Vol.2021-QS-3 No.9
2021/7/2

Hardness of efficiently generating ground states in postselected quantum computation

Yuki Takeuchi[1,a)] Yasuhiro Takahashi[1] Seiichiro Tani[1]

Abstract : Generating ground states of any local Hamiltonians seems to be impossible in quantum polynomial time. In this talk, we give evidence for the impossibility by applying an argument used in the quantum-computational-supremacy approach. More precisely, we show that if ground states of any 3-local Hamiltonians can be approximately generated in quantum polynomial time with postselection, then $\mathsf{PP} = \mathsf{PSPACE}$. Our result is superior to the existing findings in the sense that we reduce the impossibility to an unlikely relation between classical complexity classes.

1. Introduction

Quantum computing is expected to outperform classical computing. Indeed, quantum advantages have already been shown in terms of query complexity [1] and communication complexity [2]. Regarding time complexity, it is also believed that universal quantum computing has advantages over classical counterparts. For example, although an efficient quantum algorithm, i.e., Shor's algorithm, exists for integer factorization [3], there is no known classical algorithm that can do so efficiently. However, an unconditional proof that there is no such classical algorithm seems to be hard because an unconditional separation between BQP and BPP implies $\mathsf{P} \neq \mathsf{PSPACE}$. Whether $\mathsf{P} \neq \mathsf{PSPACE}$ is a long-standing problem in the field of computer science.

To give evidence of quantum advantage in terms of computational time, a sampling approach has been actively studied. This approach is to show that if the output probability distributions from a family of (non-universal) quantum circuits can be efficiently simulated in classical polynomial time, then the polynomial hierarchy (PH) collapses to its second or third level. Since it is widely believed that PH does not collapse, this approach shows one kind of quantum advantage (under a plausible complexity-theoretic assumption). This type of quantum advantage is called quantum computational supremacy [4]. The quantum-computational-supremacy approach is remarkable because it reduces the impossibility of an efficient classical simulation of quantum computing to unlikely relations between classical complexity classes (under conjectures such as the average-case hardness conjecture). Since classical complexity classes have been studied for a longer time than quantum complexity classes, unlikely relations between classical complexity classes would be more dramatic than those involving quantum complexity classes. As sub-universal quantum computing models showing quantum computational supremacy, several models have been proposed, such as boson sampling [5], [6], [7], instantaneous quantum polynomial time (IQP) [8], [9] and its variants [10], [11], [12], [13], deterministic quantum computation with one quantum bit (DQC1) [14], [15], Hadamard-classical circuit with one qubit (HC1Q) [16], and quantum random circuit sampling [17], [18], [19], [20]. A proof-of-principle demonstration of quantum computational supremacy has recently been achieved using quantum random circuit sampling with 53 qubits [21]. Regarding other models, small-scale experiments have been performed toward the goal of demonstrating quantum computational supremacy [22], [23], [24], [25], [26], [27].

On the other hand, the limitations of universal quantum computing are also actively studied (e.g., see Refs. [28], [29], [30]). Understanding these limitations is important to clarify how to make good use of universal quan-

1 NTT コミュニケーション科学基礎研究所
NTT Communication Science Laboratories, Atsugi, Kanagawa 243–0198, Japan
a) yuki.takeuchi.yt@hco.ntt.co.jp

tum computers. For example, it is believed to be impossible in the worst case to generate ground states of a given local Hamiltonian in quantum polynomial time, while their heuristic generation has been studied using quantum annealing [31], variational quantum eigensolvers (VQE) [32], and quantum approximate optimization algorithms (QAOA) [33]. Since deciding whether the ground-state energy of a given 2-local Hamiltonian is low or high with polynomial precision is a QMA-complete problem [34], if efficient generation of the ground states is possible, then $\mathsf{BQP} = \mathsf{QMA}$ that seems to be unlikely. As well as the gap between quantum and classical computing in terms of time complexity, it is hard to unconditionally show the impossibility of efficiently generating the ground states.

In this talk, we utilize a technique from the quantum-computational-supremacy approach to give new evidence for this impossibility. More precisely, in Theorem 1, we show that if the ground states of any given 3-local Hamiltonians can be approximately generated in quantum polynomial time with postselection, then $\mathsf{PP} = \mathsf{PSPACE}$. Similar to the quantum-computational-supremacy approach, this consequence leads to the collapse of a hierarchy, i.e., the counting hierarchy (CH) collapses to its first level ($\mathsf{CH} = \mathsf{PP}$). In Theorem 2, we consider a different notion of approximation and show that if the probability distributions obtained from the ground states can be approximately generated in quantum polynomial time with postselection, then $\mathsf{PP} = \mathsf{PSPACE}$. Theorem 2 studies the hardness of approximately generating the ground states from a different perspective, because it is closely related to the hardness of approximately generating the probability distributions. Our results are different from the existing ones on the impossibility of efficient ground-state generation in a sense that we reduce the impossibility to unlikely relations between classical complexity classes as in the quantum-computational-supremacy approach.

2. Preliminaries

Before we explain our results, we will briefly review preliminaries required to understand our argument. We use several complexity classes that are sets of decision problems. Here, decision problems are mathematical problems that can be answered by YES or NO. We mainly use complexity classes CH, $\mathsf{postBQP}$, and $\mathsf{postQMA}$, where the latter two are postselected versions of BQP and QMA, respectively. We assume that readers know the major complexity classes, such as P, PP, PSPACE, and PH (for their definitions, see Ref. [35]).

The class CH is the union of classes $\mathsf{C}_k\mathsf{P}$ over all non-negative integers k, i.e., $\mathsf{CH} = \cup_{k\geq 0}\mathsf{C}_k\mathsf{P}$, where $\mathsf{C}_0\mathsf{P} = \mathsf{P}$ and $\mathsf{C}_{k+1}\mathsf{P} = \mathsf{PP}^{\mathsf{C}_k\mathsf{P}}$ for all $k \geq 0$. We say that CH collapses to its k-th level when $\mathsf{CH} = \mathsf{C}_k\mathsf{P}$. The first-level collapse of CH is thought to be especially unlikely. This is because, from Toda's theorem [36], $\mathsf{PH} \subseteq \mathsf{P}^{\mathsf{PP}} \subseteq \mathsf{CH}$. Therefore, if $\mathsf{CH} = \mathsf{PP}$, then $\mathsf{PH} \subseteq \mathsf{PP}$. Although it is unknown whether this inclusion does not hold, it is used as an unlikely consequence in several papers such as Ref. [37]. At least, we can say that it is difficult to show that $\mathsf{PH} \subseteq \mathsf{PP}$ holds. This is because there exists an oracle relative to which PH (more precisely, P^{NP}) is not contained in PP [38].

The complexity class $\mathsf{postQMA}$ is defined as follows [39], [40]: a language L is in $\mathsf{postQMA}$ if and only if there exist a constant $0 < \delta < 1/2$, polynomials n, m, and k, and a uniform family $\{U_x\}_x$ of polynomial-size quantum circuits, where x is an instance, and U_x takes an n-qubit state ρ and ancillary qubits $|0^m\rangle$ as inputs, such that (i) $\Pr[p = 1 \mid \rho] \geq 2^{-k}$, where p is a single-qubit postselection register, for any ρ, (ii) if $x \in L$, then there exists a witness ρ_x such that $\Pr[o = 1 \mid p = 1, \rho_x] \geq 1/2 + \delta$ with a single-qubit output register o, and (iii) if $x \notin L$, then for any ρ, $\Pr[o = 1 \mid p = 1, \rho] \leq 1/2 - \delta$. In this definition, "polynomials" mean the ones in the length $|x|$ of the instance x. Note that $\mathsf{postQMA}$ is denoted by $\mathsf{QMA}_{\mathsf{postBQP}}$ in Ref. [39].

The following is an important lemma:

Lemma1 Any decision problem in $\mathsf{postQMA}$ can be efficiently solved using postselected polynomial-size quantum circuits if a polynomial number of copies of a ground state (i.e., a minimum-eigenvalue state) $|g\rangle$ of an appropriate 3-local Hamiltonian is given (see Fig. 1 (a)). Note that a 3-local Hamiltonian $H = \sum_{i=1}^{t} H^{(i)}$ with a polynomial t is the sum of polynomially many Hermitian operators $\{H^{(i)}\}_{i=1}^{t}$, each of which acts on at most three (possibly geometrically nonlocal) qubits. The operator norm $||H^{(i)}||$ is upper-bounded by one for any $1 \leq i \leq t$.

This lemma can be obtained by combining results in Refs. [39], [41]. The proof is given in our paper [42].

By removing ρ_x and ρ from the definition of $\mathsf{postQMA}$, the complexity class $\mathsf{postBQP}$ is defined. Since $\mathsf{PP} = \mathsf{postBQP}$ [43], readers can replace PP with $\mathsf{postBQP}$ if they are not familiar with the definition of PP.

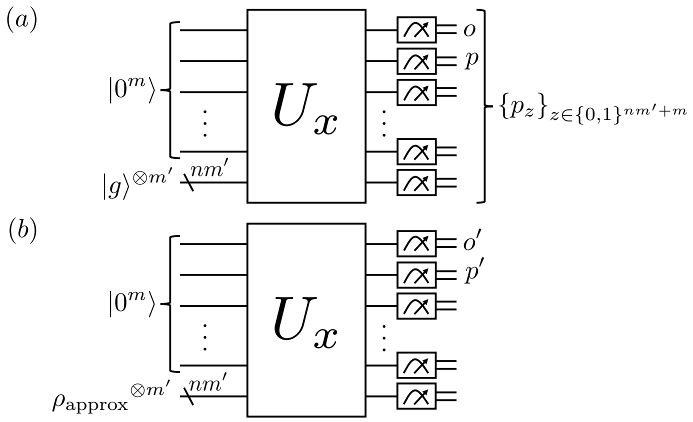

Fig. 1 (a) A quantum circuit U_x with an input state $|0^m\rangle|g\rangle^{\otimes m'}$ to decide whether $x \in L$ or $x \notin L$, where L is in $\mathsf{postQMA}$. Let o and p be output and postselection registers, respectively. If $o = p = 1$, we conclude that $x \in L$. On the other hand, if $p = 1$ and $o = 0$, then $x \notin L$. The output probability distribution of $nm' + m$ qubits is denoted by $\{p_z\}_{z\in\{0,1\}^{nm'+m}}$. Each meter symbol represents a Z-basis measurement. (b) The same quantum circuit as in Fig. 1 (a) except that $|g\rangle$ is replaced with an approximate state ρ_{approx}. The output and postselection registers are denoted by o' and p', respectively.

3. Main results

3.1 Result 1

We show that efficiently generating approximate ground states of a given 3-local Hamiltonian is hard for postselected quantum computation in the worst case. Formally, our first main result is as follows:

Theorem1 Suppose that it is possible to, for any n-qubit 3-local Hamiltonian H and polynomial s, construct a polynomial-size quantum circuit W in classical polynomial time, such that W generates an n-qubit state ρ_{approx} given the success of the postselection, satisfying $\langle g|\rho_{\text{approx}}|g\rangle \geq 1 - 2^{-s}$ for a ground state $|g\rangle$ of H, and the postselection succeeds with probability at least the inverse of an exponential. Then, $\mathsf{PP} = \mathsf{PSPACE}$.

Proof. Our goal is to show that if the quantum circuit W exists, then $\mathsf{postQMA} \subseteq \mathsf{postBQP}$. From $\mathsf{PP} \subseteq \mathsf{PSPACE}$, $\mathsf{postQMA} = \mathsf{PSPACE}$ [39], and $\mathsf{postBQP} = \mathsf{PP}$ [43], this immediately means $\mathsf{PP} = \mathsf{PSPACE}$.

First, we consider the language L that is in $\mathsf{postQMA}$. From Lemma 1, for any instance x, there exist polynomials m and m' such that a polynomial-size quantum circuit U_x with input $|0^m\rangle|g\rangle^{\otimes m'}$ efficiently decides whether $x \in L$ or $x \notin L$ under postselection of $p = 1$ (see Fig. 1 (a)). Here, $|g\rangle$ is a ground state of an n-qubit 3-local

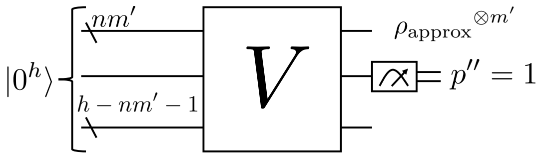

Fig. 2 A polynomial-size quantum circuit V that prepares tensor products $\rho_{\text{approx}}{}^{\otimes m'}$ of an n-qubit approximate ground state from $|0^h\rangle$ with polynomials m' and $h(\geq nm' + 1)$ when the postselection register $p'' = 1$. Note that the probability of obtaining $p'' = 1$ is at least the inverse of an exponential.

Hamiltonian H_x that depends on the instance x, n is a polynomial in $|x|$, and p is the postselection register of U_x. From the definition of $\mathsf{postQMA}$, the postselection succeds with probability $\Pr[p = 1] \geq 2^{-k}$ for a polynomial k.

Next, we show that the quantum circuit in Fig. 1 (a) can be simulated using the quantum circuit W. A classical description of H_x can be obtained in polynomial time from the instance x. From the assumption with the Hamiltonian H_x and the polynomials n, m', and k described above, we can construct the quantum circuit W such that it prepares the approximate ground state ρ_{approx} whose fidelity F with $|g\rangle$ is $(1 - \Theta(2^{-4k}))^{1/m'}$ given the success of the postselection. By repeated execution of W, we can efficiently prepare $\rho_{\text{approx}}{}^{\otimes m'}$ given the success of the postselection. In other words, from the quantum circuit W, we can construct a polynomial-size quantum circuit V that generates tensor products $\rho_{\text{approx}}{}^{\otimes m'}$ of the approximate ground state in the case of $p'' = 1$, where p'' is the postselection register of V (see Fig. 2). The fidelity between $|g\rangle^{\otimes m'}$ and $\rho_{\text{approx}}{}^{\otimes m'}$ is $F^{m'} = 1 - \Theta(2^{-4k})$. When we denote by r the success probability of postselection of W, that of V is $\Pr[p'' = 1] = r^{m'}$, which is at least the inverse of an exponential.

By combining the quantum circuit V in Fig. 2 and U_x in Fig. 1 (a), we can construct a new quantum circuit U'_x, as shown in Fig. 3. Note that since U_x is in a uniform family of polynomial-size quantum circuits as per the definition of $\mathsf{postQMA}$, it can be efficiently constructed from the instance x. The postselection register $\tilde{p}'$ of U'_x is equal to 1 if and only if the postselection registers of V and U_x are both 1. In other words, when $\tilde{p}' = 1$, the quantum circuit V outputs the correct state $\rho_{\text{approx}}{}^{\otimes m'}$, and the quantum circuit U_x is successfully postselected. Therefore, $\Pr[o' = 1 \mid p' = 1] = \Pr[\tilde{o}' = 1 \mid \tilde{p}' = 1]$, where $\tilde{o}'$ is the output register of U'_x, and o' and p' are output and postselection registers in Fig. 1 (b), respectively.

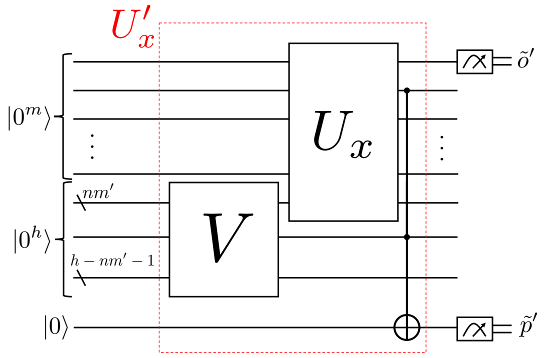

Fig. 3 By using the quantum circuit V in Fig. 2, we construct U'_x. By using this quantum circuit, we can solve any postQMA problem in quantum polynomial time with postselection, i.e., postQMA $\subseteq$ postBQP. The output and postselection registers are denoted by $\tilde{o}'$ and $\tilde{p}'$, respectively.

The only difference between Fig. 1 (a) and (b) is that the input ground states are exact or approximate ones. Hereafter, we will consider $\Pr[o'=1\mid p'=1]$ instead of $\Pr[\tilde{o}'=1\mid\tilde{p}'=1]$.

From a property of fidelity (see Theorem 9.1 and Eq. (9.101) in Ref. [44]), both $|\Pr[o=p=1]-\Pr[o'=p'=1]|$ and $|\Pr[p=1]-\Pr[p'=1]|$ are upper-bounded by $2\sqrt{1-F^{m'}}$. Therefore,

$$\begin{aligned}\Pr[o'=1\mid p'=1] &= \frac{\Pr[o'=p'=1]}{\Pr[p'=1]}\\ &\geq \frac{\Pr[o=p=1]-2\sqrt{1-F^{m'}}}{\Pr[p=1]+2\sqrt{1-F^{m'}}}.\end{aligned}$$

When $x\in L$, the inequality $\Pr[o=1\mid p=1]\geq 1/2+\delta$ holds. Therefore,

$$\begin{aligned}\Pr[o'=1\mid p'=1] &\geq \frac{(1/2+\delta)\Pr[p=1]-2\sqrt{1-F^{m'}}}{\Pr[p=1]+2\sqrt{1-F^{m'}}}\\ &= \frac{1}{2}+\delta-\frac{(3+2\delta)\sqrt{1-F^{m'}}}{\Pr[p=1]+2\sqrt{1-F^{m'}}}\\ &\geq \frac{1}{2}+\delta-\frac{(3+2\delta)\sqrt{1-F^{m'}}}{2^{-k}+2\sqrt{1-F^{m'}}},\end{aligned}$$

where we have used $\Pr[p=1]\geq 2^{-k}$ to derive the last inequality.

On the other hand, when $x\notin L$, from $\Pr[o=1\mid p=1]\leq 1/2-\delta$,

$$\begin{aligned}\Pr[o'=1\mid p'=1] &= \frac{\Pr[o'=p'=1]}{\Pr[p'=1]}\\ &\leq \frac{\Pr[o=p=1]+2\sqrt{1-F^{m'}}}{\Pr[p=1]-2\sqrt{1-F^{m'}}}\\ &\leq \frac{(1/2-\delta)\Pr[p=1]+2\sqrt{1-F^{m'}}}{\Pr[p=1]-2\sqrt{1-F^{m'}}}\\ &= \frac{1}{2}-\delta+\frac{(3-2\delta)\sqrt{1-F^{m'}}}{\Pr[p=1]-2\sqrt{1-F^{m'}}}\\ &\leq \frac{1}{2}-\delta+\frac{(3-2\delta)\sqrt{1-F^{m'}}}{2^{-k}-2\sqrt{1-F^{m'}}}.\end{aligned}$$

Since $1-F^{m'}=\Theta(2^{-4k})$, $(3+2\delta)\sqrt{1-F^{m'}}/(2^{-k}+2\sqrt{1-F^{m'}})=O(2^{-k})$ and $(3-2\delta)\sqrt{1-F^{m'}}/(2^{-k}-2\sqrt{1-F^{m'}})=O(2^{-k})$.

The remaining task is to show that the success probability $\Pr[\tilde{p}'=1]$ of postselection of U'_x is at least the inverse of an exponential, which is required in the definition of postBQP. Since $\Pr[p'=1]\geq\Pr[p=1]-2\sqrt{1-F^{m'}}$ holds, $\Pr[\tilde{p}'=1]=\Pr[p''=1]\Pr[p'=1]\geq r^{m'}(\Pr[p=1]-2\sqrt{1-F^{m'}})=\Omega(2^{-k}r^{m'})$. As a result, we can conclude that if the quantum circuit W exists, then postQMA $\subseteq$ postBQP. □

PP = PSPACE leads to the first-level collapse of the counting hierarchy, i.e., CH = PP. This is because from CH $\subseteq$ PSPACE,

$$\mathsf{PP}\subseteq\mathsf{CH}\subseteq\mathsf{PSPACE}=\mathsf{PP}.$$

Since CH = PP is unlikely as discussed in Sec. 2, Theorem 1 is evidence supporting the conclusion that generation of ground states is impossible even for postselected universal quantum computers.

Theorem 1 is interesting, because it means that although QMA $\subseteq$ postBQP [45], generating ground states of a given 3-local Hamiltonian seems to be beyond the capability of postBQP machines in the worst case. In other words, generating ground states of any 3-local Hamiltonians is just a sufficient condition to solve QMA problems, but it should not be a necessary condition.

3.2 Result 2

Here, we will focus on the output probability distribution $\{p_z\}_z$ in Fig. 1 (a). The proof of Theorem 1 implies that given the values of m and m', and the classical descriptions of H_x and U_x, it is hard to approximate $\{p_z\}_z$ with an exponentially-small additive error c' by using postselected quantum computation. Therefore, the hardness with multiplicative error $1+c'$ also holds. Here, we say that a probability distribution $\{p_z\}_z$ is generated with multiplicative error c if and only if there exists a probability distribution $\{q_z\}_z$ such that $p_z/c\leq q_z\leq cp_z$ for any z. When $p_z/(1+c')\leq q_z\leq(1+c')p_z$ holds for all z, the inequality $\sum_z|p_z-q_z|\leq c'$ also holds. Therefore, if we can show the hardness with additive error c', then the hardness with multiplicative error $1+c'$ is also shown automatically. In short, by using the argument used in the proof of Theorem 1, we can show the hardness with multiplicative error $1+c'$, which is exponentially close to

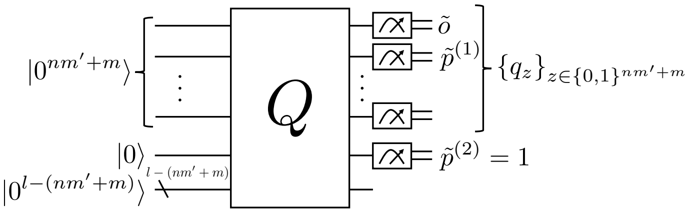

Fig. 4 A quantum circuit Q generates the output probability distribution $\{p_z\}_{z\in\{0,1\}^{nm'+m}}$ with multiplicative error c when the second postselection register $\tilde{p}^{(2)} = 1$, which occurs with probability of at least the inverse of an exponential. In other words, $p_z/c \leq q_z \leq cp_z$ for any z. The symbols $\tilde{o}$ and $\tilde{p}^{(1)}$ are the output and first postselection registers of Q, respectively.

1, for postselected quantum computation. Hereafter, we will use a different argument to show the hardness with multiplicative error $1 \leq c < \sqrt{2}$, i.e., show that in the worst case, it is hard for postselected quantum computation to prepare approximate ground states from which we can generate $\{p_z\}_z$ in Fig. 1 (a) with multiplicative error $1 \leq c < \sqrt{2}$ given the success of the postselection.

The following theorem is our second main result:

Theorem2 Suppose that it is possible to, for any n-qubit 3-local Hamiltonian H, polynomials m and m', and $(nm'+m)$-qubit polynomial-size quantum circuit U, construct an $(l+1)$-qubit polynomial-size quantum circuit Q for some polynomial $l(\geq nm'+m)$ in classical polynomial time, such that Q takes $|0^{l+1}\rangle$ and generates the distribution $\{p_z\}_{z\in\{0,1\}^{nm'+m}}$ with multiplicative error $1 \leq c < \sqrt{2}$ when the postselection succeeds (i.e., $\tilde{p}^{(2)} = 1$ in Fig. 4), where $p_z \equiv |\langle z|U(|0^m\rangle|g\rangle^{\otimes m'})|^2$ for any $z \in \{0,1\}^{nm'+m}$, $|g\rangle$ is a ground state of H, and $\Pr[\tilde{p}^{(2)} = 1] \geq 2^{-k'}$ for a polynomial k'. Then, $\mathsf{PP} = \mathsf{PSPACE}$.

The proof of Theorem 2 is given in our paper [42]. In the proof, we consider the case where all $nm'+m$ qubits in Fig. 1 (a) are measured. However, the same argument holds even when the number of measured qubits is less than $nm'+m$ as long as o and p are measured.

Acknowledgements We thank Tomoyuki Morimae for fruitful discussions. This work is supported by JST [Moonshot R&D – MILLENNIA Program] Grant Number JPMJMS2061. Y. Takeuchi is supported by MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant Number JPMXS0118067394 and JPMXS0120319794. ST is supported by the Grant-in-Aid for Transformative Research Areas No.JP20H05966 of JSPS.

References

[1] D. R. Simon, On the Power of Quantum Computation, SIAM J. Comput. **26**, 1474 (1997).

[2] R. Raz, Exponential separation of quantum and classical communication complexity, in *Proc. of the 31st Symposium on Theory of Computing* (ACM, New York, 1999), p. 358.

[3] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput. **26**, 1484 (1997).

[4] A. W. Harrow and A. Montanaro, Quantum computational supremacy, Nature (London) **549**, 203 (2017).

[5] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in *Proc. of the 43rd Symposium on Theory of Computing* (ACM, San Jose, 2011), p. 333.

[6] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph, Boson Sampling from a Gaussian State, Phys. Rev. Lett. **113**, 100502 (2014).

[7] C. S. Hamilton, R. Kruse, L. Sansoni, S. Barkhofen, C. Silberhorn, and I. Jex, Gaussian Boson Sampling, Phys. Rev. Lett. **119**, 170501 (2017).

[8] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy, Proc. R. Soc. A **467**, 459 (2011).

[9] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Average-Case Complexity Versus Approximate Simulation of Commuting Quantum Computations, Phys. Rev. Lett. **117**, 080501 (2016).

[10] Y. Takahashi, S. Tani, T. Yamazaki, and K. Tanaka, Commuting quantum circuits with few outputs are unlikely to be classically simulatable, Quantum Inf. Comput. **16**, 251 (2016).

[11] Y. Takeuchi and Y. Takahashi, Ancilla-driven instantaneous quantum polynomial time circuit for quantum supremacy, Phys. Rev. A **94**, 062336 (2016).

[12] X. Gao, S.-T. Wang, and L.-M. Duan, Quantum Supremacy for Simulating a Translation-Invariant Ising Spin Model, Phys. Rev. Lett. **118**, 040502 (2017).

[13] J. Miller, S. Sanders, and A. Miyake, Quantum supremacy in constant-time measurement-based computation: A unified architecture for sampling and verification, Phys. Rev. A **96**, 062320 (2017).

[14] T. Morimae, K. Fujii, and J. F. Fitzsimons, Hardness of Classically Simulating the One-Clean-Qubit Model, Phys. Rev. Lett. **112**, 130502 (2014).

[15] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Impossibility of Classically Simulating One-Clean-Qubit Model with Multiplicative Error, Phys. Rev. Lett. **120**, 200502 (2018).

[16] T. Morimae, Y. Takeuchi, and H. Nishimura, Merlin-Arthur with efficient quantum Merlin and quantum supremacy for the second level of the Fourier hierarchy, Quantum **2**, 106 (2018).

[17] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, Nat. Phys. **14**, 595 (2018).

[18] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, Anticoncentration theorems for schemes showing a quantum speedup, Quantum **2**, 65 (2018).

[19] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, On the complexity and verification of quantum random circuit sampling, Nat. Phys. **15**, 159 (2019).

[20] T. Morimae, Y. Takeuchi, and S. Tani, Sam-

pling of globally depolarized random quantum circuit, arXiv:1911.02220.

[21] 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).

[22] B. P. Lanyon, M. Barbieri, M. P. Almeida, and A. G. White, Experimental Quantum Computing without Entanglement, Phys. Rev. Lett. **101**, 200501 (2008).

[23] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, J. C. Gates, B. J. Smith, P. G. R. Smith, and I. A. Walmsley, Boson Sampling on a Photonic Chip, Science **339**, 6121 (2013).

[24] M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, Experimental boson sampling, Nat. Photon. **7**, 540 (2013).

[25] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvão, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, Integrated multimode interferometers with arbitrary designs for photonic boson sampling, Nat. Photon. **7**, 545 (2013).

[26] M. Bentivegna, N. Spagnolo, C. Vitelli, F. Flamini, N. Viggianiello, L. Latmiral, P. Mataloni, D. J. Brod, E. F. Galvão, A. Crespi, R. Ramponi, R. Osellame, and F. Sciarrino, Experimental scattershot boson sampling, Sci. Adv. **1**, e1400255 (2015).

[27] H. Wang, J. Qin, X. Ding, M.-C. Chen, S. Chen, X. You, Y.-M. He, X. Jiang, L. You, Z. Wang, C. Schneider, J. J. Renema, S. Höfling, C.-Y. Lu, and J.-W. Pan, Boson Sampling with 20 Input Photons and a 60-Mode Interferometer in a 10^{14}-Dimensional Hilbert Space, Phys. Rev. Lett. **123**, 250503 (2019).

[28] D. J. Bernstein, Introduction to post-quantum cryptography, in *Post-quantum Cryptography* (Springer, Berlin, 2009), p. 1.

[29] T. Morimae, Finding resource states of measurement-based quantum computing is harder than quantum computing, Phys. Rev. A **96**, 052308 (2017).

[30] A. Gheorghiu and M. J. Hoban, Estimating the entropy of shallow circuit outputs is hard, arXiv:2002.12814.

[31] T. Kadowaki and H. Nishimori, Quantum annealing in the transverse Ising model, Phys. Rev. E **58**, 5355 (1998).

[32] 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).

[33] E. Farhi, J. Goldstone, and S. Gutmann, A Quantum Approximate Optimization Algorithm, arXiv:1411.4028.

[34] J. Kempe, A. Kitaev, and O. Regev, The complexity of the local Hamiltonians problem, SIAM Journal on Computing **35**, 1070 (2006).

[35] S. Arora and B. Barak, *Computational Complexity: A Modern Approach* (Cambridge University Press, Cambridge, 2009).

[36] S. Toda, PP is as Hard as the Polynomial-Time Hierarchy, SIAM J. Comput. **20**, 865 (1991).

[37] M. Vyalyi, **QMA**=**PP** implies that **PP** contains **PH**, Electronic Colloquium on Computational Complexity, Report TR03-021 (2003).

[38] R. Beigel, Perceptrons, PP, and the polynomial hierarchy, computational complexity **4**, 339 (1994).

[39] T. Morimae and H. Nishimura, Merlinization of complexity classes above BQP, Quantum Inf. Comput. **17**, 959 (2017).

[40] N. Usher, M. J. Hoban, and D. E. Browne, Nonunitary quantum computation in the ground space of local Hamiltonians, Phys. Rev. A **96**, 032321 (2017).

[41] B. Fefferman and C. Y.-Y. Lin, A Complete Characterization of Unitary Quantum Space, in *Proc. of the 9th Innovations in Theoretical Computer Science Conference* (ITCS, Cambridge, 2018), p. 4:1.

[42] Y. Takeuchi, Y. Takahashi, and S. Tani, Hardness of efficiently generating ground states in postselected quantum computation, Phys. Rev. Research **3**, 013213 (2021).

[43] S. Aaronson, Quantum computing, post-selection and probabilistic polynomial-time, Proc. R. Soc. A **461**, 3473 (2005).

[44] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2010).

[45] C. Marriott and J. Watrous, Quantum Arthur-Merlin Games, Computational Complexity **14**, 122 (2005).