Classical simulation of DQC1$_2$ or DQC2$_1$ implies collapse of the polynomial hierarchy

Tomoyuki Morimae,$^1$ Harumichi Nishimura,$^2$ Keisuke Fujii,$^{3,4}$ and Shuhei Tamate$^{5,6}$

$^1$ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan
$^2$Graduate School of Information Science, Nagoya University, Chikusa-ku, Nagoya, Aichi, 464-8601, Japan
$^3$The Hakubi Center for Advanced Research, Kyoto University, Yoshida-Ushinomiya-cho, Sakyo-ku, Kyoto 606-8302, Japan
$^4$Graduate School of Informatics, Kyoto University, Yoshida-Hommachi, Sakyo-ku, Kyoto 606-8501, Japan
$^5$RIKEN Center for Emergent Matter Science, Wako-shi, Saitama 351-0198, Japan
$^6$National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430, Japan

(Dated: September 25, 2014)

Deterministic quantum computation with one quantum bit (DQC1) [E. Knill and R. Laflamme, Phys. Rev. Lett. 81, 5672 (1998)] is a restricted model of quantum computing where the input state is the completely-mixed state except for a single pure qubit, and a single output qubit is measured at the end of the computing. We can generalize it to the DQC$m_k$ model where $k$ input qubits are pure, and $m$ output qubits are measured. It was shown in [T. Morimae, K. Fujii, and J. F. Fitzsimons, Phys. Rev. Lett. 112, 130502 (2014)] that if the output probability distribution of the DQC$1_m$ model for $m \geq 3$ can be classically efficiently sampled, then the polynomial hierarchy collapses at the third level. In this paper, we show that the classical simulability of the DQC1$_2$ model or DQC2$_1$ model also leads to the collapse of the polynomial hierarchy at the third level. Our idea which solves the problem of the “shortage of postselected qubits” is to use the complexity class SBQP instead of postBQP.

The deterministic quantum computation with one quantum bit (DQC1), or the one clean qubit model, is a restricted model of quantum computing proposed by Knill and Laflamme [1] originally motivated by nuclear magnetic resonance (NMR) quantum information processing. The DQC1 model is illustrated in Fig. 1(a). The input of a DQC1 circuit is the completely-mixed state except for a single pure qubit, $|0\rangle\langle 0| \otimes (\frac{I}{2})^\otimes n$, where $I \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ is the two-dimensional identity operator. Any polynomial-size quantum circuit (denoted by $U$ in the figure) is applied on it, and a single output qubit is measured in the computational basis at the end of the computing in order to read out the computation result. (The measurement is denoted by $M$ in the figure.)

The DQC1 model does not seem to be universal. In fact, it is not universal under some reasonable assumptions [2]. Moreover, since any quantum computing on $2^{\otimes (n+1)}/2^{2n+1}$ is trivially classically simulable, the DQC1 model also seems to be classically simulable. However, surprisingly, it is known that the DQC1 model can efficiently solve several problems for which no efficient classical algorithms are known, such as calculations of an integrability tester [3], the spectral density [1], the fidelity decay [4], Jones and HOMFLY polynomials [5–7], and an invariant of 3-manifolds [8]. While entanglement remains bounded in the DQC1 model, there are some non-classical correlations [9–11]. In short, the DQC1 model is believed to be an intermediate model of computation between classical and universal quantum computation.

We can generalize the DQC1 model to the DQC$k_m$ model where $k$ input qubits are pure, and $m$ output qubits are measured at the end of the computing (Fig. 1(b)). In Ref. [12], it was shown that the DQC$1_m$ model with $m \geq 3$ cannot be classically efficiently simulated unless the polynomial hierarchy collapses at the third level. The proof is based on the postselected circuit of Fig. 2. The first $(n+1)$-qubit gate of the circuit is the $n$-qubit Toffoli gate $X \otimes |1\rangle\langle 1|^\otimes n + I \otimes (I^\otimes n − |1\rangle\langle 1|^\otimes n)$, which can be realized with a polynomial number of elementary gates [12]. Here, $X \equiv |0\rangle\langle 0| + |1\rangle\langle 1|$ is the bit flip operator. Two output qubits of the circuit denoted by $p$ are postselected, and the qubit denoted by $o$ is the output qubit for the decision problem. A postselection means the (fictitious) ability to project onto a specific branch of the wavefunction with unit probability. It was shown in Ref. [12] that the circuit can simulate postBQP, and therefore postDQC$1_m = \text{postBQP}$ for $m \geq 3$, where post$X$ is the class of languages recognized by a machine specified by $X$ (such as BQP and DQC$1_m$) with postselections. By using postBQP = PP [13], we obtain postDQC$1_m = \text{PP}$ for $m \geq 3$. Then from an argument similar to Refs. [15–17], we can show that if the output

![Diagram](image-url)
probability distribution of the DQC1\textsubscript{m} model for \( m \geq 3 \) can be classically efficiently sampled with a multiplicative error, then the polynomial hierarchy collapses at the third level. It is strongly believed in computer science that the polynomial hierarchy does not collapse. Therefore, the result suggests the hardness of the classical efficient simulation of the DQC1\textsubscript{m} model for \( m \geq 3 \).

![FIG. 2: The DQC1\textsubscript{2} circuit used in Ref. [12]. Two output qubits denoted by \( p \) are postselected qubits, and a single output qubit denoted by \( o \) is used to read out the output for the decision problem.](image)

Can we show a similar result for the DQC1\textsubscript{m} model with \( m \leq 2 \)? The reason why \( m \geq 3 \) is required for the proof of Ref. [12] is that, as we can see from Fig. 2, two postselected qubits are necessary: one is to prepare \(|0\rangle^\otimes n\) in order to simulate BQP circuits, and the other is for the postselection of postBQP. Therefore, the application of a similar technique to the case of \( m \leq 2 \) does not seem to be possible, since in this case at most only a single postselected qubit is available. In fact, as shown in Appendix, a direct application of the similar argument used in Ref. [12] to the DQC1\textsubscript{2} model leads to a weaker result: if the output probability distribution of the DQC1\textsubscript{2} model can be classically efficiently sampled, then BQP is in the polynomial hierarchy. Although it is believed that BQP is not in the polynomial hierarchy [13], and therefore the result somehow suggests the hardness of the classical simulation of the DQC1\textsubscript{2} model, the assumption that BQP is not in the polynomial hierarchy is much less solid than the robustness of the polynomial hierarchy.

In this paper, contrary to the intuition, we demonstrate that the classical simulability of the DQC1\textsubscript{2} model can cause the collapse of the polynomial hierarchy, which improves the result of Ref. [12] from \( m = 3 \) to \( m = 2 \). More precisely, we show that if the output probability distribution of the DQC1\textsubscript{2} model can be classically efficiently sampled (in the same sense as Refs. [12, 15, 16]), then the polynomial hierarchy collapses at the third level. We also show that a similar result can be obtained for the DQC2\textsubscript{m} model. To show these results, we no longer use the postselection technique of Refs. [12, 13, 17]. Instead, we consider the complexity class SBQP (Small Bounded error Quantum Polynomial time) [19]. As we will see, the proof with SBQP does not require any postselection qubit, which solves the problem of the “shortage of postselected qubits”.

PH, SBP, SBQP.— Before giving our results, let us review some complexity classes we will use in this paper (for details see Ref. [20]). The polynomial hierarchy is an infinite hierarchy of classes, defined by \( \Delta^p_0 = \Sigma^p_0 = \Pi^p_0 = P \), \( \Delta^p_1 = P^{\Sigma^p_0} \), \( \Sigma^p_{i+1} = NP^{\Delta^p_i} \), and \( \Pi^p_{i+1} = co-NP^{\Sigma^p_i} \). The union of all classes in the polynomial hierarchy is denoted by PH. It is known that PH \( \subseteq P^{PP} \subseteq NP^{PP} \subseteq \mathsf{NP}_{co-C_P} \mathsf{P}^{\mathsf{P}} \) \[21, 22\], where \( C_{-P} \) is one of the so-called counting complexity classes such as PP, and \( co-C_{-P} \) is known to be equal to a quantum analog of NP, called NQP \[23\].

SBP \[24\] is defined as follows: a language \( L \) is in SBP if there exist a uniform family of classical polynomial-size circuits and a polynomial \( q(n) \) such that

1. if \( w \in L \) then \( P(o = 1) \geq 2^{-q(n)} \),

2. if \( w \notin L \) then \( P(o = 1) \leq 2^{-q(n)-1} \),

where \( P(o = 1) \) is the probability that the output bit \( o \) takes 1. Note that we can take \( c_2\cdot 2^{-q(n)} \) and \( c'2^{-q(n)} \) with two constants \( c \) and \( c' \) satisfying \( 0 < c' < c \leq 1 \) instead of \( 2^{-q(n)} \) and \( 2^{-q(n)-1} \) without changing the power of SBP. The quantum analog of SBP, SBQP \[19\], is defined in the same way by replacing the classical circuit with quantum one. It is known that \( co-C_{-P} \subseteq A_{0}PP = \mathsf{SBQP} \) \[19, 23\], and \( \mathsf{SBP} \subseteq AM \subseteq \Pi^p_2 \) \[24\].

Definition of the classical simulability.— As the definition of the classical simulability, we adopt the one used in Refs. [12, 15, 16]. For any uniform family of circuits \( \{C_w\} \) \[26\], let \( P_w \) be the output probability distribution of \( C_w \). Let us assume that we perform computational-basis measurements on \( m \) output qubits of each circuit in the family. Let \( P_w(x_1, ..., x_m) \) be the probability of obtaining the measurement result \( (x_1, ..., x_m) \in \{0, 1\}^m \). We say that the family is weakly simulable with the error \( \epsilon \geq 0 \) if there exists a family of probability distributions \( \{P'_w\} \) such that it can be sampled classically in polynomial time and for any \( w \) and \( x_1, ..., x_m \) we have \[27\]

\[|P_w(x_1, ..., x_m) - P'_w(x_1, ..., x_m)| \leq \epsilon P_w(x_1, ..., x_m).\]

Result for DQC1\textsubscript{2}.— We now show that if the output probability distribution of the DQC1\textsubscript{2} model can be weakly simulable with \( 0 \leq \epsilon < \frac{1}{4} \), then SBQP \( \subseteq \mathsf{SBP} \). From this result, we obtain

\[PH \subseteq \mathsf{NP}_{co-C_{-P}} \subseteq \mathsf{NP}_{SBQP} \subseteq \mathsf{NP}_{SBP} \subseteq \mathsf{NP}_{P^P} = \Sigma^p_3,\]

which means the collapse of the polynomial hierarchy at the third level. Note that, since \( PH = co-PH \), we also obtain \( PH \subseteq \Pi^p_3 \). Therefore, more precisely, we obtain is

\[PH \subseteq \Sigma^p_3 \cap \Pi^p_3.\]

In order to show our claim, let us assume that a language \( L \) is in SBP. This means that there exist a uniform family of polynomial-size quantum circuits \( \{V_w\} \) and a polynomial \( q(n) \) such that
1. if \( w \in L \) then \( P_{SBQP}(o = 1) \geq 2^{-q(n)} \), and
2. if \( w \notin L \) then \( P_{SBQP}(o = 1) \leq 2^{-q(n)-1} \),

where \( P_{SBQP}(o = 1) \) is the probability that the output bit \( o \) takes 1. From \( V_w \), we construct the DQC1\(_2\) circuit of Fig. 3(a), whose output probability distribution \( P_{DQC12} \) satisfies

1. if \( w \in L \), then
\[
P_{DQC12}(o = 1, p = 1) = P_{DQC12}(o = 1|p = 1) \times P_{DQC12}(p = 1) \geq 2^{-q(n)-n},
\]
2. if \( w \notin L \), then
\[
P_{DQC12}(o = 1, p = 1) = P_{DQC12}(o = 1|p = 1) \times P_{DQC12}(p = 1) \leq 2^{-q(n)-1-n}.
\]

Let us assume that the output probability distribution of the DQC2 model can be weakly simulable with \( 0 \leq \epsilon < \frac{1}{3} \). Let \( P' \) be the output probability distribution of the classical simulator. Then we obtain

1. if \( w \in L \), then
\[
P'(o = 1) \geq (1 - \epsilon)P_{DQC2}(o = 1) \geq (1 - \epsilon)2^{-q(n)-n},
\]
2. if \( w \notin L \), then
\[
P'(o = 1) \leq (1 + \epsilon)P_{DQC2}(o = 1) \leq (1 + \epsilon)2^{-q(n)-1-n}.
\]

Since \( 0 \leq \epsilon < \frac{1}{3} \), \( L \) is in SBP [23]. Therefore, SBQP \( \subseteq \) SBP.

Result for DQC2\(_1\).— We can also show that if the DQC2\(_1\) model is weakly simulable with \( 0 \leq \epsilon < \frac{1}{3} \), then the polynomial hierarchy collapses at the third level.

In order to show it, let us assume that a language \( L \) is in SBP. Then there exist a uniform family of polynomial-size quantum circuits \( \{V_w\} \) and a polynomial \( q(n) \) such that

\[
1. if \ w \in L \ then \ P_{SBQP}(o = 1) \geq 2^{-q(n)},
2. if \ w \notin L \ then \ P_{SBQP}(o = 1) \leq 2^{-q(n)-1},
\]

where \( P_{SBQP}(o = 1) \) is the probability that the output bit \( o \) takes 1. From \( V_w \), we construct the DQC2\(_1\) circuit of Fig. 3(b). The output probability distribution \( P_{DQC21} \) of the circuit satisfies
\[
P_{DQC21}(o = 1) = P_{SBQP}(o = 1)2^{-n}.
\]

Let us assume that the output probability distribution of the DQC2\(_1\) model can be weakly simulable with \( 0 \leq \epsilon < \frac{1}{3} \). Let \( P' \) be the output probability distribution of the classical simulator. Then we obtain

1. if \( w \in L \), then
\[
P'(o = 1) \geq (1 - \epsilon)P_{DQC21}(o = 1) \leq (1 - \epsilon)2^{-q(n)-n},
\]
2. if \( w \notin L \), then
\[
P'(o = 1) \leq (1 + \epsilon)P_{DQC21}(o = 1) \leq (1 + \epsilon)2^{-q(n)-1-n}.
\]

Discussion.— In this paper, we have shown that the classical simulability of the DQC1\(_2\) or DQC2\(_1\) model leads to the collapse of the polynomial hierarchy at the third level.

For models where many qubits can be postselected, such as the IQP model [16], the depth-four model [15], or the DQC\(_k\) model with \( m \geq 3 \), the hardness of the classical simulation can be shown by deriving equivalences between the postselected versions of them and postBQP. However, for the DQC1\(_m\) model with \( m \leq 2 \), we cannot use that technique, since at most one qubit can be postselected. The idea of this paper which has solved the problem is to give up the postselection technique, and to use SBQP. Since a proof with SBQP does not need any postselection qubit, it is very useful when the number of output qubits is limited. For example, let us consider the model of universal quantum computing where an amplitude damping channel is applied on the output single qubit immediately before the measurement of it. With an argument similar to that of this paper, we can show that classical simulability of the model leads to the collapse of the polynomial hierarchy at the third level [29]. However, we do not know how to show it by using the postselection technique. In this way, a proof with SBQP proposed in this paper will be a strong tool for further study of border between quantum and classical superseding the postselection technique.

A result of Ref. [15], which shows that the classical simulability of the depth-four model leads to BQP \( \subseteq \) AM,
can be improved to the collapse of the polynomial hierarchy at the third level by using a proof with SBQP similar to that of this paper. However, for the depth-four model, there is a more direct proof without using SBQP: non-adaptive measurement-based quantum computing can be done in the depth four. Therefore, the DQC1 model and DQC2 model are the first examples where the utilization of SBQP is essential.

Finally, there are two challenging open problems: First, show the hardness of a classical simulation for not a sampling but a decision problem. Second, use not a multiplicative error approximation but a more experimentalist-friendly definition of approximation.

TM is supported by the Tenure Track System by MEXT Japan, and KAKENHI 26730003. HN is supported by KAKENHI 24106009, 24240001, and 25330012. KF is supported by JSPS Grant-in-Aid for Research Activity start-up 25587034.

Appendix.— We here show that if the output probability distribution of the DQC1 model is weakly simulable with $0 < \epsilon < \frac{1}{3}$, then BQP $\subseteq \Delta^P_3$.

A language $L$ is in the class post$X_\delta$ if and only if there exist an error tolerance $0 < \delta < \frac{1}{3}$ and a uniform family of postselected circuits (in the type specified by $X$, such as BQP, BQP, and DQC$k_m$) with a specified single output register $o$ (for the $L$-membership decision problem) and a specified “postselection register” $p$ such that:

1. if $w \in L$ then $P(o = 1 | p = 1) \geq \frac{1}{2} + \delta$, and
2. if $w \notin L$ then $P(o = 1 | p = 1) \leq \frac{1}{2} - \delta$.

(Note that the postselection register can be a multi-(qu)bit register for certain $X$.) For postBQP, the specification $X$ is the set of universal quantum circuits starting with $|0\rangle^{\otimes n}$. Similarly, for postBQP, it is the set of randomised classical circuits, and for postDQC$k_m$, it is the set of DQC$k_m$ circuits. Note that some classes, such as postBQP and postDQC$k_m$ ($m \geq 3$), are robust for $\delta$, and therefore we do not need to explicitly write $\epsilon$. It is known that postBQP $\equiv$ postDQC$k_m$ and postBQP $\subseteq \Delta^P_2$.

First, we show BQP $\subseteq$ postDQC$1,\delta$ for any $0 < \delta < \frac{1}{2}$. Let us assume that a language $L$ is in BQP. This means that there exists a uniform family of BQP circuits $\{V_w\}$ such that

1. if $w \in L$ then $P_{BQP}(o = 1) \geq \frac{1}{2} + \delta$, and
2. if $w \notin L$ then $P_{BQP}(o = 1) \leq \frac{1}{2} - \delta$,

where $P_{BQP}(o = 1)$ is the probability that the BQP circuit outputs $o = 1$. From $V_w$, we construct the postselected DQC1 circuit of Fig. 3(a). The measurement result of the second register (denoted by $o$ in Fig. 3(a)) behaves as

1. if $w \in L$ then $P_{DQC12}(o = 1 | p = 1) \geq \frac{1}{2} + \delta$,
2. if $w \notin L$ then $P_{DQC12}(o = 1 | p = 1) \leq \frac{1}{2} - \delta$,

where $P_{DQC12}(o = 1 | p = 1)$ is the conditional probability that the circuit of Fig. 3(a) outputs $o = 1$ given $p = 1$. Therefore, $L$ is in postDQC$1,\delta$.

Second, we show that if the DQC1 model can be weakly simulable with $0 \leq \epsilon < \frac{\delta}{1+\delta}$, then postDQC$1,\delta$ $\subseteq$ postBQP. Let us assume that $L$ is in postDQC$1,\delta$. Then, there exists a uniform family of postselected DQC1 circuits such that

1. if $w \in L$ then $P_{DQC12}(o = 1 | p = 1) \geq \frac{1}{2} + \delta$,
2. if $w \notin L$ then $P_{DQC12}(o = 1 | p = 1) \leq \frac{1}{2} - \delta$,

where $P_{DQC12}$ is the output probability distribution of the postselected DQC1 circuit. Let $P'$ be the output probability distribution of the classical simulator. Then we obtain

1. if $w \in L$ then $P'(o = 1 | p = 1) \geq \frac{1}{2} + \delta$,
2. if $w \notin L$ then $P'(o = 1 | p = 1) \leq \frac{1}{2} - \delta$.

Hence if $\epsilon < \frac{\delta}{1+\delta}$, $L$ is in postBQP.

Finally, by combining all results, we obtain that if the DQC1 model can be weakly simulable with $0 \leq \epsilon < \frac{\delta}{1+\delta}$, then BQP $\subseteq$ postDQC$1,\delta$ $\subseteq$ postBQP $\subseteq \Delta^P_2$. Since $\frac{\delta}{1+\delta} < \frac{1}{2}$ for $0 < \delta < \frac{1}{2}$, $\epsilon < \frac{1}{3}$ is the upper bound.

---

* Electronic address: morimae@gunma-u.ac.jp
† Electronic address: hnishimura@is.nagoya-u.ac.jp
‡ Electronic address: keisuke.fujii@i.kyoto-u.ac.jp
Electronic address: tamate.sh@gmail.com

[1] E. Knill and R. Laflamme, Phys. Rev. Lett. 81, 5672 (1998).
[2] A. Ambainis, L. J. Schulman, and U. V. Vazirani, Proc. of the 32nd ACM Symposium on Theory of Computing (STOC 2000).
[3] D. Poulin, R. Laflamme, G. J. Milburn, and J. P. Paz, Phys. Rev. A 68, 022302 (2003).
[4] D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Ol- livier, Phys. Rev. Lett. 92, 177906 (2004).
[5] P. W. Shor and S. P. Jordan, Quant. Inf. Comput. 8, 681 (2008).
[6] G. Passante, O. Moussa, C. A. Ryan, and R. Laflamme, Phys. Rev. Lett. 103, 250501 (2009).
[7] S. P. Jordan and P. Wocjan, Quant. Inf. Comput. 9, 264 (2009).
[8] S. P. Jordan and G. Alagic, Proc. of the Sixth Conference on Theory of Quantum Computation, Communication and Cryptography (TQC 2011).
[9] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A 72, 042316 (2005).
[10] A. Datta, A. Shaji and C. M. Caves, Phys. Rev. Lett. 100, 050502 (2008).
[11] A. Datta and G. Vidal, Phys. Rev. A 75, 042310 (2007).
[12] T. Morimae, K. Fujii, and J. F. Fitzsimons, Phys. Rev. Lett. 112, 130502 (2014).
[13] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, Phys. Rev. A 52, 3457 (1995).
[14] S. Aaronson, Proc. R. Soc. A 461, 3437-3483 (2005).
[15] B. Terhal and D. DiVincenzo, Quant. Inf. Comput. 4, 134 (2004).
[16] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. R. Soc. A 467, 2126 (2011).
[17] S. Aaronson and A. Arkhipov, Theory of Computing 9, 143 (2013).
[18] S. Aaronson, Proc. of the 42nd ACM Symposium on Theory of Computing (STOC 2010).
[19] G. Kuperberg, arXiv:0908.0512.
[20] For definitions of complexity classes, see https://complexityzoo.uwaterloo.ca/Complexity_Zoo, and references cited therein.
[21] S. Toda, SIAM J. Comput. 20, 865 (1991).
[22] J. Toran, J. ACM 38, 753 (1991).
[23] S. Fenner, F. Green, S. Homer, and R. Pruim, Proc. Roy. Soc. A 455, 3953 (1999).
[24] E. Böhler, C. Glaßer, D. Meister, J. Comput. System Sci. 72, 1043 (2006).
[25] M. Vyalyi, ECCC TR03-021 (2003).
[26] As in the standard circuit computing, we consider a uniform family of circuits in order to avoid any “hard wiring” of hard computing. In particular, as in Ref. [16], we consider a mapping \( w \rightarrow C_w \), where \( w \) is a bit string of length \( n \), \( C_w \) is a classical description of a circuit, and the mapping is computable in classical \( \text{poly}(n) \) time. The description \( C_w \) includes a specification of a sequence of gates and lines upon which they act, a specification of the inputs for all lines, and a specification of output registers and other registers such as the postselected ones.
[27] Note that this definition is essentially equivalent to the definition \( \frac{1}{c}P \leq P' \leq cP \) of Ref. [12, 16]. If we adopt this version, our results hold for \( c < \sqrt{2} \) instead of \( \epsilon < \frac{1}{3} \).
[28] Regard the event \((o = 1, p = 1)\) as the event of \( o = 1 \) in the definition of SBP.
[29] We first show that (1) the model can simulate SBQP. Then, we can show that (2) if this model can be classically sampled, \( \text{SBQP} \subseteq \text{SBP} \). This argument should be able to applied to many other models by replacing “the model” of (1) with another one.
[30] Y. Han, L. Hemaspaandra, and T. Thierauf, SIAM J. Comput. 26, 59 (1997).