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

Keisuke Fujii, Hirotada Kobayashi, Tomoyuki Morimae, Harumichi Nishimura, Shuhei Tamate, and Seiichiro Tani

Phys. Rev. Lett. **120**, 200502 — Published 17 May 2018

DOI: 10.1103/PhysRevLett.120.200502

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, §] Shuhei Tamate,[8, ¶] and Seiichiro Tani[9, **]

[1]*Department of Physics, Graduate School of Science, Kyoto University, Japan*
[2]*Photon Science Center, Graduate School of Engineering, The University of Tokyo, Japan*
[3]*JST, PRESTO, Japan*
[4]*Principles of Informatics Research Division, National Institute of Informatics, Japan*
[5]*Department of Computer Science, Gunma University, Japan*
[6]*Yukawa Institute for Theoretical Physics, Kyoto University, Japan*
[7]*Graduate School of Information Science, Nagoya University, Japan*
[8]*Research Center for Advanced Scientific and Technology (RCAST), The University of Tokyo, Japan*
[9]*NTT Communication Science Laboratories, NTT Corporation, Japan*

(Dated: April 2, 2018)

The one-clean-qubit model (or the DQC1 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 sub-universal models such as the IQP 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.

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 sub-universal quantum computing models have been demonstrated recently [13, 15–20]. 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 [21].

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 [14]. 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 non-adaptive measurement-based quantum computing is depth four.

Bremner, Jozsa, and Shepherd [15] showed that the output probability distributions of 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 fictious ability that a certain measurement result is given with probability one. Bremner, Jozsa, and Shepherd [15] introduced so-called the Hadamard gadget, which is a sub quantum circuit that enables an 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 postIQP $\subseteq$ postBPP, causes the collapse of the polynomial-time hierarchy to the third level:

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

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

Aaronson and Arkhipov [18] showed that the output probability distributions of the Boson Sampling model, which is a quantum computer that uses non-interacting 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 [15]: non-interacting bosons with postselections can simulate the Knill-Laflamme-Milburn (KLM) scheme [27], which is universal, and therefore postBosonSampling = 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 [16, 17]. The no-go result for the Boson Sampling case was given by Aaronson and Arkhipov [18]. 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 [18] needs two conjectures, the "average case vs worst case conjecture" and the "anti-concentration conjecture". The result for the IQP model [16] 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 anti-concentration lemma [28].)

The one-clean qubit model (or the DQC1 model) is another important example of the sub-universal 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 $|0\rangle\langle 0| \otimes \frac{I^{\otimes n}}{2^n}$, 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

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

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

$$p_z \equiv \mathrm{Tr}\Big[(|z\rangle\langle z| \otimes I^{\otimes(n+1-k)})U\Big(|0\rangle\langle 0| \otimes \frac{I^{\otimes n}}{2^n}\Big)U^\dagger\Big].$$

We call such a model the $\mathrm{DQC1}_k$ 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 $\frac{I}{2}$, the quantum computing is trivially simulatable with a polynomial-time classical computer, since $U\frac{I^{\otimes(n+1)}}{2^{n+1}}U^\dagger = \frac{I^{\otimes(n+1)}}{2^{n+1}}$ 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 $\mathrm{DQC1}_3$ model is classically efficiently sampled within a multiplicative error $\epsilon < 1$, then the polynomial-time hierarchy collapses to the third level [19]. The proof uses the similar idea as those for the IQP model [15] and the Boson Sampling model [18]: Ref. [19] showed $\mathrm{postDQC1}_3$ = postBQP, where $\mathrm{postDQC1}_3$ is the $\mathrm{DQC1}_3$ version of postBQP. (The proof idea is as follows. For a given postBQP circuit V, we construct the $\mathrm{DQC1}_3$ 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 qubit p_2 simulates the postselection of the original postBQP circuit V. The qubit o simulates the decision qubit of V.)

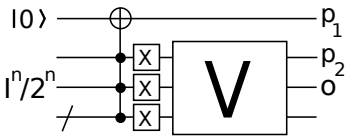

FIG. 1: The $\mathrm{DQC1}_3$ circuit used to show postBQP $\subseteq$ $\mathrm{postDQC1}_3$ in Ref. [19]. The slash "/" means multiple qubits (in this case, $n-2$ qubits), and X is applied on each qubit.

The no-go result with the additive error approximation has been recently obtained for the DQC1 model in Ref. [20]. Like the results of the IQP model [16] and the Boson Sampling model [18], the result of Ref. [20] 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 anti-concentration lemma is easily shown.

One disadvantage of these results is, however, that at least three qubits must be measured: the result of

Ref. [19] is the hardness result for $\mathrm{DQC1}_3$, and the result of Ref. [20] is that for $\mathrm{DQC1}_{n+1}$. Is it possible to show any hardness result for $\mathrm{DQC1}_1$?

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 [44]. Our main result is the following theorem:

Theorem 1. *If the output probability distribution of the DQC1$_1$ 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 $\mathrm{DQC1}_1$ circuit of Fig. 2 from a quantum circuit V_w related to a certain quantum complexity class. If the output probability distribution of the $\mathrm{DQC1}_1$ 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 hierarchy, in computer science. For details, see the proof given below.

In this theorem, the number of 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, polynomial number of qubits are measured, and therefore the sample space is exponentially large, while in the $\mathrm{DQC1}_1$ 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, $\mathrm{postDQC1}_1$ is not well defined since $\mathrm{DQC1}_1$ 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 [37], 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 $p_{acc} > 0$, and if $w \notin L$ then $p_{acc} = 0$, where p_{acc} is the acceptance probability [38]. We show that if the output probability distribution of the $\mathrm{DQC1}_1$ model is classically efficiently sampled within a multiplicative error $\epsilon < 1$, then NQP $\subseteq$ NP. If such a containment occurs, the polynomial-time hierarchy collapses to the second level, since

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

where the first containment is from Refs. [39, 40] and the second equality is from Ref. [41]. The class $\mathrm{C}_{=}\mathrm{P}$ is defined in Ref. [42], and the BP operator is defined in Ref. [43]. To derive NQP $\subseteq$ NP, we consider the $\mathrm{DQC1}_1$ circuit of Fig. 2. It is easy to verify that the probability $\tilde{p}$ of obtaining 1 when the qubit o is measured is $\tilde{p} = \frac{4p(1-p)}{2^n}$, 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 NQP $\subseteq$ NP.

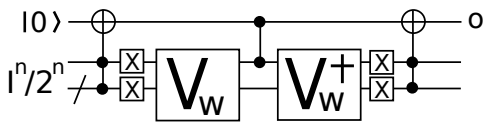

FIG. 2: The $\mathrm{DQC1}_1$ circuit used to show NQP $\subseteq$ NP.

The new idea of using NQP can be applied to other sub-universal models such as the IQP model [15] and the Boson Sampling model [18]:

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 [15, 18] 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 $\Pr_U(\text{accept}) = \Pr_V(\text{accept}|\text{postselect})$. 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

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

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

Although postDQC1$_1$ is not well defined, we can still show that the classical efficient simulation of the DQC1$_1$ model leads to postBQP = postBPP:

Theorem 3. *If the output probability distribution of the DQC1$_1$ model is classically efficiently sampled within a multiplicative error $\epsilon < 1$, then* postBQP = postBPP.

Its proof is given in the supplementary material [50]. Note that a similar proof also gives the result that calculating the output probability distribution of the DQC$_1$ model within a multiplicative error $\epsilon < 1$ is #P-hard. (For a proof, see the supplementary material) [48–50].

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 $|0\rangle\langle 0| \otimes (\frac{I^{\otimes n}}{2^n})$.
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 supplementary material [50].

Discussion.— In this paper, 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 paper by pointing out that our result reveals a non-trivial 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 log of 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 supplementary material [50].) Simulating Ising models with log-qubit quantum computing, which is an example of so called the "compressed quantum simulation", has recently been studied theoretically [46] and experimentally [47]. 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.

Keisuke Fujii is supported by KAKENHI No.16H02211, PRESTO, JST, CREST, JST, and ERATO, JST. Hirotada Kobayashi is supported by the Grant-in-Aid for Scientific Research (A) No.24240001 of the Japan Society for the Promotion of Science. Tomoyuki Morimae is supported by JST ACT-I No.JPMJPR16UP, JST PRESTO, Grant-in-Aid for Scientific Research on Innovative Areas No.15H00850 of MEXT Japan, and the Grant-in-Aid for Young Scientists (B) No.26730003 and No.17K12637 of JSPS. Harumichi Nishimura is supported by the Grant-in-Aid for Scientific Research (A) Nos.26247016 and 16H01705 of JSPS, the Grant-in-Aid for Scientific Research on Innovative Areas No.24106009 of MEXT, and the Grant-in-Aid for Scientific Research (C) No.16K00015 of JSPS. Shuhei Tamate is supported by ERATO, JST.

* Electronic address: fujii.keisuke.2s@kyoto-u.ac.jp
† Electronic address: hirotada@nii.ac.jp
‡ Electronic address: tomoyuki.morimae@yukawa.kyoto-u.ac.jp
§ Electronic address: hnishimura@is.nagoya-u.ac.jp
¶ Electronic address: tamate@qc.rcast.u-tokyo.ac.jp
** Electronic address: 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, p. 63 (1998).
[2] R. Raz, Exponential separation of quantum and classical communication complexity. Proceedings of the 31st Annual ACM Symposium on Theory of Computing, p.358 (1999).
[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, p.116 (1994).

[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. Shor, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (IEEE Press, Los Alamitos, 1994), p. 124.

[7] D. Gottesman, The Heisenberg representation of quantum computers. arXiv: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

[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 Information and Computation, **4** 134 (2004).

[14] 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.

[15] 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).

[16] 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).

[17] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Achieving quantum supremacy with sparse and noisy commuting quantum computations. arXiv:1610.01808

[18] S. Aaronson and A. Arkhipov, The computational complexity of linear optics. Theory of Computing **9**, 143 (2013).

[19] T. Morimae, K. Fujii, and J. F. Fitzsimons, Hardness of classically simulating the one clean qubit model. Phys. Rev. Lett. **112**, 130502 (2014).

[20] T. Morimae, Hardness of classically sampling one clean qubit model with constant total variation distance error. arXiv:1704.03640

[21] For the details of the polynomial-time hierarchy, see Sec.5 of Ref. [22] or the supplementary material of Ref. [23], for example.

[22] S. Arora and B. Barak, *Computational Complexity: A Modern Approach.* Cambridge University Press, Cambridge, UK.

[23] 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).

[24] S. Aaronson, Quantum computing, postselection, and probabilistic polynomial-time. Proc. Roy. 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, Efficient linear optics quantum computation, Nature **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

[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. arXiv:1105.5100

[37] L. M. Adleman, J. DeMarrais, and M. A. Huang, Quantum Computability. SIAM J. Comput. **26** 1524 (1997).

[38] When $p_{acc} > 0$, it is lowerbounded by $1/2^{poly}$ for natural universal gate sets.

[39] J. Tarui, Probabilistic polynomials, AC^0 functions and the polynomial-time hierarchy. Theor. Comput. Sci. **113**, 167 (1993).

[40] S. Toda and M. Ogiwara, Counting classes are at least as hard as the polynomial-time hierarchy. SIAM J. Comput. **21**, 316 (1992).

[41] 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).

[42] K. W. Wagner, The complexity of combinatorial problems with succinct input representation. Acta Informatica **23**, 325 (1986).

[43] U. Schöning, Probabilistic complexity classes and lowness. Journal of Computer and System Sciences **39**, 84 (1989).

[44] A related paper Ref. [45] includes the statement of Theorem 1 with no proof, while it mainly studies the error reduction of the DQC1 model.

[45] 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), pp.13:1-13:14

[46] B. Kraus, Compressed quantum simulation of the Ising model. Phys. Rev. Lett. **107**, 250503 (2011).

[47] Z. Li et al., Experimental realization of a compressed quantum simulation of a 32-spin Ising chain. Phys. Rev. Lett. **112**, 220501 (2014).

[48] 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.

[49] Calculating a function is called #P-hard if the calculation can be reduced to the calculation of the number of accepting paths for a non-deterministic Turing machine.

[50] See Supplementary Material, which includes Refs. [51–55]

[51] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, H. Weinfurter, Elementary gates for quantum computation. Phys. Rev. A **52** 3457 (1995).

[52] G. Kuperberg, How hard is it to approximate the Jones polynomial? Theory of Computing 11, 183 (2015).

[53] S. Fenner, F. Green, S. Homer, Y. Zhang, Bounds on the power of constant-depth quantum circuits. 15th International Symposium on Fundamentals of Computation Theory. Lecture Notes in Comput. Sci. **3623**, pp.44 (2005).

[54] R. Jozsa, B. Kraus, A. Miyake, and J. Watrous, Matchgate and space-bounded quantum computations are equivalent. Proc. R. Soc. A **466**, 809 (2010).

[55] 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), pp.13:1-13:14.