

Impossibility of Classically Simulating One-Clean-Qubit Model with Multiplicative Error

Keisuke Fujii,^{1,2,3,*} Hirotada Kobayashi,^{4,†} Tomoyuki Morimae,^{5,3,6,‡} Harumichi Nishimura,^{7,§}
Shuheï Tamate,^{8,||} and Seiichiro Tani^{9,¶}

¹*Department of Physics, Graduate School of Science, Kyoto University, Kyoto 606-8502, Japan*

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

³*JST, PRESTO, Kawaguchi 332-0012, Japan*

⁴*Principles of Informatics Research Division, National Institute of Informatics, Tokyo 101-8430, Japan*

⁵*Department of Computer Science, Gunma University, Kiryu 376-8515, Japan*

⁶*Yukawa Institute for Theoretical Physics, Kyoto University, Kyoto 606-8502, Japan*

⁷*Graduate School of Informatics, Nagoya University, Nagoya 464-8601, Japan*

⁸*Research Center for Advanced Scientific and Technology (RCAST), The University of Tokyo, Tokyo 153-8904, Japan*

⁹*NTT Communication Science Laboratories, NTT Corporation, Atsugi 243-0198, Japan*



(Received 25 September 2017; revised manuscript received 22 November 2017; published 17 May 2018)

The one-clean-qubit model (or the deterministic quantum computation with one quantum bit model) is a restricted model of quantum computing where all but a single input qubits are maximally mixed. It is known that the probability distribution of measurement results on three output qubits of the one-clean-qubit model cannot be classically efficiently sampled within a constant multiplicative error unless the polynomial-time hierarchy collapses to the third level [T. Morimae, K. Fujii, and J. F. Fitzsimons, *Phys. Rev. Lett.* **112**, 130502 (2014)]. It was open whether we can keep the no-go result while reducing the number of output qubits from three to one. Here, we solve the open problem affirmatively. We also show that the third-level collapse of the polynomial-time hierarchy can be strengthened to the second-level one. The strengthening of the collapse level from the third to the second also holds for other subuniversal models such as the instantaneous quantum polynomial model [M. Bremner, R. Jozsa, and D. J. Shepherd, *Proc. R. Soc. A* **467**, 459 (2011)] and the boson sampling model [S. Aaronson and A. Arkhipov, *STOC 2011*, p. 333]. We additionally study the classical simulatability of the one-clean-qubit model with further restrictions on the circuit depth or the gate types.

DOI: [10.1103/PhysRevLett.120.200502](https://doi.org/10.1103/PhysRevLett.120.200502)

What makes a quantum computing model stronger than classical computing? It is one of the most important questions in physics and computer science. Quantum advantages have been shown for several cases, such as the communication complexity [1,2] and the query complexity [3,4]. However, the ultimate question “is $BPP \neq BQP$?” remains open [5], while there are several witnesses, such as Shor’s algorithm [6], that suggest the gap.

Some restricted quantum computing models are known to be as weak as classical computing. For example, quantum computing that uses only certain types of gates, such as Clifford gates [7] or matchgates [8–12], can be classically efficiently simulated. On the other hand, quantum computational supremacy of several subuniversal quantum computing models have been demonstrated recently [13–19]. Importantly, the hardness proofs of classical simulations of these models are based on the strong belief in computer science that the polynomial-time hierarchy would not collapse [20].

Terhal and DiVincenzo [13] showed that the output probability distributions of depth-four quantum circuits cannot be classically efficiently sampled within a constant multiplicative error unless BQP is contained in AM, which

is unlikely [23]. Here, we say that a probability distribution $\{p_z\}_z$ is classically efficiently sampled within a multiplicative error ϵ if there is a classical polynomial-time algorithm that outputs z with probability q_z such that $|p_z - q_z| \leq \epsilon p_z$ for all z . The consequence, $BQP \subseteq AM$, of their result can be strengthened to the collapse of the polynomial-time hierarchy to the third level by noticing the fact that nonadaptive measurement-based quantum computing is depth four.

Bremner, Jozsa, and Shepherd [14] showed that the output probability distributions of instantaneous quantum polynomial (IQP) circuits cannot be classically efficiently sampled within a constant multiplicative error unless the polynomial-time hierarchy collapses to the third level. Here, an IQP circuit is a restricted quantum circuit where only X -diagonal gates are applied (or, equivalently, a Z -diagonal circuit is sandwiched between the global Hadamards). The essential for their proof is the complexity class, postBQP , which is the class of problems that can be solved with a polynomial-time quantum computer with postselection [24]. Here, postselection is a fictitious ability that a certain measurement result is given with probability one. Bremner, Jozsa, and Shepherd [14] introduced the

so-called the Hadamard gadget, which is a subquantum circuit that enables a Hadamard gate at any place with a postselection. By using the gadget, they showed that any quantum circuit that uses H , CZ , and $e^{iZ\theta}$, which are universal, can be written as an IQP circuit with postselections. It means that postIQP, which is the IQP version of postBQP, is equal to postBQP. Therefore, the classical efficient sampling of IQP circuits, which implies $\text{postIQP} \subseteq \text{postBPP}$, causes the collapse of the polynomial-time hierarchy to the third level:

$$\text{PH} \subseteq \text{P}^{\text{PP}} = \text{P}^{\text{postBQP}} = \text{P}^{\text{postIQP}} \subseteq \text{P}^{\text{postBPP}} \subseteq \Delta_3.$$

Here PH is the polynomial-time hierarchy, Δ_3 is in the third level of the polynomial-time hierarchy, postBPP is the BPP version of postBQP, which is actually equal to $\text{BPP}_{\text{path}} \subseteq \Delta_3$ [25], and it is known that postBQP is equal to PP [24,26].

Aaronson and Arkhipov [17] showed that the output probability distributions of the boson sampling model, which is a quantum computer that uses noninteracting bosons, cannot be classically efficiently sampled within a constant multiplicative error unless the polynomial-time hierarchy collapses to the third level. Their proof is similar to that for the IQP model [14]: noninteracting bosons with postselections can simulate the Knill-Laflamme-Milburn (KLM) scheme [27], which is universal, and therefore $\text{postBosonSampling} = \text{postBQP}$.

The multiplicative error approximation is, however, somehow a strict requirement. In fact, assuming some unproven mathematical conjectures that are different from the infiniteness of the polynomial-time hierarchy, the output probability distributions of the IQP model and the boson sampling model were shown to be hard to classically efficiently sample within a constant additive error. Here, we say that a probability distribution $\{p_z\}_z$ is classically efficiently sampled within an additive error ϵ if there is a classical polynomial-time algorithm that outputs z with probability q_z such that $\sum_z |p_z - q_z| \leq \epsilon$. The additive error approximation is a more relaxed notion of approximation, and it is also called the L1-norm error approximation or the total-variation-distance error approximation.

For the IQP model, the no-go result with the additive error approximation was proved by Bremner, Montanaro, and Shepherd [15,16]. The no-go result for the boson sampling case was given by Aaronson and Arkhipov [17]. As mentioned before, these no-go results need some unproven mathematical conjectures different from the infiniteness of the polynomial-time hierarchy. The result for the boson sampling model [17] needs two conjectures, the ‘‘average case vs worst case conjecture’’ and the ‘‘anti-concentration conjecture.’’ The result for the IQP model [15] assumes a similar average case vs worst case conjecture, but the anti-concentration one is no longer a conjecture but a mathematically proved lemma. (Recently, it was shown that two-design systems also satisfy the anticoncentration lemma [28].)

The one-clean qubit model [or the deterministic quantum computation with one quantum bit (DQC1) model] is another important example of the subuniversal quantum computing models. It was originally introduced by Knill and Laflamme [29] in 1998 to model the NMR quantum computing. The one-clean qubit model starts with the highly mixed initial state $|0\rangle\langle 0| \otimes (I^{\otimes n}/2^n)$, where $I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator. Any unitary operator U is applied on it to generate

$$U \left(|0\rangle\langle 0| \otimes \frac{I^{\otimes n}}{2^n} \right) U^\dagger, \quad (1)$$

and finally some qubits are measured in the computational basis [30]. When k output qubits are measured, the probability p_z of obtaining $z \in \{0, 1\}^k$ is

$$p_z \equiv \text{Tr} \left((|z\rangle\langle z| \otimes I^{\otimes(n+1-k)}) U \left(|0\rangle\langle 0| \otimes \frac{I^{\otimes n}}{2^n} \right) U^\dagger \right).$$

We call such a model the DQC1_k model.

The one-clean qubit model seems to be classically efficiently simulatable. In fact, if the pure state $|0\rangle$ of the initial state is replaced with the maximally mixed state $I/2$, the quantum computing is trivially simulatable with a polynomial-time classical computer, since $U(I^{\otimes(n+1)}/2^{n+1})U^\dagger = [I^{\otimes(n+1)}/2^{n+1}]$ for any unitary operator U . However, surprisingly, the one-clean qubit model can efficiently solve several problems whose classical efficient solutions are not known, such as the spectral density estimation [29], testing integrability [31], calculations of the fidelity decay [32], and approximations of the Jones polynomial, HOMFLY polynomial, and Turaev-Viro invariant [33–36].

Furthermore, it was shown that if the output probability distribution of the DQC1_3 model is classically efficiently sampled within a multiplicative error $\epsilon < 1$, then the polynomial-time hierarchy collapses to the third level [18]. The proof uses the similar idea as those for the IQP model [14] and the boson sampling model [17]: Ref. [18] showed $\text{postDQC1}_3 = \text{postBQP}$, where postDQC1_3 is the DQC1_3 version of postBQP. (The proof idea is as follows. For a given postBQP circuit V , we construct the DQC1_3 circuit in Fig. 1. The postselection on the qubit p_1 prepares the pure initial state $|0^n\rangle$, where n is the width of V . The postselection on the

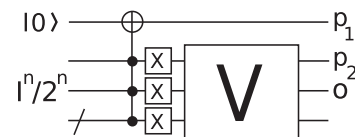


FIG. 1. The DQC1_3 circuit used to show $\text{postBQP} \subseteq \text{postDQC1}_3$ in Ref. [18]. The slash (/) means multiple qubits (in this case, $n - 2$ qubits), and X is applied on each qubit.

qubit p_2 simulates the postselection of the original postBQP circuit V . The qubit o simulates the decision qubit of V .)

The no-go result with the additive error approximation has been recently obtained for the DQC1 model in Ref. [19]. Like the results of the IQP model [15] and the boson sampling model [17], the result of Ref. [19] assumes a certain unproven mathematical conjecture, which is a slightly different form of the average case vs worst case conjecture. Interestingly, by using a special property of the DQC1 model, the anticoncentration lemma is easily shown.

One disadvantage of these results is, however, that at least three qubits must be measured: the result of Ref. [18] is the hardness result for DQC1₃, and the result of Ref. [19] is that for DQC1 _{$n+1$} . Is it possible to show any hardness result for DQC1₁?

The other open problem that these previous results leave is whether we can strengthen the third-level collapse of the polynomial-time hierarchy to a more unlikely consequence. The third-level collapse is not believed to happen in computer science, but it would be better if we could show a no-go result based on a more stable belief.

In this Letter, we solve these two open problems [37]. Our main result is the following theorem:

Theorem 1: If the output probability distribution of the DQC1₁ model is classically efficiently sampled within a multiplicative error $\epsilon < 1$, then the polynomial-time hierarchy collapses to the second level.

Remember that the classical efficient sampling of $\{p_z\}_z$ within a multiplicative error ϵ means the existence of a classically efficiently samplable distribution $\{q_z\}_z$ such that $|p_z - q_z| \leq \epsilon p_z$. The intuition behind this theorem is as follows. We construct the DQC1₁ circuit of Fig. 2 from a quantum circuit V_w related to a certain quantum complexity class. If the output probability distribution of the DQC1₁ circuit is classically efficiently sampled within a multiplicative error $\epsilon < 1$, it means that the quantum complexity class is contained in another classical complexity class. Such a containment leads to the unlikely consequence, namely, the collapse of the polynomial-time hierarchy, in computer science. For details, see the proof given below.

In this theorem, the number of the measured qubit is reduced to one from three. Furthermore, the collapse of the polynomial-time hierarchy is now to the second level rather than the third level, which is more unlikely. It is interesting to note that in the boson sampling and IQP cases, a polynomial number of qubits are measured, and therefore the sample space is exponentially large, while in the

DQC1₁ case Theorem 1 suggests that the hardness statement for the small sample space is possible.

Proof of Theorem 1.—Using the postselection technique would not work to show the theorem because of the following two reasons: First, postDQC1₁ is not well defined since DQC1₁ circuit has only a single output qubit. Second, showing postBQP = postBPP is not enough to show the collapse of the polynomial-time hierarchy to the second level. Our new idea is to use another class, NQP [39], which is one possible quantum analogue of NP. NQP is defined as follows: a language L is in NQP if and only if there exists a polynomial-time uniformly generated family of quantum circuits $\{V_w\}_w$ such that if $w \in L$ then $p_{\text{acc}} > 0$, and if $w \notin L$ then $p_{\text{acc}} = 0$, where p_{acc} is the acceptance probability [40]. We show that if the output probability distribution of the DQC1₁ model is classically efficiently sampled within a multiplicative error $\epsilon < 1$, then $\text{NQP} \subseteq \text{NP}$. If such a containment occurs, the polynomial-time hierarchy collapses to the second level, since

$$\text{PH} \subseteq \text{BP} \cdot \text{co-C=P} = \text{BP} \cdot \text{NQP} = \text{BP} \cdot \text{NP} = \text{AM},$$

where the first containment is from Refs. [41,42] and the second equality is from Ref. [43]. The class C=P is defined in Ref. [44], and the BP operator is defined in Ref. [45]. To derive $\text{NQP} \subseteq \text{NP}$, we consider the DQC1₁ circuit of Fig. 2. It is easy to verify that the probability \tilde{p} of obtaining 1 when the qubit o is measured is $\tilde{p} = [4p(1-p)/2^n]$, where $p \equiv \langle 0^n | V_w^\dagger (|1\rangle\langle 1| \otimes I^{\otimes(n-1)}) V_w | 0^n \rangle$. Therefore, if $0 < p < 1$ then $\tilde{p} > 0$, and if $p = 0$ then $\tilde{p} = 0$. (Without loss of generality, we can assume that $0 \leq p < 1$, since we can intentionally reduce the output probability by multiplying the output probability of V_w by a constant.) If \tilde{p} is classically efficiently sampled within a multiplicative error $\epsilon < 1$, it implies $\text{NQP} \subseteq \text{NP}$.

The new idea of using NQP can be applied to other subuniversal models such as the IQP model [14] and the boson sampling model [17]:

Theorem 2: If the output probability distribution of the IQP model or the boson sampling model is classically efficiently sampled within a multiplicative error $\epsilon < 1$, then the polynomial-time hierarchy collapses to the second level.

Note that the required approximation error, $\epsilon < 1$, is the same as that of the previous results [14,17] that use the postBQP technique.

Proof of Theorem 2.—We consider the boson sampling model, but it is exactly the same for the IQP model. It is known that the boson sampling model is universal under a postselection. It means that for any universal quantum circuit U , there exists a boson sampling circuit V such that $\text{Pr}_U(\text{accept}) = \text{Pr}_V(\text{accept}|\text{postselect})$. Let us consider the following quantum computing: (1) Run V . (2) Accept if the postselection is successful and V accepts. The acceptance probability of this quantum computing is



FIG. 2. The DQC1₁ circuit used to show $\text{NQP} \subseteq \text{NP}$.

$$\begin{aligned} & \Pr_V(\text{accept, postselect}) \\ &= \Pr_V(\text{accept}|\text{postselect})\Pr_V(\text{postselect}) \\ &= \Pr_U(\text{accept})\Pr_V(\text{postselect}). \end{aligned}$$

If the classical efficient sampling of $\Pr_V(\text{accept, postselect})$ is possible, then we have $\text{NQP} \subseteq \text{NP}$.

Although postDQC1_1 is not well defined, we can still show that the classical efficient simulation of the DQC1_1 model leads to $\text{postBQP} = \text{postBPP}$:

Theorem 3: If the output probability distribution of the DQC1_1 model is classically efficiently sampled within a multiplicative error $\epsilon < 1$, then $\text{postBQP} = \text{postBPP}$.

Its proof is given in the Supplemental Material [46]. Note that a similar proof also gives the result that calculating the output probability distribution of the DQC1_1 model within a multiplicative error $\epsilon < 1$ is $\#P$ -hard. (For a proof, see the Supplemental Material) [46,51,52].

The final contribution of our Letter is studying classical simulatability of the DQC1 model with additional restrictions. We first consider the logarithmic-depth DQC1_m model with polynomially large m . We show that such a model would not be classically efficiently simulatable:

Theorem 4: If the output probability distribution of the logarithmic-depth DQC1_m model with polynomially large m is classically efficiently sampled within a multiplicative error $\epsilon < 1$, then the polynomial-time hierarchy collapses to the second level.

We next consider the DQC1_m model with constant (or doubly logarithmic) depth, and show that such a model is classically simulatable:

Theorem 5: Any marginal distribution of the output probability distribution of the constant (or doubly logarithmic) depth DQC1_m model for any m can be exactly calculated in classical polynomial time.

Finally, we study the DQC1_m model whose circuit is restricted to the IQP type. In other words, we consider the following DQC1_m model, which we call the IQP- DQC1_m model: (1) The input state is $|0\rangle\langle 0| \otimes (I^{\otimes n}/2^n)$. (2) Apply $H^{\otimes(n+1)}$. Apply a polynomially many CZ gates and $e^{i\theta Z}$ gates. Apply $H^{\otimes(n+1)}$. (3) Measure m output qubits in the computational basis. We show that such a model is also classically efficiently simulatable:

Theorem 6: Any marginal distribution of the output probability distribution of the IQP- DQC1_m model for any m can be exactly calculated in classical polynomial time.

Proofs for these theorems are given in the Supplemental Material [46].

Discussion.—In this Letter, we have shown the hardness of classically simulating the DQC1_1 model. It would be important to consider an experimental implementation of our results. Although multiplicative-error sampling is difficult to realize, it might be still possible to do some proof-of-principle demonstrations with few qubits. Finally, let us conclude this Letter by pointing out that our result

reveals a nontrivial relation between the matchgate model [8–12] and the DQC1_1 model: the computational power of the log-space DQC1_1 model and that of the matchgate model are equivalent. (Here, the log-space DQC1_1 model is the DQC1_1 model with a log width; i.e., n of Eq. (1) is logarithmic with respect to the input size.) This is because, by using Fig. 2, we can show that the log-space DQC1_1 model can simulate the log-space (pure) quantum circuits, which are known to be equivalent to the matchgate model [12]. (Details are given in the Supplemental Material [46].) Simulating Ising models with log-qubit quantum computing, which is an example of so called the “compressed quantum simulation,” has recently been studied theoretically [53] and experimentally [54]. The relation between the matchgate model and the log-space DQC1_1 model therefore suggests another example of the compressed quantum simulation: fermionic systems and spin systems can be simulated with log-qubit NMR quantum computing.

K. F. is supported by the JSPS Grant-in-Aid for Scientific Research (A) No. 16H02211, JST PRESTO No. JPMJPR1668, JST CREST No. JPMJCR1673, and JST ERATO No. JPMJER1601. H. K. is supported by the JSPS Grant-in-Aid for Scientific Research (A) No. 24240001 and No. 16H01705. T. M. is supported by JST ACT-I No. JPMJPR16UP, JST PRESTO No. JPMJPR176A, the MEXT Grant-in-Aid for Scientific Research on Innovative Areas No. 15H00850, and the JSPS Grant-in-Aid for Young Scientists (B) No. 26730003 and No. 17K12637. H. N. is supported by the JSPS Grant-in-Aid for Scientific Research (A) No. 26247016, No. 24240001, and No. 16H01705, the MEXT Grant-in-Aid for Scientific Research on Innovative Areas No. 24106009, and the JSPS Grant-in-Aid for Scientific Research (C) No. 16K00015. S. Tamate is supported by JST ERATO No. JPMJER1601.

*fujii.keisuke.2s@kyoto-u.ac.jp

†hirotada@nii.ac.jp

‡tomoyuki.morimae@yukawa.kyoto-u.ac.jp

§hnishimura@is.nagoya-u.ac.jp

||tamate@qc.rcast.u-tokyo.ac.jp

¶tani.seiichiro@lab.ntt.co.jp

- [1] H. Buhrman, R. Cleve, and A. Wigderson, Quantum vs. classical communication and computation, *Proceedings of the 30th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1998), p. 63, DOI: 10.1145/276698.276713.
- [2] R. Raz, Exponential separation of quantum and classical communication complexity, *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* (ACM, New York, 1999), p. 358, DOI: 10.1145/301250.301343.
- [3] L. K. Grover, Quantum Mechanics Helps in Searching for a Needle in Haystack, *Phys. Rev. Lett.* **79**, 325 (1997).
- [4] D. R. Simon, On the power of quantum computation, *Proceedings of the 35th Annual Symposium on Foundations*

- of Computer Science* (IEEE Press, Los Alamitos, 1994), p. 116, DOI: [10.1109/SFCS.1994.365701](https://doi.org/10.1109/SFCS.1994.365701).
- [5] BPP is the class of decision problems that can be solved with classical polynomial-time randomized computing. Here, a decision problem is a problem that can be solved by answering yes or no. BQP is the class of decision problems that can be solved with polynomial-time quantum computing.
- [6] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Press, Los Alamitos, 1994), p. 124, DOI: [10.1109/SFCS.1994.365700](https://doi.org/10.1109/SFCS.1994.365700).
- [7] D. Gottesman, The Heisenberg representation of quantum computers, [arXiv:quant-ph/9807006](https://arxiv.org/abs/quant-ph/9807006).
- [8] L. G. Valiant, Quantum circuits that can be simulated classically in polynomial time, *SIAM J. Comput.* **31**, 1229 (2002).
- [9] B. M. Terhal and D. P. DiVincenzo, Classical simulation of noninteracting-fermion quantum circuits, *Phys. Rev. A* **65**, 032325 (2002).
- [10] E. Knill, Fermionic linear optics and matchgates, [arXiv:quant-ph/0108033](https://arxiv.org/abs/quant-ph/0108033).
- [11] R. Jozsa and A. Miyake, Matchgates and classical simulation of quantum circuits, *Proc. R. Soc. A* **464**, 3089 (2008).
- [12] R. Jozsa, B. Kraus, A. Miyake, and J. Watrous, Matchgate and space-bounded quantum computations are equivalent, *Proc. R. Soc. A* **466**, 809 (2010).
- [13] B. Terhal and D. P. DiVincenzo, Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games, *Quantum Inf. Comput.* **4**, 134 (2004).
- [14] 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).
- [15] 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).
- [16] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Achieving quantum supremacy with sparse and noisy commuting quantum computations, *Quantum* **1**, 8 (2017).
- [17] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, *Theory Comput.* **9**, 143 (2013).
- [18] T. Morimae, K. Fujii, and J. F. Fitzsimons, Hardness of Classically Simulating the One Clean Qubit Model, *Phys. Rev. Lett.* **112**, 130502 (2014).
- [19] T. Morimae, Hardness of classically sampling one clean qubit model with constant total variation distance error, *Phys. Rev. A* **96**, 040302(R) (2017).
- [20] For the details of the polynomial-time hierarchy, see Chapter 5 of Ref. [21] or the Supplemental Material of Ref. [22], for example.
- [21] S. Arora and B. Barak, *Computational Complexity: A Modern Approach* (Cambridge University Press, New York, USA, 2009).
- [22] 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).
- [23] AM is the class of decision problems that can be verified by an interaction between a prover and a verifier. The prover can solve any problem, while the verifier can do only polynomial-time classical randomized computing. In AM, the verifier sends a random string to the prover, and the prover replies with a polynomial-length bit string.
- [24] S. Aaronson, Quantum computing, postselection, and probabilistic polynomial-time, *Proc. R. Soc. A* **461**, 3473 (2005).
- [25] Y. Han, L. Hemaspaandra, and T. Thierauf, Threshold computation and cryptographic security, *SIAM J. Comput.* **26**, 59 (1997).
- [26] PP is the class of decision problems that can be solved with classical polynomial-time randomized computing with unbounded error.
- [27] E. Knill, R. Laflamme, and G. J. Milburn, A scheme for efficient quantum computation with linear optics, *Nature (London)* **409**, 46 (2001).
- [28] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, Anti-concentration theorems for schemes showing a quantum computational supremacy, [arXiv:1706.03786](https://arxiv.org/abs/1706.03786).
- [29] E. Knill and R. Laflamme, Power of One Bit of Quantum Information, *Phys. Rev. Lett.* **81**, 5672 (1998).
- [30] As in the definition of BQP, we here consider the usual polynomial-time uniformity for the DQC1 model.
- [31] D. Poulin, R. Laflamme, G. J. Milburn, and J. P. Paz, Testing integrability with a single bit of quantum information, *Phys. Rev. A* **68**, 022302 (2003).
- [32] D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Ollivier, Exponential Speedup with a Single Bit of Quantum Information: Measuring the Average Fidelity Decay, *Phys. Rev. Lett.* **92**, 177906 (2004).
- [33] P. W. Shor and S. P. Jordan, Estimating Jones polynomials is a complete problem for one clean qubit, *Quantum Inf. Comput.* **8**, 681 (2008).
- [34] G. Passante, O. Moussa, C. A. Ryan, and R. Laflamme, Experimental Approximation of the Jones Polynomial with One Quantum Bit, *Phys. Rev. Lett.* **103**, 250501 (2009).
- [35] S. P. Jordan and P. Wocjan, Estimating Jones and HOMFLY polynomials with one clean qubit, *Quantum Inf. Comput.* **9**, 264 (2009).
- [36] S. P. Jordan and G. Alagic, Approximating the Turaev-Viro invariant of mapping tori is complete for one clean qubit, in *Theory of Quantum Computation, Communication, and Cryptography, 6th Conference, TQC 2011*, Lect. Notes Comput. Sci. Vol. 6745 (Springer, Berlin, Heidelberg, 2014), p. 53, DOI: [10.1007/978-3-642-54429-3_5](https://doi.org/10.1007/978-3-642-54429-3_5).
- [37] A related paper, Ref. [38], includes the statement of Theorem 1 with no proof, while it mainly studies the error reduction of the DQC1 model.
- [38] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Power of quantum computation with few clean qubits, *Proceedings of 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, Leibniz International Proceedings in Informatics Vol. 55 (2016), p. 13, DOI: [10.4230/LIPIcs.ICALP.2016.13](https://doi.org/10.4230/LIPIcs.ICALP.2016.13).
- [39] L. M. Adleman, J. DeMarrais, and M. A. Huang, Quantum computability, *SIAM J. Comput.* **26**, 1524 (1997).
- [40] When $p_{\text{acc}} > 0$, it is lower-bounded by $1/2^{\text{poly}}$ for natural universal gate sets.

- [41] J. Tarui, Probabilistic polynomials, AC^0 functions and the polynomial-time hierarchy, *Theor. Comput. Sci.* **113**, 167 (1993).
- [42] S. Toda and M. Ogiwara, Counting classes are at least as hard as the polynomial-time hierarchy, *SIAM J. Comput.* **21**, 316 (1992).
- [43] S. Fenner, F. Green, S. Homer, and R. Pruim, Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy, *Proc. R. Soc. A* **455**, 3953 (1999).
- [44] K. W. Wagner, The complexity of combinatorial problems with succinct input representation, *Acta informatica* **23**, 325 (1986).
- [45] U. Schöning, Probabilistic complexity classes and lowness, *J. Comput. Syst. Sci.* **39**, 84 (1989).
- [46] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.120.200502> for the contents that cannot be included in the Letter such as the proofs of Theorems 3, 4, 5 and 6, which includes Refs. [12,47–50].
- [47] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Elementary gates for quantum computation, *Phys. Rev. A* **52**, 3457 (1995).
- [48] G. Kuperberg, How hard is it to approximate the Jones polynomial?, *Theory Comput.* **11**, 183 (2015).
- [49] S. Fenner, F. Green, S. Homer, and Y. Zhang, Bounds on the power of constant-depth quantum circuits, 15th International Symposium on Fundamentals of Computation Theory, *Lect. Notes Comput. Sci.* **3623**, 44 (2005).
- [50] B. Fefferman, H. Kobayashi, C. Y. Lin, T. Morimae, and H. Nishimura, Space-efficient error reduction for unitary quantum computations, *Proceedings of 43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, Leibniz International Proceedings in Informatics Vol. 55 (2016), p. 14, DOI: 10.4230/LIPIcs.ICALP.2016.14.
- [51] Note that approximating \tilde{p} and efficiently sampling it are different. If we can approximate \tilde{p} , we can sample it, because it is a Bernoulli distribution. (If the sample space is exponentially large, the statement is not true.) On the other hand, even if we can efficiently sample \tilde{p} , we cannot approximate it with an exponential precision.
- [52] Calculating a function is called #P-hard if the calculation can be reduced to the calculation of the number of accepting paths for a nondeterministic Turing machine.
- [53] B. Kraus, Compressed Quantum Simulation of the Ising Model, *Phys. Rev. Lett.* **107**, 250503 (2011).
- [54] Z. Li, H. Zhou, C. Ju, H. Chen, W. Zheng, D. Lu, X. Rong, C. Duan, X. Peng, and J. Du, Experimental Realization of a Compressed Quantum Simulation of a 32-Spin Ising Chain, *Phys. Rev. Lett.* **112**, 220501 (2014).