Hardness of classically sampling the one-clean-qubit model with constant total variation distance error

Tomoyuki Morimae

Phys. Rev. A **96**, 040302 — Published 5 October 2017

DOI: 10.1103/PhysRevA.96.040302

Hardness of classically sampling one clean qubit model with constant total variation distance error

Tomoyuki Morimae*

Department of Computer Science, Gunma University,

1-5-1 Tenjincho, Kiryu, Gunma, 376-0052, Japan

(Dated: July 25, 2017)

Abstract

The one clean qubit model (or the DQC1 model) is a restricted model of quantum computing where only a single input qubit is pure and all other input qubits are maximally mixed. In spite of the severe restriction, the model can solve several problems (such as calculating Jones polynomials) whose classical efficient solutions are not known. Furthermore, it was shown that if the output probability distribution of the one clean qubit model can be classically efficiently sampled with a constant multiplicative error, then the polynomial hierarchy collapses to the second level. Is it possible to improve the multiplicative error hardness result to a constant total variation distance error one like other sub-universal quantum computing models such as the IQP model, the Boson Sampling model, and the Fourier Sampling model? In this paper, we show that it is indeed possible if we accept a modified version of the average case hardness conjecture. Interestingly, the anti-concentration lemma can be easily shown by using the special property of the one clean qubit model that each output probability is so small that no concentration occurs.

* morimae@gunma-u.ac.jp

I. INTRODUCTION

The one clean qubit model (or the DQC1 model) first introduced by Knill and Laflamme [1] is a restricted model of quantum computing where only a single input qubit is pure and all other input qubits are maximally mixed. In spite of the severe restriction, surprisingly, the model can solve several problems whose efficient classical solutions are not known, such as the spectral density estimation [1], testing integrability [2], calculations of the fidelity decay [3], and approximations of the Jones polynomial, HOMFLY polynomial, and Turaev-Viro invariant [4–7]. Furthermore, it was recently shown that if the output probability distribution of the one clean qubit model is classically efficiently sampled with a constant multiplicative error, then the polynomial hierarchy collapses to the third level [8] or the second level [9]. (Here, we say that a probability distribution $\{p_z\}_z$ is sampled by a machine M with a multiplicative error $\epsilon \geq 0$ if

$$|p_z - q_z| \leq \epsilon p_z$$

is satisfied for all z, where $\{q_z\}_z$ is the output probability distribution of M.) Since a collapse of the polynomial hierarchy is not believed to happen in computer science, the results suggest the impossibility of classically simulating the one clean qubit model. Similar hardness results for constant multiplicative error sampling were also shown for other sub-universal quantum computing models, such as the IQP model [10] and the Boson Sampling model [11].

The requirement of constant multiplicative error sampling is, however, strong, and sampling with a constant total variation distance error (or the L1-norm error) is considered as more appropriate. (Here, we say that a probability distribution $\{p_z\}_z$ is sampled by a machine M with a total variation distance error $\epsilon \geq 0$ if

$$\sum_z |p_z - q_z| \leq \epsilon$$

is satisfied, where $\{q_z\}_z$ is the output probability distribution of M.) In fact, the hardness results with constant total variation distance errors were shown for the IQP model [12], the Boson Sampling model [11], and the Fourier Sampling model [13] (assuming some conjectures). Is it possible to show a similar constant-total-variation-distance-error hardness result for the one clean qubit model?

In this paper, we show that it is indeed possible if we accept a modified version of the average case hardness conjecture. Our proof is similar to those of Refs. [11–13], but

there is one interesting difference which is specific to the one clean qubit model: the anti-concentration lemma can be easily shown. For the Boson Sampling model and the Fourier Sampling model, the anti-concentration lemma is a conjecture [11, 13]. For the IQP model, it is shown with some calculations by using a special structure of IQP circuits [12]. For the present case, as we will see later, the anti-concentration lemma is easily shown by using a special property of the one clean qubit model that each probability is so small that no concentration occurs. Note that recently two-design systems have also been shown to satisfy the anti-concentration lemma [14].

Regarding the average-case-vs-worst-case hardness conjecture, on the other hand, the present result (and the IQP result) are somehow weaker than the Boson Sampling result and the Fourier Sampling result, since the average case hardness of the exact calculation is shown for the Boson Sampling and Fourier Sampling, but not for the present model and the IQP.

II. AVERAGE CASE HARDNESS CONJECTURE

As in the cases of other sub-universal quantum computing models, such as the IQP model [12], the Boson Sampling model [11], and the Fourier Sampling model [13], we need a conjecture so-called "average case hardness conjecture", which claims that the #P-hardness for the worst case can be lifted to an average case. To show our result, which is a hardness of efficient classical sampling of the one clean qubit model with a constant total variation distance error, we need the following conjecture.

Conjecture: For each n, there exists a discrete set $\mathcal{U}_{n+1}$ of uniformly-generated polynomial-time $(n+1)$-qubit unitary operators such that calculating

$$f(z,U) \equiv \langle z|U(|0\rangle\langle 0| \otimes I^{\otimes n})U^\dagger|z\rangle$$

with a multiplicative error less than $1/2$ for more than $1/6$ fraction of $(z,U) \in \{0,1\}^{n+1} \times \mathcal{U}_{n+1}$ is #P-hard.

Here, $I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator, and $|z\rangle$ is the computational-basis state corresponding to the bit string z. (For example, if $z = 010$, $|z\rangle = |010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle$.)

Unfortunately, we do not know whether the conjecture is true or not, but we can show

that it is true at least for the worst case. Here, we give two proofs for the worst-case #P-hardness.

A. First proof

Let us consider a unitary operator U such that

$$U^\dagger = \Big[I \otimes |0\rangle\langle 0|^{\otimes n} + X \otimes (I^{\otimes n} - |0\rangle\langle 0|^{\otimes n})\Big](I \otimes C),$$

where C is an n-qubit IQP circuit. Then,

$$f(0^{n+1}, U) = |\langle 0^n|C|0^n\rangle|^2.$$

For certain IQP circuits C, $\langle 0^n|C|0^n\rangle$ is related to the partition function, Z, of the Ising model [12, 15] and the gap function, $gap(f)$, of a degree-3 polynomial f over $\mathbb{F}_2$ [12]:

$$\langle 0^n|C|0^n\rangle = \frac{Z}{2^n},$$
$$\langle 0^n|C|0^n\rangle = \frac{gap(f)}{2^n}.$$

It is known that calculating $|Z|^2$ and $gap(f)^2$ with constant multiplicative errors is #P-hard [12, 15]. Hence calculating $|\langle 0^n|C|0^n\rangle|^2 = f(0^{n+1}, U)$ with constant multiplicative errors is #P-hard for certain unitary operators U, which shows the correctness of the conjecture for the worst case.

B. Second proof

We define two unitary operators U_1 and U_2 as

$$U_1^\dagger = \Big[(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|) \otimes I^{\otimes n-1}\Big](I \otimes V),$$
$$U_2^\dagger = \Big[\Big(I \otimes |0\rangle\langle 0|^{\otimes 2} + X \otimes (I^{\otimes 2} - |0\rangle\langle 0|^{\otimes 2})\Big) \otimes I^{\otimes n-2}\Big](I \otimes V),$$

where V is an n-qubit unitary operator. Then, we obtain

$$f(0^{n+1}, U_1) = \langle 0^n|V^\dagger(|0\rangle\langle 0| \otimes I^{\otimes n-1})V|0^n\rangle,$$
$$f(0^{n+1}, U_2) = \langle 0^n|V^\dagger(|0\rangle\langle 0|^{\otimes 2} \otimes I^{\otimes n-2})V|0^n\rangle.$$

Now we show that calculating $f(0^{n+1}, U_1)$ and $f(0^{n+1}, U_2)$ with a constant multiplicative error $0 \leq \epsilon < 1$ is postBQP-hard. Since postBQP = PP [16] and $\mathrm{P}^{\mathrm{PP}} = \mathrm{P}^{\#\mathrm{P}}$, it means that

the calculation is #P-hard. Proof is as follows. Let us assume that there exists an algorithm that calculates a and b such that

$$|f(0^{n+1}, U_1) - a| \leq \epsilon f(0^{n+1}, U_1),$$
$$|f(0^{n+1}, U_2) - b| \leq \epsilon f(0^{n+1}, U_2).$$

Let L be a language in postBQP. Then, for any polynomial r, there exists a uniform family $\{V_x\}_x$ of polynomial-time quantum circuits such that

- If $x \in L$ then $P_{V_x}(o = 0|p = 0) \geq 1 - 2^{-r}$.
- If $x \notin L$ then $P_{V_x}(o = 0|p = 0) \leq 2^{-r}$.

Here,

$$P_{V_x}(o = 0|p = 0) = \frac{P_{V_x}(o = 0, p = 0)}{P_{V_x}(p = 0)},$$

$P_{V_x}(o = 0, p = 0)$ is the probability that V_x outputs $(o, p) = (0, 0)$, and $P_{V_x}(p = 0)$ is the probability that V_x outputs $p = 0$.

Let us construct U_1 and U_2 by using V_x. Then, for any polynomial r, if $x \in L$,

$$\begin{aligned}\frac{b}{a} &\geq \frac{1-\epsilon}{1+\epsilon}\frac{f(0^{n+1}, U_2)}{f(0^{n+1}, U_1)} \\ &\geq \frac{1-\epsilon}{1+\epsilon}(1 - 2^{-r}),\end{aligned}$$

and if $x \notin L$,

$$\begin{aligned}\frac{b}{a} &\leq \frac{1+\epsilon}{1-\epsilon}\frac{f(0^{n+1}, U_2)}{f(0^{n+1}, U_1)} \\ &\leq \frac{1+\epsilon}{1-\epsilon}2^{-r}.\end{aligned}$$

Therefore, if we can calculate a and b, we can solve L.

III. MAIN RESULT

If we accept the conjecture, we can show the following theorem, which is the main result of the present paper.

Theorem: If there exists a probabilistic polynomial-time classical algorithm that outputs $z \in \{0, 1\}^{n+1}$ with probability $q_z(U)$ such that

$$\sum_{z \in \{0,1\}^{n+1}} |p_z(U) - q_z(U)| \leq \epsilon$$

for any $U \in \cup_n \mathcal{U}_{n+1}$, then the polynomial hierarchy collapses to the third level. Here, $\epsilon = \frac{1}{36}$ and

$$p_z(U) \equiv \langle z|U\Big(|0\rangle\langle 0| \otimes \frac{I^{\otimes n}}{2^n}\Big)U^\dagger|z\rangle.$$

The theorem says that if the output probability distribution $p_z(U)$ of the one clean qubit model can be classically efficiently sampled with the total variation distance error ϵ, then the polynomial hierarchy collapses to the third level.

Proof: Now let us give a proof of the theorem. Our proof is similar to those of Refs. [11–13] except that the anti-concentration lemma can be easily shown.

Let $\delta > 0$ be a parameter specified later. From Markov's inequality,

$$\begin{aligned}\Pr_{z,U}\Big[|p_z(U) - q_z(U)| \geq \frac{\epsilon}{2^{n+1}\delta}\Big] &\leq \frac{2^{n+1}\delta}{\epsilon}\frac{1}{2^{n+1}|\mathcal{U}_{n+1}|}\sum_{U,z}|p_z(U) - q_z(U)| \\ &\leq \delta.\end{aligned}$$

From Stockmeyer's Counting Theorem [17], there exists an $\mathrm{FBPP}^{\mathrm{NP}}$ algorithm that outputs $\tilde{q}_z(U)$ such that

$$|\tilde{q}_z(U) - q_z(U)| \leq \frac{q_z(U)}{poly}.$$

Therefore,

$$\begin{aligned}|\tilde{q}_z(U) - p_z(U)| &\leq |\tilde{q}_z(U) - q_z(U)| + |q_z(U) - p_z(U)| \\ &\leq \frac{q_z(U)}{poly} + |q_z(U) - p_z(U)| \\ &= \frac{p_z(U) + q_z(U) - p_z(U)}{poly} + |q_z(U) - p_z(U)| \\ &\leq \frac{p_z(U) + |q_z(U) - p_z(U)|}{poly} + |q_z(U) - p_z(U)| \\ &= \frac{p_z(U)}{poly} + |q_z(U) - p_z(U)|\Big(1 + \frac{1}{poly}\Big) \\ &< \frac{p_z(U)}{poly} + \frac{\epsilon}{2^{n+1}\delta}\Big(1 + \frac{1}{poly}\Big)\end{aligned}$$

with more than $1 - \delta$ fraction of (z, U).

Let $S \subseteq \{0,1\}^{n+1} \times \mathcal{U}_{n+1}$ be the set of (z, U) such that

$$\frac{\epsilon}{2^{n+1}\delta} \leq \frac{p_z(U)}{3}.$$

Since

$$\begin{aligned} p_z(U) &= \langle z|U\Big(|0\rangle\langle 0| \otimes \frac{I^{\otimes n}}{2^n}\Big)U^\dagger|z\rangle \\ &= \frac{1}{2^n}\langle z|U(|0\rangle\langle 0| \otimes I^{\otimes n})U^\dagger|z\rangle \\ &\leq \frac{1}{2^n} \times 1 = \frac{1}{2^n}, \end{aligned}$$

for all (z, U), and

$$\sum_{z\in\{0,1\}^{n+1}} p_z(U) = 1$$

for all U, we obtain

$$\begin{aligned} 1 &= \frac{1}{|\mathcal{U}_{n+1}|}\sum_{U,z} p_z(U) \\ &= \frac{1}{|\mathcal{U}_{n+1}|}\sum_{(z,U)\in S} p_z(U) + \frac{1}{|\mathcal{U}_{n+1}|}\sum_{(z,U)\notin S} p_z(U) \\ &< \frac{1}{2^n|\mathcal{U}_{n+1}|}|S| + \frac{2^{n+1}|\mathcal{U}_{n+1}| - |S|}{|\mathcal{U}_{n+1}|}\frac{3\epsilon}{2^{n+1}\delta}, \end{aligned}$$

which means

$$\frac{|S|}{2^{n+1}|\mathcal{U}_{n+1}|} > \frac{1 - \frac{3\epsilon}{\delta}}{2 - \frac{3\epsilon}{\delta}}.$$

Therefore,

$$\begin{aligned} |\tilde{q}_z(U) - p_z(U)| &< \frac{p_z(U)}{poly} + \frac{p_z(U)}{3}\Big(1 + \frac{1}{poly}\Big) \\ &= p_z(U)\Big(\frac{1}{3} + \frac{1}{poly}\Big) \end{aligned}$$

for more than

$$F \equiv 1 - \delta - \frac{1}{2 - \frac{3\epsilon}{\delta}}$$

fraction of (z, U). For example, if we take $\delta = 6\epsilon$,

$$F = \frac{1}{6}.$$

Note that

$$p_z(U) = \frac{f(z, U)}{2^n}.$$

Therefore, the above result means that there exists an $\mathrm{FBPP}^{\mathrm{NP}}$ algorithm that outputs $\tilde{q}_z(U)$ such that

$$|\tilde{q}_z(U)2^n - f(z,U)| < f(z,U)\Big(\frac{1}{3} + \frac{1}{poly}\Big) < \frac{1}{2}f(z,U)$$

for more than 1/6 fraction of (z,U). If our average-case hardness conjecture is true, it means the collapse of the polynomial hierarchy to the third level.

ACKNOWLEDGMENTS

TM is supported by JST ACT-I No.JPMJPR16UP, the Grant-in-Aid for Scientific Research on Innovative Areas No.15H00850 of MEXT Japan, and the JSPS Grant-in-Aid for Young Scientists (B) No.26730003 and No.17K12637.

[1] E. Knill, and R. Laflamme, Power of one bit of quantum information. Phys. Rev. Lett. **81**, 5672 (1998).

[2] 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).

[3] 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).

[4] P. W. Shor and S. P. Jordan, Estimating Jones polynomials is a complete problem for one clean qubit. Quantum Inf. Comput. **8**, 681 (2008).

[5] 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).

[6] S. P. Jordan and P. Wocjan, Estimating Jones and HOMFLY polynomials with one clean qubit. Quantum Inf. Comput. **9**, 264 (2009).

[7] S. P. Jordan and G. Alagic, Approximating the Turaev-Viro invariant of mapping tori is complete for one clean qubit. arXiv:1105.5100

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

[9] 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), p.13:1.

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

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

[12] 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).

[13] B. Fefferman and C. Umans, On the power of quantum Fourier sampling. arXiv:1507.05592

[14] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, Anti-concentration theorems for schemes showing a quantum computational supremacy. arXiv:1706.03786

[15] K. Fujii and T. Morimae, Quantum commuting circuits and complexity of Ising partition functions. New J. Phys. **19**, 033003 (2017).

[16] S. Aaronson, Quantum computing, postselection, and probabilistic polynomial-time. Proc. Roy. Soc. A **461**, 3473 (2005).

[17] L. Stockmeyer, On approximation algorithm for #P. SIAM J. Comput. **14**, 849-861 (1985).