Power of one nonclean qubit

Tomoyuki Morimae,[1,*] Keisuke Fujii,[2,3,†] and Harumichi Nishimura[4,‡]
[1]*ASRLD Unit, Gunma University, 1-5-1 Tenjincho, Kiryu, Gunma, 376-0052, Japan*
[2]*Photon Science Center, Graduate School of Engineering, The University of Tokyo, 2-11-16 Yayoi, Bunkyoku, Tokyo 113-8656, Japan*
[3]*JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*
[4]*Graduate School of Information Science, Nagoya University, Furocho, Chikusaku, Nagoya, Aichi, 464-8601, Japan*
(Received 8 November 2016; published 25 April 2017)

The one-clean qubit model (or the DQC1 model) is a restricted model of quantum computing where only a single qubit of the initial state is pure and others are maximally mixed. Although the model is not universal, it can efficiently solve several problems whose classical efficient solutions are not known. Furthermore, it was recently shown that if the one-clean qubit model is classically efficiently simulated, the polynomial hierarchy collapses to the second level. A disadvantage of the one-clean qubit model is, however, that the clean qubit is too clean: for example, in realistic NMR experiments, polarizations are not high enough to have the perfectly pure qubit. In this paper, we consider a more realistic one-clean qubit model, where the clean qubit is not clean, but depolarized. We first show that, for any polarization, a multiplicative-error calculation of the output probability distribution of the model is possible in a classical polynomial time if we take an appropriately large multiplicative error. The result is in strong contrast with that of the ideal one-clean qubit model where the classical efficient multiplicative-error calculation (or even the sampling) with the same amount of error causes the collapse of the polynomial hierarchy. We next show that, for any polarization lower-bounded by an inverse polynomial, a classical efficient sampling (in terms of a sufficiently small multiplicative error or an exponentially small additive error) of the output probability distribution of the model is impossible unless BQP (bounded error quantum polynomial time) is contained in the second level of the polynomial hierarchy, which suggests the hardness of the classical efficient simulation of the one nonclean qubit model.

DOI: 10.1103/PhysRevA.95.042336

To show the supremacy of quantum computing over classical computing is one of the most central research subjects in physics and computer science. Although several quantum advantages have been shown in terms of communication complexity [1,2] and query complexity [3,4], the ultimate question remains open: Is BPP (bounded error probabilistic polynomial time) equal to BQP (bounded error quantum polynomial time)?

One good strategy to study the gap between quantum and classical is restricting the quantum side. It is also important from the experimental point of view given the high technological demands for the realization of a universal quantum computer. For example, quantum computing that uses only Clifford gates [5,6] or fermionic linear optical gates (or the matchgates) [7–10] is classically efficiently simulatable. On the other hand, restricted models that do not seem to be classically efficiently simulatable do exist [11–15]. For example, if quantum computing that uses only noninteracting bosons [15] or commuting gates [12–14] (the so-called IQP model) is classically efficiently simulated, then the polynomial hierarchy collapses to the third level (or the second level [16]). Since a collapse of the polynomial hierarchy is not believed to happen, these results suggest the hardness of the classical efficient simulation of these restricted models.

The one-clean qubit model (or the DQC1 model) [17] is another restricted model of quantum computing that is believed to be stronger than classical computing. The model was originally motivated by NMR, which has over half a century of history and mature control schemes [18–20]. An NMR spin ensemble system has several physical advantages: for example, molecules consisting of a wide variety of nuclear and electron spins can be chemically synthesized. Furthermore, the macroscopic signals are obtained by virtue of the huge number of copies in the ensemble with less backaction. Finally, each spin is highly isolated from external degrees of freedom, which is favorable to avoid decoherence. For these reasons, a NMR spin ensemble system is a useful experimental setup to probe quantum many-body dynamics and, in fact, it has been applied to several quantum information processing tasks including quantum simulation [21]. However, a disadvantage of NMR is that the initialization (polarization) of a nuclear spin is not easy. Therefore, NMR quantum information processing has to be a highly-mixed-state quantum computation.

The one-clean qubit model formalizes NMR quantum information processing in the following way: First, the initial state is $|0\rangle\langle 0| \otimes (\frac{I}{2})^{\otimes n-1}$, where $I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator. Second, any (uniformly generated polynomial-time) n-qubit unitary operator is applied on it. Finally, some qubits are measured in the computational basis. (Note that, in some strict definitions, only a single qubit is allowed to be measured, or only an expectation value of a single-qubit measurement is obtained.)

If the clean qubit $|0\rangle$ 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 $U(\frac{I}{2})^{\otimes n}U^\dagger = (\frac{I}{2})^{\otimes n}$ for any unitary operator U. This example suggests that the one-clean qubit model is also classically efficiently simulatable, since only a single pure qubit does not seem to cause any drastic change. However, surprisingly, the

*morimae@gunma-u.ac.jp
†fujii@qi.t.u-tokyo.ac.jp
‡hnishimura@is.nagoya-u.ac.jp

model can efficiently solve several problems whose efficient classical solutions are not known, such as the spectral density estimation [17], testing integrability [22], calculations of the fidelity decay [23], and approximations of the Jones polynomial, HOMFLY polynomial, and Turaev–Viro invariant [24–27]. Furthermore, it was recently shown that, if the probability distribution of the measurement result on the single output qubit of the one clean qubit model is classically efficiently sampled (in terms of a multiplicative error or an exponentially small additive error), then the polynomial hierarchy collapses to the second level [16,28]. Roles of quantumness (entanglement, discord, etc.) in the one-clean qubit model has also been intensively studied [29–37].

A disadvantage of the one-clean qubit model is, however, that the clean qubit is too clean: for example, in realistic experiments, the polarization of spins in an NMR ensemble is not high enough to obtain the perfectly pure qubit (even if the algorithmic cooling or the quantum data compression [38–40] is employed). Therefore, the following important question remains open: can we show any hardness of a classical efficient simulation of a more realistic one "nonclean" qubit model?

In this paper, we consider a modified version of the one clean qubit model where the clean qubit of the initial state is not clean but depolarized [Eq. (1)]. We first show that, for any polarization, a multiplicative-error calculation of the output probability distribution of the model is possible in a classical polynomial time if we take a sufficiently large multiplicative error. Note that the result is in strong contrast with that of the ideal one-clean qubit model where the classical efficient multiplicative-error calculation (or even the sampling) with the same amount of error causes the collapse of the polynomial hierarchy [16,28]. We also point out that the bound of the multiplicative error is optimal by showing a counterexample for errors smaller than the bound. We next consider the sampling of the output probability distribution of our model. We show that for any polarization lower-bounded by an inverse polynomial, a classical efficient sampling (in terms of a sufficiently small multiplicative error or an exponentially small additive error) is impossible unless BQP is contained in the second level of the polynomial hierarchy. Since it is not believed to happen [41], the result demonstrates the power of one nonclean qubit. In short, the computational capability of the one nonclean qubit model with a small polarization exhibits a "phase transition" on the magnitude of the polarization: a classical simulation with a multiplicative error larger than the polarization is possible, but it is impossible when the error is smaller than the polarization.

Note that, with similar and other motivations, noisy versions of IQP circuits have been studied recently and shown to be hard to efficiently simulate classically [14,42]. Moreover, quantum computing that uses a universal gate set but is too noisy to realize fault-tolerant universal quantum computing was shown to be hard to classically efficiently simulate [43].

One nonclean qubit model. We consider the following model: The initial state is the n-qubit state

$$\rho_\epsilon^{\text{init}} \equiv \left(\frac{1+\epsilon}{2}|0\rangle\langle 0| + \frac{1-\epsilon}{2}|1\rangle\langle 1|\right) \otimes \left(\frac{I}{2}\right)^{\otimes(n-1)}, \quad (1)$$

where the first qubit corresponds to the nuclear spin to be probed whose polarization ϵ is relatively higher than the others but still very small. (This type of nonclean qubit model was also studied in Ref. [44].) The case $\epsilon = 1$ corresponds to the original one-clean qubit model. Any (uniformly generated polynomial-time) n-qubit unitary operator U is applied on the initial state to obtain $\rho_\epsilon \equiv U\rho_\epsilon^{\text{init}}U^\dagger$. Finally, some qubits are measured in the computational basis. If we measure all qubits, the probability p_z of obtaining the result $z \in \{0,1\}^n$ is

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

Multiplicative-error calculation. First, we consider calculations of the output probability distribution of the model. As is shown in Appendix A, the exact calculation is trivially #P hard (actually GapP complete). We therefore consider approximations; namely, multiplicative-error calculations. Here, a multiplicative-error approximation with the error $c \geqslant 0$ means that the target value p and the calculated value q satisfy $|p-q| \leqslant cp$.

Result 1. For any $0 \leqslant \epsilon < 1$, p_z can be approximated by the uniform distribution $q_z = \frac{1}{2^n}$ with any multiplicative error c that satisfies $c \geqslant \frac{\epsilon}{1-\epsilon}$.

Proof. We can show $\frac{1-\epsilon}{2^n} \leqslant p_z \leqslant \frac{1+\epsilon}{2^n}$ for any $z \in \{0,1\}^n$. Therefore,

$$\left|p_z - \frac{1}{2^n}\right| \leqslant \frac{\epsilon}{2^n} = \frac{\epsilon}{1-\epsilon}\frac{1-\epsilon}{2^n} \leqslant cp_z.$$

■

According to the result of Ref. [16], if the output probability distribution of the computational-basis measurement on the single output qubit of the one clean qubit model is classically efficiently sampled with the $c = 1 - \frac{1}{2^n}$ multiplicative error, then the polynomial hierarchy collapses to the second level (see Appendix B). Result 1 shows that the hardness result no longer holds for the one nonclean qubit case [45]. In fact, from Result 1, for any $x \in \{0,1\}$,

$$\left|\sum_{y\in\{0,1\}^{n-1}} p_{xy} - \frac{1}{2}\right| = \left|\sum_{y\in\{0,1\}^{n-1}} p_{xy} - \sum_{y\in\{0,1\}^{n-1}} \frac{1}{2^n}\right| \leqslant \sum_{y\in\{0,1\}^{n-1}} \left|p_{xy} - \frac{1}{2^n}\right| \leqslant c \sum_{y\in\{0,1\}^{n-1}} p_{xy},$$

which means that the probability $\sum_{y\in\{0,1\}^{n-1}} p_{xy}$ of obtaining $x \in \{0,1\}$ when the first qubit of our model is measured in the computational basis is approximated as $\frac{1}{2}$ (and therefore efficiently sampled classically) with the multiplicative error c. If we take the polarization ϵ as $\epsilon \leqslant \frac{1}{2} - \frac{1}{2^{n+2}-2}$, for example, c can be $c = 1 - \frac{1}{2^n}$.

Optimality of the bound. We can show that the bound $c \geqslant \frac{\epsilon}{1-\epsilon}$ of Result 1 is optimal in the following sense:

Result 2. For any $0 \leqslant \epsilon < 1$ and $c \geqslant 0$ such that $0 \leqslant c < \frac{\epsilon}{1-\epsilon}$, and for any probability distribution $q : \{0,1\}^n \ni z \mapsto q_z \in [0,1]$, there exists an n-qubit unitary operator U such that $|p_z - q_z| > cp_z$ for a certain $z \in \{0,1\}^n$.

Proof. If $q_z < \frac{1}{2^n}$ for all $z \in \{0,1\}^n$, then $\sum_{z\in\{0,1\}^n} q_z < 1$, which is a contradiction. Therefore, there is at least one $y \in \{0,1\}^n$ such that $q_y \geqslant \frac{1}{2^n}$. Let $y_1 \in \{0,1\}$ be the first bit of y. If we take $U = X^{y_1\oplus 1} \otimes I^{\otimes n-1}$,

$$\begin{aligned} p_y &= \epsilon\left\langle y\middle| U\left(|0\rangle\langle 0| \otimes \frac{I^{\otimes n-1}}{2^{n-1}}\right)U^\dagger\middle|y\right\rangle + \frac{1-\epsilon}{2^n} \\ &= \epsilon\left\langle y\middle|\left(|y_1\oplus 1\rangle\langle y_1\oplus 1| \otimes \frac{I^{\otimes n-1}}{2^{n-1}}\right)\middle|y\right\rangle + \frac{1-\epsilon}{2^n} \\ &= \frac{1-\epsilon}{2^n}, \end{aligned}$$

and therefore $|p_y - q_y| \geqslant \frac{\epsilon}{2^n}$, while $cp_y < \frac{\epsilon}{1-\epsilon}\frac{1-\epsilon}{2^n} = \frac{\epsilon}{2^n}$. Hence we obtain $|p_y - q_y| > cp_y$. ∎

Multiplicative-error sampling. We next consider the sampling. We first show the hardness result for the multiplicative-error case.

Result 3. Let us assume that, for any (uniformly generated polynomial-time) n-qubit unitary operator U, there exists a $poly(n)$-time classical probabilistic algorithm that outputs $z \in \{0,1\}^n$ with probability q_z such that

$$|p_{0^n} - q_{0^n}| \leqslant cp_{0^n}, \tag{2}$$

with a certain c that satisfies $0 \leqslant c \leqslant \epsilon - \frac{1}{\delta(n)}$ for a polynomial $\delta > 0$. Then BQP is contained in the SBP (small bounded error probability).

Note that the value of c considered in Result 3 is always smaller than that of Result 1, since $\frac{\epsilon}{1-\epsilon} - (\epsilon - \frac{1}{\delta}) \geqslant 0$ and, therefore, there is no contradiction between these two results. More importantly, since $\frac{\epsilon}{1-\epsilon} = \epsilon + O(\epsilon^2)$ for small ϵ, the combination of Result 1 and Result 3 means that the polarization ϵ is the "phase-transition point" for the multiplicative error c: if $c > \epsilon$ then the classical simulation is possible (Result 1), while if $c < \epsilon$ then it is impossible (Result 3).

There are three further remarks before the proof of Result 3. First, Result 3 implicitly assumes that ϵ is lower-bounded by an inverse polynomial, since otherwise no c can satisfy $c \leqslant \epsilon - \frac{1}{\delta}$. The assumption, $\epsilon \geqslant 1/poly$, is acceptable, since we can take such ϵ in realistic NMR experiments. (Actually, ϵ can be even a small but system-size-independent constant.) Second, the standard definition of the multiplicative-error sampling is that $|p_z - q_z| \leqslant cp_z$ for any $z \in \{0,1\}^n$ but, in Result 3, the satisfiability only for $z = 0^n$ is enough. Finally, SBP is defined in the following way [46]: A language L is in SBP if there exist a polynomial r and a uniformly generated family of polynomial-size probabilistic classical circuits such that, if $x \in L$, then the acceptance probability is $\geqslant 2^{-r(|x|)}$ and, if $x \notin L$, then the acceptance probability is $\leqslant 2^{-r(|x|)-1}$. As is shown in Appendix C, the bound $(2^{-r}, 2^{-r-1})$ can be replaced with $(a2^{-r}, b2^{-r})$ for any $0 \leqslant b < a \leqslant 1$ such that $a - b \geqslant \frac{1}{poly}$. It is known that SBP is in AM (Arthur-Merlin) [46], and therefore in the second level of the polynomial hierarchy: SBP $\subseteq$ AM $\subseteq \Pi_2^p$. Hence BQP $\subseteq$ SBP means that BQP is in the second level of the polynomial hierarchy. Note that BQP $\subseteq$ SBP itself is also unlikely, since SBP $\subseteq$ BPP$_{\text{path}}$ and there is an oracle such that BQP is not contained in BPP$_{\text{path}}$ [47].

Proof. Let us assume that a language L is in BQP. This means that for any polynomial r, there exists a uniformly generated family $\{V_x\}$ of polynomial-size quantum circuits such that

$$\langle 0^n|V_x^\dagger\left(|0\rangle\langle 0| \otimes I^{\otimes n-1}\right)V_x|0^n\rangle \begin{cases} \geqslant 1 - 2^{-r} & (x \in L) \\ \leqslant 2^{-r} & (x \notin L). \end{cases}$$

Here, $n = poly(|x|)$. Let us take $U = V_x^\dagger$. We also take r such that $\epsilon 2^{-r+1} \leqslant \frac{1}{2\delta}$.

If $x \in L$,

$$\begin{aligned} q_{0^n} &\geqslant (1-c)\left[\frac{\epsilon}{2^{n-1}}\langle 0^n|V_x^\dagger\left(|0\rangle\langle 0| \otimes I^{\otimes n-1}\right)V_x|0^n\rangle + \frac{1-\epsilon}{2^n}\right] \\ &\geqslant (1-c)\left[\frac{\epsilon}{2^{n-1}}\left(1-2^{-r}\right) + \frac{1-\epsilon}{2^n}\right] \\ &= \frac{(1-c)}{2^n}\left(1+\epsilon-\epsilon 2^{-r+1}\right). \end{aligned}$$

If $x \notin L$,

$$\begin{aligned} q_{0^n} &\leqslant (1+c)\left[\frac{\epsilon}{2^{n-1}}\langle 0^n|V_x^\dagger\left(|0\rangle\langle 0| \otimes I^{\otimes n-1}\right)V_x|0^n\rangle + \frac{1-\epsilon}{2^n}\right] \\ &\leqslant (1+c)\left[\frac{\epsilon}{2^{n-1}}2^{-r} + \frac{1-\epsilon}{2^n}\right] \\ &= \frac{(1+c)}{2^n}\left(1-\epsilon+\epsilon 2^{-r+1}\right). \end{aligned}$$

Since

$$\begin{aligned} &(1-c)\left(1+\epsilon-\epsilon 2^{-r+1}\right) - (1+c)\left(1-\epsilon+\epsilon 2^{-r+1}\right) \\ &= 2\left(\epsilon - \epsilon 2^{-r+1} - c\right) \\ &\geqslant 2\left[\epsilon - \frac{1}{2\delta} - \left(\epsilon - \frac{1}{\delta}\right)\right] \\ &= \frac{1}{\delta}, \end{aligned}$$

L is in SBP. ∎

Exponentially small additive error sampling. We can also show a similar hardness result for the exponentially small additive-error case.

Result 4. Let us assume that for any (uniformly generated polynomial-time) n-qubit unitary operator U, there exists a $poly(n)$-time classical probabilistic algorithm that outputs $z \in \{0,1\}^n$ with probability q_z such that

$$|p_{0^n} - q_{0^n}| \leqslant \eta, \tag{3}$$

with a certain η that satisfies $0 \leqslant \eta \leqslant (\epsilon - \frac{1}{\delta})2^{-n}$ for a polynomial $\delta > 0$. Then BQP is contained in SBP.

Before giving a proof, there are two remarks: First, we again implicitly assume $\epsilon \geqslant 1/poly$. Second, the assumption (3) can be replaced with the more standard assumption (L_1-norm additive-error approximation), $\sum_{z\in\{0,1\}^n} |p_z - q_z| \leqslant \eta$, since if it is satisfied then $|p_{0^n} - q_{0^n}| \leqslant \sum_{z\in\{0,1\}^n} |p_z - q_z| \leqslant \eta$, and therefore Eq. (3) is satisfied. Since Eq. (3) is weaker, we have used it.

Proof. Let us assume that a language L is in BQP, and let V_x be the corresponding circuit as assumed in the proof of Result 3. We take $U = V_x^\dagger$, and r such that $\epsilon 2^{-r+1} \leqslant \frac{1}{2\delta}$. If $x \in L$, $q_{0^n} \geqslant \frac{1}{2^n}(1+\epsilon-\epsilon 2^{-r+1} - 2^n\eta)$. If $x \notin L$, $q_{0^n} \leqslant$

$\frac{1}{2^n}(2^{-r+1}\epsilon + 1 - \epsilon + 2^n\eta)$. Since

$$\left(1+\epsilon-\epsilon 2^{-r+1}-2^n\eta\right)-\left(1-\epsilon+\epsilon 2^{-r+1}+2^n\eta\right) \geqslant 2\left[\epsilon-\frac{1}{2\delta}-\left(\epsilon-\frac{1}{\delta}\right)\right]=\frac{1}{\delta},$$

L is in SBP. ■

Discussion. In this paper, we have used a multiplicative or an exponentially small additive error in the definition of the classical samplability. It is an important open problem whether we can generalize the results to a constant or inverse-polynomial L_1-norm error as was done for the boson sampling [15], the IQP [13,14], and Fourier sampling [48]. (These results do not seem to be directly applied to the one-qubit model, even in the perfect polarization case, since the one-qubit model seems to be able to simulate standard quantum computing with only an exponentially small rate.) In the present case, however, using a multiplicative or an exponentially small additive error is justified, since in our case the model itself is noisy. In other words, we consider the following sampling problem: "sample the output probability distribution of a noisy one clean qubit model." The problem can be, of course, exactly solvable with the noisy one clean qubit model, but we have shown that solving the problem classically is impossible even with a multiplicative or an exponentially small additive error. We have therefore shown the existence of a sampling problem that can be exactly solvable by a realistic nonuniversal quantum computer but cannot be solved by a classical computer even with a multiplicative or an exponentially small additive error.

We have considered the output probability distribution of the measurements on all qubits. It is an open problem whether we can reduce the number of measured qubits to one. Furthermore, we want to improve our consequence, BQP $\subseteq$ SBP, to a more unlikely one such as the collapse of the polynomial hierarchy, but at this moment we do not know how to do it.

Finally, to conclude this paper, let us discuss roles of entanglement in NMR quantum computing. In Ref. [49], a criterion on the initial polarization below which the system becomes a separable state was derived, and it was pointed out that states used in NMR experiments are separable states. It sounds like NMR quantum information processing has no quantum power, and in fact some researchers have insisted that NMR quantum information processing is useless. The conclusion is, however, wrong. In fact, a polynomially small purity keeps the state outside the separable ball [44]. Furthermore, as is shown in the present paper, NMR quantum computing can demonstrate quantum supremacy for some sampling problems. Finally, in the first place, entanglement is not directly connected to the quantum speedup: recently it was shown that a larger entanglement does not necessarily mean a quantum speedup [50,51], and that quantum computing whose register always has a small bipartite entanglement can solve any BQP problem [52]. Interestingly, even if we consider a much weaker model, which we call separable quantum computing, where the register is always separable during the computation, its classical simulatability is not so obvious. For example, even if the register is always separable, it seems to be hard to find a separable decomposition after every local unitary gate operation, since after a local unitary gate operation, some pure states in the mixture can be entangled. Furthermore, although any discord-free quantum computation (with one- or two-qubit gates) is classically simulatable [53], a separable state can have nonzero quantum discord.

ACKNOWLEDGMENTS

We thank Animesh Datta and Aharon Brodutch for comments on our manuscript. T.M. is supported by 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 of JSPS. K.F. is supported by KAKENHI No. 16H02211, PRESTO, JST, CREST, JST, and ERATO, JST. H.N. is supported by the Grant-in-Aid for Scientific Research (A) No. 26247016 and No. 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.

APPENDIX A

It is easy to see that the exact calculation of the output probability distribution of our model is #P hard (actually, GapP complete), because the ability of the exact calculation of the output probability distribution of the model allows us to exactly calculate the output probability distribution of the one clean qubit model, which contains (in an exponentially small rate) the output probability distribution of any (polynomial-time) quantum computing [44]. It is known that the exact calculation of the output probability distribution of (polynomial-time) quantum computing is #P hard (actually GapP complete) [54].

APPENDIX B

Here we show that, if the output probability distribution of the one clean qubit model is efficiently sampled classically with the multiplicative error $c = 1 - \frac{1}{2^n}$, then NQP (nondeterministic quantum polynomial time) is in NP, which causes the collapse of the polynomial hierarchy to the second level. We follow the argument in Refs. [16,55]. Let us assume that a language L is in NQP, which means that there exists a uniformly generated family $\{V_x\}$ of polynomial-size quantum circuits such that, if $x \in L$ then $0 < p < 1$, and if $x \notin L$ then $p = 0$, where p is the acceptance probability. It was shown in Ref. [55] that from V_x, which acts on $n-1$ qubits, we can construct an n-qubit one clean qubit circuit such that the probability $\tilde{p}$ of obtaining 1 when the clean qubit is measured in the computational basis is $\tilde{p} = \frac{4}{2^{n-1}}p(1-p)$. Therefore if $x \in L$ then $\tilde{p} > 0$, and if $x \notin L$ then $\tilde{p} = 0$. Let us assume that there exists a classical polynomial-time probabilistic algorithm whose acceptance probability q satisfies $|\tilde{p} - q| \leqslant (1 - \frac{1}{2^n})\tilde{p}$. Then, if $x \in L$ we have $q \geqslant \frac{\tilde{p}}{2^n} > 0$, and if $x \notin L$ then $q \leqslant (2 - \frac{1}{2^n})\tilde{p} = 0$. Therefore, NQP is in NP, which causes the collapse of the polynomial hierarchy to the second level.

APPENDIX C

Here we show that the bound $(2^{-r},2^{-r-1})$ of SBP can be replaced with $(a2^{-r},b2^{-r})$ for any $0 \leqslant b < a \leqslant 1$ such that $a-b \geqslant \frac{1}{q}$, where $q > 0$ is a polynomial.

Since $a \geqslant b + \frac{1}{q} \geqslant \frac{1}{q}$, there exists a polynomial $k \geqslant 0$ such that $a > \frac{1}{2^k}$. Let V_x be the original circuit of SBP. We define the modified circuit V_x' in the following way: it first runs the original circuit V_x, and then accepts with probability $\frac{1}{a2^k}$ if V_x accepts. If $x \in L$, the acceptance probability of V_x' is $p_{\rm acc} \geqslant \frac{a2^{-r}}{a2^k} = \frac{1}{2^{r+k}}$. If $x \notin L$, it is

$$\begin{aligned} p_{\rm acc} &\leqslant \frac{b2^{-r}}{a2^k} \\ &= \frac{1}{2^{r+k}} \frac{a-(a-b)}{a} \\ &= \frac{1}{2^{r+k}} \left(1 - \frac{a-b}{a}\right) \\ &\leqslant \frac{1}{2^{r+k}} \left(1 - \frac{1}{q}\right). \end{aligned}$$

We run V_x' q times and accept if all results accept. If $x \in L$, the acceptance probability is $p_{\rm acc}^q \geqslant \frac{1}{2^{(r+k)q}}$. If $x \notin L$, it is

$$\begin{aligned} p_{\rm acc}^q &\leqslant \frac{1}{2^{(r+k)q}} \left(1 - \frac{1}{q}\right)^q \\ &= \frac{1}{2^{(r+k)q}} \left[\left(1 + \frac{1}{q-1}\right)^q\right]^{-1} \\ &\leqslant \frac{1}{2^{(r+k)q}} \frac{1}{2}, \end{aligned}$$

where we have used

$$\begin{aligned} \left(1 + \frac{1}{q-1}\right)^q &= \sum_{j=0}^{q} \binom{q}{j} \left(\frac{1}{q-1}\right)^j \\ &\geqslant 1 + \binom{q}{1} \frac{1}{q-1} \\ &= 1 + \frac{q}{q-1} \\ &\geqslant 2. \end{aligned}$$

[1] H. Buhrman, R. Cleve, and A. Wigderson, Quantum vs. Classical Communication and Computation, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing* (ACM, New York, USA, 1998), p. 63.

[2] R. Raz, Exponential Separation of Quantum and Classical Communication Complexity, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* (ACM, New York, USA, 1999), p. 358.

[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, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, USA, 1994), p. 116.

[5] D. Gottesman, The Heisenberg Representation of Quantum Computers, Group22: in *Proceedings of the XXII International Colloquium on Group*, edited by S. P. Corney, R. Delbourgo, and P. D. Jarvis (International Press, Cambridge, 1999), pp. 32–43.

[6] S. Aaronson and D. Gottesman, Improved simulation of stabilizer circuits, Phys. Rev. A **70**, 052328 (2004).

[7] L. G. Valiant, Quantum circuits that can be simulated classically in polynomial time, SIAM J. Comput. **31**, 1229 (2002).

[8] B. M. Terhal and D. P. DiVincenzo, Classical simulation of noninteracting-fermion quantum circuits, Phys. Rev. A **65**, 032325 (2002).

[9] E. Knill, Fermionic linear optics and matchgates, arXiv:quant-ph/0108033.

[10] R. Jozsa and A. Miyake, Matchgates and classical simulation of quantum circuits, Proc. R. Soc. London, Ser. A **464**, 3089 (2008).

[11] S. P. Jordan, Permutational quantum computing, Quantum Inf. Comput. **10**, 470 (2010).

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

[13] 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).

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

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

[16] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Power of quantum computation with few clean qubits, in *Proceedings of 43rd International Colloquium on Automata, Languages, and Programming (ICALP)* (Dagstuhl Publishing, Germany, 2016), p. 13:1.

[17] E. Knill and R. Laflamme, Power of One Bit of Quantum Information, Phys. Rev. Lett. **81**, 5672 (1998).

[18] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature (London) **414**, 883 (2001).

[19] D. G. Cory *et al.*, NMR-based quantum information processing: Achievements and prospects, Fortschr. Phys. **48**, 875 (2000).

[20] J. A. Jones, Quantum computing with NMR, Prog. Nucl. Magn. Reson. Spectrosc. **59**, 91 (2011).

[21] G. A. Álvarez, D. Suter, and R. Kaiser, Localization-delocalization transition in the dynamics of dipolar-coupled nuclear spins, Science **349**, 846 (2015).

[22] 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).

[23] 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).
[24] P. W. Shor and S. P. Jordan, Estimating Jones polynomials is a complete problem for one clean qubit, Quantum Inf. Comput. **8**, 681 (2008).
[25] 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).
[26] S. P. Jordan and P. Wocjan, Estimating Jones and HOMFLY polynomials with one clean qubit, Quantum Inf. Comput. **9**, 264 (2009).
[27] S. P. Jordan and G. Alagic, Approximating the Turaev-Viro invariant of mapping tori is complete for one clean qubit, arXiv:1105.5100.
[28] T. Morimae, K. Fujii, and J. F. Fitzsimons, Hardness of Classically Simulating the One Clean Qubit Model, Phys. Rev. Lett. **112**, 130502 (2014).
[29] A. Datta and S. Gharibian, Signatures of non-classicality in mixed-state quantum computation, Phys. Rev. A **79**, 042325 (2009).
[30] A. Datta, Ph.D. thesis, Indian Institute of Technology, 2008 (unpublished); arXiv:0807.4490.
[31] A. Datta, A. Shaji, and C. M. Caves, Quantum Discord and the Power of One Qubit, Phys. Rev. Lett. **100**, 050502 (2008).
[32] A. Datta and G. Vidal, On the role of entanglement and correlations in mixed-state quantum computation, Phys. Rev. A **75**, 042310 (2007).
[33] B. Dakić, V. Vedral, and Č. Brukner, Necessary and Sufficient Condition for Nonzero Quantum Discord, Phys. Rev. Lett. **105**, 190502 (2010).
[34] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, The classical-quantum boundary for correlations: Discord and related measures, Rev. Mod. Phys. **84**, 1655 (2012).
[35] O. Moussa, C. A. Ryan, D. G. Cory, and R. Laflamme, Testing Contextuality on Quantum Ensembles with One Clean Qubit, Phys. Rev. Lett. **104**, 160501 (2010).
[36] G. Passante, O. Moussa, and R. Laflamme, Measuring geometric quantum discord using one bit of quantum information, Phys. Rev. A **85**, 032325 (2012).
[37] M. Boyer, A. Brodutch, and T. Mor, Entanglement and deterministic quantum computing with one qubit, Phys. Rev. A **95**, 022330 (2017).
[38] L. J. Schulman and U. V. Vazirani, Molecular Scale Heat Engines and Scalable Quantum Computation, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* (ACM, New York, USA, 1999), p. 322.
[39] P. O. Boykin, T. Mor, V. Roychowdhury, F. Vatan, and R. Vrijen, Algorithmic cooling and scalable NMR quantum computers, Proc. Natl. Acad. Sci. USA **99**, 3388 (2002).
[40] R. Cleve and D. P. DiVincenzo, Schumacher's quantum data compression as a quantum computation, Phys. Rev. A **54**, 2636 (1996).
[41] S. Aaronson, BQP and the Polynomial Hierarchy, in *Proceedings of the 42nd ACM Symposium on Theory of Computing* (ACM, New York, USA, 2010), p. 141.
[42] K. Fujii and S. Tamate, Computational quantum-classical boundary of noisy commuting quantum circuits, Sci. Rep. **6**, 25598 (2016).
[43] K. Fujii, Noise threshold of quantum supremacy. arXiv:1610.03632.
[44] A. Datta, S. T. Flammia, and C. M. Caves, Entanglement and the power of one qubit, Phys. Rev. A **72**, 042316 (2005).
[45] Note that Result 1 might look strange since it says that the one nonclean qubit model is classically simulatable even when ϵ is smaller than but very close to 1, which seems to contradict to the result of Ref. [16]. However, note that, when $\epsilon \to 1$, $c \to \infty$, and therefore, as is explained in the main text, the comparison with the hardness result of Ref. [16] becomes meaningful when ϵ is below 1/2.
[46] E. Böhler, C. Glaßer, and D. Meister, Error-bounded probabilistic computations between MA and AM, J. Comput. Syst. Sci. **72**, 1043 (2006).
[47] L. Chen, A note on oracle separation for BQP, arXiv:1605.00619.
[48] B. Fefferman and C. Umans, The power of quantum Fourier sampling, arXiv:1507.05592.
[49] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Separability of Very Noisy Mixed States and Implications for NMR Quantum Computing, Phys. Rev. Lett. **83**, 1054 (1999).
[50] M. J. Bremner, C. Mora, and A. Winter, Are Random Pure States Useful for Quantum Computation?, Phys. Rev. Lett. **102**, 190502 (2009).
[51] D. Gross, S. T. Flammia, and J. Eisert, Most Quantum States are Too Entangled to be Useful as Computational Resources, Phys. Rev. Lett. **102**, 190501 (2009).
[52] M. Van den Nest, Universal Quantum Computation with Little Entanglement, Phys. Rev. Lett. **110**, 060504 (2013).
[53] B. Eastin, Simulating concordant computations, arXiv:1006.4402.
[54] L. Fortnow and J. Rogers, Complexity limitations on quantum computation, J. Comput. Syst. Sci. **59**, 240 (1999).
[55] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Impossibility of classically simulating one-clean-qubit computation, arXiv:1409.6777.