014.

[5] K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii. Quantum circuit learning. Phys. Rev. A, 98:032309, 2018.

[6] Y. Li and S. C. Benjamin. Efficient Variational Quantum Simulator Incorporating Active Error Minimization. Phys. Rev. X, 7:021050, 2017.

[7] K. Temme, S. Bravyi, and J. M. Gambetta. Error Mitigation for Short-Depth Quantum Circuits. Phys. Rev. Lett., 119:180509, 2017.

[8] S. Endo, S. C. Benjamin, and Y. Li. Practical Quantum Error Mitigation for Near-Future Applications. Phys. Rev. X, 8:031027, 2018.

[9] X. Bonet-Monroig, R. Sagastizabal, M. Singh, and T. E. O'Brien. Low-cost error mitigation by symmetry verification. Phys. Rev. A, 98:062339, 2018.

[10] A. Kondratyev. Non-Differentiable Learning of Quantum Circuit Born Machine with Genetic Algorithm. SSRN 3569226, 2020.

[11] W.-J. Huang, W.-C. Chien, C.-H. Cho, C.-C. Huang, T.-W. Huang, and C.-R. Chang. Mermin's Inequalities of Multiple Qubits with Orthogonal Measurements on IBM Q 53-qubit System. Quantum Engineering, doi: 10.1002/que2.45, 2020.

[12] T. Morimae. Verification for measurement-only blind quantum computing. Phys. Rev. A, 89:060302(R), 2014.

[13] M. Hayashi and T. Morimae. Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing. Phys. Rev. Lett., 115:220502, 2015.

[14] T. Morimae. Measurement-only verifiable blind quantum computing with quantum input verification. Phys. Rev. A, 94:042301, 2016.

[15] D. Aharonov, M. Ben-Or, E. Eban, and U. Mahadev. Interactive Proofs for Quantum Computations. 1704.04487, 2017.

[16] J. F. Fitzsimons and E. Kashefi. Unconditionally verifiable blind quantum computation. Phys. Rev. A, 96:012303, 2017.

[17] T. Morimae, Y. Takeuchi, and M. Hayashi. Verification of hypergraph states. Phys. Rev. A, 96:062321, 2017.

[18] J. F. Fitzsimons, M. Hajdušek, and T. Morimae. *Post hoc* Verification of Quantum Computation. Phys. Rev. Lett., 120:040501, 2018.

[19] Y. Takeuchi and T. Morimae. Verification of Many-Qubit States. Phys. Rev. X, 8:021060, 2018.

[20] A. Broadbent. How to Verify a Quantum Computation. Theory of Computing, 14:11, 2018.

[21] U. Mahadev. Classical Verification of Quantum Computations. In *Proc. of the 59th Annual Symposium on Foundations of Computer Science*, p. 259, 2018.

[22] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons. Resource-efficient verification of quantum computing using Serfling's bound. npj Quantum Information, 5:27, 2019.

[23] M. Hayashi and Y. Takeuchi. Verifying commuting quantum computations via fidelity estimation of weighted graph states. New J. Phys., 21:093060, 2019.

[24] A. Gheorghiu and T. Vidick. Computationally-Secure and Composable Remote State Preparation. In *Proc. of the 60th Annual Symposium on Foundations of Computer Science*, p. 1024, 2019.

[25] G. Alagic, A. M. Childs, A. B. Grilo, and S.-H. Hung. Non-interactive classical verification of quantum computation. 1911.08101, 2019.

[26] H. Zhu and M. Hayashi. Efficient Verification of Hypergraph States. Phys. Rev. Applied, 12:054047, 2019.

[27] N.-H. Chia, K.-M. Chung, and T. Yamakawa. Classical Verification of Quantum Computations with Efficient Verifier. 1912.00990, 2019.

[28] D. Markham and A. Krause. A Simple Protocol for Certifying Graph States and Applications in Quantum Networks. Cryptography, 4:3, 2020.

[29] R. Raussendorf and H. J. Briegel. A One-Way Quantum Computer. Phys. Rev. Lett., 86:5188, 2001.

[30] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of the 37th Annual Symposium on Theory of Computing*, p. 84, 2005.

[31] D. T. Smithey, M. Beck, M. G. Raymer, and A. Faridani. Measurement of the Wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum. Phys. Rev. Lett., 70:1244, 1993.

[32] Z. Hradil. Quantum-state estimation. Phys. Rev. A, 55:R1561(R), 1997.

[33] K. Banaszek, G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi. Maximum-likelihood estimation of the density matrix. Phys. Rev. A, 61:010304(R), 1999.

[34] S. T. Flammia and Y.-K. Liu. Direct Fidelity Estimation from Few Pauli Measurements. Phys. Rev. Lett., 106:230501, 2011.

[35] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis. Quantum supremacy using a programmable superconducting processor. Nature (London), 574:505, 2019.

[36] R. J. Lipton and R. E. Tarjan. A Separator Theorem for Planar Graphs. SIAM J. Appl. Math., 36:177, 1979.

[37] R. J. Lipton and R. E. Tarjan. Applications of a Planar Separator Theorem. SIAM J. Comput., 9:615, 1980.

[38] S. Ferracin, T. Kapourniotis, and A. Datta. Accrediting outputs of noisy intermediate-scale quantum computing devices. New J. Phys., 21:113038, 2019.

[39] E. Kashefi, D. Leichtle, L. Music, and H. Ollivier. Securing Quantum Computations in the NISQ Era. 2011.10005, 2020.

[40] S. Ferracin, S. T. Merkel, D. McKay, and A. Datta. Experimental accreditation of outputs of noisy quantum computers. 2103.06603, 2021.

[41] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier. Verifying BQP Computations on Noisy Devices with Minimal Overhead. 2109.04042, 2021.

[42] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang. Efficient Verification of Dicke States. Phys. Rev. Applied, 12:044020, 2019.

Transformation of an unknown unitary operation: complex conjugation

based on *Optimal universal quantum circuits for unitary complex conjugation* [IEEE]

Daniel Ebler[4 5 *] Michał Horodecki[6 †] Marcin Marciniak[1 ‡] **Tomasz Młynik**[1 §]
Marco Túlio Quintino[2 3 ¶] Michał Studziński[1 ‖]

[1] *Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics, and Informatics, University of Gdańsk, Wita Stwosza 57, 80-308 Gdańsk, Poland*
[2] *Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria*
[3] *Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3,A-1090 Vienna, Austria*
[4] *Huawei Hong Kong Research Center, Hong Kong SAR, P. R. China*
[5] *Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*
[6] *International Centre for Theory of Quantum Technologies, University of Gda´nsk, 80-952, Poland*

Abstract. Let $U \in SU(d)$ be an arbitrary unitary operator representing an arbitrary d-dimensional unitary quantum operation. We present optimal quantum circuits for transforming a number k of calls of $U : \mathbb{C}_d \to \mathbb{C}_d$ into its complex conjugate $\overline{U}$. Our circuits admit a parallel implementation and are proven to be optimal for any k and d with an average fidelity of $\langle F \rangle = \frac{k+1}{d(d-1)}$. This extends previous works which considered the scenario of a single call ($k = 1$) of the operation U, and the special case of $k = d - 1$ calls.

Keywords: Quantum circuit , Quantum channels , Quantum Combs

1 Introduction

The field of quantum information and computation typically describes how physical devices process information encoded into quantum systems. Such devices are often referred to as quantum gates in mathematical frameworks and can be combined into quantum circuits by defining the order of processing [7]. Conventionally, quantum gates were thought of as operations that take quantum states as inputs, and, after processing, output a quantum state. However, in a paradigm sometimes referred to as "higher-order quantum transformations" quantum gates rather than quantum states may be subject to transformation [8, 9]. Such higher-order quantum transformations can be viewed as a "circuit-board" approach for quantum operations, and have been found to have versatile applications encompassing quantum circuit design. When considering the transformation of an unknown unitary $U \in SU(d)$ with a function f, access to multiple copies or simply, multiple calls of the same unitary U, may be used to perform transformations $f(U)$ with higher fidelity than a single use of U. This introduces the freedom to arrange the multiple uses of U in different configurations. One could apply all uses in parallel or concatenate them in a sequence or consider the case where with indefinite causal order [4]. In particular one may analyze the performance of a general process transforming k uses of an unknown unitary operation U into its arbitrary function $f(U)$ such as unitary inversion, unitary transposition, or unitary complex conjugation [4]. The question regarding such a task is to know how well such processes, represented by quantum comb can perform in a deterministic manner. This and other similar tasks are of great importance showing theoretical limitations on potential quantum machines executing quantum program encoded in $f(U)$ and their attracted a lot of attention in recent years [1, 2, 3, 4].

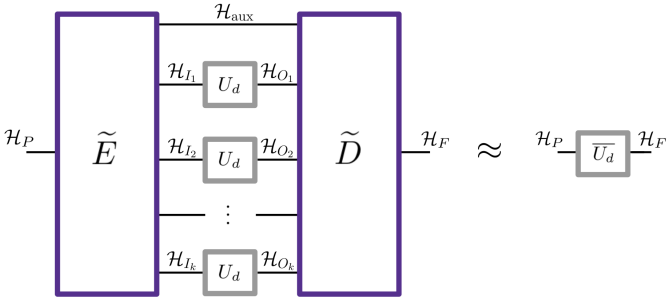


Figure 1: Parallel superchannel transforming k calls of a unitary operation $U \in SU(d)$ into its complex conjugation $\overline{U}$. Here $\widetilde{E}$ stands for an "encoder" quantum channel which is performed before the input operations $U^{\otimes k}$ and $\widetilde{D}$ stands for a "decoder" quantum channel acting after the input operations.

2 Our approach: $f(U) = \overline{U}$

We take a closer look at the case when the desired function f possesses a property of homomorphism i.e., $f(UV) = f(U)f(V)$, where $U, V \in SU(d)$, and quantum comb representing demanding process exhibits parallel structure, see for example [5]. It was shown in [6] that transformations f acting on unitary operation $U \in$

*eblerd@hku.hk
†michal.horodecki@ug.edu.pl
‡marcin.marciniak@ug.edu.pl
§tomasz.mlynik@phdstud.ug.edu.pl
¶marco.coelho_quintino@sorbonne-universite.fr
‖michal.studzinski@ug.edu.pl

$SU(d)$ as $f(U)$ can be implemented optimally by parallel circuits when f is a homomorphism. A crucial example within this class, from the point of view of quantum computing, is when $f(U) = \overline{U}$ (the bar denotes complex conjugation). A parallel designed circuit for implementation of a unitary complex conjugation is shown in Fig. 1.

Up to now, it was known how to construct optimal deterministic quantum comb which executes $U^{\otimes k} \mapsto \overline{U}$ with fidelity 1, but it demands exactly $k = d - 1$ uses [1]. This leaves the situation with access to fewer trials than k completely unsolved. In our work, we present a deterministic and universal quantum circuit that transforms k calls of an arbitrary d-dimensional unitary operator U producing $\overline{U}$ in unexplored earlier regime $k < d - 1$.

3 Used tools

Let $\widetilde{C_{\text{in}}} : \mathcal{L}(\mathcal{H}_{\boldsymbol{I}}) \to \mathcal{L}(\mathcal{H}_{\boldsymbol{O}})$ be an arbitrary input channel to a quantum circuit, which transforms it into an output channel $\widetilde{C_{\text{out}}} : \mathcal{L}(\mathcal{H}_P) \to \mathcal{L}(\mathcal{H}_F)$. The labels P and F stand for past and future, respectively (see Fig. 1). Quantum circuits designed to obtain the transformation $\widetilde{C_{\text{in}}} \mapsto \widetilde{C_{\text{out}}}$ may be analyzed by means of the encoder and decoder channels [3], a method which we describe in the following.

1. Before performing the input operation $\widetilde{C_{\text{in}}}$, we apply a quantum channel (encoder) $\widetilde{E} : \mathcal{L}(\mathcal{H}_P) \to \mathcal{L}(\mathcal{H}_{\boldsymbol{I}} \otimes \mathcal{H}_{\text{aux}})$, where $\mathcal{H}_{\text{aux}}$ is an arbitrary auxiliary (memory) space.
2. Then, the operation $\widetilde{C_{\text{in}}} \otimes \widetilde{\mathbb{I}_{\text{aux}}}$ is applied.
3. Finally, we perform a quantum channel (decoder) $\widetilde{D} : \mathcal{L}(\mathcal{H}_{\boldsymbol{O}} \otimes \mathcal{H}_{\text{aux}}) \to \mathcal{L}(\mathcal{H}_F)$ to obtain the output

$$\widetilde{C_{\text{out}}} = \widetilde{D} \circ \left(\widetilde{C_{\text{in}}} \otimes \widetilde{\mathbb{I}_{\text{aux}}}\right) \circ \widetilde{E}. \tag{1}$$

The use of k independent calls of a unitary operation U may be mathematically represented by a single operation $U^{\otimes k}$, where $\mathcal{U}(\rho) := U\rho U^\dagger$ is the unitary channel associated to the operator U. Then, by identifying $U^{\otimes k}$ as $\widetilde{C_{\text{in}}}$ in the routine described above, a parallel quantum circuit transforms k calls of U as

$$\mathcal{U}^{\otimes k} \mapsto \widetilde{D} \circ \left(\mathcal{U}^{\otimes k} \otimes \widetilde{\mathbb{I}_{\text{aux}}}\right) \circ \widetilde{E}, \tag{2}$$

as illustrated in Fig. 1.

By exploiting the Jamiołkowski-Choi isomorphism and the link product $*$ defined as $A * B := \text{tr}_2([A^{T_2} \otimes \mathbb{I}_3][\mathbb{I}_1 \otimes B])$ where $A \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$, $B \in \mathcal{L}(\mathcal{H}_2 \otimes \mathcal{H}_3)$ and T_2 is partial transposition applied on second system. We can reformulate (2) as

$$D * (|\mathbb{I}\rangle\!\rangle\langle\!\langle\mathbb{I}| \otimes C) * E = D * C * E, \tag{3}$$

where $|\mathbb{I}\rangle\!\rangle\langle\!\langle\mathbb{I}|$ is the Choi operator for the identity map $\widetilde{\mathbb{I}}$, D, C, E are Choi operators of $\widetilde{D}, \widetilde{C}, \widetilde{E}$ respectively. Thanks to the associativity and commutativity of the link product, we can represent an incomplete circuit as $S := E * D$ and we will call it superchannel. In this way, for any quantum channel C that we plug into the circuit, the output operation is described by

$$S * C = E * D * C, \tag{4}$$
$$= D * C * E, \tag{5}$$

which is a quantum channel from the past space $\mathcal{H}_P$ to the future space $\mathcal{H}_F$. As discussed earlier, since the complex conjugation function is a homomorphism, *i.e.*, $\overline{UV} = \overline{U}\,\overline{V}$, we can restrict our analysis to parallel quantum circuits. A linear operator $S \in \mathcal{L}(\mathcal{H}_O \otimes \mathcal{H}_{\mathbf{I}} \otimes \mathcal{H}_{\mathbf{O}} \otimes \mathcal{H}_F)$ is k-slot parallel superchannel if and only if

$$S \geq 0, \tag{6}$$
$$\text{tr}_F(S) = \text{tr}_{\mathbf{O}F}(S) \otimes \frac{\mathbb{I}_{\mathbf{O}}}{d_{\mathbf{O}}}, \tag{7}$$
$$\text{tr}_{\mathbf{IO}F}(S) = \text{tr}(S) \otimes \frac{\mathbb{I}_P}{d_P}, \tag{8}$$
$$\text{tr}(S) = d_P d_{\mathbf{O}}, \tag{9}$$

where $\mathcal{H}_{\boldsymbol{I}} := \mathcal{H}_{I_1} \otimes \ldots \otimes \mathcal{H}_{I_k}$, similarly, we write $\mathcal{H}_{\boldsymbol{O}} := \mathcal{H}_{O_1} \otimes \ldots \otimes \mathcal{H}_{O_k}$. Further, we have $\mathcal{H}_P \cong \mathcal{H}_F \cong \mathcal{H}_{I_i} \cong \mathcal{H}_{O_i} \cong \mathbb{C}_d$ for every $i \in \{1, \ldots, k\}$ and $\mathcal{H}_{\boldsymbol{I}} \cong \mathcal{H}_{\mathbf{O}} \cong \mathbb{C}_d^{\otimes k}$. Our target is to design a universal quantum circuit that approximates the transformation $U^{\otimes k} \mapsto f(U)$ for any $U \in SU(d)$ thus we can formulate the problem in the following way:

Given a function $f : SU(d) \to SU(d)$, find the optimal superchannel S such that: $S * |U\rangle\!\rangle\langle\!\langle U|^{\otimes k} \simeq |f(U)\rangle\!\rangle\langle\!\langle f(U)|$ for all $U \in SU(d)$ where $f(U) = \overline{U}$.

To quantify how similar two operations are alike is given by the channel fidelity. The fidelity between an arbitrary quantum channel $\widetilde{C}$ and a unitary channel acting as $\mathcal{U}(\rho) = U\rho U^\dagger$ on an input ρ is given by [12]

$$F(\widetilde{C}, \mathcal{U}) := \frac{1}{d^2}\langle\!\langle U|C|U\rangle\!\rangle, \tag{10}$$

where $|U\rangle\!\rangle$ the Choi vector of $\mathcal{U}$. A natural way to quantify the performance of a superchannel S on transforming $|U\rangle\!\rangle\langle\!\langle U|^{\otimes k}$ into $|f(U)\rangle\!\rangle\langle\!\langle f(U)|$ is given by its *average fidelity*

$$\langle F\rangle := \int_{U \in SU(d)} F\Big((S * |U\rangle\!\rangle\langle\!\langle U|^{\otimes k}), |f(U)\rangle\!\rangle\langle\!\langle f(U)|\Big)\, \mathrm{d}U, \tag{11}$$

where superchannel S has to satisfy casual constrains given by (6)-(9) and the integral is executed according to the Haar measure $\mathrm{d}U$ with respect to $SU(d)$. Authors in [4] proved that for the case of homomorphic transformations, the optimal average fidelity coincides with the optimal worst-case fidelity showing that average fidelity is a relevant figure of merit. Then in [2], when seeking for the optimal superchannels to maximize the average fidelity for a desired transformation $|U\rangle\!\rangle\langle\!\langle U|^{\otimes k} \to |f(U)\rangle\!\rangle\langle\!\langle f(U)|$ it is convenient to define the *performance operator*

$$\Omega := \frac{1}{d^2} \int_{U \in SU(d)} |f(U)\rangle\!\rangle\langle\!\langle f(U)|_{PF} \otimes |\overline{U}\rangle\!\rangle\langle\!\langle \overline{U}|_{\mathbf{IO}}^{\otimes k}\, \mathrm{d}U. \tag{12}$$

The performance operator is useful to evaluate the average fidelity of superchannel S via the relation $\langle F\rangle = \mathrm{tr}(S\Omega)$. For any given performance operator Ω, the problem of maximising the fidelity over all possible frameworks $\mathcal{S}$ of superchannels with k-slots can be phrased as

$$\max_{\mathcal{S}} \mathrm{tr}(S\Omega), \tag{13}$$

where the set $\mathcal{S} = \{parallel, sequential, general\}$. Authors [2] also showed that the dual problem of the SDP presented in (13) is given by

$$\min_{\overline{S}} \lambda \tag{14}$$

$$\text{such that: } \Omega \leq \lambda \overline{S}, \tag{15}$$

where $\overline{S}$ stands for the dual affine of the set of the desired k-slot supechannels $\mathcal{S}$. For particular case when function f is homomorphism then the performance operator respects the commutation relations for all $U, V \in SU(d)$ submit

$$[\Omega, f(V)_P \otimes \overline{V}_{\mathbf{I}}^{\otimes k} \otimes \overline{U}_{\mathbf{O}}^{\otimes k} \otimes f(U)_F] = 0. \tag{16}$$

Exploiting those commutation relations leads to

$$\Omega = \frac{1}{d^2} \sum_i \frac{(\overline{P^i_{\mathbf{I}P}} \otimes P^i_{\mathbf{O}F})}{d_i}, \tag{17}$$

where $\{P^i\}_i$ is an orthogonal basis for the linear space spanned by operators $P \in \mathcal{L}(\mathbb{C}_d^{\otimes k} \otimes \mathbb{C}_d)$ respecting $[P, \overline{U}^{\otimes k} \otimes f(U)] = 0$ for all $U \in SU(d)$, and $d_i := \mathrm{tr}(P_i P_i^\dagger)$. Given permutation relation (16) allows us to exploit the celebrated Schur-Weyl duality and show that the operators under consideration must belong to the algebra of the symmetric group $\mathcal{S}_k$.

4 Main Results

We state our main result for the transformation of an unknown unitary operation for complex conjugation.

1. The action of the encoder $E \in \mathcal{L}(\mathcal{H}_P \otimes \mathcal{H}_{\boldsymbol{I}})$, channel expressed in the Choi operator is given by

$$E := \frac{d}{\binom{d}{k+1}} A(d, k+1). \tag{18}$$

2. The decoder $D \in \mathcal{L}(\mathcal{H}_{\boldsymbol{O}} \otimes \mathcal{H}_F)$ channel expressed in Choi operator is given by

$$D := \frac{\binom{d}{k}}{\binom{d}{k+1}} A(d, k+1)_{\boldsymbol{O}F} + \left(\mathbb{I}_d^{\otimes k} - A(d,k)\right)_{\boldsymbol{O}} \otimes \sigma_F, \tag{19}$$

where $\sigma \in \mathcal{L}(\mathcal{H}_F) \cong \mathcal{L}(\mathbb{C}_d)$ is an arbitrary quantum state, *i.e.*, $\sigma \geq 0$ and $\mathrm{tr}(\sigma) = 1$ and $A(d,k)$ is projector onto antisymmetrical space.

3. Such a quantum circuit does not make use of any auxiliary space.

4. Using the methods of group representation and SDP duality theory, we solved the fidelity optimization problem, ensuring that the circuit presented in (18) and (19) is indeed the optimal one. We conclude that with the following theorem

Theorem 1. *Let $U \in SU(d)$ be a unitary operator representing an arbitrary d-dimensional unitary channel $\mathcal{U}(\rho) = U\rho U^\dagger$. When $k \leq d-1$ uses are available, the optimal quantum circuit which transforms k uses of U into its complex conjugation $\overline{U}$ attains average fidelity $\langle F\rangle = \frac{k+1}{d(d-k)}$.*

We summarize the results of Theorem 1 in the form of Fig 2 for certain dimensions d and uses k.

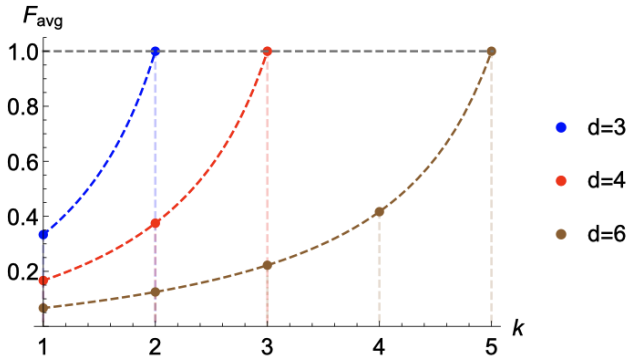


Figure 2: Average fidelity given by Theorem 1 for dimensions $d = \{3, 4, 6\}$ and uses $k = \{1, 2, 3, 4, 5\}$

References

[1] J. Miyazaki, A. Soeda, and M. Murao, Phys. Rev. Research 1, 013007 (2019).

[2] G. Chiribella and D. Ebler, New Journal of Physics 18, 093053 (2016).

[3] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. Lett. 101, 060401 (2008).

[4] Marco Túlio Quintino, Daniel Ebler, Quantum, vol. 6, p. 679 (2022).

[5] M. T. Quintino, Q. Dong, A. Shimbo, et al., Phys. Rev. A 100, 062339 (2019)

[6] A. Bisio, G. M. D'Ariano, P. Perinotti, and M. Sedlák, Physics Letters A 378, 1797–1808 (2014)

[7] M. Nielsen and I. Chuang, Natural Sciences (Cambridge University Press (2000))

[8] A. Bisio and P. Perinotti, Proceedings of the Royal Society of London Series A 475, 20180706 (2019)

[9] P. Perinotti, Tutorials, Schools, and Workshops in the Mathematical Sciences , 103–127 (2017)

[10] G. Chiribella, G. M. D'Ariano, and P. Perinotti EPL (Europhysics Letters) 83, 30004 (2008)

[11] G. Chiribella, G. M. D'Ariano, and P. Perinotti Phys. Rev. A 80, 022339 (2009)

[12] Raginsky, Physics Letters A, vol. 290, no. 1-2, pp. 11–18 (2001)

Universal, deterministic, and exact protocol to reverse qubit-unitary and qubit-encoding isometry operations

Satoshi Yoshida[1] * Akihito Soeda[1 2 3] † Mio Murao[1 4] ‡

[1] *Department of Physics, Graduate School of Science, The University of Tokyo, Hongo 7-3-1, Bunkyo-ku, Tokyo 113-0033, Japan*

[2] *Principles of Informatics Research Division, National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*

[3] *Department of Informatics, School of Multidisciplinary Sciences, SOKENDAI (The Graduate University for Advanced Studies), 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan*

[4] *Trans-scale Quantum Science Institute, The University of Tokyo, Bunkyo-ku, Tokyo 113-0033, Japan*

Abstract. In this work, we report a deterministic and exact protocol to reverse any unknown qubit-unitary and qubit-encoding isometry operations. We present the semidefinite programming (SDP) to search the Choi matrix representing a quantum circuit reversing any unitary operation. We derive a quantum circuit transforming four calls of any qubit-unitary operation into its inverse operation by imposing the $\mathrm{SU}(2)\times\mathrm{SU}(2)$ symmetry on the Choi matrix. This protocol only applies only for qubit-unitary operations, but we extend this protocol to any qubit-encoding isometry operations. For that, we derive a subroutine to transform a unitary inversion protocol to an isometry inversion protocol by constructing a quantum circuit transforming finite sequential calls of any isometry operation into random unitary operations.

Keywords: Higher-order quantum transformations, Quantum supermaps, Catalytic resource theory, Isometry operations, Encoding and decoding of quantum information

1 Background and main result

A quantum operation is reversible if and only if it is unitary [1]. Unitary operations encode quantum information reversibly, but reversible encoding of quantum information is not necessary a reversible quantum operation. General reversible encoding of a d-dimensional quantum system into a D-dimensional quantum system ($D \geq d$) is represented by an isometry operation $\widetilde{\mathcal{V}}_{d,D}(\rho) = V_{d,D}\rho V_{d,D}^\dagger$, where $V_{d,D} : \mathbb{C}^d \to \mathbb{C}^D$ is an isometry operator. Unitary operations are special cases of isometry operations where $D = d$, namely, $\widetilde{\mathcal{U}}_d(\rho) = U_d\rho U_d^\dagger$ for a unitary operator U_d. If a full description of $V_{d,D}$ is given, we can decode the original quantum information by applying a quantum operation $\widetilde{\mathcal{V}}_{\mathrm{inv}}$ satisfying $\widetilde{\mathcal{V}}_{\mathrm{inv}} \circ \widetilde{\mathcal{V}}_{d,D} = \widetilde{\mathbb{1}}_d$, where $\widetilde{\mathbb{1}}_d$ is the identity operation, and we call $\widetilde{\mathcal{V}}_{\mathrm{inv}}$ an inverse operation of $\widetilde{\mathcal{V}}$. However, a full description of $V_{d,D}$ is not necessarily available in distributed or cryptographic settings, e.g., when Alice implements $\widetilde{\mathcal{V}}_{d,D}$ in her laboratory and Bob would like to implement a decoding operation $\widetilde{\mathcal{V}}_{\mathrm{int}}$ without asking her the full description of $\widetilde{\mathcal{V}}_{d,D}$. In this situation, we need to "learn" the black box isometry $V_{d,D}$ and implement the inverse operation based on the learned data. Process tomography may be used to estimate the full description of $V_{d,D}$, but it introduces an extra resource overhead [2, 3]. Instead of storing the information of $V_{d,D}$ in a classical memory, it is possible to store it in a quantum state, but it is still impossible to retrieve the stored operation deterministically and exactly [4]. In this work, we consider the following task called *isometry inversion*: Given an unknown oracle of isometry operation $\widetilde{\mathcal{V}}_{d,D}$, the task is to implement its inverse operation $\widetilde{\mathcal{V}}_{\mathrm{inv}}$.

It is nontrivial whether such a protocol exists in quantum regime, even for the special case $D = d$ of isometry inversion, namely, unitary inversion. As often is the case with universal protocols (e.g., state cloning [5]), we cannot implement the inverse operation U_d^{-1} deterministically and exactly with a single use of U_d [6]. To avoid this no-go theorem, protocols utilizing finite calls of U_d to implement U_d^{-1} have been investigated. One trivial protocol is to perform a process tomography [2, 3] of U_d and implement the inverse operation of the estimated operation. However, this protocol needs a large number of calls of U_d and the implemented operation is non-exact. More efficient unitary inversion protocols have been proposed [7–14]. Also, Ref. [15] proposes isometry inversion protocols that use input operations in parallel. Yet, the proposed protocols so far are either *probabilistic* or *non-exact*.

Some works have investigated the fundamental limits of unitary inversion and isometry inversion. The limits of probabilistic exact or deterministic non-exact unitary inversion and isometry inversion have been investigated using semidefinite programming (SDP) [9, 15, 16]. However, the obtained numerical results are limited to small d, D and n since we need to search within a large space including all possible protocols. No-go results for deterministic exact unitary inversion are known for certain classes of protocols [7, 8, 16, 17]. It has been an open problem whether deterministic exact inversion is possible or not using more general protocols even when restricted to unitary.

In this work, we report a *deterministic* and *exact* protocol of isometry inversion for $d = 2$ and any $D \geq 2$. This

*satoshi.yoshida@phys.s.u-tokyo.ac.jp

†soeda@nii.ac.jp

‡murao@phys.s.u-tokyo.ac.jp

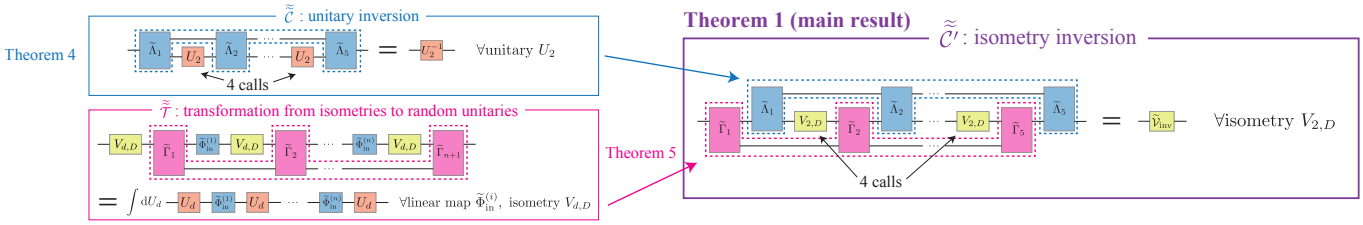


Figure 1: Construction of an isometry inversion comb $\widetilde{\widetilde{\mathcal{C}}}'$ by connecting a unitary inversion comb $\widetilde{\widetilde{\mathcal{C}}}$ and a quantum comb $\widetilde{\widetilde{\mathcal{T}}}$ transforming sequential calls of any isometry operation $\widetilde{\mathcal{V}}_{d,D}$ into sequential calls of a random unitary operation $\widetilde{\mathcal{U}}_d$.

protocol utilizes $n = 4$ calls of a qubit-encoding isometry $V_{2,D}$ in sequence with fixed quantum operations. We treat the input isometry operation as an unknown oracle (blackbox). The special case $D = 2$ of this protocol is a deterministic exact unitary inversion protocol. The main result is stated as follows.

Theorem 1. *For any given $D \geq 2$, there exists a quantum circuit transforming 4 calls of* any *qubit-encoding isometry operation $\widetilde{\mathcal{V}}_{2,D}$ given as an unknown oracle into its inverse operation $\widetilde{\mathcal{V}}_{\rm inv}$* deterministically *and* exactly.

To search isometry inversion protocols, we use the framework of quantum combs. Quantum combs are linear transformations of quantum operations that can be implemented by a quantum circuit using input operations in a fixed order. We represent quantum combs using their Choi matrices [18], and present an SDP to find deterministic exact *unitary* inversion for *any* dimension. It is shown that the maximum value of the SDP can be searched within the Choi matrices having a $\mathrm{SU}(d)\times\mathrm{SU}(d)$ symmetry, which reduces the size of the SDP. We present a deterministic exact *qubit*-unitary inversion protocol by solving the SDP and constructing the protocol. We also show that the qubit-unitary inversion protocol generates the "catalyst" state as a byproduct. This protocol applies only for qubit-unitary operations, but we extend this protocol to any *qubit-encoding isometry* operations. For that, we derive a subroutine to transform a unitary inversion protocol for *any* dimension to an isometry inversion protocol by constructing a transformation from isometry operations to random unitary operations (see Figure 1).

2 Deterministic exact qubit-unitary inversion

A quantum comb $\widetilde{\widetilde{\mathcal{C}}} : \bigotimes_{i=1}^{n}[\mathcal{L}(\mathcal{I}_i) \to \mathcal{L}(\mathcal{O}_i)] \to [\mathcal{L}(\mathcal{P}) \to \mathcal{L}(\mathcal{F})]$ can be characterized by a martix $C \in \mathcal{L}(\mathcal{P} \otimes \mathcal{I}^n \otimes \mathcal{O}^n \otimes \mathcal{F})$ called the Choi matrix [18], where $\mathcal{L}(\mathcal{H})$ denotes the space of linear operators on $\mathcal{H}$, $[\mathcal{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2)]$ denotes the space of linear operators from $\mathcal{L}(\mathcal{H}_1)$ to $\mathcal{L}(\mathcal{H}_2)$, and $\mathcal{I}^n := \bigotimes_{i=1}^{n}\mathcal{I}_i$ and $\mathcal{O}^n := \bigotimes_{i=1}^{n}\mathcal{O}_i$, as follows.

Lemma 2. [18] *Suppose a matrix $C \in \mathcal{L}(\mathcal{P}\otimes\mathcal{I}^n\otimes\mathcal{O}^n\otimes\mathcal{F})$ satisfies*

$$\begin{aligned} C &\geq 0, \\ \mathrm{Tr}_{\mathcal{I}_i} C_i &= C_{i-1} \otimes \mathbb{1}_{\mathcal{O}_{i-1}} \ \forall i \in \{1, \cdots, n+1\}, \\ C_0 &= 1, \end{aligned} \tag{1}$$

where $\mathbb{1}_{\mathcal{H}}$ is the identity operator on $\mathcal{H}$, $C_{n+1} := C$, $C_{i-1} := \mathrm{Tr}_{\mathcal{I}_i\mathcal{O}_{i-1}} C_i / \dim \mathcal{O}_{i-1}$, $\mathcal{I}_{n+1} := \mathcal{F}$, and $\mathcal{O}_0 := \mathcal{P}$. Then, there exists a circuit implementation of a quantum comb $\widetilde{\widetilde{\mathcal{C}}}$ corresponding to the Choi matrix C.

The unitary inversion condition can be formulated as an SDP by introducing a figure-of-merit called average fidelity defined as $\int \mathrm{d}U_d F(\widetilde{\widetilde{\mathcal{C}}}(\widetilde{\mathcal{U}}_d^{\otimes n}), \widetilde{\mathcal{U}}_d^{-1})$ using the Haar measure $\mathrm{d}U_d$ of $\mathrm{SU}(d)$ and the channel fidelity F.

Lemma 3. [16] *The maximal average fidelity of d-dimensional unitary inversion with n calls of the input unitary operation $\widetilde{\mathcal{U}}_d$ is calculated by the following SDP:*

$$\max \mathrm{Tr}(C\Omega_{d,n}) \text{ s.t. } C \text{ satisfies Eq. (1)}, \tag{2}$$

where $\Omega_{d,n}$ is defined as $\Omega_{d,n} := \int \mathrm{d}U_d |U_d\rangle\!\rangle\langle\!\langle U_d|^{\otimes n+1}_{\mathcal{I}^n\mathcal{F},\mathcal{O}^n\mathcal{P}}$ using the Choi vector $|U_d\rangle\!\rangle := \sum_i |i\rangle \otimes U_d |i\rangle$ for the computational basis $\{|i\rangle\}$.

It is shown that the maximum value of the SDP (2) can be searched within the set of the Choi matrices commuting with $U^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes V^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}$ for all $U, V \in \mathrm{SU}(d)$. Using this $\mathrm{SU}(d) \times \mathrm{SU}(d)$ symmetry, we reduce the number of variables in the SDP (2). We introduce a basis $\{E^{\mu}_{ij}\}$ of the set of operators on $(\mathbb{C}^d)^{\otimes n+1}$ commuting with $U^{\otimes n+1}$ for all $U \in \mathrm{SU}(d)$ [19, 20], associated to the Young-Yamanouchi basis, where μ runs in the set of Young diagrams with $n+1$ boxes and at most d rows, denoted by $\mathbb{Y}^d_{n+1}$, and i, j take the value from 1 to d_μ, where d_μ is the number of standard tableaux whose frame is μ. Any matrix C commuting with $U^{\otimes n+1}_{\mathcal{I}^n\mathcal{F}} \otimes V^{\otimes n+1}_{\mathcal{P}\mathcal{O}^n}$ for all $U, V \in \mathrm{SU}(d)$ is written by a linear combination of the tensor products $(E^{\mu}_{ij})_{\mathcal{I}^n\mathcal{F}} \otimes (E^{\nu}_{kl})_{\mathcal{P}\mathcal{O}^n}$. The partial trace of E^{μ}_{ij} in the last system and the tensor product $E^{\mu}_{ij} \otimes \mathbb{1}_{\mathbb{C}^d}$ is written simply using a similar basis $\{E^{\alpha}_{ab}\}$ for $\alpha \in \mathbb{Y}^d_n$ and $\alpha \in \mathbb{Y}^d_{n+2}$, respectively. Using these relations, we recursively derive the quantum comb condition (1) for the Choi matrix C in the form of the linear combination of $E^{\mu}_{ij} \otimes E^{\nu}_{kl}$.

By this procedure, we reduce the size of the matrix C in the SDP (2), and extend the numerical calculation of

Table 1: The maximal average fidelity of d-dimensional unitary inversion with n calls of the input unitary operation is obtained from the numerical calculation of the SDP (2). The newly obtained values compared to Ref. [16] are written with an underline.

	$n=2$	$n=3$	$n=4$	$n=5$
$d=2$	0.750	0.9330	$\underline{1}$	$\underline{1}$
$d=3$	0.3333	$\underline{0.4444}$	$\underline{0.5556}$	$\underline{0.6667}$
$d=4$	$\underline{0.1875}$	$\underline{0.2500}$	$\underline{0.3125}$	$\underline{0.3750}$
$\vdots$				

the optimal value of the SDP (2) in Ref. [16] up to $n \leq 5$ for arbitrary d (see Table 1). This numerical calculation shows the existence of a deterministic exact qubit-unitary inversion.

Theorem 4. *There exists a quantum comb $\widetilde{\widetilde{\mathcal{C}}}$ transforming 4 calls of* any *qubit unitary operation $\widetilde{\mathcal{U}}_2$ into its inverse operation $\widetilde{\mathcal{U}}_2^{-1}$* deterministically *and* exactly.

We show Theorem 4 by constructing a deterministic exact qubit-unitary inversion protocol. It is implemented using four calls of the input qubit-unitary operation U_2 and fixed quantum operations $\widetilde{\Lambda}_1$ and $\widetilde{\Lambda}_2$ and the antisymmetric state $|\psi^-\rangle \coloneqq (|01\rangle - |10\rangle)/\sqrt{2}$ (see Figure 2 and Ref. [21]). This quantum circuit implements unitary inversion since the inverse operation U_2^{-1} is applied on an arbitrary quantum state $|\phi_{\rm in}\rangle$. We also obtain an additional quantum state $(U_2 \otimes I)|\psi^-\rangle$ in the final state. Since the first call of U_2 in Figure 2 can be replaced by the quantum state $(U_2 \otimes I)|\psi^-\rangle$, we show that the quantum state $(U_2 \otimes I)|\psi^-\rangle$ is used as a "catalyst" in the qubit-unitary inversion, and we can implement the qubit-unitary inversion using three calls of U_2 with the "catalyst." This argument shows that m calls of the inverse operation can be obtained from $3m+1$ calls of the input qubit-unitary operation.

3 Construction of sequential isometry inversion protocols

We show the following theorem on isometry inversion. Combining it with Theorem 4, we obtain Theorem 1.

Theorem 5. *Suppose there exists a quantum comb $\widetilde{\widetilde{\mathcal{C}}}$ transforming n calls of any d-dimensional unitary operation $\widetilde{\mathcal{U}}_d$ to its inverse operation $\widetilde{\mathcal{U}}_d^{-1}$. Then, for any given $D \geq d$, there exists another quantum comb $\widetilde{\widetilde{\mathcal{C}}}'$ transforming n calls of any isometry operation $\widetilde{\mathcal{V}}_{d,D}$ to its inverse operation $\widetilde{\mathcal{V}}_{\rm inv}$.*

We construct a quantum comb $\widetilde{\widetilde{\mathcal{T}}}$ transforming $n+1$ calls of an isometry operation $\widetilde{\mathcal{V}}_{d,D}$ to $n+1$ calls of a random unitary operation $\widetilde{\mathcal{U}}_d$ (see the left-bottom part of Figure 1). Then, we construct an isometry inversion comb $\widetilde{\widetilde{\mathcal{C}}}'$ by connecting the given unitary inversion comb $\widetilde{\widetilde{\mathcal{C}}}$ and the quantum comb $\widetilde{\widetilde{\mathcal{T}}}$ as shown in Figure 1.

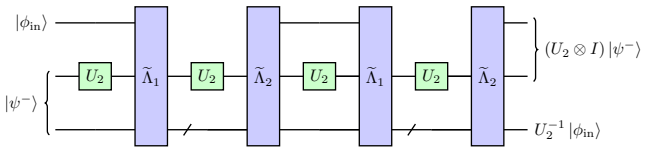


Figure 2: Deterministic exact qubit unitary inversion protocol using four calls of an input qubit-unitary operation U_2, which implements the inverse operation U_2^{-1} on an arbitrary input quantum state $|\phi_{\rm in}\rangle$ and an additional quantum state $(U_2 \otimes I)|\psi^-\rangle$. Here, $|\psi^-\rangle$ is the antisymmetric state defined as $|\psi^-\rangle \coloneqq (|01\rangle - |10\rangle)/\sqrt{2}$, and $\widetilde{\Lambda}_1$ and $\widetilde{\Lambda}_2$ are fixed quantum operations.

4 Discussions

We compare the performance of the deterministic exact unitary inversion with the previously known protocols. The optimal success probability of qubit-unitary inversion using input unitaries in parallel is $p = n/(n+3)$ [9]. The success probability is improved using a "success-or-draw" protocol to $p = 1 - (2/3)^{\lfloor n/2 \rfloor}$ [22]. To achieve $p = 1-\epsilon$, we need $n = O(\epsilon^{-1})$ (parallel) or $n = O(\log \epsilon^{-1})$ ("success-or-draw"), while our protocol only requires $n = O(1)$.

5 Conclusion and future work

This work shows the existence of deterministic exact isometry inversion protocol using 4 calls of input qubit-encoding isometry operation $\widetilde{\mathcal{V}}_{2,D}$ in sequence. We present the SDP approach to seek deterministic exact unitary inversion. We solve the SDP using the $\mathrm{SU}(d) \times \mathrm{SU}(d)$ symmetry to show the existence of a deterministic exact qubit-unitary inversion protocol. We construct a deterministic exact qubit-unitary inversion protocol, which transforms four calls of the input qubit-unitary operation U_2 to the inverse operation U_2^{-1} and the "catalyst" state. Using the "catalyst" state, we can transform $3m+1$ calls of U_2 to m calls of U_2^{-1}. Then, we show a qubit-encoding isometry inversion protocol by constructing a quantum comb transforming $n+1$ calls of any isometry operation into $n+1$ calls of a random unitary operation.

Reference [23] presents the reduction of SDPs with the $\mathrm{SU}(d)$ symmetry and a certain additional symmetry to linear programming. It is an interesting future work to invent a similar technique for the SDP of unitary inversion, which will be applied to seek deterministic exact unitary inversion for $d > 2$. This work shows a potential to use "catalysts" to transform unknown quantum operations. It is also an interesting future work to investigate the power of "catalysts" in other tasks to transform unknown quantum operations.

References

[1] M. A. Nielsen and I. Chuang, Quantum computation and quantum information (2002).

[2] I. L. Chuang and M. A. Nielsen, Journal of Modern Optics **44**, 2455 (1997).

[3] C. H. Baldwin, A. Kalev, and I. H. Deutsch, Physical Review A **90**, 012110 (2014).

[4] M. A. Nielsen and I. L. Chuang, Physical Review Letters **79**, 321 (1997).

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

[6] G. Chiribella and D. Ebler, New Journal of Physics **18**, 093053 (2016).

[7] M. Sedlák, A. Bisio, and M. Ziman, Physical review letters **122**, 170502 (2019).

[8] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Physical Review A **100**, 062339 (2019).

[9] M. T. Quintino, Q. Dong, A. Shimbo, A. Soeda, and M. Murao, Physical Review Letters **123**, 210502 (2019).

[10] I. S. Sardharwalla, T. S. Cubitt, A. W. Harrow, and N. Linden, arXiv preprint arXiv:1602.07963 (2016).

[11] M. Navascués, Physical Review X **8**, 031008 (2018).

[12] D. Trillo, B. Dive, and M. Navascués, Quantum **4**, 374 (2020).

[13] D. Trillo, B. Dive, and M. Navascués, arXiv preprint arXiv:2205.01131 (2022).

[14] P. Schiansky, T. Strömberg, D. Trillo, V. Saggio, B. Dive, M. Navascués, and P. Walther, arXiv preprint arXiv:2205.01122 (2022).

[15] S. Yoshida, A. Soeda, and M. Murao, arXiv preprint arXiv:2110.00258 (2021).

[16] M. T. Quintino and D. Ebler, Quantum **6**, 679 (2022).

[17] Z. Gavorová, M. Seidel, and Y. Touati, arXiv preprint arXiv:2011.10031 (2020).

[18] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Physical review letters **101**, 060401 (2008).

[19] M. Mozrzymas, M. Studziński, and M. Horodecki, Journal of Physics A: Mathematical and Theoretical **51**, 125202 (2018).

[20] M. Studziński, M. Mozrzymas, P. Kopszak, and M. Horodecki, IEEE Transactions on Information Theory (2022).

[21] See the Technical Manuscript for the proof of main results.

[22] Q. Dong, M. T. Quintino, A. Soeda, and M. Murao, Physical Review Letters **126**, 150504 (2021).

[23] D. Grinko and M. Ozols, arXiv preprint arXiv:2207.05713 (2022).

Perturbation theory enabled by quantum signal processing

Kosuke Mitarai[1 2 *] Kiichiro Toyoizumi[3] Wataru Mizukami[2]

[1] *Graduate School of Engineering Science, Osaka University, 1-3 Machikaneyama, Toyonaka, Osaka, Japan.*
[2] *Center for Quantum Information and Quantum Biology, Osaka University, Japan.*
[3] *Graduate School of Science and Technology, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama, Japan.*

Abstract. Perturbation theory is an important technique for reducing computational cost and providing physical insights in simulating quantum systems with classical computers. Here, we provide a quantum algorithm to obtain perturbative energies on quantum computers via quantum signal processing (QSP). We also estimate a rough computational cost of the algorithm for simple chemical systems such as water clusters and polyacene molecules. To the best of our knowledge, this is the first of such estimates for practical applications of QSP other than the Hamiltonian simulation.

Keywords: Perturbation theory, quantum signal processing, quantum simulation

1 Introduction

Perturbation theory is one of the most important techniques to understand quantum systems. It solves problems by separating them into easy parts and difficult ones, and gradually taking the effect of difficult parts into account. For weakly correlated systems, it usually gives sufficiently accurate physics. A benefit of using perturbative methods is its computational efficiency compared to the exact solvers. The computational cost to obtain an exact solution of an n-body quantum system is generally exponential to n on classical computers, while that of perturbative methods is only polynomial. Another important aspect of perturbation is its physical interpretability. It provides us insights into what effect a specific interaction of the system has on its overall physical properties.

In this work, we provide a method to implement perturbation theory on quantum computers. Our method allows one to use strongly-interacting Hamiltonians that are only solvable with quantum computers as a starting point of the perturbation. More specifically, our algorithm first constructs a ground state of an unperturbed Hamiltonian via quantum signal processing (QSP) [1–3] and fixed-point amplitude amplification [4]. Then, we generate a perturbative state by applying the inverse of an unperturbed Hamiltonian again with QSP, and obtain an expectation value of a perturbation operator via robust amplitude estimation (RAE) [5–7].

We also perform a concrete resource analysis of the algorithm for simple chemical systems such as water clusters and polyacenes to discuss its practicality. This is, to the best of our knowledge, the first such analysis of a practical application of the QSP and the QSP-based matrix inversion technique. Despite of efficiency of QSP compared to conventional techniques, it is found that our algorithm gives impractical numbers as computational cost; for example, we estimate over 10^{31} calls of block-encodings would be required to perform perturbation on a pentacene molecule. This is much larger than the cost required for naively performing the phase estimation of the total Hamiltonian, which only requires 10^{10} calls of block-encodings. While we could not achieve a reduction of computational cost like the classical perturbation theory, the other benefit of perturbation, that is, the interpretability of the result, is still an important point. Conventional techniques of quantum simulations based on phase estimation can give us energy and its eigenstates, but cannot provide us insights into why the energy is the obtained value. We, therefore, believe this work is a first step toward an "explainable" quantum simulation on fault-tolerant quantum computers.

*mitarai.kosuke.es@osaka-u.ac.jp

2 Result

First, we introduce the block-encoding [3, 8]. We say a unitary U_A block-encodes a matrix A when it has the following form:

$$U_A = \begin{pmatrix} A/\alpha & \cdot \\ \cdot & \cdot \end{pmatrix}. \tag{1}$$

with $\alpha \in \mathbb{R}$. Given a block-encoding U_A of A, we can construct a block encoding of $P(A)$ for certain polynomials $P(x)$ [1–3]. This procedure is called quantum signal processing (QSP) [1–3].

We have an n-qubit Hamiltonian $H_{\text{total}} = H + V$. We consider the Hamiltonian H and the perturbation V that can be decomposed into Pauli operators σ_ℓ as,

$$H = \sum_{\ell=1}^{L_H} h_\ell \sigma_\ell \tag{2}$$

$$V = \sum_{\ell=1}^{L_V} v_\ell \sigma_\ell \tag{3}$$

Let the ground state of H_{total} with eigenvalue E_0 be $|E_0\rangle$. Also, let an eigenstate H with an eigenvalue ϵ_i be $|\epsilon_i\rangle$. We assume that the eigenvalues are ordered in ascending order $\epsilon_0 < \epsilon_1 \leq \cdots \leq \epsilon_{2^n-1}$ and that we know Δ such that $\epsilon_1 - \epsilon_0 > \Delta$. Note that Hamiltonians H in this form can be block-encoded with $\alpha = \|\boldsymbol{h}\|_1 = \sum_\ell |h_\ell|$ [9].

It is well known that $|E_0\rangle$ can be approximated as

$$|E_0\rangle \approx |\epsilon_0^{(1)}\rangle \tag{4}$$

$$:= |\epsilon_0\rangle - \Pi(H-\epsilon_0)^{-1}\Pi V|\epsilon_0\rangle\,, \tag{5}$$

where $\Pi = I - |\epsilon_0\rangle\langle\epsilon_0|$, to the first order in $\|V\|$ if ϵ_i is not degenerate. The corresponding eigenvalue E_0 can be approximated as,

$$E_0 \approx \epsilon_0 + \epsilon_0^{(1)} + \epsilon_0^{(2)}, \tag{6}$$

where

$$\epsilon_0^{(1)} = \langle\epsilon_0|V|\epsilon_0\rangle \tag{7}$$

and

$$\epsilon_0^{(2)} = -\langle\epsilon_0| V\Pi(H-\epsilon_0)^{-1}\Pi V |\epsilon_0\rangle . \tag{8}$$

This work aims to provide quantum procedures to obtain $\epsilon_0^{(1)}$ and $\epsilon_0^{(2)}$. Our formal results can be stated as follows:

Theorem 1 *Assume that we have an estimate $\hat{\epsilon}_0$ of ϵ_0, the ground state energy of H, such that $|\hat{\epsilon}_0 - \epsilon_0| < \delta_0 < \Delta$. Moreover, assume that we can preprare a state $|\psi\rangle$ such that $|\langle\epsilon_0|\psi\rangle|^2 = p$. Then, we can estimate $\epsilon_0^{(1)}$ within an additive error of δ_1 by using*

$$\mathcal{O}\left(\frac{\|\boldsymbol{h}'\|_1\|\boldsymbol{v}\|_{2/3}}{\Delta'\delta_1\sqrt{p}}\log\left(\frac{\|V\|}{\delta_1}\right)\log\left(\sqrt{\frac{p}{1-p}}\frac{\|V\|}{\delta_1}\right)\right) \tag{9}$$

calls of a block-encoding of H', where $\Delta' = \Delta - \delta_0$ and $H' = H - \hat{\epsilon}_0$.

Theorem 2 *Let $\hat{\epsilon}_0$, δ_0, $|\psi\rangle$, Δ', H' and p be defined as in Theorem 1. Additionally, let $\Pi = I - |\epsilon_0\rangle\langle\epsilon_0|$. Then, we can estimate the second-order perturbation energy $\epsilon_0^{(2)}$ within an additive error of δ_2 by using*

$$\mathcal{O}\left(\frac{\|\boldsymbol{h}\|_1\|\boldsymbol{v}\|_{2/3}^2}{{\Delta'}^2\delta_2\sqrt{p}}\log\left(\frac{\|V\|^2}{\Delta\delta_2}\right)\log\left(\sqrt{\frac{p}{1-p}}\frac{\|V\|^2}{\Delta\delta_2}\right)\right) \tag{10}$$

calls of a block-encoding of H'.

Our approach for performing perturbation on a quantum computer is as follows:

1. Assume that we have an estimate $\hat{\epsilon}_0$ of ϵ_0 such that $|\hat{\epsilon}_0 - \epsilon_0| < \delta_0$.
2. Efficiently generate $|\epsilon_0\rangle$ via QSP-based eigenstate filtering.
3. Estimate the first-order perturbation energy by measuring $\langle\epsilon_0|V|\epsilon_0\rangle$.
4. Estimate the second-order perturbation energy by performing the Hadamard test of a unitary which approximates $\Pi(H-\epsilon_0)^{-1}\Pi$ constructed via QSP.

Note that step 1 can be performed by various techniques for ground state energy estimation e.g. [10].

For step 2 of the algorithm, we utilize the QSP-approximation of rectangular functions to prepare the reference state $|\epsilon_0\rangle$. The construction of rectangular functions closely follows that of [2, 11] but we give more detailed cost, that is, the degree of polynomial needed for their approximation, than the previous works. In the full version [12], we show that there exists a QSP-implementable polynomial $P^{\mathrm{filter}}_{\varepsilon,\kappa,x_{\mathrm{th}}}(x)$ such that,

$$\begin{aligned} P^{\mathrm{filter}}_{\varepsilon,\kappa,x_{\mathrm{th}}}(x) &> 1-\varepsilon \quad (|x| < x_{\mathrm{th}}), \\ |P^{\mathrm{filter}}_{\varepsilon,\kappa,x_{\mathrm{th}}}(x)| &< \varepsilon \quad (|x| > x_{\mathrm{th}} + \kappa), \end{aligned} \tag{11}$$

where $x_{\mathrm{th}} > 0$, $0 < \kappa < 2(1 - x_{\mathrm{th}})$ are parameters, with degree $n_{\mathrm{filter}}(\varepsilon,\kappa,x_{\mathrm{th}}) = \mathcal{O}(\log(1/\varepsilon)/\kappa)$ plotted as Fig. 1.

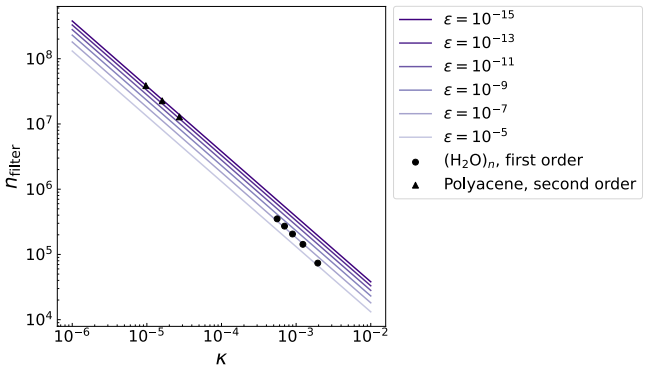


Figure 1: Values of n_{filter} calculated with $x_{\mathrm{th}} = 10^{-6}$, which is a typical value for the molecules studied in this work, and with different error parameters ε as a function of κ. Points corresponds to the values for specific molecules presented in Tables **??** and 1.

For step 4 of the algorithm, we need to implement $\Pi(H-\epsilon_0)^{-1}\Pi$. In the full version [12], we show that there exists a QSP-implementable polynomial $P^{\mathrm{ptb}}_{\varepsilon,w,w_0}(x)$ that satisfies the following conditions:

$$\left|P^{\mathrm{ptb}}_{\varepsilon,w,w_0}(x) - \frac{w}{2}\frac{1}{x}\right| < \frac{w}{2}\varepsilon \quad (w < |x| < 1) \tag{12}$$

$$\left|P^{\mathrm{ptb}}_{\varepsilon,w,w_0}(x)\right| < \frac{w}{2}\varepsilon \quad (|x| < w_0) \tag{13}$$

Its degree $n_{\mathrm{ptb}}(\varepsilon,w,w_0)$ is plotted in Fig. 2 with various parameter settings. Applying this polynomial to $H' = H - \hat{\epsilon}_0$ results in a operator that approximates $\Pi(H-\epsilon_0)^{-1}\Pi$. We set $w = \frac{\Delta-\delta_0}{\|\boldsymbol{h}'\|_1}$ and $w_0 = \frac{\delta_0}{\|\boldsymbol{h}'\|_1}$ by the same reason; the ground state energy of $H'/\|\boldsymbol{h}'\|_1$ is within $[-\delta_0/\|\boldsymbol{h}'\|_1, \delta_0/\|\boldsymbol{h}'\|_1]$ and its second largest energy is larger than $(\Delta-\delta_0)/\|\boldsymbol{h}'\|_1$.

Finally, we describe our approach for estimating the expectation values, i.e., $\langle\epsilon_0|V|\epsilon_0\rangle$ and $\langle\epsilon_0| V\Pi(H-\epsilon_0)^{-1}\Pi V |\epsilon_0\rangle$, that appears in step 3 and 4 of the algorithm. In this work, we estimate these expectation values by term-by-term basis, e.g., $\langle\epsilon_0|V|\epsilon_0\rangle = \sum_\ell v_\ell \langle\epsilon_0|\sigma_\ell|\epsilon_0\rangle$, like in the variational quantum eigensolvers. This allows us to know the contribution of each term to the total energy, which are essential for obtaining physical insights of the target system.

We utilize a state-of-the-art method called the robust amplitude estimation (RAE) [5–7], which can empirically estimate $\langle\psi|\sigma|\psi\rangle$ for a Pauli operator σ within a mean squared error of δ^2 by using $\frac{5\sqrt{2}}{2}\frac{e^2}{e-1}\frac{1}{\delta}$ calls of U_ψ which

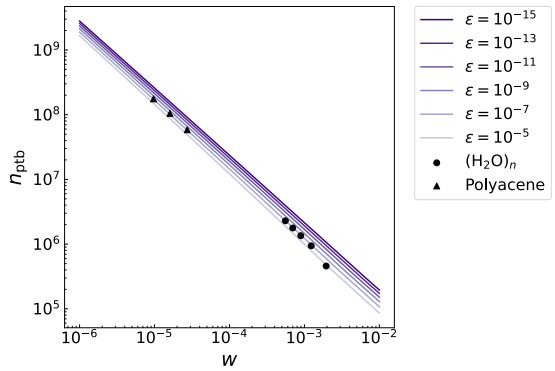


Figure 2: Values of n_{ptb} calculated with $w_0 = 10^{-6}$, which is a typical value for the molecules studied in this work, and with different error parameters ε as a function of w. Points corresponds to the values for specific molecules presented in Table 1.

Table 1: Total cost for estimating perturbation energies in terms of block-encoding calls.

System	Cost for $\epsilon_0^{(1)}$	Cost for $\epsilon_0^{(2)}$
$(H_2O)_2$	5.4×10^{10}	1.2×10^{18}
$(H_2O)_4$	1.0×10^{13}	6.8×10^{21}
$(H_2O)_6$	9.1×10^{13}	2.1×10^{23}
Tetracene	N/A	2.0×10^{30}
Pentacene	N/A	2.6×10^{31}
Hexacene	N/A	2.3×10^{32}

prepares $|\psi\rangle$ from $|0\rangle$. The technique demands us to deterministically prepare $|\epsilon_0\rangle$ but we resolve this requirement by via the fixed-point amplitude amplification algorithm [4]. The number of calls to the state preparation oracle can be optimized by the maginitude of coefficients v_ℓ; σ_ℓ with bigger v_ℓ should be measured more precisely than those with smaller v_ℓ. Using the optimized distribution of oracle calls, the total number of calls to the oracle for estimating $\langle\epsilon_0|V|\epsilon_0\rangle$ within precision of δ becomes $\mathcal{O}((\sum_\ell v_\ell^{2/3})^{3/2})/\delta$.

The overall cost in terms of the number of block-encoding calls for various molecules are calculated numerically and shown in Table 1. $(H_2O)_n$ represents water clusters and we treat intermolecular interaction as perturbation. For polyacenes, we treat the Hamiltonians acting on pi-orbitals as H and other terms as V. This choice makes $\epsilon_0^{(1)} = 0$ so we do not show the cost for $\epsilon_0^{(1)}$ for polyacenes. For details of the calculation, see the full version [12].

3 Conclusion

First, the estimated numbers are rather pessimistic; the algorithm needs over 10^{10} block-encoding calls for the simplest system considered here. However, it should be remarked that the large contribution to the overall cost comes from the expectation value estimation of the perturbation operator V. Second, although the overall cost seems to be impractical, the polynomial degrees are on the order of only 10^8 even for the largest system we considered. Hence, we might be able to perform the generation of the perturbed state in a practical time scale. Finally, it should be stressed again that the perturbative approach allows us to interpret the physical meaning of the results. We believe that, while the values of energy are indeed an important quantity, the interpretability of the results is key to the practical applications of quantum simulation algorithms. This work is only a first step toward this goal, which remains to be reached in the future.

References

[1] G. H. Low and I. L. Chuang, Phys. Rev. Lett. **118**, 010501 (2017).

[2] J. M. Martyn, Z. M. Rossi, A. K. Tan, and I. L. Chuang, PRX Quantum **2**, 040203 (2021).

[3] A. Gilyén, Y. Su, G. H. Low, and N. Wiebe, Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, p. 193–204, New York, NY, USA, 2019, Association for Computing Machinery.

[4] T. J. Yoder, G. H. Low, and I. L. Chuang, Phys. Rev. Lett. **113**, 210501 (2014).

[5] G. Wang, D. E. Koh, P. D. Johnson, and Y. Cao, PRX Quantum **2**, 010346 (2021).

[6] P. D. Johnson *et al.*, "Reducing the cost of energy estimation in the variational quantum eigensolver algorithm with robust amplitude estimation", arXiv:2203.07275, 2022.

[7] A. Katabarwa, A. Kunitsa, B. Peropadre, and P. Johnson, "Reducing runtime and error in VQE using deeper and noisier quantum circuits", arXiv:2110.10664, 2021.

[8] S. Chakraborty, A. Gilyén, and S. Jeffery, The Power of Block-Encoded Matrix Powers: Improved Regression Techniques via Faster Hamiltonian Simulation, in *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, edited by C. Baier, I. Chatzigiannakis, P. Flocchini, and S. Leonardi, , Leibniz International Proceedings in Informatics (LIPIcs) Vol. 132, pp. 33:1–33:14, Dagstuhl, Germany, 2019, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[9] R. Babbush *et al.*, Phys. Rev. X **8**, 041015 (2018).

[10] L. Lin and Y. Tong, Quantum **4**, 372 (2020).

[11] G. H. Low and I. L. Chuang, "Hamiltonian Simulation by Uniform Spectral Amplification", arXiv: 1707.05391, 2017.

[12] K. Mitarai, K. Toyoizumi, and W. Mizukami, Quantum **7**, 1000 (2023).

Circuit fidelity and computational cost of noisy quantum processing experiments

Kostyantyn Kechedzhi[1]

[1]*Google Quantum AI*

Abstract. Quantum processors surpassed the largest supercomputers for the specific computational benchmark of Random Circuit Sampling [1-5], without using quantum error correction protocols. Practical application of such noisy processors to typical tasks of simulating evolution of a quantum system in Physics and Chemistry would require computing expectation values of local observables. This adds important constraints on the resources needed for an equivalent simulation on a classical computer. In this presentation we will describe a unified framework that utilizes the underlying effective circuit volume to explain the tradeoff between the signal-to-noise ratio for a specific observable that can be achieved on a noisy quantum computer, and the corresponding classical computational cost. We apply this framework to recent quantum processor experiments of Random Circuit Sampling [5], quantum information scrambling [6], and a Floquet circuit unitary [7]. This allows us to reproduce the results of Ref. [7] in less than one second per data point using one GPU.

[1] S. Boixo, et. al., Characterizing quantum supremacy in near term devices, Nature Physics 14, 595 (2018).
[2] F. Arute, et al., Quantum supremacy using a programmable superconducting processor, Nature 574, 505 (2019).
[3] Y. Wu, et. al., Strong quantum computational advantage using a superconducting quantum processor, Physical Review Letters 127, 180501 (2021).
[4] Q. Zhu, et. al., Quantum computational advantage via 60-qubit 24-cycle random circuit sampling, Science Bulletin 67, 240 (2022).
[5] A. Morvan, et al., Phase transition in random circuit sampling, arXiv preprint arXiv:2304.11119 (2023).
[6] X. Mi, et al., Information scrambling in quantum circuits, Science 374, 1479 (2021).
[7] Y. Kim, et al., Evidence for the utility of quantum computing before fault tolerance, Nature 618, 500 (2023).

Reflections on the Life and Legacy of Göran Lindblad

Francesco Petruccione[1]

[1]*Stellenbosch University*

Abstract. This presentation offers an exploration of the life and legacy of Göran Lindblad, a pioneering figure in mathematical physics. Centered on his foundational work in open quantum systems and quantum communication, the talk will provide a snapshot of Lindblad's academic impact and influence on modern quantum technology.

Activation of genuine multipartite entanglement: Beyond the single-copy paradigm of entanglement characterisation

H. Yamasaki[1] S. Morelli[2] M. Miethlinger[3] J. Bavaresco [4] * N. Friis [3] M. Huber [3]

[1]*Department of Physics, Graduate School of Science, The University of Tokyo, Tokyo 113-0033, Japan*
[2]*BCAM - Basque Center for Applied Mathematics, Mazarredo 14, 48009 Bilbao, Spain*
[3]*Deparment of Applied Physics, University of Geneva, 1205 Geneva, Switzerland*
[4]*Atominstitut, Technical University of Vienna, 1020 Vienna, Austria*

Abstract. Entanglement shared among multiple parties presents complex challenges for the characterisation of different types of entanglement. One of the most fundamental insights is the fact that some mixed states can feature entanglement across every possible cut of a multipartite system yet can be produced via a mixture of states separable with respect to different partitions. To distinguish states that genuinely cannot be produced from mixing such partition-separable states, the term *genuine multipartite entanglement* was coined. All these considerations originate in a paradigm where only a single copy of the state is distributed and locally acted upon. In contrast, advances in quantum technologies prompt the question of how this picture changes when multiple copies of the same state become locally accessible. Here we show that multiple copies unlock genuine multipartite entanglement from partially separable states, i.e., mixtures of the partition-separable states, even from undistillable ensembles, and even more than two copies can be required to observe this effect. With these findings, we characterise the notion of genuine multipartite entanglement in the paradigm of multiple copies and conjecture a strict hierarchy of activatable states and an asymptotic collapse of the hierarchy.

Based on (the technical version follows the extended abstract):
Quantum 6, 695 (2022), arXiv:2106.01372 [quant-ph].

Keywords: Entanglement theory, genuine multipartite entanglement, many-copy activation

BACKGROUND

Entanglement shared among multiple parties is acknowledged as one of the fundamental resources driving the second quantum revolution. Yet, its detection and characterisation are complicated by several factors: among them, the computational hardness of deciding whether any given system even exhibits any entanglement at all [1] as well as the fact that the usual paradigm of local operations and classical communication (LOCC) lead to infinitely many types of entanglement [2, 3, 4, 5, 6, 7, 8] already for single copies of multipartite states. Significant effort has thus been devoted to devising practical means of entanglement certification from limited experimental data [9, 10].

One of the principal challenges for the characterisation of multipartite entanglement lies in distinguishing between *partial separability* and its counterpart, *genuine multipartite entanglement* (GME). Here, a multipartite state shared among multiple parties is said to be *partition-separable* if the density operator is written as a mixture of pure product states with respect to some fixed partition of the parties into two or more groups. A multipartite state is called *partially separable* if it can be decomposed as a mixture of partition-separable states, i.e., of states separable with respect to some (potentially different) partitions of the parties. Any state that cannot be decomposed in this way has *GME* (see Fig. 1, as well as Table 1 of the technical version). One may further classify partially separable states as k-separable states according to the maximal number k of tensor factors that all terms in the partially separable decomposition can be factorised into. If a state admits a decomposition where each term is composed of at least two tensor factors ($k = 2$), the state is called *biseparable*. Thus, every partially separable state is k-separable for some $k \geq 2$, and hence (at least) biseparable. This distinction arises naturally when considering the resources required to create a specific state: any biseparable state can be produced via LOCC in setups where all parties share classical randomness and subsets of parties share entangled states. One of the counter-intuitive features of partially separable states is the possibility for bipartite entanglement across every possible bipartition. Consequently, the notion of bipartite entanglement across partitions is insufficient to capture the notion of partial separability, and conventional methods, such as positive maps [11, 12], cannot be straightforwardly applied to reveal GME, which results in additional challenges compared to the—relatively simpler—scenario of detecting bipartite or partition entanglement (e.g., as in Ref. [13]).

An assumption inherent in the definitions above is that all parties locally act only on a single copy of the distributed state. However, in many experiments where quantum states are distributed among (potentially distant) parties, multiple independent but identically prepared copies of states are (or at least, can be) shared. For instance, exceptionally high visibilities of photonic states can only be achieved if each detection event stems from almost identical quantum states [14, 15]. Adding noise to the channel then produces the situation here: multiple copies of noisy quantum states produced in a laboratory [16, 17]. Even limited access to quantum

*jessica.bavaresco@unige.ch

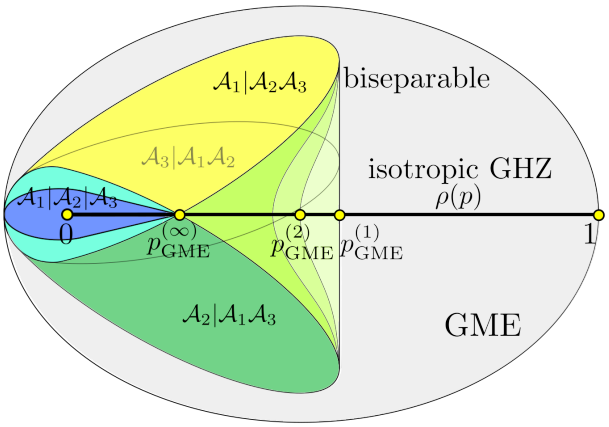


Figure 1: **GME and (partial) separability for three qubits**. All three-qubit states separable with respect to one of the three bipartitions, $\mathcal{A}_1|\mathcal{A}_2\mathcal{A}_3$ (yellow), $\mathcal{A}_2|\mathcal{A}_1\mathcal{A}_3$ (darker green), and $\mathcal{A}_3|\mathcal{A}_1\mathcal{A}_2$ (background), form convex sets, whose intersection (turquoise) contains (but is not limited to) all fully separable states $\mathcal{A}_1|\mathcal{A}_2|\mathcal{A}_3$ (dark blue). The convex hull of these partition-separable states contains all partially separable (the same as biseparable for tripartite systems) states. All states that are not biseparable are GME. States with k-copy activatable GME are contained in the set of biseparable but not partition-separable states and are conjectured to form the lighter green areas, with those states for which GME is activatable for higher values of k farther away from the border between GME and biseparability. The horizontal line represents the family of isotropic GHZ states $\rho(p)$, containing the maximally mixed state ($p = 0$) and the GHZ state ($p = 1$). The values $p_{\mathrm{GME}}^{(k)}$ indicate k-copy GME activation thresholds.

memories or signal delays then allows one to act on multiple copies of the distributed states, which is a recurring theme also in research on quantum networks [18, 19, 20]. Characterising properties of GME in multi-copy scenarios is thus not only of fundamental theoretical interest but also crucial for practical applications that require GME to be distributed, such as conference key agreement [21].

MAIN RESULTS

We demonstrate here that, unlike the distinction between separable and entangled states, the distinction between biseparability and GME is not maintained in the transition from one to many copies; i.e., partial separability is not a tensor-stable concept. As we show, for N parties $1, \ldots, N$, there exist multipartite quantum states $\rho_{\mathcal{A}_1,\mathcal{A}_2,\ldots,\mathcal{A}_N}$ that are biseparable, but which can be *activated* in the sense that sharing two copies results in a GME state, i.e., such that the joint state $\rho_{\mathcal{A}_1,\mathcal{A}_2,\ldots,\mathcal{A}_N} \otimes \rho_{\mathcal{B}_1,\mathcal{B}_2,\ldots,\mathcal{B}_N}$ of two identical copies (labelled $\mathcal{A}$ and $\mathcal{B}$, respectively) is not biseparable with respect to the partition $\mathcal{A}_1\mathcal{B}_1|\mathcal{A}_2\mathcal{B}_2|\ldots|\mathcal{A}_N\mathcal{B}_N$.

Here, we systematically investigate this phenomenon of *multi-copy GME activation*. That such activation of GME is in principle possible had previously only been noted in Ref. [22], where it was observed that two copies of a particular four-qubit state that is itself almost fully separable can become GME. By contrast, as the first main result, we show that the property of biseparability is not tensor stable in general by identifying a family of N-qubit isotropic Greenberger-Horne-Zeilinger (GHZ) states with two-copy activatable GME for all N. The isotropic GHZ states are defined as a convex combination of a pure GHZ state and the maximally mixed state, i.e., $\rho(p) \coloneqq p\,|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}| + (1-p)\,\frac{1}{2^N}\mathbb{1}_{2^N}$. To overcome the difficulty in analysing GME, the crucial technique here is to use states in X-form, i.e., those with nonzero entries of density operators only on the main diagonal and the main anti-diagonal with respect to the computational basis. For a multipartite state in the X-form, a necessary and sufficient condition of having GME reduces to positivity of the genuine multipartite (GM) concurrence, a measure of multipartite entanglement given by a polynomial function [23, 24]. Since an isotropic GHZ state is in an X-form, we can calculate the GM concurrence to certify GME. However, another difficulty in our analysis arises from the fact that multiple copies of isotropic GHZ states are no longer in the X-form. To resolve this difficulty, we exploit a Hadamard-product map of the multiple copies of isotropic GHZ states, which is implementable via stochastic LOCC (i.e., does not generate GME from partially separable states) and yet keeps the resulting state in the X-form [25]. In particular, we construct a sufficient GME criterion by converting the multi-copy isotropic GHZ states using the Hadamard-product map and applying the GM concurrence, to prove the multi-copy GME activation. We further demonstrate the existence of biseparable states within this family for which two copies are not enough to activate GME, but three copies are. Moreover, we show that the bound of p for partition-separability coincides with the asymptotic (in terms of the number of copies) GME-activation bound in the family of the isotropic GHZ states.

Multi-copy GME activation is particularly remarkable—and may appear surprising at first—because it is in stark contrast to bipartite entanglement: Two copies of states separable with respect to a fixed partition always remain partition-separable and can never become GME. However, from the perspective of entanglement distillation, such an activation seems more natural. After all, if one party shares bipartite maximally entangled states with each other party, these could be used to establish any GME state among all N parties via quantum teleportation, thus distributing GME by sharing only two-party entangled states. Such a procedure would require at least $N-1$ copies of these bipartite entangled states (in addition to a local copy of the GME state to be distributed). By contrast, already the example from Ref. [22] suggests that one does not have to go through first distilling bipartite entangled pairs, followed by teleportation, but two copies can

naturally feature GME already. While we have seen that the phenomenon of GME activation can be more than just distillation, one may still be tempted to think that distillable entanglement may be required for GME activation.

As another main result, we show that distillable entanglement is not necessary at all for the GME activation. It is known that there exist bound entangled states — entangled states that do not admit distillation of entanglement no matter how many copies are provided. In particular, all entangled states with positive partial transpose (PPT) across a given cut are undistillable. One might suspect that GME activation should not be possible for biseparable states that are PPT across every cut and hence have no distillable entanglement (even if multiple parties are allowed to collaborate). However, we here construct a biseparable state that is PPT with respect to every cut, and yet prove that multiple copies of this state have GME. A challenge in our proof is that we here cannot use the above techniques based on the X-form since the criteria on partition-separability, PPT, and GME turn out to coincide for the isotropic GHZ states. For the proof, we reduce the problem of constructing such a biseparable PPT state to that of a *PPT-triangle state* in the form of $\rho_{1,2}^{\mathrm{PPT}} \otimes \rho_{2,3}^{\mathrm{PPT}} \otimes \rho_{3,1}^{\mathrm{PPT}}$ with GME, where the subscript of each PPT state represents the pair of the parties $1, 2, 3$ between which the state is shared. Although GME witnesses based on PPT would fail to certify GME in this case, we employ a GME witness based on the lifted Choi map [26, 27] to prove the GME.

IMPACT

Our results show that a modern theory of entanglement in multipartite systems, which includes the potential to locally process multiple copies of distributed quantum states, exhibits a rich structure that goes beyond the convex structure of partially separable states on single copies. Together, our results support the following conjectures:

(i) There exists a hierarchy of k-copy activatable GME, i.e., for all $k \geq 2$, there exists a biseparable but not partition-separable state ρ such that $\rho^{\otimes k-1}$ is biseparable, but $\rho^{\otimes k}$ is GME.

(ii) GME is activatable for any biseparable but not partition-separable state (light green areas in Fig. 1) of any number of parties as $k \to \infty$.

These conjectures suggest that asymptotically, an even simpler description of multipartite entanglement might be possible; i.e., separability in multipartite systems collapses to a simple bipartite concept of separability. At the same time, we have shown that two copies are certainly not sufficient for reaching this simple limit, thus leaving the practical certification with finite copies a problem to be studied. Indeed, our results show that GME is a resource with a complex relationship to bipartite entanglement in the context of local operations and shared randomness. An array of important open questions arises from our results, which can thus be considered to establish an entirely new direction of research: first and foremost, this includes the quest for conclusive evidence for or against our conjectures. Besides determining whether these conjectures are ultimately correct or not, it will be of high interest to determine which properties (of the biseparable decompositions) of given states permit or prevent GME activation with a certain number of copies. Furthermore, from a practical point of view, our results also motivate development of a theory of k-copy multipartite entanglement witnesses, which are non-linear expressions of density matrices and allow for a more fine-grained characterisation of multipartite entanglement in networks with local memories.

References

[1] Leonid Gurvits. Classical complexity and quantum entanglement. *J. Comput. Syst. Sci.*, **69**, 448–484, (2004). [arXiv: quant-ph/0303055], Special Issue on STOC 2003.

[2] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde. Four qubits can be entangled in nine different ways. *Phys. Rev. A*, **65**, 052112, (2002). [arXiv: quant-ph/0109033].

[3] Andreas Osterloh and Jens Siewert. Constructing n-qubit entanglement monotones from antilinear operators. *Phys. Rev. A*, **72**, 012337, (2005). [arXiv: quant-ph/0410102].

[4] Julio I. de Vicente, Cornelia Spee, and Barbara Kraus. Maximally Entangled Set of Multipartite Quantum States. *Phys. Rev. Lett.*, **111**, 110502, (2013). [arXiv: 1305.7398].

[5] Katharina Schwaiger, David Sauerwein, Martí Cuquet, Julio I. de Vicente, and Barbara Kraus. Operational Multipartite Entanglement Measures. *Phys. Rev. Lett.*, **115**, 150502, (2015). [arXiv: 1503.00615].

[6] Julio I. de Vicente, Cornelia Spee, David Sauerwein, and Barbara Kraus. Entanglement manipulation of multipartite pure states with finite rounds of classical communication. *Phys. Rev. A*, **95**, 012323, (2017). [arXiv: 1607.05145].

[7] C. Spee, J. I. de Vicente, D. Sauerwein, and B. Kraus. Entangled Pure State Transformations via Local Operations Assisted by Finitely Many Rounds of Classical Communication. *Phys. Rev. Lett.*, **118**, 040503, (2017). [arXiv: 1606.04418].

[8] David Sauerwein, Nolan R. Wallach, Gilad Gour, and Barbara Kraus. Transformations among Pure Multipartite Entangled States via Local Operations are Almost Never Possible. *Phys. Rev. X*, **8**, 031020, (2018). [arXiv: 1711.11056].

[9] Géza Tóth and Otfried Gühne. Entanglement detection in the stabilizer formalism. *Phys. Rev. A*, **72**, 022340, (2005). [arXiv: quant-ph/0501020].

[10] Nicolai Friis, Giuseppe Vitagliano, Mehul Malik, and Marcus Huber. Entanglement Certification From Theory to Experiment. *Nat. Rev. Phys.*, **1**, 72–87, (2019). [arXiv: 1906.10929].

[11] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, **223**, 25, (1996). [arXiv: quant-ph/9605038].

[12] Asher Peres. Separability Criterion for Density Matrices. *Phys. Rev. Lett.*, **77**, 1413, (1996). [arXiv: quant-ph/9604005].

[13] Andrea Rodriguez-Blanco, Alejandro Bermudez, Markus Müller, and Farid Shahandeh. Efficient and Robust Certification of Genuine Multipartite Entanglement in Noisy Quantum Error Correction Circuits. *PRX Quantum*, **2**, 020304, (2021). [arXiv: 2010.02941].

[14] Siddarth Koduru Joshi, Djeylan Aktas, Sören Wengerowsky, Martin Lončarić, Sebastian Philipp Neumann, Bo Liu, Thomas Scheidl, Guillermo Currás Lorenzo, Željko Samec, Laurent Kling, Alex Qiu, Mohsen Razavi, Mario Stipčević, John G. Rarity, and Rupert Ursin. A trusted node–free eight-user metropolitan quantum communication network. *Sci. Adv.*, **6**, (2020). [arXiv: 1907.08229].

[15] Sören Wengerowsky, Siddarth Koduru Joshi, Fabian Steinlechner, Hannes Hübel, and Rupert Ursin. An entanglement-based wavelength-multiplexed quantum communication network. *Nature*, **564**, 225–228, (2018). [arXiv: 1801.06194].

[16] Sebastian Ecker, Frédéric Bouchard, Lukas Bulla, Florian Brandt, Oskar Kohout, Fabian Steinlechner, Robert Fickler, Mehul Malik, Yelena Guryanova, Rupert Ursin, and Marcus Huber. Overcoming Noise in Entanglement Distribution. *Phys. Rev. X*, **9**, 041042, (2019). [arXiv: 1904.01552].

[17] Xiao-Min Hu, Wen-Bo Xing, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, Paul Erker, and Marcus Huber. Efficient generation of high-dimensional entanglement through multipath down-conversion. *Phys. Rev. Lett.*, **125**, 090503, (2020). [arXiv: 2004.09964].

[18] Hayata Yamasaki, Alexander Pirker, Mio Murao, Wolfgang Dür, and Barbara Kraus. Multipartite entanglement outperforming bipartite entanglement under limited quantum system sizes. *Phys. Rev. A*, **98**, 052313, (2018). [arXiv: 1808.00005].

[19] Miguel Navascues, Elie Wolfe, Denis Rosset, and Alejandro Pozas-Kerstjens. Genuine Network Multipartite Entanglement. *Phys. Rev. Lett.*, **125**, 240505, (2020). [arXiv: 2002.02773].

[20] Tristan Kraft, Sébastien Designolle, Christina Ritz, Nicolas Brunner, Otfried Gühne, and Marcus Huber. Quantum entanglement in the triangle network. *Phys. Rev. A*, **103**, L060401, (2021). [arXiv: 2002.03970].

[21] Gláucia Murta, Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. Quantum conference key agreement: A review. *Adv. Quantum Technol.*, **3**, 2000025, (2020). [arXiv: 2003.10186].

[22] Marcus Huber and Martin Plesch. Purification of genuine multipartite entanglement. *Phys. Rev. A*, **83**, 062321, (2011). [arXiv: 1103.4294].

[23] Seyed Mohammad Hashemi Rafsanjani, Marcus Huber, Curtis J. Broadbent, and Joseph H. Eberly. Genuinely multipartite concurrence of N-qubit X matrices. *Phys. Rev. A*, **86**, 062303, (2012). [arXiv: 1208.2706].

[24] Zhi-Hao Ma, Zhi-Hua Chen, Jing-Ling Chen, Christoph Spengler, Andreas Gabriel, and Marcus Huber. Measure of genuine multipartite entanglement with computable lower bounds. *Phys. Rev. A*, **83**, 062325, (2011). [arXiv: 1101.2001].

[25] Ludovico Lami and Marcus Huber. Bipartite depolarizing channels. *J. Math. Phys.*, **57**, 092201, (2016). [arXiv: 1603.02158].

[26] Marcus Huber and Ritabrata Sengupta. Witnessing Genuine Multipartite Entanglement with Positive Maps. *Phys. Rev. Lett.*, **113**, 100501, (2014). [arXiv: 1404.7449].

[27] Fabien Clivaz, Marcus Huber, Ludovico Lami, and Gláucia Murta. Genuine-multipartite entanglement criteria based on positive maps. *J. Math. Phys.*, **58**, 082201, (2017). [arXiv: 1609.08126].

Simulating qubit correlations with classical communication

Martin Renner[1] * Armin Tavakoli[2] † Marco Túlio Quintino[3] ‡

[1] *University of Vienna, Faculty of Physics, Vienna Center for Quantum Science and Technology (VCQ), Boltzmanngasse 5, 1090 Vienna, Austria*
[2] *Physics Department, Lund University, Box 118, 22100 Lund, Sweden*
[3] *Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*

Abstract. We consider general prepare-and-measure scenarios in which Alice can transmit qubit states to Bob, who can perform general measurements in the form of positive operator-valued measures (POVMs). We show that the statistics obtained in any such quantum protocol can be simulated by the purely classical means of shared randomness and two bits of communication. Furthermore, we prove that two bits of communication is the minimal cost of a perfect classical simulation. In addition, we apply our methods to Bell scenarios, which extends the well-known Toner and Bacon protocol. In particular, two bits of communication are enough to simulate all quantum correlations associated to arbitrary local POVMs applied to any entangled two-qubit state. For the case of projective measurements, we provide explicit protocols that simulate perfectly the statistics of all local projective measurements on any pair of entangled qubits by communicating one classical trit. If the state is weakly entangled, already a single bit is sufficient and the expected amount of communication approaches zero in the limit where the degree of entanglement approaches zero.

This submission is mainly based on https://doi.org/10.1103/PhysRevLett.130.120801 and the presentation will also contain some results from https://arxiv.org/abs/2207.12457.

Keywords: Prepare-and-measure, Bell nonlocality, Dimension Witness, Quantum Foundations

1 Classical simulation of qubit correlations in prepare-and-measure scenarios

Quantum resources enable a sender and a receiver to break the limitations of classical communication [1–3]. Already in the simplest meaningful scenario, namely that in which the communication of a bit is substituted for a qubit, advantages are obtained in important tasks like Random Access Coding [4]. It is natural to explore the fundamental limits of quantum over classical advantages. Consider for instance the following question: You and your partner are allowed to send either a classical message of a given length (for instance one, two or even more classical bits) or one quantum bit (qubit). In the latter case, the sender is allowed to prepare the qubit in an arbitrary state and the receiver is allowed to measure the received qubit with an arbitrary measurement. If you have the choice between one qubit and one classical bit you are always better of by sending one qubit since the qubit can be used to perfectly encode one classical bit. In fact, the sender can prepare the qubit in one out of two orthogonal states and the receiver measures the received qubit in the corresponding basis. At the same time, a qubit provides an advantage over a classical bit in tasks like Random Access Coding [4]. However, to decide whether you should choose one qubit or a larger classical message such as two bits, is less obvious. Notably, Holevo's bound [5] shows that one qubit cannot be used to faithfully transmit more than one classical bit. Hence, there is at least one situation in which sending two bits is more powerful than sending one qubit. However, is it always better to send two classical bits? Our result shows that this is indeed the case. More precisely, we prove that two classical bits are sufficient to simulate any strategy that can be achieved by sending one qubit.

In fact, we consider general prepare-and-measure (PM) scenarios, in which Alice can prepare an arbitrary qubit state ρ and sends it to Bob. Secondly, Bob receives the state and performs an arbitrary quantum measurement (POVM) on the qubit to obtain an outcome b (see Fig. 1). By providing an explicit protocol, we show that any correlations they obtain in this scenario can be perfectly simulated by purely classical resources, namely shared randomness and two classical bits of communication. Moreover, we show that two bits is the minimal classical simulation cost, i.e. there exists no classical simulation that uses less communication than our protocol. This is shown through an explicit quantum protocol, based on qubit communication, that eludes a simulation with a ternary classical message.

Notably, there exists a trivial classical simulation in which Alice sends the Bloch vector coordinates of her quantum state to Bob. After that, Bob can classically compute the Born rule and samples his outcome accordingly. However, sending the coordinates requires an infinite amount of classical bits. Whether a classical simulation is possible with a finite classical message is much less trivial. Notably, the simulation protocol of Toner and Bacon showed that if we additionally restrict the quantum measurements to be projective, a classical simulation with two bits is possible [6]. However, this does not account for the full power of quantum theory. The most general measurements are known as positive operator-valued measures (POVMs). Such POVMs are even indispensable for important tasks like unambiguous state discrimination [7, 8] and hold a key role in many quantum information protocols (see e.g. [9–17]). This naturally

*martin.renner@univie.ac.at
†armin.tavakoli@teorfys.lu.se
‡Marco.Quintino@lip6.fr

Qubit $>$ 1 bit:	qubit can simulate one classical bit; qubit advantage in tasks like Random Access Coding [4] $\Longrightarrow$ Qubit performs at least as good as 1 classical bit for any task!
Qubit vs. 1 trit:	for some tasks one trit is stronger (Holevo's bound [5]); for others, one qubit is stronger (our result) $\Longrightarrow$ Choice between 1 qubit and 1 trit depends on the task!
Qubit $<$ 2 bits:	two classical bits can simulate all qubit correlations (our result) $\Longrightarrow$ Two bits perform at least as good as one qubit for any task!

Table 1: Summary: Comparing the strength of a classical and a qubit message in any prepare-and-measure scenario

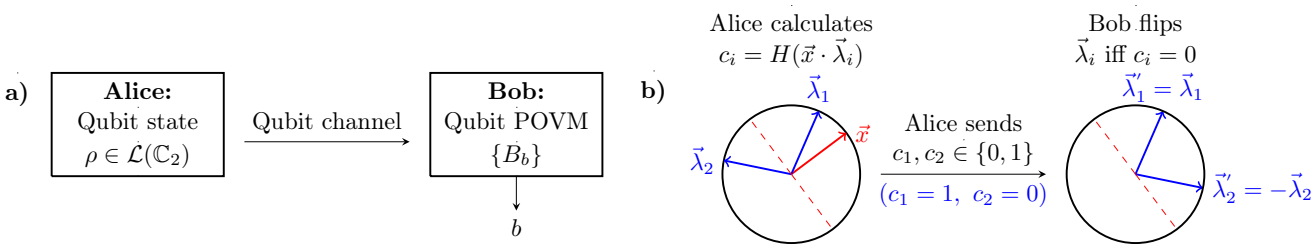


Figure 1: **a)** Quantum PM scenario: Alice sends a qubit state to Bob who performs a POVM to obtain his outcome b. **b)** A two-dimensional illustration of our classical simulation protocol: Alice and Bob share some random vectors on the Bloch-sphere $\vec{\lambda}_1$ and $\vec{\lambda}_2$. Alice sends the two bits $c_i = H(\vec{x} \cdot \vec{\lambda}_i)$ where $\vec{x}$ is the Bloch vector representation of the qubit state she wants to send and $H(\cdot)$ denotes the Heaviside function. We show that, for any state and any POVM, these two bits are sufficient for Bob to produce an outcome b that obeys the same statistics as in the quantum case.

raises the question of identifying the classical cost of simulating the most general predictions of quantum theory, based on POVMs. Notably, previous work has shown that there exists a classical simulation that requires 5.7 bits of communication on average [18]. However, that protocol has a certain probability to fail in each round, leading to an unbounded amount of communication in the worst case. In the contrary to these previous results, our protocol always succeed with two bits and allows for the most general qubit strategies including POVMs.

2 Classical simulation of local measurements on entangled qubit pairs

These results have direct applications to the task of simulating the non-local correlations of entangled quantum states. Bell's nonlocality theorem [19] shows that quantum correlations cannot be reproduced by local hidden variables. These non-local correlations are the cornerstone for many tasks in quantum information processing and found several applications in important fields like quantum cryptography [20]. In order to quantify the strength of these non-local correlations it is natural to quantify the amount of classical communication required to simulate the same statistics. More precisely, is there a classical protocol such that Alice and Bob can, for a given entangled two-qubit state, reproduce the same correlations for any local measurements on that quantum state? Since measurements are described by continuous parameters, it was even expected that the communication cost to reproduce these correlations is infinite [21]. After a sequence of improved protocols for entangled qubits [22–26], a breakthrough was made by Toner and Bacon in 2003 [6]. They showed that only two classical bits of communication are sufficient to simulate the statistics of all local projective measurements on any entangled two-qubit state. At the same time, they also show that if the state is maximally entangled, only a single bit is sufficient. Classical communication has then been established as a natural measure of Bell nonlocality [27–35] and found applications in constructing local hidden variable models [28]. However, two independent problems remained open for almost two decades [36–38]:

What about general POVMs? — The result of Toner and Bacon only applies to projective measurements. How does the communication cost changes if we consider the most general class of measurements, namely POVMs? The previously best protocol used 5.7 bits on average but an unbounded amount of communication in the worst case [18]. However, following an idea by Cerf et al. [24], we can adapt our classical protocol in the prepare-and-measure scenario to simulate the statistics obtained from arbitrary local POVMs on any entangled qubit pair with two classical bits of communication. In this way, our protocol immediately extends the Toner and Bacon model [6] to Bell scenarios involving POVMs. At the same time, we use the same amount of classical communication, in fact, two bits. If the state is maximally entangled, we also obtain a novel one bit protocol.

Why are partially entangled states harder to simulate? — The second open problem concerns the amount of communication to simulate general, partially entangled two-qubit states. Toner and Bacon have shown that a single bit of communication is sufficient to simulate all local projective measurements of a maximally entangled qubit pair. At the same time, the best protocol to simulate non-maximally entangled qubit pairs requires,

somehow counterintuitively, strictly more resources, in fact two bits. The asymmetry of partially entangled states and other evidences suggested that simulating weakly entangled states may be harder than simulating maximally entangled ones. For instance, in Ref. [39] the authors prove that at least two uses of a PR-box are required for simulating weakly entangled qubit pairs, while a single use of a PR-box is sufficient for maximally entangled qubits [40]. Additionally, weakly entangled states are strictly more robust than maximally entangled ones when the detection loophole is considered [41–44]. This raises an important foundational question [36–38]: Are partially entangled states strictly harder to simulate and therefore in a certain sense more non-local than the maximally entangled one, or, is a single bit still sufficient to simulate partially entangled qubits as well? It has been even called "a simple looking question waiting for an answer" in a recent article by Nicolas Gisin and Florian Fröwis [38]. In the second part of our work, we solve that question for weakly entangled states.

Our results — We present an explicit protocol that perfectly simulates local projective measurements on any pair of entangled qubits, $|\Psi_{AB}\rangle = \sqrt{p}\,|00\rangle + \sqrt{1-p}\,|11\rangle$, by communicating one classical trit. Additionally, when $\frac{2p(1-p)}{2p-1}\log\left(\frac{p}{1-p}\right) + 2(1-p) \leq 1$, approximately $0.835 \leq p \leq 1$, we present a classical protocol which requires only a single bit of communication. The latter model even allows a perfect classical simulation with an average communication cost that approaches zero in the limit where the degree of entanglement approaches zero ($p \to 1$). More precisely, Alice has to send the single bit only in a certain fraction of rounds. In the remaining rounds, they do not have to communicate with each other. We show that even under these circumstances a perfect simulation of all local projective measurements on weakly entangled states is possible. It is known that a simulation of a maximally entangled state without communication in some fraction of rounds is impossible. This would contradict the fact that the singlet has no local part [45, 46]. In this way, our result shows that simulating weakly entangled states requires strictly less communication resources than the maximally entangled one, solving a longstanding open problem [37, 38].

In order to derive our results we introduce a general framework to simulate entangled qubits. It is worth mentioning that this framework does not only allow us to derive our new results, it is also capable to reproduce known results in that field. Most importantly, a one-bit protocol for the maximally entangled state similar to the one from Toner and Bacon also fits into our framework [6, 28]. Independently of this, we obtain an independent proof of the result by Portmann et al. [47] which quantifies the local content of any pure entangled two-qubit state.

To conclude, we found explicit protocols that simulate the statistics of local measurements on any entangled qubit pair. If general POVMs are considered, two bits always suffices. If we restrict the measurements to be projective, we found a protocol with one trit for any state and a protocol with only a single bit if the state is weakly entangled. A natural direction is to consider classical simulations for higher-dimensional quantum PM scenarios or higher dimensional entangled quantum states. Although this has received some attention [29, 30, 34], few general results are known. Most notably, it is still an open problem whether a qutrit PM scenario can be classically simulated with a finite amount of classical bits.

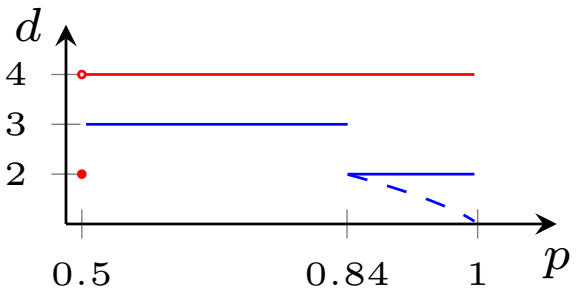


Figure 2: Summary of our results: Length of the classical message d ($d = 2$: one bit; $d = 3$: one trit; $d = 4$: two bits) required to simulate projective measurements on a general qubit pair $|\Psi_{AB}\rangle = \sqrt{p}\,|00\rangle + \sqrt{1-p}\,|11\rangle$ as a function in p. The previous best result, from Toner and Bacon [6], is presented in red. Our novel results are presented in blue. The dashed curve in blue represents the fraction of rounds where Alice needs to send a bit to Bob.

References

[1] C. H. Bennett and S. J. Wiesner, Communication via one- and two-particle operators on einstein-podolsky-rosen states, Phys. Rev. Lett. **69**, 2881–2884 (1992).

[2] R. Raz, Exponential separation of quantum and classical communication complexity, in *Proceedings of the thirty-first annual ACM symposium on Theory of computing* (1999) pp. 358–367.

[3] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis, Exponential separation of quantum and classical one-way communication complexity, in *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '04 (Association for Computing Machinery, New York, NY, USA, 2004) p. 128–137.

[4] S. Wiesner, Conjugate coding, SIGACT News **15**, 78–88 (1983).

[5] A. S. Holevo, Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel, Probl. Peredachi Inf. **9**, 3–11 (1973).

[6] B. F. Toner and D. Bacon, Communication Cost of Simulating Bell Correlations, Phys. Rev. Lett. **91**, 187904 (2003), arXiv:quant-ph/0304076 [quant-ph].

[7] I. Ivanovic, How to differentiate between non-orthogonal states, Physics Letters A **123**, 257–259 (1987).

[8] A. Peres, How to differentiate between non-orthogonal states, Physics Letters A **128**, 19 (1988).

[9] K. Banaszek, G. M. D'ariano, M. G. Paris, and M. F. Sacchi, Maximum-likelihood estimation of the density matrix, Phys. Rev. A **61**, 010304 (1999), arXiv:quant-ph/9909052 [quant-ph].

[10] J. M. Renes, Spherical-code key-distribution protocols for qubits, Phys. Rev. A **70**, 052314 (2004), arXiv:quant-ph/0402135 [quant-ph].

[11] T. Vértesi and E. Bene, Two-qubit Bell inequality for which positive operator-valued measurements are relevant, Phys. Rev. A **82**, 062115 (2010), arXiv:1007.2578 [quant-ph].

[12] N. Bent, H. Qassim, A. A. Tahir, D. Sych, G. Leuchs, L. L. Sánchez-Soto, E. Karimi, and R. W. Boyd, Experimental realization of quantum tomography of photonic qudits via symmetric informationally complete positive operator-valued measures, Phys. Rev. X **5**, 041006 (2015).

[13] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A **93**, 040102 (2016), arXiv:1505.03837 [quant-ph].

[14] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín, Unbounded randomness certification using sequences of measurements, Phys. Rev. A **95**, 020102 (2017), arXiv:1510.03394 [quant-ph].

[15] J. Bae, B. C. Hiesmayr, and D. McNulty, Linking entanglement detection and state tomography via quantum 2-designs, New Journal of Physics **21**, 013012 (2019), arXiv:1803.02708 [quant-ph].

[16] A. Tavakoli, Semi-device-independent certification of independent quantum state and measurement devices, Phys. Rev. Lett. **125**, 150503 (2020), arXiv:2003.03859 [quant-ph].

[17] A. Tavakoli, M. Farkas, D. Rosset, J.-D. Bancal, and J. Kaniewski, Mutually unbiased bases and symmetric informationally complete measurements in bell experiments, Science Advances **7**, eabc3847 (2021), arXiv:1912.03225 [quant-ph].

[18] A. A. Méthot, Simulating POVMs on EPR pairs with 5.7 bits of expected communication, European Physical Journal D **29**, 445–446 (2004), arXiv:quant-ph/0304122 [quant-ph].

[19] J. S. Bell, On the einstein podolsky rosen paradox, Physics Physique Fizika **1**, 195–200 (1964).

[20] A. K. Ekert, Quantum cryptography based on bell's theorem, Phys. Rev. Lett. **67**, 661–663 (1991).

[21] T. Maudlin, Bell's inequality, information transmission, and prism models, PSA: Proceedings of the Biennial Meeting of the Philosophy of Science Association **1992**, 404–417 (1992).

[22] G. Brassard, R. Cleve, and A. Tapp, Cost of Exactly Simulating Quantum Entanglement with Classical Communication, Phys. Rev. Lett. **83**, 1874–1877 (1999), arXiv:quant-ph/9901035 [quant-ph].

[23] M. Steiner, Towards quantifying non-local information transfer: finite-bit non-locality, Physics Letters A **270**, 239–244 (2000), arXiv:quant-ph/9902014 [quant-ph].

[24] N. J. Cerf, N. Gisin, and S. Massar, Classical Teleportation of a Quantum Bit, Phys. Rev. Lett. **84**, 2521–2524 (2000), arXiv:quant-ph/9906105 [quant-ph].

[25] A. K. Pati, Minimum classical bit for remote preparation and measurement of a qubit, Phys. Rev. A **63**, 014302 (2000), arXiv:quant-ph/9907022 [quant-ph].

[26] S. Massar, D. Bacon, N. J. Cerf, and R. Cleve, Classical simulation of quantum entanglement without local hidden variables, Phys. Rev. A **63**, 052305 (2001), arXiv:quant-ph/0009088 [quant-ph].

[27] D. Bacon and B. F. Toner, Bell Inequalities with Auxiliary Communication, Phys. Rev. Lett. **90**, 157904 (2003), arXiv:quant-ph/0208057 [quant-ph].

[28] J. Degorre, S. Laplante, and J. Roland, Simulating quantum correlations as a distributed sampling problem, Phys. Rev. A **72**, 062314 (2005), arXiv:quant-ph/0507120 [quant-ph].

[29] J. Degorre, S. Laplante, and J. Roland, Classical simulation of traceless binary observables on any bipartite quantum state, Phys. Rev. A **75**, 012309 (2007), arXiv:quant-ph/0608064 [quant-ph].

[30] O. Regev and B. Toner, Simulating quantum correlations with finite communication, SIAM Journal on Computing **39**, 1562–1580 (2010), arXiv:0708.0827 [quant-ph].

[31] C. Branciard and N. Gisin, Quantifying the Nonlocality of Greenberger-Horne-Zeilinger Quantum Correlations by a Bounded Communication Simulation Protocol, Phys. Rev. Lett. **107**, 020401 (2011), arXiv:1102.0330 [quant-ph].

[32] C. Branciard, N. Brunner, H. Buhrman, R. Cleve, N. Gisin, S. Portmann, D. Rosset, and M. Szegedy, Classical Simulation of Entanglement Swapping with Bounded Communication, Phys. Rev. Lett. **109**, 100401 (2012), arXiv:1203.0445 [quant-ph].

[33] G. Brassard, L. Devroye, and C. Gravel, Exact classical simulation of the quantum-mechanical ghz distribution, IEEE Transactions on Information Theory **62**, 876–890 (2016), arXiv:1303.5942 [cs.IT].

[34] G. Brassard, L. Devroye, and C. Gravel, Remote Sampling with Applications to General Entanglement Simulation, Entropy **21**, 92 (2019), arXiv:1807.06649 [quant-ph].

[35] E. Zambrini Cruzeiro and N. Gisin, Bell Inequalities with One Bit of Communication, Entropy **21**, 171 (2019), arXiv:1812.05107 [quant-ph].

[36] G. Brassard, Quantum communication complexity, Foundations of Physics **33**, 1593–1616 (2003).

[37] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Reviews of Modern Physics **86**, 419–478 (2014), arXiv:1303.2849 [quant-ph].

[38] N. Gisin and F. Fröwis, From quantum foundations to applications and back, Philosophical Transactions of the Royal Society of London Series A **376**, 20170326 (2018), arXiv:1802.00736 [quant-ph].

[39] N. Brunner, N. Gisin, and V. Scarani, Entanglement and non-locality are different resources, New Journal of Physics **7**, 88–88 (2005).

[40] N. J. Cerf, N. Gisin, S. Massar, and S. Popescu, Simulating Maximal Quantum Entanglement without Communication, Phys. Rev. Lett. **94**, 220403 (2005), arXiv:quant-ph/0410027 [quant-ph].

[41] P. H. Eberhard, Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment, Phys. Rev. A **47**, R747–R750 (1993).

[42] A. Cabello and J.-Å. Larsson, Minimum Detection Efficiency for a Loophole-Free Atom-Photon Bell Experiment, Phys. Rev. Lett. **98**, 220402 (2007), arXiv:quant-ph/0701191 [quant-ph].

[43] N. Brunner, N. Gisin, V. Scarani, and C. Simon, Detection Loophole in Asymmetric Bell Experiments, Phys. Rev. Lett. **98**, 220403 (2007), arXiv:quant-ph/0702130 [quant-ph].

[44] M. Araújo, M. T. Quintino, D. Cavalcanti, M. F. Santos, A. Cabello, and M. T. Cunha, Tests of Bell inequality with arbitrarily low photodetection efficiency and homodyne measurements, Phys. Rev. A **86**, 030101 (2012), arXiv:1112.1719 [quant-ph].

[45] A. C. Elitzur, S. Popescu, and D. Rohrlich, Quantum nonlocality for each pair in an ensemble, Physics Letters A **162**, 25–28 (1992).

[46] J. Barrett, A. Kent, and S. Pironio, Maximally Nonlocal and Monogamous Quantum Correlations, Phys. Rev. Lett. **97**, 170409 (2006), arXiv:quant-ph/0605182 [quant-ph].

[47] S. Portmann, C. Branciard, and N. Gisin, Local content of all pure two-qubit states, Phys. Rev. A **86**, 012104 (2012), arXiv:1204.2982 [quant-ph].

Detecting entanglement in quantum many-body systems via permutation moments

Zhenhuan Liu[1] Yifan Tang[1 2 3] Hao Dai[1] Pengyu Liu[1] Shu Chen[1] Xiongfeng Ma[1 *]

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

[2] *Department of Mathematics and Computer Science, Freie Universität Berlin, 14195 Berlin, Germany*

[3] *Department of Physics, Freie Universität Berlin, 14195 Berlin, Germany*

Abstract. In this work, we propose a framework for designing multipartite entanglement criteria based on permutation moments, which have an effective implementation with either the generalized control-SWAP quantum circuits or the random unitary techniques. As an example, in the bipartite scenario, we develop an entanglement criterion that can detect bound entanglement and show strong detection capability in the multi-qubit Ising model with a long-range XY Hamiltonian. In the multipartite case, the permutation-moment-based criteria can detect entangled states that are not detectable by any criteria extended from the bipartite case. Our framework also shows potential in entanglement quantification and entanglement structure detection. This work has been published on PRL [1].

Keywords: Multipartite Entanglement Detection, Index Permutation, State Moments, Randomized Measurements

1 Introduction

Multipartite entanglement plays an essential role in both quantum information science and many-body physics. Due to the exponentially large dimension and complex geometric structure of the state space, the detection of entanglement in many-body systems is extremely challenging in reality. Conventional means, like entanglement witness and state-moment criterion, either highly depend on the prior knowledge of the studied systems or the detection capability is relatively weak.

The index permutation criteria [2] are multipartite criteria that can be applied in systems with an arbitrary number of parties and dimensions and has many generalizations [3]. In the bipartite scenario, the permutation criteria cover the widely-used positive partial transposition (PPT) criterion [4] and the computable cross norm (CCNR) criterion [5]. However, because index permutation is an unphysical operation, and the permutation criteria are based on singular value decomposition, a highly nonlinear operation, the verification of permutation criteria is extremely resource-consuming.

In this work, we solve this problem by combing the permutation criterion with state-moment methods and propose a framework for designing multipartite entanglement criteria based on permutation moments.

2 Moment-based permutation criteria.

In general, a k-partite quantum state can be represented using a matrix with $2k$ indices, $\rho = \sum_{s_1,\cdots,s_{2k}} \rho_{s_1 s_2,\cdots,s_{2k-1}s_{2k}} |s_1 \cdots s_{2k-1}\rangle\langle s_2 \cdots s_{2k}|$, where $s_1, s_3, \ldots, s_{2k-1}$ represent the row indices, and $s_2, s_4, \ldots, s_{2k}$ represent the column ones. The two indices, s_{2r-1} and s_{2r}, denote for the r-th subsystem. By changing the order of these $2k$ indices, one gets a new matrix, $\mathcal{R}_\pi$, with $[\mathcal{R}_\pi]_{s_1 s_2,\cdots,s_{2k-1}s_{2k}} = \rho_{s_{\pi(1)}s_{\pi(2)},\cdots,s_{\pi(2k-1)}s_{\pi(2k)}}$, where π is an element of $2k$-th permutation group $\mathcal{S}_{2k}$. Using the property of index permutation, one could prove that [2]

$$\|\mathcal{R}_\pi\| = \mathrm{tr}\left(\sqrt{\mathcal{R}_\pi \mathcal{R}_\pi^\dagger}\right) = \sum_i \lambda_i \leq 1, \tag{1}$$

for all k-partite separable states, where $\{\lambda_i\}$ are the singular values of $\mathcal{R}_\pi$. The violation of this inequality indicates entanglement. In the bipartite scenario, when setting π to be $(1,2)$ and $(2,3)$, where $(\cdot,\cdot)$ denotes exchanging two indices, one gets the PPT and the CCNR criterion, respectively. As we mentioned before, the difficulty of measuring $\|\mathcal{R}_\pi\|$ hinders the further applications of permutation criteria.

To make the permutation criteria more practical, we borrow the idea from moment criteria. We find that the higher-order moments, $M_{2n}^\pi = \mathrm{tr}\big[(\mathcal{R}_\pi \mathcal{R}_\pi^\dagger)^n\big] = \sum_i \lambda_i^{2n}$ are much easier to access, according to Theorem 1. These permutation moments can help to lower bound $\|\mathcal{R}_\pi\| = \sum_i \lambda_i$ and thus infer whether the state is multipartite entangled or not. By changing the index permutation operation π and measuring different orders of moments, we generate a series of implementable multipartite entanglement criteria, which we call *moment-based permutation criterion*. The entanglement detection flowchart is shown in Fig. 1.

Theorem 1 *(Informal) Given a k-partite state ρ and the index permutation operation $\mathcal{R}_\pi$, the $2n$-th moment of $\mathcal{R}_\pi$, $M_{2n}^\pi := \mathrm{tr}\big[(\mathcal{R}_\pi \mathcal{R}_\pi^\dagger)^n\big]$, can be estimated by observable measurement on $2n$ copies of ρ,*

$$M_{2n}^\pi = \mathrm{tr}\left(O_{2n}^\pi \rho^{\otimes 2n}\right) = \frac{1}{2}\,\mathrm{tr}\left[\left(\bigotimes_{i=1}^{k} U_i^\pi + h.c.\right)\rho^{\otimes 2n}\right], \tag{2}$$

*xma@tsinghua.edu.cn

where U_i^π can be chosen from four different operators, $\overrightarrow{\Pi}_i, \overleftarrow{\Pi}_i, \mathbb{S}_i^{(2n,1)} \otimes \mathbb{S}_i^{(2,3)} \otimes \cdots \otimes \mathbb{S}_i^{(2n-2,2n-1)}$ and $\mathbb{S}_i^{(1,2)} \otimes \mathbb{S}_i^{(3,4)} \otimes \cdots \otimes \mathbb{S}_i^{(2n-1,2n)}$ depending on π. Here $\overrightarrow{\Pi}$ and $\overleftarrow{\Pi}$ are the cyclic permutation operators in different directions, satisfying $\overrightarrow{\Pi}\,|s_1, \cdots, s_{2n}\rangle = |s_{2n}, s_1, \cdots, s_{2n-1}\rangle$ and $\overleftarrow{\Pi}\,|s_1, \cdots, s_{2n}\rangle = |s_2, \cdots, s_{2n}, s_1\rangle$, $\mathbb{S}^{(u,v)}$ is the SWAP operator acting on the u-th and v-th copies.

However, Eq. (2) requires simultaneous preparation and operation of many copies of states, which is challenging for state-of-the-art devices. To solve this problem, we design protocols based on randomized measurements techniques to measure them, which only require single-copy state preparation and measurements. In the bipartite scenario, $M_n^{(1,2)} = \mathrm{tr}\left[(\mathcal{R}_{(1,2)})^n\right] = \mathrm{tr}\left[(\rho_{AB}^{T_A})^n\right]$ and $M_{2n}^{(2,3)}$ are key quantities that help to construct the weak-form PPT criteria [6, 7] and the criteria proposed later in Eq. (4) and Eq. (5), respectively. We list the sample complexities of measuring them using local or global randomized measurement techniques in Table 1, from which one could find that our new criteria have exponential advantages in sample complexity than those weak-form PPT criteria.

	Global Protocol	Local Protocol
$M_3^{(1,2)}$	$O(D^{\frac{2}{3}})$[8]	$O(D^2)$[6]
$M_4^{(2,3)}$	$O(D^{\frac{1}{2}})$	$O(D^{1.187})$

Table 1: This table shows the best-known sample complexities of measuring $M_3^{(1,2)}$ and the complexities of protocols developed in this work to measure $M_4^{(2,3)}$. D is the dimension of the underlying Hilbert space.

Adopting the Lagrange Multiplier Method, we can design a simple optimization problem to lower bound $\|\mathcal{R}_\pi\| = \sum_i \lambda_i$ using higher-order moments:

Theorem 2 *The minimum value of $\|\mathcal{R}_\pi\|$ given M_2^π, ..., M_{2n}^π is reached when there are at most n non-zero λ_is. Thus, the minimum value, denoted as $E_{2n}^\pi(\rho)$, can be evaluated by the following problem,*

$$\begin{aligned} \min_{q_1,\cdots,q_n\in\mathbb{N}} & E_{2n}^\pi(\rho) = q_1\lambda_1 + q_2\lambda_2 + \cdots + q_n\lambda_n \\ \text{s.t. } & \sum_{i=1}^n q_i\lambda_i^2 = M_2^\pi, \cdots, \sum_{i=1}^n q_i\lambda_i^{2n} = M_{2n}^\pi \\ & q_1 + q_2 + \cdots + q_n \le L, \end{aligned} \tag{3}$$

where L is the number of the singular values of $\mathcal{R}_\pi$.

As a special case, when we only know the value of M_2^π and M_4^π, the minimum of $\sum_i \lambda_i$ has an analytical form $E_4^\pi(\rho) = \sqrt{\frac{q(qM_2^\pi+U)}{q+1}} + \sqrt{\frac{M_2^\pi - U}{q+1}}$, where $q = \lfloor \frac{(M_2^\pi)^2}{M_4^\pi} \rfloor$ and $U = \sqrt{q(q+1)M_4^\pi - q(M_2^\pi)^2}$.

Now, we can formally represent the moment-based permutation criteria as

$$E_{2n}^\pi(\rho) \le 1\ ,\ \forall \pi \in \mathcal{S}_{2k}\ ,\ n \in \mathbb{N} \tag{4}$$

for all separable k-partite state ρ. In fact, $E_{2n}^\pi(\cdot)$ may not necessarily be the function of ρ. Adopting the bipartite entanglement criterion introduced in Ref. [3], we get

$$E_{2n}^{(2,3)}(\rho_{AB} - \rho_A \otimes \rho_B) \le \sqrt{(1 - \mathrm{tr}\,\rho_A^2)(1 - \mathrm{tr}\,\rho_B^2)} \tag{5}$$

for separable ρ_{AB}.

Compared with existing entanglement detection schemes based on partial transposed moments [6, 7], this framework is not only a direct generalization to multipartite entanglement, but also enhances the detection capability in the bipartite scenario. We prove that, with the second and fourth moments only, Eq. (5) can detect 3×3-dimensional bound entanglement [9].

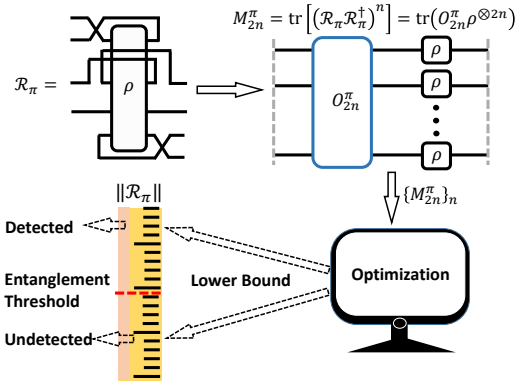


Figure 1: Flowchart of entanglement detection. To detect multipartite entanglement of ρ, one first chooses an index permutation operation π and sets $\|\mathcal{R}_\pi\|$ as the indicator. Then, one measures the permutation moments $\{M_{2n}^\pi\}_n$ to lower bound $\|\mathcal{R}_\pi\|$. If the lower bound is larger than the entanglement threshold set for $\|\mathcal{R}_\pi\|$, the multipartite entanglement is successfully detected. Otherwise, one can measure higher-order moments or pick another index permutation and repeat the procedure.

3 Bipartite Entanglement Detection

To investigate the detection capability of the moment-based permutation criteria in real physical systems, we choose a 10-qubit Ising model evolved under a long range XY Hamiltonian with open boundary condition, $H_{XY} = \sum_{i<j} J_{ij}(\hat{\sigma}_i^+\hat{\sigma}_j^- + \hat{\sigma}_i^-\hat{\sigma}_j^+) + B_z\sum_i \hat{\sigma}_i^z$. We divide the 10-qubit chain into three parts, A, B and C, where A and B constitute the local system we study, initialized to be $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes N_{AB}} + |1\rangle^{\otimes N_{AB}})$; C acts as the bath, which is initialized to be the tensor product of $|0\rangle$. We compare four implementable nonlinear criteria in detecting the entanglement within system AB. The first two criteria are Eq. (4) and Eq. (5), when setting $\pi = (2,3)$ and $n = 2$, labeled by $E_4^{(2,3)}$ and E_4^*, respectively. Others are the purity comparison criterion, labeled by P_2; and the weak-form PPT criterion based on $M_3^{(1,2)} = \mathrm{tr}\left[(\rho_{AB}^{T_A})^3\right]$ [7], labeled by P_3. The numerical simulation results in Fig. 2 shows that the moment-based permutation criteria have an obvious advantage since it detects entanglement

while all others fail in various time periods and different choices of A and B.

4 Multipartite Entanglement Detection

Another advantage of our framework lies in multipartite entanglement detection. There exist multipartite entangled states that are separable in any bipartition and thus cannot be detected by any criteria extended from the bipartite case, including the PPT and CCNR criteria. Theorem 2 provides us new means to design practical entanglement criteria for these states. We depict the sets of detectable multipartite entangled states of different criteria in Fig 2. In this work, we pick a three-qubit entangled state as an example. This state is separable in any bipartition while can be detected by Eq. (4) when setting $\pi = \binom{1,2,3,4,5,6}{1,3,2,4,5,6}$ and $n = 4$.

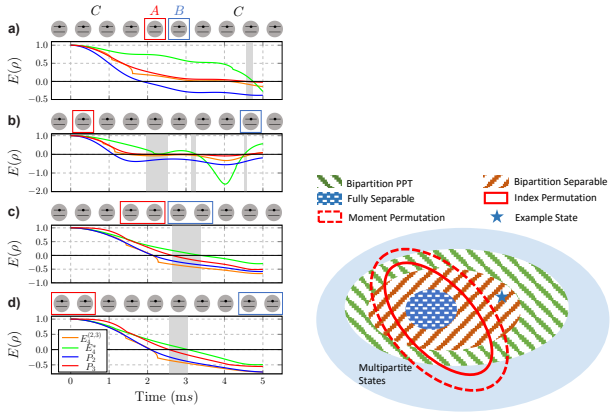


Figure 2: **Left:** We use four quantities to represent the four criteria, and the entanglement of AB is detected when the value is above zero for each criterion. The grey areas represent the time periods in which the entanglement can only be detected by the E_4^* criterion. **Right:** Illustration of different sets of detectable states. Bipartition PPT: PPT in any bipartition; Bipartition Separable: separable in any bipartition; Fully Separable: $\sum_i p_i \rho_1^i \otimes \cdots \otimes \rho_k^i$; Index Permutation: states that cannot be detected by an index permutation criterion other than the bipartite partial transposition; Moment Permutation: states that cannot be detected using finite numbers of permutation moments; Example State: a state that is separable in any bipartition while can be detected by a moment-based permutation criterion.

5 Other Remarks

As the quantity proposed in this work, $E_{2n}^{\pi}(\rho)$, has clear physical meaning, we conjecture that these quantities can be used as entanglement quantifiers. We prove this by showing that $E_{2n}^{\pi}(\rho)$ can be used to witness the entanglement phase transition in a many body localization system [1].

For multipartite quantum systems, entanglement can have a rather complex entanglement structure while the tools for detecting entanglement structure are quite restrictive. In this work, we also show that our framework can be generalized to detect the multipartite entanglement structure.

This work also inspires our new work about conformal field theory (CFT) [10], in which we use a new moment-based permutation criterion to quantify the entanglement between two disjoint intervals in one dimensional CFT. This is an open problem in CFT.

References

[1] Liu. Z. H. Detecting entanglement in quantum many-body systems via permutation moments Physical Review Letters, 2022, 129(26): 260501.

[2] Horodecki. M. Separability of mixed quantum states: linear contractions and permutation criteria Open Systems and Information Dynamics, 2006, 13: 103-111.

[3] Zhang. C. J. Entanglement detection beyond the computable cross-norm or realignment criterion. Physical Review A, 2008, 77(6): 060301.

[4] Peres. A. Separability criterion for density matrices. Physical Review Letters, 1996, 77(8): 1413.

[5] Chen. K. A matrix realignment method for recognizing entanglement. arXiv preprint quant-ph/0205017, 2002.

[6] Elben. A. Mixed-state entanglement from local randomized measurements. Physical Review Letters, 2020, 125(20): 200501.

[7] Yu. X. D. Optimal entanglement certification from moments of the partial transpose. Physical Review Letters, 2021, 127(6): 060504.

[8] Zhou. Y. Single-copies estimation of entanglement negativity. Physical Review Letters, 2020, 125(20): 200502.

[9] Bennett. C. H. Unextendible product bases and bound entanglement. Physical Review Letters, 1999, 82(26): 5385.

[10] Yin. C. Universal Entanglement and Correlation Measure in Two-Dimensional Conformal Field Theories. Physical Review Letters, 2023, 130(13): 131601.

Extended Abstract : Distilling nonlocality in quantum correlations

Sahil Gopalkrishna Naik,[1] Govind Lal Sidhardh,[1] Samrat Sen,[1] Arup Roy,[2] Ashutosh Rai,[3,4] and Manik Banik[1]

[1]*Department of Physics of Complex Systems, S.N. Bose National Center for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India.*
[2]*Department of Physics, A B N Seal College Cooch Behar, West Bengal 736101, India*
[3]*School of Electrical Engineering, Korea Advanced Institute of Science and Technology, Daejeon 34141, Republic of Korea*
[4]*Institute of Physics, Slovak Academy of Sciences, 845 11 Bratislava, Slovakia*

Abstract : Nonlocality, as established by seminal Bell's theorem, is considered to be the most striking feature of correlations present in space like separated events. Its practical application in device independent protocols, such as, secure key distribution, randomness certification *etc.*, demands identification and amplification of such correlations observed in quantum world. In this letter we study the prospect of nonlocality distillation, wherein, by applying a natural set of free operations (called wirings) on many copies of weakly nonlocal systems, one aims to generate correlations of higher nonlocal strength. In the simplest Bell scenario, we identify a protocol, namely logical OR-AND wiring, that can distil nonlocality to significantly high degree starting from arbitrarily weak quantum nonlocal correlations. As it turns out, our protocol has several interesting facets: (i) it demonstrates that set of distillable quantum correlations has non zero measure in the full eight dimensional correlation space, (ii) it can distil quantum Hardy correlations by preserving its structure, (iii) it shows that (nonlocal) quantum correlations sufficiently close to the local deterministic points can be distilled by a significant amount. Finally, we also demonstrate efficacy of the considered distillation protocol in detecting post quantum correlations.
Keywords : Quantum Correlations, Distillation , Nonlocality
Reference : Accepted in Phys. Rev. Lett. [arXiv:2208.13976v3]

Introduction: One of the most celebrated non-classical aspects of quantum mechanics was pioneered by J. S. Bell in the year 1964 [1] (see also [2]). Bell's theorem mandates departure of quantum theory from the *locally causal* world view which subsequently has been confirmed in several milestone experiments led by Clauser, Aspect, Zeilinger, and others [3–12]. Unlike other non-classical features, such as entanglement and coherence, study of nonlocality can be conducted in a device independent setting where only the input-output statistics of the device matters and one does not need to know the inner design or working mechanisms of the device [13]. Along with foundational implications, Bell nonlocality has also been identified as the necessary resource for several important protocols [14–25], which, thus, makes the question of refinement or distillation of this resource practically indispensable. Study of nonlocality distillation has two major implications – (i) practical: where one aims to distil nonlocal correlations observed in the quantum world which can be then applied to make information flow networks efficient and secure, and (ii) foundational: where the goal is to identify post quantum correlations, which, in turn, helps to understand the speciality of quantum theory among other possibilities allowed within the framework of generalized probabilistic theories. Interestingly, in Ref.[26], Forster *et al.* proposed a nonlocality distillation protocol that can extract nonlocality in stronger form starting with many copies of weakly nonlocal systems; this work has inspired a number of subsequent works consisting of interesting results on nonlocality distillation [27–41].

The research conducted so far on nonlocality

distillation is mainly focused on distilling post quantum correlations [27–32, 34–39]. Only a few protocols are known that successfully distil some quantum correlations [26, 39]. The difficulty arises due to the top-down approach considered in earlier works where one starts with some parametric family of generic no-signaling (NS) correlations, and after obtaining a successful distillation protocol the aim is to check whether for some range of the parameter values the considered NS correlations allow quantum realization or not. For the simplest bipartite case, the well known analytical criterion by Tsirelson-Landau-Masanes [42–44] and the Navascues-Pironio-Acin (NPA) criterion [45], and in general case a hierarchy of semi-definite programming conditions [46] can serve this purpose. Only in some fortunate cases sophisticated choices of the parametric class of NS correlations might lead to a desirable subset of quantum realizable correlations. However, the approach has severe pitfall when more input-output scenarios are considered, as the recent mathematical breakthrough by W. Slofstra and the subsequent results establish that the set of quantum correlations is not topologically closed [47–49]. There are only a few results that report distillation of nonlocal correlations within quantum setup [26, 39], albeit the nonlocal strength of the distilled correlation is low. Therefore the aspects of analytical and quantitative study for distillation of quantum nonlocal correlations remain open.

In this letter we primarily focus to address the former aspect of nonlocality distillation, *i.e.*, we intend to find out efficient distillation protocol(s) for quantum correlations. Interestingly, we identify a simple protocol and come up with a generic approach that successfully distil nonlocality in a large class of weakly nonlocal quantum correlations. Towards this goal, first we consider a variant of nonlocality test proposed by Lucien Hardy [50]. Success probability in Hardy's test qualifies as a measure of nonlocality for Hardy's correlations [51]. Given two copies of a quantum Hardy correlation, we show that there exists a simple wiring that can distil Hardy nonlocality. We call this wiring logical OR-AND protocol, where OR ($\vee$) and AND ($\wedge$) functions on 2-bits z_1, z_2 are defined as $\vee(z_1, z_2) = \max\{z_1, z_2\}$ and $\wedge(z_1, z_2) = \min\{z_1, z_2\}$, respectively.

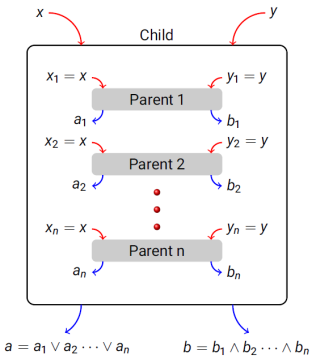


Figure 1. Multi-copy OR-AND wiring. Given n-number of parent correlations $\{\mathrm{P}_{NS}[i]\}_{i=1}^{n} \subset \mathcal{NS}$, the OR-AND wiring produce a child correlation $\mathrm{P}_{NS}^{(n)} \in \mathcal{NS}$. The outcome a on Alice's side for the child box is obtained as, $a = a_1 \vee \cdots \vee a_n = \max\{a_1, \cdots, a_n\}$ for the input $x_1 = \cdots = x_n = x$, where x_i and a_i are the input and output of the i^{th} parent. On the Bob's side, $y_1 = \cdots = y_n = y$ and $b = b_1 \wedge \cdots \wedge b_n = \min\{b_1, \cdots, b_n\}$.

The OR-AND protocol allows an immediate n-copy generalization , which can provide a substantial distillation of Hardy's success with a sufficiently large copies of initial correlations. Further, we show that the OR-AND wiring when applied to a broader class of quantum correlations yields an interesting result: an arbitrarily small violation of the Clauser-Horne-Shimony-Holt (CHSH) [3] inequality can be amplified to a significantly higher degree. Finally, by applying our protocol we demonstrate that nonlocal correlations arbitrarily close to the extreme points of the set of local correlations are always distilled, which, in turn, establishes that set of distillable quantum correlations has non-zero measure in the full eight dimensions of the correlation space. We also study distillation of post quantum correlations, and show that OR-AND protocol becomes efficient there too. In particular, we find correlations whose

post-quantum signature is established through OR-AND distillation, while the known information principles, such as nontrivial communication complexity [52] and information causality [53, 54], fail to serve the purpose.

Results:

Theorem 1. *The OR-AND wiring preserves the structure of quantum Hardy correlations and can efficiently distil the strength of success probability in Hardy's test of nonlocality.*

Theorem 2. *Starting with a quantum correlation with arbitrarily small CHSH nonlocality OR-AND wiring can yield Tsirelson gain up to* $(\approx)$ 39.75%.

Theorem 3. *CHSH nonlocality of any no-singling correlation of the form* $\tilde{\mathrm{C}}(\lambda) = \lambda \mathrm{C} + (1-\lambda)P_{L_1}$, *where* $0 < \lambda \leq 1$ *and* $\mathrm{C} \in \mathrm{ConvexHull}\ \{\mathrm{P}_{NL}, \mathrm{P}_{L_i} \mid i \in \{1, \cdots, 8\}\}$ *can be distilled through OR-AND wiring by choosing the values of* λ *sufficiently small. Furthermore,* 2*-copy OR-AND distillation is successful for all the* $\tilde{C}(\lambda)$ *correlation boxes whenever* $\lambda < \frac{2}{3}c_0$*; where* c_0 *is the* P_{NL} *fraction in* C.

Theorem 3 has profound topological implication. It establishes that the sets of no-signalling as well as quantum correlations allowing nonlocality distillation have non-zero measure in the full eight dimensional correlation space. Furthermore, it should be mentioned that the correlation box P_{L_1} appearing in Theorem 3 is not any special local deterministic box: the result holds also for all the remaining 15 local deterministic boxes on suitable relabeling of the OR-AND wiring.

Distillation of post-quantum nonlocality:

We point out that checking membership to the different levels of NPA hierarchy can become computationally expensive, particularly at higher levels of the hierarchy, whereas the distillation criteria can be far more computationally tractable. We have given an example of a correlation, that is post-quantum by observing that after 2-copy distillation using OR-AND protocol, the Hardy success goes up to 0.0925 (a value beyond the maximum possible success probaility in quantum mechanics). On the other hand, for the considered correlation, tests, like known necessary conditions for violating non-trivial computational complexity [52] (see also [63–65]) and information causality principle[53, 54], fail to detect its post-quantumness. On considering NPA criteria, a membership test into the second tier of the NPA hierarchy is required to establish the post-quantumness of this correlation. Along similar lines, one may imagine post-quantum correlations like the one discussed, which lie at further deeper levels of the NPA-hierarchy, while its post-quantumness may be conveniently detected via efficient nonlocality distillation protocols.

Discussion.– In this letter, we have established a generic approach for distillation of nonlocal correlations arising in quantum mechanics. This problem is of utmost importance as Bell nonlocal correlations are ubiquitous in device independent protocols – more the nonlocality more the utility. Interestingly, we come up with an elegant protocol, the OR-AND wiring, that distils nonlocality in quantum correlations with high efficiency. In the simplest bipartite scenario, in stark distinction with the results reported prior to our work [26–41], our protocol establishes that, within the set of full eight dimensional correlation space, the distillable quantum as well as no-signaling nonlocal correlations form subsets of non-zero measures; i.e., sector of open balls of a specified radius centered at local deterministic correlations. Moreover, by considering correlations arbitrarily close to local deterministic points, applying our protocol, with optimal number of copies, one can distill nonlocality by a significant amount both for the quantum as well as post-quantum nonsignaling correlations. As for future, it would be interesting to explore the full potential of our generic framework proposed here in distilling quantum nonlocal correlations. In particular, obtaining some bound on the relative volume of the quantum correlations in the correlation space that can be distilled under OR-AND wiring would be interesting. Furthermore a generalization of this protocol for higher input-output

as well as in multiparty scenario might be of great use.

[1] J. S. Bell; On the Einstein Podolsky Rosen paradox, Physics Physique Fizika **1**, 195 (1964).

[2] J. S. Bell; On the Problem of Hidden Variables in Quantum Mechanics, Rev. Mod. Phys. **38**, 447 (1966); N. D. Mermin; Hidden variables and the two theorems of John Bell, Rev. Mod. Phys. **65**, 803 (1993); N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner; Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt; Proposed Experiment to Test Local Hidden-Variable Theories Phys. Rev. Lett. **23**, 880 (1969).

[4] S. J. Freedman and J. F. Clauser; Experimental Test of Local Hidden-Variable Theories, Phys. Rev. Lett. **28**, 938 (1972).

[5] A. Aspect; Proposed experiment to test the nonseparability of quantum mechanics, Phys. Rev. D **14**, 1944 (1976).

[6] A. Aspect, P. Grangier, and G. Roger; Experimental Tests of Realistic Local Theories via Bell's Theorem, Phys. Rev. Lett. **47**, 460 (1981).

[7] A. Aspect, P. Grangier, and G. Roger; Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities, Phys. Rev. Lett. **49**, 91 (1982).

[8] A. Aspect, J. Dalibard, and G. Roger; Experimental Test of Bell's Inequalities Using Time-Varying Analyzers, Phys. Rev. Lett. **49**, 1804 (1982).

[9] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert; "Event-ready-detectors" Bell experiment via entanglement swapping, Phys. Rev. Lett. **71**, 4287 (1993).

[10] Jian-Wei Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger; Experimental Entanglement Swapping: Entangling Photons That Never Interacted, Phys. Rev. Lett. **80**, 3891 (1998).

[11] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger; Violation of Bell's Inequality under Strict Einstein Locality Conditions, Phys. Rev. Lett. **81**, 5039 (1998).

[12] D. Bouwmeester, Jian-Wei Pan, M. Daniell, H. Weinfurter, and A. Zeilinger; Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement, Phys. Rev. Lett. **82**, 1345 (1999).

[13] V. Scarani; The device-independent outlook on quantum physics (lecture notes on the power of Bell's theorem), Acta Physica Slovaca **62**, 347 (2012) [see also arXiv:1303.3081 [quant-ph]].

[14] A. K. Ekert; Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[15] J. Barrett, L. Hardy, and A. Kent; No Signaling and Quantum Key Distribution, Phys. Rev. Lett. **95**, 010503 (2005).

[16] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani; Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).

[17] S. Pironio, A. Acín, S Massar *et al.* Random numbers certified by Bell's theorem, Nature **464**, 1021 (2010).

[18] R. Colbeck and A. Kent; Private Randomness Expansion With Untrusted Devices, J. Phys. A: Math. Theo. **44**, 095305 (2011).

[19] R. Colbeck and R. Renner; Free randomness can be amplified, Nature Phys **8**, 450 (2012).

[20] A. Chaturvedi and M. Banik; Measurement-device-independent randomness from local entangled states, EPL **112**, 30003 (2015).

[21] A. Mukherjee, A. Roy, S. S. Bhattacharya, S. Das, Md. R. Gazi, and M. Banik; Hardy's test as a device-independent dimension witness, Phys. Rev. A **92**, 022302 (2015).

[22] A. Pappa, N. Kumar, T. Lawson, M. Santha, S. Zhang, E. Diamanti, and I. Kerenidis; Nonlocality and Conflicting Interest Games, Phys. Rev. Lett. **114**, 020401 (2015).

[23] A. Roy, A. Mukherjee, T. Guha, S. Ghosh, S. S. Bhattacharya, and M. Banik; Nonlocal correlations: Fair and unfair strategies in Bayesian games, Phys. Rev. A **94**, 032120

(2016).
[24] P. E. Frenkel and M. Weiner; On entanglement assistance to a noiseless classical channel, Quantum **6**, 662 (2022).
[25] R. K. Patra, S. G. Naik, E. P. Lobo, S. Sen, T. Guha, S. S. Bhattacharya, M. Alimuddin, and M. Banik; Classical superdense coding and communication advantage of a single quantum, arXiv.2202.06796.
[26] M. Forster, S. Winkler, and S. Wolf; Distilling Nonlocality, Phys. Rev. Lett. **102**, 120401 (2009).
[27] N. Brunner and P. Skrzypczyk; Nonlocality Distillation and Postquantum Theories with Trivial Communication Complexity, Phys. Rev. Lett. **102**, 160403 (2009).
[28] A. J. Short; No Deterministic Purification for Two Copies of a Noisy Entangled State, Phys. Rev. Lett. **102**, 180502 (2009).
[29] P. Høyer and J. Rashid; Optimal protocols for nonlocality distillation, Phys. Rev. A **82**, 042118 (2010).
[30] N. Brunner, D. Cavalcanti, A. Salles, and P. Skrzypczyk; Bound Nonlocality and Activation, Phys. Rev. Lett. **106**, 020402 (2011).
[31] M. Forster; Bounds for nonlocality distillation protocols, Phys. Rev. A **83**, 062114 (2011).
[32] J. Rashid; Limits and consequences of nonlocality distillation, PhD Thesis, University of Calgary (2012).
[33] P. Høyer and J. Rashid; Quantum nonlocal boxes exhibit stronger distillability, Mod. Phys. Lett. A **28**, 1330012 (2013).
[34] H. Ebbe and S. Wolf; Multi-User Non-Locality Amplification, IEEE Trans. Inf. Theory **60**, 1159 (2014).
[35] J. Tuziemski and K. Horodecki; On the non-locality of tripartite non-singaling boxes emerging from wirings, Quantum Inf. Comput. **15**, 1081 (2015).
[36] S. Beigi and A. Gohari; Monotone Measures for Non-Local Correlations, IEEE Trans. Inf. Theory **61**, 5185 (2015).
[37] G. Brassard, B. Salwey, and S. Wolf; Non-locality distillation as cryptographic game, IEEE Information Theory Workshop (2015).
[38] S. G. A. Brito, M. G. M. Moreno, A. Rai, and R. Chaves; Nonlocality distillation and quantum voids, Phys. Rev. A **100**, 012102 (2019).
[39] G. Eftaxias, M. Weilenmann, and R. Colbeck; Advantages of multi-copy nonlocality distillation and its application to minimizing communication complexity, Phys. Rev. Lett. **130**, 100201 (2023) [Also at arXiv:2206.02817 [quant-ph]].
[40] J. Allcock, N. Brunner, N. Linden, S. Popescu, P. Skrzypczyk, and T.s Vértesi; Closed sets of nonlocal correlations, Phys. Rev. A **80**, 062107 (2009).
[41] B. Lang, T. Vertesi, and M. Navascues; Closed sets of correlations: answers from the zoo, J. Phys. A: Math. Theo. **47**, 424029 (2014).
[42] B. S. Tsirel'son; Quantum analogues of the Bell inequalities. The case of two spatially separated domains, J. Math. Sci. **36**, 557 (1987).
[43] L. J. Landau; Empirical two-point correlation functions, Found. Phys. **18**, 449 (1988).
[44] Ll. Masanes; Necessary and sufficient condition for quantum-generated correlations, arXiv:quant-ph/0309137.
[45] M. Navascués, S. Pironio, and A. Acín; Bounding the Set of Quantum Correlations, Phys. Rev. Lett. **98**, 010401 (2007).
[46] M. Navascués, S. Pironio, and A. Acín; A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys. **10**, 073013 (2008).
[47] W. Slofstra; Tsirelson's problem and an embedding theorem for groups arising from non-local games, J. Amer. Math. Soc. **33**, 1 (2020).
[48] W. Slofstra; The set of quantum Correlations is not closed, Forum of Mathematics, Pi, 7, E1 (2019).
[49] K. Dykema, V. I. Paulsen, and J. Prakash; Non-closure of the Set of Quantum Correlations via Graphs, Commun. Math. Phys. **365**, 1125 (2019).
[50] L. Hardy; Nonlocality for two particles without inequalities for almost all entangled states, Phys. Rev. Lett. **71**, 1665 (1993).
[51] J. L. Cereceda; Quantum mechanical probabilities and general probabilistic constraints for Einstein-Podolsky-Rosen-Bohm experiments, Found. Phys. Lett. **13**, 427 (2000).
[52] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger; Limit

on Nonlocality in Any World in Which Communication Complexity Is Not Trivial, Phys. Rev. Lett. **96**, 250401 (2005).

[53] M. Pawłowski, T. Paterek, D. Kaszlikowski *et al*. Information causality as a physical principle, Nature **461**, 1101 (2009).

[54] N. Miklin and M. Pawłowski; Information Causality without Concatenation, Phys. Rev. Lett. **126**, 220403 (2021).

[55] J. Barrett, N.Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts; Nonlocal correlations as an information-theoretic resource, Phys. Rev. A **71**, 022101 (2005).

[56] S. Popescu and D. Rohrlich; Quantum nonlocality as an axiom, Found. Phys. **24**, 379 (1994).

[57] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani; Geometry of the set of quantum correlations, Phys. Rev. A **97**, 022104 (2018).

[58] A. Rai, C. Duarte, S. Brito, and R. Chaves; Geometry of the quantum set on no-signaling faces, Phys. Rev. A **99**, 032106 (2019).

[59] R. Rabelo, L. Y. Zhi, and V. Scarani; Device-Independent Bounds for Hardy's Experiment, Phys. Rev. Lett. **109**, 180401 (2012).

[60] K. P. Seshadreesan and S. Ghosh; Constancy of maximal nonlocal probability in Hardy's nonlocality test for bipartite quantum systems, J. Phys. A: Math. .Theo. **44**, 315305 (2011).

[61] A. Rai, M. Pivoluska, S. Sasmal, M. Banik, S. Ghosh, and M. Plesch; Self-testing quantum states via nonmaximal violation in Hardy's test of nonlocality, Phys. Rev. A **105**, 052227 (2022).

[62] B. S. Cirel'son; Quantum generalizations of Bell's inequality, Lett. Math. Phys. **4**, 93 (1980).

[63] W. van Dam; Implausible consequences of superstrong nonlocality, Nat. Comput. **12**, 9 (2013) [see also arXiv:quant-ph/0501159].

[64] G. Brassard; Is information the key?. Nature Phys. **1**, 2 (2005).

[65] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf; Nonlocality and communication complexity, Rev. Mod. Phys. **82**, 665 (2010).

[66] M. Navascues and H. Wunderlich; A glance beyond the quantum model, Proc. Roy. Soc. Lond. **A466**, 881 (2009).

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

[68] J. I de Vicente; On nonlocality as a resource theory and nonlocality measures, J. Phys. A: Math. Theor. **47**, 424017 (2014).

[69] E. Wolfe, D. Schmid, A.B. Sainz, R. Kunjwal, and R.W. Spekkens; Quantifying Bell: the Resource Theory of Nonclassicality of Common-Cause Boxes, Quantum **4**, 280 (2020).

[70] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters; Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett. **76**, 722 (1996); C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher; Concentrating partial entanglement by local operations, Phys. Rev. A **53**, 2046 (1996).

Thermodynamically ideal quantum-state inputs to any device

Paul M. Riechers[1] * Chaitanya Gupta[2] Artemy Kolchinsky[3] Mile Gu[4 5 6]

[1] *Beyond Institute for Theoretical Science, San Francisco, CA, USA*
[2] *Department of Applied Mathematics and Theoretical Physics, University of Cambridge, UK*
[3] *Universal Biology Institute, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan*
[4] *Nanyang Quantum Hub, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore*
[5] *CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, Singapore 117543, Singapore*
[6] *Centre for Quantum Technologies, National University of Singapore, Singapore*

Abstract. We investigate and ascertain the ideal inputs to any finite-time quantum thermodynamic process. We demonstrate that the expectation values of entropy flow, heat, and work can all be determined via Hermitian observables of the initial state. These Hermitian operators encapsulate the breadth of behavior and the ideal inputs for common thermodynamic objectives. We show how to construct these Hermitian operators from measurements of thermodynamic output from a finite number of effectively arbitrary inputs. Behavior of a small number of test inputs thus determines the full range of thermodynamic behavior from all quantum states.

Keywords: quantum thermodynamics, dissipation, generalized Bloch vectors, optimization

1 Introduction

Throughout its history, thermodynamics primarily investigated the efficiency of various control processes for implementing a desired functionality. However, the complementary question of *which initial physical states produce the best thermodynamic behavior* remains relatively unexplored. Indeed, there is a historical reason for this: In equilibrium transformations, the system always stays infinitesimally close to equilibrium, so there is no sense in asking about alternative inputs to the process. Yet modern devices transform quantum and classical system rapidly. These finite-time nonequilibrium transformations have highly non-trivial initial-state dependence. Here we explore the ideal thermodynamic inputs to such devices, where the system can be arbitrarily far from equilibrium throughout the transformation.

The initial-state dependence of entropy production and associated thermodynamic quantities has been explored only recently in relation to the ideal inputs, via mismatch costs [1, 2, 3, 4]. However, the minimally dissipative input was only characterized in the case of reset processes [3, 4] and, even then, a construction was only given for qubits [3]. In the following, we constructively identify the thermodynamically ideal inputs for a much broader class of objectives, including heat minimization, maximizing work extraction, and maximizing gain in free energy. Moreover, the ideal inputs are characterized and constructively identified for systems of arbitrary finite dimensions, for any finite-time process. The results thus apply broadly to quantum processes—whether minimizing decoherence or optimizing for energetic efficiency—wherever finite-time thermodynamics is relevant.

*pmriechers@gmail.com

2 Framework

Expectation values in quantum thermodynamics typically either take the form of a linear functional

$$\langle X \rangle_{\rho_0} = \mathrm{tr}(\rho_0 \mathcal{X}) \ , \tag{1}$$

or a particular type of nonlinear function involving a change in von Neumann entropy

$$f_{\rho_0}^{(\mathcal{X})} := \mathrm{tr}(\rho_0 \mathcal{X}) + S(\rho_\tau) - S(\rho_0) \ . \tag{2}$$

Through our study, we discover the optimal initial state that extremizes these quantities in general.

Any density matrix of a d-dimensional quantum system has a unique decomposition in any traceless and mutually orthogonal Hermitian operator basis $\vec{\Gamma} = (\Gamma_1, \Gamma_2, \ldots \Gamma_{d^2-1})$ with $\mathrm{tr}(\Gamma_m \Gamma_n) = \eta \, \delta_{m,n}$, described by the *generalized Bloch vector* $\vec{b}_t \in \mathbb{R}^{d^2-1}$ via

$$\rho_t = I/d + \vec{b}_t \cdot \vec{\Gamma} \ . \tag{3}$$

Leveraging this general Bloch decomposition of the initial state, we find that we can express each expectation value in Eq. (1) as

$$\langle X \rangle_{\rho_0} = \langle X \rangle_{I/d} + \vec{b}_0 \cdot \vec{x} \ , \tag{4}$$

where $\vec{x} \in \mathbb{R}^{d^2-1}$ is the relevant *thermodynamic vector*

$$\vec{x} = \mathrm{tr}(\vec{\Gamma} \mathcal{X}) \ . \tag{5}$$

Conversely, the thermodynamic operators can be constructed from the thermodynamic vectors:

$$\mathcal{X} = \langle X \rangle_{I/d} \, I + \vec{x} \cdot \vec{\Gamma} / \eta \ . \tag{6}$$

We find that both $\langle X \rangle_{I/d}$ and the thermodynamic vector $\vec{x}$ can be obtained linear algebraically from experimental measurements of thermodynamic output from a

finite number of almost arbitrary inputs. Via Eq. (6), this allows us to experimentally reconstruct the thermodynamic operators from observations of any process.

Crucially, *we have derived several theorems and several algorithms that show how to obtain the ideal quantum inputs either analytically or numerically from the Hermitian thermodynamic operator* $\mathcal{X}$ [5].

3 Example: Nonequilibrium thermodynamics of a qubit-reset device

Quantum computing requires a mechanism for resetting each qubit to the computational-basis state $|0\rangle = \sigma_z |0\rangle$. Different implementations of the same task will however have distinct sets of thermodynamically ideal inputs. Nonequilibrium thermodynamic quantities are determined less by *what* you do than *how* you do it.

For a paradigmatic illustration of our results, we consider a device for qubit reset that works by changing both the energy gap and spatial orientation of the energy eigenstates of the qubit, while the qubit is weakly coupled to a thermal environment.

To determine how the device's thermodynamic behavior depends on the input state, we track the evolution of four randomly sampled initial density matrices, together with the thermodynamic output from each of these four inputs. From the matrix of Bloch vectors and the measured thermodynamic output, we construct the Hermitian thermodynamic operators. The expected-heat and expected-work operators, $\mathcal{Q}$ and $\mathcal{W}$, allow us to determine (i) the ideal inputs leading to minimal and maximal heat and work, and (ii) the full range of heat and work that can be attained by *any* input to the device. These are obtained from the extremal eigenvalues and associated eigenstates of the thermodynamic operators.

Diversity among ideal inputs for thermodynamic objectives Simple combination and manipulation of the heat and work operators reveals the diversity of ideal inputs for a multitude of different thermodynamic objectives, as shown in Fig. 1.

In this example, with a single environmental bath at constant temperature T, entropy flow to the environment is simply related to heat out of the system via $\Phi = -Q/T$. The expected-entropy-flow operator is thus simply related to the expected-heat operator in this case, via $\mathbf{\Phi} = -\mathcal{Q}/T$. Meanwhile, the expected-energy-change operator is simply $\mathcal{Q} + \mathcal{W}$.

Bounding the behavior of all inputs Continuing our example of the qubit-reset dynamics, we now leverage our results to identify the extremal thermodynamic behavior that can be attained by any input throughout the process.

Fig. 2 demonstrates that thermodynamic observations from just four inputs yield the full range of thermodynamic behavior from any input. For example, the min and max expected work at any time $t \in [0, \tau]$, obtainable from alternative inputs, is determined by the expected-work operator at that time. The expected-work operator at any time is constructed from the expected work performed on each of the four test inputs up to that time. Determining the ranges of work, energy change, and heat thus reduces to determining eigenvalue ranges of the respective Hermitian operators.

Determining the range of entropy production throughout the process is somewhat more complicated, although it still only requires the data from four test inputs. Notably, in the bottom panel of Fig. 2, we find the states of minimal and maximal entropy production at times before the state is fully reset. This employs the novel gradient-descent algorithm that we developed on the manifold of density matrices for quantum systems of any dimension.

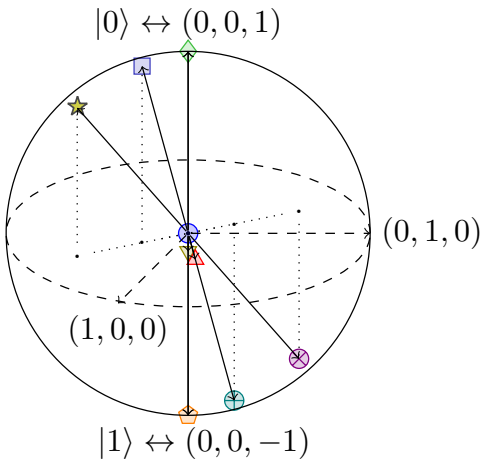
4 Summary of Results

For any process, entropy flow, heat, and work can all be extremized by pure input states—eigenstates of the respective operators. In contrast, the input states that minimize entropy production or maximize the change in free energy are non-pure mixed states obtained from the operators as the solution of a convex optimization problem. To attain these, we provide an easily implementable gradient descent method on the manifold of density matrices, where an analytic solution yields a valid direction of descent at each iterative step. Ideal inputs within a limited domain, and their associated thermodynamic operators, are easily obtained. This allows analysis of ideal thermodynamic inputs within quantum subspaces of infinite-dimensional quantum systems; it also allows analysis of ideal inputs in the classical limit. Our examples illustrate the diversity of 'ideal' inputs: Distinct initial states minimize entropy production, extremize the change in free energy, and maximize work extraction.

5 Conclusion

We have determined the ideal inputs that minimize or maximize various thermodynamic quantities for any fixed process that transforms a physical system in finite time. Many of these optimal inputs turn out to be pure states corresponding to eigenstates of Hermitian thermodynamic operators. We showed how to reconstruct these operators via observed behavior from a finite number of experimentally accessible input states. Another class of thermodynamic quantities, based on entropies, have mixed-state minimizers but pure-state maximizers. The Hermitian thermodynamic operators determine these ideal states too. Our examples illustrate the incompatibility of common objectives: The 'ideal' input depends on whether one intends to minimize heat, minimize entropy production, maximize free-energy gain, maximize work extraction, etc.

This investigation of ideal initial states complements the centuries-old tradition of rather seeking ideal protocols with an assumed initial state. Whether or not a protocol is ideal, our results highlight the initial-state dependence of a device's performance across thermodynamic metrics, and expose the breadth of its possible behavior. While we emphasized thermodynamics, the



Objective		Ideal input	
min entropy production	$\text{argmin}_{\rho_0} \langle \Sigma \rangle_{\rho_0}$	mixed	$\vec{a}_0 \approx (-0.02, 0.03, -0.15)$
max free-energy gain	$\text{argmax}_{\rho_0} \Delta \mathcal{F}_t$	mixed	$\vec{a}_0 \approx (0, 0, -0.10)$
min entropy change	$\text{argmax}_{\rho_0} \Delta S_t$	mixed	$\vec{a}_0 = (0, 0, 0)$
max heat exhausted max entropy production max entropy flow	$\text{argmax}_{\rho_0} \langle -Q \rangle_{\rho_0} =$ $\text{argmax}_{\rho_0} \langle \Sigma \rangle_{\rho_0} =$ $\text{argmax}_{\rho_0} \langle \Phi \rangle_{\rho_0}$	pure	$\vec{a}_0 \approx (0.13, -0.20, 0.97)$
min heat exhausted min entropy flow	$\text{argmin}_{\rho_0} \langle -Q \rangle_{\rho_0} =$ $\text{argmin}_{\rho_0} \langle \Phi \rangle_{\rho_0}$	pure	$\vec{a}_0 \approx (-0.13, 0.20, -0.97)$
min free-energy change min energy change	$\text{argmin}_{\rho_0} \Delta \mathcal{F}_t =$ $\text{argmin}_{\rho_0} \langle Q + W \rangle_{\rho_0}$	pure	$\vec{a}_0 \approx (0, 0, 1)$
max energy change	$\text{argmax}_{\rho_0} \langle Q + W \rangle_{\rho_0}$	pure	$\vec{a}_0 \approx (0, 0, -1)$
min work	$\text{argmin}_{\rho_0} \langle W \rangle_{\rho_0}$	pure	$\vec{a}_0 \approx (-0.32, 0.49, -0.81)$
max work	$\text{argmax}_{\rho_0} \langle W \rangle_{\rho_0}$	pure	$\vec{a}_0 \approx (0.32, -0.49, 0.81)$
max entropy change	$\text{argmax}_{\rho_0} \Delta S_t$	pure	anywhere on Bloch shell

Figure 1: Diversity of ideal inputs for a finite-time qubit-reset process, displayed on and in the Bloch sphere. The states extremizing heat, work, and energy-change all lie on the surface of the Bloch sphere, in the direction of a maximal eigenstate of the corresponding thermodynamic operators. The entire surface of the Bloch sphere maximizes entropy gain. Minimal entropy production and maximal free energy gain are achieved by non-trivial mixed-state inputs. The change in entropy is minimized by the fully-mixed input. Entropy production is maximized by the same pure-state input that maximizes heat exhaustion. The greatest loss of free energy occurs for the same pure-state input that loses the most energy.

results of this paper extend easily to other domains—where the ideal inputs, as judged by some other criteria, like maximizing the yield of a desired quantum output state [6], will be obtained from the linear operators induced by those criteria.

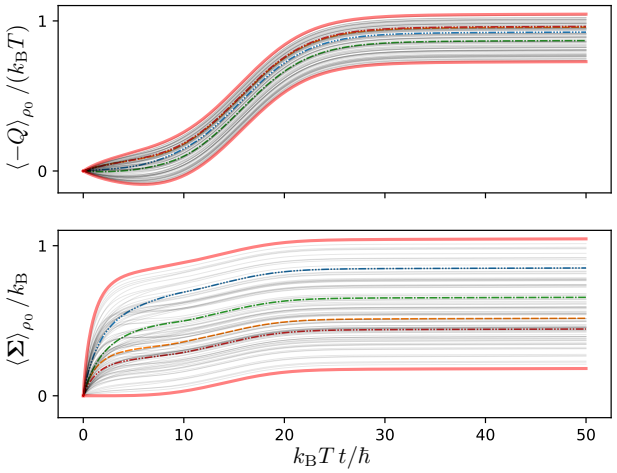


Figure 2: Tracking the behavior of four inputs is enough to bound the behavior of all other inputs to a qubit process. Here we show the the range of expectation values for exhausted heat and entropy production throughout a finite-time qubit-reset process. The expectation values from four random inputs are shown as dashed lines. This allows construction of the thermodynamic operator $\mathcal{Q}$ throughout time. (top) Maximal and minimal heat, corresponding to extremal eigenvalues of $\mathcal{Q}$, shown as thick red solid lines; (bottom) Maximal and minimal entropy production, obtained from gradient descent/ascent, shown as thick red solid lines. These extrema bound the behavior of all other inputs, including the behavior of 100 other random initial conditions shown as thin gray lines.

References

[1] A. Kolchinsky and D. H. Wolpert. Dependence of dissipation on the initial distribution over states. *Journal of Statistical Mechanics: Theory and Experiment*, 2017(8):083202, 2017.

[2] P. M. Riechers and M. Gu. Initial-state dependence of thermodynamic dissipation for any quantum process. *Phys. Rev. E*, 103:042145, Apr 2021.

[3] P. M. Riechers and M. Gu. Impossibility of achieving Landauer's bound for almost every quantum state. *Phys. Rev. A*, 104:012214, Jul 2021.

[4] A. Kolchinsky and D. H. Wolpert. Dependence of integrated, instantaneous, and fluctuating entropy production on the initial state in quantum and classical processes. *Phys. Rev. E*, 104:054107, Nov 2021.

[5] P. M. Riechers and C. Gupta and A. Kolchinsky and M. Gu. Thermodynamically ideal quantum-state inputs to any device. arXiv 2305.00616

[6] N. Yunger Halpern and D. T. Limmer. Fundamental limitations on photoisomerization from thermodynamic resource theories. *Physical Review A*, 101(4):042116, 2020.

Quantum dichotomies and coherent thermodynamics beyond first-order asymptotics

P. Lipka-Bartosik, C.T. Chubb, J.M. Renes, M. Tomamichel, K. Korzekwa

May 22, 2023

We address the problem of exact and approximate transformation of quantum dichotomies in the asymptotic regime, i.e., the existence of a quantum channel $\mathcal{E}$ mapping $\rho_1^{\otimes n}$ into $\rho_2^{\otimes R_n n}$ with an error ϵ_n (measured by trace distance) and $\sigma_1^{\otimes n}$ into $\sigma_2^{\otimes R_n n}$ exactly, for a large number n. We derive second order asymptotic expressions for the optimal transformation rate R_n in the small, moderate, large and zero-error regimes for an arbitrary pair (ρ_1, σ_1) of initial states and a commuting pair (ρ_2, σ_2) of final states. We also prove that for σ_1 and σ_2 given by thermal Gibbs states, the derived optimal transformation rates in the first three regimes can be attained by thermal operations. This allows us, for the first time, to study the second order asymptotics of thermodynamic state interconversion with fully general initial states that may have coherence between different energy eigenspaces. Thus, we discuss the optimal performance of thermodynamic protocols with coherent inputs and describe three novel resonance phenomena allowing one to significantly reduce transformation errors induced by finite-size effects. What is more, our result on quantum dichotomies can also be used to obtain, up to second order asymptotic terms, optimal conversion rates between pure bipartite entangled states under local operations and classical communication.

Introduction: One of the fundamental questions in quantum statistical inference is whether one quantum dichotomy, i.e., a pair of quantum states (ρ_1, σ_1), can be transformed into another one, (ρ_2, σ_2), using a quantum channel. In other words, whether there exists a completely positive trace-preserving map $\mathcal{E}$ such that $\rho_2 = \mathcal{E}(\rho_1)$ and $\sigma_2 = \mathcal{E}(\sigma_1)$. If so, we write $(\rho_1, \sigma_1) \succ (\rho_2, \sigma_2)$. We can further relax this condition by requiring that the two states are only reproduced approximately by the channel. That is, we write $(\rho_1, \sigma_1) \succ_{(\epsilon_\rho, \epsilon_\sigma)} (\rho_2, \sigma_2)$ if and only if there exists a quantum channel $\mathcal{E}$ such that

$$\|\mathcal{E}(\rho_1) - \rho_2\|_{\mathrm{tr}} \leq \epsilon_\rho \quad \text{and} \quad \|\mathcal{E}(\sigma_1) - \sigma_2\|_{\mathrm{tr}} \leq \epsilon_\sigma, \tag{1}$$

where $\|X\|_{\mathrm{tr}} = \frac{1}{2}\mathrm{tr}|X|$ denotes the trace distance. For the commuting case, when $[\rho_1, \sigma_1] = [\rho_2, \sigma_2] = 0$, the necessary and sufficient conditions for the existence of such a channel are known and captured by the seminal result of Blackwell [1]. However, such conditions in the general non-commutative case so far seem out of reach in the single-shot regime [2–8].

In this contribution we address this problem in the asymptotic regime, i.e., for quantum dichotomies $(\rho_1^{\otimes n}, \sigma_1^{\otimes n})$ and $(\rho_2^{\otimes R_n n}, \sigma_2^{\otimes R_n n})$ with large n and $\epsilon_\sigma = 0$, and for the half-commuting case with $[\rho_1, \sigma_1] \neq 0$ and $[\rho_2, \sigma_2] = 0$. We then employ the obtained solutions to study the optimal thermodynamic transformations from general input states within the resource theory of quantum thermodynamics [9–11], where one is allowed to process quantum systems only via *thermal operations* [12]. Recall that a quantum channel $\mathcal{E}$ acting on a system with Hamiltonian H is a thermal operation if and only if it can be written as

$$\mathcal{E}[\rho] = \mathrm{tr}_{B'}\left[U\left(\rho \otimes \gamma_B\right)U^\dagger\right], \qquad \gamma_B = \frac{e^{-\beta H_B}}{\mathrm{tr}(e^{-\beta H_B})}, \tag{2}$$

where β is the inverse temperature of the ancillary bath B in a thermal Gibbs state γ_B and described by a Hamiltonian H_B, U is a unitary that conserves the total energy, $[U, H \otimes \mathbb{1}_B + \mathbb{1} \otimes H_B] = 0$, and the partial trace can be performed over any subsystem B' of the joint system.

Main contributions: Let R_n^* be the largest rate R_n such that

$$(\rho_1^{\otimes n}, \sigma_1^{\otimes n}) \succ_{(\epsilon, 0)} (\rho_2^{\otimes R_n n}, \sigma_2^{\otimes R_n n}) \tag{3}$$

for states $\rho_1 \ll \sigma_1$, $\rho_2 \ll \sigma_2$. Also, let

$$D(\rho\|\sigma) := \mathrm{tr}\left(\rho\left(\log\rho - \log\sigma\right)\right), \qquad V(\rho\|\sigma) := \mathrm{tr}\left(\rho\left(\log\rho - \log\sigma\right)^2\right) - D(\rho\|\sigma)^2, \tag{4}$$

denote the relative entropy and relative entropy variance, let

$$D_\alpha(\rho\|\sigma) = \frac{1}{\alpha-1}\max\left\{\log \mathrm{Tr}\left(\sqrt{\rho}\sigma^{\frac{1-\alpha}{\alpha}}\sqrt{\rho}\right)^\alpha, \log \mathrm{Tr}\left(\sqrt{\sigma}\rho^{\frac{\alpha}{1-\alpha}}\sqrt{\sigma}\right)^{1-\alpha}\right\} \tag{5}$$

denote the sandwiched Rényi relative entropy, and

$$\xi := \frac{V(\rho_1\|\sigma_1)/D(\rho_1\|\sigma_1)}{V(\rho_2\|\sigma_2)/D(\rho_2\|\sigma_2)}, \qquad S_\nu^{-1}(\epsilon) = \inf_{x\in(\epsilon,1)} \sqrt{\nu}\Phi^{-1}(x) - \Phi^{-1}(x-\epsilon), \tag{6}$$

denote the reversibility parameter [13, 14] and the inverse of the cumulative distribution function for the so-called sesquinormal distribution S_ν, which we introduce in this contribution.

For $[\rho_2, \sigma_2] = 0$, we then have the following results on transforming quantum dichotomies:

- In the small deviation regime, for any fixed $\epsilon \in (0,1)$, the optimal rate is given by

$$R_n^*(\epsilon) = \frac{D(\rho_1\|\sigma_1)}{D(\rho_2\|\sigma_2)}\left[1 + \sqrt{\frac{V(\rho_2\|\sigma_2)}{nD(\rho_1\|\sigma_1)D(\rho_2\|\sigma_2)}}S_\xi^{-1}(\epsilon)\right] + o(1/\sqrt{n}). \tag{7}$$

- In the moderate deviation regime, for any $a \in (0,1)$ and the accepted error level of $\epsilon_n = \exp(-\lambda n^a)$ for some $\lambda > 0$, the optimal rate is given by

$$R_n^*(\epsilon_n) = \frac{D(\rho_1\|\sigma_1) - \left|1-\xi^{-1/2}\right|\sqrt{2\lambda V(\rho_1\|\sigma_1)n^{a-1}}}{D(\rho_2\|\sigma_2)} + o\left(\sqrt{n^{a-1}}\right). \tag{8}$$

- In the large deviation regime, for any constant $\lambda > 0$ and the accepted error level of $\epsilon_n = \exp(-\lambda n)$, the optimal rate is bounded by

$$\limsup_{n\to\infty} R_n^*(\epsilon_n) \le U(\lambda) \quad \text{and} \quad \liminf_{n\to\infty} R_n^*(\epsilon_n) \ge L(\lambda), \tag{9}$$

  where the explicit forms of $U(\lambda)$ and $L(\lambda)$, based on two variants of the Rényi relative entropy, are given in the technical manuscript, and $U(\lambda) = L(\lambda)$ if $[\rho_1, \sigma_1] = 0$.

- The optimal zero-error rate is given by

$$\lim_{n\to\infty} R_n^*(0) = \min_{\alpha\in\overline{\mathbb{R}}} \frac{D_\alpha(\rho_1\|\sigma_1)}{D_\alpha(\rho_2\|\sigma_2)}. \tag{10}$$

- For $[\rho_2, \sigma_2] \neq 0$, corresponding upper bounds on the optimal rate hold in all regimes.

The above technical results lead us to the following results concerning quantum thermodynamics:

- For σ_1 and σ_2 given by thermal states γ_1 and γ_2, the optimal transformation rates that we derived (excluding the zero-error case) can be attained by thermal operations. Thus, Eqs. (7)-(9) describe optimal rates R_n^* for state transformations under thermal operations between n copies of generic quantum states ρ_1 and $R_n^* n$ copies of energy-incoherent states ρ_2. Note that it also proves that up to second-order asymptotics and for final energy-incoherent states, the sets of thermal operations and Gibbs-preserving operations [15] have the same power.

- Consider the following ϵ-approximate work-assisted transformation via thermal operations:

$$\rho_1^{\otimes n} \otimes |0\rangle\langle 0|_W \xrightarrow[\mathrm{TO}]{\epsilon} \rho_2^{\otimes R_n n} \otimes |1\rangle\langle 1|_W, \tag{11}$$

  where W is the ancillary battery system with an energy gap $w = w_1 n + w_2\sqrt{n}$ with constant w_1 and w_2, and the target state ρ_2 is energy-incoherent. Then, for any fixed transformation error $\epsilon \in (0,1)$, the optimal rate R_n^* is given by

$$R_n^*(\epsilon) = \frac{D(\rho_1\|\gamma_1) - \beta w_1}{D(\rho_2\|\gamma_2)} + \frac{\sqrt{V(\rho_1\|\gamma_1)}S_{1/\xi'}^{-1}(\epsilon) - \beta w_2}{\sqrt{n}D(\rho_2\|\gamma_2)} + o(1/\sqrt{n}), \tag{12}$$

  where

$$\xi' := \frac{V(\rho_1\|\gamma_1)}{D(\rho_1\|\gamma_1) - \beta w_1}\Big/\frac{V(\rho_2\|\gamma_2)}{D(\rho_2\|\gamma_2)}. \tag{13}$$

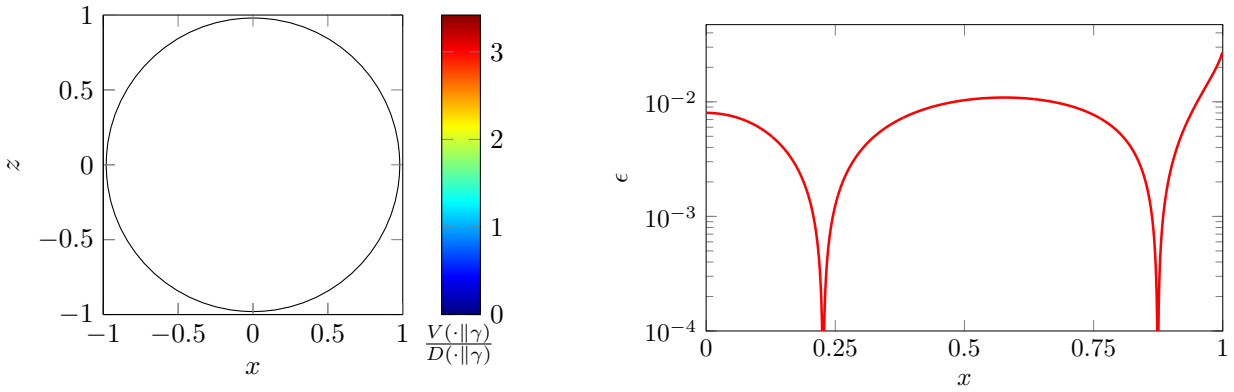


Figure 1: **Coherent resonance in thermodynamic transformations of two-level systems.** Left: the ratio $V(\rho\|\gamma)/D(\rho\|\gamma)$ (encoding the resonance condition) for qubit states lying in the xz plane of the Bloch sphere for a thermal state $\gamma = \mathrm{diag}(0.95, 0.05)$ (indicated by a white triangle). The white disk corresponds to the final state $\rho_2 = \mathrm{diag}(0.75, 0.25)$, while the dashed white line indicates a family of initial states $\rho_1(x)$ with diagonal $(0.85, 0.15)$ and off-diagonal elements equal to $\sqrt{0.85 \cdot 0.15}x$ for $x \in [0, 1]$. Right: threshold transformation error ϵ required to achieve the asymptotic transformation rate $D(\rho_1(x)\|\gamma)/D(\rho_2\|\gamma)$ for finite number n of transformed systems (i.e., ϵ such that the second order correction term in Eq. (7) disappears). Resonance is obtained when the relative free energy fluctuations V/D are the same for the initial state $\rho_1(x)$ and the final state ρ_2, i.e., when $\nu = 1$.

Discussion: Our results provide a framework to study the second order asymptotics of thermodynamic state transformations [16, 17] for fully general input states with coherence between different energy eigenspaces, thus for the first time going beyond the semi-classical regime with no quantum interference effects. As a result, we can investigate optimal performance of various thermodynamic protocols with coherent inputs. In particular, we obtain that one can extract

$$W = \frac{1}{\beta}\left(nD(\rho\|\gamma) + \sqrt{nV(\rho\|\gamma)}\Phi^{-1}(\epsilon) + o(\sqrt{n})\right) \tag{14}$$

of ϵ-deterministic work from n copies of the system in a general state ρ. Analogously, we also derived the thermodynamic cost W_{cost} of ϵ-deterministic erasure of information from n copies of a system in a state ρ, and showed that the number M of messages that can be encoded into $\rho^{\otimes n}$ via thermal operations [18] allowing for decoding probability $1 - \epsilon$ satisfies $\log M = \beta W$ with W specified above. Importantly, in all these protocols the optimal final states are always energy-incoherent, and thus our results allow to study them in full generality.

Our results also show that by appropriately tuning the initial and final states so that the reversibility parameter $\xi = 1$, the second order correction to the optimal rate may vanish in the limit of zero transformation error, and so, up to higher order terms, one obtains a reversible transformation (with no free energy dissipation). This intriguing phenomenon, termed resource resonance, was first predicted in Ref. [14] for the case of energy-incoherent initial and final states. The results we present in this contribution allow us to extend the resource resonance phenomenon in three novel ways. First, we extend it to *coherent resonance*, in which the coherence present in the initial state of the processed system can be exploited to significantly reduce the transformation error ϵ when processing a finite number of copies n of a quantum system. In Fig. 1, we present the non-trivial dependence of the transformation error ϵ on the coherence level x for examplary qubit systems, where we can observe two resonant values of x for which error-free and dissipationless transformations (up to second order asymptotics) are possible. This clearly illustrates that quantum coherence can play an important role in avoiding free energy dissipation in thermodynamic transformations of quantum states. Second, we can achieve *work-assisted resonance*, where the dissipation is avoided by charging/discharging a battery by an amount w_1 that sets ξ' from Eq. (13) to 1. And third, by extending to large and extreme deviation analyses, it can be seen that there exists an even stronger notion of resonance, which we term *strong resonance*, in which errors are not just exponentially suppressed, but entirely eliminated.

References

[1] D. Blackwell, "Equivalent comparisons of experiments," *Ann. Math. Stat.*, **24**, pp. 265–272, (1953).

[2] K. Matsumoto, "An example of a quantum statistical model which cannot be mapped to a less informative one by any trace preserving positive map," *arXiv:1409.5658*, (2014).

[3] A. Jenčová, "Comparison of quantum binary experiments," *Rep. Math. Phys.*, **70**, 2, pp. 237–249, (2012).

[4] D. Reeb, M. J. Kastoryano, and M. M. Wolf, "Hilbert's projective metric in quantum information theory," *J. Math. Phys.*, **52**, 8, p. 082201, (2011).

[5] F. Buscemi, "Comparison of quantum statistical models: equivalent conditions for sufficiency," *Commun. Math. Phys.*, **310**, 3, pp. 625–647, (2012).

[6] P. Alberti and A. Uhlmann, "A problem relating to positive linear maps on matrix algebras," *Rep. Math. Phys.*, **18**, 2, pp. 163–176, (1980).

[7] F. Buscemi, D. Sutter, and M. Tomamichel, "An information-theoretic treatment of quantum dichotomies," *Quantum*, **3**, p. 209, (2019).

[8] F. Buscemi and G. Gour, "Quantum relative lorenz curves," *Phys. Rev. A*, **95**, p. 012110, (2017).

[9] M. Horodecki and J. Oppenheim, "Fundamental limitations for quantum and nanoscale thermodynamics," *Nat. Commun.*, **4**, (2013).

[10] F. G. S. L. Brandão, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, "Resource theory of quantum states out of thermal equilibrium," *Phys. Rev. Lett.*, **111**, p. 250404, (2013).

[11] F. G. S. L. Brandão, M. Horodecki, N. H. Y. Ng, J. Oppenheim, and S. Wehner, "The second laws of quantum thermodynamics," *Proc. Natl. Acad. Sci. U.S.A.*, **112**, p. 3275, (2015).

[12] D. Janzing, P. Wocjan, R. Zeier, R. Geiss, and T. Beth, "Thermodynamic cost of reliability and low temperatures: tightening Landauer's principle and the second law," *Int. J. Theor. Phys.*, **39**, 12, pp. 2717–2753, (2000).

[13] W. Kumagai and M. Hayashi, "Second-order asymptotics of conversions of distributions and entangled states based on Rayleigh-normal probability distributions," *IEEE Trans. Inf. Theory*, **63**, 3, pp. 1829–1857, (2017).

[14] K. Korzekwa, C. T. Chubb, and M. Tomamichel, "Avoiding irreversibility: Engineering resonant conversions of quantum resources," *Phys. Rev. Lett.*, **122**, p. 110403, (2019).

[15] P. Faist, J. Oppenheim, and R. Renner, "Gibbs-preserving maps outperform thermal operations in the quantum regime," *New J. of Phys.*, **17**, p. 043003, (2015).

[16] C. T. Chubb, M. Tomamichel, and K. Korzekwa, "Beyond the thermodynamic limit: finite-size corrections to state interconversion rates," *Quantum*, **2**, p. 108, (2018).

[17] W. Kumagai and M. Hayashi, "Second-order asymptotics of conversions of distributions and entangled states based on Rayleigh-normal probability distributions," *IEEE Trans. Inf. Theory*, **63**, pp. 1829–1857, (2017).

[18] K. Korzekwa, Z. Puchała, M. Tomamichel, and K. Życzkowski, "Encoding classical information into quantum resources," *IEEE Trans. Inf. Theory*, **68**, p. 4518, (2022).

Catalysts enable the decomposition of thermal operations into simpler operations

Jeongrak Son[1] * Nelly H. Y. Ng[1] †

[1] *School of Physical and Mathematical Sciences, Nanyang Technological University, 637371, Singapore*

Abstract. In thermodynamic resource theories, the most popular set of free operations is the thermal operation, assuming access to any energy-preserving unitaries between the system and the bath. However, the real implementation of such operations is improbable due to their generality. We show that catalysts, auxiliary states that assist the evolution while retaining their state, are extremely useful in boosting more experiment-friendly operations to approach usual thermal operations: when catalysts can be chosen arbitrarily, thermal operations with catalysts can be fully emulated; even when catalysts are restricted, the advantage remains significant. We also provide some intuition on why catalysts are useful.

Keywords: resource thoery, quantum thermodynamics, quantum catalysis

1 Motivation

When studying thermodynamics as a resource theory, different choices of free operations are available. The most popular option is to allow the attachment of a thermal bath in the Gibbs state at a specific temperature, followed by the application of a global energy-preserving unitary, and finally tracing out the bath. These operations form a set of channels, known as thermal operations (TO) [1]. Choosing thermal operations as the set of free operations provides fundamental limits, as it considers any unitaries that obey the first law of thermodynamics. Moreover, for initial states that are incoherent in the energy basis, characterizing possible transitions becomes straightforward using thermomajorization relations, which rely only on the energy level populations of the initial and target states. However, for any practical settings, assuming all energy preserving unitaries to be available is unrealistic. Therefore, alternative choices for free operations become necessary.

Elementary thermal operations (ETO) [2] was proposed to remedy this issue by imposing an additional restriction on energy-preserving unitaries within TO. In ETO, the set of free operations consists of sequences of TO channels, each acting on only two system levels at a time, or their convex combinations. Remarkably, each two-system-level TO can be implemented by Jaynes-Cummings type interactions, which are well-studied in various experimental setups. Their concatenations are also more experimentally feasible compared to arbitrary energy-preserving unitaries of TO. Nevertheless, two major problems hinder further research on this version of free operations. Firstly, ETO is strictly weaker than TO for state transitions. Secondly, characterizing reachable final states under ETO is extremely difficult, even when the initial state is energy-incoherent.

To strengthen the capabilities of ETO, we introduced catalytic transformations. Catalysts are auxiliary states that interact with both the system and the bath during the state transformation process. However, they return to their original state at the end of the procedure. Sometimes, when a transformation $\rho \to \rho'$ is not possible using any free operation, an extended transformation $\rho \otimes \sigma \to \rho' \otimes \sigma$ is achievable via some free operation [3]. In this case, σ serves as an (exact) catalyst. Catalytic transformations are justified as the resource in the catalyst state σ remains intact, and the returned state can be used to activate similar processes repeatedly. In particular, we adopt the most conservative notion of catalysts, where they should be recovered without any error or correlation to the system. We study three different scenarios of catalytic ETO [4, 5]: the most general case, where any catalyst state is allowed; the use of any Gibbs state with the ambient temperature as the catalyst; and the utilization of small catalysts with fixed dimensionality. In particular, we provide the full characteriztion of catalytic ETO in the former two cases.

Surprisingly, catalysts also enhance another class of weaker operations, namely Markovian thermal operations (MTO). MTO has a different operational motivation: it assumes that the thermal bath remains in equilibrium throughout the evolution [6]. We demonstrate that with arbitrary states and with Gibbs states, catalytic version of MTO also coincides with the corresponding catalytic ETO. Consequently, catalysis collapses the hierarchy of thermal processes for all known restricted versions of TO.

For the computability problem, we have made significant progress in deriving analytical results for constructing final states under ETO. Notably, for certain special classes of initial states, an efficient method of determining the complete set of reachable final states is found.

2 Elementary thermal operations with Gibbs state catalysts

Gibbs states are natural equilibrium states at fixed temperature, since they are completely passive and have maximum entropy with the fixed average energy. This motivates the assumption that we have access to any Gibbs state thermalized with the environment, i.e. Gibbs states are free states of TO. Combined with the fact that

*jeongrak.son@e.ntu.edu.sg
†nelly.ng@ntu.edu.sg

any concatenation and convex combination of TOs can be represented as a single TO channel, choosing a Gibbs state as a catalyst does not yield any additional advantage – instead, one can incorporate that catalyst state into the bath state itself.

However, for ETO and MTO, concatenations of channels cannot be expressed as a single ETO or MTO channel, leaving room for potential improvements through the use of a Gibbs state catalyst. In fact, by exclusively employing Gibbs state catalysts, we achieve full TO state transitions[1]. Another merit of this approach is that Gibbs states are assumed to be readily accessible, unlike other catalyst states that often require fine-tuning. We denote the set of final states reachable from an initial state ρ via free operations X as $\mathcal{R}_X(\rho)$. We also use the abbreviations GC-ETO and GC-MTO to refer to ETO and MTO using Gibbs catalysts, respectively.

Theorem 1 $\mathcal{R}_{\mathrm{GC-ETO}}(\rho) = \mathcal{R}_{\mathrm{GC-MTO}}(\rho) = \mathcal{R}_{\mathrm{TO}}(\rho)$.

Note that this result holds for any initial state ρ, including *energy coherent* states. The inclusion $\mathcal{R}_{\mathrm{GC-ETO}}(\rho), \mathcal{R}_{\mathrm{GC-MTO}}(\rho) \subset \mathcal{R}_{\mathrm{TO}}$ follows immediately from the fact that ETO and MTO themselves are subsets of TO, and Gibbs catalysts are useless for TO. The other direction can be obtained by decomposing a given TO. Each TO assumes a thermal bath and an energy-preserving unitary. We consider this thermal bath as a Gibbs state catalyst for ETO or MTO. Now recall that all system-bath energy preserving unitaries form a Lie group, where the corresponding Lie algebra is given by the set of $-iH_{\mathrm{int}}$, where H_{int} are interaction Hamiltonians commuting with the total Hamiltonian. Then it is known that any element of the Lie group can be written as a finite product of two-level energy-preserving unitaries whose generators form the basis of the Lie algebra. Since the bath is now a catalyst, which is part of the system, it is not traced out after each unitary and each two-level unitary is a valid ETO or MTO. It is an ETO since it only acts on two levels of the system plus catalyst; it is an MTO since no (non-Markovian) bath is required. At the end, we fully thermalize the catalyst so that it goes back to the Gibbs state. Full thermalization is also permitted in ETO and MTO. Therefore, the full protocol is ETO and MTO with a Gibbs state catalysis.

The above result establishes the existence of an exact decomposition, but not a construction. An easy (approximate) construction can be achieved by expressing the original unitary in a Trotter-Suzuki form, where each term corresponds to a two-level energy-preserving unitary. By increasing the number of Trotter steps, the error can be made arbitrarily small.

From this proof sketch, we can infer that the main value provided by the Gibbs state catalyst is its non-Markovianity, or in other words, its ability to retain memory throughout the process. A similar observation can be made when the catalyst is not necessarily in a Gibbs state and is small. Such intuition can provide a different perspective for investigating other catalytic setups.

[1] Theorems 1 and 2 are stronger than the results already included in our preprint [5], which only guarantees the approximate recovery of TO state transitions.

3 Elementary thermal operations with arbitrary catalysts

As a corollary of Theorem 1, we have $\mathcal{R}_{\mathrm{GC-ETO}}(\rho \otimes \sigma) = \mathcal{R}_{\mathrm{GC-MTO}}(\rho \otimes \sigma) = \mathcal{R}_{\mathrm{TO}}(\rho \otimes \sigma)$, when incorporating an additional catalyst σ. This allows us to recover catalytic thermal operations (CTO).

Theorem 2 $\mathcal{R}_{\mathrm{CETO}}(\rho) = \mathcal{R}_{\mathrm{CMTO}}(\rho) = \mathcal{R}_{\mathrm{CTO}}(\rho)$.

Here, C(E)(M)TO refers to the catalytic versions of (E)(M)TO, where we have access to any catalyst state.

Again, the existence of an exact decomposition is shown for *any* initial state ρ. That is, we fully solve the problem of general catalytic elementary thermal operations and catalytic Markovian thermal operations.

However, this time, the (approximate) construction is not as straightforward as in the GC-ETO case. The complication arises from the requirement that the additional catalyst σ must be recovered *exactly* and *without correlation*, even though the final state only needs to be reached with an arbitrarily small error. Nonetheless, a similar Trotterization strategy can be employed for energy incoherent initial states ρ.

In sum, catalytic thermal operations can be decomposed into simpler catalytic operations without the need for highly demanding types of interactions. The trade-off, however, is that a longer sequence of unitaries is needed, and the memory of the Gibbs state should remain intact in the typically noisy environment.

4 Elementary thermal operations with small catalysts

We have demonstrated that the hierarchy between TO, ETO, and MTO collapses when large catalysts are available. However, to maximize the value of easier operations, it is crucial to investigate whether catalysts can also be small, allowing for control over only a small system plus catalyst composite. To showcase the power of small catalysts, we focus on the minimal nontrivial model of a qutrit system with the help of small catalysts whose size varies from dimension two to thirty. Also, we restrict our analysis to energy incoherent initial states, as determining the feasibility of transitions for energy coherent systems remains an open problem.

In the simplest scenarios involving a qutrit system and a qubit catalyst, characterizing the complete set of reachable states is computationally tractable. For typical states, a qubit catalyst can activate CETO processes that (partially) bridge the gap between TO and ETO or go beyond the set $\mathcal{R}_{\mathrm{TO}}$. This offers a significant advantage from an implementation perspective. Instead of dealing with generic interactions between the system and a potentially complicated bath, by increasing the size of the total system from dimension three to six, a collection of thermal harmonic oscillators and Jaynes-Cummings

type interactions can execute the same, or sometimes even more powerful, operations.

For higher-dimensional catalysts, the exhaustive computation of the reachable states becomes infeasible. Therefore, we impose restrictions on our initial states.

Remark 1 *Suppose that ρ is an energy incoherent, whose energy population is given by* $\mathrm{p} = (p_1, \cdots, p_d)$ *with respect to energy levels ordered as $E_1 \leq E_2 \leq \cdots \leq E_d$. When the ambient temperature is β^{-1} and ρ satisfies $p_1 e^{\beta E_1} \leq p_2 e^{\beta E_2} \leq \cdots \leq p_d e^{\beta E_d}$ or $p_1 e^{\beta E_1} \geq p_2 e^{\beta E_2} \geq \cdots \geq p_d e^{\beta E_d}$, we refer to ρ as a* monotonic β-order state.

Then the following theorem holds.

Theorem 3 *If ρ is a monotonic β-order state with dimension d, it is possible to verify the feasibility of a transition from ρ to ρ' via ETO in $\mathcal{O}(d^2)$ time.*

This is a dramatic improvement compared to the generic computation time scaling as $\mathcal{O}(d^{2d!})$.

A notable class of states with monotonic β-order is the set of Gibbs states with different temperatures. Therefore, we can investigate the operationally important task of cooling from one thermal state to another[2].

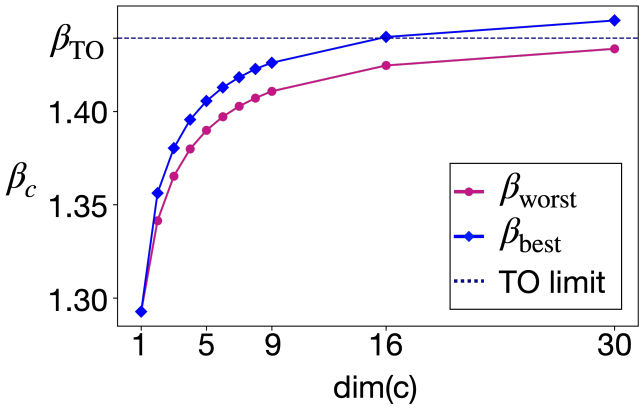


Figure 1: The cooling of a thermal qutrit state to another thermal qutrit state via (C)ETO with small catalysts. The blue diamonds represent the best results obtained from our sample of catalysts, while the purple circles mark the worst results. The initial inverse temperature is $\beta_h = 0.5$, the ambient inverse temperature is $\beta = 1$, and the final temperature is denoted as β_c^{-1}. The TO limit is indicated by β_{TO} (shown as a black dashed line), and the result with $\dim(\mathrm{c}) = 1$ represents the ETO limit. The energy levels of the system are given as $(0, 0.4, 0.5)$.

In Fig. 1, we sampled catalysts in the restricted pool, where the catalyst Hamiltonian is trivial and the initial system-catalyst composite has monotonic β-order. The gap between the ETO and TO limits is bridged with small catalysts and when $\dim(\mathrm{c}) = 16$ some catalytic ETOs outperform TO limit of cooling. Interestingly, the worst performing catalysts turned out to be the Gibbs states, which approach the TO limit as the dimension grows, as expected from Thm. 1. Therefore, within this restricted range of catalysts, any catalysts outperform Gibbs catalysts, which reduces the need of fine-tuning the catalyst state.

[2]This part of the result has not been included in our preprint [4] yet, but it will be included in the revised version soon.

5 Free energy dynamics during catalytic processes

Finally, we examine how free energies change in a particular CETO process where the system is a qutrit and the catalyst is a qubit to better understand what is happening during the catalytic process. When TO channel is applied, non-equilibrium free energy, defined as the average energy minus temperature times entropy, cannot increase. Since each ETO step is also a TO channel, the same constraint holds. This can be seen in the total free energy, since the channel acts on the total (system plus catalyst) state.

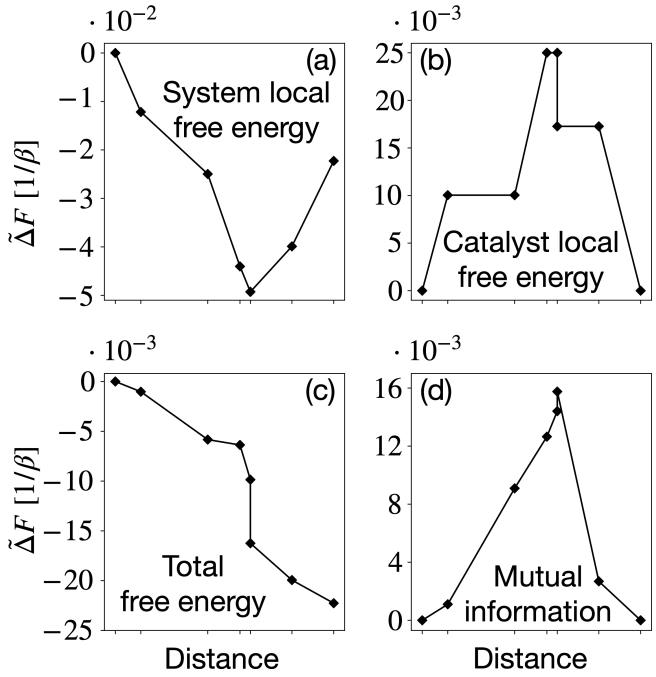


Figure 2: The change in non-equilibrium free energies after each CETO step. (a) and (b) tracts the free energy of the system and catalyst reduced states, while (c) shows the total free energy of the system-catalyst composite. (d) captures the correlation between the system and the catalyst by their mutual information. x-axes are scaled by the distance in the barycentric representation between the system reduced states before and after the ETO step.

The most interesting part of Fig. 2 is panel (a), where the system free energy decreases initially, but increases in the later time, which is impossible if the system evolves without a catalyst. Fig. 2 thus exhibits the non-Markovian effect of the catalyst. Qualitatively, catalysts are useful for their capability of storing free energy during the process and releaseing it back to the system at the later stage. This observation could provide novel insights when designing good catalytic protocols.

References

[1] D. Janzing, P. Wocjan, R. Zeier, R. Geiss, and T. Beth. Thermodynamic cost of reliability and low temperatures: tightening Landauer's principle and the second law. *Int. J. Theor. Phys.*, 39:2717–2753, 2000.

[2] M. Lostaglio, Á. M. Alhambra, and C. Perry. Elementary Thermal Operations. *Quantum.*, 2:52, 2018.

[3] D. Jonathan and M. B. Plenio. Entanglement-assisted local manipulation of pure quantum states. *Phys. Rev. Lett.*, 83:3566–3569, 1999.

[4] J. Son and N. H. Y. Ng. Catalysis in Action via Elementary Thermal Operations. arXiv:2209.15213, 2022.

[5] J. Son and N. H. Y. Ng. A hierarchy of thermal processes collapses under catalysis. arXiv:2303.13020, 2023.

[6] M. Lostaglio and K. Korzekwa. Continuous thermomajorization and a complete set of laws for Markovian thermal processes. *Phys. Rev. A.*,106:012426, 2022.

Catalysis cannot overcome bound entanglement

Ludovico Lami[1] Bartosz Regula[2] Alexander Streltsov[3]

[1]*QuSoft and University of Amsterdam, Science Park 123, 1098 XG Amsterdam, the Netherlands*
[2]*RIKEN Center for Quantum Computing (RQC), Wako, Saitama 351-0198, Japan*
[3]*Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland*

Abstract. The use of ancillary quantum systems known as catalysts is known to be able to enhance the capabilities of entanglement transformations under local operations and classical communication. However, the limits of these advantages have not been determined, and in particular it is not known if such assistance can overcome the known restrictions on asymptotic transformation rates — notably the existence of bound entangled (undistillable) states. Here we establish a general limitation of entanglement catalysis: we show that catalytic transformations can never allow for the distillation of entanglement from a bound entangled state, even if the catalyst may become correlated with the system of interest, and even under permissive choices of free operations. This precludes the possibility that catalysis can make entanglement theory asymptotically reversible. Our methods are based on new asymptotic bounds for the distillable entanglement and entanglement cost assisted by correlated catalysts. Extending our approach beyond entanglement theory, we show that catalysts also cannot enable reversibility in the manipulation of quantum coherence, establishing even stronger restrictions on asymptotic catalytic transformations in this resource theory.

Keywords: entanglement distillation, relative entropies, catalytic state transformations

Full paper: **arXiv:2305.03489**

The study of quantum entanglement as a resource has been one of the most fundamental problems in the field of quantum information ever since its inception [1]. To utilize this resource efficiently, it is often required to transform and manipulate entangled quantum systems, which leads to the well-studied question of how quantum states can be converted using only local operations and classical communication (LOCC) [2, 3]. The limits of such conversion capability are represented by asymptotic transformation rates, which are particularly important in the context of purifying noisy quantum states into singlets Φ_2, a task known as entanglement distillation, as well as for the reverse task of using such singlets to synthesize noisy quantum states. This leads to the notions of *distillable entanglement* $E_d(\rho)$ [2], which tells us how many copies of Φ_2 we can extract from a given state ρ, and of *entanglement cost* $E_c(\rho)$ [3], which tells us how many copies of a pure singlet are needed to obtain ρ.

A phenomenon that can severely restrict our ability to extract entanglement is known as *bound entanglement* [4]: there exist states from which no entanglement can be distilled, even though their entanglement cost is non-zero. A consequence of this is the irreversibility of entanglement theory — after performing a transformation $\rho \to \omega$, one may not be able to realize the reverse process $\omega \to \rho$ and recover all of the supplied copies of ρ. This contrasts with the asymptotic reversibility of theories such as classical and quantum thermodynamics [5–7]. Although reversibility may still hold in some restricted cases (e.g., for all bipartite pure quantum states [3, 5]), and there are even approaches that may enable reversibility by suitably relaxing the restrictions on the allowed physical transformations [8–10], irreversibility is often a fundamental property of the theory of quantum entanglement [11]. It is then important to understand how, if at all, irreversibility can be overcome.

A promising approach to increase the capabilities of entanglement transformations is the use of so-called *catalysts* [12], that is, ancillary systems that can be employed in the conversion protocol, but must eventually be returned in an unchanged state. Although this phenomenon has been shown to be remarkably powerful in the context of single- and many-copy transformations [12–18], it is unknown whether catalysis can enhance the asymptotic conversion rates. This motivates in particular an important question: is the use of catalysis enough to facilitate the reversibility of entanglement theory?

In this work [19], we close this question by showing that even very permissive forms of catalytic transformations are insufficient to distill entanglement from bound entangled states. Specifically, we show that the catalytically distillable entanglement of any state with positive partial transpose (PPT) is zero, which is strictly less than its catalytic entanglement cost. The result relies on the establishment of a general upper bound on distillable entanglement under catalytic LOCC operations, namely, the relative entropy of PPT entanglement, which was known to be an upper bound only in conventional, non-catalytic protocols [20, 21]. We show that this limitation persists even if one allows the catalyst to build up correlations with the main system, as well as if one allows sets of operations larger than LOCC, in particular all PPT-preserving transformations. This presents a very general limitation on the power of catalytic transformations of entangled states. We additionally study the applications of various resource monotones to constraining asymptotic state conversion with catalytic assistance, obtaining a number of bounds that may be of independent interest.

We further demonstrate the power of our methods by applying them to another quantum resource that is closely related to entanglement, namely, *coherence* [22–25]. In this context, incoherent operations (IO) [23, 24] have emerged as the main example of a set of operations that are sufficiently powerful to allow for generic coherence distillation [26], yet not powerful enough to enable full reversibility. It is natural to ask whether one could improve either distillation or dilution under IO via catalysis. Here we answer this question in the negative in the most general sense: neither the IO distillable coherence nor the IO coherence

cost are affected by the introduction of catalysts.

Preliminaries We use $\mathrm{SEP}(A\!:\!B)$ to denote the set of states σ_{AB} which are separable across the bipartition $A\!:\!B$. The notation $\mathrm{PPT}(A\!:\!B)$ will be used to denote the set of positive partial transpose states, i.e., ones for which the partially transposed operator σ_{AB}^{Γ} is also a valid quantum state. States which are not in PPT will be conventionally called NPT (non-positive partial transpose).

Even though the choice of LOCC in the context of entanglement transformations is well motivated from a practical perspective, in many settings there exist other possible choices of allowed 'free' operations; let us then use $\mathcal{F}$ to denote the chosen set of such permitted protocols. One such choice is the set of so-called PPT operations [27], or the even larger choice of all PPT-preserving operations PPTP [28], i.e., all maps $\Lambda : AB \to A'B'$ such that $\Lambda(\sigma_{AB}) \in \mathrm{PPT}(A'\!:\!B')$ for all $\sigma_{AB} \in \mathrm{PPT}(A\!:\!B)$.

Given two bipartite states ρ_{AB} and $\omega_{A'B'}$, we say that the transformation from ρ_{AB} to $\omega_{A'B'}$ is possible via operations in $\mathcal{F}$ assisted by catalysts if there exists a finite-dimensional state τ_{CD} and an operation $\Lambda \in \mathcal{F}\left(AC : BD \to A'C : B'D\right)$ such that

$$\Lambda\left(\rho_{AB} \otimes \tau_{CD}\right) = \omega_{A'B'} \otimes \tau_{CD}. \tag{1}$$

We denote this by $\rho_{AB} \xrightarrow{\mathcal{F}^c} \omega_{A'B'}$. More generally, we say that the transformation is possible via operations in $\mathcal{F}$ assisted by *correlated catalysts* [29–31] and we write $\rho_{AB} \xrightarrow{\mathcal{F}^{cc}} \omega_{A'B'}$, if there exists a finite-dimensional state τ_{CD} and an operation $\Lambda \in \mathcal{F}\left(AC : BD \to A'C : B'D\right)$ such that

$$\mathrm{Tr}_{CD}\, \Lambda\left(\rho_{AB} \otimes \tau_{CD}\right) = \omega_{A'B'} \tag{2}$$

and

$$\mathrm{Tr}_{A'B'}\left[\Lambda\left(\rho_{AB} \otimes \tau_{CD}\right)\right] = \tau_{CD}. \tag{3}$$

This relaxed notion allows for the output state of the protocol to be correlated between the main system (AB) and catalyst (CD), as long the marginal systems satisfy the required constraints. Crucially, correlated catalysis is a strictly more powerful framework than standard catalysis, and allowing for such correlations can greatly enlarge the set of achievable state transformations, even already in the one-shot regime [30–36].

Let us now define the notion of asymptotic transformation rates. Given any allowed choice of transformations $\widetilde{\mathcal{F}} \in \{\mathcal{F}, \mathcal{F}^c, \mathcal{F}^{cc}\}$, we write $\rho_{AB} \xrightarrow{\widetilde{\mathcal{F}}} \approx_\varepsilon \omega_{A'B'}$ if there exists a state $\omega'_{A'B'}$ such that

$$\rho_{AB} \xrightarrow{\widetilde{\mathcal{F}}} \omega'_{A'B'}\,, \qquad \frac{1}{2}\left\|\omega'_{A'B'} - \omega_{A'B'}\right\|_1 \leq \varepsilon\,. \tag{4}$$

For every pair of states ρ_{AB} and $\omega_{A'B'}$, the corresponding asymptotic rate is given by

$$\begin{aligned} &R_{\widetilde{\mathcal{F}}}\left(\rho_{AB} \to \omega_{A'B'}\right) \\ &\coloneqq \sup\left\{R :\ \rho_{AB}^{\otimes n} \xrightarrow{\widetilde{\mathcal{F}}} \approx_{\varepsilon_n} \omega_{A'B'}^{\otimes \lceil Rn \rceil},\ \lim_{n\to\infty} \varepsilon_n = 0\right\}. \end{aligned} \tag{5}$$

The distillable entanglement and entanglement cost under operations in $\widetilde{\mathcal{F}}$ are then defined by

$$E_{d,\,\widetilde{\mathcal{F}}}\left(\rho\right) \coloneqq R_{\widetilde{\mathcal{F}}}\left(\rho \to \Phi_2\right), \quad E_{c,\,\widetilde{\mathcal{F}}}\left(\rho\right) \coloneqq \frac{1}{R_{\widetilde{\mathcal{F}}}\left(\Phi_2 \to \rho\right)}, \tag{6}$$

where $\Phi_2 \coloneqq |\Phi_2\rangle\langle\Phi_2|$ with $|\Phi_2\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Conventionally, the notation E_d and E_c is used to refer to $E_{d,\,\mathrm{LOCC}}$ and $E_{c,\,\mathrm{LOCC}}$.

An entangled state σ_{AB} is called bound entangled if $E_{d,\mathrm{LOCC}}(\sigma_{AB}) = 0$. A particularly useful criterion to detect undistillability was established in [4]: if a state σ_{AB} is PPT, then $E_{d,\mathrm{LOCC}}(\sigma_{AB}) = 0$. As $E_{c,\mathrm{LOCC}}(\sigma_{AB}) > 0$ for any entangled state σ_{AB} [37], this means that any PPT σ_{AB} which is not separable has a non-zero entanglement cost, while no entanglement can be extracted from it.

Monotones A very common way to constrain entanglement transformations, also in the asymptotic transformation regime, is to use so-called entanglement monotones, also known as entanglement measures [38]. These are functions M which satisfy $M(\Lambda(\rho_{AB})) \leq M(\rho_{AB})$ for all free operations $\Lambda \in \mathcal{F}$. It is well known that, if the monotone satisfies weak additivity, i.e., $M(\rho^{\otimes n}) = nM(\rho)$, as well as a stronger form of continuity known as asymptotic continuity [39, 40], then the (non-catalytic) transformation rate is bounded as [28, 41]

$$R_{\mathcal{F}}(\rho \to \omega) \leq \frac{M(\rho)}{M(\omega)}. \tag{7}$$

Monotones are typically chosen so that they are normalized on the maximally entangled state, i.e., $M(\Phi_2) = 1$. Any such monotone then satisfies [42]

$$E_{d,\mathcal{F}}(\rho) \leq M(\rho) \leq E_{c,\mathcal{F}}(\rho). \tag{8}$$

A particularly important example of an LOCC monotone that obeys the above requirements is the regularized relative entropy of (PPT) entanglement

$$D^{\infty}_{\mathrm{PPT}}(\rho) \coloneqq \lim_{n\to\infty} \min_{\sigma \in \mathrm{PPT}(A^{\otimes n}:B^{\otimes n})} \frac{1}{n} D(\rho^{\otimes n} \| \sigma), \tag{9}$$

where the quantum relative entropy is defined by $D(\omega\|\tau) \coloneqq \mathrm{Tr}\,\omega\left(\log_2\omega - \log_2\tau\right)$ [43, 44].

The situation is much more intricate when it comes to catalytic transformations [17, 45, 46]. To establish a similar bound, it appears that several more assumptions about the given monotone are needed. In particular, if we also assume full additivity (i.e., $M(\rho_{AB} \otimes \omega_{A'B'}) = M(\rho_{AB}) + M(\omega_{A'B'})$ for any $\rho_{AB}, \omega_{A'B'}$) and strong superadditivity (i.e., $M(\rho_{AA':BB'}) \geq M(\rho_{AB}) + M(\rho_{A'B'})$), then we analogously obtain

$$R_{\mathcal{F}^{cc}}(\rho \to \omega) \leq \frac{M(\rho)}{M(\omega)} \tag{10}$$

(see [19] for a proof). However, to date, there are only two LOCC monotones that are known to satisfy all the required assumptions: the squashed entanglement E_{sq} [47] and the conditional entanglement of mutual information E_I [48, 49], both of which are however typically difficult to evaluate. Importantly, as the regularized relative entropy $D^{\infty}_{\mathrm{PPT}}$ is not known to satisfy the above properties, we do not yet know whether it is monotone under asymptotic correlated–catalytic protocols. This entails that we cannot straightforwardly use it to bound $E_{d,\mathrm{LOCC}^{cc}}$ or $E_{c,\mathrm{LOCC}^{cc}}$. Any attempt to establish readily computable asymptotic bounds on transformations with correlated catalysts therefore requires a completely different approach than conventional, non-catalytic bounds.

Results Our main technical contribution is the establishment of two very general bounds on correlated catalytic transformations, and in particular the recovery of the regularized relative entropy as an upper bound for distillation.

Proposition 1. *For all states ρ_{AB}, the distillable entanglement and entanglement cost under PPT-preserving operations assisted by correlated catalysts satisfy*

$$E_{d,\,\mathrm{PPT}^{cc}}(\rho_{AB}) \leq D^{\infty}_{\mathrm{PPT}}(\rho_{AB}) \leq D_{\mathrm{PPT}}(\rho_{AB}) \tag{11}$$

and

$$E_{c,\,\mathrm{PPT}^{cc}}(\rho_{AB}) \geq D^{\mathbb{PPT},\infty}_{\mathrm{PPT}}(\rho_{AB}) \geq D^{\mathbb{PPT}}_{\mathrm{PPT}}(\rho_{AB})\,, \tag{12}$$

where

$$D^{\mathbb{PPT}}_{\mathrm{PPT}}(\rho) \coloneqq \inf_{\sigma\in\mathrm{PPT}} \sup_{\mathbb{M}\in\mathbb{PPT}} D\big(\mathbb{M}(\rho)\,\big\|\,\mathbb{M}(\sigma)\big) \tag{13}$$

is the measured relative entropy of entanglement [50] under PPT measurements $\mathbb{PPT}$, and $D^{\mathbb{PPT},\infty}_{\mathrm{PPT}}$ is its regularization.

The key consequences of this result, as well as some additional insights that follow from our approach, are summarized in the following theorem.

Theorem 2. *The following holds:*

(a) A PPT state cannot be converted to an NPT state by means of PPT-preserving operations assisted by correlated catalysts, including all catalytic LOCC protocols.

(b) In particular, not even a single copy of Φ_2 can be distilled with error $\varepsilon < 1/2$ by an unbounded number of copies of any given PPT state via LOCC or PPT-preserving operations assisted by correlated catalysts.

(c) Therefore, all PPT entangled states ρ_{AB} are bound entangled under LOCC or PPT-preserving operations assisted by correlated catalysts, but have non-zero cost under LOCC assisted by correlated catalysts. More formally, if ρ_{AB} is PPT entangled then

$$\begin{aligned} &E_{d,\,\mathrm{LOCC}^{cc}}(\rho_{AB}) = E_{d,\,\mathrm{PPT}^{cc}}(\rho_{AB}) = 0,\\ &E_{c,\,\mathrm{LOCC}^{cc}}(\rho_{AB}) > 0\,. \end{aligned} \tag{14}$$

(d) ***Consequently, entanglement theory is irreversible even under LOCC assisted by correlated catalysts.***

Let us remark here that a different notion of 'catalytic irreversibility' was previously considered in the seminal work of Vidal and Cirac [51]. However, the transformations considered there are much more restricted than the ones allowed in our approach — indeed, they are not truly 'catalytic' in the sense that the preservation of the assisting ancillary system is not actually required, and furthermore no correlations are permitted between the main and the ancillary systems. Our setting is thus strictly more general than that of [51], and as far as we know it is not possible to retrieve our findings on catalytic bound entanglement using results from [51] only.

An additional consequence of the bound in Proposition 1 is that the entanglement cost of any NPT entangled state is non-zero, even under PPT-preserving operations assisted by correlated catalysis.

A crucial ingredient in our proofs is the measured relative entropy of entanglement $D^{\mathbb{PPT}}_{\mathrm{PPT}}$, which belongs to a family of entanglement measures first studied by Piani in a pioneering work [50]. An important feature of this quantity is that it satisfies strong superadditivity, and in fact it allows for the establishment of a superadditivity–like relation for the relative entropy of entanglement D_{PPT} itself: it holds that [50]

$$D_{\mathrm{PPT}}\left(\rho_{AA':BB'}\right) \geq D_{\mathrm{PPT}}(\rho_{A:B}) + D^{\mathbb{PPT}}_{\mathrm{PPT}}(\rho_{A':B'}). \tag{15}$$

This remarkable relation allows us to avoid having to rely solely on the properties of D_{PPT}, which — as we discussed before — are not sufficient to use this quantity in the catalytic setting.

Coherence Quantum coherence is another important example of quantum resource [22–25]. On the formal level, its theory shares many similarities with entanglement. Instead of separable states here we have incoherent states, i.e., states that are diagonal in a fixed basis (computational basis). The unit of pure coherence is the coherence bit $|+\rangle \coloneqq \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$. As for the set of free operations, several choices are possible, including strictly incoherent operations (SIO) [24, 26, 52–54], incoherent operations (IO) [23, 24], dephasing-covariant incoherent operations (DIO) [55–57], maximal incoherent operations (MIO) [22].

For each one of these sets $\mathcal{F}$, and for each $\widetilde{\mathcal{F}} \in \{\mathcal{F}, \mathcal{F}^c, \mathcal{F}^{cc}\}$, we can define the corresponding distillable coherence $C_{d,\,\widetilde{\mathcal{F}}}$ and coherence cost $C_{c,\,\widetilde{\mathcal{F}}}$ as in (6), by replacing Φ_2 with $|+\rangle\langle+|$. All of these quantities have been computed in the unassisted case where catalysis is not considered [24, 54, 57]. For example, it is known that for $\mathcal{F} \in \{\mathrm{IO}, \mathrm{DIO}, \mathrm{MIO}\}$ the distillable coherence satisfies $C_{d,\,\mathcal{F}}(\rho) = C_r(\rho) \coloneqq S(\Delta(\rho)) - S(\rho)$, where C_r is known as the relative entropy of coherence [23, 24]. Here, $\Delta(\cdot) \coloneqq \sum_i |i\rangle\langle i|\,(\cdot)\,|i\rangle\langle i|$ is the dephasing map. On the contrary, coherence is generically bound, i.e., undistillable, under SIO [26]. As for the coherence cost, $C_{c,\,\mathrm{DIO}}(\rho) = C_{c,\,\mathrm{MIO}}(\rho) = C_r(\rho)$ so that the theory is reversible under MIO/DIO, while under SIO/IO it holds that $C_{c,\,\mathrm{SIO}}(\rho) = C_{c,\,\mathrm{IO}}(\rho) = C_f(\rho) \coloneqq \inf_{\rho=\sum_x p_x \psi_x} \sum_x p_x S(\Delta(\psi_x))$, where the infimum that defines the coherence of formation C_f is over all pure state decompositions of ρ [24].

We can now meaningfully ask: *does catalysis help asymptotically in either coherence distillation or coherence dilution?* Since coherence is already reversible under DIO and MIO, we focus on SIO and IO. The result below answers this question very generally in the negative for dilution under both SIO and IO, and for distillation under IO.

Proposition 3. *The IO distillable coherence and the SIO/IO coherence cost of any state do not change if one allows assistance by either catalysts or correlated catalysts. Formally, for $\mathcal{F} \in \{\mathrm{IO}, \mathrm{IO}^c, \mathrm{IO}^{cc}\}$, and for all states ρ,*

$$C_{d,\,\mathcal{F}}(\rho) = C_r(\rho)\,. \tag{16}$$

Analogously, for $\widetilde{\mathcal{F}} \in \{\mathrm{SIO}, \mathrm{SIO}^c, \mathrm{SIO}^{cc}, \mathrm{IO}, \mathrm{IO}^c, \mathrm{IO}^{cc}\}$ and for all ρ,

$$C_{c,\,\mathcal{F}}(\rho) = C_f(\rho)\,. \tag{17}$$

The above result shows conclusively that the fundamental irreversibility of the resource theory of quantum coherence under SIO/IO persists even if catalytic transformations are included into the picture, a finding that goes substantially beyond what was previously known [24].

References

[1] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, 2009.

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

[3] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, 1996.

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

[5] Sandu Popescu and Daniel Rohrlich. Thermodynamics and the measure of entanglement. *Phys. Rev. A*, 56:R3319–R3321, 1997.

[6] Pawel Horodecki, Ryszard Horodecki, and Michal Horodecki. Entanglement and thermodynamical analogies. 1998.

[7] Fernando G. S. L. Brandão, Michał Horodecki, Jonathan Oppenheim, Joseph M. Renes, and Robert W. Spekkens. Resource Theory of Quantum States Out of Thermal Equilibrium. *Phys. Rev. Lett.*, 111:250404, 2013.

[8] K. Audenaert, M. B. Plenio, and J. Eisert. Entanglement Cost under Positive-Partial-Transpose-Preserving Operations. *Phys. Rev. Lett.*, 90:027901, 2003.

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

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

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

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

[13] Runyao Duan, Yuan Feng, and Mingsheng Ying. Entanglement-assisted transformation is asymptotically equivalent to multiple-copy transformation. *Phys. Rev. A*, 72:024306, 2005.

[14] Matthew Klimesh. Inequalities that Collectively Completely Characterize the Catalytic Majorization Relation. 2007.

[15] S. Turgut. Catalytic transformations for bipartite pure states. *J. Phys. A: Math. Theor.*, 40:12185, 2007.

[16] Naoto Shiraishi and Takahiro Sagawa. Quantum Thermodynamics of Correlated-Catalytic State Conversion at Small Scale. *Phys. Rev. Lett.*, 126:150502, 2021.

[17] Tulja Varun Kondra, Chandan Datta, and Alexander Streltsov. Catalytic Transformations of Pure Entangled States. *Phys. Rev. Lett.*, 127:150503, 2021.

[18] Patryk Lipka-Bartosik and Paul Skrzypczyk. Catalytic Quantum Teleportation. *Phys. Rev. Lett.*, 127:080502, 2021.

[19] L. Lami, B. Regula, and A. Streltsov. Catalysis cannot overcome bound entanglement. *Preprint arXiv:2305.03489*, 2023.

[20] V. Vedral and M. B. Plenio. Entanglement Measures and Purification Procedures. *Phys. Rev. A*, 57:1619–1633, 1998.

[21] Masahito Hayashi. *Quantum Information: An Introduction*. Springer Science & Business Media, 2006.

[22] Johan Aberg. Quantifying Superposition. 2006.

[23] T. Baumgratz, M. Cramer, and M. B. Plenio. Quantifying Coherence. *Phys. Rev. Lett.*, 113:140401, 2014.

[24] Andreas Winter and Dong Yang. Operational resource theory of coherence. *Phys. Rev. Lett.*, 116:120404, 2016.

[25] Alexander Streltsov, Gerardo Adesso, and Martin B. Plenio. Quantum coherence as a resource. *Rev. Mod. Phys.*, 89:041003, 2017.

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

[27] E. M. Rains. A semidefinite program for distillable entanglement. *IEEE Trans. Inf. Theory*, 47:2921–2933, 2001.

[28] Michal Horodecki. Entanglement Measures. *Quant. Inf. Comput.*, 1:3–26, 2001.

[29] Johan Åberg. Catalytic Coherence. *Phys. Rev. Lett.*, 113:150402, 2014.

[30] Matteo Lostaglio, Kamil Korzekwa, David Jennings, and Terry Rudolph. Quantum Coherence, Time-Translation Symmetry, and Thermodynamics. *Phys. Rev. X*, 5:021001, 2015.

[31] Henrik Wilming, Rodrigo Gallego, and Jens Eisert. Axiomatic Characterization of the Quantum Relative Entropy and Free Energy. *Entropy*, 19:241, 2017.

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

[33] N. Shiraishi and T. Sagawa. Quantum thermodynamics of correlated-catalytic state conversion at small scale. *Phys. Rev. Lett.*, 126:150502, 2021.

[34] T. V. Kondra, C. Datta, and A. Streltsov. Catalytic transformations of pure entangled states. *Phys. Rev. Lett.*, 127:150503, 2021.

[35] Soorya Rethinasamy and Mark M. Wilde. Relative entropy and catalytic relative majorization. *Phys. Rev. Res.*, 2:033455, 2020.

[36] H. Wilming. Entropy and Reversible Catalysis. *Phys. Rev. Lett.*, 127:260402, 2021.

[37] Dong Yang, Michał Horodecki, Ryszard Horodecki, and Barbara Synak-Radtke. Irreversibility for All Bound Entangled States. *Phys. Rev. Lett.*, 95:190501, 2005.

[38] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying Entanglement. *Phys. Rev. Lett.*, 78:2275–2279, 1997.

[39] Matthew J. Donald and Michał Horodecki. Continuity of relative entropy of entanglement. *Physics Letters A*, 264:257–260, 1999.

[40] Barbara Synak-Radtke and Michał Horodecki. On asymptotic continuity of functions of quantum states. *J. Phys. A: Math. Gen.*, 39:L423, 2006.

[41] Matthew J. Donald, Michał Horodecki, and Oliver Rudolph. The uniqueness theorem for entanglement measures. *J. Math. Phys.*, 43:4252–4272, 2002.

[42] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for entanglement measures. *Phys. Rev. Lett.*, 84:2014–2017, 2000.

[43] Hisaharu Umegaki. Conditional expectation in an operator algebra, IV (Entropy and information). *Kodai Math. Sem. Rep.*, 14:59–85, 1962.

[44] Fumio Hiai and Dénes Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Commun. Math. Phys.*, 143:99–114, 1991.

[45] Roberto Rubboli and Marco Tomamichel. Fundamental Limits on Correlated Catalytic State Transformations. *Phys. Rev. Lett.*, 129:120506, 2022.

[46] C. Datta, T. V. Kondra, M. Miller, and A. Streltsov. Catalysis of entanglement and other quantum resources. 2022.

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

[48] D. Yang, M. Horodecki, and Z. D. Wang. Conditional entanglement. 2007.

[49] D. Yang, M. Horodecki, and Z. D. Wang. An additive and operational entanglement measure: Conditional entanglement of mutual information. *Phys. Rev. Lett.*, 101:140501, 2008.

[50] M. Piani. Relative Entropy of Entanglement and Restricted Measurements. *Phys. Rev. Lett.*, 103:160504, 2009.

[51] G. Vidal and J. I. Cirac. Irreversibility in Asymptotic Manipulations of Entanglement. *Phys. Rev. Lett.*, 86:5803–5806, 2001.

[52] Benjamin Yadin, Jiajun Ma, Davide Girolami, Mile Gu, and Vlatko Vedral. Quantum Processes Which Do Not Use Coherence. *Phys. Rev. X*, 6:041028, 2016.

[53] Qi Zhao, Yunchao Liu, Xiao Yuan, Eric Chitambar, and Xiongfeng Ma. One-Shot Coherence Dilution. *Phys. Rev. Lett.*, 120:070403, 2018.

[54] L. Lami. Completing the Grand Tour of Asymptotic Quantum Coherence Manipulation. *IEEE Trans. Inf. Theory*, 66:2165–2183, 2020.

[55] Eric Chitambar and Gilad Gour. Critical examination of incoherent operations and a physically consistent resource theory of quantum coherence. *Phys. Rev. Lett.*, 117:030401, 2016.

[56] Iman Marvian and Robert W. Spekkens. How to quantify coherence: Distinguishing speakable and unspeakable notions. *Phys. Rev. A*, 94:052324, 2016.

[57] Eric Chitambar. Dephasing-covariant operations enable asymptotic reversibility of quantum resources. *Phys. Rev. A*, 97:050301, 2018.

Quantum simulation of partial differential equations via Schrodingerisation

Nana Liu[1]

[1]*Shanghai Jiao Tong University*

Abstract. Quantum simulators were originally proposed to be helpful for simulating one partial differential equation (PDE) in particular – Schrodinger's equation. If quantum simulators can be useful for simulating Schrodinger's equation, it is hoped that they may also be helpful for simulating other PDEs. It turns out that by transforming a linear partial differential equation (PDE) into a higher-dimensional space, it can be transformed into a system of Schrodinger's equations, which is the natural dynamics of quantum devices. This new method – called Schrodingerisation [1,2] – allows one to simulate, in a simple way, any general linear partial differential equation and system of linear ordinary differential equations via quantum simulation.

This formulation gives us enough flexibility to allow simulation on both qubit-based and continuous-variable quantum systems. The continuous-variable representation is via qumodes and can be more natural for PDEs since, unlike most computational methods, one does not need to discretise the PDE first. In this way, we can directly map D-dimensional linear PDEs onto a (D + 1)-qumode quantum system where analog Hamiltonian simulation on (D + 1) qumodes can be used [3].

I will introduce the idea of Schrodingerisation and a body of work using this framework. I show how this method can be applied to linear PDEs, certain nonlinear PDEs and nonlinear ordinary differential equations (ODEs) [4, 5]. It can also be applied to problems in discrete linear dynamics systems and linear algebra [6] by transforming iterative methods in linear algebra into evolution of ODEs. For realistic problems, this method can be adapted to also solve boundary value problems like physical boundary conditions, interface conditions [7] and quantum dynamics with artificial boundary conditions [8]. I will also present new protocols for simulating linear PDEs with random coefficients [3, 9], which is important in uncertainty quantification.

[1] Quantum simulation of partial differential equations via Schrodingerisation, Shi Jin, Nana Liu, Yue Yu, arXiv: 2212.13969, 2022

[2] Quantum simulation of partial differential equations: applications and detailed analysis, Shi Jin, Nana Liu, Yue Yu, arXiv: 2212.14703, Physical Review A (Accepted), 2023

[3] Analog quantum simulation of partial differential equations, Shi Jin, Nana Liu, arXiv: 2308.00646, 2023

[4] Quantum algorithms for computing observables of nonlinear partial differential equations, Shi Jin, Nana Liu, arXiv: 2022.07834

[5] Time complexity analysis of quantum algorithms via linear representations for nonlinear ordinary and partial differential equations, Shi Jin, Nana Liu, Yue Yu, Journal of Computational Physics, Vol 487, 112149, 2023

[6] Quantum simulation of discrete linear dynamical systems and simple iterative methods in linear algebra via Schrodingerisation, Shi Jin, Nana Liu, arXiv: 2304.02865, 2023

[7] Quantum simulation for partial differential equations with physical boundary or interface conditions, Shi Jin, Xiantao Li, Nana Liu, Yue Yu, arXiv:2305.02710, 2023

[8] Quantum Simulation for Quantum Dynamics with Artificial Boundary Conditions, Shi Jin, Xiantao Li, Nana Liu, Yue Yu, arXiv:2304.00667 2023

[9] Quantum algorithms for uncertainty quantification: application to partial differential equations, Francoise Golse, Shi Jin, Nana Liu, arXiv: 2022.112200, 2022

Quantum State Preparation with Optimal Circuit Depth: Implementations and Applications

Xiao-Ming Zhang[1] Tongyang Li[1] Xiao Yuan[1] *

[1] *Center on Frontiers of Computing Studies, Department of Computer Science, Peking University, Beijing, China*

Abstract. We show that any n-qubit quantum state can be prepared with a $\Theta(n)$-depth circuit using only single- and two-qubit gates. For sparse quantum states with $d \geqslant 2$ non-zero entries, we can reduce the circuit depth to $\Theta(\log(nd))$ with $O(nd \log d)$ ancillary qubits. The algorithm for sparse states is exponentially faster than best-known results and the number of ancillary qubits is nearly optimal and only increases polynomially with the system size. We discuss applications of the results in different quantum computing tasks, such as Hamiltonian simulation, solving linear systems of equations, and realizing quantum random access memories.

Keywords: quantum state preparation, quantum circuit, Hamiltonian simulation, quantum random access memory

1 Background

Quantum state preparation (QSP) is one of the most fundamental tasks in quantum information processing (QIP). For a n-qubit system, the goal of QSP is to construct the quantum state

$$|\psi\rangle = \sum_{k=0}^{2^n-1} a_k |k\rangle \tag{1}$$

from a trivial initial state, such as $|0\rangle^{\otimes n}$, and given the classical description of $[a_0, a_1, \cdots, a_{2^n-1}]$. Here, $a_k \in \mathbb{C}$, $\sum_{k=0}^{N-1} |a_k|^2 = 1$, and $|k\rangle \equiv |k_n k_{n-1} \cdots k_1\rangle$ being the basis with bits k_j for $j = 1, 2, \ldots, n$. QSP is also of practical interest, as it determines the efficiency of inputting classical data into a quantum computer. QSP plays a critical subroutine for many quantum algorithms in machine learning [12–14] and quantum simulation [5, 15]. As an example, block-encoding has broad applications in Hamiltonian simulation, solving linear systems, etc. It can be realized with QSP together with a selector oracle.

Circuit depth measures the runtime of QSP. Without ancillary qubit, exponential circuit depth is inevitable to prepare an arbitrary quantum state [17]. Leveraging ancillary qubits, the circuit depth could be reduced to be sub-exponential scaling [18, 19, 22, 23], indicating a space-time trade-off of QSP.

On the other hand, in minimizing circuit depth, the sub-exponential circuit depth is only achievable with exponential space complexity, which could be challenging for near-term quantum devices. Moreover, strong data structure assumptions leave space for quantum-inspired classical algorithms. With a classical data structure enabling l^2 sampling, there are classical algorithms with poly-logarithmic runtime dequantizing the quantum algorithms for recommendation systems [20], solving linear systems [2, 7], semidefinite programs [3], etc. These results show that space resources should not be neglected when discussing the quantum exponential advantages.

In practice, the data may behave with a certain structure enabling the significant simplification of QSP. Therefore, a task of more practical interest is to find QSP protocol for target states with certain structures. A typical scenario that has both theoretical and practical relevance is the sparse quantum state, because *sparsity* is a very common property in both classical and quantum information processing. Using a constant number of ancillary qubits, arbitrary d-sparse quantum states (with d non-zero entries) can be prepared using a circuit depth of $O(dn)$ [6, 9, 16]. However, it was unclear if the QSP for sparse target state could be further sped up. The fundamental speed limit of sparse state preparation is still an open question, which is important for studying the ultimate power of QIP.

2 General state preparation

For arbitrary target states, we developed a QSP protocol with linear circuit depth. The result is summarized as follows.

Theorem 1 *With only single- and two-qubit gates, an arbitrary n-qubit quantum state can be deterministically prepared with a circuit depth $\Theta(n)$ and $O(2^n)$ ancillary qubits.*

Theorem. 1 saturates the circuit depth lower bound [19, 22]. We were aware that there are other two comparable schemes also achieving linear circuit depth with $O(2^n)$ [19] and $\tilde{O}(2^n)$ [18] ancillary qubits shortly before our work. Our scheme is simpler, because each qubit only connects to a constant number (three) of other qubits, while [18, 19] assume all-to-all connectivity (Fig. 1).

The hardware architecture used for general state preparation is illustrated in Fig. 1. In practical implementation, it can be realized with non-local quantum gates based on teleportated CNOT gates. Alternatively, it can also be realized fault-tolerantly with *nearest-neighbour coupled* qubit arrays based on surface code and lattice surgery, at the cost of a mild increasing of ancillary qubit complexity to $O(n^2 2^n)$.

*xiaoyuan@pku.edu.cn

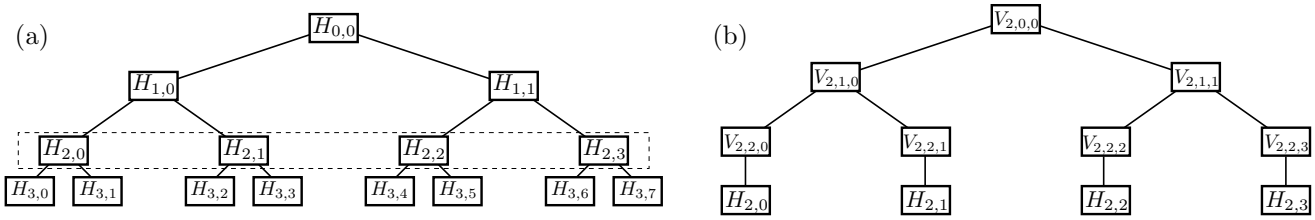


Figure 1: Hardware architecture for general QSP taking $n = 3$ as an example. Each rectangle represents a qubit and each solid line represents the connectivity between two qubits. (a) The architecture contains a binary tree H with $(n + 1)$ layers. (b) Each layer of H connects to the leaf layer of another binary tree. For example, the third layer of H connects to a three-layer binary tree.

Table 1: Space and time complexities for SLS when $|b\rangle$ contains $d = O(\text{poly}(n))$ nonzero elements. "$O(1)$-sparse" corresponds to $P, \alpha, d = O(1)$. We have defined $\kappa_F \equiv \|\hat{H}\|_F/\|\hat{H}\|$ with $\|\cdot\|_F$ the Frobenius norm, and κ is the condition number of H. Both quantum sequential and quantum parallel methods use the algorithm in [4] with the qubitization technique for Hamiltonian simulation [15], and the sparse state preparation method in Theorem. 2. See technical manuscript for details.

Algorithm	Time	Space	Time ($O(1)$-sparse)	Space ($O(1)$-sparse)
Quantum-inspired [2, 7]	$\tilde{O}(\text{poly}(n, \kappa, \kappa_F))$	$O(n2^n P)$	$\tilde{O}(\text{poly}(n, \kappa, \kappa_F))$	$O(n2^n)$
Quantum sequential	$\tilde{O}(nP\alpha\,\text{poly}(\kappa))$	$O(\log P + \text{poly}(n))$	$\tilde{O}(n\,\text{poly}(\kappa))$	$O(n)$
Quantum parallel	$\tilde{O}(\log(nP)\alpha\,\text{poly}(\kappa))$	$O(P\,\text{poly}(n))$	$\tilde{O}(\log(n)\text{poly}(\kappa))$	$O(n)$

3 Sparse state preparation

For sparse target states, we developed an independent protocol with circuit depth increasing logarithmically with both qubit number n and the number of nonzero elements of the target state d. The result is summarized as follows.

Theorem 2 *With only single- and two-qubit gates, an arbitrary n-qubit, d-sparse ($d \geqslant 2$) quantum state can be deterministically prepared with a circuit depth $\Theta(\log(nd))$ and $O(nd \log d)$ ancillary qubits.*

Theorem. 2 improves the best-known circuit depth for sparse state preparation [6, 9, 16] *exponentially*, and also saturates the fundamental lower bound of circuit depth. The required number of ancillary qubits increases only (near) linear with n and d, while only constant connections between qubits are required.

4 Applications

Based on the QSP results in Theorem. 1 and Theorem. 2, and other relevant techniques, we find applications in the fields of Hamiltonian simulation and quantum machine learning. The applications are summarized as follows.

Quantum simulation. We have considered the quantum simulation with Hamiltonian in the form of

$$H = \sum_{p=1}^{P} \alpha_p V_p, \tag{2}$$

where $P = O(\text{poly}(n))$, $\alpha_p > 0$, and $\hat{V}(p) = \bigotimes_{l=0}^{n-1} \hat{V}_l(p)$ and $\hat{V}_l(p) \in \text{SU}(2)$. This type of Hamiltonians contains most of the scenarios in condense matter physics and quantum chemistry. By combining our QSP protocol and relevant techniques with the qubitization algorithm [15], we develop an algorithm for simulating e^{-iHt} with runtime $O\left(\log(nP)(\alpha t + \log(1/\varepsilon))\right)$, where $\alpha = \sum_p \alpha_p$ and ε is the error. As a comparison, for conventional methods based on ancillary-free state preparation, the runtime is typically linear with n and P.

Quantum solving linear system (SLS). Given a square matrix H and vector b, the task for quantum SLS is to output a wave function $|x\rangle$ proportional to $H^{-1}b$. It has been shown that quantum algorithms can solve the quantum SLS problem with polylogarithmic runtime [1, 4, 12, 21]. However, provided similar data structure for classical algorithms, the same task can be equivalently solved using quantum-inspired algorithms, also with polylogarithmic runtime [2, 7, 20]. So it remains open questions whether the exponential quantum advantage for SLS exists, and in what scenarios it can be expected. Based on our sparse state preparation and relevant techniques, we show that when b is sparse, and H can be decomposed in the form of Eq. (2) , there exist exponential quantum advantages, even compared to the best-known classical quantum-inspired algorithm. The comparison is summarized in Table. 1.

Quantum random access memory (QRAM). QRAM is an important type of data structures for quantum machine learning [8, 10, 11]. Conventional scheme for QRAM requires $O(\log N)$ circuit depth using $O(N)$ ancillary qubits, where N is the data dimension. We show that when the classical data is sparse, both space and time resources for QRAM can be significantly reduced. In particular, for N-dimensional classi-

cal data with d non-zero elements, our protocol requires $O(\log(d \log N))$ circuit depth and $O(d \log N)$ ancillary qubit. When d is independent of n, exponential improvement can be expected for both time and space complexities.

5 Significance

We have answered the question of what is the fundamental speed limit of preparing sparse and non-sparse quantum states. Moreover, the resource, such as connectivity, ancillary qubit number, and classical preprocessing time required to achieve the speed limit cannot be significantly reduced further. Based on our techniques for QSP, we find exponential speedups in the fields of Hamiltonian simulation, solving linear systems and QRAM. Our results therefore provide significant advances in QIP, in both fundamental and application aspects.

Technical version:
https://doi.org/10.1103/PhysRevLett.129.230504

References

[1] Shantanav Chakraborty, András Gilyén, and Stacey Jeffery. The power of block-encoded matrix powers: Improved regression techniques via faster Hamiltonian simulation. In *Proceedings of the 46th International Colloquium on Automata, Languages, and Programming*, volume 132 of *Leibniz International Proceedings in Informatics*, pages 33:1–33:14, 2019.

[2] Nai-Hui Chia, András Gilyén, Tongyang Li, Han-Hsuan Lin, Ewin Tang, and Chunhao Wang. Sampling-based sublinear low-rank matrix arithmetic framework for dequantizing quantum machine learning. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 387–400, 2020.

[3] Nai-Hui Chia, Tongyang Li, Han-Hsuan Lin, and Chunhao Wang. Quantum-inspired sublinear algorithm for solving low-rank semidefinite programming. In *45th International Symposium on Mathematical Foundations of Computer Science (MFCS 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020.

[4] 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, 2017.

[5] Andrew M Childs, Dmitri Maslov, Yunseong Nam, Neil J Ross, and Yuan Su. Toward the first quantum simulation with quantum speedup. *Proc. Natl. Acad. Sci.*, 115(38):9456–9461, 2018.

[6] Tiago ML de Veras, Leon D da Silva, and Adenilton J da Silva. Double sparse quantum state preparation. *arXiv:2108.13527*, 2021.

[7] András Gilyén, Zhao Song, and Ewin Tang. An improved quantum-inspired algorithm for linear regression. *arXiv:2009.07268*, 2020.

[8] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum random access memory. *Phys. Rev. Lett.*, 100:160501, Apr 2008.

[9] Niels Gleinig and Torsten Hoefler. An efficient algorithm for sparse quantum state preparation. In *2021 58th ACM/IEEE Design Automation Conference (DAC)*, pages 433–438, 2021.

[10] Connor T Hann, Chang-Ling Zou, Yaxing Zhang, Yiwen Chu, Robert J Schoelkopf, Steven M Girvin, and Liang Jiang. Hardware-efficient quantum random access memory with hybrid quantum acoustic systems. *Phys. Rev. Lett.*, 123(25):250501, 2019.

[11] Connor T. Hann, Gideon Lee, S.M. Girvin, and Liang Jiang. Resilience of quantum random access memory to generic noise. *PRX Quantum*, 2:020311, Apr 2021.

[12] Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.*, 103(15):150502, 2009.

[13] Iordanis Kerenidis and Anupam Prakash. Quantum recommendation systems. *arXiv:1603.08675*, 2016.

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

[15] Guang Hao Low and Isaac L Chuang. Hamiltonian simulation by qubitization. *Quantum*, 3:163, 2019.

[16] Emanuel Malvetti, Raban Iten, and Roger Colbeck. Quantum circuits for sparse isometries. *Quantum*, 5:412, 2021.

[17] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[18] Gregory Rosenthal. Query and depth upper bounds for quantum unitaries via Grover search. *arXiv:2111.07992*, 2021.

[19] Xiaoming Sun, Guojing Tian, Shuai Yang, Pei Yuan, and Shengyu Zhang. Asymptotically optimal circuit depth for quantum state preparation and general unitary synthesis. *arXiv:2108.06150v2*, 2021.

[20] Ewin Tang. A quantum-inspired classical algorithm for recommendation systems. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 217–228, 2019.

[21] Leonard Wossnig, Zhikuan Zhao, and Anupam Prakash. Quantum linear system algorithm for dense matrices. *Phys. Rev. Lett.*, 120(5):050502, 2018.

[22] Xiao-Ming Zhang, Man-Hong Yung, and Xiao Yuan. Low-depth quantum state preparation. *Phys. Rev. Research*, 3:043200, Dec 2021.

[23] Zhicheng Zhang, Qisheng Wang, and Mingsheng Ying. Parallel quantum algorithm for hamiltonian simulation. *arXiv:2105.11889*, 2021.

The Nonequilibrium Cost of Accurate Information Processing

Giulio Chiribella[1 2 3 *] Fei Meng[1 4] Renato Renner[5] Man-Hong Yung[6]

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong SAR, China*
[2] *Department of Computer Science, University of Oxford, Parks Road, Oxford, UK*
[3] *Perimeter Institute for Theoretical Physics, 31 Caroline St North, Waterloo, ON N2L 2Y5, Canada*
[4] *Department of Physics, Southern University of Science and Technology, Shenzhen 518055, China*
[5] *Institute for Theoretical Physics, ETH Zürich*
[6] *Shenzhen Key Laboratory of Quantum Science and Engineering, Shenzhen 518055, China*
[7] *Department of Computer Science, City University of Hong Kong, Hong Kong SAR, China*

Abstract. Accurate information processing is crucial both in technology and in nature. To achieve it, any information processing system needs a supply of resources away from thermal equilibrium. Here we establish a fundamental limit on the accuracy achievable with a given amount of nonequilibrium resources. The limit applies to arbitrary information processing tasks and arbitrary information processing systems subject to the laws of quantum mechanics. It is easily computable and is expressed in terms of an entropic quantity, which we name reverse entropy, associated to a time reversal of the information processing task under consideration. The limit is achievable for all deterministic classical computations and for all their quantum extensions. As an application, we establish the optimal tradeoff between nonequilibrium and accuracy for the fundamental tasks of storing, transmitting, cloning, and erasing information. Our results set a target for the design of new devices approaching the ultimate efficiency limit, and provide a framework for demonstrating thermodynamical advantages of quantum devices over their classical counterparts. This work has been published on Nature Communication **13**, 7155 (2022).

Keywords: quantum thermodynamics, resource theory, quantum advantage

1 Introduction

At the fundamental level, information is stored into patterns that stand out from the thermal fluctuations of the surrounding environment. In order to achieve deviations from thermal equilibrium, any information processing machine needs supplies of systems in a non-thermal state, e.g. batteries. For example, an ideal copy machine for classical data replication requires at least one clean bit initialized in a pure state, say $|0\rangle$, for every bit it copies [1]. Without sufficient supply of non-thermal state, coppying cannot be made perfect. For a general information processing task, a fundamental question is: what is the minimum amount of nonequilibrium needed to achieve a target level of accuracy? This question is especially prominent at the quantum scale, where many tasks cannot be achieved perfectly even in principle, as illustrated by the no-cloning theorem.

In recent years, there has been a growing interest in the interplay between quantum information and thermodynamics [2, 3, 4], motivated both by fundamental questions [5, 6, 7, 8, 9] and by the experimental realisation of new quantum devices [10, 11, 12]. Research in this area led to the development of resource-theoretic frameworks that can be used to study thermodynamics beyond the macroscopic limit [13, 14, 15, 16, 17, 18, **?**, 19, 20]. These frameworks have been applied to characterise thermodynamically allowed state transitions, to evaluate the work cost of logical operations [21, 22] and to study information erasure and work extraction in the quantum regime [23, 24, 25]. From a different perspective, relations between accuracy and entropy production have been investigated in the field of stochastic thermodynamics [26, 27, 28, 29, 30], referring to specific physical models such as classical Markovian systems in nonequilibrium steady states.

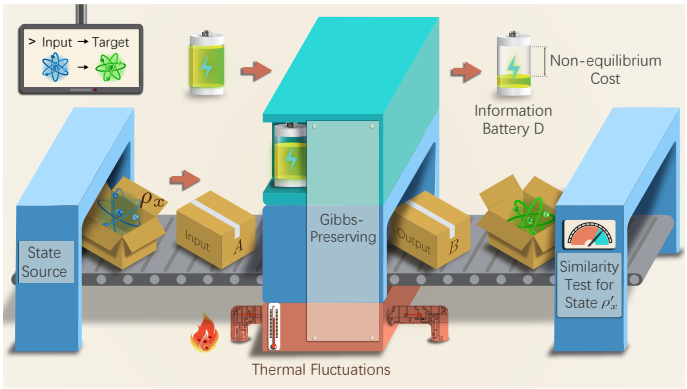


Figure 1: **The nonequilibrium cost of accurate information processing.** A source generates a set of input states for an information processing machine. The machine uses an information battery (a supply of qubits initialised in a fixed pure state) and thermal fluctuations (a reservoir in the Gibbs state as a source of randomness) to transform the input state ρ_x into an approximation of the ideal target state ρ'_x. Finally, the similarity between the output and the target is assessed by a measurement. The number of pure qubits consumed by the machine is the nonequilibrium cost that needs to be paid in order to achieve the desired level of accuracy.

Here, we establish a fundamental tradeoff between accuracy and nonequilibrium, valid at the quantum scale

*giulio@cs.hku.hk

and applicable to arbitrary information processing tasks. Our main result is a bound of nonequilibrium cost by the accuracy, expressed in terms of an entropic quantity, which we call the reverse entropy, associated to a time reversal of the information processing task under consideration. The bound depends only on the task itself, and not on any particular quantum channel implementing it. The bound is attainable for a broad class of tasks, including all deterministic classical computations and all quantum extensions thereof. For the task of erasing, our results generalize Landauer's principle to imperfect erasure. For the tasks of storage, transmission, and cloning of quantum information, our results reveal a thermodynamic advantage of quantum setups over all classical setups that measure the input and generate their output based only on the measurement outcomes. In the cases of storage and transmission, we show that quantum machines can break the ultimate classical limit on the amount of work required to achieve a desired level of accuracy. This result enables the demonstration of work-efficient quantum memories and quantum communication systems outperforming all possible classical setups.

Our results establish a direct link between thermodynamic resources and the accuracy of information processing. They set an ideal target for the design of new devices, and provide a framework for demonstrating a thermodynamic advantage of quantum devices in fundamental tasks such as storing, copying, and transmitting information.

2 Results

The nonequilibrium cost of accuracy. Fundamentally, the goal of information processing is to set up a desired relation between inputs and outputs. In the quantum domain, information processing tasks are often associated to ideal state transformations $\rho_x \mapsto \rho'_x$, in which an input state described by a density operator ρ_x has to be converted into a target output state described by another density operator ρ'_x, where x is a parameter in some given set X. From now on, the input system is denoted by A whose Gibbs state is denoted by Γ_A and the output system is B, whose Gibbs state is Γ_B.

Since every realistic machine is subject to imperfections, the physical realisations of an ideal information processing task can have varying levels of accuracy. Operationally, the accuracy can be quantified by performing a test on the output of the machine and by assigning a score to the outcomes of the measurement. The resulting measure of accuracy is given by the expectation value of a suitable observable O_x, used to assess how similar the output is to the target state ρ'_x. In the worst case over all possible inputs, the accuracy achieved in a given task $\mathcal{T}$ has the expression $\mathcal{F}_{\mathcal{T}}(\mathcal{M}) = \min_x \mathrm{Tr}[O_x \mathcal{M}(\rho_x)]$, where $\mathcal{M}$ is the quantum channel describing the action of the machine.

Accurate information processing generally requires an initial supply of systems away from equilibrium. The amount of nonequilibrium required to implement a given task can be rigorously quantified in a resource theoretic framework where Gibbs states are regarded as freely available, and the only operations that can be performed free of cost are those that transform Gibbs states into Gibbs states [22]. These operations, known as Gibbs preserving, are the largest class of processes that maintain the condition of thermal equilibrium. The initial nonequilibrium resources can be represented in a canonical form by introducing an information battery [21, 22], consisting of an array of qubits with degenerate energy levels. The battery starts off with some qubits in a pure state (hereafter called the "clean qubits"), while all the remaining qubits are in the maximally mixed state. To implement the desired information processing task, the machine will operate jointly on the input system and on the information battery, as illustrated in Figure 1.

The number of clean qubits used by a machine (modeled by a quantum channel $\mathcal{M}$) is an important measure of efficiency, hereafter called the nonequilibrium cost. Let us denote by $c(\mathcal{M}, \Pi_A)$ the minimal nonequilibrium cost required for implementing a given machine $\mathcal{M}$ on input states in the subspace specified by a projector Π_A. When the input subspace is invariant under time evolution, namely $[\Pi_A, H_A] = 0$, where H_A is the Hamiltonian of the input system, the nonequilibrium cost is given [22] by the max relative entropy, $c(\mathcal{M}, \Pi_A) = D_{\max}(\mathcal{M}(\Pi_A \Gamma_A \Pi_A) || \Gamma_B)$ with $D_{\max}(\rho||\sigma) = \log_2 \left\| \sigma^{-\frac{1}{2}} \rho \sigma^{-\frac{1}{2}} \right\|$. We will focus on the cases where the input subspace is invariant under time evolution. This is not a strict restriction, since when the inputs span the whole space, Π_A becomes the identity operator and the requirement is automatically fullfilled.

Then the nonequilibrium cost for achieving accuracy F in a task $\mathcal{T}$ is $c_{\mathcal{T}}(F) := \min\{c(\mathcal{M}, \Pi_A) \mid \mathcal{F}_{\mathcal{T}}(\mathcal{M}) \geq F\}$, minimizing over all possible machines $\mathcal{M}$, which can be formulated as a semi-definite program(SDP). Note that the the specification of the input subspace is included in the task $\mathcal{T}$.

Solving the SDP, we obtain a universal bound for the one-shot nonequilibrium cost, valid for all quantum systems and to all information processing tasks:

$$c_{\mathcal{T}}(F) \geq \kappa_{\mathcal{T}} + \log F \,, \tag{1}$$

where $\kappa_{\mathcal{T}} := -\log F_{\max}^{\mathcal{T}_{\mathrm{rev}}}$ is an entropic quantity, which we call the reverse entropy, and $F_{\max}^{\mathcal{T}_{\mathrm{rev}}}$ is the maximum accuracy allowed by quantum mechanics to a time-reversed information processing task $\mathcal{T}_{\mathrm{rev}} : \rho'_x \mapsto \rho_x, \forall\, x \in X$. Note that the reverse entropy is a monotonically decreasing function of $F_{\max}^{\mathcal{T}_{\mathrm{rev}}}$, and becomes zero when the time-reversed task can be implemented with unit accuracy. Crucially, the reverse entropy depends only on the task under consideration, and not on a specific quantum channel used to implement the task. In fact, the reverse entropy is well defined even for tasks that cannot be perfectly achieved by any quantum channel, as in the case of ideal quantum cloning, and even for tasks that are not formulated in terms of state transitions (see Methods in the published version [31]). This bound is proved to be tight for a number of information processing tasks,

notably including all classical computations and all quantum extensions thereof.

Limit on the accuracy of classical machines. A classical machine can be modelled as a machine that measures the input and produces an output based on the measurement result, which is entanglement breaking. Here we show that entanglement breaking machines satisfy a stricter bound. The minimum nonequilibrium cost over all entanglement breaking machines, denoted by $c^{\rm eb}_{\mathcal{T}}(F)$, must satisfy the inequality

$$c^{\rm eb}_{\mathcal{T}}(F) \geq \max\{\kappa_{\mathcal{T}}, \kappa_{\mathcal{T}^*}\} + \log F\,, \qquad (2)$$

where $\kappa_{\mathcal{T}}$ is the reverse entropy of the state transformation task $\rho_x \to \rho'_x$, and $\kappa_{\mathcal{T}^*}$ is the reverse entropy of the transposed task $\mathcal{T}^*$, corresponding to the state transformation $\rho_x \mapsto (\rho'_x)^T$. This bound can be used to demonstrate that a thermodynamic advantage of general quantum machines over all entanglement binding machines, including in particular all classical machines. For example, we proved that the non-equilibrium cost used by a classical machine to achieve certain level of accuracy, is strictly larger than that of a general quantum machine, as shown in Fig.2

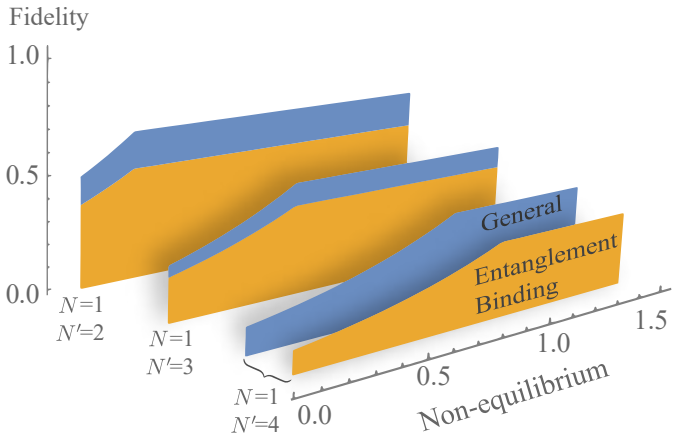


Figure 2: **Entanglement binding machines vs general quantum machines.** The figure illustrates the accessible regions for the cloning fidelity for various values of N and N' in the case of qubits with degenerate Hamiltonian. The values of the fidelity in the blue region are attainable by general quantum machines, while the values in the orange region are attainable by entanglement binding machines. The difference between the two regions indicates a thermodynamic advantage of general quantum machines over all classical machines.

Thermodynamic signature of geniune quantum devices. Quantum machines that are able to preserve free entanglement also offer a thermodynamic advantage in the storage and transmission of quantum states, corresponding to the ideal state transformation $\rho_x \mapsto \rho_x$ where x parametrises the states of interest. In theory, a noiseless quantum machine can achieve perfect accuracy at zero work cost. In practice, however, the transmission is always subject to errors and inefficiencies, resulting into nonunit fidelity and/or nonzero work. For this reason, realistic experiments that aim to demonstrate genuine quantum transmission or storage need criteria to demonstrate superior performance with respect to all classical setups. A popular approach is to demonstrate an experimental fidelity larger than the maximum fidelity achievable by classical schemes. In the qubit case, the maximum classical fidelity is $F^{\rm eb}_{\rm max} = 2/3$ [32], and is often used as a benchmark for quantum communication experiments [33, 34, 35]. Here we provide a different benchmark, in terms of the nonequilibrium cost needed to achieve a target fidelity F. We show that the minimum nonequilibrium cost over all entanglement breaking machines for the storage/transmission of qubit states is

$$c^{\rm eb}_{\rm store/transmit}(F) = \log\left[F + e^{\frac{\Delta E}{kT}}\,\frac{(2F-1)^2}{1-F}\right], \qquad (3)$$

where ΔE is the energy gap of the qubit. Eq. (3) is valid for every qubit Hamiltonian and for every value of F in the interval $[F^{\rm eb}_{\rm min}, F^{\rm eb}_{\rm max}]$, with $F^{\rm eb}_{\rm max} = 2/3$ and $F^{\rm eb}_{\rm min} = (e^{\frac{\Delta E}{kT}}+1)/(2e^{\frac{\Delta E}{kT}}+1)$. The minimum cost $c^{\rm eb}_{\rm store/store}(F)$ can be achieved by state estimation, and therefore can be regarded as the classical limit on the nonequilibrium cost.

For every $F > F_{\rm min}$, the minimum nonequilibrium cost (3) is strictly larger than zero for every nondegenerate Hamiltonian. Since the nonequilibrium cost is a lower bound to the work cost, Eq. (3) implies that every entanglement breaking machine with fidelity F requires at least $kT(\ln 2)\, c^{\rm eb}_{\rm store/transmit}(F)$ work. In theory, this value can be used as a benchmark to certify genuine quantum information processing: every realistic setup that achieves fidelity F with less than $kT\ln\left[F + e^{\frac{\Delta E}{kT}}\,(2F-1)^2/(1-F)\right]$ work will necessarily exhibit a performance that cannot be achieved by any classical setup. Notably, the presence of a thermodynamic constraint (either on the nonequilibrium or on the work) provides a way to certify a quantum advantage even for noisy implementations of quantum memories and quantum communication systems with fidelity below the classical fidelity threshold $F_{\rm max} = 2/3$. This points out new paths in certifying quantum devices but also poseses challenges to acccurately measure the thermodynamic cost of quantum processes experimentally.

3 Conclusion.

We derive fundamental trade-off between the nonequilibirum cost and the accuracy of information processing. Our bound is applicable to single-shot experiments and we prove that they reduce to conventional thermodynamics in the asymptotic limit. Our conceptual contribution is to move from previous results [21, 22] on the nonequilibrium cost of quantum channels to arbitrary information processing tasks. This enables us to establish thermodynamic advantages of quantum devices in transmitting, storing, and cloning quantum information over their classical counterparts.

References

[1] C. H. Bennett, International Journal of Theoretical Physics **21**, 905 (1982).

[2] J. Goold, M. Huber, A. Riera, L. Del Rio, and P. Skrzypczyk, Journal of Physics A: Mathematical and Theoretical **49**, 143001 (2016).

[3] S. Vinjanampathy and J. Anders, Contemporary Physics **57**, 545 (2016).

[4] F. Binder, L. A. Correa, C. Gogolin, J. Anders, and G. Adesso, Fundamental Theories of Physics **195**, 1 (2018).

[5] S. Lloyd, Nature **406**, 1047 (2000).

[6] T. Sagawa and M. Ueda, Physical Review Letters **102**, 250602 (2009).

[7] N. Linden, S. Popescu, and P. Skrzypczyk, Physical Review Letters **105**, 130401 (2010).

[8] J. M. Parrondo, J. M. Horowitz, and T. Sagawa, Nature Physics **11**, 131 (2015).

[9] J. Goold, M. Paternostro, and K. Modi, Physical Review Letters **114**, 060602 (2015).

[10] J. Baugh, O. Moussa, C. A. Ryan, A. Nayak, and R. Laflamme, Nature **438**, 470 (2005).

[11] S. Toyabe, T. Sagawa, M. Ueda, E. Muneyuki, and M. Sano, Nature Physics **6**, 988 (2010).

[12] M. D. Vidrighin, O. Dahlsten, M. Barbieri, M. Kim, V. Vedral, and I. A. Walmsley, Physical Review Letters **116**, 050401 (2016).

[13] D. Janzing, P. Wocjan, R. Zeier, R. Geiss, and T. Beth, International Journal of Theoretical Physics **39**, 2717 (2000).

[14] M. Horodecki, P. Horodecki, and J. Oppenheim, Physical Review A **67**, 062104 (2003).

[15] F. G. Brandao, M. Horodecki, J. Oppenheim, J. M. Renes, and R. W. Spekkens, Physical Review Letters **111**, 250404 (2013).

[16] M. Horodecki and J. Oppenheim, Nature Communications **4**, 2059 (2013).

[17] F. Brandao, M. Horodecki, N. Ng, J. Oppenheim, and S. Wehner, Proceedings of the National Academy of Sciences **112**, 3275 (2015).

[18] F. G. S. L. Brandão and G. Gour, Phys. Rev. Lett. **115**, 070503 (2015).

[19] G. Gour, M. P. Müller, V. Narasimhachar, R. W. Spekkens, and N. Y. Halpern, Physics Reports **583**, 1 (2015).

[20] G. Gour, D. Jennings, F. Buscemi, R. Duan, and I. Marvian, Nature Communications **9**, 1 (2018).

[21] P. Faist, F. Dupuis, J. Oppenheim, and R. Renner, Nature Communications **6**, 7669 (2015b).

[22] P. Faist and R. Renner, Physical Review X **8**, 021011 (2018).

[23] L. Del Rio, J. Åberg, R. Renner, O. Dahlsten, and V. Vedral, Nature **474**, 61 (2011).

[24] J. Åberg, Nature Communications **4**, 1 (2013).

[25] P. Skrzypczyk, A. J. Short, and S. Popescu, Nature Communications **5**, 1 (2014).

[26] U. Seifert, Physica A: Statistical Mechanics and its Applications **504**, 176 (2018).

[27] A. C. Barato and U. Seifert, Physical Review Letters **114**, 158101 (2015).

[28] T. R. Gingrich, J. M. Horowitz, N. Perunov, and J. L. England, Physical Review Letters **116**, 120601 (2016).

[29] A. C. Barato and U. Seifert, Physical Review X **6**, 041053 (2016).

[30] J. M. Horowitz and T. R. Gingrich, Nature Physics **16**, 15 (2020).

[31] G. Chiribella, F. Meng, R. Renner, and M.-H. Yung, Nature Communications **13**, 7155 (2022).

[32] S. Massar and S. Popescu, in *Asymptotic Theory Of Quantum Statistical Inference: Selected Papers* (World Scientific, 2005) pp. 356–364.

[33] B. Li, Y. Cao, Y.-H. Li, W.-Q. Cai, W.-Y. Liu, J.-G. Ren, S.-K. Liao, H.-N. Wu, S.-L. Li, L. Li, *et al.*, Physical Review Letters **128**, 170501 (2022).

[34] Y. Zhong, H.-S. Chang, A. Bienfait, É. Dumur, M.-H. Chou, C. R. Conner, J. Grebel, R. G. Povey, H. Yan, D. I. Schuster, *et al.*, Nature **590**, 571 (2021).

[35] P. Kurpiers, P. Magnard, T. Walter, B. Royer, M. Pechal, J. Heinsoo, Y. Salathé, A. Akin, S. Storz, J.-C. Besse, *et al.*, Nature **558**, 264 (2018).

Experimental realization of entangled coherent states in a trapped ion system

Honggi Jeon[1 2] Jiyong Kang[2 3] Jaeun Kim[2 3] Wonhyeong Choi[2 3 4]
Kyunghye Kim[2 3] Taehyun Kim[2 3 4 5 6 *]

[1] *Department of Physics and Astronomy, Seoul National University, Seoul 08826, Republic of Korea*
[2] *Automation and System Research Institute, Seoul National University, Seoul 08826, Republic of Korea*
[3] *Department of Computer Science and Engineering, Seoul National University, Seoul 08826, Republic of Korea*
[4] *Inter-university Semiconductor Research Center, Seoul National University, Seoul 08826, Republic of Korea*
[5] *Institute of Computer Technology, Seoul National University, Seoul 08826, Republic of Korea*
[6] *Institute of Applied Physics, Seoul National University, Seoul 08826, Republic of Korea*

Abstract. The entangled coherent state, a multipartite extension of the cat state, has been studied in such various fields as quantum optics, quantum information, and quantum communication. It has been experimentally realized with photons and microwave cavities, but not with trapped ions although they have been extensively used in the study of non-classical states. Here, we report the generation and basic characterization of an entangled coherent state that consists of two orthogonal motional modes of a single trapped ion. We generate an entangled coherent state with spin-dependent force and heralded measurement of the spin state, and then observe the modulation of the parity in one of the two modes. We also utilize the two dimensional spin-dependent force to realize Mølmer–Sørensen gates with motion in multiple directions.

Keywords: coherent state, cat state, trapped ion, entanglement, Molmer-Sorensen gate

1 Introduction

In recent decades, there has been extensive theoretical and experimental exploration focused on the coherent state [1]. This particular quantum state possesses remarkably classical attributes due to its minimal spread in phase space, and its time evolution follows the trajectory of a classical harmonic oscillator [2]. The entangled coherent state, an extension of the coherent state to multiple modes, has proven to be a valuable theoretical tool in diverse areas such quantum optics, quantum computing, and quantum communication. Despite their sensitivity to decoherence, entangled coherent states have been experimentally realized in a few experiments involving photons [3] and microwave cavities [4, 5]. The trapped ion has been a very useful tool for studying the quantum world because of its isolation from the environment and precise controllability. Various theoretical studies have explored the implementation of entangled coherent states in trapped ion systems [6, 7, 8, 9], but none have been experimentally implemented so far.

In this work, we present results on the generation and basic characterization of the entangled coherent state of a trapped ion's two-dimensional motion. To accomplish this, we implement a simultaneous spin-dependent force (SDF) on the ion along the two principal axes, X and Y. We accomplish this by carefully adjusting the transverse trap potential to achieve nearly isotropic trap, resulting in the X and Y modes having similar secular frequencies.

We generate Lissajous-curve-like motion in two dimensions with a signle ion, with various commensurate oscillation periods in each direction and observe corresponding periodic variation in the spin state [10]. Then, we decouple the spin from the motion with projective measurement [11] and herald the generation of the entangled coherent state of motion in two transverse axes. Subsequently, we proceed to observe the modulation of phonon number parity, which arises due to the cyclic entanglement and disentanglement of the two motional modes. Additionally, in an ion chain comprising two ions, we successfully generate a Bell state by utilizing the Mølmer–Sørensen(MS) interaction [12, 13]. The geometric phase accumulation is facilitated through motion occurring in two spatial dimensions, which leads to a reduced requirement for the Rabi frequency compared to the one-dimensional scenario.

2 Parity of entangled coherent states

We realize the simultaneous excitation of the X and Y mode by implementing the following interaction Hamiltonian with a bichromatic beam:

$$\hat{H} = \frac{\hbar\Omega\eta_X}{2}\left(\hat{a}_X e^{-i(\delta_X t+\phi_M)} + \hat{a}_X^\dagger e^{i(\delta_X t+\phi_M)}\right)\hat{\sigma}_{\phi_S} + \frac{\hbar\Omega\eta_Y}{2}\left(\hat{a}_Y e^{-i(\delta_Y t+\phi_M)} + \hat{a}_Y^\dagger e^{i(\delta_Y t+\phi_M)}\right)\hat{\sigma}_{\phi_S} \quad (1)$$

η_j and δ_j are the Lamb-Dicke factor for the j-th axis and the detuning from the secular frequency of the j-th axis, and $\hat{a_j}(\hat{a_j}^\dagger)$ is the phonon annihilation (creation) operator for the j-th axis. Ω is the Rabi frequency of the Raman transition. The motion and spin phase of spin-dependent interaction is proportional to the difference, $\phi_M = (\phi_b - \phi_r)/2$, and sum, $\phi_S = (\phi_b + \phi_r)/2$, of the laser phases for the blue and red sidebands, ϕ_b and ϕ_r.

When the above Hamiltonian is applied to the quatnum state of a single ion for a duration t, we get the following wave funtion where $\alpha(t)$ and $\beta(t)$ represent the coordinate of the X and Y mode coherent states in their

*taehyun@snu.ac.kr

respective phase spaces. $|+\rangle$ and $|-\rangle$ are the eigenstates of the spin operator defined by the SDF.

$$|\psi(t)\rangle = \frac{1}{\sqrt{2}}(|+\rangle\,|\alpha(t)\rangle\,|\beta(t)\rangle + |-\rangle\,|-\alpha(t)\rangle\,|-\beta(t)\rangle) \quad (2)$$

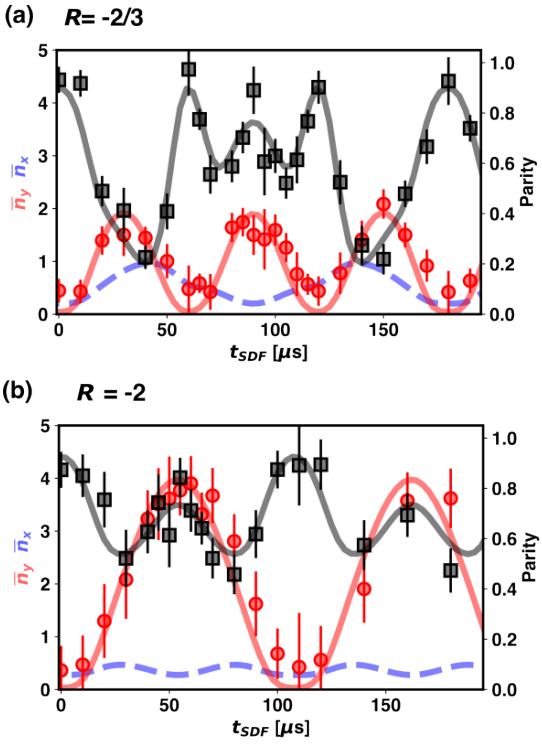


Figure 1: The X mode cat state and the Y mode cat state are excited and de-excited at different frequencies, corresponding to (a) $R = \delta_X/\delta_Y = -2/3$ and (b) $R = \delta_X/\delta_Y = -2$. The black data points are the parity of the Y mode phonon distribution, and the solid lines are fits to the theory. The red data points are mean phonon numbers calculated from the phonon distribution. The red solid lines are the phonon number time evolution predicted from the fitting results.

With a heralded measurement, we project the spin to $|\downarrow\rangle$ resulting in an entangled coherent state of the X and Y modes:

$$|\psi_{ECS}(t)\rangle = |\downarrow\rangle \frac{|\alpha(t)\rangle\,|\beta(t)\rangle + |-\alpha(t)\rangle\,|-\beta(t)\rangle}{\sqrt{2+2e^{-2(|\alpha(t)|^2+|\beta(t)|^2)}}} \quad (3)$$

For various values of $R = \delta_X/\delta_Y$, we observed the time evolution of the phonon distribution of the Y mode, which is modulated by the periodic entanglement with the X mode. The results are shown in Fig. 1. The periodic modulation in the parity of the Y mode is clearly visible and agrees with the theoretical prediction, signaling the entanglement between the X and the Y mode cat states.

3 Mølmer–Sørensen gate with two-dimensional motion

Next, we drive MS interaction in two-dimension by applying the two-dimensional SDF to a chain of two ions

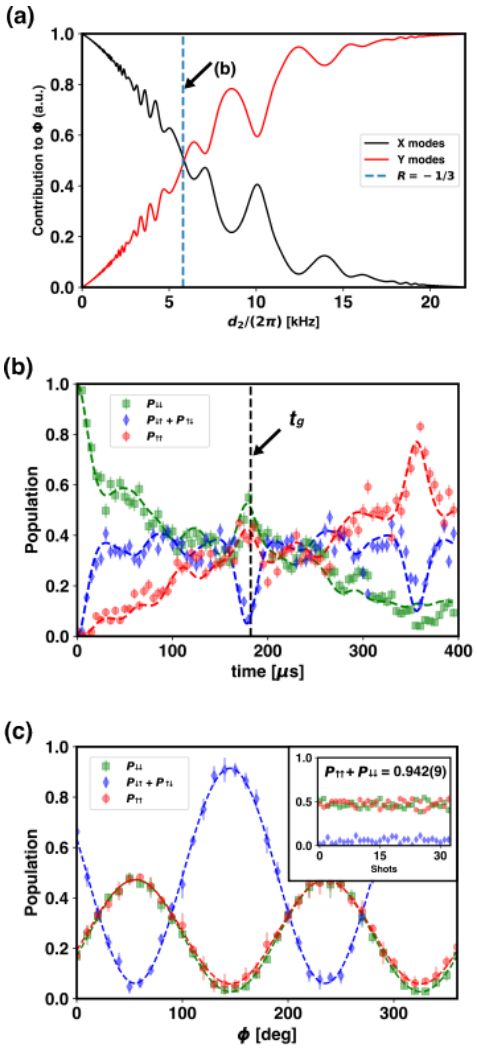


Figure 2: (a) Contribution of the X modes and Y modes to the required geometric phase at various gate detunings. (b) Time evolution of the qubit states under 2D MS interaction. (c) Parity oscillation of the two-qubit states. Population measurement results over 32 trials are shown in the inset.

and observed the successful generation of the Bell state, $1/\sqrt{2}(|00\rangle + |11\rangle)$. In 2D MS interaction, both the X and Y axes phase spaces contribute to the geometric phase, which reduces the required Rabi frequency by approximately $1/\sqrt{2}$. In our case, the two axes contribute equally at a gate detuning $d_2/(2\pi) \simeq 6$ kHz, where d_2 is the detuning between the laser and the center-of-mass mode of the X mode. It is indicated by an arrow in Fig. 2(a) and we observed the time evolution of the two-qubit states, which is shown in Fig. 2(b). By fitting the time evolution results, we confirmed that the required Rabi frequency is $2\pi \times 81.3 \pm 0.6$ kHz which is indeed 28.3% lower compared to using only the X axis, and 30.1% lower compared to using only the Y axis, at the same gate time and gate detuning. From the parity oscillation and population measurement results, we measre a gate fidelity of 89.7 ± 0.6 % which is comparable to our single axis Mølmer–Sørensen gate fidelity, 93.2 ± 0.6 %.

4 Conclusion

We have experimentally implemented two-dimensional SDF by exciting the two transverse modes of a single trapped ion with bichromatic laser beams. We observed the periodic entanglement and disentanglement of the two cat states in the two motional modes, which resulted in the modulation of the phonon number parity. We also trapped a chain of two ions and realized 2D MS interaction with the 2D SDF. The observed time evolution agrees with theoretical prediction, and confirms that the required Rabi frequency is reduced because more phase spaces contribute to the accumulation of geometric phase.

5 Additional Information

A preprint with technical details of this work is available online [14].

References

[1] R. J. Glauber, Phys. Rev. **131**, 2766 (1963).

[2] B. C. Sanders, J. Phys. A: Math. Theor. **45**, 244002 (2012).

[3] A. Ourjoumtsev, F. Ferreyrol, R. Tualle-Brouri, and P. Grangier, Nature Phys **5**, 189 (2009).

[4] Z. Wang, Z. Bao, Y. Wu, Y. Li, W. Cai, W. Wang, Y. Ma, T. Cai, X. Han, J. Wang, Y. Song, L. Sun, H. Zhang, and L. Duan, Science Advances **8**, eabn1778 (2022).

[5] C. Wang, Y. Y. Gao, P. Reinhold, R. W. Heeres, N. Ofek, K. Chou, C. Axline, M. Reagor, J. Blumoff, K. M. Sliwa, L. Frunzio, S. M. Girvin, L. Jiang, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, Science **352**, 1087 (2016).

[6] C. C. Gerry, Phys. Rev. A **55**, 2478 (1997).

[7] X.-B. Zou, J. Kim, and H.-W. Lee, Phys. Rev. A **63**, 065801 (2001).

[8] E. Solano, R. L. d. M. Filho, and N. Zagury, J. Opt. B: Quantum Semiclass. Opt. **4**, S324 (2002).

[9] Z.-R. Zhong, X.-J. Huang, Z.-B. Yang, L.-T. Shen, and S.-B. Zheng, Phys. Rev. A **98**, 032311 (2018).

[10] R. F. Rossetti, G. D. d. M. Neto, J. C. Egues, and M. H. Y. Moussa, EPL **115**, 53001 (2016).

[11] D. Kienzler, C. Flühmann, V. Negnevitsky, H.-Y. Lo, M. Marinelli, D. Nadlinger, and J. Home, Phys. Rev. Lett. **116**, 140402 (2016).

[12] A. Sørensen and K. Mølmer, Phys. Rev. A **62**, 022311 (2000).

[13] J. Benhelm, G. Kirchmair, C. F. Roos, and R. Blatt, Nature Phys **4**, 463 (2008).

[14] H. Jeon, J. Kang, J. Kim, W. Choi, K. Kim, and T. Kim 10.48550/arXiv.2305.00820 (2023).

General Distance Balancing for Quantum Locally Testable Codes

Adam Wills[1 2 *] Ting-Chun Lin[1 3 †] Min-Hsiu Hsieh[1 ‡]

[1] *Hon Hai Research Institute, Taipei*
[2] *DAMTP, Centre for Mathematical Sciences, University of Cambridge, Cambridge CB30WA, UK*
[3] *Department of Physics, University of California San Diego, CA*

Abstract.
In this paper [1], we consider the distance balancing of quantum locally testable codes (qLTCs) using any classical code (with independent checks), where previously only the repetition code had been analysed. Our main result is that the new soundness is at least the old soundness divided by the classical code length (up to a constant factor).

We discuss applications to existing constructions [2, 3, 4], from which we obtain qLTCs of multiple new parameters. In particular, we obtain codes for which soundness times distance exceeds locality with dimension arbitrarily close to square-root, where the previous best was a constant.

Keywords: Quantum locally testable codes, soundness, distance balancing, homological product

1 Extended Abstract

For several decades, researchers have searched for error-correcting codes, both classical and quantum, with novel parameters. The results of this search have had, and continue to have, wide-reaching implications in practice, and also in theory - in areas far beyond the theory of coding alone. A handful of conjectures have been formed over what parameters may be allowed to exist for both classical and quantum codes. There have been some successes, but several natural open problems remain.

The three most commonly considered parameters in the field of LDPC (low-density parity check) coding, whether classical or quantum, are dimension, distance and locality. Let us give a non-technical idea of what these are. A code's dimension is the number of (qu)bits of information that it may be used to encode, while its distance is closely related to the maximum size of an error against which the code may protect. Locality requires a somewhat more technical description involving checks, but it will suffice to say here that locality is (roughly) the maximum number of (qu)bits on which the code acts simultaneously when attempting to determine whether an error has occurred.

It is then natural for one to consider infinite families of codes of a growing size, denoted by N, and the question that one might ask is whether there exists such a family for which these three parameters may simultaneously scale optimally. This requires the dimension and distance to be as large as possible, linear ($\Theta(N)$), and the locality to be as small as possible, constant ($\Theta(1)$). An affirmative answer to this in the classical case has been known since the work of Gallager some 60 years ago [5], but the same result in the quantum case (formerly known as the qLDPC conjecture) was not known until 2021 [6], after two decades of progress.

There are then many further requests that one could make of the code (strictly 'infinite family of codes'). One of the most important is local testability, which is closely related to the parameter 'soundness'. The question behind local testability is, roughly speaking, whether one may determine (with a certain probability) whether a given string of (qu)bits is a valid codeword, by looking at only some small subset of the (qu)bits. The fewer (qu)bits need be viewed to determine this, the better the soundness of the code.

In the classical case, this concept, although simple, has influenced many areas of computer science including cryptography, property testing and many more. Most importantly, locally testable codes play a pivotal role in the proofs of the famed PCP theorem - see for example [7]. As for constructing these codes, the c^3 - conjecture, positing the existence of codes with optimal dimension, distance and locality, as well as the largest possible (constant) soundness, was answered in the affirmative in 2021, almost simultaneously to the resolution of the qLDPC conjecture.

The concept of local testability for quantum codes was first introduced in 2013 by Aharonov and Eldar [9] and is, as an area of study, still likely in its infancy. The notion quickly garnered attention when it was proved in [10] that quantum locally testable codes (qLTCs) of certain parameters would imply the famous NLTS conjecture of Freedman and Hastings [11]. This latter conjecture was subsequently resolved independently [12] but constructing qLTCs with new parameters remains an important, wide-open area due to the hope that qLTCs could have as extensive applications as their classical counterparts, in particular to a possible 'qPCP theorem'.

The end goal of constructing qLTCs of better parameters is to construct a code (again, strictly, 'family of codes') for which the four given parameters (dimension, distance, soundness and locality) are simultaneously optimised. The existence of such a code is the postulate of the qLTC conjecture. Whilst it is hoped that such codes exist, there is no guarantee that they do. In an effort towards resolving this, a line of research has begun constructing codes in new parameter regimes in order to establish what is, in fact, possible.

*adamjwills7248@gmail.com
†til022@ucsd.edu
‡min-hsiu.hsieh@foxconn.com

There have been three papers prior to the present work that aimed to construct qLTCs of new parameters [2, 3, 4]. The former two, [2] and [3], respectively introduce the hypersphere product code and the hemicubic code. These each have very good soundness and locality as well as good distance, but both suffer from the notable deficiency of having constant dimension. Meanwhile, [4] introduces four constructions of qLTCs displaying a variety of parameters. We must be brief here, and so we display only the parameters of all the above constructions most relevant to us: those of the hemicubic code and those of the third construction of [4]. We remind the reader that the qLTC conjecture requires soundness as large as $\Theta(1)$, distance and dimension as large as $\Theta(N)$, as well as locality as small as $\Theta(1)$, in terms of the number of physical qubits N.

Table 1: The parameters of the hemicubic code [3] and the third construction of [4] are shown respectively below. Again, only these two most important to us are displayed for the sake of brevity - but we recommend page 4 of [4] for full details. We note that the latter parameters represent a whole collection of codes - both n and l may be allowed to vary. Examples of this construction may be found via the substitution of values. For example, with N physical qubits, one may set $n = \Theta\left(\frac{N}{\log(N)}\right)$ and $l = \Theta(\log(N))$ to obtain a code of inverse-logarithmic soundness, dimension equal to $\Theta\left(\frac{N}{\log(N)}\right)$, logarithmic distance and constant locality.

	Hemicubic Code [3]	Thm 1.3 of [4]
Physical Qubits	N	$\mathcal{O}(nl)$
Soundness	$\Omega\left(\frac{1}{\log(N)}\right)$	$\Omega(1/l)$
Distance	$\Theta\left(\sqrt{N}\right)$	$\Theta\left(\min(n,l)\right)$
Dimension	$\Theta(1)$	$\Theta(n)$
Locality	$\mathcal{O}\left(\log(N)\right)$	$\Theta(1)$

The constructions of [2] and [3] are largely geometric in nature, whereas those of [4] are more algebraic. In particular, the latter paper makes use of a technique known as 'distance balancing' which is based on a construction from algebraic topology known as the homological product of chain complexes. The distance balancing procedure was previously used in the construction of better qLDPC codes in the pursuit of the qLDPC conjecture. The idea is as follows. Quantum codes (at least the ones we are interested in) have two distances: the X - distance and the Z - distance, unlike classical codes which have one. These two distances are respectively related to the code's ability to correct bit flip errors and phase flip errors. The 'distance' of the quantum code is then the minimum of these two values.

Distance balancing then addresses the issue that arises when a code has good X - distance, but poor Z - distance, or vice versa. A distance balancing procedure will improve the scaling of the worse distance, at the expense of the scaling of the better distance, so that the overall 'distance' of the code may be improved. The first distance balancing construction to be considered was due to Hastings in [13] and an improved method was given in [14] (their Theorem 4.2). The latter paper allows for the combination, via the homological product, of the quantum code with some classical code in order to perform the desired distance balancing. This paper allows for any classical code to be used in this role[1], whereas the former paper of Hastings analyses only the case where the classical code is the repetition code.

The results on the parameters that result from the distance balancing in [14] are stated informally below.

Theorem 1 (Theorem 4.2 of [14], Informal.) *Let us denote the inputted quantum code as Q and the classical code to be used for the distance balancing as C. Let us denote the number of physical (qu)bits of each code as $N(Q)$ and $N(C)$, the dimension of each code as $\dim(Q)$ and $\dim(C)$, the X - and Z - distances of Q as $d_X(Q)$ and $d_Z(Q)$, and finally the distance of C as $d(C)$. The relevant quantities scale under the distance balancing construction as follows.*

$$\begin{aligned} N(Q) &\mapsto \Theta\left(N(Q)N(C)\right) \\ \dim(Q) &\mapsto \dim(Q)\dim(C) \\ d_X(Q) &\mapsto d_X(Q)d(C) \\ d_Z(Q) &\mapsto d_Z(Q) \end{aligned}$$

It is also true that the locality of the resultant quantum code will scale with the maximum of the localities of the inputted quantum code and the classical code that is used. Therefore, when using an optimal classical LDPC code (with constant locality and linear dimension and distance), the scaling of the X - distance is improved at the expense of worsened Z - distance scaling, the scaling of dimension is improved, while the scaling of locality is (at worst) preserved. If the desire is instead to improve the Z - distance at the expense of the X - distance, we simply take the dual of the quantum code before and after the distance balancing is applied. The dual is a simple homological operation that serves only to swap the role of X and Z.

The construction due to Hastings is exactly the same as the above, but the analysis is limited to the case of the classical code being the repetition code. The repetition code is a classical code with linear distance and constant locality, but with the deficiency of having constant dimension. Therefore, under this distance balancing, the same facts about the changes in parameters go through, except that the dimension scaling now worsens.

However, Hastings considers something that Evra et al. do not: soundness. The result relevant to us is stated below.

[1] Here, an important technical caveat for the distance balancing is that the classical code must have independent checks, although this is not in any way restrictive given that optimal classical LDPC codes with independent checks exist [5].

Theorem 2 (Lemma 7 of [13], Informal) *With the same notation as in Theorem 1 and denoting the soundness of the inputted quantum code as $\rho(Q)$, when using a repetition code of length l to balance distances, the soundness changes as follows:*

$$\rho(Q) \mapsto \Omega\left(\frac{\rho(Q)}{l}\right).$$

Our technical contribution is then to generalise this result to the work of [14], in which distance balancing is performed with any classical code. From our paper [1], this is stated as follows:

Theorem 3 (Theorem 1.1 of [1], Informal) *We use the same notation as Theorems 1 and 2. When distance balancing with any classical code[2] of length t, the soundness scales, under reasonable assumptions, as*

$$\rho(Q) \mapsto \Omega\left(\frac{\rho(Q)}{t}\right).$$

We hope this result proves useful in future to obtain codes of new parameters. For now, we discuss applications that can already be stated. The most obvious such application, although not the best, is to the improvement of the parameters of Theorem 1.3 of [4]. The authors first produce a quantum code of constant soundness, linear Z - distance, constant X - distance, linear dimension and constant locality, which is then an ideal candidate for distance balancing. Their Theorem 1.3 then follows from the applications of Theorems 1 and 2 to this code, giving the former parameters shown in Table 2. We may therefore directly improve the dimension scaling by distance balancing with an optimal classical LDPC code rather than the repetition code, as shown in the following table.

Table 2: The first set of parameters on which we improve, and that improvement, is given below. The dimension scaling remains optimal (linear) during distance balancing, rather than becoming worse.

	Thm 1.3 of [4]	New Parameters (1)
Physical Qubits	$\mathcal{O}(nl)$	$\mathcal{O}(nt)$
Soundness	$\Omega(1/l)$	$\Omega(1/t)$
Distance	$\Theta(\min(n,l))$	$\Theta(\min(n,t))$
Dimension	$\Theta(n)$	$\Theta(nt)$
Locality	$\Theta(1)$	$\Theta(1)$

There is a better application of this result, both in terms of the immediate applicability and, we hope, in terms of the applicability to future constructions. The idea here is not really 'distance balancing' at all, although it uses the above distance balancing construction with an optimal classical LDPC code. This is an idea that was used previously in the search for qLDPC codes of new parameters in the setting where one has a code of very good distance but poor dimension - see for example [15].

The procedure is: to any quantum code, first apply distance balancing so as to improve the X - distance, and then apply distance balancing again so as to improve the Z - distance. We will refer to this procedure as 'double distance balancing'. With a classical code length of t, it has the effect of increasing the number of physical qubits by a factor of $\Theta(t^2)$, increasing both distances by a factor of $\Theta(t)$, increasing the dimension by a factor of $\Theta(t^2)$, preserving the locality (at worst) and decreasing the soundness by a factor of $\mathcal{O}(t^2)$.

Ultimately, double distance balancing increases the dimension up to linear, causes the distance to tend towards a square-root and decreases the soundness - but now we have a lower bound on this decrease. Note that this application was impossible before the present work because the constancy of the dimension of the repetition code leads to the dimension scaling worsening during this procedure. With this, any qLTC representing a point in parameter space may be turned into a line in parameter space; the discovery of one new qLTC now immediately implies the discovery of a whole collection.

The best current application of this is to the hemicubic codes of Leverrier et al. [3]. Again, an infinite collection of parameters is obtained by doing this. We now display the general parameters obtained, as well as two examples.

Table 3: The parmeters of the hemicubic code, followed by the general set of new parameters that arises from applying double distance balancing to it, and two examples that follow via a classical code length of $t = \sqrt{\log(n)}$ and $t = n^{\alpha}$, respectively.

	Hemicubic Code [3]	(General) New Parameters (2)
Physical Qubits	n	$\Theta\left(nt^2\right)$
Soundness	$\Omega\left(\frac{1}{\log(n)}\right)$	$\Omega\left(\frac{1}{\log(n)t^2}\right)$
Distance	$\Theta\left(\sqrt{n}\right)$	$\Theta\left(\sqrt{n}t\right)$
Dimension	$\Theta(1)$	$\Theta\left(t^2\right)$
Locality	$\Theta\left(\log(n)\right)$	$\mathcal{O}\left(\log(n)\right)$
	(Example) New Parameters (2)	(Example) New Parameters (2)
Physical Qubits	N	N
Soundness	$\Omega\left(\frac{1}{\log(N)^2}\right)$	$\Omega\left(\frac{1}{N^{\frac{2\alpha}{1+2\alpha}}\log(N)}\right)$
Distance	$\Theta\left(\sqrt{N}\right)$	$\Theta\left(\sqrt{N}\right)$
Dimension	$\Theta\left(\log(N)\right)$	$\Theta\left(N^{\frac{2\alpha}{1+2\alpha}}\right)$
Locality	$\mathcal{O}\left(\log(N)\right)$	$\mathcal{O}\left(\log(N)\right)$

Finally, we mention that the parameter regime of 'distance × soundness > locality' is a well-motivated regime to consider in the area of local testability. Here, we obtain codes in this regime of dimension $\Theta(N^{\frac{1}{2}-\epsilon})$ for any $\epsilon > 0$, where the previous best was a constant.

[2]The technical caveat of independence of checks is needed here, as it is in Theorem 1, but, again, this is not restrictive.

References

[1] A. Wills, T. C. Lin, M. H. Hsieh. General Distance Balancing for Quantum Locally Testable Codes. arXiv:2305.00689 [quant-ph], 2023.

[2] M. B. Hastings. Quantum codes from high-dimensional manifolds. arXiv:1608.05089 [quant-ph], 2016.

[3] A. Leverrier, V. Londe, G. Zémor. Towards local testability for quantum coding. arXiv:1911.03069 [quant-ph], 2019.

[4] A. Cross, Z. He, A. Natarajan, M. Szegedy, G. Zhu. Quantum Locally Testable Code with Exotic Parameters. arXiv:2209.11405 [cs.IT], 2022.

[5] R. Gallager. Low-density parity-check codes IRE Transactions on information theory 8.1 (1962): 21-28.

[6] P. Panteleev, G. Kalachev. Asymptotically Good Quantum and Locally Testable Classical LDPC Codes arXiv:2111.03654 [cs.IT], 2021.

[7] I. Dinur. The pcp theorem by gap amplification. *Journal of the ACM (JACM)*, 54(3):12–es, 2007.

[8] I. Dinur, S. Evra, R. Livne, A. Lubotzky, S. Mozes. Locally Testable Codes with constant rate, distance, and locality. arXiv:2111.04808 [cs.IT], 2021.

[9] D. Aharonov, L. Eldar. Quantum Locally Testable Codes. arXiv:1310.5664 [quant-ph], 2013.

[10] L. Eldar, A. W. Harrow. Local Hamiltonians Whose Ground States are Hard to Approximate arXiv:1510.02082 [quant-ph], 2015.

[11] M. H. Freedman, M. B. Hastings. Quantum Systems on Non-k-Hyperfinite Complexes: A Generalization of Classical Statistical Mechanics on Expander Graphs arXiv:1301.1363 [quant-ph], 2013.

[12] A. Anshu, N. P. Breuckmann, C. Nirkhe. NLTS Hamiltonians from good quantum codes arXiv:2206.13228 [quant-ph], 2022.

[13] M. B. Hastings. Weight Reduction for Quantum Codes. arXiv:1611.03790 [quant-ph], 2016.

[14] S. Evra, T. Kaufman, G. Zémor. Decodable Quantum LDPC Codes beyond the $\sqrt{n}$ Distance Barrier Using High-Dimensional Expanders. *SIAM J. on Comp.*, (0):FOCS20–276, 2022.

[15] P. Panteleev, G. Kalachev. Quantum LDPC Codes with Almost Linear Minimum Distance. arXiv:2012.04068 [cs.IT], 2020.

Two instances of random access code in the quantum regime

Nitica Sakharwade[1 2 3 *] Michał Studziński[4 †] Michał Eckstein[5 ‡]
Paweł Horodecki[1 6 §]

[1] *International Centre for Theory of Quantum Technologies (ICTQT), University of Gdańsk, Jana Bażynskiego 8, 80-309 Gdańsk, Poland*
[2] *Perimeter Institute for Theoretical Physics, Waterloo, Canada*
[3] *Department of Physics and Astronomy, University of Waterloo, Waterloo, Canada*
[4] *Institute of Theoretical Physics and Astrophysics and National Quantum Information Centre in Gdańsk, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, Wita Stwosza 57, 80-952 Gdańsk, Poland* [5] *Institute of Theoretical Physics*
[5] *Institute of Theoretical Physics, Jagiellonian University, ul. Łojasiewicza 11, 30–348 Kraków, Poland*
[6] *Faculty of Applied Physics and Mathematics, National Quantum Information Centre, Gdansk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland*

Abstract. We consider two classes of quantum generalisations of Random Access Code (RAC) and study lower bounds for probabilities of success for such tasks. The first class is based on a random access code with quantum inputs and output known as No-Signalling Quantum RAC (NS-QRAC) [A. Grudka *et al.* Phys. Rev. A **92**, 052312 (2015)], where unbounded entanglement and constrained classical communication are allowed, which can be seen as quantum teleportation with constrained classical communication. The second class is based on a random access code with a quantum channel and shared entanglement [A. Tavakoli *et al.* PRX Quantum 2 (4) 040357 (2021)] which can be seen as quantum dense coding with constrained quantum channel.

Keywords: Quantum teleportation, quantum dense coding, quantum random access codes.

This abstract submission to AQIS 2023 is based on the arXiv preprint [1] which is now accepted to New Journal of Physics with DOI 10.1088/1367-2630/acd716.

1 Motivation

Quantum information processing protocols offer an unprecedented advantage over classical schemes [2] providing new resources [3] for computation, communication or cryptography. In realistic scenarios, one has to cope with noise and other factors affecting protocols' efficiency. One such limiting constraint is the amount of available (quantum or classical) resources [4, 5]. Such a limiting constraint within the context of Quantum communication protocols can be quantified through constraints on signalling resources (quantum or classical) and no-signalling resources (shared randomness or entanglement) [6]. While bipartite communication protocols, such as Quantum teleportation [7] and Dense-coding [8], focus on perfect quantum encoding and decoding over a classical channel, or on perfect classical encoding and decoding over a quantum channel, respectively, one need not always require perfect transmission.

One such class of (bipartite, one-way communication) protocols that have been studied are the (Classical) Random Access Codes (RACs), where Alice wishes to encode a long string into fewer signalling resources such that Bob can decode some part of the string by his choice, unknown to Alice, with a probability higher than the guessing probability. Some Quantum generalisations of RACs have been studied such as considering the channel shared by Alice to Bob to be Quantum, called Quantum RAC (or QRAC) [9, 10], or aiding the classical channel with Entanglement, called Entanglement Assisted RAC (or EA-RAC) [11], although these do not exhaust all possibilities of quantum generalisations for RACs, which we will outline and further study in this work.

2 Quantum regimes for Random Access Codes

The quantum generalisations for RACs can be categorised using Figure 1. Here Alice encodes multiple states ρ_i into a smaller message m with the aid of some No-Signalling Resources. Bob wishes to decode ρ_c given his choice bit c. The following generalisations may be considered:

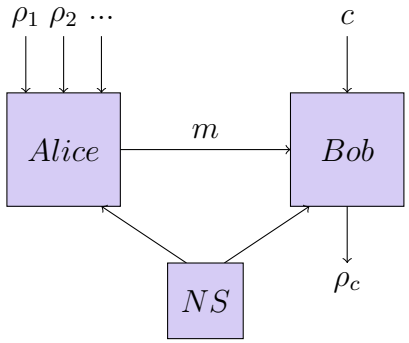


Figure 1: Possible quantum generalisations to Random Access Codes

*nitica.sakh@gmail.com
†studzinski.m.g@gmail.com
‡michal.eckstein@uj.edu.pl
§pawhorod@pg.edu.pl

- The inputs ρ_i of Alice and outputs ρ_c of Bob are classical or quantum
- The message m sent by Alice to Bob is classical or quantum
- They share no-signalling resources such as entanglement
- The channel on which the message is sent has constrained or unconstrained capacity
- If they share some no-signalling resource if it is bounded or unbounded

We tabulate the quantum generalisations, from the literature as well as the ones pertinent to our work, in terms of the above list in Table 1.

One class of quantum generalisations of RAC concerns using quantum resources for transmission of classical information, which fall into three broad categories where: 1) the communication channel is quantum and the parties share randomness — Quantum Random Access Codes with Shared Randomness (QRAC-SR) [12] (Row 2 of Table 1), 2) the channel is classical and the parties share entanglement — Entanglement Assisted Random Access Codes (EA-RAC) [11] (Row 3 of Table 1) and most recently, where 3) the channel is quantum and the parties share entanglement [13] — which we will refer to as Quantum Random Access Codes with Shared Entanglement (QRAC-SE) (Row 4 of Table 1). In Section III B of [13] quantum upper bounds were studied for a lower number of inputs. In this work, we study lower bounds for QRAC-SE for a higher number of inputs, which we will also employ for our modification of the NS-QRAC scenario.

Another class of quantum generalisation of RAC concerns the transmission of quantum information, rather than classical bits, which has been dubbed No-Signalling Quantum Random Access Code (NS-QRAC) [14] (Row 5 of Table 1). The authors of [14] consider a restricted classical channel and unbounded No-Signalling resources and achieve the logical bound using PR boxes. In this work, we consider the quantum lower bound, which was left as an open question (Row 6 of Table 1). Further, we analyse two modifications to the NS-QRAC scenario. First 1) we consider a quantum channel instead of a classical channel shared between the two parties (Row 7 of Table 1) and next 2) we consider a constrained entanglement scenario with unbounded classical communication which we call Constrained-No-Signalling Quantum Random Access Code (CNS-QRAC) (Row 8 of Table 1), which has not been considered before in the literature.

Therefore, in this work, we provide lower bounds for the probability of success of these two different classes of quantum random access codes. We show that some of the considered tasks are operationally equivalent to teleportation and dense coding with constrained resources.

Scenario	Input	Channel	NS resource	Output
RAC	Cl	Cl	SR	Cl
QRAC	Cl	Q	SR	Cl
EA-RAC	Cl	Cl	Ent.	Cl
QRAC-SE	Cl	Q	Ent.	Cl
NS-QRAC	Q	Con. Cl	Unb NS	Q
NS-QRAC	Q	Con. Cl	Unb Ent.	Q
NS-QRAC	Q	Con. Q	Unb Ent.	Q
CNS-QRAC	Q	UnC. Cl	B Ent.	Q

Table 1: Quantum generalisations of RACs. Here NS stands for non-signalling, Cl stands for classical, Q for quantum, Con. stands for Constrained, UnCon. stands for Unconstrained, SR stands for Shared Randomness and Ent. stands for entanglement, NS for No-Signalling resources Unb for Unbounded and B for Bounded.

3 Results and Outline

The arXiv preprint [1] is organised as follows:

In Sec. II we consider, as a warm-up, the task of quantum teleportation with constrained classical resources. We show, using the notion of generalised Bell states, that the maximal fidelity of a teleported state equals k/d^2, where d is the Hilbert space dimension and $k < d^2$ is the number of bits of classical communication transmitted by Alice to Bob.

Sec. III concerns the NS-QRAC scenario as presented in [14], in which Bob aims at reproducing at his output one of the two qubits possessed by Alice. In doing so, Bob is equipped with two bits of classical communication received from Alice, as well as two maximally entangled pairs. We show that this problem can be seen as a constrained teleportation task. We provide a quantum lower bound, $P_{\text{succ}}^{\text{QM}} = \frac{5}{8}$, for the success of such a task for the qubit case. It proves a clear separation from a post-quantum scenario, with Alice and Bob sharing two PR-boxes, in which case $P_{\text{succ}}^{\text{PR}} = 1$, as shown in [14]. This fact can be utilised to perform foundational tests of quantum theory — see [15].

In Sec. IV, we introduce and study Quantum Random Access Code with Shared Entanglement (QRAC-SE), the setup for which was first seen in [13]. It concerns the classical information to be encoded and decoded (like in the classical RAC) while using *both* a quantum channel as well as a shared entanglement resource. The QRAC-SE brings together QRAC which uses a quantum channel but no entanglement [12] and EA-RAC which involves entanglement but employs a classical channel [11]. We show that this problem can be seen as a constrained dense coding protocol, which is dual to the constrained quantum teleportation considered in the previous sections. Namely, here the parties have more classical input than they can send perfectly using qudit dense coding [16]. We provide and analyse the efficiency of such protocols which can be quantified in two ways: by calculating 1) the minimum probability of success of decoding either of two strings, each of which consists of two digits of base-d or 2) the average probability of success of the protocol (over all possible strings). We show that in the qubit case, both these measures coincide. The encoding by Alice utilises the roots of the generalised Pauli matrices, as well as Gray codes [17] and its non-Boolean generalisations [18, 19], which is an example of a single distance

code. We also present analysis for higher dimensions, $d = 3, 4$ and show that the two measures of efficiency differ (in contrast to $d = 2$) — the interpretation of this fact is also discussed. Doriguello et al. [20] have studied RAC variations extended to Boolean functions denoted by the prefix $f-$, including $f-$QRAC and $f-$EA-RAC. We show a proof of concept of extending QRAC-SE to encode Boolean functions of initial classical information called $f-$QRAC-SE.

In Sec. V we revisit and provide a modification for the NS-QRAC scenario as presented in [14], in which Bob aims at reproducing at his output one of the two qubits possessed by Alice. In doing so, Bob is equipped with one qubit received from Alice, as well as three maximally entangled pairs. This modification is in some sense a truly Quantum RAC problem since the information to be encoded as well as the channel shared by the parties is quantum. We show that the quantum lower bound for the success of such a task coincides with that of QRAC-SE studied in Sec. IV ($P_{\text{succ}}^{\text{QM}} \approx 0.728$), which is a better bound than the scenario in Sec. III.

Finally, in Sec VI, we consider a second modification of the NS-QRAC scenario, in which Bob aims at reproducing at his output one of the two qubits possessed by Alice. Here we consider constrained No-Signalling resources while allowing unbounded classical information to be sent from Alice and Bob — we call these Constrained-No-Signalling Quantum Random Access Codes (CNS-QRAC). We provide a quantum lower bound, $P_{\text{succ}}^{\text{QM}} = \frac{3}{4}$, for the success of such a task for the qubit case. We further generalise the protocol to the case of $N \geq 2$ inputs of d-level quantum systems and show that $P_{\text{succ}}^{\text{QM}}(d, N) \leq (N + d - 1)/(dN)$. Furthermore, we discuss an 'asymmetric' scenario in which the input quantum systems are chosen randomly with prescribed probabilities $\{p_i\}_{i=1}^{N}$. We present an algorithmic solution for this case using constraints coming from entanglement monogamy by exploiting the framework of universal asymmetric quantum cloning machines [21, 22]. However, the interesting aspect of this scenario is that here the transmission of quantum information does not go from the single system to two receivers — as it is the case in standard quantum channel capacity restrictions based on quantum cloning (see for example [23, 24]). Rather, the transmission goes from the composite system of two 'senders' who cooperate quantumly to transfer quantum information to a single receiver. Since the 'senders' are required to transmit different quantum information, which is also supposed to come as an *alternative* rather then jointly, there seems to be no *a priori* reasons why the cloning bound should be obeyed. Nevertheless, it turns out to apply in such a scenario as well.

4 Discussion and outlook

We studied two instances of random access codes using quantum information. The first one involved remote access to one of the two given quantum states *via* an NS-QRAC box implemented quantumly in the 'distant labs' paradigm. We considered a variation where a constrained quantum channel is used as contrasted to a constrained classical channel used in [14]. This, in a way, is the most natural quantum version of the $2 \to 1$ classical RAC problem, because we have remote access to one of two qubits transmitted over a qubit channel. In this case, we found a lower bound for the probability of success $P_{\text{succ}}^{\text{QM}} \geq 0.728$.

We also considered another modification — the CNS-QRAC, where we find that the trade-off for information transmission corresponds to a typical monogamy relation. In this case, we provided a reasonable upper bound for the probability of success for a general CNS-QRAC with N input states of dimension d. An interesting aspect of this scenario is that here the transmission of quantum information does not involve a single sender and two receivers, as it is the case in the standard quantum channel capacity restrictions based on quantum cloning (see for example [23, 24]). Instead, the transmission goes from the composite system of two 'senders' who cooperate quantumly to transfer quantum information to a single receiver. Since the 'senders' are required to transmit different quantum information, which is also supposed to come as an *alternative* rather than jointly, there seems to be no *a priori* reasons why the cloning bound should be obeyed. Nevertheless, it turns out to apply in such a scenario as well.

An interesting open problem is to extend this analysis to the quantumly simulable NS boxes, where the two parties may interact (see [25], [26]). Clearly, when the labs are far apart, such boxes are super-quantum. In fact — as shown in a recent paper [27] — its subclasses with classical inputs are even interconvertible with PR boxes with the help of shared entanglement and local operations. Hence, at the intuitive level, it is possible that the corresponding CNS-QRAC might allow both (all) fidelities to be perfect, but this conjecture would need further investigation.

The second instance of random access codes, and to some extent a complementary scenario, has been introduced here to analyse the power of quantum entanglement when aiding quantum random access coding. To this end, we have defined and studied quantum random access codes with shared entanglement and a quantum channel. An interesting aspect of this problem occurs for the class of QRAC-SE $2_{d^2} \xrightarrow{p,1_{d^2}} (1_d, 1_d)$ problems, as the encoding by Alice depends on the existence of generalised Gray codes. This should be compared with the problem of QRAC-SR [12], where Alice's encoding depends on finding some form of symmetric quantum states in the Bloch sphere. The presented explicit protocols provide lower bounds for the probabilities of success. It is an open problem to find the relevant upper bounds, perhaps using numerical methods similar to the techniques involved in finding the upper bounds in [13]. Lastly, we provided a proof of concept for extending the QRAC-SE to $f-$QRAC-SE over Boolean functions, similar to the studies of $f-$QRAC in [20], which may inspire an interesting line of future research.

References

[1] N. Sakharwade, M. Studziński, M. Eckstein, and P. Horodecki, "Two instances of random access code in the quantum regime," *arXiv preprint arXiv:2208.14422*, 2022.

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[3] E. Chitambar and G. Gour, "Quantum resource theories," *Reviews of Modern Physics*, vol. 91, p. 025001, Apr 2019.

[4] K. Korzekwa, Z. Puchała, M. Tomamichel, and K. Życzkowski, "Encoding classical information into quantum resources," *arXiv preprint arXiv:1911.12373*, 2019.

[5] C.-Y. Hsieh, "Communication, dynamical resource theory, and thermodynamics," *PRX Quantum*, vol. 2, p. 020318, May 2021.

[6] M. M. Wilde, *Quantum information theory*. Cambridge University Press, 2013.

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.

[8] D. Bruß, M. Lewenstein, A. Sen, U. Sen, G. M. D'Ariano, and C. Macchiavello, "Dense coding with multipartite quantum states," *International Journal of Quantum Information*, vol. 4, no. 03, pp. 415–428, 2006.

[9] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, p. 78–88, Jan. 1983.

[10] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, "Dense quantum coding and quantum finite automata," *J. ACM*, vol. 49, p. 496–511, July 2002.

[11] M. Pawłowski and M. Żukowski, "Entanglement-assisted random access codes," *Physical Review A*, vol. 81, no. 4, p. 042326, 2010.

[12] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, "Quantum random access codes with shared randomness," *arXiv preprint arXiv:0810.2937*, 2008.

[13] A. Tavakoli, J. Pauwels, E. Woodhead, and S. Pironio, "Correlations in entanglement-assisted prepare-and-measure scenarios," *PRX Quantum*, vol. 2, no. 4, p. 040357, 2021.

[14] A. Grudka, M. Horodecki, R. Horodecki, and A. Wójcik, "Nonsignaling quantum random access-code boxes," *Physical Review A*, vol. 92, no. 5, p. 052312, 2015.

[15] M. Eckstein and P. Horodecki, "Probing the limits of quantum theory with quantum information at subnuclear scales," *Proceedings of the Royal Society A*, vol. 478, no. 2259, p. 20210806, 2022.

[16] X. Liu, G. Long, D. Tong, and F. Li, "General scheme for superdense coding between multiparties," *Physical Review A*, vol. 65, no. 2, p. 022304, 2002.

[17] F. Gray, "Pulse code communication," *United States Patent Number 2632058*, 1953.

[18] M. Er, "On generating the n-ary reflected gray codes," *IEEE transactions on computers*, vol. 100, no. 8, pp. 739–741, 1984.

[19] B. D. Sharma and R. K. Khann, "On m-ary gray codes," *Information Sciences*, vol. 15, no. 1, pp. 31–43, 1978.

[20] J. F. Doriguello and A. Montanaro, "Quantum random access codes for boolean functions," *Quantum*, vol. 5, p. 402, 2021.

[21] A. Kay, D. Kaszlikowski, and R. Ramanathan, "Optimal cloning and singlet monogamy," *Physical review letters*, vol. 103, no. 5, p. 050501, 2009.

[22] R. F. Werner, "Optimal cloning of pure states," *Phys. Rev. A*, vol. 58, pp. 1827–1832, Sep 1998.

[23] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, "Optimal universal and state-dependent quantum cloning," *Phys. Rev. A*, vol. 57, pp. 2368–2378, Apr 1998.

[24] T. S. Cubitt, M. B. Ruskai, and G. Smith, "The structure of degradable quantum channels," *Journal of Mathematical Physics*, vol. 49, no. 10, p. 102104, 2008.

[25] M. Piani, M. Horodecki, P. Horodecki, and R. Horodecki, "On quantum non-signalling boxes," *Phys. Rev. A*, vol. 74, p. 012305, 2006.

[26] D. Schmid, D. Rosset, and F. Buscemi, "The type-independent resource theory of local operations and shared randomness," *Quantum*, vol. 4, p. 262, Apr 2020.

[27] D. Schmid, H. Du, M. Mudassar, G. Coulter-de Wit, D. Rosset, and M. J. Hoban, "Postquantum common-cause channels: the resource theory of local operations and shared entanglement," *Quantum*, vol. 5, p. 419, Mar 2021.

Long-range data transmission in a fault-tolerant quantum bus architecture

Shin Ho Choe[1 2 *] Robert Koenig[1 2 †]

[1] *School of Computation, Information and Technology, Technical University of Munich*
[2] *Munich Center for Quantum Science and Technology (MCQST), Munich, Germany*

Abstract. We propose a scheme for fault-tolerant long-range entanglement generation at the ends of a rectangular array of qubits of length R with a square cross section of $m = O(\log^2 R)$ qubits. It is realized by a constant-depth circuit and produces a constant-fidelity entangled Bell-pair (independent of R) for arbitrary local stochastic noise of strength below an experimentally realistic threshold value. Conversely, we show that any scheme for noise-resilient distance-R entanglement generation realized by a constant-depth circuit needs at least $m = \Omega(\log R)$ qubits per repeater station. A key element of our construction is a robust single-shot decoding procedure for the 2D surface code.

Keywords: fault-tolerant quantum computing, long-range entanglement generation

1 Introduction

Long-range entanglement is a key resource for a variety of information-processing protocols ranging from (distributed) quantum computation and sensing [1, 2, 3, 4, 5, 6, 7] to communication and cryptography [8, 9, 10, 11, 12]. A repeater-based entanglement-generation protocol seeks to establish entanglement between qubits located at the ends of a line of repeater stations. This task is non-trivial because neighboring stations are connected by noisy quantum channels.

2 Our scheme

2.1 An architecture using nearest-neighbor operations.

Here we propose a scheme for long-range entanglement-generation based on a quasi-1D array of qubits. The latter consists of R square slices of $d \times d$ qubits, see Fig. 1b. Each square slice is associated with a repeater, and entanglement is generated at the two ends (at distance R). The scheme starts in a product state $|0\rangle^{\otimes n}$ of all qubits, applies a depth-6 Clifford circuit $W = W_6 \cdots W_1$ (where each gate layer W_j consists of geometrically local one- and two-qubit gates on the array), and finally performs single-qubit measurements simultaneously on all but two qubits $\{q_1, q_2\}$. In particular, every processing step involves only operations between neighboring repeaters and operations within each repeater. The latter are local if the qubits at each repeater are arranged on a square lattice. By construction, the post-measurement state on qubits $\{q_1, q_2\}$ is the two-qubit Bell state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ up to a Pauli correction $Z_{q_1}^{\alpha(s)} X_{q_1}^{\beta(s)}$ on qubit q_1, where $(\alpha(s), \beta(s))$ can be efficiently computed from the measurement results s. In particular, since the entire scheme is realized by a constant-depth circuit, this is a low-latency scheme: the entanglement is available after a constant amount of time (independent of R). We note that the Pauli correction can be accounted for by classical post-processing if e.g., the entanglement is used for subsequent computation realized by magic states and Clifford circuits.

2.2 Noise-resilience against local stochastic noise.

How well does our scheme perform under noise? While repeater-based schemes are often analyzed using simplifying assumptions such as i.i.d. Pauli noise or the availability of ideal operations at each repeater station, our scheme allows to provide a full analysis of general (correlated) circuit-level noise: We consider a situation where all operations (state preparation, gates and measurements) are affected by noise. Specificallly, we use the concept of local stochastic noise, a general notion of errors introduced in [13] to model situations where the noise is "locally decaying" but otherwise arbitrary, see also [14]. Formally, a Pauli error E (a random variable on the n-qubit Pauli group) is a local stochastic error of strength $p \in [0, 1]$, written in $E \sim \mathcal{N}(p)$, if the probability of having non-trivial Pauli errors on each qubit of any subset of $k \leq n$ qubits is at most p^k. A noisy execution of the quantum circuit W is obtained by replacing the circuit W by $W_{\text{noisy}} = E_{d+1} E_d W_d \cdots E_2 W_2 E_1 W_1 E_0$ with $E_j \sim \mathcal{N}(p)$ for each j (here $d = 6$ is the circuit depth). Here the random variables $\{E_j\}_{j=0}^{d+1}$ need not be independent: We only require that each marginal distribution $E_j \sim \mathcal{N}(p)$ is local stochastic.

Since all gate layers in our protocol are Clifford unitaries, all errors E_j can be commuted forward or backward. This transforms a noisy execution of quantum circuit W into the form $W_{\text{noisy}} = W_d \cdots W_{t+1} E W_t \cdots W_1$ for any $t \in \{0, \ldots, d\}$ with $E \sim \mathcal{N}\left(p^{O(1)}\right)$, see [15, Lemma 11]. To establish noise-resilience of our protocol, it is thus sufficient to consider (with the choice $t = d$) a circuit of the form $W_{\text{noisy}} = EW$, where W is a depth-6 Clifford unitary. In our case, $W|0\rangle^{\otimes n}$ is a 3D cluster state on an elongated slab $\mathcal{C}[d \times d \times R]$ of dimensions $d \times d \times R$. Our main result is the following threshold theorem:

*shinho.choe@tum.de
†robert.koenig@tum.de

Theorem 1 (Long-range entanglement generation) *Consider a cluster state $W|0\rangle^{\otimes n}$ associated with the lattice $\mathcal{C}[d \times d \times R]$ where $d \geq 3$ is arbitrary. Suppose the measurement pattern in Fig. 1b is applied to a corrupted cluster state $EW|0\rangle^{\otimes n}$, where $E \sim \mathcal{N}(p)$ is a local stochastic error. Then there are two efficiently computable functions α, β taking the collection s of measurement outcomes to bits such that the post-measurement state on qubits q_1, q_2 is the state $Z_{q_2}^{\alpha(s)} X_{q_2}^{\beta(s)} \Phi$ with probability at least $1 - 5006p$, for any $0 < p \leq p_0 \approx 2 \times 10^{-4}$ and any $R \leq \frac{1}{\sqrt{d}} \left(\frac{1}{10\sqrt{p}}\right)^{d-2}$.*

Considering each $d \times d$-slice of the lattice $\mathcal{C}[d \times d \times R]$ as a repeater station, we have $m = \Theta(d^2)$ qubits per repeater. Theorem 1 thus implies that below the threshold error strength p_0,

$$m = \Theta(\log^2 R) \tag{1}$$

qubits per repeater are sufficient to establish constant-fidelity over distance R.

2.3 A converse to low-latency entanglement generation

Our scheme is an example of a low-latency scheme realized by a constant-depth (adaptive) circuit. Adaptivity refers to the fact that a Pauli correction depending on the measurement outcomes is applied to the post-measurement state. We ask whether our scheme is optimal and find the following converse:

Theorem 2 (Converse for low-latency entanglement generation) *Consider a scheme for entanglement generation over distance R realized by a constant-depth quantum adaptive circuit which achieves constant fidelity using m qubits per repeater. If it is resilient to arbitrary local stochastic noise of strength below a constant $p_0 > 0$, then we must have $m = \Omega(\log R)$.*

Closing the gap between the achievability result 1 and the converse 2 will most likely require considering a different resource state and measurement pattern. Indeed, we show that the bound on our protocol given in Theorem 1 (i.e., Eq. (1)) is tight (and this applies to any protocol where α, β are replaced by different functions).

2.4 Application: Fault-tolerant measurement of non-local constant-weight stabilizers

Because of the simplicity of the involved operations, our scheme can act as a data bus which can exchange information between various components as first studied in [16]. Our protocol could be especially beneficial in the setting where gates or measurements need to be performed between spatially distant qubits. Such a need arises for example when using a quantum low-density parity check (LDPC) code whose stabilizer generators are not spatially local. With our scheme, we can design a quasi-2D architecture that allows for the application of joint measurements on any subset of size $\ell = O(1)$ of n qubits using a total of $O(n \cdot \mathsf{polylog}(n))$ qubits, see [17].

2.5 Single-shot surface code decoding

A main building block for our entanglement generation method is a novel protocol for fault-tolerant single-shot surface code decoding. It is illustrated in Fig. 1a and has the following properties:

Theorem 3 (Single-shot surface code decoding) *Consider a distance-d surface code with $d \geq 2$. Suppose the measurement pattern of Fig. 1a is applied to a state $E\overline{\Psi} \in \left(\mathbb{C}^2\right)^{\otimes n}$, where $\overline{\Psi}$ is the encoded state associated with a logical qubit state $\Psi \in \mathbb{C}^2$ and $E \sim \mathcal{N}(p)$ is a local stochastic error. Then there are two efficiently computable functions α, β taking the collection s of measurement outcomes to bits such that the post-measurement state on qubit q is the state $Z_q^{\alpha(s)} X_q^{\beta(s)} \Psi$ with probability at least $1 - 94p$, for any $p \leq p_0 := \frac{1}{144} \approx 7 \times 10^{-3}$.*

Combining the measurement pattern of Fig. 1a with a single-qubit correction $Z_q^{\alpha(s)} X_q^{\beta(s)}$ thus transfers the encoded logical state to the qubit q. This can then be further processed: For example, subsequent measurement in the computational or T-basis thus gives a fault-tolerant measurement of $\overline{Z}$ and $\overline{T}$, thus subsuming the protocols proposed earlier in [15, 18]. (We note that [18] uses an identical measurement pattern for the logical $\overline{T}$-measurement.) More generally, one may apply arbitrary quantum information-processing steps to the logical information by operating on q.

3 Main idea

3.1 Single-shot decoding

To illustrate the ideas underlying our single-shot decoding strategy, consider the repetition code with n qubits labeled by elements $j \in \mathbb{Z}_n$ and stabilizer generators $\{S_j = Z_j Z_{j+1}\}_{j \in \mathbb{Z}_n}$, where addition is modulo n. Let us assume that n is odd such that we have logical operators $\overline{X} = \prod_{j \in \mathbb{Z}_n} X_j$ and $\overline{Z} = \prod_{j \in \mathbb{Z}_n} Z_j$. We can write $\overline{Z}$ as

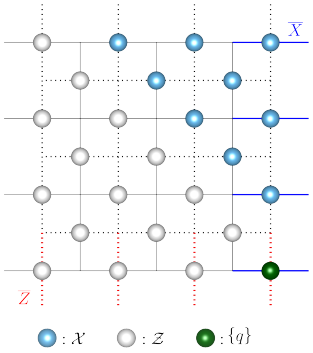
$$\overline{Z} = Z_0 \prod_{j \in \mathcal{L}_Z} Z_j \quad \text{where} \quad \mathcal{L}_Z = \{1, \ldots, n-1\} . \tag{2}$$

We note that a logical Pauli-Z operator in this code can equivalently be realized by a single-qubit operator Z_j on any qubit $j \in \mathbb{Z}_n$, but we will use (2) for our example. Suppose our goal is to transform an encoded state $\overline{\Psi} \in (\mathbb{C}^2)^{\otimes n}$ into a single-qubit state Ψ on qubit 0 that has the same Pauli-Z-expectation value as $\overline{\Psi}$, i.e., $\langle \Psi | Z | \Psi \rangle = \langle \overline{\Psi} | \overline{Z} | \overline{\Psi} \rangle$. This can be achieved by

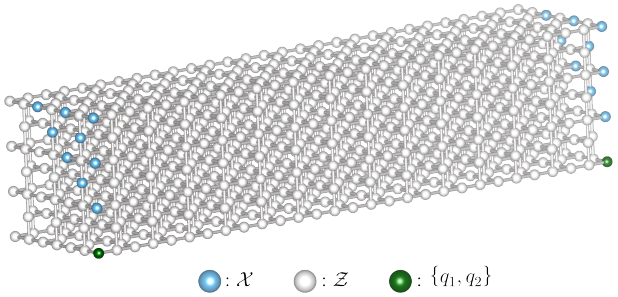
(i) measuring each qubit $j \in \mathcal{L}_Z$ in the computational basis, getting outcome $z_j \in \{0, 1\}$.

(ii) computing the parity $\alpha(z) := \bigoplus_{j \in \mathcal{L}_Z} z_j$ and "correcting", i.e., applying $X^{\alpha(z)}$ to qubit 0.

This protocol is not fault-tolerant: i.i.d. bit-flip errors on each qubit result in a wrong parity $\alpha(z)$ with probability exponentially close to $1/2$ (in n), thus the "visibility" of the Pauli-Z operator becomes negligible for large n. A better protocol is obtained by observing



(a) A surface code of distance d



(b) A cluster state on the lattice $\mathcal{C}[d \times d \times R]$. Entanglement is established between q_1 and q_2.

Figure 1: Measurement patterns of (a) the single-shot distance-d (here for $d = 4$) surface code decoding protocol and (b) the long-range entanglement generation procedure using a lattice $\mathcal{C}[d \times d \times R]$. Qubits belonging to $\mathcal{X}$ are measured in the Hadamard basis, whereas qubits belonging to $\mathcal{Z}$ are measured in the computational basis. The first protocol transfers encoded logical information to physical qubit q. The second protocol generates a Bell pair between qubits q_1 and q_2.

that the measurement results $\{z_j\}_{j=1}^{n-1}$ determine syndrome bits $s = \{s_j := z_j \oplus z_{j+1}\}_{j=1}^{n-2}$. Note that this is only partial syndrome information for the repetition code since qubit 0 is not measured and syndrome bits associated with S_0 and S_{n-1} are missing. Nevertheless, when measuring an encoded state $X(E)\overline{\Psi}$ corrupted by a Pauli error $X(E) = \prod_{j\in E} X_j$, $E \subseteq \mathbb{Z}_n$, this partial syndrome s determines a certain partial boundary $s = \partial E \subseteq \{1, \ldots, n-2\}$ of the error set E. Here ∂E is obtained by taking the "usual" boundary map $\partial : \mathbb{Z}_2^E \to \mathbb{Z}_2^V$ taking the edges E of the cycle graph to its vertices $V = \mathbb{Z}_n$, and subsequently restricting (projecting) to the vertices $\{1, \ldots, n-2\}$. We can think of ∂E as the boundary of E in a decoding graph T_{dec} that has distinguished external vertices. In our case, T_{dec} is a line graph with n vertices, where $\{0, n-1\}$ is the set of external vertices. This motivates the following improved protocol.

(i) measure each qubit $j \in \mathcal{L}_Z$ in the computational basis, getting outcome $z_j \in \{0, 1\}$. Compute the syndrome $s = \{s_j := z_j \oplus z_{j+1}\}_{j=1}^{n-2}$.

(ii) compute $\widehat{E} = \mathsf{MinMatch}(s)$. Here $\mathsf{MinMatch}$ produces a minimum matching on the decoding graph T_{dec}: An error of the form $X(\widehat{E})$ is consistent with the observed syndrome s.

(iii) compute the parity $\alpha(z) := \bigoplus_{j\in\mathcal{L}_X}(z_j \oplus \delta_{j\in\widehat{E}})$ and apply a local "correction" operator $X^{\alpha(z)}$ to qubit 0.

It is easy to check that this modified protocol is fault-tolerant against i.i.d. Pauli errors with Bernoulli-p distribution: For $p \leq p_0$ below some threshold value p_0, the residual (logical) error on qubit 0 has probability of order $O(p)$ independently of the system size n. In fact, our work provides a combinatorial framework for showing, more generally, that such a scheme is resilient to local stochastic errors, and show that for surface codes, both X- and Z-type logical information is transferred to a single qubit.

3.2 Long-range entanglement generation

As shown in the pioneering work [19], the cluster state has localizable entanglement on the two boundaries: A surface-code encoded Bell pair can be created by measuring "bulk qubits" up to a (computable) residual local stochastic error (see Ref. [15, Theorem 23]). Combining this with our single-shot surface code decoding protocol yields our entanglement-generation scheme. However, our analysis leading to Theorem 1 considers the entire process (instead of studying the two stages individually) in order to establish a stringent bound on the error threshold. The converse follows by considering certain concrete strength-p local stochastic errors and showing that the resulting state is separable with high probability.

References

[1] David P. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48(9-11):771–783, 2000.

[2] John Preskill. Quantum computing: pro and con. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):469–486, 1998.

[3] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello. Distributed quantum computation over noisy channels. *Phys. Rev. A*, 59:4249–4254, Jun 1999.

[4] Rodney Van Meter, W. J. Munro, Kae Nemoto, and Kohei M. Itoh. Arithmetic on a distributed-memory quantum multicomputer. *J. Emerg. Technol. Comput. Syst.*, 3(4), jan 2008.

[5] Beals Robert, Brierley Stephen, Gray Oliver, Harrow Aram W., Kutin Samuel, Linden Noah, Shepherd Dan, and Stather Mark. Efficient distributed quantum computing. *Proc. R. Soc. A.*, 469(20120686.20120686), 2013.

[6] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin. A quantum network of clocks. *Nature Physics*, 10(8):582–587, august 2014.

[7] Zachary Eldredge, Michael Foss-Feig, Jonathan A. Gross, S. L. Rolston, and Alexey V. Gorshkov. Optimal and secure measurement protocols for quantum sensor networks. *Phys. Rev. A*, 97:042337, Apr 2018.

[8] Nicolas Gisin and Rob Thew. Quantum communication. *Nature Photonics*, 1:1749–4893, March 2007.

[9] H.J. Kimble. The quantum internet. *Nature*, 453:1476–4687, June 2008.

[10] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.

[11] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore*, pages 175–179, December 1984.

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

[13] Daniel Gottesman. Fault-tolerant quantum computation with constant overhead, 2013.

[14] Omar Fawzi, Antoine Grospellier, and Anthony Leverrier. Constant overhead quantum fault-tolerance with quantum expander codes. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 743–754, 2018.

[15] Sergey Bravyi, David Gosset, Robert Koenig, and Marco Tomamichel. Quantum advantage with noisy shallow circuits in 3D. *Nature Physics*, 16(10):1040–1045, October 2020.

[16] Gavin K. Brennen, Daegene Song, and Carl J. Williams. Quantum-computer architecture using nonlocal interactions. *Phys. Rev. A*, 67:050302, May 2003.

[17] Shin Ho Choe and Robert Koenig. Long-range data transmission in a fault-tolerant quantum bus architecture, 2022. available at arXiv:2209:09774.

[18] Daniel Litinski. Magic State Distillation: Not as Costly as You Think. *Quantum*, 3:205, December 2019.

[19] Robert Raussendorf, Sergey Bravyi, and Jim Harrington. Long-range quantum entanglement in noisy cluster states. *Physical Review A*, 71(6):062313, June 2005.

Unified direct parameter estimation via quantum reservoirs

Yinfei Li[1] Sanjib Ghosh[2] * Jiangwei Shang[1] † Qihua Xiong[2 3] Xiangdong Zhang[1]

[1] *Key Laboratory of Advanced Optoelectronic Quantum Architecture and Measurement of Ministry of Education, School of Physics, Beijing Institute of Technology, Beijing 100081, China*

[2] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*

[3] *State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China*

Abstract. Parameter estimation is an indispensable task in various applications of quantum information processing. To predict parameters in the post-processing stage, it is inherent to first perceive the quantum state with a measurement protocol and store the information acquired. In this work, we propose a general framework for constructing classical approximations of arbitrary quantum states with quantum reservoir networks. A key advantage of our method is that only a single local measurement setting is required for estimating arbitrary parameters, while most of the previous methods need exponentially increasing number of measurement settings. Moreover, this estimation scheme is extendable to higher-dimensional systems and hybrid systems with non-identical local dimensions, which makes it exceptionally generic.

Keywords: shadow estimation, quantum reservoir, parameter estimation

Parameter estimation plays a central role in the implementation of various quantum technologies, such as quantum computing, quantum communication and quantum sensing. This highlights that extracting information from a quantum system to a classical machine lies at the heart of quantum physics. The prominent technique for this task, quantum tomography, studies the reconstruction methods of density matrices for quantum states. The density matrix captures all the information of a quantum system, and is useful in predicting properties of it. However, the curse of dimensionality has emerged with the advent of the noisy intermediate-scale quantum (NISQ) era, which renders it infeasible to obtain a complete description of quantum systems with a large number of constituents. Moreover, a full description is often superfluous in tasks where only key properties are relevant. As a consequence, the concept of shadow tomography is proposed to focus on predicting certain properties of a quantum system [1].

A particularly important progress in the study of shadow tomography is the advancement of randomized measurements [2, 3], the virtue of which is highlighted as *"Measure first, ask questions later"* [4]. The randomized measurement protocols proposed by Huang, Kueng and Preskill construct approximate representations of the quantum system, namely classical shadows, via Pauli group and Clifford group measurements [3]. The single-snapshot variance upper bound of classical shadows is determined by the so-called shadow norm. They proved that the shadow norm of classical shadows with global measurements is asymptotically optimal for linear functions as it matches the information-theoretic lower bound. In addition, the statistical fluctuation can be further suppressed by constructing classical shadows with optimized positive operator-valued measures (POVMs). The classical shadows are highly efficient in the estimation of various properties in the post-processing phase, the benefits of which extend to entanglement detection, characterization of topological order, machine learning for many-body problems, etc. However, these protocols pose a challenge in experiments due to the need for exponentially increasing measurement settings to achieve an arbitrary accuracy. Hence, techniques like de-randomization and measurement settings such as symmetric informationally complete positive operator-valued measures (SIC POVMs) are introduced to tackle this problem. Moreover, the theoretical results are based on the fact that multi-qubit Clifford groups are unitary 3-designs, which is not the case for arbitrary qudit systems. The generalization of these results to higher-dimensional systems typically require complex unitary ensembles that are hard to implement. Therefore, a general method for direct estimation with a single measurement setting is highly desirable.

Recently, quantum neural networks are widely studied as promising artificial neural networks due to their enhanced information feature space supported by the exponentially large Hilbert space. Unlike traditional computing frameworks, neural networks learn to perform complex tasks based on training rather than predefined algorithms or strategies. With the capacity to produce data that displays atypical statistical patterns, quantum neural networks have the potential to outperform their classical counterparts. However, training a quantum neural network can be equally hard. Indeed, it has been shown that training of quantum neural networks could be exceptionally difficult owing to the barren plateaus or far local minima in the training landscapes. This is the reason that quantum neural networks are often limited to shallow circuit depths or small number of qubits. A trending line of research that circumvents this issue is quantum reservoir processing (QRP) [5, 6], which is a quantum analogy of recurrent networks.

In this work we present a direct parameter estimation scheme via quantum neural networks, which overcomes the obstacles faced by randomized measurement proto-

*sanjibghosh@baqis.ac.cn

†jiangwei.shang@bit.edu.cn

cols by harnessing the richness of QRP. In QRP, training is completely moved out of the main network to a single output layer, such that the training becomes a linear regression eliminating the possibility of producing barren plateaus or local minima. Such a quantum neural network retains its quantum enhanced feature space while being trainable via a fast and easy mechanism. Based on this efficiently trainable QRP, we establish a unified measurement protocol for direct quantum parameter estimations. A scheme of minimal quantum hardware comprising pair-wise connected quantum nodes is developed to estimate arbitrary parameters of a quantum state. As major advantages, our scheme requires single-qubit measurements, only in a single setting, and a logarithmic network size $\sim \ln d$ with respect to the dimension d of the input state. All of these are particularly favorable for actual physical implementations.

Furthermore, we establish rigorous performance guarantee by adopting the mindset of shadow estimation. According to Born's rule, one measurement of a quantum state is analogous to sampling a probability distribution once. Thus, learning properties of a quantum state involves measuring identical and independently distributed (i.i.d.) samples of the quantum state a certain number of times. To estimate M observables of the state within an additive error ϵ and with constant confidence, the number of i.i.d. input samples consumed scales as $O\big(F_{\text{res}} \ln M/\epsilon^2\big)$. The factor F_{res} represents the variance upper bound of the single sample estimator, which depends solely on the observables and the reservoir dynamics, and its magnitude is comparable to that of the shadow norm. As a direct consequence of the pair-wise reservoir dynamics, F_{res} for a k-local observable is the product of that for each single-qubit observable. We support the theoretical results with extensive numerical simulations.

References

[1] S. Aaronson. Shadow tomography of quantum states. In *Proc. of the 50th ACM STOC*, pages 325–338, 2018.

[2] J. Paini, A. Kalev. An approximate description of quantum states. *arXiv*:1910.10543.

[3] H-Y. Huang, R. Kueng, J. Preskill. Predicting many properties of a quantum system from very few measurements. *Nat. Phys.* 16, 1050, 2020.

[4] A. Elben, S. T. Flammia, H-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, P. Zoller. The randomized measurement toolbox. *Nat. Rev. Phys.* 5, 9, 2023.

[5] S. Ghosh, A. Opala, M. Matuszewski, T. Paterek, T. C. H. Liew. Quantum reservoir processing. *npj Quantum Inf.* 5, 35, 2019.

[6] K, Nakajima. Physical Reservoir Computing—an Introductory Perspective. *Jpn. J. Appl. Phys.* 59, 060501, 2020.

Constructing decoders for quantum information based on complementarity

Yoshifumi Nakata[1] * Takaya Matsuura[2] † Masato Koashi[3 4] ‡

[1] *Yukawa Institute for Theoretical Physics, Kyoto University, Japan*
[2] *Centre for Quantum Computation & Communication Technology, School of Science, RMIT University, Melbourne VIC 3000, Australia*
[3] *Photon Science Center, Graduate School of Engineering, The University of Tokyo, Japan*
[4] *Department of Applied Physics, Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

Abstract. This work introduces a general decoder construction called Classical-to-Quantum (C-to-Q) decoders, which extend the complementarity principle in decoding quantum information from noisy quantum systems. The C-to-Q decoder is constructed from two quantum measurements that decode classical information defined in two different bases, and its decoding error is determined by the errors of the two decoding measurements and the degree of complementarity between the two bases. As an application, the Hayden-Preskill protocol, a toy model of the black hole information paradox, is analyzed based on the C-to-Q decoder, providing an improved decoding scheme with better error exponents compared to previous results.

Keywords: Quantum error correction, Complementarity, Hayden-Preskill

Introduction and a brief summary of results

Reversing the effects of quantum noise and recovering quantum information from a noisy system plays a central role in the theory of quantum information and computation as well as in fundamental physics aiming to understand complex quantum physics by a quantum information approach. It is accomplished by utilizing quantum error correction (QEC), in which constructing a decoder is particularly important. So far, little is explored about explicit constructions of decoders for a general class of quantum error correcting codes (QECCs), except the one based on the Petz map that has been successful in investigating quantum capacities [1, 2], quantum Markov chains [3, 4], and fundamental physics [5].

Random encoding is an example of QECCs that remains largely unexplored in terms of decoding methods. It was originally introduced in information theory as an analytical technique and later has found many applications in theoretical physics. Despite having a good understanding of its encoding based on the theory of unitary designs [6–8], decoding has not been fully investigated yet. A decoder for random encoding is of particular interest in the gauge-gravity correspondence in fundamental physics since it provides a dictionary that translates one language to the other [5, 9]. This is especially the case in the study of the black hole information paradox, a long-standing open problem in fundamental physics [10–14].

Unlike the difficulty in constructing general decoders, decoding a certain class of QECCs, such as the Calderbank-Shor-Steane (CSS) codes [15, 16], is relatively straightforward. This is because CSS codes merge two classical codes, one for Pauli-X and the other for -Z, making decoding of the quantum information into decoding of two types of classical information, which is easier to deal with. This feature of the decoders for CSS codes should be extendable to any QECCs since the feature is a consequence of the property of quantum information itself, not of CSS codes. Namely, quantum information consists of two types of classical information defined in two bases complementary to each other, such as the Pauli-X and -Z. This property can be further traced back to the complementarity principle of quantum mechanics [17]; for a complete description of quantum systems, revealing two mutually exclusive features is necessary. The complementarity principle have also played a prominent role in other fields of quantum information theory such as quantum key distribution [18, 19] and quantum state merging [20].

In our study (preprint [21]), we examine the role of the complementarity principle in the decoding of quantum information, and present a

*yoshifumi.nakata@yukawa.kyoto-u.ac.jp
†takaya.matsuura@rmit.edu.au
‡koashi@qi.t.u-tokyo.ac.jp

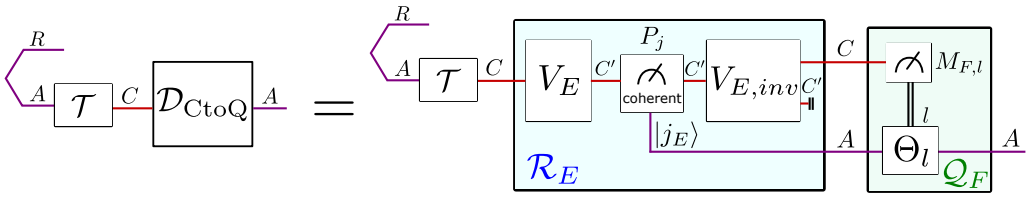


Figure 1: A diagram of the C-to-Q decoder $\mathcal{D}_{\mathrm{CtoQ}}^{C\to A}$ constructed from two POVMs M_E and M_F, which consists of two CPTP maps, $\mathcal{R}_E$ and $\mathcal{Q}_F$. The first one $\mathcal{R}_E$ is designed for coherently measuring the noisy system C and storing the outcome in the auxiliary system A. To this end, we use the Naimark extension of the POVM M_E, i.e., a pair of an isometry V_E and projections $\{P_j\}_{j=0}^{d-1}$. The outcome is coherently recorded in A as $|j_E\rangle^A$. The second channel $\mathcal{Q}_F$ is to measure C by the POVM M_F and apply a unitary Θ_l on A depending on the outcome l, which works as a 'quantum eraser'. See Sec.III.B in [21] for details.

general and explicit method for constructing decoders for any given QECC. We call this decoder *Classical-to-Quantum (C-to-Q)* decoder since it is constructed from two positive-operator-valued measures (POVMs) for decoding two types of classical information, each defined in a distinct basis of the quantum system. The underlying idea is to use one POVM for 'coherently measuring' the noisy system, and the other for the 'quantum eraser', which will be of independent interest (Sec.III.B.1 in [21]). We show that the decoding error for quantum information by the C-to-Q decoder is characterized by the decoding errors of classical information obtained through the two POVMs and by the degree of complementarity of the two bases in which the two types of classical information are embedded. In particular, if the two bases are mutually unbiased, the decoding error can completely be characterized by the two POVMs. Importantly, the C-to-Q decoder is nearly optimal if the POVMs for decoding classical information are optimal, in the sense that its decoding error for quantum information is at worst square root of the decoding error by an optimal decoder (Sec.III.B.2 in [21]). The construction of the C-to-Q decoder, as it directly connects classical and quantum information, has a direct implication on classical and quantum capacities; for a given noisy channel, no encoder can simultaneously achieve classical capacity for two types of classical information defined in two different bases, unless the classical capacity coincides with the quantum capacity (Sec.III.B.2 in [21]).

We then apply the C-to-Q decoder, constructed from two POVMs similar to the pretty-good measurements (PGMs) [22], to the Hayden-Preskill protocol [10], which is a qubit toy model of the black hole information paradox based on random encoding. We establish a sufficient condition for reliable decoding of classical and quantum information in general cases (Sec.III.C in [21]) without relying on the common assumption of Haar scrambling. Subsequently, we calculate the decoding errors explicitly, assuming Haar scrambling (Sec.III.D in [21]). Compared to the previous results based on the decoupling approach [23–25], our approach improves the exponents of the decoding errors both for classical and quantum information. This implies that employing the C-to-Q decoder could improve all analyses based on the decoupling approach.

The impact of our results is multifold. From a theoretical and foundational standpoint, we have conducted a quantitative exploration of the application of the complementarity principle in decoding quantum information from noisy systems. While this principle is expected to underlie quantum error correction, its comprehensive and quantitative investigation has been lacking, except in specific contexts [26]. Therefore, our work establishes a step toward understanding QEC from the fundamental principle of quantum theory. Moreover, the practical utility of the C-to-Q decoder is noteworthy as it simplifies the search for an optimal decoder for QECCs to the search for two optimal positive-operator-valued measures (POVMs) for decoding classical information. We also demonstrated the practicality of the C-to-Q decoder by applying it to the Hayden-Preskill protocol. We not only provide an explicit decoder but also improve the previous results. These advancements hold significance for fundamental physics as the development of explicit decoding schemes for the Hayden-Preskill protocol has been sought after in the context of gauge-gravity correspondence.

Our work broadly contributes to the theory of quantum information and computation, both fundamentally and practically, since decoders are at the center of all studies in the field. It also has impact on an interdisciplinary topics, which will be a

benefit in our community as well since it extends the future scope of the field to broader disciplines.

Main result 1: Constructing a C-to-Q decoder

Let $\mathcal{T}^{A\to C}$ be a composite quantum channel of an encoding map and a noisy channel in the context of QEC. Given $\mathcal{T}^{A\to C}$ and a decoder $\mathcal{D}^{C\to A}$, the error on decoding *quantum* information is defined as $\Delta_q(\mathcal{D}|\mathcal{T}) := \frac{1}{2}\left\|\Phi^{AR} - \mathcal{D}^{C\to A}\circ\mathcal{T}^{A\to C}(\Phi^{AR})\right\|_1$, where Φ^{AR} is a maximally entangled state (MES) between A and R with dimension d. An error on decoding *classical* information in the basis $W := \{|j_W\rangle\}_{j=0}^{d-1}$, which we refer to as W-classical information, is defined for a POVM $M = \{M_j\}_{j=0}^{d-1}$ as $\Delta_{cl,W}(M|\mathcal{T}) := \frac{1}{d}\sum_{i\neq j}\mathrm{Tr}\left[\mathcal{T}^{A\to C}(|i_W\rangle\langle i_W|^A)M_j^C\right]$. See Sec.III.A in [21] for more details.

Let $E := \{|j_E\rangle\}_j$ and $F := \{|l_F\rangle\}_l$ be bases in a d-dimensional Hilbert space $\mathcal{H}^A$. For a given quantum channel $\mathcal{T}^{A\to C}$, let $M_E := \{M_{E,j}^C\}_j$ and $M_F := \{M_{F,l}^C\}_l$ be POVMs for decoding E- and F-classical information from the noisy system C, respectively. We denote the decoding errors by $\Delta_{cl,E}(M_E|\mathcal{T})$ and $\Delta_{cl,F}(M_F|\mathcal{T})$. In the C-to-Q decoder, we use one POVM, say M_E, for constructing a channel $\mathcal{R}_E^{C\to AC}$ that measures C and stores the outcome coherently in an auxiliary system A, and the other POVM, M_F, for constructing a channel $\mathcal{Q}_F^{CA\to A}$ that plays the role of quantum eraser. See the caption of Fig. 1 for the outline of the construction as well as Sec.III.B in [21]. The C-to-Q decoder $\mathcal{D}_{\mathrm{CtoQ}}^{C\to A}$ is given by $\mathcal{D}_{\mathrm{CtoQ}}^{C\to A} := \mathcal{Q}_F^{CA\to A}\circ\mathcal{R}_E^{C\to CA}$ (See Sec.III.B in [21] for more detail).

Theorem 1 (Classical-to-Quantum decoder) *In the setting described above, the C-to-Q decoder $\mathcal{D}_{\mathrm{CtoQ}} = \mathcal{Q}_F^{CA\to A}\circ\mathcal{R}_E^{C\to CA}$ constructed from the POVMs M_E and M_F satisfies*

$$\Delta_q(\mathcal{D}_{\mathrm{CtoQ}}|\mathcal{T}) \le \sqrt{\Delta_{cl,E}\left(2-\Delta_{cl,E}(M_E|\mathcal{T})\right)} + \sqrt{\Delta_{cl,F}(M_F|\mathcal{T})} + \sqrt{\Xi_{EF}}, \tag{1}$$

where $\Xi_{EF} := 1 - \min_{l=0,\dots,d-1} F_{BC}(\mathrm{unif}_d, p_l)$ with a Bhattacharyya distance F_{BC} between the uniform distribution unif_d and the probability distribution $p_l = \{p_l(j) = |\langle j_E|l_F\rangle|^2\}_{j=0}^{d-1}$.

Note that Ξ_{EF} measures how far the two bases E and F are from mutually unbiased; $\Xi_{EF} = 0$ if and only if (E, F) is mutually unbiased such as Pauli-X and -Z bases. To better understand the C-to-Q decoder, it is helpful to closely look at each step. First, the channel $\mathcal{R}_E$ transforms the noisy state $\mathcal{T}^{A\to C}(\Phi^{AR})$ into a GHZ-like state defined on the E bases in CRA with the error $\Delta_{cl,E}$. The GHZ-like state is then transformed by $\mathcal{Q}_F$ based on the quantum eraser. The quantum eraser is ideally achieved by measuring C of the GHZ-like state in the basis mutually unbiased to E and applying a correction to A. However, since only the measurement error in the F basis is a priori given, we use the POVM M_F instead of the ideal one, resulting, with the error $\Delta_{cl,F}$, in a state Ψ_{AR} that differs from Φ_{AR}. Finally, the infidelity between the obtained state Ψ_{AR} and the initial state Φ_{AR} is upper-bounded by Ξ_{EF}. In total, this scheme works with an error characterized by $\Delta_{cl,E}$, $\Delta_{cl,F}$, and Ξ_{EF}.

Main result 2: Decoding the Hayden-Preskill protocol by the C-to-Q decoder

The Hayden-Preskill protocol is a toy model of the black hole information paradox [10]. Let B_{in} be an N-qubit system, and $\xi^{B_{\mathrm{in}}}$ be its initial state, whose purification is denoted by $|\xi\rangle^{B_{\mathrm{in}}B_{\mathrm{rad}}}$. A k-qubit quantum information A is combined with B_{in} and undergoes a given unitary dynamics U^S, where $S = AB_{\mathrm{in}}$. The system S is then randomly split into two subsystems S_{in} and S_{rad}. The goal is to clarify the number ℓ of qubits in S_{rad} for which the k-qubit information is decodable from $B_{\mathrm{rad}}S_{\mathrm{rad}}$. The problem can be rephrased as transmitting quantum information via a quantum erasure channel [27, 28] with erasure rate $1-\ell/(N+k)$. However, unlike the usual scenario, encoding is done by a given unitary U^S, not by the best possible encoding map.

Based on the decoupling, it has already been shown that there exists a decoder $\mathcal{D}$ and decoding POVMs M_W for $W = X, Z$ such that $\mathbb{E}_{U\sim\mathsf{H}}\left[\Delta_{cl,W}(M_W|\xi,U)\right] \le \mathbb{E}_{U\sim\mathsf{H}}\left[\Delta_q(\mathcal{D}|\xi,U)\right] \le 2^{(\ell_{\mathrm{th}}-\ell)/2}$, where $\ell_{\mathrm{th}} = k+(N-H_2(B_{\mathrm{in}})_\xi)/2$ with the collision entropy $H_2(B_{\mathrm{in}})_\xi$. A concrete construction of the decoders in a general situation has been open [5, 9]. The C-to-Q decoder with PGM-like POVMs, which we call pPGMs, provides an explicit decoder for quantum information. The decoding errors satisfy, for sufficiently large N,

$$\mathbb{E}_{U\sim\mathsf{H}}\left[\Delta_{cl}(M_{\mathrm{pPGM}}|\xi,U)\right] \lesssim 4^{\ell_{\mathrm{th}}-\ell}, \tag{2}$$

and

$$\mathbb{E}_{U\sim\mathsf{H}}[\Delta_q(\mathcal{D}_{\mathrm{CtoQ}}|\xi,U)] \lesssim (1+\sqrt{2})2^{\ell_{\mathrm{th}}-\ell}. \tag{3}$$

Compared to the previous results, these improve the error exponents by factor 4 for classical information and by factor 2 for quantum information. See Sec.III.D in [21] for the details.

References

[1] H. Barnum and E. Knill. Reversing quantum dynamics with near-optimal quantum and classical fidelity. *J. Math. Phys.*, 43:2097, 2002.

[2] S. Beigi, N. Datta, and F. Leditzky. Decoding quantum information via the Petz recovery map. *J. Math. Phys.*, 57:082203, 2016.

[3] P. Hayden, R. Jozsa, D. Petz, and A. Winter. Structure of States Which Satisfy Strong Subadditivity of Quantum Entropy with Equality. *Commun. Math. Phys.*, 246:359–374, 2004.

[4] O. Fawzi and R. Renner. Quantum Conditional Mutual Information and Approximate Markov Chains. 340:575–611, 2015.

[5] G. Penington, S. H. Shenker, D. Stanford, and Z. Yang. Replica wormholes and the black hole interior. *J. High Energy Phys.*, 2022:205, 2022.

[6] O. Szehr, F. Dupuis, M. Tomamichel, and R. Renner. Decoupling with unitary approximate two-designs. *New J. Phys.*, 15:053022, 2013.

[7] Y. Nakata, C. Hirche, C. Morgan, and A. Winter. Decoupling with random diagonal unitaries. *Quantum*, 1:18, 2017.

[8] Y. Nakata, E. Wakakuwa, and H. Yamasaki. One-shot quantum error correction of classical and quantum information. *Phys. Rev. A*, 104:012408, 2021.

[9] B. Yoshida and A. Kitaev. Efficient decoding for the hayden-preskill protocol. *arXiv:1710.03363*, 2017.

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

[11] 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.

[12] P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida. Chaos in quantum channels. *J. High Energy Phys.*, 2016:4, 2016.

[13] D. A. Roberts and B. Yoshida. Chaos and complexity by design. *J. High Energ. Phys.*, 2017:121, 2017.

[14] Y. Nakata, E. Wakakuwa, and M. Koashi. Black holes as clouded mirrors: the hayden-preskill protocol with symmetry. *arXiv:2007.00895*, 2020.

[15] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996.

[16] A. M. Steane. Error Correcting Codes in Quantum Theory. *Phys. Rev. Lett.*, 77:793–797, 1996.

[17] N. Bohr. The Quantum Postulate and the Recent Development of Atomic Theory1. *Nature*, 121:580–590, 1928.

[18] Joseph M. Renes and Jean-Christian Boileau. Physical underpinnings of privacy. *Phys. Rev. A*, 78:032335, Sep 2008.

[19] M. Koashi. Simple security proof of quantum key distribution based on complementarity. *New Journal of Physics*, 11(4):045018, 2009.

[20] Jean-Christian Boileau and Joseph M. Renes. Optimal state merging without decoupling. In Andrew Childs and Michele Mosca, editors, *Theory of Quantum Computation, Communication, and Cryptography*, pages 76–84, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[21] Yoshifumi Nakata, Takaya Matsuura, and Masato Koashi. Constructing quantum decoders based on complementarity principle, 2022.

[22] P. Hausladen and W. K. Wootters. A 'Pretty Good' Measurement for Distinguishing Quantum States. *Journal of Modern Optics*, 41:2385–2390, 1994.

[23] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Theory*, 51:44–55, 2005.

[24] I. Devetak and A. Winter. Relating Quantum Privacy and Quantum Coherence: An Operational Approach. *Phys. Rev. Lett.*, 93:080501, 2004.

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

[26] Joseph M. Renes. Uncertainty relations and approximate quantum error correction. *Phys. Rev. A*, 94:032314, Sep 2016.

[27] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin. Capacities of Quantum Erasure Channels. *Phys. Rev. Lett.*, 78:3217–3220, 1997.

[28] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-Assisted Classical Capacity of Noisy Quantum Channels. *Phys. Rev. Lett.*, 83:3081–3084, 1999.

Universal sampling lower bounds for quantum error mitigation

Ryuji Takagi[1 2 *] Hiroyasu Tajima[3 †] Mile Gu[3 5 6 ‡]

[1] *Department of Basic Science, University of Tokyo, Komaba, Meguro-ku, Tokyo 153-0041, Japan*
[2] *Nanyang Quantum Hub, School of Physical and Mathematical Sciences, Nanyang Technological University, 637371, Singapore 100190*
[3] *Department of Communication Engineering and Informatics, University of Electro-Communications, Chofugaoka, Chofu, Tokyo, 182-8585, Japan*
[4] *JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*
[5] *Centre for Quantum Technologies, National University of Singapore, 117543, Singapore*
[6] *MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, Singapore*

Abstract. Although numerous quantum error-mitigation protocols have been proposed as means to suppress noise effects on intermediate-scale quantum devices, their general potential and limitations have still been elusive. In particular, to understand the ultimate feasibility of quantum error mitigation, it is crucial to characterize the fundamental sampling cost — how many times an arbitrary mitigation protocol must run a noisy quantum device. Here, we establish universal lower bounds on the sampling cost for quantum error mitigation to achieve the desired accuracy with high probability. Our bounds apply to general mitigation protocols, including the ones involving nonlinear postprocessing. We further show that the number of samples required for a wide class of protocols to mitigate errors in layered circuits must grow exponentially with the circuit depth for various noise models, revealing the fundamental obstacles in showing useful applications of noisy near-term quantum devices.

Keywords: quantum error mitigation, NISQ computing

1 Overview

As recent technological developments have started to realize controllable small-scale quantum devices, a central problem in quantum information science has been to pin down what can and cannot be accomplished with noisy intermediate-scale quantum (NISQ) devices [2]. One of the most relevant issues in understanding the ultimate capability of quantum hardware is to characterize how well noise effects could be circumvented. As an alternative to quantum error correction, quantum error mitigation has recently attracted much attention as a potential tool to help NISQ devices realize useful applications [3, 4]. It is thus of primary interest from practical and foundational viewpoints to understand the ultimate feasibility of quantum error mitigation — although numerous quantum error-mitigation protocols have been proposed, **their general potential and limitations have still been elusive**.

Quantum error mitigation runs the available noisy quantum devices many times and applies postprocessing to the collected data, aiming to extract the classical information of interest. Therefore, the crucial quantity that determines the feasibility of quantum error mitigation is the *sampling cost*, the number of times one needs to run the available noisy device to ensure the desired computational accuracy. Various quantum error mitigation strategies proposed so far indeed face this problem — they tend to require exponentially many samples with respect to the circuit size [5–9]. The natural question then is whether there is a hope to come up with a new error mitigation that avoids this hurdle or this is a universal feature shared by all quantum error mitigation protocols. Addressing this question needs the evaluation of the *necessary* sampling cost incurred on the general class of error-mitigation protocols.

In this work [1], we provide the **first universal bounds for the sampling cost applicable for general error-mitigation protocols**. Our results apply to general error-mitigation protocols including the ones involving nonlinear postprocessing — such as virtual distillation [10–12], symmetry verification [13], and subspace expansion [14–16] — which constitute a large class of protocols [8, 10–25]. We also show that our bounds are tight in terms of error scaling. As an application, we show that the required samples for a wide class of mitigation protocols to error-mitigate layered circuits under various noise models — including the depolarizing and stochastic Pauli noise as examples — must grow exponentially with the circuit depth to achieve the target performance. This turns the conjecture that quantum error mitigation would generally suffer from the exponential sampling overhead into formal relations [1]. Our results disclose the fundamental limitations underlying the general error-mitigation strategies that include existing protocols [6–22, 24, 25, 28–32] and the ones yet to be discovered, being analogous to the performance converse bounds established in several other disciplines — such as thermodynamics [33–35], quantum communication [36, 37], and quantum resource theories [38, 39] — that contributed to characterize the ultimate operational capability allowed in each physical setting.

2 Framework

Suppose we wish to obtain the expectation value of an observable $A \in \mathbb{O}$ for an ideal state $\rho \in \mathbb{S}$ where $\mathbb{O}$ and $\mathbb{S}$ are some sets of observables and states that error mitigation aims to get good estimates for. In the mitigation procedure, one can first modify the circuit, e.g., use a different choice of unitary gates, apply nonadaptive operations, and supply ancillary qubits — the allowed modifications are determined by the capability of the available device. Together with the noise

*ryuji.takagi@phys.c.u-tokyo.ac.jp
†hiroyasu.tajima@uec.ac.jp
‡mgu@quantumcomplexity.org

[1] The previous works of Refs. [26, 27] addressed related questions in terms of different figures of merit but did not fully prove the exponential blow up of the sample number, which is the most operationally relevant quantity.

present in the modified circuit, this turns the original unitary $\mathcal{U}$ into some quantum channel $\mathcal{F}$, which produces a distorted state ρ'. The distorted state can be represented in terms of the ideal state ρ by $\rho' = \mathcal{E}(\rho)$ where we call $\mathcal{E} := \mathcal{F} \circ \mathcal{U}^\dagger$ an effective noise channel. The second step consists of collecting N samples $\{\mathcal{E}_n(\rho)\}_{n=1}^N$ of distorted states represented by a set of effective noise channels $\mathbb{E} := \{\mathcal{E}_n\}_{n=1}^N$ and applying an trailing quantum process $\mathcal{P}_A$ over them. The trailing process $\mathcal{P}_A$ then outputs an estimate represented by a random variable $\hat{E}_A(\rho)$ for the true expectation value $\mathrm{Tr}(A\rho)$ (see also Fig. 1 (a)). The main focus of our study is the sampling number N, the total number N of distorted states used in the error mitigation process.

3 Sampling lower bounds

We now consider the required samples to ensure the target performance. The performance of quantum error mitigation can be defined in multiple ways. Here, we consider two possible performance quantifiers that are operationally relevant.

Our first performance measure is the combination of the accuracy of the estimate and the success probability. This closely aligns with the operational motivation, where one would like an error mitigation strategy to be able to provide a good estimate for each observable in $\mathbb{O}$ and an ideal state in $\mathbb{S}$ at a high probability. This can be formalized as a condition

$$\mathrm{Prob}(|\,\mathrm{Tr}(A\rho) - \hat{E}_A(\rho)| \le \delta) \ge 1-\varepsilon,\ \forall \rho \in \mathbb{S},\ \forall A \in \mathbb{O} \tag{1}$$

where δ is the target accuracy and $1-\varepsilon$ is the success probability (see also Fig. 1 (a)). To formulate our result, let us define the observable-dependent distinguishability with respect to a set $\mathbb{O}$ of observables as $D_{\mathbb{O}}(\rho,\sigma) := \max_{A\in\mathbb{O}} |\,\mathrm{Tr}[A(\rho-\sigma)]|$. We then obtain the following sampling lower bound.

Theorem 1. *Suppose that an error-mitigation strategy achieves (1) with some $\delta \ge 0$ and $0 \le \varepsilon \le 1/2$ with N distorted states characterized by the effective noise channels $\mathbb{E} = \{\mathcal{E}_n\}_{n=1}^N$. Then, the sample number N is lower bounded as*

$$N \ge \max_{\substack{\rho,\sigma\in\mathbb{S} \\ D_{\mathbb{O}}(\rho,\sigma)\ge 2\delta}} \min_{\mathcal{E}\in\mathbb{E}} \frac{\log\left[\frac{1}{4\varepsilon(1-\varepsilon)}\right]}{\log\left[1/F(\mathcal{E}(\rho),\mathcal{E}(\sigma))\right]}, \tag{2}$$

where $F(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ is the (square) fidelity.

This result tells that if the noise effect brings states close to each other, it incurs an unavoidable sampling cost to error mitigation. The minimization over $\mathbb{E}$ chooses the effective noise channel that least reduces the infidelity. On the other hand, the maximum over the ideal states represents the fact that to mitigate two states ρ and σ that are separated further than 2δ in terms of observables in $\mathbb{O}$, the sample number N that achieves the accuracy δ and the success probability $1-\varepsilon$ must satisfy the lower bounds with respect to ρ and σ.

Let us now consider our second performance measure based on the standard deviation and the bias of the estimate. Let $\sigma_A^{\mathrm{QEM}}(\rho)$ be the standard deviation of $\hat{E}_A(\rho)$ for an observable $A \in \mathbb{O}$, which represents the uncertainty of the final estimate of an error mitigation protocol. Since a good error mitigation should come with a small fluctuation in its outcome, the standard deviation of the underlying distribution for the estimate can serve as a performance quantifier. However, the standard deviation itself is not sufficient to characterize the error mitigation performance, as one can easily come up with a useless strategy that always outputs a fixed outcome, which has zero standard deviation. This issue can be addressed by considering the deviation of the expected value of the estimate from the true expectation value called bias, defined as $b_A(\rho) := \langle \hat{E}_A(\rho)\rangle - \mathrm{Tr}(A\rho)$ for a state $\rho \in \mathbb{S}$ and an observable $A \in \mathbb{O}$ (see also Fig. 1). To assess the performance of error-mitigation protocols, we consider the worst-case error among possible ideal states and measurements. This motivates us to consider the maximum standard deviation $\sigma_{\max}^{\mathrm{QEM}} := \max_{A\in\mathbb{O}} \max_{\rho\in\mathbb{S}} \sigma_A^{\mathrm{QEM}}(\rho)$ and the maximum bias $b_{\max} := \max_{A\in\mathbb{O}} \max_{\rho\in\mathbb{S}} b_A(\rho)$. Then, we obtain the following sampling lower bound in terms of these performance quantifiers.

Theorem 2. *The sampling cost for an error-mitigation strategy with the maximum standard deviation $\sigma_{\max}^{\mathrm{QEM}}$ and the maximum bias $b_{\max}$ is lower bounded as*

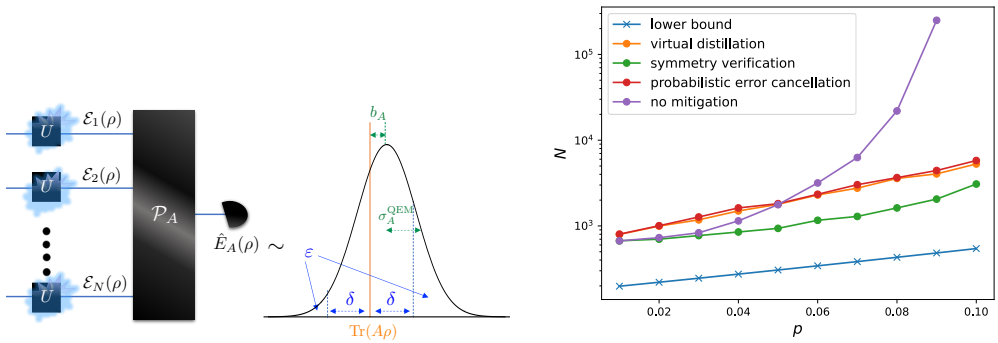
$$N \ge \max_{\substack{\rho,\sigma\in\mathbb{S} \\ D_{\mathbb{O}}(\rho,\sigma)-2b_{\max}\ge 0}} \min_{\mathcal{E}\in\mathbb{E}} \frac{\log\left[1-\frac{1}{\left(1+\frac{2\sigma_{\max}^{\mathrm{QEM}}}{D_{\mathbb{O}}(\rho,\sigma)-2b_{\max}}\right)^2}\right]^{-1}}{\log\left[1/F(\mathcal{E}(\rho),\mathcal{E}(\sigma))\right]}. \tag{3}$$

This result represents the trade-off between the standard deviation, bias, and the required sampling cost. To realize the small standard deviation and bias, error mitigation needs to use many samples; in fact, the lower bound diverges at the limit of $\sigma_{\max}^{\mathrm{QEM}} \to 0$ whenever there exist states $\rho,\sigma \in \mathbb{S}$ such that $D_{\mathbb{O}}(\rho,\sigma) \ge 2b_{\max}$. On the other hand, a larger bias results in a smaller sampling lower bound, indicating a potential to reduce the sampling cost by giving up some bias.

The bounds in Theorems 1, 2 are universally applicable to arbitrary error mitigation protocols in our framework and thus are not expected to give good estimates for a given specific error-mitigation protocol in general (just as there is a huge gap between the Carnot efficiency and the efficiency of most of the practical heat engines). Nevertheless, it is still insightful to investigate how our bounds are compared to existing mitigation protocols. Rather remarkably, we show that the error scaling of the lower bound in Theorem 2 can be achieved by the probabilistic error cancellation method in a certain scenario, showing the tightness of our bound in Theorem 2 as well as the optimality of probabilistic error cancellation in terms of error scaling; details can be found in Appendix D of the technical manuscript. In Fig. 1 (b), we also numerically study the bound in Theorem 1 to mitigate local depolarizing noise in relation to several specific error-mitigation methods. This shows that our bound can provide nontrivial lower bounds in this setting, with the gap being the factor of 3 to 6 in the studied range. Although this does not guarantee (and we do not even expect) that our bound behaves similarly for other scenarios in general, this ensures that there is a setting in which the bound in Theorem 1 can provide a nearly tight estimate.

4 Noisy layered circuits

The above results clarify the close relation between the sampling cost and state distinguishability. As an application



(a) (b)

Figure 1: (a) Framework of quantum error mitigation. (b) The lower bound in Theorem 1 and the actual samples N used for several specific error-mitigation protocols to mitigate 7-qubit local depolarizing noise with noise strength p. Details in Appendix E of the technical manuscript.

of our general bounds, we study the inevitable sample overhead to mitigate noise in the circuits consisting of multiple layers of unitaries. Although we here focus on the local depolarizing noise, our results can be extended to a number of other noise models.

Suppose that an M-qubit quantum circuit consists of layers of unitaries, each of which is followed by a local depolarizing noise $\mathcal{D}_p^{\otimes M}$ with $\mathcal{D}_p = (1-p)\,\mathrm{id} + p\mathbb{I}/2$. Although the noise strength can vary for different locations, we suppose that at least L layers are followed by the local depolarizing noise with noise strength of at least γ and call these layers $U_1, U_2, \ldots, U_L$. We aim to estimate ideal expectation values for the target states $\mathbb{S}$ and observables $\mathbb{O}$ by using N such noisy layered circuits. Here, we consider the error mitigation protocols that apply an arbitrary trailing process over N distorted states and any unital operations (i.e., operations that preserve the maximally mixed state) before and after U_l.

Theorem 3. *Suppose that an error-mitigation strategy described above is applied to an M-qubit circuit to mitigate local depolarizing channels with strength at least γ that follow L layers of unitaries, and achieves (1) with some $\delta \geq 0$ and $0 \leq \varepsilon \leq 1/2$. Then, if there exist at least two states $\rho, \sigma \in \mathbb{S}$ such that $D_{\mathbb{O}}(\rho,\sigma) \geq 2\delta$, the required sample number N is lower bounded as*

$$N \geq \frac{(1-2\varepsilon)^2}{2\ln(2)\, M(1-\gamma)^{2L}}. \tag{4}$$

This result particularly shows that the required number of samples must grow exponentially with the circuit depth L, revealing the fundamental obstacles in showing useful applications of noisy near-term quantum devices. We remark that the bound always holds under the mild condition, i.e., $D_{\mathbb{O}}(\rho,\sigma) \geq 2\delta$ for some $\rho, \sigma \in \mathbb{S}$. This reflects that, to achieve the desired accuracy δ satisfying this condition, error mitigation really needs to extract the expectation values about the observables in $\mathbb{O}$ and the states in $\mathbb{S}$, prohibiting it from merely making a random guess. In the technical manuscript, we also obtain a similar exponential growth of the required sample overhead for a fixed bias and standard deviation.

As we discuss in Appendix I of the technical manuscript, we can extend these results to a wide class of noise models, including stochastic Pauli, global depolarizing, and thermal noise. The case of thermal noise particularly provides an intriguing physical interpretation: the sampling cost N required to mitigate thermal noise after time t is characterized by the loss of free energy $N = \Omega(1/[F(\rho_t) - F_{\mathrm{eq}}])$ where ρ_t is the state at time t and F_{eq} is the equilibrium free energy. This in turn shows that the necessary sampling cost grows as $N = \Omega(e^{\alpha_{\mathrm{ent}} t})$ where α_{ent} is a constant characterized by the minimum entropy production rate.

5 Discussion

We established sampling lower bounds imposed on the general quantum error-mitigation protocols. Our results formalize the idea that the reduction in the state distinguishability caused by noise and error-mitigation processes lead to the unavoidable operational cost for quantum error mitigation. We then showed that error-mitigation protocols with certain intermediate operations and an arbitrary trailing process require the number of samples that grows exponentially with the circuit depth to mitigate various types of noise. We presented these bounds with respect to two performance quantifiers — accuracy and success probability, as well as the standard deviation and bias — each of which has its own operational relevance. Our bounds provide fundamental limitations that universally apply to general mitigation protocols, clarifying the underlying principle that regulates error-mitigation performance.

References

[1] Ryuji Takagi, Hiroyasu Tajima, and Mile Gu. Universal sampling lower bounds for quantum error mitigation. 2022.

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

[3] Sam McArdle, Suguru Endo, Alán Aspuru-Guzik, Simon C. Benjamin, and Xiao Yuan. Quantum computational chemistry. *Rev. Mod. Phys.*, 92:015003, Mar 2020.

[4] Suguru Endo, Zhenyu Cai, Simon C. Benjamin, and Xiao Yuan. Hybrid quantum-classical algorithms and quantum error mitigation. *J. Phys. Soc. Japan*, 90(3):032001, 2021.

[5] Xiao Yuan, Zhen Zhang, Norbert Lütkenhaus, and Xiongfeng Ma. Simulating single photons with realistic photon sources. *Phys. Rev. A*, 94:062305, Dec 2016.

[6] Kristan Temme, Sergey Bravyi, and Jay M. Gambetta. Error mitigation for short-depth quantum circuits. *Phys. Rev. Lett.*, 119:180509, Nov 2017.

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

[8] Suguru Endo, Simon C. Benjamin, and Ying Li. Practical quantum error mitigation for near-future applications. *Phys. Rev. X*, 8:031027, Jul 2018.

[9] Sergey Bravyi, Sarah Sheldon, Abhinav Kandala, David C. Mckay, and Jay M. Gambetta. Mitigating measurement errors in multiqubit experiments. *Phys. Rev. A*, 103:042605, Apr 2021.

[10] Bálint Koczor. Exponential error suppression for near-term quantum devices. *Phys. Rev. X*, 11:031057, Sep 2021.

[11] William J. Huggins, Sam McArdle, Thomas E. O'Brien, Joonho Lee, Nicholas C. Rubin, Sergio Boixo, K. Birgitta Whaley, Ryan Babbush, and Jarrod R. McClean. Virtual distillation for quantum error mitigation. *Phys. Rev. X*, 11:041036, Nov 2021.

[12] Piotr Czarnik, Andrew Arrasmith, Lukasz Cincio, and Patrick J. Coles. Qubit-efficient exponential suppression of errors. February 2021.

[13] X. Bonet-Monroig, R. Sagastizabal, M. Singh, and T. E. O'Brien. Low-cost error mitigation by symmetry verification. *Phys. Rev. A*, 98:062339, Dec 2018.

[14] Jarrod R. McClean, Mollie E. Kimchi-Schwartz, Jonathan Carter, and Wibe A. de Jong. Hybrid quantum-classical hierarchy for mitigation of decoherence and determination of excited states. *Phys. Rev. A*, 95:042308, Apr 2017.

[15] Jarrod R. McClean, Zhang Jiang, Nicholas C. Rubin, Ryan Babbush, and Hartmut Neven. Decoding quantum errors with subspace expansions. *Nat. Comm.*, 11(1):636, January 2020.

[16] Nobuyuki Yoshioka, Hideaki Hakoshima, Yuichiro Matsuzaki, Yuuki Tokunaga, Yasunari Suzuki, and Suguru Endo. Generalized quantum subspace expansion. *Phys. Rev. Lett.*, 129:020502, Jul 2022.

[17] Zhenyu Cai. Quantum Error Mitigation using Symmetry Expansion. *Quantum*, 5:548, September 2021.

[18] Zhenyu Cai. Multi-exponential error extrapolation and combining error mitigation techniques for NISQ applications. *npj Quantum Inf.*, 7(1):80, May 2021.

[19] Rawad Mezher, James Mills, and Elham Kashefi. Mitigating errors by quantum verification and postselection. *Phys. Rev. A*, 105:052608, May 2022.

[20] Enrico Fontana, Ivan Rungger, Ross Duncan, and Cristina Cîrstoiu. Spectral analysis for noise diagnostics and filter-based digital error mitigation. June 2022.

[21] Thomas E. O'Brien, Stefano Polla, Nicholas C. Rubin, William J. Huggins, Sam McArdle, Sergio Boixo, Jarrod R. McClean, and Ryan Babbush. Error mitigation via verified phase estimation. *PRX Quantum*, 2:020317, May 2021.

[22] Daniel Bultrini, Max Hunter Gordon, Piotr Czarnik, Andrew Arrasmith, Patrick J. Coles, and Lukasz Cincio. Unifying and benchmarking state-of-the-art quantum error mitigation techniques. July 2021.

[23] Paul D. Nation, Hwajung Kang, Neereja Sundaresan, and Jay M. Gambetta. Scalable mitigation of measurement errors on quantum computers. *PRX Quantum*, 2:040326, Nov 2021.

[24] Armands Strikis, Dayue Qin, Yanzhu Chen, Simon C. Benjamin, and Ying Li. Learning-based quantum error mitigation. *PRX Quantum*, 2:040330, Nov 2021.

[25] Yifeng Xiong, Soon Xin Ng, and Lajos Hanzo. Quantum error mitigation relying on permutation filtering. *IEEE Trans. Commun.*, 70(3):1927–1942, 2022.

[26] Ryuji Takagi, Suguru Endo, Shintaro Minagawa, and Mile Gu. Fundamental limits of quantum error mitigation. *npj Quantum Inf.*, 8:114, September 2022.

[27] Samson Wang, Piotr Czarnik, Andrew Arrasmith, M. Cerezo, Lukasz Cincio, and Patrick J. Coles. Can error mitigation improve trainability of noisy variational quantum algorithms? 2021.

[28] Piotr Czarnik, Andrew Arrasmith, Patrick J. Coles, and Lukasz Cincio. Error mitigation with Clifford quantum-circuit data. *Quantum*, 5:592, November 2021.

[29] Angus Lowe, Max Hunter Gordon, Piotr Czarnik, Andrew Arrasmith, Patrick J. Coles, and Lukasz Cincio. Unified approach to data-driven quantum error mitigation. *Phys. Rev. Research*, 3:033098, Jul 2021.

[30] Mingxia Huo and Ying Li. Dual-state purification for practical quantum error mitigation. *Phys. Rev. A*, 105:022427, Feb 2022.

[31] Kun Wang, Yu-Ao Chen, and Xin Wang. Mitigating Quantum Errors via Truncated Neumann Series. November 2021.

[32] Andrea Mari, Nathan Shammah, and William J. Zeng. Extending quantum probabilistic error cancellation by noise scaling. *Phys. Rev. A*, 104:052607, Nov 2021.

[33] Sadi Carnot. Reflections on the motive power of fire, and on machines fitted to develop that power. *Paris: Bachelier*, 108:1824, 1824.

[34] R. Landauer. Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.*, 5(3):183, 1961.

[35] Fernando Brandão, Michał Horodecki, Nelly Ng, Jonathan Oppenheim, and Stephanie Wehner. The second laws of quantum thermodynamics. *Proc. Natl. Acad. Sci. U.S.A.*, 112:3275, 2015.

[36] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. *Phys. Rev. Lett.*, 83:3081, Oct 1999.

[37] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nat. Commun.*, 8:15043, 2017.

[38] Bartosz Regula and Ryuji Takagi. Fundamental limitations on distillation of quantum channel resources. *Nat. Commun.*, 12:4411, 2021.

[39] Kun Fang and Zi-Wen Liu. No-go theorems for quantum resource purification: New approach and channel theory. *PRX Quantum*, 3:010337, Mar 2022.

A Race Track Trapped-Ion Quantum Processor

Michael Mills[1]

[1]*Quantinuum*

Abstract. We describe and benchmark a new quantum charge-coupled device (QCCD) trapped-ion quantum computer based on a linear trap with periodic boundary conditions, which resembles a race track. The new system successfully incorporates several technologies crucial to future scalability, including electrode broadcasting, multi-layer RF routing, and magneto-optical trap (MOT) loading, while maintaining, and in some cases exceeding, the gate fidelities of previous QCCD systems. The system is initially operated with 32 qubits, but future upgrades will allow for more. We benchmark the performance of primitive operations, including an average state preparation and measurement error of 1.6(1)e-3, an average single-qubit gate infidelity of 2.5(3)e-5, and an average two-qubit gate infidelity of 1.84(5)e-3. The system-level performance of the quantum processor is assessed with mirror benchmarking, linear cross-entropy benchmarking, a quantum volume measurement of QV = 2^{16}, and the creation of 32-qubit entanglement in a GHZ state. We also tested application benchmarks including Hamiltonian simulation, QAOA, error correction on a repetition code, and dynamics simulations using qubit reuse. We also discuss future upgrades to the new system aimed at adding more qubits and capabilities.

An invertible map between Bell non-local and contextuality scenarios arXiv: 2211.12550

Victoria J Wright[1] * Máté Farkas[1] †

[1] *ICFO—The Institute of Photonic Sciences, Mediterranean Technology Park, Avinguda Carl Friedrich Gauss, 3, 08860 Castelldefels, Barcelona*

Abstract.
We present an invertible map between correlations in any bipartite Bell scenario and behaviours in a family of contextuality scenarios. The map takes local, quantum and non-signalling correlations to non-contextual, quantum and contextual behaviours, respectively. Consequently, we find that the membership problem of the set of quantum contextual behaviours is undecidable, the set cannot be fully realised via finite dimensional quantum systems and is not closed. Finally, we show that neither this set nor its closure is the limit of a sequence of computable supersets, due to the result MIP*=RE.

Keywords: non-locality, generalised contextuality, semidefinite programming

Introduction Bell non-locality [1] is a property of correlations observed between space-like separated experiments. Bell non-local correlations are impossible in any locally realistic theory, such as those of classical physics. Such correlations are, however, allowed in quantum theory. Beyond their fundamental relevance these correlations have technological applications such as secure random number generation [2] and cryptography [3].

Generalised contextuality [4] similarly describes correlations that are absent from classical physics but instead of space-like separation, these correlations occur in experiments where there are *operationally equivalent* experimental procedures. For example, two preparation procedures for a system are operationally equivalent if no measurement on the system can distinguish which preparation procedure was used, even after many rounds of preparation and measurement. Contextual correlations have also found practical relevance, for example, in state discrimination [5] and demonstrating quantum advantage in communication tasks [6].

These two types of experiments both distinguish quantum physics from its classical counterpart, so one can ask whether they are independent of each other, whether they share a common underlying mechanism or, more strongly, whether one subsumes the other. It is not uncommon to hear in the contextuality community that non-locality is "an example" of contextuality. This work puts a formal meaning to this claim in the case of two-party non-locality and generalised contextuality. Our results show that combining quantum contextuality and the no-signalling principle exactly constraints non-local correlations to those allowed for in quantum theory. We then use this connection to prove fundamental results about quantum contextuality.

Generalised contextuality In this work a contextuality scenario is a prepare-and-measure experiment with a fixed number of preparations, measurements and outcomes, in which some operational equivalences must hold between the preparations (more generally, equivalences between measurements and transformations can also be considered). Two preparations, P and P', are operationally equivalent, $P \simeq P'$, if they give the same statistics for every measurement on the system. A theory describing these measurements would say the probabilities, $q(a|P, M)$ and $q(a|P', M)$, of seeing an outcome a of a measurement M when the system was prepared as per procedure P or P' should be equal for all measurements, M, and their outcomes, a.

The correlations observed in a contextuality scenario reveal a difference between non-contextual theories, such as classical physics, quantum theory and more general contextual theories, as depicted in each square on the right hand side of Fig. 1. Analogously to how quantum non-locality does not extend to all non-signalling correlations in Bell scenarios, quantum contextuality does not extend to all contextual correlations.

The map One way to enforce operational equivalences between preparations is by using the setup of a Bell non-locality experiment (known as a Bell scenario), under the assumption that no signal can travel faster than light. Let Alice and Bob share many copies of a physical system. If Alice selects and performs a measurement x on each of her parts, then the statistics Bob can observe by measuring his parts at any the time before a signal could have arrived must not depend on x, otherwise he could infer Alice's choice x. Thus, the average preparation of Bob's system given any choice, x, of Alice must be operationally equivalent to that given any other choice, x', of Alice. In this way, a Bell scenario is viewed as a *remote*-preparation and measurement experiment with preparation equivalences given by the no-signalling constraints.

This connection between two party Bell scenarios and (prepare-and-measure) contextuality scenarios is described in various works[1] [10, 5, 11]. In general, the re-

*victoriawright@icfo.eu
†matefarkas@icfo.eu

[1] Viewing a Bell scenario as a remote-preparation and measurement experiment has also been used to link entanglement and contextuality [7], as well as non-locality and quantum advantage in

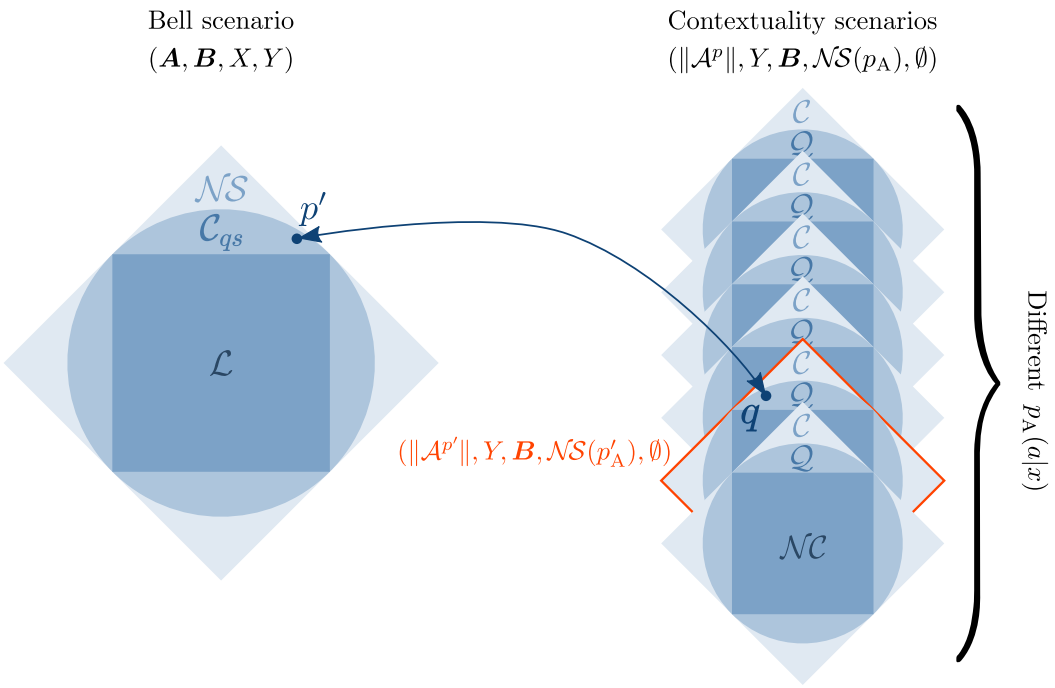


Figure 1: A schematic representation of the invertible map between correlations in a Bell scenario and correlations in a family of contextuality scenarios. Here $q(b|[a|x], y) = p'(a, b|x, y)/p'_{\mathrm{A}}(a|x)$. The sets $\mathcal{L}$, $\mathcal{C}_{qs}$ and $\mathcal{NS}$ represent the local, quantum spatial and no-signalling sets in Bell scenarios, respectively, while $\mathcal{NC}$, $\mathcal{Q}$ and $\mathcal{C}$ represent the non-contextual, quantum and contextual sets in contextuality scenarios, respectively. See the main text for details.

lationship is described via examples and the general case is not addressed. We formalise the relationship defining an invertible map in the general case.

Explicitly, let $P_{a|x}$ describe the preparation procedure for Bob's system in which Alice chooses a measurement x and sees an outcome a. When Alice chooses measurement x the average preparation of Bob's system is described by the mixture $\sum_a p_{\mathrm{A}}(a|x)P_{a|x}$, where $p_{\mathrm{A}}(a|x)$ is Alice's marginal probability distribution of seeing outcome a given that she chose input x in the Bell scenario. No-signalling implies that this preparation should be operationally equivalent to $\sum_a p_{\mathrm{A}}(a|x')P_{a|x'}$ for any other input x' of Alice.

Viewing the Bell scenario as a contextuality scenario with Alice performing the preparation procedures and Bob the measurements, the probability, q, that Bob sees outcome b given that preparation $P_{a|x}$ was performed and he chose measurement y is given by:

$$q(b|[a|x], y) = \frac{p(a, b|x, y)}{p_{\mathrm{A}}(a|x)}\,, \tag{1}$$

where $p(a, b|x, y)$ is the probability of Alice and Bob seeing outcomes a and b, given they gave inputs x and y, respectively, when the experiment is viewed as a Bell scenario.

This equation maps the correlations in a Bell scenario to correlations in one of a family of contextuality scenarios, defined by (i) the number of preparations $P_{a|x}$, measurements y and possible outcomes b, each of which only depend on the numbers of inputs and outputs of the Bell scenario, and, (ii) the operational equivalences

$$\sum_a p_{\mathrm{A}}(a|x)P_{a|x} \simeq \sum_a p_{\mathrm{A}}(a|x')P_{a|x'} \tag{2}$$

for all pairs x and x' of inputs for Alice. These equivalences vary based on the correlation, $p(a, b|x, y)$, since they depend on Alice's marginals $p_{\mathrm{A}}(a|x) = \sum_b p(a, b|x, y)$. This variation is the main reason why one Bell scenario maps to a family of contextuality scenarios, see Fig. 1.

Note that if Alice has some outcomes which never occur, $p_{\mathrm{A}}(a|x) = 0$, we map to a contextuality scenario without the preparation $P_{a|x}$. In order for the map to be invertible we also add an index to record where the zero probability outcome should be added back in to the Bell scenario. We show that our map, loosely given by Eq. (1), takes correlations that are (i) local to non-contextual correlations, (ii) quantum[2] to quantum correlations and (iii) non-signalling to general contextual correlations.

We then show the map to be invertible, with the inverse similarly preserving the three relationships above. In the quantum case we use the Schrödinger-HJW theorem [12], which gives an explicit construction to show that a quantum system can be steered into any assemblage of quantum states non-locally. Density operators obeying preparation equivalences of the form in Eq. (2) form an assemblage, and the Schrödinger-HJW theorem

oblivious communication tasks [8, 9].

[2]The quantum Bell correlations we consider are those given by the tensor product formalism for potentially infinite dimensional quantum systems, often denoted $\mathcal{C}_{qs}$ for quantum spatial correlations.

gives a construction for the quantum realisation of the corresponding non-local correlation.

It was previously thought that all contextuality scenarios of a certain kind (in which there are no measurement equivalences and the preparation equivalences comprise various decompositions of one single hypothetical preparation) could be mapped to Bell scenarios in this manner [5, Sec. VII]. However, we find examples of such scenarios in which this mapping is not possible. Of course, this does not rule out an isomorphism in this case but a different map would be required.

Consequences Firstly, imagine if it were possible to produce a correlation outside of the quantum set, $\mathcal{C}_{qs}$, in a Bell scenario. Then, if we believe no signal can travel faster than light (ensuring the preparation equivalences hold when viewing the Bell scenario as a contextuality scenario with remote preparation), our map shows we would also be able to observe a superquantum contextual correlation, i.e. a correlation outside the quantum set, $\mathcal{Q}$. In other words, the no-signalling principle together with quantum correlations constrain non-local correlations to exactly the quantum spatial correlations, $\mathcal{C}_{qs}$.

Secondly, the existence of our isomorphism gives various corollaries about the set of quantum correlations in contextuality scenarios.

Corollary 1 *The membership problem for the set of quantum behaviours in a contextuality scenario is undecidable.*

Corollary 2 *The set of behaviours deriving from finite-dimensional quantum systems in contextuality scenarios is a strict subset of its infinite-dimensional counterpart.*

Corollary 3 *In general, the set of behaviours in a contextuality scenario is not closed.*

Corollary 4 *No hierarchy of computable supersets converges to the quantum contextual set $\mathcal{Q}$ or its closure $\overline{\mathcal{Q}}$ for all contextuality scenarios.*

This final corollary shows that the semidefinite programming (SDP) hierarchies approximating the set of quantum contextual correlations [13, 14] do not, in general, converge to the quantum set or its closure. This result follows from showing that a computable hierarchy of outer approximations converging to the quantum set of contextual behaviours would give rise to an algorithm capable of deciding the weak membership problem for the closure $\mathcal{C}_{qa}$ of $\mathcal{C}_{qs}$. However, this problem is known to be undecidable as a consequence of the result MIP* = RE [15].

Outlook Corollary 4 raises several open questions. To what superset, $\mathcal{Q}_\infty$, of quantum behaviours do the SDP hierarchies in Refs. [13, 14] converge? What would be the image of $\mathcal{Q}_\infty$ in the Bell setting under our mapping? A natural candidate could be the set of quantum commuting correlations. If this is the case, does $\mathcal{Q}_\infty$ have a physical interpretation in the contextuality setting? Alternatively, the image of $\mathcal{Q}_\infty$ might provide a new outer approximation of the set $\mathcal{C}_{qs}$.

More generally, our map opens a path to better understanding quantum contextuality and the technologies it powers. For example, there is potential to translate self-testing results and device-independent security proofs from non-locality to contextuality, where the technologically demanding requirement of space-like separation can be replaced by an assumption that allows trust in the operational equivalences, a tradeoff which will be preferable in some settings.

References

[1] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, 2014.

[2] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[3] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* , 98:230501, 2007.

[4] Robert W Spekkens. Contextuality for preparations, transformations, and unsharp measurements. *Phys. Rev. A*, 71(5):052108, 2005.

[5] David Schmid and Robert W Spekkens. Contextual advantage for state discrimination. *Phys. Rev. X*, 8(1):011015, 2018.

[6] Armin Tavakoli and Roope Uola. Measurement incompatibility and steering are necessary and sufficient for operational contextuality. *Phys. Rev. Research*, 2(1):013011, 2020.

[7] Martin Plávala and Otfried Gühne. Contextuality as a precondition for entanglement. *arXiv:2209.09942*, 2022.

[8] Alley Hameedi, Armin Tavakoli, Breno Marques, and Mohamed Bourennane. Communication games reveal preparation contextuality. *Phys. Rev. Lett.*, 119:220402, 2017.

[9] Debashis Saha and Anubhav Chaturvedi. Preparation contextuality as an essential feature underlying quantum communication advantage. *Phys. Rev. A*, 100(2):022108, 2019.

[10] Yeong-Cherng Liang, Robert W. Spekkens, and Howard M. Wiseman. Specker's parable of the overprotective seer: A road to contextuality, nonlocality and complementarity. *Phys. Rep.*, 506(1):1 – 39, 2011.

[11] David Schmid, Robert W. Spekkens, and Elie Wolfe. All the noncontextuality inequalities for arbitrary prepare-and-measure experiments with respect to any fixed set of operational equivalences. *Phys. Rev. A*, 97:062103, Jun 2018.

[12] K Kirkpatrick. The Schrödinger-HJW theorem. *Found. Phys. Lett.*, 19:95, 2006.

[13] Armin Tavakoli, Emmanuel Zambrini Cruzeiro, Roope Uola, and Alastair A Abbott. Bounding and simulating contextual correlations in quantum theory. *PRX Quantum*, 2(2):020334, 2021.

[14] Anubhav Chaturvedi, Máté Farkas, and Victoria J Wright. Characterising and bounding the set of quantum behaviours in contextuality scenarios. *Quantum*, 5:484, 2021.

[15] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*=RE. *arXiv:2001.04383*, 2020.

Virtual quantum resource distillation

Xiao Yuan[1 2 3] Bartosz Regula[4 5] Ryuji Takagi[6] Mile Gu[6 7 8]

[1]*Center on Frontiers of Computing Studies, Peking University, Beijing 100871, China*
[2]*School of Computer Science, Peking University, Beijing 100871, China*
[3]*Stanford Institute for Theoretical Physics, Stanford University, Stanford California 94305, USA*
[4]*Mathematical Quantum Information RIKEN Hakubi Research Team, RIKEN Cluster for Pioneering Research (CPR) and RIKEN Center for Quantum Computing (RQC), Wako, Saitama 351-0198, Japan*
[5]*Department of Physics, Graduate School of Science, The University of Tokyo, Bunkyo-ku, Tokyo 113-0033, Japan*
[6]*Nanyang Quantum Hub, School of Physical and Mathematical Sciences, Nanyang Technological University, 637371, Singapore*
[7]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore*
[8]*CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, Singapore 117543, Singapore*

Abstract. Distillation, or purification, is central to the practical use of quantum resources in noisy settings often encountered in quantum communication and computation. Conventionally, distillation requires using some restricted 'free' operations to convert a noisy state into one that approximates a desired pure state. Here, we propose to relax this setting by only requiring the approximation of the measurement statistics of a target pure state, which allows for additional classical postprocessing of the measurement outcomes. We show that this extended scenario, which we call *virtual resource distillation*, provides considerable advantages over standard notions of distillation, allowing for the purification of noisy states from which no resources can be distilled conventionally. We show that general states can be virtually distilled with a cost (measurement overhead) that is inversely proportional to the amount of existing resource, and we develop methods to efficiently estimate such cost via convex and semidefinite programming, giving several computable bounds. We consider applications to coherence, entanglement, and magic distillation, and an explicit example in quantum teleportation (distributed quantum computing).

Keywords: quantum resources, entanglement distillation, error mitigation

Full paper: arXiv:2303.00955

Introduction A particularly important task in the manipulation of quantum resources is resource distillation, aiming to extract optimal resources — typically pure, highly resourceful ones — from non-optimal ones, using only free operations. Resource distillation is critical since it provides a systematic approach to obtain ideal resources from ones that are possibly damaged by implementation imperfections and the noisy environments in which near-term quantum technologies operate.

Conventional studies focus on unconditional resource distillation, in that the distilled resource could be used almost exactly as the optimal resource. Many powerful theoretical results have been obtained for one-shot and asymptotic resource distillation for general and specific resource theories [1–3]. Yet, especially in the one-shot scenario, fundamental limitations exist that prohibit resource distillation even for highly resourceful objects, either demanding many copies of the resource object to enable a successful conversion, or incurring large errors in the process. Are there more efficient resource distillation schemes in less restrictive settings?

Here [4], we answer in the affirmative by proposing a new paradigm of virtual resource distillation. We observe first that in most quantum information protocols, the output of a circuit is destined for measurement. Therefore, we focus on recovering classical expectation values of the target optimal resources. Without physically having the optimal resource, we can virtually simulate it, in the sense that any operation and measurement on the target resource can be approximated to any desired accuracy. We show that virtual distillation enables us to effectively increase the distillation efficiency at an increased cost in the measurement samples. We study the properties of this cost, showing how it could be bounded using resource monotones and calculated via efficient semidefinite programs. We illustrate that various limitations on conventional distillation schemes can be circumvented by employing virtual distillation, enabling resource distillation in situations where the extraction of resources is otherwise impossible. In the technical manuscript, we give examples of virtual distillation for coherence, entanglement, and magic, and discuss the application in quantum teleportation.

Background A resource theory of states consists of two parts: the set of free states $\mathcal{F}$ and the set of free operations $\mathcal{O}$. A weak and undemanding assumption about the free operations $\Lambda \in \mathcal{O}$ is the so-called 'golden rule', which states that $\Lambda(\sigma) \in \mathcal{F}, \forall \sigma \in \mathcal{F}$. The set of all operations that satisfy the golden rule, called resource non-generating (RNG) operations, is then the largest set of free operations. In most state resource theories, we can define an optimal unit pure resource state, denoted as ψ. A common task is to consider the conversion between a given state ρ and the optimal unit state ψ. The one-shot resource distillation rate

$$D^{\varepsilon}(\rho) = \max_{\Lambda \in \mathcal{O}} \left\{ m : \frac{1}{2} \left\| \Lambda(\rho) - \psi^{\otimes m} \right\|_1 \leq \varepsilon \right\} \qquad (1)$$

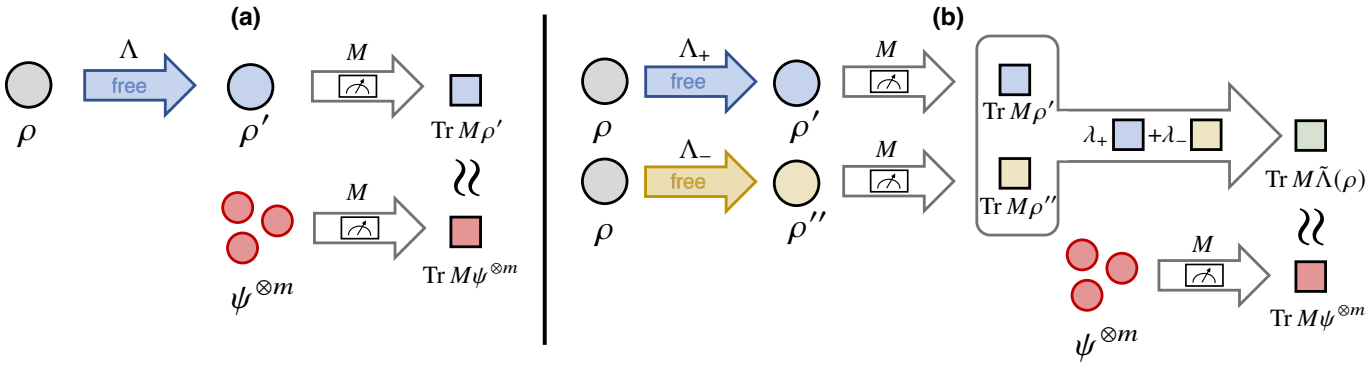


Figure 1: Illustration of two different approaches to resource distillation. (a) Conventional resource distillation, which employs a free operation Λ to map ρ into a state such that, for any measurement M, the statistics of the output state approximate the statistics of the target state $\psi^{\otimes m}$. (b) Virtual distillation, which approximates the measurement statistics of $\psi^{\otimes m}$ by using the virtual operation $\tilde{\Lambda} = \lambda_+\Lambda_+ + \lambda_-\Lambda_-$, a linear combination of free operations $\Lambda_\pm$.

then defines number of optimal states we can synthesize with ρ at allowable error $\epsilon \in [0, 1)$. A central task in resource theories is to determine $D^\varepsilon(\rho)$ as well as the rate when more copies of the input state are available.

Virtual resource distillation We consider the general context of using a resource within a quantum information processing protocol where the ultimate goal is to emit classical data. In such cases, the protocol involves applying certain operations $\mathcal{N}$ on the resource state (possibly together with other states), after which classical outputs are obtained by measurement of some Hermitian observable M. In order for a distillation protocol Λ to be successful, we thus require that measuring $\mathcal{N} \circ \Lambda(\rho)$ approximates the measurement outcomes of $\mathcal{N}(\psi^{\otimes m})$ for any choice of a channel $\mathcal{N}$ and measurement M. Since applying a channel $\mathcal{N}$ cannot make the error any larger, our requirement is equivalent to the statement that

$$\left|\mathrm{Tr}M\Lambda(\rho) - \mathrm{Tr}M\psi^{\otimes m}\right| \leq \varepsilon \tag{2}$$

for any Hermitian operator M satisfying $0 \leq M \leq I$. At this stage, this condition is actually the same as the one for conventional distillation in Eq. (1), so we have gained no advantage. However, since $\mathrm{Tr}M\Lambda(\rho)$ is a classical result, we can further apply a classical post-processing: we can consider a linear combination of the classical results $\sum_j \lambda_j \mathrm{Tr}\left(M\Lambda_j(\rho)\right) = \mathrm{Tr}\left(M\sum_j \lambda_j\Lambda_j(\rho)\right)$ using different choices of $\{\Lambda_j\} \subseteq \mathcal{O}$ and real coefficients λ_j satisfying $\sum_j \lambda_j = 1$. Grouping free operations with the same sign together, we can extend Eq. (2) to $\left|\mathrm{Tr}\left[M\left(\lambda_+\Lambda_+(\rho) - \lambda_-\Lambda_-(\rho)\right)\right] - \mathrm{Tr}M\psi^{\otimes m}\right| \leq \varepsilon$. where $\lambda_\pm = \sum_{j:\mathrm{sign}(j)=\pm 1}\lambda_j \geq 0$, $\lambda_+ - \lambda_- = 1$, and $\Lambda_\pm = \frac{1}{\lambda_\pm}\sum_{j:\mathrm{sign}(j)=\pm 1}\lambda_j\Lambda_j$. This is equivalent to the virtual distillation condition $\frac{1}{2}\left\|\tilde{\Lambda}(\rho) - \psi^{\otimes m}\right\|_1 \leq \varepsilon$, where we define $\tilde{\Lambda} = \lambda_+\Lambda_+ - \lambda_-\Lambda_-$ to be a virtual operation, see also Fig. 1.

We can effectively implement $\tilde{\Lambda}$ by following a Monte Carlo–based approach previously used in simulation of quantum circuits [5, 6] and quantum error mitigation [7–9]. Notice that for any M, we have $\mathrm{Tr}M\tilde{\Lambda}(\rho) = C\big[\mathrm{sign}(\Lambda_+)p_+\mathrm{Tr}M\Lambda_+(\rho) + \mathrm{sign}(\Lambda_-)p_-\mathrm{Tr}M\Lambda_-(\rho)\big]$. Therefore, we can obtain $\mathrm{Tr}M\tilde{\Lambda}(\rho)$ by randomly applying $\Lambda_\pm$ with probability $p_\pm = \lambda_\pm/(\lambda_+ + \lambda_-)$ and multiply each classical outcome by $C\mathrm{sign}(\Lambda_\pm) = \pm C$. Here, $C := \lambda_+ + \lambda_- \geq 1$ contributes to a larger variance of the outcome distribution. This essentially increases the number of required samples by a factor of C^2 compared to the case of conventional distillation where resource state ψ itself is available. Thus, the effective number of ψ virtually obtained as $\tilde{\Lambda}(\rho)$ is reduced by a factor of $1/C^2$ for the purpose of estimating the expectation value of an observable with the desired accuracy.

This observation motivates us to define the one-shot virtual resource distillation rate as

$$\mathfrak{D}^\varepsilon(\rho) = \max_m \frac{m}{\mathfrak{C}_d^\epsilon(\rho, m)^2}, \tag{3}$$

with the overhead $\mathfrak{C}_d^\epsilon(\rho, m)$ of virtual operations defined by

$$\mathfrak{C}_d^\epsilon(\rho, m) = \inf_{\substack{\tilde{\Lambda}=\lambda_+\Lambda_+-\lambda_-\Lambda_- \\ \lambda_+-\lambda_-=1 \\ \Lambda_\pm\in\mathcal{O},\lambda_\pm\geq 0}} \left\{\lambda_+ + \lambda_- : \frac{1}{2}\left\|\tilde{\Lambda}(\rho) - \psi^{\otimes m}\right\|_1 \leq \varepsilon\right\}. \tag{4}$$

The virtual distillation rate $\mathfrak{D}^\varepsilon$ can be considered as a generalization of the conventional distillation rate D^ε, which would be recovered by restricting the optimization in (4) to the case of $\lambda_- = 0$. This immediately implies that the one-shot distillation rate satisfies $D^\varepsilon(\rho) \leq \mathfrak{D}^\varepsilon(\rho)$. In fact, we show shortly that the virtual distillation rate can be non-zero even when $D^\varepsilon(\rho) = 0$. It is also easy to verify that both the virtual distillation rate $\mathfrak{D}^\varepsilon(\rho)$ and the inverse overhead $1/\mathfrak{C}_d^\epsilon(\rho, m)$ are resource monotones. Since $\mathfrak{D}^\varepsilon(\rho)$ is fully determined by $\mathfrak{C}_d^\epsilon(\rho, m)$, we focus on the estimation of $\mathfrak{C}_d^\epsilon(\rho, m)$ in the following.

Estimation of $\mathfrak{C}_d^\epsilon(\rho, m)$.— We introduce upper and lower bounds on $\mathfrak{C}_d^\epsilon(\rho, m)$ in general quantum state resource theories. The bounds rely on two ingredients. First, we introduce two related optimization problems,

$\zeta^s_\epsilon(\rho,k)$ and $\zeta^g_\epsilon(\rho,k)$, which we will show to satisfy an extremely powerful property: in very general classes of quantum resources, the resource overhead $\mathfrak{C}^\epsilon_d(\rho,m)$ can be both upper and lower bounded using $\zeta^s_\epsilon(\rho,k)$ or $\zeta^g_\epsilon(\rho,k)$ with different choices of parameter k, giving the problems $\zeta^{s/g}_\epsilon$ an explicit operational application. Importantly, both ζ^s_ϵ and ζ^g_ϵ are convex optimization problems, and in many relevant resource theories (e.g. coherence, magic states, or non-PPT entanglement), they are efficiently computable as semidefinite programs (SDP).

The second ingredient that our bounds rely on are three different resource measures for the target pure resource state ψ — the generalised robustness [10] $R^g_{\mathcal{F}}(\rho)$, the standard robustness $R^s_{\mathcal{F}}(\rho)$ [10], and the resource fidelity $F_{\mathcal{F}}(\rho) \coloneqq \max_{\sigma\in\mathcal{F}} \left(\mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}\right)^2$. Our first result is then as follows.

Result 1. *Let ψ denote the optimal resource and $\mathcal{O}$ be the class of RNG operations. When $F_{\mathcal{F}}(\psi^{\otimes m})^{-1} = R^{s/g}_{\mathcal{F}}(\psi^{\otimes m}) + 1$ the overhead $\mathfrak{C}^\epsilon_d(\rho,m)$ of virtual distillation is $\mathfrak{C}^\epsilon_d(\rho,m) = \zeta^{s/g}_\epsilon\left(\rho, F_{\mathcal{F}}(\psi^{\otimes m})^{-1}\right)$.*

We stress that the above result applies to many important resource theories of interest, e.g. when the target ψ is a maximally entangled state in entanglement theory, or a maximally coherent state in the theory of coherence. Recall that the problems $\zeta^{s/g}_\epsilon$ are often efficiently computable, allowing for an exact evaluation of $\mathfrak{C}^\epsilon_d$ in relevant cases. Next, we show that the cost is not only computable numerically, but in fact an exact expression for it can be obtained in terms of a resource monotone $f_{\mathcal{O}}(\rho,m)$ that measures the maximum overlap between $\Lambda(\rho)$ and $\psi^{\otimes m}$ as $f_{\mathcal{O}}(\rho,m) \coloneqq \max_{\Lambda\in\mathcal{O}} \mathrm{Tr}[\Lambda(\rho)\psi^{\otimes m}]$. This will be possible whenever there exists a free "generalized twirling" operation [11] $\mathcal{T} \in \mathcal{O}$ of the form $\mathcal{T}(\rho) = \mathrm{Tr}[\psi^{\otimes m}\rho]\,\psi^{\otimes m} + \mathrm{Tr}[(I-\psi^{\otimes m})\rho]\,\sigma^\star$ for some $\sigma^\star \in \mathcal{F}$ with $\mathrm{Tr}[\psi\sigma^\star] = 0$, which is true for many resource theories of practical interest, such as entanglement and magic theory for specific target states.

Result 2. *Suppose a free generalized twirling operation exists. Then $\mathfrak{C}^\epsilon_d(\rho,m) = \max\left\{\frac{2(1-\epsilon)}{f_{\mathcal{O}}(\rho,m)} - 1, 1\right\}$.*

Importantly, Ref. [11] showed that the existence of a twirling operation is guaranteed whenever $F_{\mathcal{F}}(\psi^{\otimes m})^{-1} = 1 + R^s_{\mathcal{F}}(\psi^{\otimes m})$ for RNG operations, which gives a condition for equality which is easy to verify.

We thus give an alternative characterization of $\mathfrak{C}^\epsilon_d(\rho,m)$ via the resource monotone $f_{\mathcal{O}}(\rho,m)$. We note that while Result 1 can provide an exact characterization of the virtual distillation overhead without the need for an explicit optimization over the allowed free operations, Result 2 is applicable also for general free operations that are weaker than RNGs. Therefore, these results can be applicable to complementary scenarios.

Surpassing conventional limitations Distillation in the conventional sense is constrained by many no-go theorems that restrict what transformations can be achieved in certain regimes. A clear-cut way to understand the advantages of virtual distillation is to observe how it can overcome such limitations.

Consider, for instance, zero-error distillation ($\epsilon = 0$). In such a case, conventional distillation schemes are significantly limited: they cannot, for example, distill *any* pure states from states which are highly mixed (full- or almost full-rank, depending on the theory) [2, 3, 12], not even when many copies of input states are available, and not even probabilistically [2, 13]. Virtual distillation suffers from no such no-go limitation: even full-rank states allow for distillation with a finite overhead cost.

An even stronger limitation constrains the one-shot distillation from isotropic states ρ_p in theories such as quantum entanglement or coherence. Here, no free operation can improve the fidelity of ρ_p with a maximally resourceful state, making distillation impossible from a single copy of ρ_p for all small values of ϵ [14, 15]; virtual distillation allows one to surpass such restrictions.

In the technical manuscript [4], we also discuss applications of virtual resource distillation in coherence, entanglement, and magic.

Conclusions In this work, we introduce virtual resource distillation, an extended framework of resource distillation that takes integrates classical linear posspprocessing into free operations. We derive computable convex or semi-definite programming for the cost and show it is linearly related to the inverse of a resource monotone. We consider examples of coherence, entanglement, and magic, and calculate the virtual distillation rate for examples resource states. The results are applicable for many scenarios, such as quantum teleportation using noisy entangled state, fault-tolerant quantum computing using noisy magic states, etc. While this work only consider specific example optimal resource states, the results are also applicable to any pure resource states. The results are also applicable to other resource theories, such as uniformity and thermodynamics [16]. We also study virtual distillation of quantum channels, applicable to resource theories such as the theory of quantum communication.

References

[1] Zi-Wen Liu, Kaifeng Bu, and Ryuji Takagi. One-shot operational quantum resource theory. *Phys. Rev. Lett.*, 123:020401, Jul 2019.

[2] Kun Fang and Zi-Wen Liu. No-go theorems for quantum resource purification. *Phys. Rev. Lett.*, 125:060405, Aug 2020.

[3] Bartosz Regula and Ryuji Takagi. Fundamental limitations on distillation of quantum channel resources. *Nat. Commun.*, 12:4411, 2021.

[4] X. Yuan, R. Takagi, B. Regula, , and M. Gu. Virtual quantum resource distillation. *arXiv preprint arXiv:2303.00955*, 2023.

[5] Yongdan Yang, Bing-Nan Lu, and Ying Li. Accelerated quantum Monte Carlo with mitigated error on noisy quantum computer. *PRX Quantum*, 2:040361, Dec 2021.

[6] Tianyi Peng, Aram W. Harrow, Maris Ozols, and Xiaodi Wu. Simulating large quantum circuits on a small quantum computer. *Phys. Rev. Lett.*, 125:150504, Oct 2020.

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

[8] Suguru Endo, Zhenyu Cai, Simon C. Benjamin, and Xiao Yuan. Hybrid quantum-classical algorithms and quantum error mitigation. *J. Phys. Soc. Jpn.*, 90(3):032001, 2021.

[9] Kristan Temme, Sergey Bravyi, and Jay M. Gambetta. Error mitigation for short-depth quantum circuits. *Phys. Rev. Lett.*, 119:180509, Nov 2017.

[10] Guifré Vidal and Rolf Tarrach. Robustness of entanglement. *Phys. Rev. A*, 59(1):141, 1999.

[11] Ryuji Takagi, Bartosz Regula, and Mark M. Wilde. One-shot yield-cost relations in general quantum resource theories. *PRX Quantum*, 3:010348, Mar 2022.

[12] Kun Fang and Zi-Wen Liu. No-go theorems for quantum resource purification: New approach and channel theory. *PRX Quantum*, 3:010337, Mar 2022.

[13] Bartosz Regula. Probabilistic Transformations of Quantum Resources. *Phys. Rev. Lett.*, 128:110505, 2022.

[14] Adrian Kent. Entangled Mixed States and Local Purification. *Phys. Rev. Lett.*, 81:2839–2841, 1998.

[15] Bartosz Regula. Tight constraints on probabilistic convertibility of quantum states. *Quantum*, 6:817, September 2022.

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

Unitary channel discrimination beyond group structures: Advantages of sequential and indefinite-causal-order strategies

Jessica Bavaresco[1] * Mio Murao[2] Marco Túlio Quintino[3]

[1]*Deparment of Applied Physics, University of Geneva, 1205 Geneva, Switzerland*
[2]*Department of Physics, Graduate School of Science, The University of Tokyo, Tokyo 113-0033, Japan*
[3]*Sorbonne Université, CNRS, LIP6, F-75005 Paris, France*

Abstract. For minimum-error channel discrimination tasks that involve only unitary channels, we show that sequential strategies may outperform parallel ones. Additionally, we show that general strategies that involve indefinite causal order are also advantageous for this task. However, for the task of discriminating a uniformly distributed set of unitary channels that forms a group, we show that parallel strategies are indeed optimal, even when compared to general strategies. We also show that strategies based on the quantum switch cannot outperform sequential strategies in the discrimination of unitary channels. Finally, we derive an absolute upper bound for the maximal probability of successfully discriminating any set of unitary channels with any number of copies, for the most general strategies that are suitable for channel discrimination. Our bound is tight since it is saturated by sets of unitary channels forming a group k-design.

Based on (the technical version follows the extended abstract):
J. Math. Phys. 63, 042203 (2022), arXiv:2105.13369 [quant-ph] and
Phys. Rev. Lett. 127, 200504 (2021), arXiv:2011.08300 [quant-ph].

Keywords: Channel discrimination, unitary discrimination, higher-order operations, indefinite causal order, computer assisted proofs

The discrimination of different hypothesis is a fundamental part of the scientific method that finds application in the most distinct areas, such as information theory [1], bioinformatics [2], machine learning [3], and behavioral and social sciences [4]. In a discrimination task, one seeks for the best manner to decide whether a particular hypothesis is the most likely to be the best description of some scenario or experiment. An important, albeit general, instance of a discrimination task consists in identifying between different input-output relations, or different causal-effect dynamics a physical system may undergo.

In its most fundamental level, closed-system dynamics in quantum theory are described by unitary operations. Hence, being able to discriminate between different unitary operations is a ubiquitous task within quantum theory and quantum technologies. Examples of tasks directly related to our ability to discriminate unitary operations are quantum metrology [5, 6], quantum hypothesis testing [7], quantum parameter estimation [8], alignment and transmission of reference frames [9, 10], and discrimination and tomography of quantum circuit elements [11].

Discrimination tasks are also relevant to the field of computer science. An oracle, which is an abstract machine used to study decision problems, may be understood as a black box that solves certain problems with a single operation. From a quantum computational perspective, a quantum oracle is a unitary operation whose internal mechanisms are unknown, and are employed in seminal quantum algorithms such as the Deustch-Josza algorithm [12], Grover's algorithm [13], and Simon's algorithm [14]. These oracle-based quantum algorithms may be recast as unitary discrimination tasks [15].

Such practical and fundamental interest has motivated an extensive study of the discrimination of unitary channels within the context of quantum information theory, leading to a plethora of interesting results.

Contrarily to the problem of quantum state discrimination [16], in which two states cannot be perfectly distinguished with a finite number of uses, or copies, unless their are orthogonal, it has been remarkably shown that any pair of unitary channels can indeed always be perfectly distinguished with a finite number of copies [17, 18]. Moreover, perfect discrimination of a pair of unitary channels can always be achieved by a parallel scheme [17, 18] (see also Ref. [19]). Even when perfect discrimination is not possible, sequential strategies can never outperform parallel strategies in a task of discrimination between a pair of unitary channels [20]. Concerning the discrimination of sets of more than two unitary channels, when considering unitaries which are a representation of a group and uniformly distributed, Ref. [20] showed once more that, for any number of copies, sequential strategies are not advantageous when compared to parallel strategies. For related tasks such as error-free and unambiguous unitary channel discrimination [21], unitary estimation [20], unitary learning [22], and unitary store-and-retrieve [23], parallel strategies were also proven to be optimal. Up to this point, no unitary channel minimum-error discrimination task in which sequential strategies outperform parallel strategies are known, to the extent of our knowledge.

In this work, we start by constructing a unified framework for channel discrimination, for both unitary and also general channels, that encompasses discrimination tasks between any number of candidate channels and that allow for the use of any number of copies. We formalized under a single umbrella the well-known parallel (i.e. non adaptive) and sequential (i.e. adaptive) strategies of

*jessica.bavaresco@unige.ch

discrimination, as well as a new general class of strategies that involve indefinite causal order.

FRAMEWORK

The task of minimum-error channel discrimination works as follows: With some probability p_i, Alice is given an unknown quantum channel $\widetilde{C}_i : \mathcal{L}(\mathcal{H}^I) \to \mathcal{L}(\mathcal{H}^O)$, drawn from an ensemble $\mathcal{E} = \{p_j, \widetilde{C}_j\}_{j=1}^N$ that is known to her. Being allowed to use a finite number of copies of $\widetilde{C}_i$, her task is to determine which channel she received by performing operations on it and guessing the value of $i \in \{1, \ldots, N\}$. If Alice is allowed to use one copy of the channel she received, the most general quantum operations she could apply are to send part of a potentially entangled state $\rho \in \mathcal{L}(\mathcal{H}^I \otimes \mathcal{H}^{\text{aux}})$ through the channel $\widetilde{C}_i$, and jointly measure the output with a positive operator-valued measure (POVM) $M = \{M_a\}, M_a \in \mathcal{L}(\mathcal{H}^O \otimes \mathcal{H}^{\text{aux}})$, announcing the outcome of her measurement as her guess. Then, her probability of correctly guessing the value i is given by $p_{\text{succ}} \coloneqq \sum_{i=1}^N p_i \text{Tr}\left[(\widetilde{C}_i \otimes \widetilde{\mathbb{1}})(\rho)\, M_i\right]$, where $\widetilde{\mathbb{1}}$ is the identity map on $\mathcal{L}(\mathcal{H}^{\text{aux}})$. Alice can improve her chances by optimizing her operations based on her knowledge of the ensemble. Her maximal probability of success is then given by $p^*_{\text{succ}} \coloneqq \max_{\{\rho,M\}} p_{\text{succ}}$, where the optimization occurs over all possible strategies $\{\rho, M\}$.

Now if Alice is given access to two or more copies of the unknown channel C_i, things become more interesting, since now she has the freedom of choosing how to concatenate these copies of the channel in order to gain more information about them. The manner, and in particular, the order with which she applies these channels give rise to different classes of strategies.

Parallel strategies are the ones that consist of sending each system that composes a multipartite state through one of the copies of the unknown channel, in such a way that the output of each copy does not interact with the input of the others, and jointly measuring the output state at the end (see Fig. 1(a)).

Sequential strategies consist of sending a quantum systems through the first copy of the unknown channel, and its output system is allowed to be sent as input of the next copy, while general CPTP maps may act on the systems in between copies. The final output is measured by a POVM (see Fig. 1(b)).

General strategies, on the other hand, are strategies that are defined without imposing any particular order under which the copies of the unknown channel will be applied. They are defined by the most general higher-order operations that can transform k quantum channels into a joint probability distribution. They can be regarded as the most general 'measurement' that acts jointly on k quantum channels, yielding a classical output . By characterising such class of strategies we find out that, indeed, some valid general strategies act on the copies of the unknown channel with an *indefinite causal order* [24] (see Fig. 1(c)).

We characterise all of these strategies in terms of *testers*, which are sets of positive-semidefinite operators that satisfy some linear constraints that specify the class of strategies to which they belong.

RESULTS

Most results in the literature of unitary channel discrimination focus on tasks that either involve discriminating between a pair of unitaries, or between a set of unitaries that form the unitary representation of a group. Until this point, not a single example of a unitary discrimination task for which parallel strategies were not optimal was known. In our work, we first show that when the set of unitary channels being discriminated forms a group and is distributed according to a uniform probability distribution, then indeed parallel strategies are optimal, even when comparing against general strategies that employ indefinite causal order. However, when considering sets of more than two unitaries that either do not form a group or are not distributed according to a uniform probability distribution, we show that sequential strategies may in fact outperform parallel strategies, just as general strategies may outperform sequential ones, forming a strict hierarchy of discrimination strategies. We then show that a class of indefinite-causal-order strategies that are constructed from switch-like processes do not provide advantage over sequential strategies for any set of unitary channels. Finally, we provide an absolute upper bound for the maximal probability of successful discrimination of any sets of unitary channels under any strategies and show that our bound can be saturated.

In summary, our main results consist of the following:

Result 1. For ensembles composed of a uniform probability distribution and a set of unitary channels that forms a group up to a global phase, in discrimination tasks that allow for k copies, parallel strategies are optimal, even when considering general strategies.

Result 2. There exist ensembles of unitary channels for which sequential strategies of discrimination outperform parallel strategies. Moreover, sequential strategies can achieve perfect discrimination in some scenarios where the maximal probability of success of parallel strategies is strictly less than one.

Result 3. There exist ensembles of unitary channels for which general strategies of discrimination outperform sequential strategies.

Result 4. The action of the switch-like process on k copies of a unitary channel can be equivalently described by a sequential process that acts on k copies of the same unitary channel.

Result 5. Let $\mathcal{E} = \{p_i, U_i\}_{i=1}^N$ be an ensemble composed of N d-dimensional unitary channels and a uniform probability distribution. The maximal probability of successful discrimination of a general strategy with k copies is upper

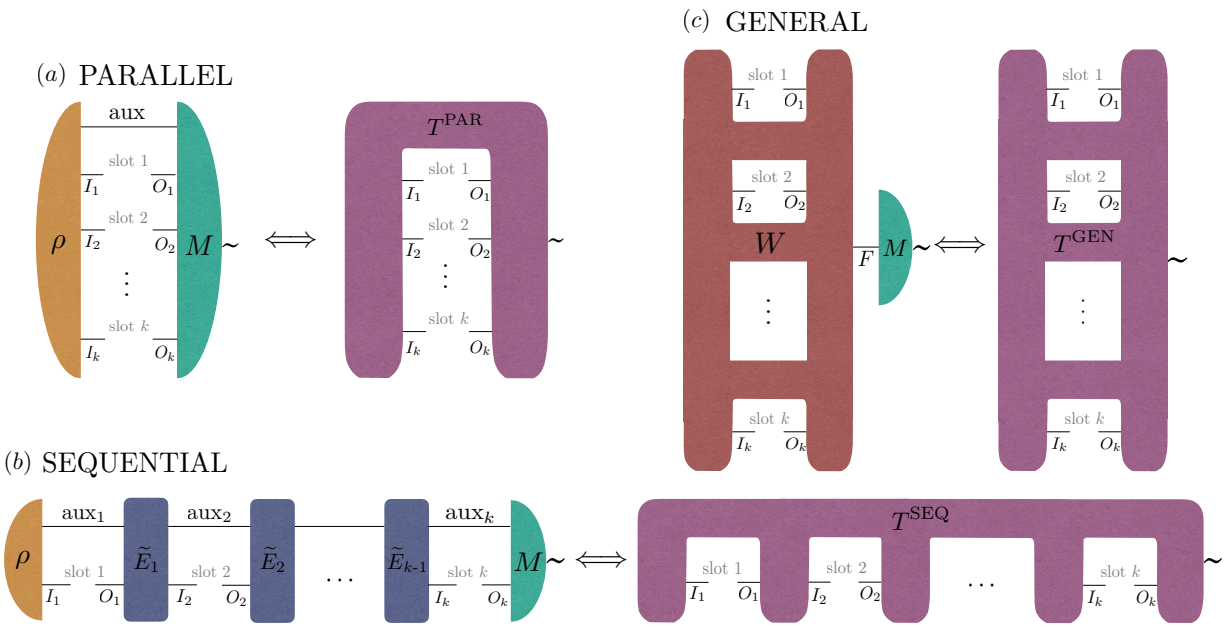


Figure 1: Schematic representation of the realization of every k-copy (a) parallel tester T^{PAR} with a state ρ and a POVM M, (b) sequential tester T^{SEQ} with a state ρ, channels $\widetilde{E}_i$, $i \in \{1, k-1\}$, and a POVM M, and (c) general tester T^{GEN} with a process matrix W and a POVM M.

bounded by

$$P^{\mathrm{GEN}} \leq \frac{1}{N} \frac{(k+d^2-1)!}{k!(d^2-1)!}, \tag{1}$$

This bound is attained by ensembles of unitary channels where the set of unitaries form a group k-design, and as a consequence of Result 1, can be optimally discriminated by parallel strategies.

METHODS

We remark that to prove some of out results that involve showing the gap between the performance of different classes of strategies for a fixed ensemble of channels, we developed and applied a method of *computer-assisted proofs*.

In our framework, the problem of computing the maximal probability of successful discrimination of a given channel ensemble under any of our classes of strategies, as we show, can be solved through semidefinite programming (SDP). SDPs can be solved by efficient numerical packages, however, despite being in practice accurate, these methods suffer from imprecision that arises from the use of floating-point variables [25, 26]. In order to overcome this issue, we developed and applied an algorithm of computer-assisted proofs (see [27, 28] for other examples) to obtain rigorous upper and lower bounds for maximal probabilities of successful discrimination, arriving at a result that has the same mathematical rigour of an analytical proof. Our algorithms are described in Ref. [29], while our results for unitary channels are in Ref. [30]. All our code is available at the repositories in Refs [31] and [32].

References

[1] R. Blahut. Hypothesis testing and information theory. *IEEE Transac. on Inf. Theory*, **20**, 405-417, (1974).

[2] Sergei L. Kosakovsky Pond, Simon D. W. Frost, and Spencer V. Muse. HyPhy: Hypothesis testing using phylogenies. *Bioinformatics*, **21**, 676-679, (2004).

[3] Judea Pearl. Probabilistic reasoning in intelligent systems: networks of plausible inference, (Elsevier, 2014).

[4] Raymond S Nickerson. Null hypothesis significance testing: a review of an old and continuing controversy. *Psych. Methods*, **5**, 241, (2000).

[5] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum Metrology. *Phys. Rev. Lett.*, **96**, 010401, (2006). [arXiv: quant-ph/0509179].

[6] Luca Pezzè, Augusto Smerzi, Markus K. Oberthaler, Roman Schmied, and Philipp Treutlein. Quantum metrology with nonclassical states of atomic ensembles. *Rev. of Modern Phys.*, **90**, 035005, (2018). [arXiv: 1609.01609].

[7] Masahito Hayashi. Quantum hypothesis testing and discrimination of quantum states. *Springer Berlin Heidelberg*, 69–91, (2006).

[8] Matteo GA Paris. Quantum estimation for quantum technology. *Int. J. Quantum Inf.*, **7**, 125–137, (2009). [arXiv: 0804.2981].

[9] G. Chiribella, G. M. D'Ariano, P. Perinotti, and M. F. Sacchi. Efficient Use of Quantum Resources for the

Transmission of a Reference Frame. *Phys. Rev. Lett.*, **93**, 180503, (2004). [arXiv: quant-ph/0405095].

[10] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. Reference frames, superselection rules, and quantum information. *Rev. of Modern Phys.*, **79**, 555-609, (2007). [arXiv: quant-ph/0610030].

[11] G. Chiribella, G. M. D'Ariano, and P. Perinotti. Quantum circuit architecture. *Phys. Rev. Lett.*, **101**, 060401, (2008). [arXiv: 0712.1325].

[12] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proc. of the Royal Society of London: Math. and Phys. Sciences*, **439**, 553–558, (1992).

[13] Lov K Grover. A framework for fast quantum mechanical algorithms. *Proc. of STOC*, 53–62, (1998). [arXiv: quant-ph/9711043].

[14] D. R. Simon. On the power of quantum computation. *Proc. of Symp. on Found. of Comp. Science*, 116–123, (1994).

[15] Anthony Chefles, Akira Kitagawa, Masahiro Takeoka, Masahide Sasaki, and Jason Twamley. Unambiguous discrimination among oracle operators. *J. Phys. A: Math. General*, **40**, 10183-10213, (2007). [arXiv: quant-ph/0702245].

[16] Carl W. Helstrom. Quantum detection and estimation theory. *J. Stat. Phys.*, **1**, 231–252, (1969).

[17] A. Acín. Statistical distinguishability between unitary operations. *Phys. Rev. Lett.*, **87**, 177901, (2001). [arXiv: quant-ph/0102064].

[18] G. Mauro D'Ariano, Paoloplacido Lo Presti, and Matteo G. A. Paris. Using entanglement improves the precision of quantum measurements. *Phys. Rev. Lett.*, **87**, 270404, (2001). [arXiv: quant-ph/0109040].

[19] Runyao Duan, Yuan Feng, and Mingsheng Ying. Entanglement is not necessary for perfect discrimination between unitary operations. *Phys. Rev. Lett.*, **98**, 100503, (2007). [arXiv: quant-ph/0601150].

[20] Giulio Chiribella, Giacomo M. D'Ariano, and Paolo Perinotti. Memory effects in quantum channel discrimination. *Phys. Rev. Lett.*, **101**, 180501, (2008). [arXiv: 0803.3237].

[21] Giulio Chiribella, Giacomo Mauro D'Ariano, and Martin Roetteler. Identification of a reversible quantum gate: assessing the resources. *New J. Phys.*, **15**, 103019, (2013). [arXiv: 1306.0719].

[22] Alessandro Bisio, Giulio Chiribella, Giacomo Mauro D'Ariano, Stefano Facchini, and Paolo Perinotti. Optimal quantum learning of a unitary transformation. *Phys. Rev. A*, **81**, 032324, (2010). [arXiv: 0903.0543].

[23] Michal Sedlák, Alessandro Bisio, and Mário Ziman. Optimal Probabilistic Storage and Retrieval of Unitary Channels. *Phys. Rev. Lett.*, **122**, 170502, (2019). [arXiv: 1809.04552].

[24] O. Oreshkov, F. Costa, and Č. Brukner. Quantum correlations with no causal order. *Nat. Commun.*, **3**, 1092, (2012). [arXiv: 1105.4464].

[25] https://floating-point-gui.de.

[26] Floating-point arithmetic: Wikipedia.

[27] Helfried Peyrl and Pablo A. Parrilo. Computing sum of squares decompositions with rational coefficients. *Theoretical Computer Science*, **409**, 269-281, (2008).

[28] Siegfried M. Rump. Verification methods: Rigorous results using floating-point arithmetic. *Acta Numerica*, **19**, 287–449, (2010).

[29] Jessica Bavaresco, Mio Murao, and Marco Túlio Quintino. Strict hierarchy between parallel, sequential, and indefinite-causal-order strategies for channel discrimination. *Accepted at Phys. Rev. Letters*, (2021). [arXiv: 2011.08300].

[30] Jessica Bavaresco, Mio Murao, and Marco Túlio Quintino. Unitary channel discrimination beyond group structures: Advantages of sequential and indefinite-causal-order strategies. (2021). [arXiv: 2105.13369].

[31] https://github.com/mtcq/channel_discrimination.

[32] https://github.com/mtcq/unitary_channel_discrimination.

Unbiased Random Circuit Compiler for Time-Dependent Hamiltonian Simulation

Xiao-Ming Zhang[1] Zixuan Huo[1] Kecheng Liu[1] Zixuan Huo[1] Ying Li[3]
Xiao Yuan[1] *

[1] *Center on Frontiers of Computing Studies, Department of Computer Science, Peking University, Beijing, China*
[3] *Graduate School of China Academy of Engineering Physics, Beijing 100193, China*

Abstract. We develop a time-dependent Hamiltonian simulation algorithm with circuit depth independent of the algorithmic error. Compared to the continuous-qDRIFT method, the single- and two-qubit gate complexity is reduced from $O(\Lambda^2/\varepsilon)$ to $O(\Lambda^2)$, where Λ is the time integration of the Hamiltonian strength and ε is the algorithmic error. The number of measurement repetition, $O(1/\varepsilon^2)$ is comparable to existing methods.

Keywords: Time-dependent Hamiltonian simulation, qDRIFT, Dyson expansion

1 Background and introduction

Time-dependent Hamiltonian simulation (TDHS) can be used to explore rich physics phenomena, ranging from adiabatic quantum evolution [1] to driven systems under highly-oscillated external driving fields [18] and chemical reactions [7, 21]. Moreover, time-independent Hamiltonians can be transformed to a time-dependent one in the interaction picture, providing significant improvements to the performance of Hamiltonian simulation [16].

All existing TDHS algorithms are approximate and hence biased. We have to increase the circuit depth to reduce the algorithmic error ε. For example, based on product formula [2, 7, 14, 19, 24, 25], the gate count scales as $O(\mathrm{poly}(1/\varepsilon))$, restricting the precision that can be achieved when the circuit depth is limited. The complexity can be improved to be polylogarithmic with algorithms beyond the product formula framework [3, 5–7, 9, 15–17, 20, 23]. But these methods require ancillary qubits and oracles based on multi-qubit entangling gates, so their implementations are actually more challenging for intermediate-scale problems and near-term quantum devices, as shown in Ref. [10].

We propose an unbiased random circuit compiler (URCC) for general time-dependent Hamiltonian simulation. The accuracy can be arbitrarily small by just increasing the number of measurements. For each run of the quantum circuit, the single- and two-qubit gate count of our method is $O(\Lambda^2)$, where Λ is the time integration of total Hamiltonian strength. In particular, the gate count is independent of the accuracy and number of terms in the Hamiltonian. As a comparison, the continuous qDRIFT method [7] (the generalization of qDRIFT [8] to time-dependent cases) has gate count $O(\Lambda^2/\varepsilon)$, while measurement repetition $O(1/\varepsilon^2)$ is comparable to our method . Moreover, our method is compatible with simultaneous measurement techniques, such as classical shadow [13] and group measurement [22].

Algorithm overview.— Given a time-dependent Hamiltonian $H(t)$ and quantum state $|\psi_0\rangle$, the quantum state after time $\tau > 0$ is $|\psi_\tau\rangle = U(0,\tau)|\psi_0\rangle$, where $U(0,\tau) = \mathcal{T}\exp\left[-i\int_0^\tau dt H(t)\right]$. Here, $\mathcal{T}$ is the time-ordering operator. We care about the expectation value of observable $\hat{O}$, i.e. $\langle O\rangle = \mathrm{tr}\left(\hat{O}U(0,\tau)|\psi_0\rangle\langle\psi_0|U(0,\tau)^\dagger\right)$. Our algorithm outputs an unbiased estimator for $\langle O\rangle$ by the combination of three different techniques: Dyson expansion of time-dependent evolution [11], classical unbiased continuous sampling of the linear combination of unitaries [12], and leading order rotation [26]. The main difference from existing Dyson expansion based algorithms [7, 9, 15, 16] is that we are performing classical sampling according to the *exact* Dyson expansion without truncation, which is the origin of the *unbiased* property of our method. Although there are infinite number of terms in the expansion, such sampling can be realized efficiently by a poisson distribution and a continuous sampling techniques (see Algorithm 1,2 in the technical version).

An overview of our algorithm is provided in Fig. 1(a). Based on the Dyson expansion to infinite orders, we first rewrite the evolution as the linear combination of Pauli strings (LCPS). Then, we develop an unbiased and efficient circuit sampling algorithm according to the LCPS. The variance of such LCPS-based sampling is, however, exponential with respect to the time integral of Hamiltonian strength. We then apply the leading order rotation technique, which combines the zero and the first order of the Dyson expansion into a rotation operator with $O(n)$ circuit depth. This reduces the variance of unbiased sampling from exponential to polynomial.

The process above works for evolution with small τ. For large τ, we divide the total evolution into N_{seg} segments. Let $\Lambda = \int_0^\tau h_{\mathrm{tot}}(t)dt$, to control the total variance to a constant value, it suffice to set $N_{\mathrm{seg}} = O(\Lambda^2)$. Therefore, the total single- and two-qubit gate count of our algorithm is $O(\Lambda^2 n)$ for n qubit systems, which is independent of ε. If we further assume that the Hamiltonian is k-local, the gate count becomes $N_{\mathrm{gate}} = O(\Lambda^2 k)$.

Numerical examples.— We provide two numerical examples and compare the performance to c-qDRIFT.

*xiaoyuan@pku.edu.cn

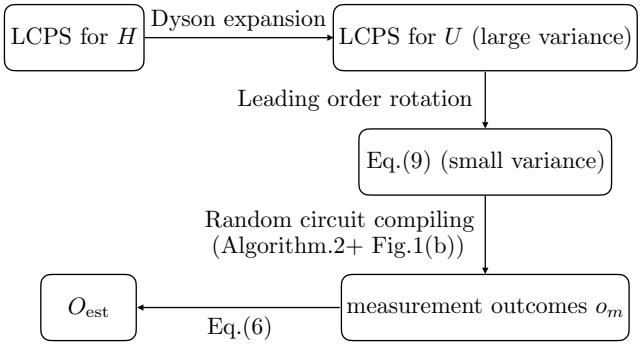


Figure 1: (a) Overview of the URCC algorithm for short-time evolution. See technical version for details.

The first example is the many-body spin model under interaction picture. The effective Hamiltonian has the form $\tilde{H}(t) = J/2\,(\cos(2\omega t)G_1 + \sin(2\omega t)G_2)$, where $G_1 = \sum_{k=1}^{n-1} \hat{X}_k\hat{X}_{k+1} + \hat{Y}_k\hat{Y}_{k+1}$ and $G_2 = \sum_{k=1}^{n-1}(-1)^k(\hat{X}_k\hat{Y}_{k+1} - \hat{Y}_k\hat{X}_{k+1})$. Fig. 2(a) shows the error versus M under fixed single- and two-qubit gate counts for both algorithms. The error of our method always reduces with increasing M. On the other hand, the error for c-qDRIFT converges to a fixed value. In particular, we observe > 10 times reduction of the error with $M > 10^7$. Fig. 2(c), shows the single- and two-qubit gate count ratio for c-qDRIFT to URCC method under different M. The gate count ratio is larger for larger M. With $M \propto 1/\varepsilon_{\text{tot}}^2$, the gate count ratios always increase with $1/\varepsilon_{\text{tot}}$. For fixed M, the gate count ratios also increase in general, but drop slightly when ε_{tot} is close to the sampling error, i.e. the minimal error that can be achieved.

Similar to qDRFIT, the gate count of the URCC method is independent of the number of terms in Hamiltonian. So it is suitable for models with large P, such as molecular systems. Here, we take the adiabatic ground state preparation for H_2 [4] as an example. The observable for energy is the Hamiltonian itself, which should be decomposed into Pauli strings. URCC is compatible with measurement techniques, and we take the grouping measurements as an example [22] to reduce the number of measurements. In Fig. 2(b), we demonstrate the total error versus M for c-qDRFIT and URCC methods. Fig. 2(d) demonstrates the single- and two-qubit gate count ratios. Similar to the spin model example, our method shows significant improvement.

Significance.— For the first time, we developed a quantum algorithm for time-dependent Hamiltonian simulation with gate count independent of simulation accuracy. Our algorithm is one of the most promising methods in the NISQ era, especially for many-body and molecular systems. First, arbitrary accuracy can be achieved only by increasing the sampling size, while keeping qubit and gate numbers unchanged. This is a significant advantage for NISQ hardware, where the qubit and gate numbers are limited. Second, the gate count is independent of the number of terms in the Hamiltonian, which

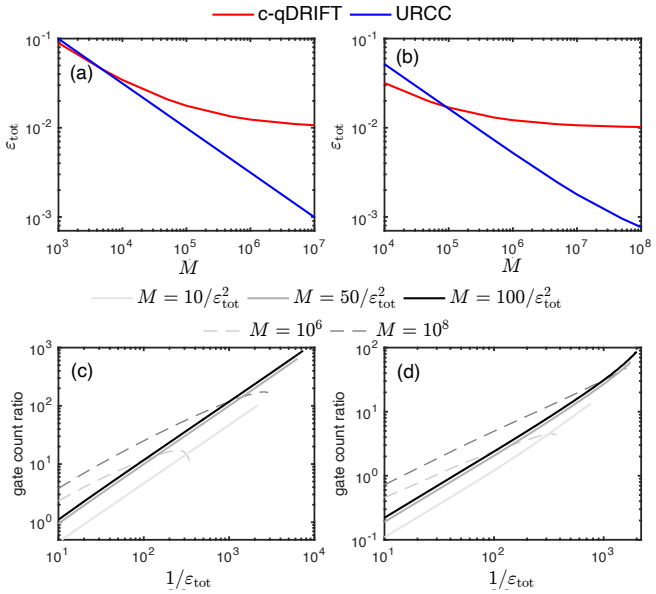


Figure 2: Numerical simulation results. (a) and (b): Error versus the number of measurements. (c) and (d): Single- and two-qubit gate count ratios for different M. (a) and (c) and correspond to the spin model in interaction picture. (b) and (d) correspond to the adiabatic ground state preparation for H_2.

is typically a large value for many-body and molecular systems.

References

[1] Tameem Albash and Daniel A Lidar. Adiabatic quantum computation. *Reviews of Modern Physics*, 90(1):015002, 2018.

[2] Dong An, Di Fang, and Lin Lin. Time-dependent unbounded hamiltonian simulation with vector norm scaling. *Quantum*, 5:459, 2021.

[3] Dong An, Di Fang, and Lin Lin. Time-dependent hamiltonian simulation of highly oscillatory dynamics and superconvergence for schrödinger equation. *Quantum*, 6:690, 2022.

[4] Alán Aspuru-Guzik, Anthony D Dutoi, Peter J Love, and Martin Head-Gordon. Simulated quantum computation of molecular energies. *Science*, 309(5741): 1704–1707, 2005.

[5] Dominic W Berry, Andrew M Childs, Richard Cleve, Robin Kothari, and Rolando D Somma. Exponential improvement in precision for simulating sparse hamiltonians. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 283–292, 2014.

[6] 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(9):090502, 2015.

[7] Dominic W Berry, Andrew M Childs, Yuan Su, Xin Wang, and Nathan Wiebe. Time-dependent hamiltonian simulation with l^1-norm scaling. *Quantum*, 4:254, 2020.

[8] Earl Campbell. Random compiler for fast hamiltonian simulation. *Phys. Rev. Lett.*, 123(7):070503, 2019.

[9] Yi-Hsiang Chen, Amir Kalev, and Itay Hen. Quantum algorithm for time-dependent hamiltonian simulation by permutation expansion. *PRX Quantum*, 2(3):030342, 2021.

[10] Andrew M Childs, Dmitri Maslov, Yunseong Nam, Neil J Ross, and Yuan Su. Toward the first quantum simulation with quantum speedup. *Proc. Natl. Acad. Sci.*, 115(38):9456–9461, 2018.

[11] Freeman J Dyson. The radiation theories of tomonaga, schwinger, and feynman. *Physical Review*, 75 (3):486, 1949.

[12] Paul K Faehrmann, Mark Steudtner, Richard Kueng, Mária Kieferová, and Jens Eisert. Randomizing multi-product formulas for hamiltonian simulation. *Quantum*, 6:806, 2022.

[13] Hsin-Yuan Huang. Learning quantum states from their classical shadows. *Nature Reviews Physics*, 4 (2):81–81, 2022.

[14] Jacky Huyghebaert and Hans De Raedt. Product formula methods for time-dependent schrodinger problems. *Journal of Physics A: Mathematical and General*, 23(24):5777, 1990.

[15] Mária Kieferová, Artur Scherer, and Dominic W Berry. Simulating the dynamics of time-dependent hamiltonians with a truncated dyson series. *Phys. Rev. A*, 99(4):042314, 2019.

[16] Guang Hao Low and Nathan Wiebe. Hamiltonian simulation in the interaction picture. *arXiv:1805.00675*, 2018.

[17] Kaoru Mizuta and Keisuke Fujii. Optimal time-periodic hamiltonian simulation with floquet-hilbert space. *arXiv:2209.05048*, 2022.

[18] Changsuk Noh and Dimitris G Angelakis. Quantum simulations and many-body physics with light. *Reports on Progress in Physics*, 80(1):016401, 2016.

[19] David Poulin, Angie Qarry, Rolando Somma, and Frank Verstraete. Quantum simulation of time-dependent hamiltonians and the convenient illusion of hilbert space. *Phys. Rev. Lett.*, 106(17):170501, 2011.

[20] Abhishek Rajput, Alessandro Roggero, and Nathan Wiebe. Hybridized methods for quantum simulation in the interaction picture. *Quantum*, 6:780, 2022.

[21] Markus Reiher, Nathan Wiebe, Krysta Marie Svore, Dave Wecker, and Matthias Troyer. Elucidating reaction mechanisms on quantum computers. *Proceedings of the National Academy of Sciences*, 114:7555 – 7560, 2016.

[22] Vladyslav Verteletskyi, Tzu-Ching Yen, and Artur F Izmaylov. Measurement optimization in the variational quantum eigensolver using a minimum clique cover. *The Journal of chemical physics*, 152(12): 124114, 2020.

[23] Jacob Watkins, Nathan Wiebe, Alessandro Roggero, and Dean Lee. Time-dependent hamiltonian simulation using discrete clock constructions. *arXiv:2203.11353*, 2022.

[24] Dave Wecker, Matthew B. Hastings, Nathan Wiebe, Bryan K. Clark, Chetan Nayak, and Matthias Troyer. Solving strongly correlated electron models on a quantum computer. *Phys. Rev. A*, 92:062318, Dec 2015.

[25] Nathan Wiebe, Dominic Berry, Peter Høyer, and Barry C Sanders. Higher order decompositions of ordered operator exponentials. *Journal of Physics A: Mathematical and Theoretical*, 43(6):065203, 2010.

[26] Yongdan Yang, Bing-Nan Lu, and Ying Li. Accelerated quantum monte carlo with mitigated error on noisy quantum computer. *PRX Quantum*, 2(4): 040361, 2021.

Quantum Phase Processing and its Applications in Estimating Phase and Entropies

Youle Wang[1] Lei Zhang[1] Zhan Yu[1] Xin Wang[1] *

[1] *Institute for Quantum Computing, Baidu Research, Beijing 100193, China*

Abstract. Quantum computing can provide speedups in solving many problems as the evolution of a quantum system is described by a unitary operator in an exponentially large Hilbert space. Such unitary operators change the phase of their eigenstates and make quantum algorithms fundamentally different from their classical counterparts. Based on this unique principle of quantum computing, we develop a new algorithmic toolbox "Quantum phase processing" that can directly apply arbitrary trigonometric transformations to eigenphases of a unitary operator. The quantum phase processing circuit is constructed simply, consisting of single-qubit rotations and controlled-unitaries, typically using only one ancilla qubit. Besides the capability of phase transformation, quantum phase processing in particular can extract the eigen-information of quantum systems by simply measuring the ancilla qubit, making it naturally compatible with indirect measurement. Quantum phase processing complements a powerful framework known as quantum singular value transformation and leads to more intuitive and efficient quantum algorithms for solving problems that are particularly phase-related. As a notable application, we propose a new quantum phase estimation algorithm without quantum Fourier transform, which requires the fewest ancilla qubits and matches the best performance so far. We further exploit the power of our method by investigating a plethora of applications in Hamiltonian simulation, entanglement spectroscopy and quantum entropies estimation, demonstrating improvements or optimality for almost all cases. Note that the technical version is attached.

Keywords: Quantum signal processing, quantum phase estimation, quantum entropies estimation

Introduction. Quantum computing has been applied in areas such as breaking cryptographic systems [1], searching databases [2], and simulating quantum systems [3]. Recent advances in quantum computing show that *quantum singular value transformation* (QSVT) [4] formalizes a unified framework of the most known quantum algorithms [5], leading to various applications [6–13]. The framework of QSVT was originated from a technique called *quantum signal processing* (QSP) [14, 15]. By interleaving single-qubit signal unitaries and signal processing unitaries, QSP is able to implement a transformation of the signal in $\mathrm{SU}(2)$.

There are several conventions of QSP varied by choosing different signal unitaries. In the construction of QSVT, Gilyén et al. [4] chose the signal unitary to be a reflection, then extended the signal unitary to a multi-qubit block encoding with the idea of qubitization [16], which naturally leads to a Chebyshev polynomial transformation on the singular values of a block-encoded linear operator. In recent work, Yu et al. [17] developed a new convention of QSP by choosing the signal unitary as a z-rotation and adding an extra signal processing unitary. Such a modified QSP could implement arbitrary complex trigonometric polynomials, which naturally corresponds to the phase transformation. The ability of processing phase plays a central role in many quantum algorithms. For example, *phase kickback*, where the phase of the target qubits is kicked back to the ancilla qubit, is intensively used almost everywhere in quantum computing. With the help of controlled-unitary operators, many quantum algorithms utilize phase kickback to extract information of large unitary operations from phases of ancilla qubits, also known as indirect measurements, such as the quantum phase estimation [18, 19], the swap test [20, 21], the Hadamard test [22], and the one-clean-qubit model [23]. Hence, it is of great interest and necessity to explore a generalized toolbox based on the trigonometric QSP that could interpret those phase-related quantum algorithms, which may further lead to improved performances or new quantum algorithms.

Overview of results. We develop an algorithmic toolbox "Quantum phase processing" and investigate its applications in quantum computing. In particular, we establish the following:

1. We leverage QPP to design an efficient quantum phase estimation that uses only one ancilla qubit and matches the best query complexity so far. QPP enables the algorithm to directly classify phases of a unitary and then locate the target phase by an intuitive idea of binary search, making it fundamentally different from the traditional phase estimation based on quantum Fourier transform.
2. We propose a generic QPP-based method of quantum entropies estimation that demonstrates improvements over previous works. In particular, the QPP-based quantum entropies estimation does not require the quantum amplitude estimation, signifi-

*wangxin73@baidu.com

cantly reducing the demand for quantum resources compared to the related algorithms using QSVT, which is more friendly to near-term quantum devices than previous methods.

3. We further showcase applications of QPP in Hamiltonian simulation. The method of Hamiltonian simulation matches the previously optimal query complexity.

Quantum phase processing. Our first contribution is to develop a generic toolbox of quantum phase processing for higher dimension systems, which generalizes the trigonometric QSP [17] to process a multi-qubit unitary U by replacing the signal unitary $R_z(x)$ with controlled-U and its inverse. The quantum phase processing circuit of the unitary U is defined as

$$V^L_{\omega,\boldsymbol{\theta},\boldsymbol{\phi}}(U) \coloneqq R_z^{(0)}(\omega)R_y^{(0)}(\theta_0)R_z^{(0)}(\phi_0)\left[\prod_{l=1}^{L/2}\begin{bmatrix}U^\dagger & 0\\ 0 & I\end{bmatrix}R_y^{(0)}(\theta_{2l-1})R_z^{(0)}(\phi_{2l-1})\begin{bmatrix}I & 0\\ 0 & U\end{bmatrix}R_y^{(0)}(\theta_{2l})R_z^{(0)}(\phi_{2l})\right], \quad (1)$$

where $R_y^{(0)}$ and $R_z^{(0)}$ are rotation gates applied on the first qubit. Then we could measure the first ancilla qubit and achieve an evolution of the input state upon post-selection of the measurement result being $|0\rangle$. The intuition lying behind the extension is that controlled-U and its inverse are naturally multi-qubit analogs of R_z gates, which was frequently used in previous works [10, 15, 16, 24].

Theorem 1 (Quantum phase evolution) *Given an n-qubit unitary $U = \sum_{j=0}^{2^n-1} e^{i\tau_j}|\chi_j\rangle\langle\chi_j|$ and an n-qubit state $|\psi\rangle = \sum_{j=0}^{2^n-1}\alpha_j|\chi_j\rangle$, for any trigonometric polynomial $F(x) = \sum_{j=-L}^{L} c_j e^{ijx}$ with $\|\boldsymbol{c}\|_1 \leq 1$, there exists a QPP $V(U)$ of $2L$ layers such that $(\langle 0|\otimes I^{\otimes n})\,V(U)\,|0,\psi\rangle = \sum_{j=0}^{2^n-1}\alpha_j F(\tau_j)\,|\chi_j\rangle$.*

The theorem shows that QPP can act in a similar manner to QSVT, but transforming eigenphases of a unitary rather than singular values of an embedded linear operator. Moreover, the achievable transformation of QPP is arbitrary complex trigonometric polynomial, which overcomes the parity constraint of Chebyshev polynomials in QSVT without using linear-combination-of-unitaries. Other than implementing the phase evolution, QPP is natively compatible with the indirect measurement, which could directly extract eigen-information of a unitary by measuring the single ancilla qubit.

Theorem 2 (Quantum phase evaluation) *Given an n-qubit unitary $U = \sum_{j=0}^{2^n-1} e^{i\tau_j}|\chi_j\rangle\langle\chi_j|$ and an n-qubit state ρ, for any real-valued trigonometric polynomial $F(x) = \sum_{j=-L}^{L} c_j e^{ijx}$ with $\|\boldsymbol{c}\|_1 \leq 1$, there exists a QPP $V(U)$ of L layers such that $\hat{\rho} = V(U)(|0\rangle\langle 0|\otimes\rho)V(U)^\dagger$ satisfies $\mathrm{tr}\left[(Z^{(0)}\otimes I)\cdot\hat{\rho}\right] = \sum_{j=0}^{2^n-1} p_j F(\tau_j)$, where $p_j = \langle\chi_j|\,\rho\,|\chi_j\rangle$ and $Z^{(0)}$ is a Pauli-Z observable acting on the first qubit.*

Such a useful feature enables QPP to process and extract the eigen-information without quantum amplitude estimation as used in QSVT, which significantly reduces the demand for quantum resources and hence is more friendly to near-term quantum devices. Next we will show that QPP is a powerful tool for designing efficient and intuitive quantum algorithms, including quantum phase estimation, Hamiltonian simulation, and quantum entropies estimation.

Quantum phase estimation. To show the power of QPP on solving phase-related problems, our second contribution is to propose a new quantum phase estimation algorithm without using quantum Fourier transform, which requires only one ancilla qubit and matches the best performance so far. The main idea is to find a trigonometric polynomial that approximates a step function, so that we could use QPP to locate the eigenphases by a binary search procedure. Specifically, given a unitary U and an eigenstate $|\chi\rangle$ with eigenvalue $e^{i\tau}$, for any $\Delta \in (0,\pi)$ and $\varepsilon \in (0,1)$, there exists a QPP $V(U)$ with $L = \mathcal{O}(\frac{1}{\Delta}\log\frac{1}{\varepsilon})$ layers such that $V(U)\,|0,\chi\rangle = \sqrt{1-\varepsilon}\,|0,\chi\rangle + \sqrt{\varepsilon}\,|1,\chi\rangle$ if $\tau \in [\Delta, \pi-\Delta)$, and $V(U)\,|0,\chi\rangle = \sqrt{\varepsilon}\,|0,\chi\rangle + \sqrt{1-\varepsilon}\,|1,\chi\rangle$ if $\tau \in (-\pi+\Delta, -\Delta]$. Measuring the ancilla qubit decides which subinterval the eigenphase τ belongs to with high probability. Next we apply a phase shift $e^{i\zeta}$ to U to move to the middle point of the designated subinterval, then $V(e^{i\zeta}U)$ determines the next subinterval. Repeating the binary search procedure shrinks the phase interval until QPP cannot decide next subintervals, i.e. $\tau \in [\zeta_l, \zeta_r]$ and $|\zeta_r - \zeta_l| \approx 2\Delta$. Then we apply QPP on $(e^{i\zeta}U)^d$ for some appropriate integer d so that the binary search procedure can continue to locate the amplified phase $d\tau \in [d\zeta_l, d\zeta_r]$. Repeating the entire procedure above gives an estimation of phase τ up to required precision. We establish the following result describing *the QPP-based quantum phase search algorithm*: Given a unitary U and an eigenstate $|\chi\rangle$ of U with eigenvalue $e^{i\tau}$, there exists an algorithm that uses one ancilla qubit and $\widetilde{\mathcal{O}}\left(\frac{1}{\delta}\log(\frac{1}{\varepsilon})\right)$ queries to controlled-U to obtain an

estimation of τ up to δ precision with probability at least $1-\varepsilon$.

Quantum entropies estimation. Our third contribution is to propose a generic method of QPP-based quantum entropies estimation that demonstrate improvements over previous works. Our method assumes access to a purification oracle U_ρ that prepares a purification of a quantum state ρ. Following [16], one can construct a qubitized block encoding $\hat{U}_\rho$ such that eigenvalues $\{p_j\}$ of ρ and eigenphases $\{\tau_j\}_j$ of $\hat{U}_\rho$ correlate as $p_j = \cos(\pm\tau_j)$ under an appropriate subspace. Note that quantum entropies of a quantum state ρ can be interpreted as the corresponding classical entropies of the eigenvalues of ρ. The main idea of our QPP-based method is to find polynomials that approximate the classical entropic functions, then quantum entropies can be naturally estimated via phase evaluation of $\hat{U}_\rho$ by Theorem 2. We present the general method of quantum entropies estimation as follows.

Theorem 3 *Suppose ρ and σ are n-qubit states. Given an oracle access to a qubitized block encoding $\hat{U}_\sigma$ of σ with m ancilla qubits, for any real-valued polynomial $f(x) = \sum_{k=0}^{L} c_j x^k$ with $\|\boldsymbol{c}\|_1 \leq 1$, there exists a QPP circuit $V(\hat{U}_\sigma)$ of L layers such that $\hat{\rho} = V(\hat{U}_\sigma)(|0^{\otimes(m+1)}\rangle\langle 0^{\otimes(m+1)}| \otimes \rho)V(\hat{U}_\sigma)^\dagger$ satisfies $\mathrm{tr}\left[(Z^{(0)} \otimes I)\cdot\hat{\rho}\right] = \mathrm{tr}(\rho f(\sigma))$, where $f(\sigma) \coloneqq \sum_{k=0}^{L} c_j \sigma^k$.*

Let $\gamma > 0$ be a lower bound of non-zero eigenvalues of ρ and σ, we select a polynomial $f(x)$ that approximates the function $\ln(x)$ on $[\gamma, 1]$ to estimate the von Neumann entropy $S(\rho)$ and the quantum relative entropy $D(\rho \parallel \sigma)$. For estimating the quantum α-Rényi entropy $S_\alpha(\rho)$ with $\alpha \in (0,1)\cup(1,+\infty)$, we select a polynomial $f(x)$ that approximates the function $x^{\alpha-1}$ on $[\gamma, 1]$. In this application of QPP on entropies estimation, we fully leverage its compatibility with the indirect measurement, which enable us to extract entropies by simply measuring the first ancilla qubit.

We here remark the advantages of our method. Compared with previous works that used QSVT and amplitude estimation to estimate von Neumann entropies [6, 25], the QPP method has a higher computational overhead but a shorter circuit depth and fewer ancilla qubits. For quantum α-Rényi entropies where α is an integer, QPP establishes an efficient algorithm for entanglement spectroscopy that significantly reduces the width of circuit compared to previous algorithms [26, 27], from $\Theta(n\alpha)$ to $4n+1$ without using qubit resets [28]. For a more general case that α is a non-integer, the QPP method improves the query complexity in [29], in which the authors applied the DQC1 model on QSVT.

Hamiltonian simulation. We then utilize QPP to solve the Hamiltonian simulation problem with access to the block encoding of a Hamiltonian, which matches the optimal query complexity. By the qubitization technique [16], one could construct a qubitized block encoding $\hat{U}_H$ such that eigenvalues of H and eigenphases of $\hat{U}_H$ correlate as $\lambda = \cos(\pm\tau_\lambda)$. Since the time-evolution operator e^{-iHt} can be decomposed as $e^{-i\lambda t}$, the main idea is applying QPP on $\hat{U}_H$ to transform eigenphases as $\tau_\lambda \mapsto e^{-i\lambda t}$. We select the trigonometric polynomial $F(x)$ to approximate the function $f(x) = e^{-i\cos(x)t}$ with desired precision. Then applying the trigonometric polynomial $F(x)$ on each eigenphase τ_λ approximates $f(\tau_\lambda) = e^{-i\cos(\tau_\lambda)t} = e^{-i\lambda t}$, which provides a precise approximation of the time-evolution operator e^{-iHt}. Since the method follows the same idea as in [16], the query complexity also matches the optimal result.

Comparison to related works. QPP generalizes the trigonometric QSP by extending the R_z rotation instead of the reflection in the Chebyshev-based QSP as QSVT did [4]. Due to the distinctions between trigonometric and Chebyshev-based QSP, our results show that QPP essentially complements the existing QSVT paradigm. To be specific, QPP implements arbitrary complex trigonometric polynomial, which overcomes the parity constraints in QSVT and thus exempts the use of linear-combination-of-unitaries in certain cases. Notably, QPP could work without amplitude estimation, which requires shorter circuits and less coherence time than QSVT, and hence might be more friendly to near-term quantum hardware. Further, QPP natively inherits the trick of phase kickback, making it suitable for designing phase-related quantum algorithms.

Concluding remarks. QPP is a powerful tool for unifying and designing quantum algorithms related to eigenphase transformation and processing, which complements the framework of QSVT. Moreover, QPP is naturally compatible with indirect measurements, which could extract desired eigen-information by measuring a single ancilla qubit. By implementing different trigonometric polynomials, we have applied QPP to solve various problems including phase estimation, quantum entropies estimation, and Hamiltonian simulation, which recover or improve prior best results. Overall, the QPP algorithmic toolbox provides a new perspective of understanding and designing phase-related quantum algorithms for physics, chemistry, machine learning and beyond.

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. ISSN 0097-5397. doi: 10.1137/S0097539795293172. URL http://epubs.siam.org/doi/10.1137/S0097539795293172.

[2] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*, pages 212–219, New York, New York, USA, 1996. ACM Press. ISBN 0897917855. doi: 10.1145/237814.237866. URL http://portal.acm.org/citation.cfm?doid=237814.237866.

[3] Seth Lloyd. Universal Quantum Simulators. *Science*, 273(5278):1073–1078, aug 1996. ISSN 0036-8075. doi: 10.1126/science.273.5278.1073. URL http://www.sciencemag.org/cgi/doi/10.1126/science.273.5278.1073.

[4] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 193–204, June 2019. doi: 10.1145/3313276.3316366. URL http://arxiv.org/abs/1806.01838.

[5] John M. Martyn, Zane M. Rossi, Andrew K. Tan, and Isaac L. Chuang. A Grand Unification of Quantum Algorithms. *PRX Quantum*, 2(4):040203, December 2021. ISSN 2691-3399. doi: 10.1103/PRXQuantum.2.040203.

[6] András Gilyén and Tongyang Li. Distributional property testing in a quantum world. In *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*, pages 25:1–25:19, 2020. doi: 10.4230/LIPIcs.ITCS.2020.25. URL https://doi.org/10.4230/LIPIcs.ITCS.2020.25.

[7] Lin Lin and Yu Tong. Near-optimal ground state preparation. *Quantum*, 4:372, December 2020. doi: 10.22331/q-2020-12-14-372.

[8] Seth Lloyd, Bobak T. Kiani, David R. M. Arvidsson-Shukur, Samuel Bosch, Giacomo De Palma, William M. Kaminsky, Zi-Wen Liu, and Milad Marvian. Hamiltonian singular value transformation and inverse block encoding, May 2021.

[9] Lin Lin and Yu Tong. Heisenberg-limited ground-state energy estimation for early fault-tolerant quantum computers. *PRX Quantum*, 3(1):010318, 2022. URL https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.3.010318.

[10] Yulong Dong, Lin Lin, and Yu Tong. Ground state preparation and energy estimation on early fault-tolerant quantum computers via quantum eigenvalue transformation of unitary matrices. *arXiv preprint arXiv:2204.05955*, 2022. URL https://arxiv.org/abs/2204.05955.

[11] András Gilyén and Alexander Poremba. Improved Quantum Algorithms for Fidelity Estimation, March 2022.

[12] Patrick Rall. Faster Coherent Quantum Algorithms for Phase, Energy, and Amplitude Estimation. *Quantum*, 5:566, October 2021. doi: 10.22331/q-2021-10-19-566. URL https://quantum-journal.org/papers/q-2021-10-19-566/.

[13] Patrick Rall and Bryce Fuller. Amplitude Estimation from Quantum Signal Processing, September 2022.

[14] Guang Hao Low, Theodore J. Yoder, and Isaac L. Chuang. Methodology of Resonant Equiangular Composite Quantum Gates. *Physical Review X*, 6(4):041067, December 2016. doi: 10.1103/PhysRevX.6.041067.

[15] Guang Hao Low and Isaac L Chuang. Optimal hamiltonian simulation by quantum signal processing. *Physical review letters*, 118(1):010501, 2017. URL https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.118.010501.

[16] Guang Hao Low and Isaac L. Chuang. Hamiltonian Simulation by Qubitization. *Quantum*, 3:163, July 2019. ISSN 2521-327X. doi: 10.22331/q-2019-07-12-163.

[17] Zhan Yu, Hongshun Yao, Mujin Li, and Xin Wang. Power and limitations of single-qubit native quantum neural networks, May 2022.

[18] A. Yu Kitaev. Quantum measurements and the Abelian Stabilizer Problem, November 1995.

[19] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 454(1969):339–354, January 1998. doi: 10.1098/rspa.1998.0164.

[20] Adriano Barenco, André Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello. Stabilization of Quantum Computations by Symmetrization. *SIAM Journal on Computing*, 26(5):1541–1557, October 1997. ISSN 0097-5397. doi: 10.1137/S0097539796302452.

[21] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum Fingerprinting. *Physical Review Letters*, 87(16):167902, September 2001. doi: 10.1103/PhysRevLett.87.167902.

[22] Dorit Aharonov, Vaughan Jones, and Zeph Landau. A Polynomial Quantum Algorithm for Approximating the Jones Polynomial. *Algorithmica*, 55(3):395–421, November 2009. ISSN 1432-0541. doi: 10.1007/s00453-008-9168-0.

[23] E. Knill and R. Laflamme. Power of One Bit of Quantum Information. *Physical Review Letters*, 81 (25):5672–5675, December 1998. doi: 10.1103/PhysRevLett.81.5672.

[24] Thais de Lima Silva, Lucas Borges, and Leandro Aolita. Fourier-based quantum signal processing. June 2022. doi: 10.48550/arXiv.2206.02826.

[25] Tom Gur, Min-Hsiu Hsieh, and Sathyawageeswar Subramanian. Sublinear quantum algorithms for estimating von Neumann entropy, November 2021.

[26] Sonika Johri, Damian S. Steiger, and Matthias Troyer. Entanglement spectroscopy on a quantum computer. *Physical Review B*, 96(19):195136, November 2017. doi: 10.1103/PhysRevB.96.195136.

[27] Yigit Subasi, Lukasz Cincio, and Patrick J. Coles. Entanglement spectroscopy with a depth-two quantum circuit. *Journal of Physics A: Mathematical and Theoretical*, 52(4):044001, January 2019. ISSN 1751-8113, 1751-8121. doi: 10.1088/1751-8121/aaf54d.

[28] Justin Yirka and Yigit Subasi. Qubit-efficient entanglement spectroscopy using qubit resets. *Quantum*, 5:535, September 2021. ISSN 2521-327X. doi: 10.22331/q-2021-09-02-535.

[29] Sathyawageeswar Subramanian and Min-Hsiu Hsieh. Quantum algorithm for estimating α-Renyi entropies of quantum states. *Physical Review A*, 104(2):022428, August 2021. doi: 10.1103/PhysRevA.104.022428.

Exponential quantum amplitude amplification via quantum iterative power algorithms

Thi Ha Kyaw[1 2 3 *] Micheline B. Soley[4 5 6 7 †] Brandon Allen[6 7] Paul Bergold[8]
Chong Sun[2] Victor S. Batista[6 7 9 ‡] Alán Aspuru-Guzik[2 3 10 11 §]

[1]*LG Electronics Toronto AI Lab, Toronto, Ontario M5V 1M3, Canada*
[2]*Department of Chemistry, University of Toronto, Toronto, Ontario M5G 1Z8, Canada*
[3]*Department of Computer Science, University of Toronto, Toronto, Ontario M5S 2E4, Canada*
[4]*Department of Chemistry, University of Wisconsin-Madison, 1101 University Ave., Madison, WI 53706, USA*
[5]*Department of Physics, University of Wisconsin-Madison, 1150 University Ave., Madison, WI 53706, USA*
[6]*Yale Quantum Institute, Yale University, P.O. Box 208334, New Haven, CT 06520-8263, USA*
[7]*Department of Chemistry, Yale University, P.O. Box 208107, New Haven, CT 06520, USA*
[8]*Department of Mathematics, University of Surrey, Guildford, United Kingdom*
[9]*Energy Sciences Institute, Yale University, P.O. Box 27394, West Haven, CT 06516-7394, USA*
[10]*Vector Institute for Artificial Intelligence, Toronto, Ontario M5S 1M1, Canada*
[11]*Canadian Institute for Advanced Research, Toronto, Ontario M5G 1Z8, Canada*

Abstract. The search for the ground state of a quantum system Hamiltonian is a typical application of a quantum computer even though the computational complexity is of QMA-hard. In practice, knowing some partial information about the studied system, one could simplify such problem. Here, we show analytically that there exists an exponential amplitude amplification at every step of the quantum iterative power algorithms as compared to the quantum imaginary time evolution algorithm, within the constraint the quantum ansatz circuit used. We also provide numerical evidence to support our analytical results.

Keywords: Quantum iterative power algorithms, ground state search, quantum algorithms

1 Introduction

Quantum computers promise exponential speedup over classical counterparts in solving certain tasks [1]. When fault-tolerant general-purpose quantum computers become available, adiabatic state preparation and quantum phase estimation may become the standard quantum routines for determining the ground-state energy of sophisticated physical Hamiltonians [2, 3, 4, 5]. However, such schemes are very costly in terms of required overhead and hence are not suitable for the current era of noisy intermediate-scale quantum (NISQ) hardware [6, 7, 8, 9, 10]. This limitation of quantum computers today shifts central attention towards low-depth hybrid quantum-classical algorithms, known as NISQ algorithms [11, 12, 13, 14]. The variational quantum eigensolver (VQE) [15, 16] serves as a prototypical example, as an algorithm that computes the expectation value of a Hamiltonian, which is measured on a quantum machine, resulting in a cost function with a set of variational parameters, which are optimized using classical computers. The process is repeated until the cost function reaches its local minimum.

On the other hand, the variational quantum simulator [17] has been proposed for hybrid quantum-classical simulations of quantum dynamics based on the McLachlan's variational principle [18, 19], including quantum imaginary time evolution to prepare ground states [18, 19, 20]. Here, we introduce the "quantum iterative power algorithm" inspired by the variational quantum simulator to provide an accelerated method to the general problem of global optimization with near term quantum computers.

Global optimization is central to many important problems in science and engineering, from back-propagation in machine learning [21] and molecular geometry optimization/protein structure prediction [22, 23] to route planning and control of drone/unmanned aerial vehicles [24]. However, the brute force approach of considering each possible element of a search space often becomes computationally intractable. For example, identification of the optimal configuration of a protein faces Levinthals paradox [25] that the native configuration must be identified out of about 10^{300} possibilities. This has inspired a broad array of both classical [26] and quantum computing [27] optimizers. Recently, we have shown that tensor trains [28, 29] (also known as matrix product states) provide a way to vastly reduce the computational cost of exploring low-rank optimization cost functions, and have employed the approach to introduce an optimization algorithm that deterministically explores the full search space in data-compressed form, the tensor-train "iterative power algorithm (IPA)" [30].

We recognize the strategy of tensor-train IPA can be implemented on quantum computers to enable global optimization of an even broader class of optimization problems. In tensor-train IPA, the optimization cost function of interest is taken to be a potential energy surface. A density is initialized in the potential energy surface, and an oracle is iteratively applied in a sifting approach akin

*thiha.kyaw@lge.com
†msoley@wisc.edu
‡victor.batista@yale.edu
§alan@aspuru.com

to imaginary time propagation (with infinite mass) to localize the density as a delta function at the global minimum position. The expectation value of position then gives the location of the global minimum. Tensor-train IPA represents the density and potential energy surface as tensor trains to avoid calculation of the cost function everywhere in search space, which is efficient for representation of problems amenable to low-rank representations, such as prime factorization or molecular geometry optimization [30]. However, the tensor-train strategy faces the roadblock that highly-correlated systems cannot be efficiently represented in low-rank tensor-train format. In contrast, quantum computers excel in the simulation of highly-correlated systems, as the coupling or entanglement between qubits is limited only by the choice of ansatz [31].

The quantum iterative power algorithm (QIPA) takes advantage of the high degree of entanglement possible on quantum computers with a hybrid variational scheme. In standard variational approaches such as the variational quantum eigensolver (VQE) [15, 16], classical optimizers are used to determine the parameters of a quantum circuit, which are used to prepare trial wavefunctions measured to obtain expectation values. Analogously, the variational quantum simulator [17] evolves the parameters that define the time-evolved wavefunction by using a classical computer that integrates the Euler–Lagrange equation obtained from the Schrödinger equation with the McLachlans variational principle. Parameters required by the Euler–Lagrange equation are obtained with a quantum circuit with a small number of quantum operations. QIPA generalizes the variational quantum approach to evolve an initial wavefunction such that the corresponding probability density (modulus squared of the wavefunction) becomes localized at the global minimum of a given cost function. As in IPA, the propagator of QIPA is not limited to the imaginary time quantum propagator enabling the use of other propagators that are maximal at the minimum of the cost function.

2 Results

We are interested in a particular case of global optimization involving the search of the ground state of a Hamiltonian $\hat{H}$: a problem that is typically solved by the imaginary time propagation. QIPA can solve the same problem analogously by using $\hat{H}$ in the normalized oracle function $f(\hat{H};\tau)$ that acts on the initial wavefunction $|\psi(0)\rangle$, as follows (onwards setting $\hbar = 1$):

$$\begin{aligned} |\psi(\tau)\rangle &= f(\hat{H};\tau)\,|\psi(0)\rangle \\ &= \frac{U(\tau)\,|\psi(0)\rangle}{\sqrt{\langle U(\tau)\psi(0)|U(\tau)\psi(0)\rangle}}, \end{aligned} \tag{1}$$

where $U(\tau)$ is an arbitrary oracle function with maximum at the global minimum position of the potential energy surface M, or here the Hamiltonian $\hat{H}$. In the following, we show that oracles defined by concatenated exponential functions,

$$U(\tau) = U_n(\tau) = \beta_n(-\hat{H}\tau)) = e^{b_n\beta_{n-1}(-\hat{H}\tau)}, \tag{2}$$

with $n \geq 1$ the number of concatenated exponentials, $\beta_0(y) = y$, $\beta_1(y) = e^{b_1 y}, \beta_2(y) = e^{b_2 e^{b_1 y}}, \ldots$ and real constants $b_1, \ldots, b_n \neq 0$, provide effective QIPAs based on a generalization of the McLachlans variational principle. For example, the oracle defined by the double-exponential $U_2(\tau) = e^{e^{-\tau\hat{H}}}$ is obtained by setting $n = 2$ and $b_2 = b_1 = 1$.

We remark that the choice of U_1 corresponds to the standard quantum imaginary time evolution (QITE), which is widely used in quantum Monte Carlo algorithms. Refs. [18, 19] show that one can perform imaginary time evolution [20] with unitary gates defined by Eq. (1) with $n = 1$ that evolve the initial state according to the Wick-rotated Schrödinger equation: $\partial\,|\psi(\tau)\rangle/\partial\tau = -\Big(\hat{H} - E_1(\tau)\Big)\,|\psi(\tau)\rangle$, where $E_1(\tau) = \langle\psi(\tau)|\,\hat{H}\,|\psi(\tau)\rangle$. Here, we introduce a family of near-term quantum algorithms defined by β_n with $n \geq 1$ that evolve the initial state according to the generalized Wick-like-rotated Schrödinger equation:

$$\begin{aligned} \frac{\partial}{\partial\tau}\,|\psi(\tau)\rangle = -\prod_{k=1}^{n} b_k \Big(\hat{H}\exp(\hat{S}_{n-1}) \\ - \mathrm{Re}\langle\hat{H}\exp(\hat{S}_{n-1})\psi(\tau)\mid\psi(\tau)\rangle\Big)\,|\psi(\tau)\rangle\,, \end{aligned} \tag{3}$$

where $\hat{S}_{n-1} = \sum_{k=1}^{n-1} b_k\beta_{k-1}(-\hat{H}\tau)$.

With the choice $n = 2$ and $b_2 = b_1 = 1$ we arrive at a double-exponential function and the following Wick-like-rotated Schrödinger equation:

$$\frac{\partial}{\partial\tau}\,|\psi(\tau)\rangle = -\Big(\hat{H}e^{-\hat{H}\tau} - E_2(\tau)\Big)\,|\psi(\tau)\rangle\,, \tag{4}$$

with $E_2(\tau) = \langle\psi(\tau)\mid\hat{H}e^{-\hat{H}\tau}\mid\psi(\tau)\rangle$. According to the McLachlan's variational principle, when we constrain the equation of motion as such

$$\delta\left\|\Big(\partial/\partial\tau + \Big[\hat{H}e^{-\hat{H}\tau} - E_2(\tau)\Big]\Big)\,|\psi(\tau)\rangle\right\|^2 = 0, \tag{5}$$

the result is equivalent in finding a solution of the linear equation: $\sum_m A_{k,m}\dot{\theta}_m = C_k$, where the entries of the symmetric and positive semi-definite matrix $\mathbf{A}$ and the right-hand side $\mathbf{C}$ can be computed on a quantum computer by deploying the Hadamard tests. The parameters $\boldsymbol{\theta}$ are updated with $\dot{\boldsymbol{\theta}}$ for a short time step $\delta\tau > 0$ according to the Euler method as $\boldsymbol{\theta}(\tau + \delta\tau) \approx \boldsymbol{\theta}(\tau) + \dot{\boldsymbol{\theta}}(\tau)\delta\tau$. The underlying assumption is that we can approximate $|\psi(\tau)\rangle$ by $|\phi(\boldsymbol{\theta}(\tau))\rangle = U(\theta_1(\tau))U(\theta_2(\tau))\cdots U(\theta_{\mathcal{N}_\theta}(\tau))\,|\bar{0}\rangle$, where $|\bar{0}\rangle = |0\rangle^{\otimes\mathcal{N}}$ and $U(\theta_1(\tau)), \ldots, U(\theta_{\mathcal{N}_\theta}(\tau))$ are parameterized quantum circuits (PQCs), with $\boldsymbol{\theta} = (\theta_1, \ldots, \theta_{\mathcal{N}_\theta})$ the corresponding real-valued parameter vector.

2.1 Exponential amplitude amplification

To precisely define what exponential amplitude amplification means, let us look at a general setting where we are interested to find a unique ground state $|\Psi\rangle$ of a quantum system $\hat{H}$, assuming no degeneracy. In variational quantum algorithms, one is interested to find the ground

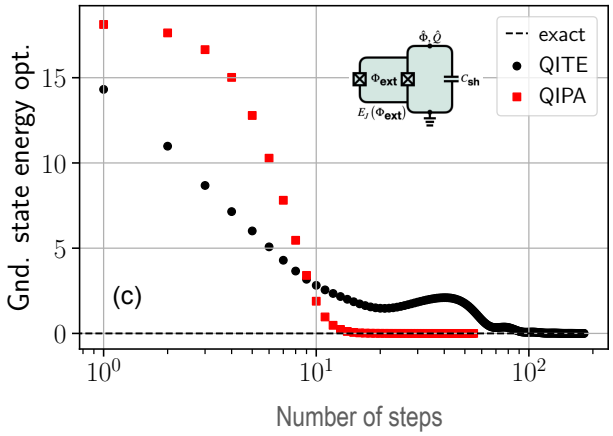


Figure 1: Ground-state energy optimization plot for a flux tunable transmon at the external flux $f = 0.25$ as a function of the number of iteration steps for both QIPA and QITE, 4-qubit numerical experiments. In all results, both QIPA and QITE are run with the same time step $\delta\tau$ for a fair comparison. Here QIPA runs require significantly fewer steps to reach the convergence criteria.

state as close as possible using hybrid quantum-classical approach and would end up obtaining an approxiate state $|\Phi\rangle$, where $|\langle\Psi|\Phi\rangle| = \gamma$. It was recently shown that $\gamma \propto \exp(-\mathcal{N})$ [32] as the system size $\mathcal{N}$ grows for complex chemical molecular systems. In a specific condition that we are interested in (within the reach of the variational quantum ansatz), we prove analytically that γ can be amplified in exponentially less number of timesteps defined by the ratio $\iota = \lambda_{1,U_1}/\lambda_{2,U_1}$. The number of timesteps necessary to achieve more than 50% fidelity with the final desired quantum state is upper bounded by $k_{QIPA}/k_{QITE} \geq \log\iota/\iota$. We are aware that local quantum Hamiltonian ground state problem is QMA-complete and our approach does not change such problem's computational complexity class. We are merely pointing out that there is a special case with the proposed algorithm, where we are able to converge the solution in exponentially less number of steps as compared to the existing QITE program. See Fig.1 for additional numerical evidences where we find the ground state energy of a flux tunable transmon at the external flux parameter $f = 0.25$ as a function of the number of iteration steps for both QIPA and QITE. QIPA runs require significantly fewer steps to reach the set convergence criteria.

We remark that we used double-exponential oracle function as a particular working example. Other types of oracle functions such as $U(\tau) = \mathrm{sech}(\hat{H}\tau)$ can also be used. The choice of an oracle function highly depends on the problem considered and the desired rate of convergence. The change in oracle function would result in the different convergence rate, with $k_{QIPA}/k_{QITE} \geq \varepsilon$, with $\varepsilon \ll 1$.

2.2 Resource estimate and error analysis

In general, for an $\mathcal{N}$-qubit system with Hamiltonian $\hat{H}$ with $\mathcal{N}_H \geq 1$ Pauli words and a parameterized wavefunction $|\phi(\boldsymbol{\theta})\rangle$ (where τ dependency $\boldsymbol{\theta}(\tau)$ is understood throughout) with $\mathcal{N}_\theta \geq 1$ parameters, the upper bound for the number of distinct measurements $\mathcal{N}_A$ required to obtain the matrix $\mathbf{A}$ for QIPA via the Hadamard test and the number of gates required are $\mathcal{N}_\theta(\mathcal{N}_\theta - 1)/2$ and $G_{\mathcal{N}_A} \geq \mathcal{N}_\theta$, respectively. Such an estimate can be understood as the number of times required to completely evaluate all the $\mathbf{A}$ matrix elements since $\mathbf{A}$ is symmetric. Moreover, to obtain the vector $\mathbf{C}$, the number of measurements and gates required (assuming a second-order Taylor series expansion of the required function of the Hamiltonian) are $\mathcal{N}_\theta$ and $G_{\mathcal{N}_C} \geq \mathcal{N}_H + \mathcal{N}_H^2 + \mathcal{N}_H^3 + \mathcal{N}_\theta$, respectively. '>' sign in $G_{\mathcal{N}_A}$ and $G_{\mathcal{N}_C}$ holds when two-qubit gates are not parameterized, while '=' sign holds when they are parameterized. Assuming a polynomial scaling: $\mathcal{N}_H = \mathcal{O}(\mathcal{N}^h), \mathcal{N}_\theta = \mathcal{O}(\mathcal{N}^d)$, the leading order becomes $\mathcal{N}_A = \mathcal{O}(\mathcal{N}^d)$ and $\mathcal{N}_C = \mathcal{O}(\mathcal{N}^{\max(3h,d)})$, respectively. In comparison, in QITE, one needs $\mathcal{N}_A = \mathcal{O}(\mathcal{N}^d)$ and $\mathcal{N}_C = \mathcal{O}(\mathcal{N}^{\max(h,d)})$, with the same number of Hadamard test measurements required. In general, QIPA yields improved convergence in shorter times compared to QITE, requiring the same number of Hadamard test operations and a higher number of unitary gates. More importantly, we have also estimated that the error from the Taylor expansion causing the major difference between QITE and QIPA is given by $\epsilon = \sqrt{\Delta^2\delta\tau^2 + \mathcal{O}(\delta\tau^3)} \leq \Delta\delta\tau + \mathcal{O}(\delta\tau^{3/2})$, where $\Delta^2 = \langle\Psi(t)|\left((1 + e^{-\hat{H}\delta\tau})^2/(\delta\tau^2) + 2(e^{-\hat{H}\delta\tau} - 1)\hat{H}/\delta\tau - (e^{-\hat{H}\delta\tau} - 2)\hat{H}^2\right)|\Psi(t)\rangle$.

3 Conclusion

In summary, we have presented a family of generalized imaginary-time-like near-term quantum algorithms which we coin the "quantum iterative power algorithm," inspired by its classical counterpart. (Plural "algorithms" is used since depending on the choice of oracle function, the performance and behaviour will differ. However, they all fall under the same family.) We have analyzed its convergence rate. One caveat is that since the proposed algorithm relies heavily on the ansatz circuit used, its convergence rate is difficult to discern in the generic case. We have also determined QIPA's estimated resource count as well as analytical error analysis, and demonstrated it can outperform the quantum imaginary time evolution while it reduces the number of required iterations, at the cost of a moderate increase in the number of gates. We note that even when the initial quantum state has an exponentially small overlap with the final target state, QIPA needs only a polynomial number of steps to reach convergence. This is particularly important when starting with an initial state defined by a uniform superposition, or a low-rank reference state for a highly correlated system [32]. Furthermore, we have used the three numerical case studies – quantum computer-aided design of a superconducting transmon,

to highlight how QIPA outperforms QITE.

References

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

[2] Ala'n Aspuru-Guzik, Anthony D. Dutoi, Peter J. Love, and Martin Head-Gordon. Simulated Quantum Computation of Molecular Energies. *Science*, 309(5741):1704–1707, September 2005.

[3] I. M. Georgescu, S. Ashhab, and Franco Nori. Quantum simulation. *Rev. Mod. Phys.*, 86(1):153–185, March 2014.

[4] Yudong Cao, Jonathan Romero, Jonathan P. Olson, Matthias Degroote, Peter D. Johnson, Mária Kieferová, Ian D. Kivlichan, Tim Menke, Borja Peropadre, Nicolas P. D. Sawaya, et al. Quantum Chemistry in the Age of Quantum Computing. *Chem. Rev.*, 119(19):10856–10915, October 2019.

[5] Sam McArdle, Suguru Endo, Alán Aspuru-Guzik, Simon C. Benjamin, and Xiao Yuan. Quantum computational chemistry. *Rev. Mod. Phys.*, 92(1):015003, March 2020.

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

[7] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, October 2019.

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

[9] Yulin Wu, Wan-Su Bao, Sirui Cao, Fusheng Chen, Ming-Cheng Chen, Xiawei Chen, Tung-Hsun Chung, Hui Deng, Yajie Du, Daojin Fan, et al. Strong Quantum Computational Advantage Using a Superconducting Quantum Processor. *Phys. Rev. Lett.*, 127(18):180501, October 2021.

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

[11] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S. Kottmann, Tim Menke, et al. Noisy intermediate-scale quantum algorithms. *Rev. Mod. Phys.*, 94(1):015004, February 2022.

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

[13] Jules Tilly, Hongxiang Chen, Shuxiang Cao, Dario Picozzi, Kanav Setia, Ying Li, Edward Grant, Leonard Wossnig, Ivan Rungger, George H. Booth, et al. The Variational Quantum Eigensolver: a review of methods and best practices. *arXiv:2111.05176*, November 2021.

[14] Dmitry A Fedorov, Bo Peng, Niranjan Govind, and Yuri Alexeev. VQE method: A short survey and recent developments. *Mater. Theory*, 6(1):1–21, 2022.

[15] 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(4213):1–7, July 2014.

[16] Jarrod R. McClean, Jonathan Romero, Ryan Babbush, and Alán Aspuru-Guzik. The theory of variational hybrid quantum-classical algorithms. *New J. Phys.*, 18(2):023023, February 2016.

[17] Ying Li and Simon C Benjamin. Efficient variational quantum simulator incorporating active error minimization. *Physical Review X*, 7(2):021050, 2017.

[18] Sam McArdle, Tyson Jones, Suguru Endo, Ying Li, Simon C Benjamin, and Xiao Yuan. Variational ansatz-based quantum simulation of imaginary time evolution. *npj Quantum Inf.*, 5(1):1–6, 2019.

[19] Xiao Yuan, Suguru Endo, Qi Zhao, Ying Li, and Simon C Benjamin. Theory of variational quantum simulation. *Quantum*, 3:191, 2019.

[20] Mario Motta, Chong Sun, Adrian T. K. Tan, Matthew J. O'Rourke, Erika Ye, Austin J. Minnich, Fernando G. S. L. Brandão, and Garnet Kin-Lic Chan. Determining eigenstates and thermal states on a quantum computer using quantum imaginary time evolution. *Nat. Phys.*, 16(2):205–210, February 2020.

[21] Léon Bottou, Frank E Curtis, and Jorge Nocedal. Optimization methods for large-scale machine learning. *Siam Review*, 60(2):223–311, 2018.

[22] David J Wales and Harold A Scheraga. Global optimization of clusters, crystals, and biomolecules. *Science*, 285(5432):1368–1372, 1999.

[23] Ken A Dill, S Banu Ozkan, M Scott Shell, and Thomas R Weikl. The protein folding problem. *Annu. Rev. Biophys.*, 37:289, 2008.

[24] Walton Pereira Coutinho, Maria Battarra, and Jörg Fliege. The unmanned aerial vehicle routing and trajectory optimisation problem, a taxonomic review. *Comput. Ind. Eng.*, 120:116–128, 2018.

[25] Cyrus Levinthal. How to fold graciously. *Mossbauer spectroscopy in biological systems*, 67:22–24, 1969.

[26] Gerhard Venter. *Review of Optimization Techniques*. John Wiley & Sons, Ltd, Chichester, England, UK, December 2010.

[27] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing*, pages 212–219. Association for Computing Machinery, New York, NY, USA, July 1996.

[28] Ivan Oseledets and Eugene Tyrtyshnikov. TT-cross approximation for multidimensional arrays. *Linear Algebra Appl.*, 432(1):70–88, January 2010.

[29] I. V. Oseledets. Tensor-Train Decomposition. *SIAM J. Sci. Comput.*, September 2011.

[30] Micheline B Soley, Paul Bergold, and Victor S Batista. Iterative power algorithm for global optimization with quantics tensor trains. *J. Chem. Theory Comput.*, 17(6):3280–3291, 2021.

[31] Sukin Sim, Peter D. Johnson, and Alán Aspuru-Guzik. Expressibility and Entangling Capability of Parameterized Quantum Circuits for Hybrid Quantum-Classical Algorithms. *Adv. Quantum Technol.*, 2(12):1900070, December 2019.

[32] Seunghoon Lee, Joonho Lee, Huanchen Zhai, Yu Tong, Alexander M. Dalzell, Ashutosh Kumar, Phillip Helms, Johnnie Gray, Zhi-Hao Cui, Wenyuan Liu, et al. Is there evidence for exponential quantum advantage in quantum chemistry? *arXiv*, August 2022.

[33] Suguru Endo, Zhenyu Cai, Simon C. Benjamin, and Xiao Yuan. Hybrid Quantum-Classical Algorithms and Quantum Error Mitigation. *J. Phys. Soc. Jpn.*, 90(3):032001, February 2021.

[34] Suguru Endo, Simon C. Benjamin, and Ying Li. Practical Quantum Error Mitigation for Near-Future Applications. *Phys. Rev. X*, 8(3):031027, July 2018.

[35] Kristan Temme, Sergey Bravyi, and Jay M. Gambetta. Error Mitigation for Short-Depth Quantum Circuits. *Phys. Rev. Lett.*, 119(18):180509, November 2017.

[36] Matthew Otten and Stephen K. Gray. Accounting for errors in quantum algorithms via individual error reduction. *npj Quantum Inf.*, 5(11):1–6, January 2019.

[37] Armands Strikis, Dayue Qin, Yanzhu Chen, Simon C. Benjamin, and Ying Li. Learning-based quantum error mitigation. *arXiv*, May 2020.

[38] Sergey Bravyi, Sarah Sheldon, Abhinav Kandala, David C. Mckay, and Jay M. Gambetta. Mitigating measurement errors in multiqubit experiments. *Phys. Rev. A*, 103(4):042605, April 2021.

[39] Niladri Gomes, Anirban Mukherjee, Feng Zhang, Thomas Iadecola, Cai-Zhuang Wang, Kai-Ming Ho, Peter P. Orth, and Yong-Xin Yao. Adaptive Variational Quantum Imaginary Time Evolution Approach for Ground State Preparation. *Adv. Quantum Technol.*, 4(12):2100114, December 2021.

[40] Zi-Jian Zhang, Jinzhao Sun, Xiao Yuan, and Man-Hong Yung. Low-depth Hamiltonian Simulation by Adaptive Product Formula. *arXiv2011.05283*, November 2020.

From the Hardness of Detecting Superpositions to Cryptography: Quantum Public Key Encryption and Commitments (Extended Abstract)

Minki Hhan[1] * Tomoyuki Morimae[2] † Takashi Yamakawa[2 3] ‡

[1] *Quantum Universe Center, Korea Institute for Advanced Study, Seoul 02455, Korea*
[2] *Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto 606-8502, Japan*
[3] *NTT Social Informatics Laboratories, Tokyo 180-8585, Japan*

Abstract. Recently, Aaronson, Atia, and Susskind (arXiv:2009.07450) showed that detecting interference between two orthogonal states is as hard as swapping these states. While their original motivation was quantum gravity, we show its applications in quantum cryptography.

1. We construct the first public key encryption scheme from cryptographic *non-abelian* group actions. This resolves an open question posed by Ji et al. (TCC '19).
2. We give a simple and efficient compiler that converts the flavor of quantum bit commitments, showing that two different notions of quantum bit commitment are essentially the same. Our compiler calls the base scheme only once. Previously, all known compilers call the base schemes polynomially many times (Crépeau et al., Eurocrypt '01 and Yan, Asiacrypt '22).

Keywords: Cryptography, Public-key encryption, Quantum bit commitment, Group action

1 Introduction

When can we *efficiently* distinguish a superposition of two orthogonal states from their probabilistic mix? They can be certainly distinguished if we drop the *efficiency*, but with the restricted resource it is unclear.

A folklore answer to this question was that we can distinguish them whenever we can map one of the states to the other. Recently, Aaronson, Atia and, Susskind [1] gave a complete answer to the question. They confirmed that the folklore was almost correct but what actually characterizes the distinguishability is the ability to *swap* the two states rather than the ability to map one of the states to the other.[1]

We explain their result in more detail by using the example of Schrödinger's cat following [1]. Let $|\text{Alive}\rangle$ and $|\text{Dead}\rangle$ be orthogonal states, which can be understood as the states of alive and dead cats in Schrödinger's cat experiment. Then, the authors show that one can efficiently swap $|\text{Alive}\rangle$ and $|\text{Dead}\rangle$, or more formally there is an efficiently computable unitary U such that

$$U|\text{Dead}\rangle = |\text{Alive}\rangle \text{ and } U|\text{Alive}\rangle = |\text{Dead}\rangle$$

if and only if there is an efficient distinguisher that distinguishes two states

$$|\psi\rangle = \frac{|\text{Alive}\rangle + |\text{Dead}\rangle}{\sqrt{2}} \text{ and } |\phi\rangle = \frac{|\text{Alive}\rangle - |\text{Dead}\rangle}{\sqrt{2}}$$

with certainty. Note that distinguishing $|\psi\rangle$ and $|\phi\rangle$ is equivalent to distinguishing $\frac{|\text{Alive}\rangle+|\text{Dead}\rangle}{\sqrt{2}}$ and the uniform probabilistic mix of $|\text{Alive}\rangle$ and $|\text{Dead}\rangle$.[2]

Moreover, they showed that the equivalence is robust in the sense that a partial ability to swap $|\text{Alive}\rangle$ and $|\text{Dead}\rangle$, i.e.,

$$|\langle\text{Dead}|U|\text{Alive}\rangle + \langle\text{Alive}|U|\text{Dead}\rangle| = \Gamma$$

for some $\Gamma > 0$ is equivalent to the distinguishability of $|\psi\rangle$ and $|\phi\rangle$ with advantage $\Delta = \Gamma/2$. They give an interpretation of their result that observing interference between alive and dead cats is "necromancy-hard", i.e., at least as hard as bringing a dead cat back to life.

While their original motivation was from quantum gravity, we find their result interesting from cryptographic perspective. Roughly speaking, the task of swapping $|\text{Alive}\rangle$ and $|\text{Dead}\rangle$ can be thought of as a kind of search problem where one is given $|\text{Alive}\rangle$ (resp. $|\text{Dead}\rangle$) and asked to "search" for $|\text{Dead}\rangle$ (resp. $|\text{Alive}\rangle$). On the other hand, the task of distinguishing $|\psi\rangle$ and $|\phi\rangle$ is apparently a decision problem.

From this perspective, we can view their result as a "search-to-decision" reduction. Search-to-decision reductions have been playing the central role in cryptography, e.g., the celebrated Goldreich-Levin theorem [13]. Based on this observation, we tackle the following two problems in quantum cryptography.[3]

Public key encryption from non-abelian group actions. Brassard and Yung [5] initiated the study of cryptographic group actions. We say that a group G acts on a set S by an action $\star : G \times S \to S$ if the following are satisfied:

*minkihhan@kias.ac.kr
†tomoyuki.morimae@yukawa.kyoto-u.ac.jp
‡takashi.yamakawa.ga@hco.ntt.co.jp

[1] We remark that the meaning of "swap" here is different from that of the SWAP gate as explained below.

[2] The distinguishing advantage is (necessarily) halved. This can be seen by observing that the mixture of $|\psi\rangle$ and $|\phi\rangle$ is the same with the mixture of $|\text{Alive}\rangle$ and $|\text{Dead}\rangle$.

[3] It may be a priori unclear why these problems are related to [1]. This will become clearer in the full version.

1. For the identity element $e \in G$ and any $s \in S$, we have $e \star s = s$.
2. For any $g, h \in G$ and any $s \in S$, we have $(gh) \star s = g \star (h \star s)$.

For a cryptographic purpose, we assume (at least) that the group action is one-way, i.e., it is hard to find g' such that $g' \star s = g \star s$ given s and $g \star s$. The work of [5] proposed instantiations of such cryptographic group actions based on the hardness of discrete logarithm, factoring, or graph isomorphism problems.

Cryptographic group actions are recently gaining a renewed attention from the perspective of *post-quantum* cryptography. Ji et al. [17] proposed new instantiations of cryptographic group actions based on general linear group actions on tensors. Alamati et al. [2] proposed isogeny-based instantiations based on earlier works [9, 7]. Both of them are believed to be secure against quantum adversaries.

An important difference between the instantiations in [17] and [2] is that the former considers *non-abelian* groups whereas the latter considers *abelian* groups.

Abelian group actions are particularly useful because they give rise to a non-interactive key exchange protocol similar to Diffie-Hellman key exchange [11]. Namely, suppose that $s \in S$ is published as a public parameter, Alice publishes $g_A \star s$ as a public key while keeping g_A as her secret key, and Bob publishes $g_B \star s$ as a public key while keeping g_B as his secret key. Then, they can establish a shared key $g_A \star (g_B \star s) = g_B \star (g_A \star s)$. On the other hand, an eavesdropper Eve cannot know the shared key since she cannot know g_A or g_B by the one-wayness of the group action.[4] This also naturally gives a public key encryption (PKE) scheme similar to ElGamal encryption [12].

The above construction does not work if G is a non-abelian group. Indeed, cryptographic applications given in [17] are limited to *Minicrypt* primitives [16], i.e., those that do not imply PKE in a black-box manner. Thus, [17] raised the following open question:[5]

> **Question 1:** *Can we construct PKE from non-abelian group actions?*

Flavor conversion for quantum bit commitments. Commitments are one of the most important primitives in cryptography. It enables one to "commit" to a (classical) bit[6] in such a way that the committed bit is hidden from other parties before the committer reveals it, which is called the *hiding* property, and the committer cannot change the committed bit after sending the commitment, which is called the *binding* property.

One can easily see that it is impossible for *classical* commitments to achieve both hiding and binding properties against unbounded-time adversaries. It is known to be impossible even with *quantum* communication [18, 19]. Thus, it is a common practice in cryptography to relax either of them to hold only against computationally bounded adversaries. We say that a commitment scheme is computationally (resp. statistically) binding/hiding, if it holds against (classical or quantum depending on the context) polynomial-time (resp. unbounded-time) adversaries. Then, there are the following two *flavors* of commitments: One is computationally hiding and statistically binding, and the other is computationally binding and statistically hiding.[7] In the following, whenever we require statistical hiding or binding, the other one should be understood as computational one since it is impossible to statistically achieve both of them as already explained.

In classical cryptography, though commitments of both flavors are known to be equivalent to the existence of one-way functions [20, 15, 14], there is no known direct conversion between them that preserves efficiency or the number of interactions. Thus, their constructions have been studied separately.

Recently, Yan [21], based on an earlier work by Crépeau, Légaré, and Salvail [10], showed that the situation is completely different for quantum bit commitments, which rely on quantum communication between the sender and receiver. First, he showed a round-collapsing theorem, which means that any interactive quantum bit commitments can be converted into non-interactive one. Then he gave a conversion that converts the flavor of any non-interactive quantum bit commitments.

Though Yan's conversion gives a beautiful equivalence theorem, a disadvantage of the conversion is that it does not preserve the efficiency. Specifically, it calls the base scheme polynomially many times (i.e., $\Omega(\lambda^2)$ times for the security parameter λ). Then, it is natural to ask the following question:

> **Question 2:** *Is there an efficiency-preserving flavor conversion for quantum bit commitments?*

2 Our Result

We answer both questions affirmatively using (a generalization of) the result of [1].

For **Question 1**, we construct a PKE scheme with quantum ciphertexts based on non-abelian group actions. This resolves the open problem posed by [17].[8] Our main

[4] For the actual security proof, we need a stronger assumption than the one-wayness. This is similar to the necessity of decisional Diffie-Hellman assumption, which is stronger than the mere hardness of the discrete logarithm problem, for proving security of Diffie-Hellman key exchange.

[5] The statement of the open problem in [17] is quoted as follows: "*Finally, it is an important open problem to build quantum-secure public-key encryption schemes based on hard problems about GLAT or its close variations.*" Here, GLAT stands for General Linear Action on Tensors, which is their instantiation of non-abelian group action. Thus, **Question 1** is slightly more general than what they actually ask.

[6] We can also consider commitments for multi-bit strings. But we focus on *bit* commitments in this paper.

[7] Of course, we can also consider computationally hiding and computationally binding one, which is weaker than both flavors.

[8] The statement of their open problem (quoted in Footnote 5) does not specify if we are allowed to use quantum ciphertexts. Thus, we claim to resolve the problem even though we rely on quantum ciphertexts. If they mean *post-quantum* PKE (which has classical ciphertexts), this is still open.

construction only supports classical one-bit messages, but we can convert it into one that supports quantum multi-qubit messages by hybrid encryption with quantum one-time pad as shown in [6]. Interestingly, ciphertexts of our scheme are quantum even if messages are classical. We show that our scheme is IND-CPA secure if the group action satisfies *pseudorandomness*, which is a stronger assumption than the one-wayness introduced in [17]. In addition, we show a "win-win" result similar in spirit to [22]. We show that if the group action is one-way, then our PKE scheme is IND-CPA secure *or* we can construct one-shot signatures [3] using the group action.[9] Note that constructing one-shot signatures has been thought to be a very difficult task. The only known construction is relative to a classical oracle and there is no known construction in the standard model. Even for its significantly weaker variant called tokenized signatures [4], the only known construction in the standard model is based on indistinguishability obfuscation [8]. Given the difficulty of constructing tokenized signatures, let alone one-shot signatures, it is reasonable to conjecture that our PKE scheme is IND-CPA secure if we built it on "natural" one-way group actions. Our PKE scheme is constructed through an abstraction called *swap-trapdoor function pairs* (STFs), which may be of independent interest.

For **Question 2**, We give a new conversion between the two flavors of quantum commitments. That is, for $\mathrm{X}, \mathrm{Y} \in \{\text{computationally,statistically,perfectly}\}$, if the base scheme is X-hiding and Y-binding, then the resulting scheme is Y-hiding and X-binding. Our conversion calls the base scheme only once in superposition. Specifically, if Q_b is the unitary applied by the sender when committing to $b \in \{0,1\}$ in the base scheme, the committing procedure of the resulting scheme consists of a single call to Q_0 or Q_1 controlled by an additional qubit (i.e., application of a unitary such that $|b\rangle|\psi\rangle \mapsto |b\rangle(Q_b|\psi\rangle)$) and additional constant number of gates. For the security proof of our conversion, we develop a generalization of the result of [1] considering auxiliary quantum inputs.

We show several applications of our conversion. We remark that our conversion does not give any new feasibility result since similar conversions with worse efficiency were already known [10, 21]. However, our conversion gives schemes with better efficiency in terms of the number of calls to the building blocks.

References

[1] S. Aaronson, Y. Atia, and L. Susskind. On the hardness of detecting macroscopic superpositions. *Electron. Colloquium Comput. Complex.*, page 146, 2020.

[2] N. Alamati, L. De Feo, H. Montgomery, and S. Patranabis. Cryptographic group actions and applications. In S. Moriai and H. Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 411–439. Springer, Heidelberg, Dec. 2020.

[3] R. Amos, M. Georgiou, A. Kiayias, and M. Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In K. Makarychev, Y. Makarychev, M. Tulsiani, G. Kamath, and J. Chuzhoy, editors, *52nd ACM STOC*, pages 255–268. ACM Press, June 2020.

[4] S. Ben-David and O. Sattath. Quantum tokens for digital signatures. Cryptology ePrint Archive, Paper 2017/094, 2017. `https://eprint.iacr.org/2017/094`.

[5] G. Brassard and M. Yung. One-way group actions. In A. J. Menezes and S. A. Vanstone, editors, *CRYPTO'90*, volume 537 of *LNCS*, pages 94–107. Springer, Heidelberg, Aug. 1991.

[6] A. Broadbent and S. Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 609–629. Springer, Heidelberg, Aug. 2015.

[7] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes. CSIDH: An efficient post-quantum commutative group action. In T. Peyrin and S. Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, Heidelberg, Dec. 2018.

[8] A. Coladangelo, J. Liu, Q. Liu, and M. Zhandry. Hidden cosets and applications to unclonable cryptography. In T. Malkin and C. Peikert, editors, *CRYPTO 2021, Part I*, volume 12825 of *LNCS*, pages 556–584, Virtual Event, Aug. 2021. Springer, Heidelberg.

[9] J.-M. Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291, 2006. `https://eprint.iacr.org/2006/291`.

[10] C. Crépeau, F. Légaré, and L. Salvail. How to convert the flavor of a quantum bit commitment. In B. Pfitzmann, editor, *EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 60–77. Springer, Heidelberg, May 2001.

[11] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory*, 22(6):644–654, 1976.

[12] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and D. Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 10–18. Springer, Heidelberg, Aug. 1984.

[13] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *21st ACM STOC*, pages 25–32. ACM Press, May 1989.

[9] This is a simplified claim and some subtle issues about uniformness of the adversary and "infinitely-often security" are omitted here. See the full version for the formal statement.

[14] I. Haitner and O. Reingold. Statistically-hiding commitment from any one-way function. In D. S. Johnson and U. Feige, editors, *39th ACM STOC*, pages 1–10. ACM Press, June 2007.

[15] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SIAM J. Comput.*, 28(4):1364–1396, 1999.

[16] R. Impagliazzo. A personal view of average-case complexity. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference, Minneapolis, Minnesota, USA, June 19-22, 1995*, pages 134–147. IEEE Computer Society, 1995.

[17] Z. Ji, Y. Qiao, F. Song, and A. Yun. General linear group action on tensors: A candidate for post-quantum cryptography. In D. Hofheinz and A. Rosen, editors, *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 251–281. Springer, Heidelberg, Dec. 2019.

[18] H.-K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997.

[19] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414, 1997.

[20] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, Jan. 1991.

[21] J. Yan. General properties of quantum bit commitments. In *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part IV*, pages 628–657. Springer, 2023.

[22] M. Zhandry. Quantum lightning never strikes the same state twice. In Y. Ishai and V. Rijmen, editors, *EUROCRYPT 2019, Part III*, volume 11478 of *LNCS*, pages 408–438. Springer, Heidelberg, May 2019.

Stream privacy amplification for quantum cryptography

Yizhi Huang,[1] Xingjian Zhang,[1] and Xiongfeng Ma[1,*]

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

Abstract. Privacy amplification is the key step to guarantee the security of quantum communication. The existing security proofs require accumulating a large number of raw key bits for privacy amplification. This is similar to block ciphers in classical cryptography that would delay the final key generation since an entire block must be accumulated before privacy amplification. Moreover, any leftover errors after information reconciliation would corrupt the entire block. By modifying the security proof based on quantum error correction, we develop a stream privacy amplification scheme, which resembles the classical stream cipher. This scheme can output the final key in a stream way, prevent error from spreading, and hence can put privacy amplification before information reconciliation. The stream scheme can also help to enhance the security of trusted-relay quantum networks and improve the practicality of randomness extraction for quantum random number generators.

I. INTRODUCTION

Quantum key distribution (QKD) aims at generating information-theoretic secure key strings between two distant parties by exploiting properties of quantum mechanics [1, 2]. The postprocessing of QKD can be divided into quantum bit error correction and phase error correction [3], corresponding to information reconciliation and privacy amplification [4]. Between them, privacy amplification is the key step to guarantee the security of quantum communication [5, 6]. The existing security proofs require accumulating a large number of raw key bits for privacy amplification. This is similar to block ciphers in classical cryptography that would delay the final key generation since an entire block must be accumulated before privacy amplification. Moreover, any leftover errors after information reconciliation would corrupt the entire block.

To solve these problems, we reexamine the security proof for QKD based on quantum error correction [3], where privacy amplification is reduced from phase error correction [4]. As a clear and simple showcase, we mainly focus on the Bennett-Brassard-1984 QKD protocol (BB84) [1] and go back to the original security proof by Lo and Chau [3]. By rearranging the phase error correcting gates and error syndrome measurement, we divide privacy amplification into two steps: (a) generate pseudo-random bits from a pre-shared key seed and a hash function; (b) XOR the pseudo-random string from (a) and the reconciled key. We also prove that the hashing matrix in (a) can be reused. Then, Alice and Bob can generate pseudo-random bits offline. For real-time privacy amplification, they only need to perform the XOR operation in a bitwise manner. In the spirit of stream ciphers, the new scheme is conceptually different from the existing block privacy amplification schemes. Such an essential difference guarantees the new scheme with the following practical features: 1. it can output final key bits in a stream way; 2. it will not spread the errors of the input bit stings; 3. it can be carried out before information reconciliation.

II. SKETCH OF THE NEW REDUCTION

Our new reduction is based on the security proof for QKD using quantum error correction [3], in which the two communication parties, Alice and Bob, can apply the quantum circuit shown in Figure 1 to do the quantum bit and phase error correction and get information-theoretic secure key strings. We can further reduce the procedure to a prepare-and-measure one by moving the final measurement to the front of quantum error correction following the spirit of Shor-Preskill's security proof [4]. Then, bit error correction becomes classical bilateral error correction and phase error correction becomes privacy amplification. Due to the joint measurement introduced in the security proof, each final key bit depends on the measurement results from all the n qubits. Hence, for privacy amplification, Alice and Bob need to wait for all the quantum states to be transmitted and measured in a QKD session. We call it *block* privacy amplification.

Here, to render stream privacy amplification, we rearrange the reduction of the phase error correcting gates and keep the individual Z-basis measurements in the quantum phase error correction. The key idea of our new reduction is to cancel all the Hadamard gates in quantum phase error correction, shown in Figure 1. The CNOT gate in the circuit always appears in pairs on Alice's and Bob's sides. We focus on one pair of CNOT gates in quantum phase error correction part, as depicted in Figure 2(a). The main steps of reduction are as follows:

1. Noticing $H^2 = I$, we add two consecutive Hadamard gates after each output qubits of the CNOT gate.

2. The four Hadamard gates before and after each CNOT gate exchange the roles of control and target qubits, $H^{\otimes 2} C_{\alpha\beta} H^{\otimes 2} = C_{\beta\alpha}$, where $C_{\alpha\beta}$ denotes a CNOT gate with control qubit α and target qubit β and $C_{\beta\alpha}$ is the other way around.

3. For Bob's data qubit, the phase-error correcting operator I/σ_x becomes I/σ_z since $\sigma_z = H\sigma_x H$, as shown in Figure 2(b).

4. Since the new phase-error correcting operator I/σ_z does not affect the Z-basis measurement, it can be skipped along with the error syndrome measurements on the ancillary qubits. The rest operations commute with the dephasing operation, $\Delta_{Z^{\otimes n}}$. Alice and Bob can add Z-basis measurements on ancillary qubits after the CNOT gates, since they are irrelevant at that point.

5. Finally, Alice and Bob can move the final measurement before quantum error correction, as shown in Figure 2(c).

So far, we only consider one CNOT gate. The hash operation in phase error correction shown in Figure 1 is composed of many CNOT gates. This reduction also works for the general hash operation case. With this argument, by inserting consecutive Hadamard gates $H^2 = I$ after each CNOT gate of phase error correction part in Figure 1, we can reduce the whole quantum error correction circuit to the "measurement + postprocessing" case, as shown in Figure 2(d).

With the new reduction, the final key is determined by single-qubit measurements plus bit flips. The Z-basis measurement on the ancillary EPR pairs would provide Alice and Bob with a secure key *seed*. The bit flips are controlled by the seed and the hashing matrix. Then, the ith final key

* xma@tsinghua.edu.cn

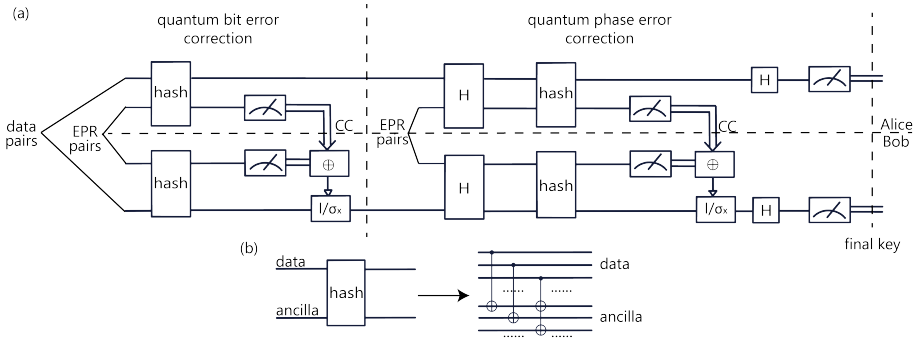


FIG. 1. (a) Quantum bit and phase error correction. The measurements in all the figures are Z-basis measurements by default. "CC" is short for classical communication. The $\oplus$ operation means XOR operations on classical bit strings. H represents the Hadamard gate applied to each of the involved qubits. I/σ_x represents identity or σ_x operation on the qubits depending on the error syndrome. (b) In the linear case, the hash functions can be represented by matrices and realized by a series of CNOT gates between data (as control) and ancillary (as target) qubits. The measurement outcomes of ancillary qubits would give the parity information of the data qubits.

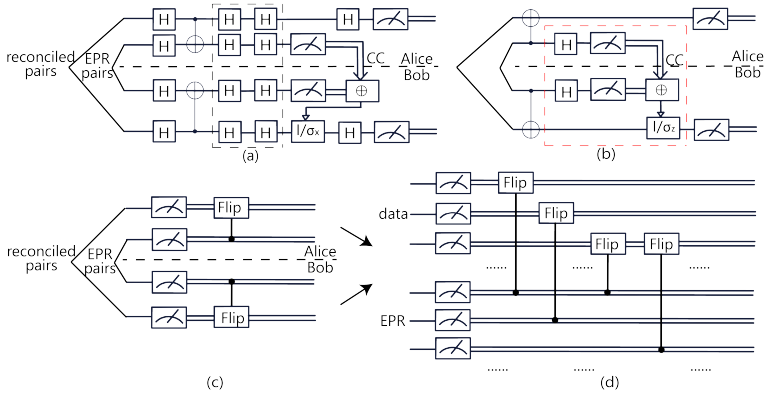


FIG. 2. Circuit (a) is derived from the quantum phase error correction step in Figure 1 by adding Hadamard gates in dashed boxes which form identity operations. We take one pair of CONT operations for illustration. Circuit (b) is equivalent to Circuit (a) by considering the following facts: $H^{\otimes 2}C_{\alpha\beta}H^{\otimes 2} = C_{\beta\alpha}$; $H^2 = I$; $H\sigma_x H = \sigma_z$. Since neither the identity nor the σ_z gate affects the Z-basis measurement, the operations in the dashed box of Circuit (b) are redundant and can be removed. Then by moving the Z-basis measurement on ancillary qubits before hash operation and changing quantum-control-flips to classical-control-flips, Circuit (b) turns into Circuit (c), a "measurement + postprocessing" case. Circuit (d) shows the case of multiple CNOT pairs taking the hashing circuit in Figure 1 (b) as an example. In the end, both Alice and Bob employ Circuit (d) to get final key strings.

bit, extracted from the ith data qubit, is independent of the other data qubits. Hence, the new procedure can output the final key in a stream, i.e., the users can get a secure key bit once a pair of raw key bits is reconciled successfully between Alice and Bob. Following the name of stream cipher in classical cryptography, we call it *stream* privacy amplification, as presented in Box 1. The hashing matrix M in Step 1 is the transpose of the original hashing matrix used in the quantum phase error correction phase of Figure 1, because the original hashing matrix acts on X basis while M acts on Z basis.

Box 1: Stream privacy amplification

After information reconciliation, denote Alice and Bob's reconciled key as $\vec{a} \in \{0,1\}^n$.

1. Alice and Bob randomly choose a hashing matrix M of size $nh(e_p) \times n$.
2. Alice and Bob use an $nh(e_p)$-bit seed, $\vec{d} \in \{0,1\}^{nh(e_p)}$, to generate a pseudo-random string, $\vec{d}\cdot M$, where the dot product between the row vector and the matrix need to take modulo 2 addition.
3. The final key is given by $\vec{k} = \vec{d}\cdot M \oplus \vec{a}$.

Note that in Step 1, Alice and Bob can generate an identical random hashing matrix locally with a pre-shared key and never reveal it to public. Then, they can prepare this matrix and the pseudo-random string (Step 2) before quantum transmission. A naive implementation of this approach, in which Alice and Bob generate M and $\vec{d}$ in each run of the privacy amplification, could consume too many pre-shared secure bits, as for most of the universal hashing matrices, the number of random bits required to generate the matrix is larger than the data size n. Fortunately, with the following theorem, Alice and Bob can reuse the private hashing matrix in multiple QKD sessions with a failure probability increasing linearly, satisfying the composable security definition [7, 8]. Since the failure probability can be exponentially small, the same hashing matrix can be used for many QKD sessions. Therefore, the cost of generating this hashing matrix is shared with these sessions, making the average cost negligible.

Theorem 1 (Reuse of hashing matrix in privacy amplification)**.** *Given a QKD session, the failure probability of a randomly chosen hashing matrix for privacy amplification is upper bounded by ε. Then, for m QKD sessions, if Alice and Bob applies the same randomly chosen matrix for each session, the probability that privacy amplification fails in at least one session is upper bounded by $m\varepsilon$.*

III. POSSIBLE APPLICATIONS AND ADVANTAGES

Firstly, our new scheme can work for any block size in both QKD and quantum random number generator (QRNG) implementations. In order to make privacy amplification efficient, Alice and Bob can employ a large data size without causing delays in real-time key generation. Compared with the previous ones, the unique feature of the new scheme — stream output — can make QKD more practical in scenarios like the satellite-to-ground link [9].

Besides, Alice and Bob can perform Steps 1 and 2 in Box 1 and prepare the pseudo-random string in advance before running QKD/QRNG sessions. They only need to run Step 3 in privacy amplification during real-time QKD, which is essentially composed of simple XOR operations and much faster than hash operations. In block privacy amplification, the computational complexity of the matrix multiplication with Toeplitz hashing is $O(n \log n)$ with the fast Fourier transform algorithm, where n is the length of reconciled key string [10, 11]. In contrast, the computational complexity of Step 3 is n and hence stream privacy amplification is faster in real-time QKD and QRNG, especially when the data size is large. At this point, we also do a numerical experiment of quantum random number extraction using 131Mb raw data [12]. The results show that, our stream scheme only takes less than *0.38s* in real-time processing, while the conventional block scheme takes more than *380s*.

Moreover, the bit-error locations in the input string will remain the same after stream privacy amplification since the final key bit is only decided by the pseudo-random bit and the raw key bit at the same location. As a result, the errors will not spread out, and then privacy amplification can even be performed before information reconciliation. This feature increases flexibility of data postprocessing. For example, privacy amplification and information reconciliation can be performed in parallel. The recently proposed scenario of distributed private randomness distillation [13] is also a potential application of our scheme.

Our stream privacy amplification scheme can also be combined with with delayed privacy amplification to further reduce the trustworthiness of intermediate relays [14, 15]. After information reconciliation, all relays swap the keys by announcing the XOR results of two neighboring keys. Then, Alice and Bob would share a reconciled key string $\vec{a}$, which is also known to relays. Notice that Alice and Bob perform the steps in Box 1 locally. In particular, in Step 2, they generate the pseudo-random string $\vec{d} \cdot M$ privately. Hence, the relays cannot know the final key without $\vec{d} \cdot M$. If the relays want to learn the final key, they need to figure out $\vec{d}$ and M. The seed $\vec{d}$ is private and changes in every QKD session. The hashing matrix M, on the other hand, is reused for many sessions in stream privacy amplification, so the relays might figure it out from final and reconciled key strings in past sessions by methods like differential cryptanalysis. These analysis methods often consume a lot of computational resources. For an even higher security level with fewer assumptions on the relays, we can add another layer of security based on the computational complexity on intermediate nodes. In practice, this combined scheme further reduces the requirement of the trustworthiness of relays and enhances the security of trusted-relay QKD networks.

IV. CONCLUSION AND OUTLOOK.

In this work, we propose a stream privacy amplification scheme, where Alice and Bob locally generate a pseudo-random bit string and XOR it with the reconciled key to get the final key. This scheme has a stream output feature and hence can prevent unpleasant delay and error spreading in practice. We need to emphasize that although we reduce the stream privacy amplification from the Lo-Chau security proof, the technique is independent of security proofs. Other security proof methods, such as Koashi's complementarity approach [16], can also be easily extended to the stream privacy amplification case. Moreover, the concept is rather generic and can be applied to other QKD schemes. The practical issues would also affect the parameter settings of stream privacy amplification, especially the length of the seed string and the size of the hashing matrix. One can combine the new scheme with existing analysis methods to deal with these practical issues, such as the Gottesman-Lo-Lütkenhaus-Preskill framework [17]. The further applications of stream privacy amplification in other quantum cryptography tasks like quantum oblivious transfer [18, 19] are also worth studying.

Here, our proof is mainly based on phase-error correction. According to [20], this approach is equivalent to the one based on the quantum leftover hashing lemma [21] in general. It is an interesting direction to reconsider our scheme from the entropic point of view.

Due to the similarity between our security analysis and stream cipher in classical cryptography, our new scheme also inspires a new perspective to examine classical encryption algorithms information theoretically through quantum information theories. Rigorous assessment of classical encryption algorithms, such as AES and lattice-based encryption, is often a formidable challenge. To our best knowledge, little consideration has been put forward in the context of the information-theoretic study of these encryption algorithms.

The related work is published in [22].

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India, 1984) pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. **17**, 210 (1988).
[6] U. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[7] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, in *Proceedings of the Second International Conference on Theory of Cryptography*, TCC'05 (Springer-Verlag, Berlin, Heidelberg, 2005) pp. 386–406.
[8] R. Renner and R. König, in *Proceedings of the Second International Conference on Theory of Cryptography*, TCC'05 (Springer-Verlag, Berlin, Heidelberg, 2005) pp. 407–425.
[9] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, Phys. Rev. Lett. **120**, 030501 (2018).
[10] X. Ma, Z. Zhang, and X. Tan, arXiv preprint arXiv:1109.6147 (2011).
[11] M. Hayashi and T. Tsurumaru, IEEE Trans. Inf. Theory **62**, 2213 (2016).
[12] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, Review of Scientific Instruments **86**, 063105 (2015).
[13] D. Yang, K. Horodecki, and A. Winter, Phys. Rev. Lett. **123**, 170501 (2019).
[14] C.-H. F. Fung, X. Ma, H. F. Chau, and Q.-y. Cai, Phys. Rev. A **85**, 032308 (2012).
[15] W. Stacey, R. Annabestani, X. Ma, and N. Lütkenhaus, Phys. Rev. A **91**, 012338 (2015).

[16] M. Koashi, New J. Phys. **11**, 045018 (2009).
[17] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Info. Comput. **4**, 325 (2004).
[18] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, in *Advances in Cryptology — CRYPTO '91*, edited by J. Feigenbaum (Springer Berlin Heidelberg, Berlin, Heidelberg, 1992) pp. 351–366.
[19] C.-Y. Wei, X.-Q. Cai, B. Liu, T.-Y. Wang, and F. Gao, IEEE Trans Comput **67**, 2 (2017).
[20] T. Tsurumaru, arXiv preprint arXiv:2009.08823 (2020).
[21] R. Renner, Int. J. Quantum Inf. **6**, 1 (2008).
[22] Y. Huang, X. Zhang, and X. Ma, PRX Quantum **3**, 020353 (2022).

Mode-pairing quantum key distribution

Yizhi Huang,[1] Hao-Tao Zhu,[2,3,4] Hui Liu,[2,3,4] Pei Zeng,[2,3,4] Mi Zou,[2,3,4] Hongyi Zhou,[1] Yunqi Dai,[5] Shibiao Tang,[5] Hao Li,[6] Lixing You,[6] Zhen Wang,[6] Yu-Ao Chen,[2,3,4] Xiongfeng Ma,[1,*] Teng-Yun Chen,[2,3,4,†] and Jian-Wei Pan[2,3,4,‡]

[1] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*
[2] *Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China*
[3] *CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*
[4] *Hefei National Laboratory, University of Science and Technology of China, Hefei, Anhui 230088,China*
[5] *QuantumCTek Corporation Limited, Hefei, Anhui, China*
[6] *State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai, China*

Abstract. In the last two decades, quantum key distribution networks based on telecom fibers have been implemented at metropolitan and intercity scales. However, a major hurdle is the exponential decay of the key rate with increasing transmission distance. Recently proposed schemes aim to overcome this limitation by utilizing long-arm single-photon interferometers between communication parties. However, the technical challenge of achieving phase-locking between independent lasers remains. To address this challenge, we propose a mode-pairing measurement-device-independent quantum key distribution scheme. This scheme determines the encoded key bits and bases during post-processing, eliminating the need for global phase-locking. By employing two off-the-shelf lasers, we achieve a quadratic improvement in key-rate performance compared to conventional measurement-device-independent schemes for metropolitan and intercity distances. Additionally, for longer distances, we significantly enhance the key rate by three orders of magnitude using 304 km commercial fiber and 407 km ultra-low-loss fiber. We expect this ready-to-implement high-performance scheme to be widely used in future intercity quantum communication networks. The MP scheme and its experimental demonstration presented here are elaborated upon in our associated publications [1, 2].

Quantum key distribution (QKD) [3, 4], as a building block of quantum networks, allows remote communication parties to establish a secure key based on the laws of quantum physics [5, 6]. Currently, many QKD networks of various sizes have been implemented worldwide, such as metropolitan and intercity scales. For a metropolitan network, the loss budget between two nodes is around 10 dB. Usually, the network users are connected to trusted nodes as service providers. For an intercity network, the single-link loss is typically 20 dB. Often, we need to set up trusted relays outside of cities. In practice, when one of the trusted nodes is compromised, the network security can be severely damaged. Also, it is difficult and expensive to ensure the security of relay nodes outside cities. Moreover, due to the complicated construction of single-photon detectors, imperfect detection devices would introduce security loopholes.

To close the detection loopholes and reduce the number and cost of trusted nodes, Lo et al. proposed measurement-device-independent quantum key distribution (MDI-QKD) [7]. In a generic MDI-QKD setup, the two communication parties, Alice and Bob, emit encoded laser pulses to a detection site, owned by an untrusted party, Charlie. Charlie employs an interferometer as a quantum relay to correlate the received quantum signals. Charlie announces interference measurement results, based on which Alice and Bob can extract secure key bits. The security of MDI-QKD requires no assumption on how Charlie performs measurement and announcement, making it naturally immune to all the detection attacks.

The main bottleneck of the practical implementation of QKD networks lies in the exponential decay of the key rate with respect to the transmission distance. In the conventional MDI-QKD schemes, Alice and Bob encode information into two optical modes, such as two adjacent pulses [8]. This type of encoding, namely two-mode encoding, is relatively simple to implement since it does not require additional devices and modulation. However, the performance of two-mode encoding schemes is limited by the overall channel transmittance η. Another type of MDI-QKD, twin-field QKD [9], can achieve a quadratic improvement in the key rate. We refer to this as one-mode encoding. In one-mode encoding schemes, Alice and Bob encode information into a single optical pulse, and then Charlie performs a single-photon interference to correlate pulses from two users. This type of encoding, however, is highly sensitive to environmental noise. Thus, one has to stabilize the phases between the

* xma@tsinghua.edu.cn
† tychen@ustc.edu.cn
‡ pan@ustc.edu.cn

lasers at the two user ends using global phase-locking techniques to realize these QKD schemes [10–12], which remains challenging and impractical for large-scale applications. From the comparison of the existing MDI-QKD schemes above, it seems that we cannot simultaneously enjoy the advantages of one-mode schemes (i.e., quadratic improvement in successful detection) and two-mode schemes (i.e., stable optical interference), due to an intrinsic trade-off between the information-encoding efficiency and robustness.

To achieve both high performance and simple implementation, we propose a mode-pairing (MP) MDI-QKD scheme, which a hybrid encoding method. We give a detailed description of the MP scheme in Box 1.

Box 1: Mode-pairing scheme

1. **State preparation:** In the i-th round ($i = 1, 2, ..., N$), Alice prepares coherent state $\left|\sqrt{\mu_i^a}\exp(\mathrm{i}\phi_i^a)\right\rangle$ on the optical mode A_i with intensity μ_i^a chosen from $\{0, \mu\}$ randomly and phase ϕ_i^a uniformly chosen from $[0, 2\pi)$. Similarly, Bob randomly chooses μ_i^b, ϕ_i^b and prepares $\left|\sqrt{\mu_i^b}\exp\left(\mathrm{i}\phi_i^b\right)\right\rangle$ on mode B_i.

2. **State transmission and measurement:** Alice and Bob send the pulses on modes A_i and B_i, respectively, to Charlie, who is supposed to perform the single-photon interference measurement and announces the clicks of detectors L and/or R.
Alice and Bob repeat the above two steps for N rounds. Then, they postprocess the data as follows.

3. **Mode pairing:** For all rounds with successful detection, in which one and only one of the two detectors clicks, Alice and Bob apply a strategy of grouping two clicked rounds as a pair. The encoded phases and intensities in these two rounds form a data pair. The detailed pairing strategy can be found in [1].

4. **Basis assignment:**Based on the intensities of the two paired rounds indexed by i and j, Alice labels the 'basis' of the data pair as Z if the intensities are $(0, \mu)$ or $(\mu, 0)$, as X if the intensities are (μ, μ), or as '0' if the intensities are $(0, 0)$. Bob sets the basis using the same method. Alice and Bob announce the basis of each data pair. If they both announce the basis X or Z, they maintain the data pairs, whereas otherwise, the data pairs are discarded.

5. **Key mapping:** For each Z-pair on location i, j, Alice sets her key to $\chi_a = 0$ if the intensity of the i-th pulse is $\mu_i^a = 0$ and $\chi_a = 1$ if $\mu_j^a = 0$. For each X-pair on location i, j, the key is extracted from the relative phase, $\chi_a = \lfloor(\phi_j^a - \phi_i^a)/\pi \mod 2\rfloor$ and Alice announces $\theta_a = (\phi_j^a - \phi_i^a) \mod \pi$. Bob also assigns his raw key bits χ_b and announces θ_b. The only difference is that, for Z-pairs Bob sets the raw key bit χ_b to be 1 if $\mu_i^b = 0$ and $\chi_b = 0$ if $\mu_j^b = 0$. As an extra step on the X-pairs, if Charlie's detection announcement is (L, L) or (R, R), Bob keeps the bit χ_b; otherwise, if Charlie's announcement is (L, R) or (R, L), Bob flips χ_b. For the X-pairs, if $\theta_a = \theta_b$, Alice and Bob keep the key; otherwise, they discard it.

6. **Parameter estimation:** Alice and Bob use Z-pairs with different intensity settings to estimate the number of clicked single-photon pairs M_{11}^Z using the decoy-state method. The X-pairs are used to estimate the single-photon phase error rate $e_{11}^{Z,ph}$. They also record the total number and the quantum bit error rate of the Z-pairs, denoted as $M_{\mu\mu}$ and $E_{\mu\mu}$, respectively.

7. **Key distillation:** Alice and Bob use the (μ, μ)-pairs to generate key bits. They perform error correction and privacy amplification according to the key rate formula evaluated by M_{11}^Z, $e_{11}^{Z,ph}$, $M_{\mu\mu}$ and $E_{\mu\mu}$.

The core observation of the MP scheme is that the two optical modes used to encode the relative information can be determined after Charlie's announcement. At the encoding and detecting stage, Alice and Bob only consider a single mode and do not require coincidence detection in predetermined locations. At the postprocessing stage, they generate the raw key bits from two pulses and avoid the global phase-locking requirement. Therefore, the users can achieve a quadratic improvement in key rate with simple hardware implementation.

The final key length of the MP scheme is given by,

$$K = M_{11}^Z\left[1 - h\left(e_{11}^{Z,ph}\right)\right] - fM_{\mu\mu}h\left(E_{\mu\mu}\right), \qquad (1)$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is binary entropy function and f is the error correction efficiency. The single-photon component of the Z-basis pairs, M_{11}^Z, and the corresponding phase error rate, $e_{11}^{Z,ph}$, can be estimated by the decoy-state method. The number of pairs used to distill final key bits, $M_{\mu\mu}$, and the bit error rate, $E_{\mu\mu}$, can be directly obtained from the experiment.

By adopting two off-the-shelf lasers, we realize this high-performance MDI-QKD without global phase locking. To this end, we adjust the original MP-QKD proto-

col and introduce phase reference estimation techniques to deal with the frequency fluctuation of two independent lasers. The experimental setup is shown in Fig. 1. Alice and Bob employ the off-the-shelf continuous-wave lasers whose linewidth is 2 kHz and center wavelength is 1550.12 nm. An intensity modulator chops the emitted light into pulses of width 400 ps at 625 MHz. Then, the key and basis information is encoded into these pulses by two Sagnac rings and three phase modulators for different intensities and phases. Afterward, pulses are attenuated to the single-photon level by an electrical variable optical attenuator and transmitted to Charlie for interference detection. We consider the experimental settings under the scenario of metropolitan and intercity quantum networks. Hence, we perform the experiment via 101, 202, 304 km standard and 407 km ultra-low-loss optical fibers. The detailed experiment parameters can be found in [2].

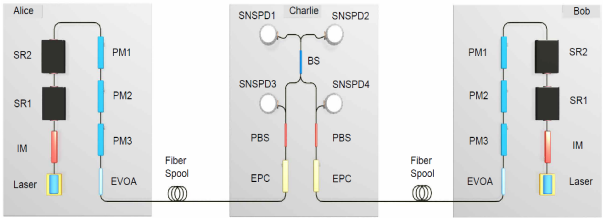


FIG. 1. Experimental setup. Alice's and Bob's setups are identical, but their encoding modulations are independent. The continuous-wave laser is chopped into discrete pulses by an intensity modulator (IM). Then these pulses are randomly modulated into one of the four intensities — strong, signal, decoy, and vacuum pulses — with the aid of two Sagnac rings (SR1, SR2). Three phase modulators (PM1, PM2, PM3) are used for phase encoding and active phase randomization. The encoded pulses are attenuated to the single-photon level by an electrical variable optical attenuator (EVOA) and transmitted to Charlie. Before interference measurements, the pulse polarisation is aligned by an electric polarization controller (EPC) and a polarization beamsplitter (PBS). Finally, the signals are detected by superconducting nanowire single-photon detectors (SNSPDs). SNSPD1 and SNSPD2 are used for interference detection, and SNSPD3 and SNSPD4 are used for polarization feedback and arriving time feedback. Note that we do not carry out any phase-locking operations in the setup. Note that we do not carry out any phase-locking operations in the setup.

The key rates for different transmission distances are presented in Fig. 2. Here, the Z-basis error rate is in the order of 10^{-4} with the two Sagnac rings and the intensity modulator, giving over 40 dB of extinction ratio for the signal and vacuum states. We also compare the experimental results with numerical simulations along with previous experiments. As shown in the key-rate figure, under the intercity communication distances (101 km and 202 km), the key rate-transmittance relation of our system follows $R = O(\sqrt{\eta})$ rather than $O(\eta)$, indicating a quadratic improvement in the key rate.

For longer communication distances, even with higher X-basis error rates caused by larger phase fluctuations,

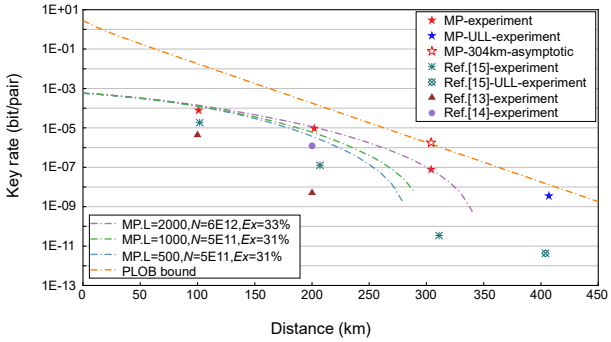


FIG. 2. Key-rate performance. The experimental rate–distance performance of MP-QKD, compared with the theoretical simulations, along with the existing two-mode MDI-QKD experimental results [14–16] and the linear key rate bound. Data points marked by red and blue stars are key rates of our system using commercial fibers and ultra-low loss (ULL) fibers, respectively. We also show the key rate for the 304 km asymptotic case based on the experimental results, which is marked by the white star.

the system can still maintain a key rate-transmittance relationship well above $R = O(\eta)$. Our system realizes key rates of 19.2 and 0.769 bits per second, respectively, via 304 km and 407 km fibers, three orders of magnitude higher than those of the existing MDI-QKD experiments [16]. Besides, we give the key rate of the 304km asymptotic case based on the experimental data in the figure and show that our system has the potential to break the linear bound [17].

Our experiment shows that the MP-QKD scheme owns clear advantages over the existing MDI-QKD implementations, especially in the regime of metropolitan and intercity distances. We anticipate the MP-QKD system and similar designs to improve the performance of quantum communication networks. Also, we expect that the design of the MP-QKD experiment will be helpful for the construction of quantum repeaters, as well as extending the reach of the quantum internet.

[1] P. Zeng, H. Zhou, W. Wu, and X. Ma, Nature Communications **13**, 3903 (2022).
[2] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, Z. Wang, Y.-A. Chen, X. Ma, T.-Y. Chen, and J.-W. Pan, Phys. Rev. Lett. **130**, 030801 (2023).
[3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems*

and Signal Processing (IEEE Press, New York, 1984) pp. 175–179.
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[8] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[9] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Nature **557**, 400 (2018).
[10] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **124**, 070501 (2020).
[11] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, *et al.*, Nature Photonics **14**, 422 (2020).
[12] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, *et al.*, Nat. Photon. **15**, 570 (2021).
[13] Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, Phys. Rev. A **95**, 012333 (2017).
[14] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, Optica **7**, 238 (2020).
[15] R. I. Woodward, Y. Lo, M. Pittaluga, M. Minder, T. Paraiso, M. Lucamarini, Z. Yuan, and A. Shields, NPJ Quantum Inf. **7**, 1 (2021).
[16] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **117**, 190501 (2016).
[17] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).

Convex optimization for non-equilibrium steady states on a hybrid quantum processor

Jonathan Wei Zhong Lau[*1] [†] Lim Kian Hwee[‡1] [§] Kishor Bharti[2] [¶]
Leong-Chuan Kwek[1] [‖] Sai Vinjanampathy[3] [**]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2] *Institute of High Performance Computing (IHPC), Agency for Science Technology and Research (A*STAR), 1 Fusionopolis Way, #16-16 Connexis, Singapore 138632, Republic of Singapore*
[3] *Centre of Excellence in Quantum Information, Computation, Science and Technology, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India*

Abstract. Finding the transient and steady-state properties of open quantum systems is a central problem in various fields of quantum technologies. Here, we present a quantum-assisted algorithm to determine the steady states of open system dynamics. By reformulating the problem of finding the fixed point of Lindblad dynamics as a feasibility semidefinite program, we bypass several well known issues with variational quantum approaches to solving for steady states. We demonstrate that our hybrid approach allows us to estimate the steady states of higher dimensional open quantum systems and discuss how our method can find multiple steady states for systems with symmetries.

Keywords: Quantum Algorithms, Open Quantum Systems

- arXiv link: https://arxiv.org/abs/2204.03203
- Link to PRL version: https://journals.aps.org/prl/accepted/89070Y9fG231e080555b71d3129c75799282760bc

Introduction.— Understanding open system evolution is central to modern quantum technologies such as computing, thermodynamics [1, 2, 3], chemistry [4], and quantum transport [5]. Since such evolution maps initial quantum states to future states, both transient and steady state properties are available in the structure of the evolution operator. Sparing few analytically tractable systems, generic open system evolution has to be solved numerically to understand both transient and steady state dynamics of the system. Such classical simulation techniques are limited due to the exponential growth of Hilbert space. Some specific sampling problems can be simulated classically [6, 7, 8, 9] and tensor networks can be deployed for scenarios with limited entanglement growth [10, 11, 12, 13, 14, 15, 16, 17]. For generic open system evolution by contrast, such a classical simulation is limited to few dozen qubits in the presence of symmetries. Usually, such problems are either simplified by the presence of strong local dissipators which reduce the amount of entanglement generated or by low dimensionality of the problem. Outside of these special cases, the issue of generic open system evolution has remained unsolved.

Open system dynamics under Born, Markov and secular approximations are often described by a time-local master equation given by $\dot{\rho} = L[\rho]$ where

$$L[\rho] = -i[H,\rho] + \sum_n \gamma_n \left(A_n \rho A_n^\dagger - \frac{1}{2}\{A_n^\dagger A_n, \rho\} \right).$$

Such an evolution preserves conditions for valid density matrices. The transient and steady states of this evolution are characterized by the spectrum of the Liouville superoperator [5], defined by the vectorization $B\rho C \rightarrow C^* \otimes B\,|\rho\rangle$. Steady states are understood to satisfy $L[\rho] = 0$ or equivalently $\mathcal{L}\,|\rho\rangle = 0$, where $\mathcal{L}$ is the Liouville superoperator that arises from the vectorisation of L. Since these steady states do not usually correspond to a thermal equilibrium, they are referred to as non-equilibrium steady states (NESS). We refer to the problem of obtaining the steady state(s) of a given Liouville evolution as the NESS problem, which is solved classically by matrix diagonalization. However, due to the increase in dimensionality, diagonalization of the full spectrum is usually unfeasible. Furthermore, the evolution of n-dimensional density matrices in Liouville space are represented by $n^2 \times n^2$ matrices. This squared dimensionality implies that numerical techniques can find the entire spectrum of only modest open quantum systems, usually relying on Arnoldi type methods [18, 19, 20, 21], which become quite cumbersome for many-body systems of moderate size.

In this paper, we propose a hybrid algorithm for the determination of NESS. Through our approach, the steady state problem can be recast as solving a feasibility semidefinite program (SDP) [22, 23, 24]. We show that such an approach to find the NESS is viable on a NISQ device. Our first contribution is to restate the NESS problem as a feasibility SDP, which is an SDP where the goal is to find a feasible solution satisfying the positive semidefinite and linear constraints [22, 23, 24]. Our second contribution is that we do not use a variational quantum state/circuit as the ansatz [25, 26, 27, 28]. By

*Equal contribution
†E0032323@u.nus.edu
‡Equal contribution
§E0014608@u.nus.edu
¶bharti_kishor@ihpc.a-star.edu.sg
‖cqtklc@gmail.com
**sai@phy.iitb.ac.in

doing so, we bypass the problems [29, 30, 31, 32] associated with training variational quantum algorithms with their non-convex landscape, which is known to be non-deterministic polynomial-time (NP) hard [33, 34, 35]. We show that our algorithm naturally enforces positivity constraint of a physical density matrix and provides methods to enforce additional constraints systematically while retaining the advantages of quantum-assisted methods [36, 37, 30, 38, 32], like providing a method to systematically gain a more expressible, problem aware ansatz.

Quantum Feasibility SDP Approach.— We circumvent the non-convex optimization problem in the Liouville space by optimizing over the convex set of density matrices. This allows us to directly apply a feasibility SDP, one consequence of which is that we can now systematically enforce the positive semidefinite condition. A feasibility SDP admits the following form: Find X, $X \in S_+^l$, such that $\mathrm{Tr}(C_k X) = v_k$, $\forall k \in 1, 2, \ldots c$. Here, $\mathcal{S}_+^l$ represents the set of $l \times l$ symmetric PSD matrices. This is the problem of determining if it is possible to find a matrix X subject to the PSD constraint and the other given constraints. The matrices C_k belong to the set of symmetric matrices $\mathcal{S}^l$ for $k \in \{1, 2, \cdots c\}$. The k-th element of vector $v \in \mathbb{R}^c$ is denoted by v_k. SDPs can be formulated for complex-valued matrices via a cone of Hermitian positive semidefinite matrices i.e. $X \in \mathcal{H}_+^l$. Since SDPs for real valued matrices are a special case of SDPs for complex-valued matrices, we will consider the latter case in this paper. Since $\dot{\rho} = L[\rho]$ is linear in ρ, the NESS problem is a feasibility SDP.

We consider a state ansatz of the form

$$\rho = \sum_{i,j} \beta_{ij} \left|\chi_i\right\rangle \left\langle\chi_j\right| . \tag{1}$$

Here, β_{ij} are matrix elements of a positive semidefinite matrix β, whereas $|\chi_i\rangle$ states can be from any set of quantum states. We see that β being positive semidefinite is both a necessary and sufficient condition for ρ to be positive semidefinite. The condition $\mathrm{Tr}\,(\rho) = 1$ becomes $\mathrm{Tr}\,(\beta E) = 1$, where E is a matrix with matrix elements $E_{ij} = \langle\chi_i|\chi_j\rangle$.

With the chosen ansatz, the NESS problem becomes

$$\text{Find } \beta \text{ s.t.} - i(D\beta E - E\beta D)$$
$$+ \sum_n \gamma_n \left(R_n \beta R_n^\dagger - \frac{1}{2} F_n \beta E - \frac{1}{2} E \beta F_n \right) = 0, \tag{2}$$
$$\beta \succcurlyeq 0, \tag{3}$$
$$\mathrm{Tr}(\beta E) = 1, \tag{4}$$

where γ_n are the strengths of the dissipators, D, R, F are matrices defined as $D_{ij} = \langle\chi_i|H|\chi_j\rangle$, $(R_n)_{ij} = \langle\chi_i|A_n|\chi_j\rangle$ and $(F_n)_{ij} = \langle\chi_i|A_n^\dagger A_n|\chi_j\rangle$. This reduction of the NESS problem to a feasibility SDP [23] defined over β is motivated by the idea that a judicious choice of the states $|\chi_i\rangle$ in some problem-aware manner could possibly allow us to do an optimisation over a smaller dimensional convex landscape (compared to ρ). Furthermore, the positive semidefiniteness condition of ρ. can be enforced naturally. We utilize CVX [39], that relies on a disciplined convex programming algorithm [40, 41].

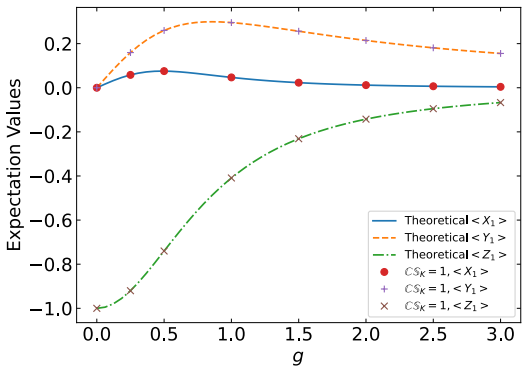


Figure 1: Expectation values for two qubit transverse field Ising model. γs set at 1. Fidelity is equal to 1 for all values of g. Our method gives strong agreement with the theoretical results.

We can also easily enforce additional linear constraints of the form $\mathrm{Tr}(\beta X) = x$, where X and x are arbitrary matrices and values respectively. This feature of our scheme is absent in the existing algorithms for solving NESS on NISQ devices and is further discussed below.

The overlap values for the matrix elements of the E, D, R, F matrices can be measured on a NISQ quantum computer [42]. In general, how we choose the $|\chi_i\rangle$ states to form our ansatz will contribute strongly to how our algorithm scales. For a general Hamiltonian, absent of exploitable symmetries, the size of the optimal ansatz will grow exponentially with the size of the problem. Even in the worst case where we require exponentially large numbers of $|\chi_i\rangle$ states in our ansatz, we do not map the problem to an equivalent one in Liouville space and avoid the aforementioned squared dimensionality that comes from doing optimization in Liouville space. Hence in the worst case, our method is at least quadratically better than analogous variational algorithms.

The algorithm can hence be summarised as (a) choose a hybrid ansatz for ρ using a set of chosen quantum states $\{|\chi_i\rangle\}$ (b) calculate the entries of the overlap matrices on the quantum computer, (c) we use the matrices in a SDP optimization routine run on a classical computer to obtain the approximate NESS.

Examples.— We demonstrate our algorithm with some examples. Consider a two qubit transverse field Ising model with the Hamiltonian $H_2 = (1/2)\sigma_Z^1\sigma_Z^2 + g\sigma_X^1 + g\sigma_X^2$, together with local dissipators $A_1 = \sigma_Z^1$, $A_2 = (1/2)(\sigma_X^1 - i\sigma_Y^1)$, $A_3 = \sigma_Z^2$ and $A_4 = (1/2)(\sigma_X^2 - i\sigma_Y^2)$. For all instances presented in Fig. 1, our hybrid algorithm outputs a density matrix ρ that is unit trace, Hermitian, positive semidefinite and that fulfils the NESS condition $\dot{\rho} = 0$. To study the robustness of the algorithm for larger chains, in Fig. 2 we show simulation results for the transverse field Ising model up to eight qubits.

We note that for the model chosen, as g increases, the exact NESS solution has larger rank and is less sparse.

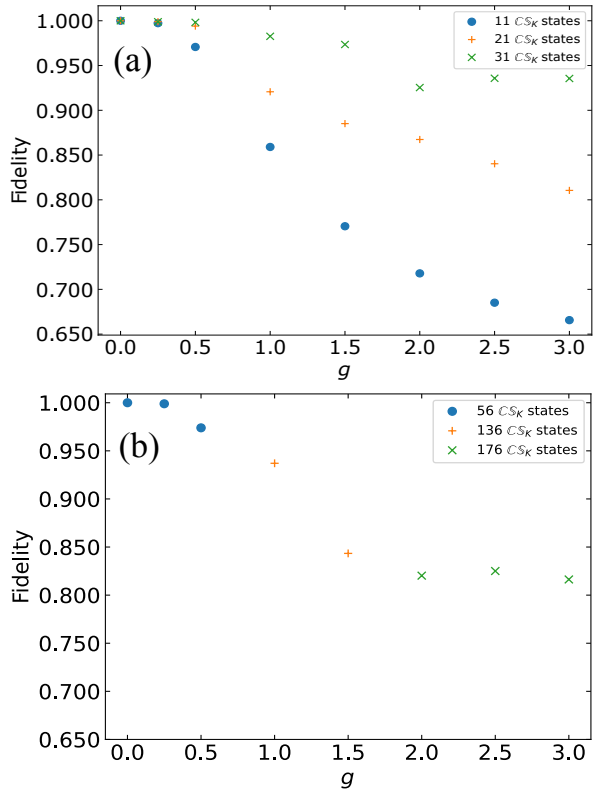


Figure 2: Results for the transverse field Ising model with local dissipators described in the main text. The corresponding fidelity value between the state obtained and the theoretical state, for $\mathbb{CS}_K$ ansatz of different ansatz sizes K, are compared. **a)** Results for 5 qubits. **b)** Results for 8 qubits. For larger g, we note that the exact NESS becomes much less sparse. To continue to obtain good fidelities in this regime, we require larger number of states in our ansatz.

We find that for such situations, a larger ansatz size is needed to obtain an approximate NESS with similar fidelity. We also note that the $\mathbb{CS}_K$ ansatz performs efficiently when the steady states are low rank. When this is not the case, it is expected that any NISQ algorithm based on such ansatzes will underperform.

Strong symmetries.— One additional complication with the NESS problem is that systems with symmetries can exhibit multiple NESS [5]. Our algorithm can also be extended to certain cases where multiple NESSs are expected.

Generalization of our method for multiple NESS.— We can systematically obtain all the physical steady states that exist in all the symmetry subspaces for quantum systems with multiple steady states, if we have knowledge of the full Lindbladian. The simplest way would be to directly construct an ansatz that lies in the desired symmetry subspace. If we have the capacity on the quantum computer to generate such states, which has been demonstrated for Dicke states [43] and states that conserve total magnetization in the XXZ Heisenberg chain [44], we can simply generate such a set of states and use that to construct our hybrid ansatz for our algorithm. This method has the added advantage of reducing the size of the ansatz, due to the reduction of the possible solution space. For example, we use the quantum circuit proposed in [44] for the eight qubit XXZ Heisenberg chain with dephasing noise and obtained a fidelity of nearly 1 to the theoretical NESS in the $m = 4$ symmetry subspace with only 28 states in our ansatz. Here, m is the eigenvalue of the total magnetization operator M. However, this method is limited due to difficulty in devising circuits that conserve a general symmetry. Thus, we also propose two general methods to find multiple NESS.

The first method utilizes the SDP structure of the optimization. For each operator N_k that corresponds to the kth strong symmetry in our system, a NESS is found that is in the symmetry subspace corresponding to a particular eigenvalue n_k of N_k, by including the linear constraint $\mathrm{Tr}(\beta\tilde{N}_k) = n_k$ in the SDP, where $(\tilde{N}_k)_{ij} = \langle\chi_i| N_k |\chi_j\rangle$. These additional linear constraints are additional, efficiently implementable, hyperplanes in the parameter space that the optimizer needs to fulfil.

As an example, we consider a XXZ Heisenberg chain on a system with n qubits, $H_{XXZ} = \sum_{j=1}^{n-1} \sigma_X^j \sigma_X^{j+1} + \sigma_Y^j \sigma_Y^{j+1} + \Delta\sigma_Z^j \sigma_Z^{j+1}$, and dephasing noise, defined by the n jump operators $L_i = \sigma_Z^i$. The total magnetization $M = \sum_{i=1}^{n} \sigma_Z^i$ commutes with the Hamiltonian and all jump operators L_i, generating a strong symmetry given by $S_z = e^{i\phi M}$. This gives rise to $n + 1$ magnetization blocks, each associated with an eigenvalue of M and has its own unique NESS.

Considering the additional constraint $\mathrm{Tr}(\beta\tilde{M}) = m$, where $\tilde{M}_{ij} = \langle\chi_i| M |\chi_j\rangle$, our first method is able to obtain a solution which is in the m magnetization symmetry sector of M that agrees with the exact results. We emphasize that the usage of the quantum computer scales linearly with the number of constraints, as we do not need to measure the D, E, F, R matrices several times.

The second method does not require us to add additional constraints into the SDP, which allows our classical post processing to be more numerically stable. It utilizes the structure of a Vandermonde matrix to systematically remove the contributions from unwanted subspaces by applying the symmetry operator to the state.

References

[1] Frauke Schwarz, Ireneusz Weymann, Jan von Delft, and Andreas Weichselbaum. Nonequilibrium steady-state transport in quantum impurity models: A thermofield and quantum quench approach using matrix product states. *Phys. Rev. Lett.*, 121(13):137702, 2018.

[2] Tatsuhiko N Ikeda and Masahiro Sato. General description for nonequilibrium steady states in periodically driven dissipative quantum systems. *Science advances*, 6(27):eabb4019, 2020.

[3] Shachar Fraenkel and Moshe Goldstein. Entanglement measures in a nonequilibrium steady state: Ex-

act results in one dimension. *SciPost Phys.*, 11:85, 2021.

[4] Alexandra E Raeber and David A Mazziotti. Non-equilibrium steady state conductivity in cyclo [18] carbon and its boron nitride analogue. *Physical Chemistry Chemical Physics*, 22(41):23998–24003, 2020.

[5] D Manzano and PI Hurtado. Harnessing symmetry to control quantum transport. *Advances in Physics*, 67(1):1–67, 2018.

[6] WMC Foulkes, Lubos Mitas, RJ Needs, and Guna Rajagopal. Quantum monte carlo simulations of solids. *Reviews of Modern Physics*, 73(1):33, 2001.

[7] Zheng Yan, Lode Pollet, Jie Lou, Xiaoqun Wang, Yan Chen, and Zi Cai. Interacting lattice systems with quantum dissipation: A quantum monte carlo study. *Phys. Rev. B.*, 97(3):035148, 2018.

[8] Alexandra Nagy and Vincenzo Savona. Driven-dissipative quantum monte carlo method for open quantum systems. *Phys. Rev. A.*, 97(5):052129, 2018.

[9] Alexandra Nagy and Vincenzo Savona. Variational quantum monte carlo method with a neural-network ansatz for open quantum systems. *Phys. Rev. Lett.*, 122(25):250501, 2019.

[10] Michael Zwolak and Guifré Vidal. Mixed-state dynamics in one-dimensional quantum lattice systems: a time-dependent superoperator renormalization algorithm. *Phys. Rev. Lett.*, 93(20):207205, 2004.

[11] Frank Verstraete, Juan J Garcia-Ripoll, and Juan Ignacio Cirac. Matrix product density operators: Simulation of finite-temperature and dissipative systems. *Phys. Rev. Lett.*, 93(20):207204, 2004.

[12] Roman Orus and Guifre Vidal. Infinite time-evolving block decimation algorithm beyond unitary evolution. *Phys. Rev. B.*, 78(15):155117, 2008.

[13] Jian Cui, J Ignacio Cirac, and Mari Carmen Bañuls. Variational matrix product operators for the steady state of dissipative quantum systems. *Phys. Rev. Lett.*, 114(22):220601, 2015.

[14] Albert H Werner, Daniel Jaschke, Pietro Silvi, Martin Kliesch, Tommaso Calarco, Jens Eisert, and Simone Montangero. Positive tensor network approach for simulating open quantum many-body systems. *Phys. Rev. Lett.*, 116(23):237201, 2016.

[15] Adil A Gangat, I Te, and Ying-Jer Kao. Steady states of infinite-size dissipative quantum chains via imaginary time evolution. *Phys. Rev. Lett.*, 119(1):010501, 2017.

[16] Augustine Kshetrimayum, Hendrik Weimer, and Román Orús. A simple tensor network algorithm for two-dimensional steady states. *Nat. Communications*, 8(1):1–7, 2017.

[17] Frank Verstraete, Valentin Murg, and J Ignacio Cirac. Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems. *Advances in physics*, 57(2):143–224, 2008.

[18] Cornelius Lanczos. An iteration method for the solution of the eigenvalue problem of linear differential and integral operators. *J. Res. Natl. Bur. Stand. B*, 45:255–282, 1950.

[19] Walter Edwin Arnoldi. The principle of minimized iterations in the solution of the matrix eigenvalue problem. *Quarterly of applied mathematics*, 9(1):17–29, 1951.

[20] Richard B Lehoucq, Danny C Sorensen, and Chao Yang. *ARPACK users' guide: solution of large-scale eigenvalue problems with implicitly restarted Arnoldi methods*. SIAM, 1998.

[21] Yousef Saad. *Numerical methods for large eigenvalue problems: revised edition*. SIAM, 2011.

[22] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM review*, 38(1):49–95, 1996.

[23] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[24] Henry Wolkowicz, Romesh Saigal, and Lieven Vandenberghe. *Handbook of semidefinite programming: theory, algorithms, and applications*, volume 27. Springer Science & Business Media, 2012.

[25] Nobuyuki Yoshioka, Yuya O Nakagawa, Kosuke Mitarai, and Keisuke Fujii. Variational quantum algorithm for nonequilibrium steady states. *Phys. Rev. R.*, 2(4):043289, 2020.

[26] Huan-Yu Liu, Tai-Ping Sun, Yu-Chun Wu, and Guo-Ping Guo. Variational quantum algorithms for the steady states of open quantum systems. *Chinese Physics Letters*, 38(8):080301, 2021.

[27] Marco Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, et al. Variational quantum algorithms. *Nat. Reviews Physics*, pages 1–20, 2021.

[28] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S Kottmann, Tim Menke, et al. Noisy intermediate-scale quantum (nisq) algorithms. *arXiv preprint arXiv:2101.08448*.

[29] Kishor Bharti, Tobias Haug, Vlatko Vedral, and Leong-Chuan Kwek. Nisq algorithm for semidefinite programming. *arXiv preprint arXiv:2106.03891*.

[30] Tobias Haug and Kishor Bharti. Generalized quantum assisted simulator. *arXiv preprint arXiv:2011.14737*.

[31] Jonathan Wei Zhong Lau, Tobias Haug, Leong Chuan Kwek, and Kishor Bharti. Nisq algorithm for hamiltonian simulation via truncated taylor series. *arXiv preprint arXiv:2103.05500*.

[32] Kian Hwee Lim, Tobias Haug, Leong-Chuan Kwek, and Kishor Bharti. Fast-forwarding with nisq processors without feedback loop. *Quantum Science and Technology*, 2021.

[33] Lennart Bittel and Martin Kliesch. Training variational quantum algorithms is np-hard. *Phys. Rev. Lett.*, 127(12):120502, 2021.

[34] Eric Anschuetz, Jonathan Olson, Alán Aspuru-Guzik, and Yudong Cao. Variational quantum factoring. In *International Workshop on Quantum Technology and Optimization Problems*, pages 74–85. Springer, 2019.

[35] Xuchen You and Xiaodi Wu. Exponentially many local minima in quantum neural networks. In *International Conference on Machine Learning*, pages 12144–12155. PMLR, 2021.

[36] Kishor Bharti. Quantum assisted eigensolver. *arXiv preprint arXiv:2009.11001*.

[37] Kishor Bharti and Tobias Haug. Iterative quantum-assisted eigensolver. *Phys. Rev. A.*, 104(5):L050401, 2021.

[38] Jonathan Wei Zhong Lau, Kishor Bharti, Tobias Haug, and Leong Chuan Kwek. Noisy intermediate scale quantum simulation of time dependent hamiltonians. *arXiv preprint arXiv:2101.07677*.

[39] Michael Grant and Stephen Boyd. Cvx: Matlab software for disciplined convex programming, version 2.1, 2014.

[40] Michael Grant, Stephen Boyd, and Yinyu Ye. Disciplined convex programming. In *Global optimization*, pages 155–210. Springer, 2006.

[41] Michael C Grant and Stephen P Boyd. Graph implementations for nonsmooth convex programs. In *Recent advances in learning and control*, pages 95–110. Springer, 2008.

[42] Kosuke Mitarai and Keisuke Fujii. Methodology for replacing indirect measurements with direct measurements. *Phys. Rev. R.*, 1(1):013006, 2019.

[43] Muthumanimaran Vetrivelan and Sai Vinjanampathy. Near-deterministic weak-value metrology via collective non-linearity. *Quantum Science and Technology*, 7(2):025012, 2022.

[44] Chufan Lyu, Xusheng Xu, Manhong Yung, and Abolfazl Bayat. Symmetry enhanced variational quantum eigensolver. *arXiv preprint arXiv:2203.02444*, 2022.

Theoretical Guarantees for Permutation-Equivariant Quantum Neural Networks

Martín Larocca[1] * Louis Schatzki[1 2] Quynh T. Nguyen[1 3] Frédéric Sauvage[1]
M. Cerezo[1] †

[1] *Los Alamos National Laboratory, Los Alamos, NM 87545, USA*
[2] *University of Illinois Urbana-Champaign, Illinois 61820, USA*
[3] *Harvard University, Cambridge, Massachusetts 02138, USA*

Abstract. Despite the potential of quantum machine learning models, numerous obstacles need to be surmounted, including loss landscapes riddled with barren plateaus and afflicted by numerous local minima. Recently, the nascent field of geometric quantum machine learning (GQML) has emerged as a potential solution to some of those issues. The key insight of GQML is that one should design architectures exploiting the symmetries of the problem at hand. Here, we focus on problems with permutation symmetry and derive a series of remarkable performance results for permutation-equivariant quantum neural networks: absence of barren plateaus, efficient overparametrization, and generalization from few data.

Keywords: Quantum Machine Learning, Geometric Deep Learning, Representation Theory

Introduction. Quantum Machine Learning (QML) holds great potential to accelerate data analysis [1, 2, 3, 4]. Despite its promise, there are several fundamental challenges to overcome, such as designing models which do not incur issues such as barren plateaus [5, 6, 7, 8]. To tackle this challenge, the field of *Geometric QML* (GQML) has been recently developed [9, 10, 11, 12]. GQML is inspired by the tremendous success of *geometric deep learning* in classical machine learning [13, 14, 15, 16], and it provides us with guidelines to create so-called *equivariant Quantum Neural Networks* (QNNs) which encode as inductive biases the underlying symmetries of the problem at hand.

Scope. In this work we argue that S_n-equivariant QNNs do not suffer from most of the issues haunting general QNNs: they do not exhibit barren plateaus, can be efficiently overparametrized, and generalize well with few training points. We argue that the reason behind these gracious features is that the vast geometric priors greatly reduce the circuit expressiveness to the right search space. Taken together, our results provide the first theoretical guarantees for equivariant QNNs and the potential of GQML.

Supervised QML. Here we consider a supervised learning task where we are given repeated access to a *training set* $S = \{\rho_i, y_i\}_{i=1}^N$, where ρ_i are n-qubit quantum states and y_i labels produced by some unknown function $y_i = f(\rho_i)$. We make no assumptions regarding the origins of ρ_i, meaning that these can correspond to classical data embedded in quantum states [17, 18], or to quantum data, i.e., data obtained from some quantum mechanical process [19, 20, 21]. Our goal is to train a model h to produce labels that closely match those of f over the training set (low training error), but also over new data instances (low generalization error). In particular, we parameterize h through a *quantum neural network* (QNN), i.e., a unitary map $\mathcal{U}_{\boldsymbol{\theta}}(\rho) = U(\boldsymbol{\theta})\rho U(\boldsymbol{\theta})^\dagger$ composed of M layers as

$$\mathcal{U}_{\boldsymbol{\theta}} = \mathcal{U}^M_{\theta_M} \circ \cdots \circ \mathcal{U}^1_{\theta_1}\,, \quad \text{where} \quad \mathcal{U}^l_{\theta_l}(\rho) = e^{-i\theta_l H_l}\rho e^{i\theta_l H_l}\,.$$

Here, the layers of the QNN are obtained from some set of Hermitian *generators* $\{H_l\}$, so that $U(\boldsymbol{\theta}) = \prod_{l=1}^M e^{-i\theta_l H_l}$. We assume that h depends on some loss function $\mathcal{L}(\boldsymbol{\theta}; \rho_i) = \text{Tr}[\mathcal{U}_{\boldsymbol{\theta}}(\rho_i)O]$ with O a Hermitian observable. We train the parameters $\boldsymbol{\theta}$ by minimizing an empirical loss function $\hat{L}(\boldsymbol{\theta}) = \sum_{i=1}^N c_i \mathcal{L}(\boldsymbol{\theta}; \rho_i)$.

GQML and label symmetries. As previously mentioned, GQML provides guidelines to incorporates symmetries from the data into h [12]. In particular, we are interested in considering *label symmetries*. Given a compact group G and some unitary representation R acting on quantum states, we say that the label-producing function f has a label symmetry if $f(R(g)\rho R(g)^\dagger) = f(\rho)$ for all $g \in G$. Evidently, when searching for models h to predict outputs of f, it is natural to restrict our search to the space of models that respect such label symmetries. In this context, GQML provides a construc-

*larocca@lanl.gov
†cerezo@lanl.gov

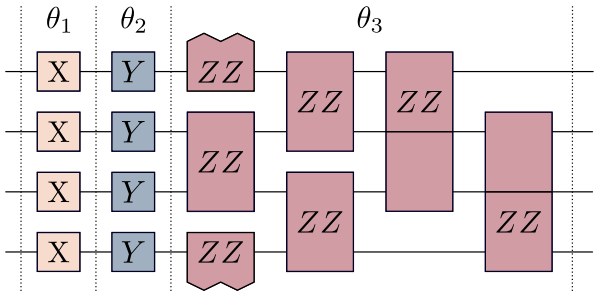


Figure 1: Quantum circuit for an S_n-equivariant QNN. Color represents parameter sharing.

tive approach to create G-invariant models, resting on the concept of *equivariance* [12].

Invariance from equivariance. We say an operator O is G-equivariant iff for all elements $g \in G$, $[O, R(g)] = 0$. A unitary layer $\mathcal{U}$ is G-equivariant iff it is generated by a G-equivariant Hermitian operator. By the previous definition, G-equivariant unitaries are *maps that commute with the action of the group* $\mathcal{U}^l_{\theta_l}(R(g)\rho R(g)^\dagger) = R(g)\mathcal{U}^l_{\theta_l}(\rho)R(g)^\dagger$. Finally, we say an M-layered QNN is G-equivariant if *each* of its layers is equivariant. The previous then provides a recipe to build models whose outputs remain invariant under the action of the group:

Proposition: *Models with equivariant QNNs and measurement operators give rise to invariant models* $\mathcal{L}(\boldsymbol{\theta}; R(g)\rho R(g)^\dagger) = \mathcal{L}(\boldsymbol{\theta}; \rho)$ *for all* $\boldsymbol{\theta}$ *and* ρ.

Permutation symmetry. One of the most widespread symmetries are permutation symmetries. Examples include: learning over a set of elements, problems defined on graphs (such as condensed matter systems), dealing with molecular systems, and evaluating genuine multipartite entanglement. For these problems it is natural to ask the model to be independent of the way we choose to label the individual units.

S_n-equivariant QNNs. We focus on the special case where G is the symmetric group S_n and R is the *qubit-defining* representation that permutes qubits via $R(\pi \in S_n)\bigotimes_{i=1}^n |\psi_i\rangle = \bigotimes_{i=1}^n |\psi_{\pi^{-1}(i)}\rangle$. The following set of generators can be shown to be S_n-equivariant (see Fig. 1)

$$\mathcal{G} = \left\{ \frac{1}{n}\sum_{j=1}^n X_j, \frac{1}{n}\sum_{j=1}^n Y_j, \frac{2}{n(n-1)}\sum_{k<j} Z_j Z_k \right\} . \quad (1)$$

Representation theory interlude. A notable result from representation theory is that given a representation of a group, it decomposes into an orthogonal direct sum of fundamental building-blocks known as *irreducible representations* (irreps). The qubit-defining representation of S_n and the equivariant unitaries take, under some appropriate global change of basis, the block-diagonal form:

$$R(\pi \in S_n) \cong \bigoplus_\lambda \bigoplus_{\mu=1}^{d_\lambda} r_\lambda(\pi) = \bigoplus_\lambda r_\lambda(\pi) \otimes \mathbb{1}_{d_\lambda}, \quad (2)$$
$$U(\boldsymbol{\theta}) \cong \bigoplus_\lambda \mathbb{1}_{m_\lambda} \otimes U_\lambda(\boldsymbol{\theta}) .$$

Here r_λ are m_λ-dimensional irreps of S_n, each of which appears d_λ times. Crucially, the only irreps appearing correspond to two-row *Young diagrams* and can be parametrized by a single integer m, as $\lambda \equiv \lambda(m) = (n-m, m)$, where $m = 0, 1, \ldots, \lfloor \frac{n}{2} \rfloor$. It can be shown that $d_\lambda = n - 2m + 1$ and $m_\lambda = \frac{n!(n-2m+1)!}{(n-m+1)!m!(n-2m)!}$. Since d_λ is in $\mathcal{O}(n)$, whereas some m_λ grow exponentially with the number of qubits, equivariant operators are composed of linear-sized blocks repeated a (potentially) exponential number of times. This hints at the reason why S_n-equivariant models train and generalize well: fully parametrizing them only requires $\sum_\lambda d_\lambda^2 \in \mathcal{O}(n^3)$ real-valued parameters, as opposed to the 4^n required in the universal case.

Barren Plateaus. Barren plateaus are one of the main challenges to the success of QML models using QNNs [1]. When a model exhibits a barren plateau, the loss landscape becomes, on average, exponentially flat and featureless (indicated by $\mathrm{Var}_{\boldsymbol{\theta}}[\partial_\mu \hat{L}(\boldsymbol{\theta})]$ vanishing exponentially with the problem size) [5, 6, 22, 23, 7, 24, 25, 26, 27, 28, 29, 30, 31]. While a great deal of effort has been put forward towards creating strategies capable of mitigating the effect of barren plateaus [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43], the "holy grail" in QML is identifying architectures which are immune to barren plateaus altogether, and thus enjoy trainability guarantees. Examples of such architectures are shallow hardware efficient ansatzes [6], quantum convolutional neural networks [8], and Ising model variational Hamiltonian ansatzes [31, 29]. Here we prove that a new architecture can be added to this list: S_n-equivariant QNNs.

Before continuing, we introduce some notation. Let B^ν_λ be the restriction of an operator B to the copy of an irrep λ indexed by ν. In particular, if B is an equivariant operator one can see that $B^\nu_\lambda = B^{\nu'}_\lambda$. Our first main result is

Theorem 1 *Assuming enough circuit depth M the loss $\hat{L}(\boldsymbol{\theta})$ for an S_n-equivariant QNN and measurement has $\langle \partial_\mu \hat{L}(\boldsymbol{\theta})\rangle_{\boldsymbol{\theta}} = 0$ and*

$$\mathrm{Var}_{\boldsymbol{\theta}}[\partial_\mu \hat{L}(\boldsymbol{\theta})] = \sum_\lambda \frac{2d_\lambda}{(d_\lambda^2-1)^2} \Delta(H_{\mu,\lambda})\Delta(O_\lambda)\Delta(\sum_{\nu=1}^{m_\lambda} \sigma^\nu_\lambda) , \quad (3)$$

where $\Delta(B) = \mathrm{Tr}[B^2] - \frac{\mathrm{Tr}[B]^2}{\dim(B)}$ *and* $\sigma = \sum_i c_i \rho_i$.

We use representation theory to find exact expressions for the terms in Eq. (3).

Theorem 2 *Let A be a S_n-equivariant operator. Then for any $\chi = X, Y, Z$, we have*

$$\begin{cases} \text{If } A = \sum_{j=1}^n \chi_j\,, & \text{then } \Delta(A_\lambda) = 2\binom{d_\lambda+1}{3}\,, \\ \text{If } A = \sum_{k<j} \chi_j \chi_k\,, & \text{then } \Delta(A_\lambda) = \frac{8}{3}\binom{d_\lambda+2}{5}\,, \\ \text{If } A = \prod_{j=1}^n \chi_j & \text{then } \Delta(A_\lambda) = \frac{d_\lambda^2 - 1 + n \bmod 2}{d_\lambda}\,. \end{cases} \tag{4}$$

Here we highlight the crucial fact that when using S_n-equivariant QNNs one can measure *global observables*, i.e., operators acting non-trivially on all qubits such as $\prod_{j=1}^n X_j$, without incurring barren plateaus. This is in stark contrast to other QNN architectures, where global measurements lead to barren plateaus and only local measurements avoid them [6]. From Theorem 1 we then find

Corollary 3 *An equivariant QNN with generators from $\mathcal{G}$ and a measurement from $\mathcal{M}$ will not have barren plateaus if there exists at least one irrep λ such that $\Delta(\sum_{\nu=1}^{m_\lambda} \sigma_\lambda^\nu) \in \Omega(1/\operatorname{poly}(n))$, as then $\mathrm{Var}_{\boldsymbol{\theta}}[\partial_\mu \hat{L}] \in \Omega\left(\frac{1}{\operatorname{poly}(n)}\right)$.*

Note that Corollary 3 holds iff $\Delta(\sum_{\nu=1}^{m_\lambda} \sigma_\lambda^\nu) \in \Omega(1/\operatorname{poly}(n))$. This condition is expected as we do not expect trainability for *any* dataset. In fact similar terms always appear when proving absence of barren plateaus (see [6, 8, 29]). Below we identify scenarios where the S_n-equivariant QNN is trainable but also when it is untrainable.

Overparametrization and generalization. Recently, Ref. [44] proposed a study of overparametrization in the context of QML models, showing that there exists a clear phase transition in the trainability of under- and overparametrized QNNs. Namely, it was shown that below some critical number of parameters (underparametrized) the optimizer greatly struggled to minimize the loss function, whereas beyond that number of parameters (overparametrized) it converged exponentially fast to solutions. A model is overparametrized when the number of parameters M satisfies $M \sim \dim(\mathfrak{g})$. Here $\mathfrak{g}$ is the *Dynamical Lie Algebra* (DLA) given by $\mathfrak{g} = \mathrm{span}(\langle i\mathcal{G}\rangle_{\mathrm{Lie}})$, i.e., the Lie algebra generated by taking all nested commutators of the circuit generators. Intuitively, the DLA controls the expressibility of an ansatz. While most ansatzes have a $\dim(\mathfrak{g}) \in \mathcal{O}(2^n)$ [44], and thus require an exponential number of parameters to be overparametrized, we show that this is not the case for S_n-equivariant QNNs. In fact, only a polynomial number of parameters are required to reach overparametrization:

Theorem 4 *An S_n-equivariant QNN can be overparametrized with $\Theta(n^3)$ parameters.*

Lastly, we also show that S_n-equivariant QNNs should generalize well via a covering net argument. We define the generalization error of a model with parameters $\boldsymbol{\theta}$ as $\mathrm{gen}(\boldsymbol{\theta}) = |\mathcal{L}(\boldsymbol{\theta}) - \hat{\mathcal{L}}(\boldsymbol{\theta})|$., where $\mathcal{L}(\boldsymbol{\theta}) = \mathbb{E}_{\rho\sim P}[c(y)\mathcal{L}_{\boldsymbol{\theta}}(\rho)]$ is the true loss of the model.

Theorem 5 *With probability at least $1-\delta$, for $\boldsymbol{\theta}^*$ some trained set of parameters, we have*

$$\mathrm{gen}(\boldsymbol{\theta}^*) \leq \mathcal{O}\left(\sqrt{\frac{Te_{n+1}}{M}} + \sqrt{\frac{\log(1/\delta)}{M}}\right). \tag{5}$$

Outlook– Ref. [45] recently proposed an algorithm for simulating *certain* S_n-equivariant circuits. However, we note that the claims of this manuscript to not reduce the impact of our work. For instance, the methods in Ref. [45] only work when we can have efficient access to a classical description of both the initial states (data) and measurements (a requirement not needed for our theorems). For example, in the case of graph state encoding, this would amount to some sort of tomography (e.g., we need quantum resources such as the application of a not-near-term Schur-transform circuit) to express the encoded graph state in terms of a basis of the DLA which can be later propagated using the structure constants they derive [46]. Moreover, even in this case the scaling of the 'classical' algorithm is prohibitively expensive (e.g., computing the structure constants is in $\mathcal{O}(n^{15})$). As such, it is not clear what are the relevant, near-term, and realistic cases where the results of [46] hold, but where one could not use an equivariant QNN.

Moreover, we remark that the authors in [46] claim: *Small groups of symmetry leave too large of an effective dimension for the problem to be tractable via quantum computation. On the contrary, very restrictive symmetries render a problem classically tractable. Between these two regions lies an area of promise where quantum computers may offer an advantage.* We want to note that we do not think there is enough evidence to substantiate such a statement, and more work is needed to asses whether S_n-equivariant learning tasks do not hold room for advantage.

Link to the Manuscript:
https://arxiv.org/abs/2210.09974

References

[1] M. Cerezo, G. Verdon, H.-Y. Huang, L. Cincio, and P. J. Coles, Nature Computational Science 10.1038/s43588-022-00311-3 (2022).

[2] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, Nature **549**, 195 (2017).

[3] M. Schuld and N. Killoran, Physical Review Letters **122**, 040504 (2019).

[4] M. Schuld, I. Sinayskiy, and F. Petruccione, Contemporary Physics **56**, 172 (2015).

[5] J. R. McClean, S. Boixo, V. N. Smelyanskiy, R. Babbush, and H. Neven, Nature Communications **9**, 1 (2018).

[6] M. Cerezo, A. Sone, T. Volkoff, L. Cincio, and P. J. Coles, Nature Communications **12**, 1 (2021).

[7] Z. Holmes, K. Sharma, M. Cerezo, and P. J. Coles, PRX Quantum **3**, 010313 (2022).

[8] A. Pesah, M. Cerezo, S. Wang, T. Volkoff, A. T. Sornborger, and P. J. Coles, Physical Review X **11**, 041011 (2021).

[9] M. Larocca, F. Sauvage, F. M. Sbahi, G. Verdon, P. J. Coles, and M. Cerezo, PRX Quantum **3**, 030341 (2022).

[10] J. J. Meyer, M. Mularski, E. Gil-Fuster, A. A. Mele, F. Arzani, A. Wilms, and J. Eisert, arXiv preprint arXiv:2205.06217 (2022).

[11] F. Sauvage, M. Larocca, P. J. Coles, and M. Cerezo, arXiv preprint arXiv:2207.14413 https://doi.org/10.48550/arXiv.2207.14413 (2022).

[12] Q. T. Nguyen, L. Schatzki, P. Braccia, M. Ragone, M. Larocca, F. Sauvage, P. J. Coles, and M. Cerezo, arXiv preprint arXiv:2210.08566 (2022).

[13] T. Cohen and M. Welling, in *International conference on machine learning* (PMLR, 2016) pp. 2990–2999.

[14] R. Kondor and S. Trivedi, in *International Conference on Machine Learning* (PMLR, 2018) pp. 2747–2755.

[15] M. M. Bronstein, J. Bruna, T. Cohen, and P. Veličković, arXiv preprint arXiv:2104.13478 (2021).

[16] A. Bogatskiy, S. Ganguly, T. Kipf, R. Kondor, D. W. Miller, D. Murnane, J. T. Offermann, M. Pettee, P. Shanahan, C. Shimmin, *et al.*, arXiv preprint arXiv:2203.06153 (2022).

[17] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow, and J. M. Gambetta, Nature **567**, 209 (2019).

[18] M. Schuld and F. Petruccione, *Supervised learning with quantum computers*, Vol. 17 (Springer, 2018).

[19] I. Cong, S. Choi, and M. D. Lukin, Nature Physics **15**, 1273 (2019).

[20] L. Schatzki, A. Arrasmith, P. J. Coles, and M. Cerezo, arXiv preprint arXiv:2109.03400 (2021).

[21] M. C. Caro, H.-Y. Huang, M. Cerezo, K. Sharma, A. Sornborger, L. Cincio, and P. J. Coles, Nature Communications **13**, 4919 (2022).

[22] K. Sharma, M. Cerezo, L. Cincio, and P. J. Coles, Physical Review Letters **128**, 180505 (2022).

[23] Z. Holmes, A. Arrasmith, B. Yan, P. J. Coles, A. Albrecht, and A. T. Sornborger, Physical Review Letters **126**, 190501 (2021).

[24] M. Cerezo and P. J. Coles, Quantum Science and Technology **6**, 035006 (2021).

[25] C. O. Marrero, M. Kieferová, and N. Wiebe, PRX Quantum **2**, 040316 (2021).

[26] T. L. Patti, K. Najafi, X. Gao, and S. F. Yelin, Physical Review Research **3**, 033090 (2021).

[27] A. Uvarov and J. D. Biamonte, Journal of Physics A: Mathematical and Theoretical **54**, 245301 (2021).

[28] S. Thanasilp, S. Wang, N. A. Nghiem, P. J. Coles, and M. Cerezo, arXiv preprint arXiv:2110.14753 (2021).

[29] M. Larocca, P. Czarnik, K. Sharma, G. Muraleedharan, P. J. Coles, and M. Cerezo, Quantum **6**, 824 (2022).

[30] S. Wang, E. Fontana, M. Cerezo, K. Sharma, A. Sone, L. Cincio, and P. J. Coles, Nature Communications **12**, 1 (2021).

[31] R. Wiersema, C. Zhou, Y. de Sereville, J. F. Carrasquilla, Y. B. Kim, and H. Yuen, PRX Quantum **1**, 020319 (2020).

[32] E. Grant, L. Wossnig, M. Ostaszewski, and M. Benedetti, Quantum **3**, 214 (2019).

[33] A. Skolik, J. R. McClean, M. Mohseni, P. van der Smagt, and M. Leib, Quantum Machine Intelligence **3**, 1 (2021).

[34] S. H. Sack, R. A. Medina, A. A. Michailidis, R. Kueng, and M. Serbyn, PRX Quantum **3**, 020365 (2022).

[35] A. Rad, A. Seif, and N. M. Linke, arXiv preprint arXiv:2203.02464 (2022).

[36] L. Broers and L. Mathey, arXiv preprint arXiv:2111.08085 (2021).

[37] H.-Y. Liu, T.-P. Sun, Y.-C. Wu, Y.-J. Han, and G.-P. Guo, arXiv preprint arXiv:2112.10952 (2021).

[38] L. Friedrich and J. Maziero, Physical Review A **106**, 042433 (2022).

[39] A. Kulshrestha and I. Safro, *2022 IEEE International Conference on Quantum Computing and Engineering (QCE)*, , 197 (2022).

[40] A. A. Mele, G. B. Mbeng, G. E. Santoro, M. Collura, and P. Torta, arXiv preprint arXiv:2206.01982 (2022).

[41] K. Zhang, M.-H. Hsieh, L. Liu, and D. Tao, arXiv preprint arXiv:2203.09376 (2022).

[42] H. R. Grimsley, N. J. Mayhall, G. S. Barron, E. Barnes, and S. E. Economou, npj Quantum Information **9**, 19 (2023).

[43] M. Cerezo, K. Sharma, A. Arrasmith, and P. J. Coles, npj Quantum Information **8**, 1 (2022).

[44] M. Larocca, N. Ju, D. García-Martín, P. J. Coles, and M. Cerezo, arXiv preprint arXiv:2109.11676 (2021).

[45] E. R. Anschuetz, A. Bauer, B. T. Kiani, and S. Lloyd, arXiv preprint arXiv:2211.16998 (2022).

[46] E. R. Anschuetz and B. T. Kiani, Nature Communications **13**, 7760 (2022).

Flexible learning of quantum states with generative query neural networks

Yan Zhu[1] Ya-Dong Wu[1] * Ge Bai[1] Dong-Sheng Wang[2] Yuexuan Wang[1 3]
Giulio Chiribella[1 4 5] †

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*
[2] *CAS Key Laboratory of Theoretical Physics, Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100190, People's Republic of China*
[3] *College of Computer Science and Technology, Zhejiang University, Hangzhou, China*
[4] *Department of Computer Science, Parks Road, Oxford, OX1 3QD, United Kingdom*
[5] *Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*

Abstract. Deep neural networks are a powerful tool for characterizing quantum states. Existing networks are typically trained with experimental data gathered from the quantum state that needs to be characterized. But is it possible to train a neural network offline, on a different set of states? Here we introduce a network that can be trained with classically simulated data from a fiducial set of states and measurements, and can later be used to characterize quantum states that share structural similarities with the fiducial states. With little guidance of quantum physics, the network builds its own data-driven representation of quantum states, and then uses it to predict the outcome statistics of quantum measurements that have not been performed yet. The state representation produced by the network can also be used for tasks beyond the prediction of outcome statistics, including clustering of quantum states and identification of different phases of matter.

The full paper is available at https://www.nature.com/articles/s41467-022-33928-z.

Keywords: Quantum state learning, Generative query network, Representation learning of quantum states, Many-body ground states, Continuous-variable states, Clustering

1 Introduction

The dramatic development of artificial intelligence inspired new methods of quantum state characterization, in which techniques from the field of machine learning [5] are used to learn descriptions of quantum states from experimental data [20, 18, 17, 6, 9, 16, 3, 2, 13, 12, 11, 15]. In the existing quantum applications, neural networks are typically trained using experimental data generated from the specific quantum state that needs to be characterized. As a consequence, the information learnt in the training phase cannot be directly transferred to other states: for a new quantum state, a new training must be carried out. This limitation affects the efficiency of the network in scenarios where multiple quantum states need to be characterized.

In this paper, we develop a flexible model of neural network that can be trained offline using simulated data from a fiducial set of states and measurements, and is capable of learning multiple quantum states, provided that the states to be learnt share structural similarities with the fiducial states, such as being ground states in the same phase of a quantum manybody system. Our model, called generative query network for quantum state learning (GQNQ), takes advantage of a technique originally developed in classical image processing for learning 3D scenes from 2D snapshots taken from different viewpoints [7]. The key idea is to use a representation network [4] to construct a lower-dimensional representation of quantum states, and then to feed this representation into a generation network [8] that predicts the outcome statistics of quantum measurements that have not been performed yet. The state representation produced by GQNQ enables applications where multiple states have to be compared, such as state clustering or the identification of different phases of matter.

2 Framework

In this work we adopt a learning framework inspired by the task of "pretty good tomography" [1]. An experimenter has a source that produces quantum systems in some unknown quantum state ρ. The experimenter's goal is to characterize ρ, becoming able to make predictions on the outcome statistics of a set of measurements of interest, denoted by $\mathcal{M}$. Each measurement $\boldsymbol{M} \in \mathcal{M}$ corresponds to a positive operator-valued measure (POVM), that is, a set of positive operators $\boldsymbol{M} := (M_j)_{j=1}^k$ acting on the system's Hilbert space and satisfying the normalization condition $\sum_{j=1}^k M_j = \mathbb{1}$.

To characterize the state ρ, the experimenter performs a finite number of measurements $\boldsymbol{M}_i$, $i \in \{1, \dots, s\}$, picked at random from $\mathcal{M}$. This random subset of measurements will be denoted by $\mathcal{S} = \{\boldsymbol{M}_i\}_{i=1}^s$. Each measurement in $\mathcal{S}$ is performed multiple times on independent copies of the quantum state ρ, obtaining a vector of experimental frequencies $\boldsymbol{p}_i$. Note that in general $\mathcal{S}$ is not informationally complete.

The goal of the experimenter is to predict the outcome statistics of a new, randomly chosen measurement $\boldsymbol{M}' \in \mathcal{M} \setminus \mathcal{S}$. For this purpose, the experimenter uses the assistance of an automated learning system (e.g. a neural network), hereafter called the learner. For each measurement $\boldsymbol{M}_i \in \mathcal{S}$, the experimenter provides the learner with a pair $(\boldsymbol{m}_i, \boldsymbol{p}_i)$, where $\boldsymbol{m}_i$ is a parametriza-

*yadongwu@hku.hk
†giulio@cs.hku.hk

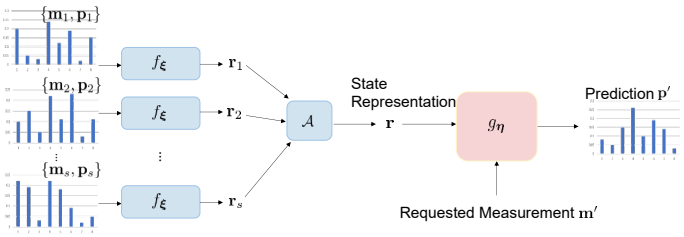


Figure 1: The neural network stucture of GQNQ

tion of the measurement $\boldsymbol{M}_i$, and $\boldsymbol{p}_i$ is the vector of experimental frequencies for the measurement $\boldsymbol{M}_i$. To obtain a prediction for a new, randomly chosen measurement $\boldsymbol{M}' \in \mathcal{M} \setminus \mathcal{S}$, the experimenter provides the learner with its parametrization $\boldsymbol{m}'$. The learner's goal is to predict the correct outcome probabilities $\left(\mathrm{tr}\left(\rho M'_j\right)\right)_{j=1}^{k}$.

3 Neural Network Structure

Our model of learner, GQNQ, is a neural network composed of two main parts: a representation network and a generation network, whose combination is called a generative query network [7]. This type of neural network was originally developed for learning 3D scenes from 2D snapshots taken from different viewpoints. The intuition for adapting this model to the quantum domain is that the statistics of a fixed quantum measurement can be regarded as a lower-dimensional projection of a higher-dimensional object (the quantum state), similar to a 2D projection of a 3D scene.

The structure of GQNQ is illustrated in Fig. 1. Consider a given set of s POVM measurements $\boldsymbol{m}_1, \ldots, \boldsymbol{m}_s$, and its corresponding outcome statistics $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_s$ with respect to an unknown quantum state ρ. For each pair of input $(\boldsymbol{m}_i, \boldsymbol{p}_i)$, the representation network $f_{\boldsymbol{\xi}}$ outputs a representation $\boldsymbol{r}_i := f_{\boldsymbol{\xi}}(\boldsymbol{m}_i, \boldsymbol{p}_i)$. Using the set of $\{\boldsymbol{r}_i\}_{i=1}^{s}$, an aggregate function outputs a representation $\boldsymbol{r}$ of state ρ. GQNQ is not constrained to a specific choice of representation, like a density matrix. This additional freedom enables the network to construct a lower-dimensional representation of quantum states with sufficiently regular structure, such as ground states in well-defined phases of matter.

Once a state representation has been produced, the next step is to predict the outcome statistics for a new quantum measurement on the state ρ. Receiving the representation $\boldsymbol{r}$ and a random query $\boldsymbol{m}'$, the generation network $g_{\boldsymbol{\eta}}$ produces prediction $\boldsymbol{p}' = g_{\boldsymbol{\eta}}(\boldsymbol{r}, \boldsymbol{m}')$. When GQNQ is used to characterize multiple quantum states $\rho^{(j)}$, $j \in \{1, \ldots, K\}$, the above procedure is repeated for each state $\rho^{(j)}$.

4 Results

4.1 Quantum State Learning: Numerical Experiments

We test GQNQ using the ground states of a one-dimensional transverse-field Ising model and the ground states of a one-dimensional XXZ model. These two models correspond to the Hamiltonians

$$H = -\left(\sum_{i=0}^{L-2} J_i \sigma_i^z \sigma_{i+1}^z + \sum_{j=0}^{L-1} \sigma_j^x\right), \tag{1}$$

and

$$H = -\left[\sum_{i=0}^{L-2} \Delta_i (\sigma_i^x \sigma_{i+1}^x + \sigma_i^y \sigma_{i+1}^y) + \sigma_i^z \sigma_{i+1}^z\right], \tag{2}$$

respectively. In the Ising Hamiltonian (1), positive (negative) coupling parameters J_i correspond to ferromagnetic (antiferromagnetic) interactions. For the XXZ Hamiltonian (2), the ferromagnetic phase corresponds to coupling parameters Δ_i in the interval $(-1, 1)$. If instead the coupling parameters fall in the region $(-\infty, -1) \cup (1, \infty)$, the Hamiltonian is said to be in the XY phase [21]. For the ground states of the Ising model (1), we choose each coupling parameter J_i at random following a Gaussian distribution with standard deviation $\sigma = 0.1$ and mean J. Similarly, for the ground states of the XXZ model (2), we choose each parameter Δ_i at random following a Gaussian distribution with standard deviation 0.1 and mean value Δ.

We first consider the six-qubit scenario where $\mathcal{M}$ is the set of 729 six-qubit measurements consisting of local Pauli measurements on each qubit. GQNQ is trained using measurement data from measurements in $\mathcal{M}$ on states of the above types. We consider both the scenario where all training data come from states of the same type, and where states of different types are used. Given raw measurement data (either true ourtomce probability distribution or finite statistics obtained by sampling the true probability distribution a finite number of times) on only $s = 30$ random Pauli bases, GQNQ predicts the outcome probabilities of all the other possible Pauli basis measurements, whose classical fidelities are summarized in Table 1. The dimension of state representation $\boldsymbol{r}$ is set to be 32, which is half of the Hilbert space dimension.

We then investigate the second scenario for ground states of XXZ model where the number of qubits is 10, 20 and 50, and the measurement settings include only Pauli basis measurements on nearest-neighbour qubits. The results are illustrated in Fig. 2. For XXZ model, the average classical fidelities in the XY phase are lower than those in the ferromagnetic interaction region, which is reasonable due to higher quantum fluctuations in the XY phase [14]. At the phase transition points $\Delta = \pm 1$, the average classical fidelities drop more significantly, partly because the abrupt changes of ground state properties at the critical points make the quantum state less predictable, and partly because the states at phase transition points are less represented in the training data set. Here the dimension of state representation $\boldsymbol{r}$ is chosen to be 24, which guarantees a good performance in our numerical experiments.

GQNQ can also be applied to online learning of quantum states. In each round of online learning, newly collected measurement data are fed into the representation

Table 1: Average classical fidelities between the predictions of GQNQs and the ground truths with respect to different types of six-qubit states.

Types of states for training and test	noiseless	50 shots	10 shots
(i) Ising ground states with ferromagnetic bias	0.9870	0.9869	0.9862
(ii) Ising ground states with antiferromagnetic bias	0.9869	0.9867	0.9849
(iii) Ising ground states with no bias	0.9895	0.9894	0.9894
(iv) XXZ ground states with ferromagnetic bias	0.9809	0.9802	0.9787
(v) XXZ ground states with XY phase bias	0.9601	0.9548	0.9516
(vi) (i)-(v) together	0.9567	0.9547	0.9429

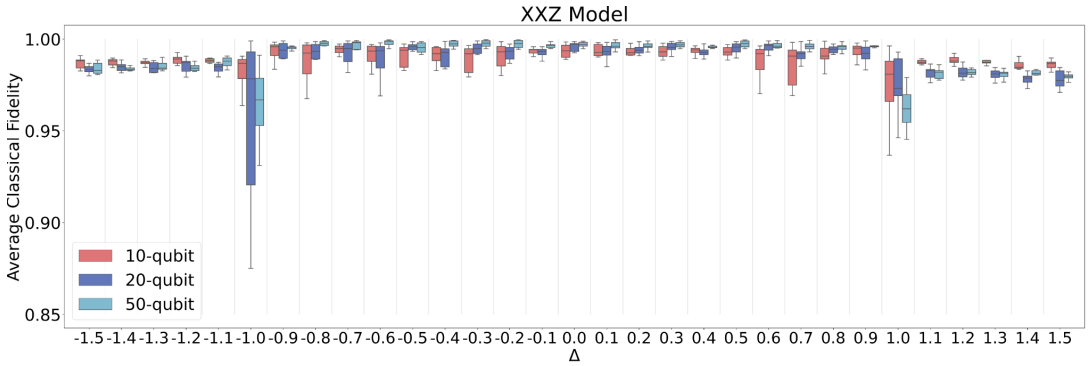


Figure 2: The figure shows the performances of three GQNQs for ten-, twenty- or fifty-qubit ground states of XXZ model (2), respectively, with respect to different values of $\Delta \in \{-1.5, -1.4, \ldots, 1.5\}$ by boxplots [19]. Given outcome probability distributions for all $\boldsymbol{m} \in \mathcal{S}$, each box shows the average classical fidelities of predicted outcome probabilities, averaged over all measurements in $\mathcal{M} \setminus \mathcal{S}$, for ten instances.

network to update the state representation, and the updated representation is fed into the generation network to update the predictions.

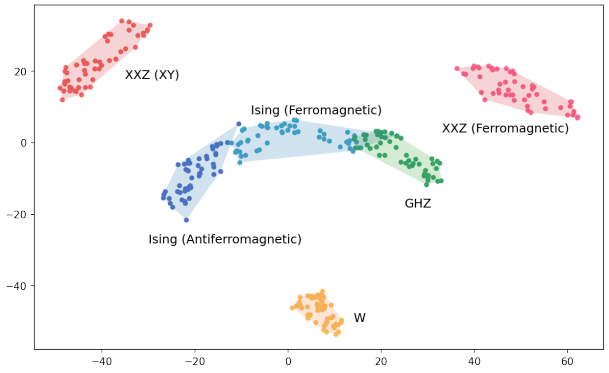


Figure 3: The figure shows two-dimensional embeddings of representations of Ising model (ferromagnetic and antiferromagnetic) ground state, XXZ model (ferromagnetic and XY phase) ground state, GHZ state with local rotations and W state with local rotations.

4.2 Interpretable State Representations

The state representation $\boldsymbol{r}$ constructed in the last section contains key information about the associated quantum state ρ, and can be used to perform other downstream tasks beyond the prediction of outcome probability distributions for unmeasured POVMs. We show that clusters naturally emerge from the state representations produced by GQNQ. To visualize the clusters, we feed the state representation vectors constructed from noiseless input data into a t-SNE algorithm [10], which produces a mapping of the representation vectors into a two-dimensional plane, according to their similarities. We performed numerical experiments using the types of six-qubit states in Table 1 together with locally rotated GHZ states and locally rotated W states. The figure shows that states with significantly different physical properties correspond to distant points in the two-dimensional embedding, while states with similar properties naturally appear in clusters.

References

[1] Aaronson, S.: The learnability of quantum states. Proc. R. Soc. A **463**(2088), 3089–3114 (2007)

[2] Ahmed, S., Sánchez Muñoz, C., Nori, F., Kockum, A.F.: Classification and reconstruction of optical quantum states with deep neural networks. Phys. Rev. Res. **3**, 033278 (Sep 2021). https://doi.org/10.1103/PhysRevResearch.3.033278

[3] Ahmed, S., Sánchez Muñoz, C., Nori, F., Kockum, A.F.: Quantum state tomography with conditional generative adversarial networks. Phys. Rev. Lett. **127**, 140502 (Sep 2021). https://doi.org/10.1103/PhysRevLett.127.140502

[4] Bengio, Y., Courville, A., Vincent, P.: Representation learning: A review and new perspectives. IEEE

Trans. Pattern Anal. Mach. Intell. **35**(8), 1798–1828 (2013)

[5] Carleo, G., Cirac, I., Cranmer, K., Daudet, L., Schuld, M., Tishby, N., Vogt-Maranto, L., Zdeborová, L.: Machine learning and the physical sciences. Rev. Mod. Phys. **91**, 045002 (Dec 2019). https://doi.org/10.1103/RevModPhys.91.045002

[6] Carrasquilla, J., Torlai, G., Melko, R.G., Aolita, L.: Reconstructing quantum states with generative models. Nat. Mach. Intell. **1**(3), 155–161 (2019)

[7] Eslami, S.A., Rezende, D.J., Besse, F., Viola, F., Morcos, A.S., Garnelo, M., Ruderman, A., Rusu, A.A., Danihelka, I., Gregor, K., et al.: Neural scene representation and rendering. Science **360**(6394), 1204–1210 (2018)

[8] Foster, D.: Generative deep learning: teaching machines to paint, write, compose, and play. O'Reilly Media (2019)

[9] Iten, R., Metger, T., Wilming, H., del Rio, L., Renner, R.: Discovering physical concepts with neural networks. Phys. Rev. Lett. **124**, 010508 (Jan 2020). https://doi.org/10.1103/PhysRevLett.124.010508

[10] Van der Maaten, L., Hinton, G.: Visualizing data using t-sne. J. Mach. Learn. Res. **9**(11) (2008)

[11] Palmieri, A.M., Kovlakov, E., Bianchi, F., Yudin, D., Straupe, S., Biamonte, J.D., Kulik, S.: Experimental neural network enhanced quantum tomography. NPJ Quantum Inf. **6**, 20 (2020)

[12] Quek, Y., Fort, S., Ng, H.K.: Adaptive quantum state tomography with neural networks. NPJ Quantum Inf. **7**, 105 (2021)

[13] Rocchetto, A., Grant, E., Strelchuk, S., Carleo, G., Severini, S.: Learning hard quantum distributions with variational autoencoders. NPJ Quantum Inf. **4**, 28 (2018)

[14] Samaj, L.: Introduction to the statistical physics of integrable many-body systems. Cambridge University Press (2013)

[15] Smith, A.W.R., Gray, J., Kim, M.S.: Efficient quantum state sample tomography with basis-dependent neural networks. PRX Quantum **2**, 020348 (Jun 2021). https://doi.org/10.1103/PRXQuantum.2.020348

[16] Tiunov, E.S., Tiunova, V., Ulanov, A.E., Lvovsky, A., Fedorov, A.K.: Experimental quantum homodyne tomography via machine learning. Optica **7**(5), 448–454 (2020)

[17] Torlai, G., Mazzola, G., Carrasquilla, J., Troyer, M., Melko, R., Carleo, G.: Neural-network quantum state tomography. Nat. Phys. **14**(5), 447–450 (2018)

[18] Torlai, G., Melko, R.G.: Latent space purification via neural density operators. Phys. Rev. Lett. **120**, 240503 (Jun 2018). https://doi.org/10.1103/PhysRevLett.120.240503

[19] Williamson, D.F., Parker, R.A., Kendrick, J.S.: The box plot: a simple visual method to interpret data. Ann. Intern. Med. **110**(11), 916–921 (1989)

[20] Xu, Q., Xu, S.: Neural network state estimation for full quantum state tomography. arXiv preprint arXiv:1811.06654 (2018)

[21] Yang, C.N., Yang, C.P.: One-dimensional chain of anisotropic spin-spin interactions. i. proof of bethe's hypothesis for ground state in a finite system. Phys. Rev. **150**, 321–327 (Oct 1966)

Investigations of the Quantum Boundary and Device-independent Applications

Yuan Liu[1] Shuai Zhao[1] Ho Yiu Chung[1] Ravishankar Ramanathan[1] *
Paweł Horodecki[2 3]

[1] *Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*
[2] *International Centre for Theory of Quantum Technologies, University of Gdańsk, Wita Stwosza 63, 80-308 Gdańsk, Poland*
[3] *Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gabriela Narutowicza 11/12, 80-233 Gdańsk, Poland*

Abstract. The set of correlations between measurement outcomes observed by separated parties in a Bell test is of vital importance in Device-Independent (DI) information processing. However, characterising this set of quantum correlations is a hard problem, with a number of open questions. Here, we present families of quantum Bell inequalities that approximate this set in Bell scenarios with an arbitrary number of players, settings and outcomes, and study their applications to device-independent information processing. Firstly, in the Bell scenario of two players with two k-outcome measurements, we derive inequalities that show a separation of the quantum boundary from classes of non-local faces of the non-signaling polytope of dimension $\leq 4k-4$, extending previous results from nonlocality distillation and the collapse of communication complexity. Secondly, in the scenario of two players with m binary measurements, we derive a weighted chained Bell inequality that serves to self-test the maximally entangled state of two qubits. Finally, in Bell scenarios of two players with binary outcomes, we derive a low-dimensional region of the quantum boundary that coincides with the boundary of the set of classical correlations in these scenarios. In [26], we introduce a family of tilted Hardy paradoxes that allow to self-test general pure two-qubit entangled states, as well as certify up to 1 bit of local randomness with arbitrarily limited measurement independence. We then use these tilted Hardy tests to obtain an improvement in the generation rate in the state-of-art randomness amplification protocols against adversaries holding quantum as well as non-signaling side information. Other than that, we propose a family of Hardy tests for maximally entangled states of local dimension $4, 8$ that allow to certify up to the maximum possible $2\log d$ bits of global randomness.

Keywords: Quantum Boundary, Device-independent cryptography applications, self-test, randomness extraction.

In this manuscript, we introduce our two recent works, both of which are aimed at advancing the field of quantum foundation and quantum cryptography research. The first study delves into the exploration of quantum boundaries, with the complete text provided in the Appendix for reference. The second study focuses on device-independent randomness extraction with arbitrarily limited measurement independence, employing a family of tilted Hardy paradoxes to achieve this goal [26]. The latter work is currently processed in the journal Quantum.

1 Part I: Investigations of the Quantum Boundary

One of the most striking features of quantum mechanics is non-locality, the phenomenon of violation of Bell inequalities by separated physical systems. The correlations between local measurement outcomes on such systems show, in a fully device-independent manner, that quantum theory differs fundamentally from all classical theories that are constrained by the principle of local causality [1, 2]. Besides their foundational interest, in recent years, the quantum correlations have been shown to be a vital resource in device-independent (DI) information processing applications, such as quantum key distribution [3, 4], randomness extraction and expansion [5, 6], self-testing of quantum states and measurements [7, 8], and reduction of communication complexity [9].

The Bell inequalities delineate the boundary of the set of classical correlations, and any violation of a Bell inequality indicates that the observed distribution of conditional measurement outcomes is nonlocal. Moreover, the verification of nonlocal correlations (and the correct execution of DI tasks built upon these) can be performed by simple statistical tests of the measurement devices and a fundamental rule of nature, viz. the no-superluminal signaling principle of relativity. While the classification of the entire set of Bell inequalities for arbitrary number of measurement systems, inputs and outputs is a challenge, at least a systematic method for the identification of novel Bell inequalities is known since the work by Pitowsky [10].

On the other hand, the set of behaviors (conditional probability distributions for outcomes conditioned on the different inputs) obtainable in quantum theory, denoted Q, is known to lie in between the classical set L and the general no-signaling set NS [11]. The set Q is convex but is in general not a polytope unlike L and NS. The characterisation of the boundary of Q via the derivation of (in general, non-linear) quantum Bell inequalities has proven to be a much more challenging task [12] and only a few examples have been found so far [15, 16, 14, 17, 13, 18]. For fundamental reasons as well as to identify the optimal quantum correlations for different applications, it is of importance to characterize the set of quantum correlations, and understand how it fits in between the polytopes of classical and general non-signaling correlations.

Specific DI applications demand quantum correlations that exhibit particular properties. For instance, the task of randomness amplification [19, 20, 21, 22, 23, 24, 26, 25] requires the use of quantum correlations that lie on the no-signaling boundary to allow extraction of randomness from arbitrarily weak seeds. As such, the quantum correlations exhibiting pseudo-telepathy [27, 28] or demonstrating the Hardy para-

*ravi@cs.hku.hk

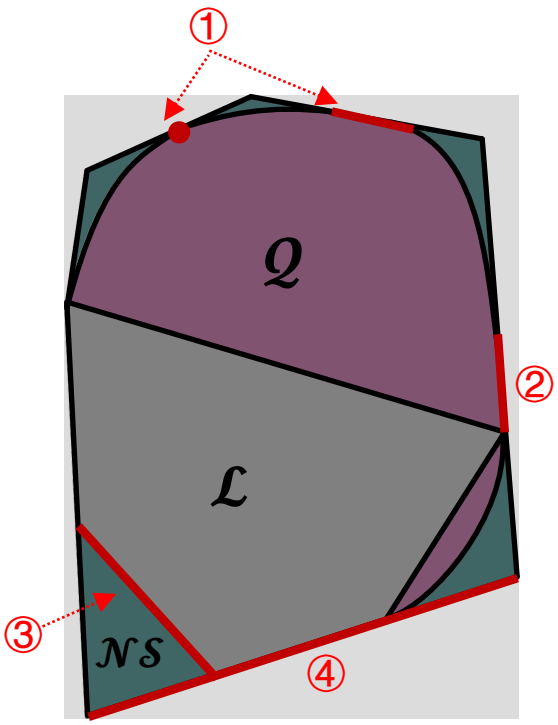


Figure 1: Relationship of the quantum set Q, classical set L and no-signaling set NS. Classical set L and no-signaling set NS are convex polytopes. Quantum set Q is a convex set, it may saturate the no-signaling boundaries with (②) or without (①) a local deterministic vertex on the no-signaling boundaries, and it may also coincide the classical boundaries with (④) or without (③) a non-local no-signaling vertex on the classical boundaries.

dox [29, 30] have found use in this task. Similarly, another important task that has gained prominence in recent years is self-testing, namely the unique identification (up to local isometries) of a quantum state and measurements, solely from the observed correlations in a Bell test. As such, this task requires the identification of quantum correlations that can be generated in such a unique manner. Finally, the study of the boundary of the quantum set is also important from a fundamental viewpoint in the problem of identifying appropriate information-theoretic principles that single out the set of quantum correlations from amongst general no-signaling ones. Of particular importance are the principle of information causality [31], macroscopic locality [32], local orthogonality [33], no advantage in non-local computation [18], and the collapse of communication complexity [34], all of which have been shown to lead to non-trivial bounds on the set of quantum correlations. The identification of non-local no-signaling boxes that are excluded from the quantum set serves as a useful testing ground and pointers towards the ultimate principle picking out the quantum set. Other fundamental questions regarding the boundary of the quantum set include 2 out of the 29 open problems in quantum information listed in [35].

In this work, we explore the boundary of the quantum set with specific regard to regions coinciding with a no-signaling or a local boundary, and non-trivial regions leading to self-testing. To do this, we expand on a class of (non-linear) inequalities defining the boundary of the Almost Quantum Set [36]. Such inequalities were used to exclude all non-local vertices of the no-signaling polytope (for arbitrary number of parties, inputs and outputs) by one of us in [37]. Here, we explore these inequalities to exclude further non-trivial regions of the no-signaling polytope. Specifically, in the $(2,2,k)$ Bell scenario (with two players performing two measurements with k outcomes each), we derive optimal inequalities that show the exclusion of all non-local faces of the no-signaling polytope of dimension up to $4k-4$. This extends the known region of excluded boxes from the no-signaling boundary obtained in [16], and through the procedure of non-locality distillation [15, 38] and the collapse of communication complexity [39]. Secondly, we derive a class of tight quantum Bell inequalities in the $(2,m,2)$ Bell scenario (with two players performing m binary measurements) and show their usefulness in self-testing the two-qubit singlet state. In this regard, we generalise the results regarding the self-testings of the singlet in the $(2,2,2)$ scenario obtained in [40] and the self-testing of the correlations leading to the optimal violation of the chained Bell inequality in [41]. Finally, we study the faces of the correlation set (excluding the local marginals), and identify low-dimensional regions in which the quantum correlation set coincides with the classical correlation polytope. In this regard, we generalise the results obtained by Linden et al. in [18].

2 Part II: Device-independent Applications

One of the most fundamental features of quantum mechanics is the presence of correlations that cannot be explained by any local hidden variable theory [42, 43]. Apart from being of fundamental interest, this phenomenon of Bell non-locality has led to the powerful idea of device-independent (DI) quantum key distribution [3, 4], randomness generation [5, 6] and certification of quantum systems [7, 44].

The strength of the device-independent paradigm is that no assumption on the nature of the systems subject to measurement needs to be made. Indeed, one may simply consider the systems participating in the Bell experiment to be (two or more) black boxes that parties provide an input to and obtain an outcome from, not taking into account the complex details of the physical implementation at all. The observation of a Bell inequality violation then allows one to make nontrivial deductions about the nature of the systems under study, such as the presence of entanglement, or a lower bound on the system dimension, or the non-determinism of the measurement outputs. In the extreme case, observation of maximum violation of certain Bell inequalities even permits the device-independent certification (*self-testing*) [44] of the quantum state and measurements performed on the system, i.e., their uniqueness up to irrelevant local equivalences.

Such self-testing has obvious advantages over traditional certification methods such as those based on quantum tomography [45], and a lot of attention has therefore been devoted recently to designing Bell inequalities suited for self-testing different entangled quantum states. However, DI certification based on the violation of Bell inequalities nevertheless still relies upon some assumptions, the foremost being the requirements of no-signaling between the local systems (typically en-

forced by space-like separation), and that the measurements on the local systems are chosen freely and randomly.

This latter requirement known as measurement independence is typically justified by the assumption that the parties hold independent and trusted random number generators (i.e., trusted and private random seeds). However, this assumption is clearly incongruous with the very framework of device-independence, wherein all devices held by the honest parties may have been tampered with, or even provided by, an adversary. To elaborate, consider the adversarial scenario wherein an adversary Eve has had access to the very devices used by the honest parties in the protocol. If such an adversary was able to influence the local random number generators held by the parties, then she would be able to ensure that the parties only hold imperfect seeds (about which Eve has some side information). In the extreme case, Eve may even be able to prepare devices that only operate according to local hidden variable behaviors, and yet appear non-local to the parties due to the imperfection of their seeds. Indeed, when no measurement independence at all is available, one cannot demonstrate any non-locality. It is therefore of vital importance to extend the studies on device-independent certification (as well as other tasks such as key distribution and random number generation) to the scenario in which only limited (arbitrarily small) measurement independence is available [19, 20, 21, 22, 23, 24].

As a model of an imperfect seed, one may consider the ε-SV source [46], a model of a biased coin where the individual coin tosses are not independent but rather the bits R_i produced by the source obey $\frac{1}{2}-\varepsilon \leq P(R_i=0|R_{i-1},\ldots,R_1,W) \leq \frac{1}{2}+\varepsilon$. The parameter $0 \leq \varepsilon < \frac{1}{2}$ described the reliability of the source, with $\varepsilon = 0$ being the ideal random seed and W denotes any side information, possibly held by an adversary. It is worth remarking that more general 'min-entropy' sources are also possible, wherein only a lower bound on the min-entropy (the negative logarithm of the maximum probability of any output string) produced by the source is assumed.

With regards to the task of self-testing, an important result was the formulation of a general class of Bell inequalities known as the tilted-CHSH inequalities suitable for self-testing general pure two-qubit entangled states. Specifically, in the simplest bipartite Bell scenario with two binary observables A_0, A_1 for Alice and two binary observables B_0, B_1 for Bob, the following family of tilted CHSH operators was introduced in [47]

$$I_\alpha = \alpha A_0 + A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1, \qquad (1)$$

where $\alpha \in [0,2)$ is a parameter with $\alpha = 0$ corresponding to the well-known CHSH operator. The maximum value of this tilted CHSH quantity in classical theories is easily seen to be $2+\alpha$. In [48], it was shown that the optimal quantum value of $I_\alpha^{\max} = \sqrt{8+2\alpha^2}$ can only be achieved when specific reference observables A_x, B_y are measured on the state $|\psi_\theta\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with $\theta = \frac{1}{2}\arctan\sqrt{\frac{2}{\alpha^2}-\frac{1}{2}}$. Specifically, it was shown that the observation of the expectation value $\langle I_\alpha\rangle \geq I_\alpha^{\max} - \varepsilon$ for the tilted CHSH operator by measuring a physical state $|\tilde{\psi}\rangle$ with observables $\tilde{A}_x$ and $\tilde{B}_y$ implies the existence of an isometry $\Phi = \Phi_A \otimes \Phi_B$ and a state $|\text{junk}\rangle$ such that $\|\Phi\left(\tilde{A}_x \otimes \tilde{B}_y|\tilde{\psi}\rangle\right) - |\text{junk}\rangle \otimes (A_x \otimes B_y)|\psi\rangle\| \leq \varepsilon'$, where $x, y \in \{-1, 0, 1\}$ (with subscript -1 indicating the identity operator) and where $\varepsilon' = O\left(\sqrt{\varepsilon}\right)$. The family of tilted CHSH inequalities has since played a crucial role in several aspects, including (a) showing the quantitative inequivalence between the amount of non-locality and the amount of certified randomness [47], (b) being the building block that enabled the self-testing of all bipartite pure (two-qudit) entangled states [49], (c) enabling the formulation of a device-independent quantum random number generation (DIQRNG) protocol that only requires a sublinear amount of quantum communication [50] (i.e., produces n bits of output randomness with a total of $nS(\theta) = \Omega(n^k \log n)$ with $7/8 < k < 1$ ebits where $S(\theta) = h_2(\sin^2\theta)$ is the entropy of entanglement of $|\psi_\theta\rangle$ expressed in terms of the binary entropy h_2, and (d) unbounded randomness certification from a single pair of entangled qubits using a sequence of measurements [51].

A natural question is whether a corresponding family of inequalities can be formulated in the scenario of (arbitrarily) limited measurement independence so that the above (and further such DI) results can be achieved in the setting when the parties are not assumed to possess perfect random seeds. In [26], we answer this question in the positive by formulating a class of tilted Hardy paradoxes that allow to self-test general pure two-qubit entangled states (except the maximally entangled state). As shown in [52], tests of Hardy paradoxes (in an equivalent formulation as 'measurement-dependent' locality inequalities) allow for arbitrary small measurement independence making them ideal candidates for device-independent tasks when only weak seeds are available. We derive expressions for the amount of randomness that can be certified from the maximum violation of the tilted Hardy tests in terms of the *guessing probability* by an adversary holding a quantum system that is potentially correlated to the devices involved in the test. We compute the guessing probability in the noisy scenario of non-maximal violation, here distinguishing between two cases: (a) a scenario of colored noise where the 'zero' constraints in the tilted Hardy paradox are satisfied but the non-zero Hardy probability is non-maximal, and (b) a scenario of white noise where we consider the non-maximal violation of a Bell expression derived from the tilted Hardy paradox. While an amount of local randomness up to the maximum possible value of 1 bit can be certified by the tilted Hardy tests, the amount of global randomness is limited to a value of approximately 1.6806 bits. Nevertheless, we show that the derived results present an improvement in generation rate over the state-of-art protocols of randomness amplification against quantum adversaries. We present a class of Hardy paradoxes with more inputs and outputs that potentially allows to certify the maximal amount of global randomness of $2\log d$ bits for dimensions $d = 4, 8$. To do this, we exploit a recently discovered connection between Hardy paradoxes and substructures of Kochen Specker proofs termed 01-gadgets [53]. Finally, we derive the analytical expression for the guessing probability in the scenario of an adversary that is allowed to prepare bipartite devices for the honest parties constrained only by the no-signaling principle, a result that also finds application in the state-of-art protocols for randomness amplification against no-signaling adversaries [23].

References

[1] J. S. Bell. The theory of local beables. *Epistemological Letters*, (1975).

[2] J. S. Bell. Free variables and local causality. In *Quantum mechanics, high energy physics and accelerators. Selected papers of John S. Bell (with commentary)*, (1995).

[3] J. Barrett, L. Hardy, and A. Kent. No Signaling and Quantum Key Distribution. *Physical Review Letters*, 95(1) :010503, (2005).

[4] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Physical Review Letters*, 98(23) :230501, (2007).

[5] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464(7291): 1021 – 1024, (2010).

[6] S. Pironio and S. Massar. Security of practical private randomness generation. *Physical Review A*, 87(1) :012336, (2013).

[7] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 503 – 509. IEEE, (1998).

[8] D. Mayers and A. Yao. Self testing quantum apparatus. *arXiv:quant-ph/0307205*.

[9] H. Buhrman, R. Cleve, S. Massar, and R. De Wolf. Nonlocality and communication complexity. *Reviews of modern physics*, 82(1): 665, (2010).

[10] I. Pitowsky. Correlation polytopes: Their geometry and complexity. *Mathematical Programming*, 50: 395 – 414, (1991).

[11] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3): 379 – 385, (1994).

[12] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani. Geometry of the set of quantum correlations. *Physical Review A*, 97(2): 022104, (2018).

[13] R. Ramanathan. Violation of all two-party facet bell inequalities by almost-quantum correlations. *Physical Review Research*, 3(3): 033100, (2021).

[14] M. L. Almeida, J.-D. Bancal, N. Brunner, A. Acín, N. Gisin, and S. Pironio. Guess your neighbor's input: A multipartite nonlocal game with no quantum advantage. *Physical Review Letters*, 104(23): 230404, (2010).

[15] A. Rai, C. Duarte, S. Brito, and R. Chaves. Geometry of the quantum set on no-signaling faces. *Physical Review A*, 99(3): 032106, (2019).

[16] K.-S. Chen, G. N. M. Tabia, C. Jebarathinam, S. Mal, J.-Y. Wu, and Y.-C. Liang. Quantum correlations on the no-signaling boundary: self-testing and more. *arXiv: 2207.13850*.

[17] R. Ramanathan, A. Kay, G. Murta, and P. Horodecki. Characterising the Performance of XOR Games and the Shannon Capacity of Graphs. *Physical Review Letters*, 113(24): 240401, (2014).

[18] N. Linden, S. Popescu, A. J. Short, and A. Winter. Quantum Nonlocality and Beyond: Limits from Nonlocal Computation. *Physical Review Letters*, 99(18): 180502, (2007).

[19] R. Colbeck and R. Renner. Free randomness can be amplified. *Nature Physics*, 8(6): 450 – 453, (2012).

[20] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín. Full randomness from arbitrarily deterministic events. *Nature Communications*, 4(1): 1 – 7, (2013).

[21] R. Ramanathan, F. G. S. L. Brandão, K. Horodecki, M. Horodecki, P. Horodecki, and H. Wojewódka. Randomness Amplification under Minimal Fundamental Assumptions on the Devices. *Physical Review Letters*, 117(23): 230501, (2016).

[22] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewódka. Realistic noise-tolerant randomness amplification using finite number of devices. *Nature Communications*, 7(1): 1 – 6, (2016).

[23] R. Ramanathan, M. Horodecki, H. Anwer, S. Pironio, K. Horodecki, M. Grünfeld, S. Muhammad, M. Bourennane, and P. Horodecki. Practical No-signaling proof Randomness Amplification using Hardy paradoxes and its experimental implementation. *arXiv: 1810.11648*.

[24] M. Kessler and R. Arnon-Friedman. Device-Independent Randomness Amplification and Privatization. *IEEE Journal on Selected Areas in Information Theory*, 1(2): 568 – 584, (2020).

[25] R. Ramanathan, M. Banacki, and P. Horodecki. No-signaling-proof randomness extraction from public weak sources. *arXiv: 2108.08819*.

[26] S. Zhao, R. Ramanathan, Y. Liu, and P. Horodecki. Tilted Hardy paradoxes for device-independent randomness extraction. *arXiv: 2205.02751*.

[27] G. Brassard, A. Broadbent, and A. Tapp. Quantum Pseudo-Telepathy. *Foundations of Physics*, 35(11): 1877 – 1907, (2005).

[28] R. Renner and S. Wolf. Quantum Pseudo-Telepathy and the Kochen-Specker Theorem. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, pages 322 – 322. IEEE, (2004).

[29] L. Hardy. Nonlocality for two particles without inequalities for almost all entangled states. *Physical Review Letters*, 71(11): 1665, (1993).

[30] D. Boschi, S. Branca, F. De Martini, and L. Hardy. Ladder Proof of Nonlocality without Inequalities: Theoretical and Experimental Results. *Physical Review Letters*, 79(15): 2755, (1997).

[31] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski. Information causality as a physical principle. *Nature*, 461(7267): 1101 – 1104, (2009).

[32] M. Navascués and H. Wunderlich. A glance beyond the quantum model. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 466(2115): 881 – 890, (2010).

[33] T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, and A. Acín. Local orthogonality as a multipartite principle for quantum correlations. *Nature Communications*, 4(1) :2263, (2013).

[34] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Physical Review Letters*, 96(25): 250401, (2006).

[35] O. Krueger and R. F. Werner. Some Open Problems in Quantum Information Theory. *arXiv: quant-ph/0504166*.

[36] M. Navascués, Y. Guryanova, M. J. Hoban, and A. Acín. Almost quantum correlations. *Nature Communications*, 6(1): 6288, (2015).

[37] R. Ramanathan, J. Tuziemski, M. Horodecki, and P. Horodecki. No Quantum Realization of Extremal No-signaling Boxes. *Physical Review Letters*, 117(5): 050401, (2016).

[38] S. G. A. Brito, M. G. M. Moreno, A. Rai, and R. Chaves. Nonlocality distillation and quantum voids. *Physical Review A*, 100(1): 012102, (2019).

[39] M.-O. Proulx, A. Broadbent and P. Botteron Extending the Known Region of Nonlocal Boxes that Collapse Communication Complexity. *arXiv: 2302.00488*.

[40] Y. Wang, X. Wu, and V. Scarani. All the self-testings of the singlet for two binary measurements. *New Journal of Physics*, 18(2): 025021, (2016).

[41] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín. Self-testing protocols based on the chained bell inequalities. *New Journal of Physics*, 18(3): 035013, (2016).

[42] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10): 777, (1935).

[43] 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).

[44] D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Information & Computation*, 4(4): 273 – 286, (2004).

[45] K. T. Goh, C. Perumangatt, Z. X. Lee, A. Ling, and V. Scarani. Experimental comparison of tomography and self-testing in certifying entanglement. *Physical Review A*, 100(2) :022305, (2019).

[46] M. Santha and U. V. Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of Computer and System Sciences*, 33(1): 75 – 87, (1986).

[47] A. Acín, S. Massar, and S. Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108(10): 100402, (2012).

[48] C. Bamps and S. Pironio. Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing. *Physical Review A*, 91(5): 052111, (2015).

[49] A. Coladangelo, K. T. Goh, and V. Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8(1): 1 – 5, (2017).

[50] C. Bamps, S. Massar, and S. Pironio. Device-independent randomness generation with sublinear shared quantum resources. *Quantum*, 2: 86, (2018).

[51] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín. Unbounded randomness certification using sequences of measurements. *Physical Review A*, 95(2): 020102, (2017).

[52] G. Pütz, D. Rosset, T. J Barnea, Y.-C. Liang, and N. Gisin. Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality. *Physical Review Letters*, 113(19): 190402, (2014).

[53] R. Ramanathan, Y. Liu, and P. Horodecki. Large violations in Kochen Specker contextuality and their applications. *New Journal of Physics*, 24(3): 033035, (2022).

Extended Abstract: Principle of information causality rationalizes quantum composition

Ram Krishna Patra,[1] Sahil Gopalkrishna Naik,[1] Edwin Peter Lobo,[2]
Samrat Sen,[1] Govind Lal Sidhardh,[1] Mir Alimuddin,[1] and Manik Banik[1]

[1]*Department of Physics of Complex Systems,*
S. N. Bose National Center for Basic Sciences,
Block JD, Sector III, Salt Lake, Kolkata 700106, India.
[2]*School of Physics, IISER Thiruvananthapuram, Vithura, Kerala 695551, India.*

Principle of information causality, proposed as a generalization of no signaling principle, can outcast beyond quantum nonlocal correlations as unphysical [Nature **461**, 1101 (2009)]. Here we show that this principle provides physical rationale towards Hilbert space composition of multipartite quantum systems. In accordance with no signaling condition, state and effect spaces of a composite system can allow different possible mathematical descriptions even when the individual systems are assumed to be quantum. While in one extreme the state space becomes quite exotic and permits composite states that are not allowed in quantum theory, in the other extreme it contains only separable states and the resulting theory becomes local. As we show, none of these compositions does commensurate with information causality, and hence get invalidated to be the bona-fide description of nature. Information causality, therefore, promises physical ground towards self-duality of state and effect cones for composite quantum systems.

Keyword - Information Causality Principle, Generalized Probability Theory, Composition of Local Quantum System

Reference - Phys. Rev. Lett. 130, 110202

Introduction.– Quantum mechanics is the most effective theory to describe almost all the natural phenomena. However, the theory, starting from its inception, engenders huge debates regarding its interpretation [1–8] that persists till date [9, 10]. Quantum formalism starts with abstract mathematical description of Hilbert space and cries for its physical justification. The celebrated no-signaling (NS) principle, that prohibits instantaneous communication between distant parties, cannot serve the purpose alone. It allows a broad variety of mathematical models as the possible candidate of the theory of nature. Interestingly, inspired by the studies in quantum information theory, during the recent past, several novel principles have been proposed to circumvent the limitation of NS principle [11–16]. These new principles quite efficiently identify some beyond quantum NS correlations as unphysical and thus adduce physical justification(s) to quantum correlations.

In this work we analyze one of the intriguing principles called information causality (IC), proposed nearly a decade back [13]. IC can be envisaged as a generalization of the NS condition. It lim-

its the information gain that a receiver (say Bob) can reach about a previously unknown to him data set of a sender (say Alice), by using two types of resources: (i) all his local resources that might be correlated with the sender, and (ii) some physical system carrying bounded amount of information from Alice to Bob. Both these resources can further be of different kinds – classical, quantum, and beyond quantum; and IC principle provides a way to test their physicality. Although the correlated resources by themselves have no communication utility, as shown in the seminal superdense coding paper [17], a quantum correlation *viz.* entanglement can double up the communication capacity of a quantum channel. The power of entanglement, however, is limited in a way as it cannot enhance communication capacity of a classical channel. Principle of IC generalizes this no-go by limiting Bob's information gain to be at most m bits when m classical bits are communicated by Alice to him and he is allowed to use any of his local resources that might be correlated with Alice. Quite interestingly several NS correlations violate this principle and thus considered as unphysical [18–21]. In essence, restricting the type-(ii) resources to be classical, the IC principle discards some of the type-(i) resources as unphysical.

Here we study the reverse scenario, *i.e.*, restricting the type-(i) resources to be classical we show that some type-(ii) resources are not compatible with IC and hence deem unphysical. We consider the scenario where individual systems are assumed to be quantum, but their composition can be modelled by any theory that satisfy the NS condition. Even for two quantum systems several consistent compositions are possible among which quantum theory is one of the examples. The state space of the resulting system lies in between two extremes – maximal tensor product state space and minimal tensor product state space [22]. While the maximal one grants exotic joint states that are not allowed in quantum theory, the minimal one allows only separable states. It turns out that the system obtained through maximal tensor product of two elementary quantum violates the IC principle. This is quite remarkable as all the NS correlations obtained from beyond quantum states are in fact quantum simulable and hence cannot yield beyond quantum nonlocal correlation [23]. We then show that minimal tensor product composition of two elementary quantum also violates the IC principle. This is even more striking as the resulting theory is local by construction.

IC discards extreme compositions of elementary quantum.– We consider the scenario where Alice can communicate some abstract physical system to Bob with whom she can share pre-shared randomness. Within the mathematical framework of generalized probability theory (GPT) [24–28] such an elementary system $\mathcal{S}$ can be specified by the tuple of normalized state and effect spaces, *i.e.* $\mathcal{S} \equiv (\Omega, \mathcal{E})$. Sometime it is convenient to deal with unnormalized states and effects that form convex cones embedded in some $\mathbb{R}^n$. A GPT also captures the description of the composite system $\mathcal{S}^{AB} \equiv (\Omega^{AB}, \mathcal{E}^{AB})$ consisting of component subsystems $\mathcal{S}^A \equiv (\Omega^A, \mathcal{E}^A)$ and $\mathcal{S}^B \equiv (\Omega^B, \mathcal{E}^B)$. Under the restriction of NS and local tomography [29] the composite state space

Ω^{AB} lies in between two extremes – (i) the maximal tensor product state space and (ii) the minimal tensor product state space [22]. For instance, the state cone of a quantum system associated with a Hilbert space $\mathcal{H}$ is the set of positive semidefinite operators $\mathcal{P}(\mathcal{H}) \subset \mathcal{L}(\mathcal{H})$ acting on $\mathcal{H}$, whereas the normalized states are the set of density operators $\mathcal{D}(\mathcal{H})$; Here $\mathcal{L}(\mathcal{H})$ denotes the set of all linear operators acting on $\mathcal{H}$. For two quantum systems associated with Hilbert spaces $\mathcal{H}^A$ and $\mathcal{H}^B$ respectively, the state cone for maximal tensor product system is given by

$$\begin{aligned}\Omega^{AB}{}_{+}[\max] := \\ \{\mathcal{W} \in \mathcal{L}(\mathcal{H}^A \otimes \mathcal{H}^B) | \operatorname{Tr}[\mathcal{W}(\pi_A \otimes \pi_B)] \geq 0 \\ \forall \pi_A \in \mathcal{P}(\mathcal{H}^A) \text{ and } \forall \pi_B \in \mathcal{P}(\mathcal{H}^B)\}.\end{aligned}$$

Clearly, $\Omega^{AB}_{+}[\max]$ contains all the quantum states $\mathcal{P}(\mathcal{H}^A \otimes \mathcal{H}^B)$, and furthermore it encompasses states that are not allowed in quantum theory. For example, entanglement witness that are not bona-fide quantum states [30] are valid states in this composite model. The effect cone is constructed in accordance with the no-restriction hypothesis that allows all mathematically consistent effects in the theory:

$$\begin{aligned}\mathcal{E}^{AB}_{+}[\max] := \{\pi \mid \pi = \sum_i \pi_i^A \otimes \pi_i^B;\ \pi_i^A \in \mathcal{P}(\mathcal{H}^A) \\ \pi_i^B \in \mathcal{P}(\mathcal{H}^B)\}.\end{aligned}$$

$\mathcal{E}^{AB}_{+}[\max]$ also forms a cone which is dual to the state cone $\Omega^{AB}_{+}[\max]$. In the other extreme, minimal tensor product contains only separable states, but the effect space gets enlarged here. More particularly, the role of state and effect cones of maximal tensor product are interchanged in the minimal case,

$$\Omega^{AB}_{+}[\min] := \mathcal{E}^{AB}_{+}[\max] \ \& \ \mathcal{E}^{AB}_{+}[\min] := \Omega^{AB}_{+}[\max].$$

Quantum composition lies in between and the state and effect cones becomes self dual in this case, *i.e.*, $\Omega^{AB}_{+}[Q] = \mathcal{P}(\mathcal{H}^A \otimes \mathcal{H}^B) = \mathcal{E}^{AB}_{+}[Q]$. Contributions of the present work are the following two theorems:

Theorem 1. *Maximal tensor product of two elementary quantum violates the IC principle.*

Theorem 2. *Minimal tensor product of two elementary quantum violates the IC principle.*

Discussion.– The notion of composition is one of the guiding tools to fabricate our worldview – while complex objects are composed of elementary parts, some compositions deem implausible [31]. The idea becomes important even while constructing theories in Physics [32–34]. In this work we study this particular aspect while considering multiple quantum systems. Interestingly, we show that the principle of Information Causality [13] plays crucial role in selecting the quantum composition among different mathematical possibilities. In the process it discards even a local theory as unphysical, which might make IC champion over the other principles [14–16]. As IC can derive some structural aspect of quantum theory it thus brings some physical ground justifying Hilbert space formulation of the theory. The potentiality arises from the communication aspect of IC principle which invokes preparations (for encoding) and measurements (for decoding) of the involved systems and thus becomes more structure sensitive. As for future it would be quite interesting to see

what other structural aspects of multipartite quantum systems can be rationalized with IC as the study in the present work is limited to bipartite compositions only.

[1] D. Bohm; A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I, Phys. Rev. **85**, 166 (1952).

[2] H. Everett; "Relative State" Formulation of Quantum Mechanics, Rev. Mod. Phys. **29**, 454 (1957).

[3] J. A. Wheeler; Assessment of Everett's "Relative State" Formulation of Quantum Theory, Rev. Mod. Phys. **29**, 463 (1957).

[4] L. E. Ballentine; The Statistical Interpretation of Quantum, Rev. Mod. Phys. **42**, 358 (1970).

[5] R. B. Griffiths; Consistent histories and the interpretation of quantum mechanics, J. Stat. Phys. **36**, 219 (1984).

[6] G. C. Ghirardi, A. Rimini, and T. Weber; Unified dynamics for microscopic and macroscopic systems, Phys. Rev. D **34**, 470 (1986).

[7] R. Omnès; Consistent interpretations of quantum mechanics, Rev. Mod. Phys. **64**, 339 (1992).

[8] C. A. Fuchs and R. Schack; Quantum-Bayesian coherence, Rev. Mod. Phys. **85**, 1693 (2013).

[9] M. Tegmark; The Interpretation of Quantum Mechanics: Many Worlds or Many Words? Fortsch. Phys. **46**, 855 (1998).

[10] M. Schlosshauer, J. Kofler, and A. Zeilinger; A Snapshot of Foundational Attitudes Toward Quantum Mechanics, Stud. Hist. Phil. Mod. Phys. **44**, 222 (2013).

[11] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, and F. Unger; Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial, Phys. Rev. Lett. **96**, 250401 (2006).

[12] W. van Dam; Implausible consequences of superstrong nonlocality, Nat. Comput. **12**, 9 (2013).

[13] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski; Information causality as a physical principle, Nature **461**, 1101 (2009).

[14] M. Navascués and H. Wunderlich; A glance beyond the quantum model, Proc. R. Soc. London A **466**, 881 (2010).

[15] T. Fritz, A.B. Sainz, R. Augusiak, J Bohr Brask, R. Chaves, A. Leverrier, and A. Acín; Local orthogonality as a multipartite principle for quantum correlations, Nat Commun **4**, 2263 (2013).

[16] B. Amaral, M. T. Cunha, and A. Cabello; Exclusivity principle forbids sets of correlations larger than the quantum set, Phys. Rev. A **89**, 030101(R) (2014).

[17] C. H. Bennett and S. J. Wiesner; Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states, Phys. Rev. Lett. **69**, 2881 (1992).

[18] A. Ahanj, S. Kunkri, A. Rai, R. Rahaman, and P. S. Joag; Bound on Hardy's nonlocality from the principle of information causality, Phys. Rev. A **81**, 032103 (2010)

[19] S. Das, M. Banik, M. R. Gazi, A. Rai, S. Kunkri, and R. Rahaman; Bound on tri-partite Hardy's nonlocality respecting all bi-partite principles, Quantum Inf Process **12**, 3033 (2013).

[20] Md. R. Gazi, M. Banik, S. Das, A. Rai, and S. Kunkri; Macroscopic locality with equal bias reproduces with high fidelity a quantum distribution achieving the Tsirelson's bound, Phys. Rev. A **88**, 052115 (2013).

[21] N. Miklin and M. Pawłowski; Information Causality without Concatenation, Phys. Rev. Lett. **126**,

220403 (2021).

[22] I. Namioka and R. R. Phelps; Tensor products of compact convex sets, Pac. J. Math. **31**, 469 (1969).

[23] H. Barnum, S. Beigi, S. Boixo, M. B. Elliott, and S. Wehner; Local Quantum Measurement and No-signaling Imply Quantum Correlations, Phys. Rev. Lett. **104**, 140401 (2010).

[24] J. Barrett; Information processing in generalized probabilistic theories, Phys. Rev. A **75**, 032304 (2007).

[25] G. Chiribella, G. M. D'Ariano, and P. Perinotti; Informational derivation of quantum theory, Phys. Rev. A **84**, 012311 (2011).

[26] H. Barnum and A. Wilce; Information processing in convex operational theories, Electron. Notes Theor. Comput. Sci. **70**, 3 (2011).

[27] L. Masanes and M. P. Müller; A derivation of quantum theory from physical requirements, New J. Phys. **13**, 063001 (2011).

[28] M. Plávala; General probabilistic theories: An introduction, arXiv:2103.07469 [quant-ph].

[29] H. Barnum and A. Wilce; Local Tomography and the Jordan Structure of Quantum Theory, Found. Phys. **44**, 192 (2014).

[30] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki; Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[31] L. S. Penrose and R. Penrose; Impossible objects: A special type of visual illusion, Br. J. Psychol. **49**, 31 (1958).

[32] L. Hardy; On the theory of composition in physics, in Computation, Logic, Games, and Quantum Foundations, The Many Facets of Samson Abramsky, edited by B. Coecke, L. Ong, and P. Panangaden, Lecture Notes in Computer Science Vol. 7860 (Springer, Berlin, Heidelberg, 2013), 10.1007/978-3-642-38164-5_7.

[33] L. Hardy; Operational General Relativity: Possibilistic, Probabilistic, and Quantum, arXiv:1608.06940 [gr-qc].

[34] A. D. Bhowmik, P. Parashar, G. Kar, and M. Banik; From no causal loop to absoluteness of cause: discarding the quantum NOT logic, arXiv:2109.09953 [quant-ph].

Mutually unbiased measurements

Máté Farkas[1] *

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

Abstract. We introduce mutually unbiased measurements (MUMs), a generalisation of mutually unbiased bases (MUBs). The MUM definition naturally arises as the unique maximisier of a family of Bell inequalities, as well as a dimension-independent generalisation of the complementarity property of MUBs. We develop an algebraic characterisation of MUMs and show that—while exhibiting many similarities—MUMs are strictly more general than MUBs, and that the number of MUMs with a fixed number of outcomes is unbounded. We then extend the family of Bell inequalities from a pair of MUMs to an arbitrary number of them, and tackle the long-standing open problem of the number of MUBs in composite dimensions through numerical optimisation of Bell inequalities.

Keywords: quantum measurements, mutually unbiased bases, Bell inequalities, device-independence

Submission based on *Science Advances* **7**, eabc3847 (2021), *Quantum* **6**, 778 (2022), and *IEEE Transactions on Information Theory* **69**(6), 3814–3824 (2023) with many co-authors.

Mutually unbiased bases (MUBs) [1] are highly symmetric pairs of orthonormal bases in complex Hilbert spaces: the magnitude of the overlap between any two vectors from the two different bases is uniform. That is, two orthonormal bases $\{|p_a\rangle\}_{a=1}^d$ and $\{|q_b\rangle\}_{b=1}^d$ on $\mathbb{C}^d$ are MUBs if

$$|\langle p_a|q_b\rangle| = 1/\sqrt{d} \quad \forall a, b.$$

A pair of MUBs can also be described by a complex Hadamard matrix (H such that $HH^\dagger = d\mathbb{I}$ and $|H_{ab}| = 1$) containing all the phases, $H_{ab} = \sqrt{d}\langle p_a|q_b\rangle$. For later convenience, it is worth noting that such a Hadamard matrix can be brought to a *dephased* form ($H_{1b} = H_{a1} = 1$ for all a, b) by a suitable unitary transformation and by attaching phases to the MUB vectors.

MUBs are ubiquitous in various areas of quantum information theory through the corresponding rank-1 projective measurements $\{P_a = |p_a\rangle\langle p_a|\}_{a=1}^d$ and $\{Q_b = |q_b\rangle\langle q_b|\}_{b=1}^d$. Among other tasks, they are optimal for state determination [2], highly useful in quantum cryptography [3, 4, 5] and in quantum communication protocols [6, 7]. Their usefulness in these tasks can be traced back to their *complementarity* property, which can also be thought of as an alternative definition of MUBs: if a rank-1 projective measurement yields a definite outcome on some quantum state, then a rank-1 projective measurement unbiased to it will yield a uniformly random outcome on the same state.

Due to their highly symmetric structure and extensive use in quantum information, significant research effort has been invested into studying MUBs in both the mathematics and the physics community. However, despite all these efforts, there are still open questions regarding the structure of MUBs. Most notably, the number of bases that are pairwise unbiased (in the following, "the number of MUBs") is unknown in composite dimensions. This problem was mentioned in Zauner's PhD thesis in 1999, in which he conjectured that there are no more than three MUBs in dimension six [8]. Up to date, we only know that there are at least three and at most seven MUBs in dimension six, and it is commonly believed that Zauner's conjecture holds.

In this work, we study the structure of MUBs through the lens of *Bell scenarios* [9], which will also lead to a natural generalisation of MUBs. In a Bell scenario, two distant parties—Alice and Bob—perform repeated measurements on a shared physical system. The experiment is described by the conditional probability distribution $p(a, b|x, y)$ specifying the probability of Alice (Bob) obtaining the measurement outcome a (b) upon selecting the measurement x (y). These distributions are often called *correlations* or *behaviours*.

Sharing a quantum state and performing local quantum measurements on it in a Bell scenario can lead to *nonlocal* correlations. These are correlations that do not have a *local realist* explanation—that is, they cannot be thought of as a probabilistic mixture of correlations in which the local outcomes only depend on the local measurement choices. These local correlations form a convex polytope, and the hyperplanes separating this polytope from more general quantum correlations are called *Bell inequalities* (a Bell inequality essentially specifies a bound on the value of a linear functional—*Bell functional*—over all local correlations). While the original interest in Bell inequalities lies in the fact that they witness nonlocality, their maximal quantum violation is also of fundamental interest, since these characterise the correlations achievable in quantum theory.

In this work, we first devise a family of Bell inequalities, parametrised by an integer $d \geq 2$, which are maximally violated by MUBs in dimension d. In the nonlocal scenario where our Bell inequalities are defined (see Fig. 1), Bob has access to two measurements with d outcomes each, $\{P_b\}_{b=1}^d$ and $\{Q_b\}_{b=1}^d$: these will be the MUB measurements in the optimal realisation that gives rise to the maximal violation. Alice, on the other hand, has access to d^2 measurements (indexed by x_1x_2 such that $x_1, x_2 \in \{1, \ldots, d\} \equiv [d]$) with three outcomes each. The

*mate.farkas@icfo.eu

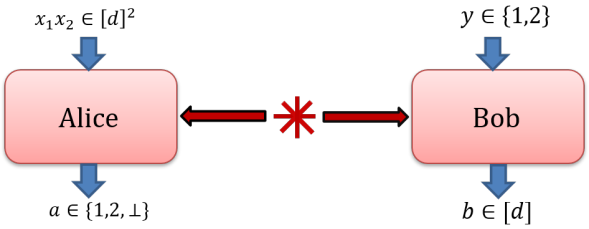


Figure 1: Bell scenario for two MUBs of dimension d. Alice receives one of d^2 inputs and produces a ternary output while Bob receives a binary input and produces a d-valued output.

idea is that in the optimal realisation, the first two outcomes of the measurement indexed by x_1x_2 correspond to the projections onto the two eigenstates of the rank-two operator $P_{x_1} - Q_{x_2}$. The third outcome projects onto the kernel of $P_{x_1} - Q_{x_2}$, which is non-empty whenever $d > 2$. In the inequality, we enforce the use of this third outcome by introducing a penalty term whenever Alice outputs one of the first two outcomes.

We prove the maximal value of our Bell inequalities for every d, and that the maximal quantum violation certifies (self-tests) the maximally entangled state of dimension d, $|\phi_d^+\rangle \equiv 1/\sqrt{d}\sum_{j=1}^{d}|jj\rangle$. Furthermore, the maximal violation certifies the following algebraic relations of Bob's measurement operators:

$$dP_aQ_bP_a = P_a, \quad dQ_bP_aQ_b = Q_b \quad \forall a, b.$$

We call a pair of measurements satisfying these relations *mutually unbiased measurements* (MUMs). In particular, it is easy to see that any pair of MUBs are also MUMs. In fact, the MUM definition is equivalent to the MUB definition if we require all the operators to be rank-1 (or equivalently, if we restrict the dimension to be the same as the outcome number).

Crucially, the MUM definition is equivalent to complementarity without the rank-1 constraint: the statement that a pair of measurements are MUMs is equivalent to the statement that they are projective, and that if one of them yields a definite outcome on a quantum state then the other one yields a uniformly random outcome on the same state. Hence, one can think of MUMs as an operational definition of MUB-ness: MUMs perfectly capture complementarity, but do not require specifying the Hilbert space dimension (that is, the definition is "device-independent"). There are further operational properties that link MUMs to MUBs: in particular, any pair of d-outcome MUMs satisfies the same entropic uncertainty relations and admits the same generalised incompatibility robustness as an arbitrary pair of MUBs in dimension d. Moreover, MUMs are among the most incompatible pairs of measurements for a fixed outcome number (similarly to MUBs, which are among the most incompatible pairs of measurements in a given dimension).

Regarding the mathematical description, a pair of MUMs is described by a *Hadamard matrix of unitaries*. This is a block matrix H such that $HH^\dagger = d\mathbb{I}$, with unitary blocks, where the block size equals the rank of each projection in the MUMs. Clearly, Hadamard matrices of unitaries with block size one are just complex Hadamard matrices, and we recover the MUB definition. Similarly to dephasing a complex Hadamard matrix, one can also bring a Hadamard matrix of unitaries to a *canonical form*, in which the first row and the first column of the unitary blocks are identity operators.

This characterisation of MUMs allows us to formally study the MUB-MUM correspondence. In particular, while we saw that every pair of MUBs is also a pair of MUMs, the converse turns out not to be true, and MUMs are more general than MUBs. The simplest class of measurement pairs that satisfy the MUM conditions but that are not MUBs is simply direct sums of MUBs. That is, measurements acting on a direct sum Hilbert space with d-dimensional summands, such that restricted to any of these summands, the measurements are MUBs. We prove a simple characterisation of direct sums of MUBs: they correspond to MUMs such that all the unitary operators commute in the canonical form of the corresponding Hadamard matrix of unitaries.

Using this characterisation, we provide examples of MUMs that are not direct sums of MUBs for outcome numbers four, five and six. Furthermore, we construct an isomorphism between Hadamard matrices of unitaries of block size two, and quaternionic Hadamard matrices. This isomorphism allows us to systematically construct MUMs that are not direct sums of MUBs from dephased quaternionic Hadamard matrices with non-commuting entries. We construct such examples for many small prime outcome numbers, and construct an infinite family for outcome number four. Last, we show an even stronger difference between MUMs and MUBs: using the Choi isomorphism and a semidefinite programming (SDP) characterisation, we show that there exist MUM pairs that cannot be mapped to a pair of MUBs by any completely positive unital map.

Another crucial difference arises when one looks at the number of MUMs for a fixed number of outcomes: in stark contrast to the number of MUBs in a fixed dimension, we show that there exist an unbounded number of MUMs for any fixed number of outcomes. We prove this by an explicit construction using Hilbert spaces of unbounded dimension.

With this understanding of the structure of MUMs, we attempt to tackle Zauner's conjecture through Bell inequalities. Namely, we are looking to find Bell inequalities that are maximally violated if and only if n MUBs exist in dimension d. Given our Bell inequalities for MUMs and the above results, there are two main challenges that we are facing: first, we need to extend our Bell inequalities to an arbitrary number of MUMs, and then we need to restrict the dimension of the measurements (since there exist an arbitrary number of MUMs for a fixed outcome number, but restricting the dimension recovers MUBs).

To extend our Bell inequalities to n MUMs with d outcomes each, we give n measurement settings to Bob

instead of just two. Then, to each pair of Bob's measurements, we associate d^2 measurements for Alice, with three outcomes each. We then define the final Bell inequality as a sum of the original Bell inequalities for every pair of Bob's measurements and the corresponding d^2 measurements of Alice. It is then clear that the maximal violation is achieved if and only if Bob's measurements are n MUMs with d outcomes each. In particular, the maximal violation is reached by any set of n MUBs in dimension d. Thus, we conclude that n MUBs in dimension d exist if and only if the maximum quantum violation of the corresponding Bell inequality is reached in dimension d. Hence, we turned the problem of finding MUBs into the optimisation problem of finding the maximum value of a Bell inequality in a fixed dimension.

In order to perform this optimisation, we employed three numerical methods. First, we notice that by fixing the state in the Bell scenario to the maximally entangled state in dimension d, the optimisation becomes a bilinear optimisation problem in terms of Alice's and Bob's measurement operators. Fixing Alice's measurements, finding the optimal measurements for Bob is a standard SDP, and vice versa. Thus, successively optimising over either Alice's or Bob's measurement operators, the *see-saw* algorithm eventually converges to a (local) maximum.

Second, by further requiring Alice's operators to be the optimal ones for any fixed selection of Bob's operators, we eliminate Alice's operators from the optimisation. This comes at the cost of the objective function becoming non-linear in Bob's operators. We employ a general non-linear SDP optimisation technique—with a guarantee of converging to a generalised stationary point—to perform this maximisation [10].

The third technique that we apply is another non-linear optimisation technique inspired by simulated annealing [11]. In an iterative fashion, we update Bob's measurement bases via a small perturbation. We accept the new bases if they lead to an improved Bell violation, but only accept with a certain ("temperature"-dependent) probability if they lead to a smaller Bell violation. Accepting updates in the "wrong" direction allows the algorithm to escape local maxima. By successively decreasing the temperature parameter, we end up with more stringent update conditions, and eventually the algorithm converges to a local maximum.

All three methods correctly identify known cases in low dimensions, that is, find MUBs in cases where it is known that they exist, and do not find MUBs in cases where it is known that they do not exist. Moreover, in the cases where MUBs do not exist, all three methods converge to (numerically) the same set of bases. We finally apply our techniques to some unknown cases, most notably to four bases in dimension six, where the three methods converge to the same set of bases, which are not MUBs. These results (see Table 1) provide further numerical evidence to Zauner's conjecture. Furthermore, the simulated annealing methods also suggest that there are no more then three MUBs in dimension ten.

Since the above methods provide lower bounds on the Bell violation by explicit measurement constructions, they can only be used to prove the existence of MUBs. In order to prove non-existence (i.e., to prove Zauner's conjecture), *upper* bounds are necessary. One method for upper bounding Bell inequality violations in a given dimension was provided by Navascués and Vértesi [12]. This method allows us to numerically rule out four MUBs in dimension two (a known result). However, applying this method to higher dimensions is computationally very costly. Furthermore, it is difficult to derive analytic results with this method, as it requires random sampling of so-called moment matrices until these matrices span the space of matrices that can be generated in a fixed dimension.

An alternative technique for upper bounding Bell violations in a fixed dimension is the SDP hierarchy of Moroder et al. [13]. Every level of the hierarchy is a standard SDP, providing increasingly tighter bounds on a Bell inequality violation with a restriction on the entanglement negativity of the shared state. Since the entanglement negativity is bounded in a fixed dimension, this restriction effectively restricts the dimension. In order to obtain an analytic bound, one may look at the dual of the SDP. In particular, any feasible point of the dual SDP provides a valid analytic bound on the Bell violation. We may make an educated guess on the optimal solution to the dual SDP by first noting that the Moroder hierarchy is a modification of the so-called NPA hierarchy, which provides upper bounds on Bell violations without the entanglement restriction [14]. Then, we note that the dual SDP of the NPA hierarchy is a so-called sum-of-squares (SOS) decomposition, and we can find an SOS decomposition for our MUB inequalities already on the first level of the NPA hierarchy. In a future work, we plan to investigate the dual of the Moroder hierarchy, and adapt this SOS decomposition in order to find analytic upper bounds for our (and other) Bell inequalities in a fixed dimension. Apart from the prospect of analytically proving Zauner's conjecture, this technique would provide us a tool to analytically bound Bell violations in fixed dimensions.

Table 1: Normalised difference between the maximal quantum value of the Bell inequality for n MUBs in dimension d and the maximal value found in dimension d using our numerical tools. Zero indicates that we found MUBs, while non-zero values indicate that we did not.

n \ d	2	3	4	5	6
2	0.00000	0.00000	0.00000	0.00000	0.00000
3	0.00000	0.00000	0.00000	0.00000	0.00000
4	**0.01440**	0.00000	0.00000	0.00000	**0.00004**
5	-	**0.00391**	0.00000	0.00000	-
6	-	-	**0.00161**	0.00000	-
7	-	-	-	**0.00091**	-

References

[1] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 08(04):535–640, 2010.

[2] I D Ivonovic. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14(12):3241–3245, 1981.

[3] G. Brassard C. H. Bennett. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (IEEE, 1984)*, 175:8, 1984.

[4] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[5] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81:3018–3021, 1998.

[6] Armin Tavakoli, Alley Hameedi, Breno Marques, and Mohamed Bourennane. Quantum random access codes using single d-level systems. *Phys. Rev. Lett.*, 114:170502, 2015.

[7] Máté Farkas and Jędrzej Kaniewski. Self-testing mutually unbiased bases in the prepare-and-measure scenario. *Phys. Rev. A*, 99:032316, 2019.

[8] Gerhard Zauner. Grundzüge einer nichtkommutativen designtheorie. *PhD thesis*, 1999.

[9] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, 2014.

[10] Hiroshi Yamashita, Hiroshi Yabe, and Kouhei Harada. A primal–dual interior point method for nonlinear semidefinite programming. *Mathematical programming*, 135(1):89–121, 2012.

[11] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi. Optimization by simulated annealing. *Science*, 220(4598):671–680, 1983.

[12] Miguel Navascués and Tamás Vértesi. Bounding the set of finite dimensional quantum correlations. *Phys. Rev. Lett.*, 115:020501, 2015.

[13] Tobias Moroder, Jean-Daniel Bancal, Yeong-Cherng Liang, Martin Hofmann, and Otfried Gühne. Device-independent entanglement quantification and related applications. *Phys. Rev. Lett.*, 111:030501, 2013.

[14] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, 2007.

Remote preparation and manipulation of non-Gaussian states with quantum advantage

Yu Xiang[1 2 *] Qiongyi He[1 2 3 4]

[1]*State Key Laboratory for Mesoscopic Physics, School of Physics, Frontiers Science Center for Nano-optoelectronics, Peking University, Beijing 100871, China*
[2]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan, Shanxi 030006, China*
[3]*Peking University Yangtze Delta Institute of Optoelectronics, Nantong, Jiangsu, China*
[4]*Hefei National Laboratory, Hefei 230088, China*

Abstract. How to remotely prepare and manipulate quantum states between remote users is one of the core issues in constructing quantum networks. Quantum entanglement can provide an efficient means to solve this problem. For some continuous-variable (CV) states, the Wigner function can reach negative values. This Wigner negativity can ensure superior metrological power in quantum metrology tasks, and offers insight into studying fundamental quantum mechanics, such as the classical-quantum boundary. In recent two years, we has made some progress on this topic, including proposing a series of novel theoretical schemes for remote generation and manipulation of non-Gaussian states based on quantum steering, and then collaborated with experimental groups to implement them. These results pave the way for exploiting Wigner negativity as a valuable resource for numerous quantum information protocols.

Keywords: EPR steering, Non-Gaussian states, Remote state preparation

As the core resource of quantum communication, quantum computation, and sensing technologies, quantum entanglement has become the focus of research in the international scientific and technological community. Irrespective of the physical implementation, quantum information processing can be divided into two types according to the degree of freedom used to encode information: the use of discrete variables (e.g., qubit) and that of high-dimensional, continuous-variable (CV) states (e.g., Gaussian state). As the CV system can generate quantum entanglement deterministically and keep high long-range transmission efficiency, it acts as an important resource for quantum communication, quantum cryptography, and other applications, while related theoretical and experimental research has developed rapidly. Compared with the widely studied CV Gaussian systems, continuous-variable (CV) complex (non-Gaussian) states have attracted much attention as indispensable resources for universal quantum computing. As two typical classes of non-Gaussian states, Schrödinger's cat state and Wigner-negative state have become popular research subjects.

It has been recently proved that quantum steering [1, 2, 3] proves a necessary requirement to remotely prepare a Wigner-negative state [4]. In multi-mode CV systems, we quantitatively studied the remote preparation and distribution of Wigner negativity that is remotely created via multipartite EPR steering, in which non-Gaussian operations performed on one steered node of quantum network produce Wigner negativity in different distant nodes, as shown in Fig. 1. By constructing Coffman-Kundu-Wootters (CKW) type monogamy constraint, it has been revealed that the generated Wigner negativity cannot be freely distributed among users, which reads as

$$\mathcal{N}_{B_1B_2\ldots B_n}(\mathcal{L}_{A|B_1B_2\ldots B_n}) \geq \sum_{i=1}^{n} \mathcal{N}_{B_i}(\mathcal{L}_{A|B_i}), \quad (1)$$

where $\mathcal{N}_{B_j\ldots B_k}$ denotes the Wigner negativity created in the set of modes $(B_j \ldots B_k)$ by performing some appropriate operations $\mathcal{L}_{A|B_j\ldots B_k}$ on subsystem A. This indicates that the sum of the Wigner negativities generated in the individual modes cannot exceed their intergroup negativity.

Additionally, for one of the commonly used non-Gaussian operations, photon subtraction $\mathcal{S}$, we derive the amount of generated Wigner negativity can be fully char-

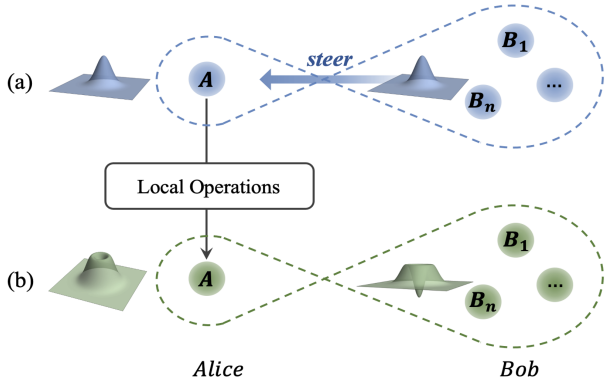


Figure 1: Scheme of the remote generation of Wigner negativity through EPR steering in a multipartite scenario. (a) The initial Gaussian steerable system; (b) After some appropriate local operations on the steered mode hold by Alice, the steering subsystem hold by Bob becomes non-Gaussian with Wigner negativity.

*xiangy.phy@pku.edu.cn

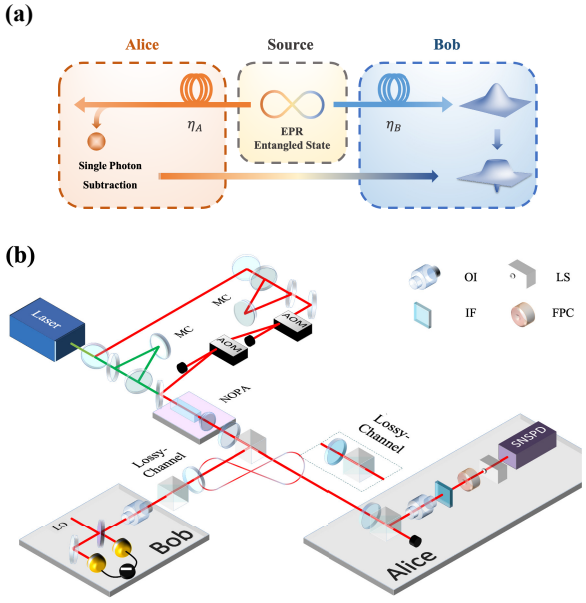


Figure 2: The principle and experimental setup. (a) Schematic of the remote preparation of Wigner negativity. We first prepare a Gaussian EPR entangled state and then transmit two entangled optical fields to two distant nodes controlled by Alice and Bob, where the lossy channels are characterized by η_A and η_B, respectively. Then once Alice successfully performs a single-photon subtraction from her mode, the remote Bob's mode collapses to a Wigner-negative state. (b) Experimental setup. Two acousto-optic modulators (AOM) controlled by the periodically signals are used to chop the seed beam. The NOPA is composed of a type-II KTP crystal and a concave mirror with 50 mm radius. Lossy channel is simulated by the combination of a half wave plate (HWP) and a polarization beamsplitter (PBS). The optical isolators are used to avoid the back scattered light to the NOPA cavity. SNSPD: superconducting nanowire single-photon detector, LO: local oscillator, MC: mode cleaner, OI: optical isolator, LS: laser shutter, IF: interference filter, FPC: Fabry-Perot cavity.

acterized by the purity of the initial states, i.e.,

$$\mathcal{N}_B(\mathcal{S}_{A|B}) = 2\left[\frac{e^{\frac{\mu_A\mu_B-\mu_{AB}\mu_A}{\mu_{AB}-\mu_A\mu_B}}(\mu_A\mu_B-\mu_{AB})}{\mu_{AB}(\mu_A-1)}-1\right]. \tag{2}$$

Hence, EPR steering provides a necessary bridge to induce Wigner negativity, but it is insufficient to unambiguously quantify the created Wigner negativity. This work has been published in npj Quantum Information [5].

After making this theoretical progress, we collaborated with the group of Prof. Xiaolong Su at Shanxi University and realized the remote preparation of Wigner-negative states between space-separated stations for the first time. Based on two-mode EPR entangled optical fields, the qualitative and quantitative relationship between quantum steering and generated Wigner negativity have been verified. The principle and experimental setup are shown in Fig. 2. In this scheme, two optical modes of a CV EPR entangled state are sent to Alice and Bob, respectively. Through quantum tomography and homodyne detection on each mode, the covariance matrix of the initial Gaussian system can be reconstructed, hence, the Gaussian entanglement can be fully analyzed. Alice then performs single-photon subtraction by splitting her mode with a beam splitter with around 4% reflectivity and implementing single-photon detection on it. When a photon is detected by the superconducting nanowire single-photon detector, which means the photon is successfully subtracted, Wigner negativity is immediately generated in Bob's mode. By adjusting the channel transmission efficiency on Bob's side, it was experimentally verified that Bob can only obtain a non-Gaussian state with Wigner negativity when Bob can steer Alice's state. Moreover, it is also demonstrated that the remotely generated Wigner negativity has superior metrological power in quantum precision measurement. This work has been published in Physical Review Letters [6].

References

[1] E. Schrödinger, Proc. Cambridge Philos. Soc. **31**, 555–563 (1935).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777–780 (1935).

[3] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[4] M. Walschaers, N. Treps, Phys. Rev. Lett. **124**, 150501 (2020).

[5] Y. Xiang, S. Liu, J. Guo, Q. Gong, N. Treps, Q. He, M. Walschaers, npj Quantum Information **8**, 21 (2022).

[6] S. Liu, D. Han, N. Wang, Y. Xiang, F. Sun, M. Wang, Z. Qin, Q. Gong, X. Su, Q. He, Phys. Rev. Lett. **128**, 200401 (2022)