Hardness of Classically Simulating the One-Clean-Qubit Model

Tomoyuki Morimae,[1,*] Keisuke Fujii,[2,3,†] and Joseph F. Fitzsimons[4,5,‡]
[1]*ASRLD Unit, Gunma University, 1-5-1 Tenjin-cho Kiryu-shi Gunma-ken, 376-0052, Japan*
[2]*The Hakubi Center for Advanced Research, Kyoto University, Yoshida-Ushinomiya-cho, Sakyo-ku, Kyoto 606-8302, Japan*
[3]*Graduate School of Informatics, Kyoto University, Yoshida Honmachi, Sakyo-ku, Kyoto 606-8501, Japan*
[4]*Singapore University of Technology and Design, 20 Dover Drive, 138682, Singapore*
[5]*Center for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, 117543, Singapore*

(Received 20 January 2014; published 2 April 2014)

Deterministic quantum computation with one quantum bit (DQC1) [E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998)] is a model of quantum computing where the input is restricted to containing a single qubit in a pure state and has all other qubits in a completely mixed state. Only the single pure qubit is measured at the end of the computation. While it is known that DQC1 can efficiently solve several problems for which no known classical efficient algorithms exist, the question of whether DQC1 is really more powerful than classical computation remains open. In this Letter, we introduce a slightly modified version of DQC1, which we call $\mathbf{DQC1}_{\boldsymbol{k}}$, where $\boldsymbol{k}$ output qubits are measured, and show that $\mathbf{DQC1}_{\boldsymbol{k}}$ cannot be classically efficiently simulated for any $\boldsymbol{k} \geq 3$ unless the polynomial hierarchy collapses at the third level.

DOI: 10.1103/PhysRevLett.112.130502 PACS numbers: 03.67.Ac, 89.70.Eg

While large scale universal quantum computers may be many years off, several intermediate models of quantum computation have been discovered which may prove significantly easier to implement in practice. These intermediate models of computation do not offer the full potential of universal quantum computation, but are, nonetheless, believed to be hard to simulate classically. Motivated by nuclear magnetic resonance (NMR) quantum information processing, Knill and Laflamme [1] proposed a restricted model of quantum computing, known as deterministic quantum computation with one quantum bit (DQC1), or the one clean qubit model. As is shown in Fig. 1(a), a DQC1 circuit consists of the input state in a highly mixed state which is acted upon by a number of quantum gates polynomial in the size of the input, followed by a computational basis measurement of the first qubit. The initial state of the system is given by $\rho_{\text{in}}^{(n+1)} \equiv |0\rangle\langle 0| \otimes (I/2)^{\otimes n}$ where I is the two-dimensional identity operator. We call this state "the highly mixed input state." Naively, one might expect this model to be easy to simulate classically, since any time evolution of a single qubit state can be trivially simulated efficiently by a classical computer, and the completely mixed state seems to lack "quantumness," due to a lack of entanglement and discord. However, the surprising result of Ref. [1] is that DQC1 can efficiently solve certain problems for which no efficient classical algorithms are known. For example, the quantum circuit represented in Fig. 1(b) can be used to estimate the normalized trace of any n-qubit unitary operator U [1], a problem which is complete for the class of decision problems answerable within this model with bounded error [2]. This is possible due, in part, to the fact that, while entanglement remains bounded in DQC1 circuits, the interaction between the mixed register and the pure qubit leads to the presence of significant nonclassical correlations [3,4].

While it does not seem that this model supports universal quantum computation [5], it can efficiently solve problems for which no efficient classical algorithm is known, such as spectral density estimation [1], testing integrability [6], calculation of fidelity decay [7], and approximation of the Jones and HOMFLY polynomials [8–10]. An algorithm for approximating an invariant of three-manifolds was also proposed [11]. Since the estimation of the normalized trace of a unitary matrix seems to be hard for classical computers [12], and DQC1 does not seem to be universal, the DQC1 model appears to represent a model of computation which is intermediate classical and universal quantum computation.

Although the presence of nontrivial quantum discord and entanglement within DQC1 circuits is seen as an indication that the trace of n-qubit unitary matrix is classically hard to compute [3,12], ruling out many classical approaches to simulation [4], it is an open problem whether DQC1 really

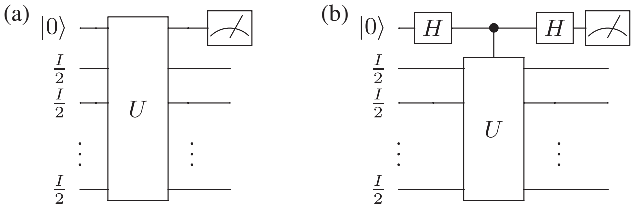

FIG. 1. The one clean qubit model. (a) A circuit of the DQC1 model, (b) a circuit of the DQC1 model whose output can evaluate $\mathrm{Tr}(U)$, for which classical efficient algorithm is not known. All measurements are assumed to be in the computational basis.

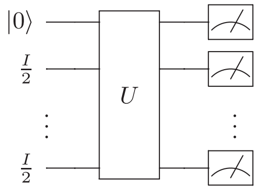

FIG. 2. A circuit of the DQC1$_{n+1}$.

represents a more powerful model than purely classical computation. In this Letter, we show that a slightly modified version of DQC1, which we call DQC1$_{n+1}$, is hard to be classically efficiently simulated unless the polynomial hierarchy (PH) collapses at the third level. The DQC1$_{n+1}$ model is equivalent to the DQC1 model except that all $n+1$ output qubits (instead of the single qubit) are measured at the end of the computation (see Fig. 2). We shall show that this result hardness holds even if we consider measurements on only a constant number of output qubits. Thus, we demonstrate an inextricable link between the computational hardness of simulating circuits with one clean qubit and a widely accepted conjecture from computational complexity theory. PH is a natural way of classifying the complexity of problems (languages) beyond the usual NP (nondeterministic polynomial time, which includes "traveling salesman" and "satisfiability" problems). It is strongly believed in computer science that NP includes nonpolynomial-time problems. Similarly, there is a weaker, but still solid belief that PH does not collapse.

Our argument is based on the seminal results by Terhal and DiVincenzo [13], Bremner, Jozsa, and Shepherd [14], and Aaronson and Arkhipov [15]. These papers introduced models of quantum computing that are not universal but cannot be classically efficiently simulated unless some plausible assumptions in computer science are violated. The essential idea behind all of these results is that, when postselected, some superficially naive circuits can simulate universal bounded error quantum polynomial time computation (BQP) or postselected universal bounded error quantum polynomial time computation (post-BQP). In this context, postselection means the (fictitious) ability to project onto a specific branch of the wave function with unit probability. Therefore, if the probability distributions of the outputs of such naive circuits can be classically efficiently simulated, this means that the classical computer with a postselection can also efficiently simulate BQP or post-BQP circuits, which violate certain strongly believed conjectures in computer science.

Using such an approach, Terhal and DiVincenzo [13] showed that it is hard to simulate quantum circuits with depth four. They derived the result by noticing the fact that nonadaptive Gottesman-Chuang quantum circuits [16] can be written with depth-four circuits. Bremner, Jozsa, and Shepherd [14] showed that a class of quantum circuits known as instantaneous quantum polynomial-time (IQP) circuits [17] cannot be classically efficiently simulated unless PH collapses at the third level. An n-qubit IQP circuit is a circuit that consists of the input state $|0\rangle^{\otimes n}$, a polynomial number of mutually commuting quantum gates, and computational-basis measurement on all n output qubits at the end of the computation. Each of the quantum gates in this model can be assumed to be of the form $D(\theta_j, S_j) \equiv \exp[i\theta_j \otimes_{k=1}^{n} X_k^{s_j^k}]$, where $\theta_j \in \mathbb{R}$, X_k is the Pauli X operator acting on the kth qubit, and $S_j \equiv (s_j^1, \ldots, s_j^n) \in \{0,1\}^n$. What Bremner, Jozsa, and Shepherd showed was that postselected IQP circuits can simulate post-BQP circuits. By combining this with a previous result of Aaronson [18], that post-BQP $=$ PP (probabilistic polynomial time), they concluded that if IQP circuits can be classically efficiently simulated, PH collapses at the third level. Finally, Aaronson and Arkhipov [15] showed a hardness proof for classical simulations given of noninteracting bosons [19] which made use of probabilistic entangling gates due to Knill, Laflamme, and Milburn [20], to show that such systems can simulate BQP circuits, and, hence, post-BQP circuits, if the postselection is possible on the occupancy of modes [21].

Here, we make use of a similar approach. We show that if postselections of the measurement results are possible, DQC1$_{n+1}$ can simulate post-BQP circuits. Then, by using the fact that post-BQP $=$ PP, we conclude that if DQC1$_{n+1}$ can be efficiently classically simulated, the polynomial hierarchy collapses at the third level.

Before proceeding to the proof of our results, we first clarify what we mean by classically efficient simulation. We adopt the definition used by Bremner, Jozsa, and Shepherd [14]. (They call the definition "weakly" simulatable with multiplicative error $c \geq 1$. But, in this Letter, we sometimes omit the word "weakly" for simplicity, since we consider only this definition.) For any uniform family of circuits $\{C_w\}$ [22], let P_w be the output probability distribution of C_w. Let us assume that we perform computational-basis measurements on the k output qubits of each of a uniform family of quantum circuits. Let $P_w(m_1, \ldots, m_k)$ be the probability of obtaining measurement result $(m_1, \ldots, m_k) \in \{0,1\}^k$. We say that the family is (weakly) simulatable with multiplicative error $c \geq 1$ if, for any marginal distribution $P_w(x_1, \ldots, x_r)$ of $P_w(m_1, \ldots, m_k)$, there exists a (family of) probability distributions P'_w such that it can be sampled classically in a polynomial time, and for all variables and w we have

$$\frac{1}{c} P_w(x_1, \ldots, x_r) \leq P'_w(x_1, \ldots, x_r) \leq c P_w(x_1, \ldots, x_r).$$

(Note that the circuit size is included in the input complexity.)

We now give a more precise definition of our model. A DQC1$_k$ circuit consists of the highly mixed input state $\rho_{\text{in}}^{(n+1)}$, to which a polynomial number of quantum gates chosen from a discrete approximately universal gate set are applied, followed by measurement of k labeled qubits in the computational basis. Clearly, then, DQC1 is equivalent to the special case of $k = 1$. At the opposite extreme, as is shown in Fig. 2, the DQC1_{n+1} model is equivalent to the DQC1 model except that all output qubits are measured at the end of the computation.

With this definition in place, we can now make a precise statement of our main result: if DQC1_{n+1} is classically simulatable with multiplicative error $1 \leq c < \sqrt{2}$, then PH collapses at the third level. Further, this result can be refined to show that the same result holds if DQC1_{n+1} is replaced by DQC1_3.

In order to prove these claims, we begin by clarifying the definition of postselected computation classes [14]. A language L is in the class post-X if and only if there exists an error tolerance $0 < \delta < \frac{1}{2}$ and a uniform family of postselected circuits (in the type specified by X, such as BQP, IQP, etc.) with a specified single (qu)bit output register O_w (for the L-membership decision problem) and a specified multi(qu)bit "postselection register" P_w [23] such that: (1) if $w \in L$, then $\mathrm{Prob}(O_w = 1|P_w = 0\ldots0) \geq \frac{1}{2} + \delta$, and (2) if $w \notin L$, then $\mathrm{Prob}(O_w = 1|P_w = 0\ldots0) \leq \frac{1}{2} - \delta$. For post-BQP, the specification X is the set of universal quantum circuits starting with input fixed as $|0\rangle^{\otimes n}$. Similarly, for a postselected universal bounded error probabilistic polynomial time computation (post-BPP), it is the set of randomized classical circuits with input fixed in the zero state, and for post-DQC1_k, it is the set of DQC1_k circuits, i.e., the highly mixed input state $\rho_{\mathrm{in}}^{(n+1)}$, a polynomial number of quantum gates on it, and the measurement of k labeled qubits in the computational basis.

As discussed earlier, it has previously been established that post-BQP = PP [18]. Furthermore, a nontrivial containment for post-BPP is known. Let PH denote the polynomial hierarchy: the union of an infinite hierarchy of classes Σ_kP, Δ_kP, and Π_kP for $(k = 0, 1, 2, \ldots)$ where $\Sigma_0\mathrm{P} = \Delta_0\mathrm{P} = \Pi_0\mathrm{P} = \mathrm{P}$ and $\Sigma_{k+1} = \mathrm{NP}^{\Sigma_k\mathrm{P}}$, $\Delta_{k+1}\mathrm{P} = \mathrm{P}^{\Sigma_k\mathrm{P}}$, and $\Pi_{k+1} = \text{co-NP}^{\Sigma_k\mathrm{P}}$. It is known that $\mathrm{P}^{\text{post-BPP}} \subseteq \Delta_3\mathrm{P}$ [14], and $\mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$ [24].

We now proceed to show that post-DQC1_{n+1} = post-BQP. First, post-DQC$1_k \subseteq$post-BQP is easy to show for any k since the mixed-state input can be simulated with BQP circuits by adding ancilla qubits and entangling them with qubits used in the computation, to leave the reduced system in the same mixed state as used for DQC1_k. Hence, post-DQC$1_{n+1} \subseteq$post-BQP. Next, we show the opposite containment, post-DQC$1_{n+1} \supseteq$post-BQP. Let us consider an n-qubit cluster state $|G\rangle$, which is a universal resource state for the measurement-based quantum computing [25]. Consider the DQC1_{n+1} circuit (shown in Fig. 3) with the gate $(I \otimes \otimes_{j=1}^{n} V_j)W$, where V_j is any single-qubit unitary gate, and $W \equiv X \otimes |G\rangle\langle G| + I \otimes (I^{\otimes n} - |G\rangle\langle G|)$. The unitary operator W can be uniformly generated since the m-controlled Toffoli gate, $|0\rangle\langle 0|^{\otimes m} \otimes X + (I^{\otimes m} - |0\rangle\langle 0|^{\otimes m}) \otimes I$, can be uniformly generated without requiring any ancilla qubits [26], and a unitary transformation that takes $|0\ldots0\rangle$ to a cluster state can be uniformly generated without requiring any ancilla qubits. The state after the application of W is $\frac{1}{2^n}|1\rangle\langle 1| \otimes |G\rangle\langle G| + \frac{1}{2^n}|0\rangle\langle 0| \otimes (I^{\otimes n} - |G\rangle\langle G|)$.

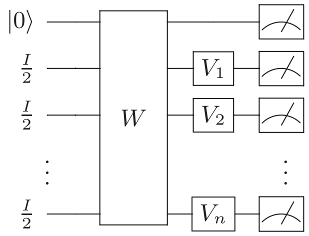

FIG. 3. A circuit of the DQC1_{n+1} model which implements postselected measurement based quantum computation.

Therefore, if we postselect on the first qubit being in state $|1\rangle$, we obtain the n-qubit cluster state $|G\rangle$. Generally, measurement based computation requires that adaptive single qubit measurements be made based on previous measurement outcomes in order to achieve deterministic quantum computation. However, since we are allowing for postselection, by postselecting measurement outcomes on one for nonoutput qubits, it is possible to fix the measurement bases before beginning the computation, and hence, postselection combined with the circuit in Fig. 3 is sufficient to implement postselected BQP circuits with only polynomial overhead, and so post-DQC$1_{n+1} \supseteq$ post-BQP.

Finally, we show that the classical simulatability of DQC1_{n+1} leads to post-DQC$1_{n+1} \subseteq$post-BPP, following the argument of Bremner, Jozsa, and Shepherd. Assume that DQC1_{n+1} is simulatable with multiplicative error $c \geq 1$. Let (O_w, P_w) and (O'_w, P'_w) denote the output and postselection registers for postselected DQC1_{n+1} circuits and postselected randomized classical circuits, respectively. Then,

$$\mathrm{Prob}(O'_w = x|P'_w = 0\ldots0) = \frac{\mathrm{Prob}(O'_w = x, P'_w = 0\ldots0)}{\mathrm{Prob}(P'_w = 0\ldots0)} \geq \frac{1}{c^2}\mathrm{Prob}(O_w = x|P_w = 0\ldots0),$$

and

$$\mathrm{Prob}(O'_w = x|P'_w = 0\ldots0) = \frac{\mathrm{Prob}(O'_w = x, P'_w = 0\ldots0)}{\mathrm{Prob}(P'_w = 0\ldots0)} \leq c^2\mathrm{Prob}(O_w = x|P_w = 0\ldots0).$$

Let us assume that a language L is in post-DQC1_{n+1}. Then, (1) if $w \in L$, then $\mathrm{Prob}(O'_w = 1|P'_w = 0\ldots0) \geq \frac{1}{c^2}(\frac{1}{2} + \delta)$, (2) if $w \notin L$, then $\mathrm{Prob}(O'_w = 1|P'_w = 0\ldots0) \leq c^2(\frac{1}{2} - \delta)$. If $c < \sqrt{2}$, L is necessarily in post-BPP. (Note that it is assumed that δ can be made arbitrarily close to $1/2$. It is proved by noticing the equivalence between post-DQC1_{n+1} and post-BQP, and the coherent amplification of BQP acceptance probabilities). This would imply that post-DQC$1_{n+1}$$\subseteq$post-BPP, and hence, $\Delta_3\mathrm{P}\supseteq\mathrm{P}^{\text{post-BPP}} = \mathrm{P}^{\mathrm{PP}}\supseteq\mathrm{PH}$, which shows the collapse of PH at the third level. Hence, we have shown that the classical simulatability of DQC1_{n+1} leads to the collapse of PH at the third level.

We now turn our attention to the case where measurements are available only on some constant number of output qubits. This more accurately reflects the situation in NMR experiments, as the DQC1 model was originally proposed to model. In order to show that post-BQP$\subseteq$post-DQC1_3, we consider the circuit shown in Fig. 4. Taking $W' = X \otimes |0\rangle\langle 0| \otimes |G\rangle\langle G| + I \otimes (I- |0\rangle\langle 0| \otimes |G\rangle\langle G|)$, the state after applying W' and selecting on the first qubit being in the state $|1\rangle$ is $|0\rangle \otimes |G\rangle$, which is the same as in the previous proof with the addition of an ancilla qubit initialized to $|0\rangle$. As before, the local unitaries $\{V_i\}$ are used to align the local measurements which drive the computation with the computational basis. However, rather than directly measure each nonoutput qubit, the multiply controlled Toffoli gate is used to compute the logical AND of these outcomes on the ancilla qubit. Thus, rather than postselecting on a particular string of outcomes, it suffices to postselect on the single ancilla bit in order to implement any postselected quantum circuit. Finally the output qubit must be measured in order to determine the result of the computation. Thus, only three measurements, with postselection on two of the output bits is necessary in order to implement postselected quantum circuits, and hence, post-BQP$\subseteq$post-DQC1_3. Following our previous argument, if DQC1_3 were classically simulatable with a multiplicative error less than $\sqrt{2}$, then post-BQP $=$ post-DQC$1_3$$\subseteq$post-BPP, and hence, PH would collapse at the third level.

In this Letter, we have shown that classical efficient simulation of DQC1_k for any $k \geq 3$ is impossible unless PH collapses at the third level. While we have derived this result using the measurement based model, we note that our results can also be recast in terms of the circuit model [27]. The ultimate goal is, of course, to show the impossibility of a classical efficient simulation of DQC1. However, there is a link between these two problems. Shor and Jordan [8] showed that the probability of obtaining the all zero string result for a DQCk_k circuit, where there are k pure qubits which can be measured, is equal to the probability of obtaining the zero result for a DQC1 circuit for trace estimation. Here, we have shown that DQC1_3 is hard to classically simulate, and the Shor-Jordan result seems to indicate that the output bit of DQC1 somehow "contains" the hard result of DQC1_3. While their result does not directly extend the postselection argument to DQC1 circuits with a single measurement, it does show a tantalizing link between the problems, and hence, we are lead to conjecture that the result we present here can be extended to DQC1 circuits with only a single measurement. Such a result would be a major step toward resolving the computational power of DQC1 circuits.

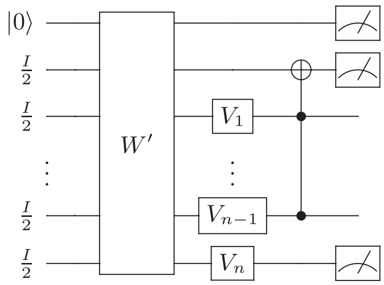

FIG. 4. A circuit of the DQC1_3 model which implements postselected measurement based quantum computation.

We also note here that the notion of approximate sampling used in the present Letter (which is also the one used in Refs. [14,15]) is artificially strong. The natural notion of classical simulation is to sample from a probability distribution of $1/\text{poly}$ total variation distance from the output distribution of the device being simulated. It is an important open problem to prove that classical samplings with that natural error bound for a one clean qubit model (or other models [14,15]) would violate some plausible computational complexity assumptions. Finally, we mention that due to the postselected nature of the proof technique, we still do not know of a nonpromise problem solvable in probabilistic polynomial time by DQC1_k and plausibly not in classical probabilistic polynomial time. Furthermore, it is not known whether the DQC1_k is fault tolerant, and it seems to be not.

We thank Michael Bremner, Animesh Datta, Oded Regev, Daniel Shepherd, and two anonymous referees for helpful comments on the manuscript. T. M. is supported by Tenure Track System by MEXT Japan. K. F. is supported by JSPS Grant-in-Aid for Research Activity Start-up Grant No. 25887034. J. F. F. is supported by the National Research Foundation and the Ministry of Education, Singapore. This material is based on research funded in part by the Singapore National Research Foundation under NRF Grant No. NRF-NRFF2013-01.

[*] morimae@gunma-u.ac.jp
[†] keisukejayorz@gmail.com
[‡] joseph_fitzsimons@sutd.edu.sg

[1] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[2] D. Shepherd, arXiv:quant-ph/0608132.
[3] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
[4] A. Datta and G. Vidal, Phys. Rev. A **75**, 042310 (2007).

[5] A. Ambainis, L. J. Schulman, and U. V. Vazirani, in *Proceedings of the Thirty Second Annual ACM Symposium on Theory of Computing : Portland, Oregon, 2000* (ACM Press, New York, 2000), p. 697.

[6] D. Poulin, R. Laflamme, G. J. Milburn, and J. P. Paz, Phys. Rev. A **68**, 022302 (2003).

[7] D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Ollivier, Phys. Rev. Lett. **92**, 177906 (2004).

[8] P. W. Shor and S. P. Jordan, Quantum Inf. Comput. **8**, 681 (2008).

[9] G. Passante, O. Moussa, C. A. Ryan, and R. Laflamme, Phys. Rev. Lett. **103**, 250501 (2009).

[10] S. P. Jordan and P. Wocjan, Quantum Inf. Comput. **9**, 264 (2009).

[11] S. P. Jordan and G. Alagic, arXiv:1105.5100.

[12] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).

[13] B. Terhal and D. DiVincenzo, Quantum Inf. Comput. **4**, 134 (2004).

[14] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. R. Soc. A **467**, 459 (2010).

[15] S. Aaronson and A. Arkhipov, Theory Comput. **9**, 143 (2013).

[16] D. Gottesman and I. L. Chuang, Nature (London) **402**, 390 (1999).

[17] K. Fujii and T. Morimae, arXiv:1311.2128.

[18] S. Aaronson, Proc. R. Soc. A **461**, 3473 (2005).

[19] S. Aaronson, Proc. R. Soc. A **467**, 3393 (2011).

[20] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).

[21] Aaronson and Arkhipov also gave a direct proof of the result without using the postselection argument [15].

[22] 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. [14], 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 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.

[23] While post-BQP and post-BPP are usually defined with only a two-dimensional output register, their power is not increased by changing the size of this register.

[24] S. Toda, SIAM J. Comput. **20**, 865 (1991).

[25] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).

[26] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).

[27] M. Bremner and D. Shepherd, and separately Oded Regev (private communication).