Efficient Classical Simulation of Clifford Circuits with Nonstabilizer Input States

Kaifeng Bu and Dax Enshan Koh

Phys. Rev. Lett. **123**, 170502 — Published 23 October 2019

DOI: 10.1103/PhysRevLett.123.170502

Efficient classical simulation of Clifford circuits with nonstabilizer input states

Kaifeng Bu[1,2,*] and Dax Enshan Koh[3,†]

[1] *School of Mathematical Sciences, Zhejiang University, Hangzhou, Zhejiang 310027, China*
[2] *Department of Physics, Harvard University, Cambridge, Massachusetts 02138, USA*
[3] *Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*

We investigate the problem of evaluating the output probabilities of Clifford circuits with nonstabilizer product input states. First, we consider the case when the input state is mixed, and give an efficient classical algorithm to approximate the output probabilities, with respect to the l_1 norm, of a large fraction of Clifford circuits. The running time of our algorithm decreases as the inputs become more mixed. Second, we consider the case when the input state is a pure nonstabilizer product state, and show that a similar efficient algorithm exists to approximate the output probabilities, when a suitable restriction is placed on the number of qubits measured. This restriction depends on a magic monotone that we call the Pauli rank. We apply our results to give an efficient output probability approximation algorithm for some restricted quantum computation models, such as Clifford circuits with solely magic state inputs (CM), Pauli-based computation (PBC) and instantaneous quantum polynomial time (IQP) circuits. Finally, we discuss the relationship between Pauli rank and stabilizer rank.

I. INTRODUCTION

One of the main motivations behind the field of quantum computation is the expectation that quantum computers can solve certain problems much faster than classical computers. This expectation has been driven by the discovery of quantum algorithms which can solve certain problems believed to be intractable on a classical computer. A famous example of such a quantum algorithm is due to Shor, whose eponymous algorithm can solve the factoring problem exponentially faster than the best classical algorithms we know today [1, 2].

With the advent of noisy intermediate-scale quantum (NISQ) devices [3], an important near-term milestone in the field is to demonstrate that quantum computers are capable of performing computational tasks that classical computers cannot, a goal known as *quantum supremacy* [4, 5]. Several restricted models of quantum computation have been proposed as candidates for demonstrating quantum supremacy. These include boson sampling [6], the one clean qubit model (DQC1) [7, 8], instantaneous quantum polynomial-time (IQP) circuits [9], Hadamard-classical circuits with one qubit (HC1Q) [10], Clifford circuits with magic initial states and nonadaptive measurements [11–13], the random circuit sampling model [14, 15], and conjugated Clifford circuits (CCC) [16]. These models are potentially good candidates for quantum supremacy because they can solve sampling problems that are conjectured to be intractable for classical computers, and are conceivably easier to implement in experimental settings.

In contrast to the above models, quantum circuits with Clifford gates and stabilizer input states are not a candidate for quantum supremacy, because they can be efficiently simulated on a classical computer using the Gottesman-Knill simulation algorithm [17]. The Gottesman-Knill algorithm, however, breaks down and efficient classical simulability can be proved to be impossible (under plausible assumptions) when Clifford circuits are modified in various ways, under various notions of simulation [11–13, 16]. For example, it can be proved under plausible complexity assumptions that no efficient classical sampling algorithm exists that can sample from the output distributions of Clifford circuits with general product state inputs when the number of measurements made is of order $O(n)$ [11].

In this paper, we present two new efficient classical algorithms for approximately evaluating the output probabilities of Clifford circuits with nonstabilizer inputs. Our first algorithm shows that the output distribution of Clifford circuits with mixed product states can be efficiently approximated, with respect to the l_1 norm, for a large fraction of Clifford circuits. This algorithm explicitly reveals the role of mixedness of the input states in affecting the running time of the simulation, which decreases as the inputs become more mixed.

Our second algorithm shows that such an efficient approximation algorithm still exists in the case where the inputs are pure nonstabilizer states, as long as we impose a suitable restriction on the number of measured qubits. This restriction depends on a magic monotone called the Pauli rank that we introduce in this paper. This algorithm also explicitly links the simulation time to the amount of magic in the input states, and implies that for Clifford circuits with magic input states, it is possible in certain cases to achieve an efficient classical approximation of the output probability even when $O(n)$ qubits are measured. Note that our results do not contradict the hardness results given in [11], which are about worst-case hardness, instead of average-case hardness. We also apply our results to give an efficient approximation algorithm for some restricted quantum computation models, like Clifford circuits with solely magic state inputs (CM), Pauli-based computation (PBC) and instantaneous quantum polynomial time (IQP) circuits. Finally, we discuss the relationship between Pauli rank and stabilizer rank.

II. MAIN RESULTS

Let P^n be the set of all Hermitian Pauli operators on n qubits, i.e., operators that can be written as the n-fold ten-

* kfbu@fas.harvard.edu
† daxkoh@mit.edu

sor product of the single-qubit Pauli operators $\{I,X,Y,Z\}$ with sign ± 1. The Clifford unitaries on n qubits are the unitaries that maps Pauli operators to Pauli operators, that is, $\mathcal{C}l_n = \{U \in U(2^n) : UPU^\dagger \in P^n, \forall P \in P^n\}$. Stabilizer states are pure states of the form $U|0\rangle^{\otimes n}$ [18], where U is some Clifford unitary.

Here, we consider Clifford circuits with product input states $|0\rangle\langle 0|^{\otimes n} \otimes_{i=1}^m \rho_i$, and measurements on k qubits. If either m or k is $O(\log n)$, the output probabilities can be efficiently simulated classically by the Gottesman-Knill theorem [11, 17]. However, if both m and k are greater than $O(\log n)$, we show that the output probability of such circuits can still be approximated efficiently with respect to the l_1 norm for a large fraction of Clifford circuits.

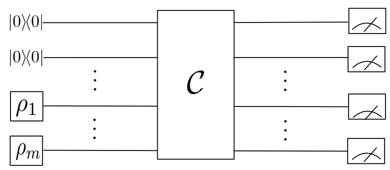

FIG. 1. A circuit diagram of Clifford circuits with product state inputs, which could be either pure or mixed.

A. Mixed input states

We first consider the case where all ρ_i are mixed states and give an efficient classical algorithm to approximate the output probabilities.

Theorem 1. *Consider the class of circuits on $n+m$ qubits with input state $|0\rangle\langle 0|^{\otimes n} \otimes_{i=1}^m \rho_i$, Clifford operation $\mathcal{C}$, and measurements on each qubit in the computational basis. Then for all $\alpha > 0$, there exists a classical algorithm that when given a circuit from the above class, approximates the output probabilities of the circuit up to l_1 norm δ in time $(n+m)^{O(1)} m^{O(\log(\sqrt{\alpha}/\delta)/\lambda)}$ for at least a $1-\frac{2}{\alpha}$ fraction of circuits $\mathcal{C}$, where the Clifford operation $\mathcal{C}$ is uniformly randomly chosen, and $\lambda = \min\{\lambda_i\}_i$, with $\lambda_i = 1-\sqrt{2\,\mathrm{Tr}\left[\rho_i^2\right]-1}$, is a measure of the mixedness of the input state ρ_i.*

The proof of the Theorem is presented in Section A of the Supplementary Material [19]. If the parameters α, δ and λ are constants, then the running time is polynomial in n. The theorem shows that the efficiency of this classical algorithm increases with the mixedness of the input states. Here we usually consider the case where $m \geq 1$. When $m = 0$, the corresponding circuit can be efficiently simulated by the Gottesman-Knill Theorem [17].

Next, we show that the result in Theorem 1 can be easily generalized to quantum circuits $\mathcal{C}$ which are slightly beyond Clifford circuits. To this end, we consider the Clifford hierarchy, a class of operations introduced by Gottesman and Chuang [20] that has important applications in fault-tolerant quantum computation and teleportation-based state injection. Let $\mathcal{C}l_n^{(3)}$ be the third level of the Clifford Hierarchy, i.e., $\mathcal{C}l_n^{(3)} = \{U \in U(2^n) : UPU^\dagger \in \mathcal{C}l_n, \forall P \in P^n\}$. There are several important gates in the third level of Clifford Hierarchy, such as the $\pi/8$ gate (which we denote T) and the CCZ gate [21]. (Note that the set $\mathcal{C}l_n^{(3)}$ is not closed under multiplication. For example, $TH, T \in \mathcal{C}l_n^{(3)}$, but $THT \notin \mathcal{C}l_n^{(3)}$.) The following corollary shows that adding gates in $\mathcal{C}l^{(3)}$ to the circuits in Theorem 1 does not change (up to polynomial overhead) the efficiency of the classical simulation.

Corollary 2. *Let $\mathcal{C} = \mathcal{C}_1 \circ V$ be a quantum circuit with input states $|0\rangle\langle 0|^{\otimes n} \otimes_{i=1}^m \rho_i$, where the gates in the circuit $\mathcal{C}_1$ are taken from the set of Clifford gates on $n+m$ qubits $\mathcal{C}l_{n+m}$ and V is taken from the third level of Clifford hierarchy $\mathcal{C}l_m^{(3)}$ acting on $n+1,\ldots,n+m$-th qubits. Assume that each qubit is measured in the computational basis. Then, Theorem 1 still holds if we replace $\mathcal{C}$ in Theorem 1 with $\mathcal{C}$ defined above.*

Here, the notation $A \circ B$, where A and B are circuits, refers to the circuit formed from applying the circuit B followed by the circuit A. The key property we use here is that the gates in the third level of the Clifford Hierarchy map Pauli operators to Clifford unitaries, which makes the proof of Theorem 1 still hold. (See a discussion of this in the Section A of the Supplementary Material [19].) Although $\mathcal{C}l_n^{(3)}$ is not a group, the diagonal gates in $\mathcal{C}l_n^{(3)}$, denoted as $\mathcal{C}l_{n,d}^{(3)}$, forms a group [21, 22]. Since the T gate and CCZ gate both belong to $\mathcal{C}l_{n,d}^{(3)}$, the result in Theorem 1 still holds for the quantum circuits $\mathcal{C} = \mathcal{C}_1 \circ \mathcal{C}_2$ where gates in $\mathcal{C}_1$ and $\mathcal{C}_2$ are chosen from $\mathcal{C}_{n+m}$ and $\mathcal{C}l_{m,d}^{(3)}$ respectively.

Since noise is inevitable in real physical experiments, it is important to consider the effects of noise in quantum computation. Recently, it has been demonstrated that if there is some noise on the random quantum gates [23] or measurements of IQP circuits [24], then there exists an efficient classical simulation of the output distribution of quantum circuits. In the rest of this subsection, we apply our results to two important subuniversal quantum circuits with noisy input states and give an efficient classical approximation algorithm for the output probabilities of the corresponding quantum circuits.

Example 1—First, we consider Clifford circuits with magic input states. It is well known that the Clifford + T gate set is universal for quantum computation. By magic state injection, circuits with this gate set can be efficiently simulated by Clifford circuits with magic state $|T\rangle$ inputs, where $|T\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$. It has been shown that $\mathsf{postCM} = \mathsf{postBQP}$ [13], and thus output probabilities are #P-hard approximate up to some constant relative error [25–27]. However, if there is some independent depolarizing error acting on each input magic state, e.g., the input state on each register is $(1-\varepsilon)|T\rangle\langle T| + \varepsilon\frac{I}{2}$, then Theorem 1 implies directly that there exists a classical algorithm to approximate the output probability up to l_1 norm δ in time $n^{O(\log(1/\delta)/\varepsilon)}$ for a large fraction of the CM circuits with noisy inputs.

Example 2—IQP circuits have a simple structure with input states $|0\rangle^{\otimes n}$ and gates of the form $H^{\otimes n} D H^{\otimes n}$, where the diagonal gates in D are chosen from the gate set $\{Z, S, T, CZ\}$. It has been shown that $\mathsf{postIQP} = \mathsf{postBQP}$ [9] and thus, the output probabilities are #P-hard to approximate up to some constant relative error [25–27]. Also, if there is some depolarizing noise acting on each input state $|0\rangle$, i.e., each input state is a mixed state $(1-\varepsilon)|0\rangle\langle 0|+\varepsilon\frac{I}{2}$, then if we follow a similar proof to that of Theorem 1, we find that there exists a classical algorithm to approximate the output probability up to l_1 norm δ in time $n^{O(\log(1/\delta)/\varepsilon)}$ for a large fraction of such IQP circuits. (The proof is presented in Section B of the Supplementary Material [19] in detail, which depends on the output distribution of IQP circuits in Section C of the Supplementary Material [19].)

B. Pure nonstabilizer input states

As we can see, the running time in Theorem 1 blows up if the input state ρ_i is pure. Here, we consider the case where all ρ_i are pure nonstabilizer states, that is Clifford gates with the input state $|0\rangle^{\otimes n}\otimes_{i=1}^m|\psi_i\rangle$.

For pure states $|\psi\rangle$, the stabilizer fidelity [28] is defined as follows

$$F(\psi)=\max_{|\phi\rangle}|\langle\phi|\psi\rangle|^2, \tag{1}$$

where the maximization is taken over all stabilizer states. Here, we define

$$\mu(\psi):=2(1-F(\psi)). \tag{2}$$

It is easy to see that $\mu(\psi)=0$ iff $|\psi\rangle$ is a stabilizer state. Thus, μ measures the amount of magic of a state. Since each $|\psi_i\rangle$ is not a stabilizer state, it follows that $\mu(\psi_i)>0$.

Next, let us introduce the Pauli rank for pure single qubit states $|\psi\rangle$. First, we write a pure state $|\psi\rangle$ in terms of its Bloch sphere representation $|\psi\rangle\langle\psi|=\frac{1}{2}\sum_{s,t\in\{0,1\}}\psi_{st}X^sZ^t$, where $\psi_{00}=1$ and $|\psi_{01}|^2+|\psi_{10}|^2+|\psi_{11}|^2=1$. We define the Pauli rank $\chi(\psi)$ to be the number of nonzero coefficients ψ_{st}. By the definition of Pauli rank, it is easy to see that $2\le\chi(\psi)\le 4$, and that $|\psi\rangle$ is a stabilizer state iff $\chi(\psi)=2$. Since each input state $|\psi_i\rangle$ is a nonstabilizer state, it follows that $\chi(\psi_i)=3$ or 4. For example, for the magic state $|T\rangle$, the corresponding Pauli rank $\chi=3$. For n-qubit systems, the Pauli rank serves as a good candidate for a magic monotone as it is easier to compute than other magic monotones which require a minimization over all stabilizer states [29–31]. (See a discussion of Pauli rank for n-qubit systems in Section D3 of the Supplementary Material [19].

Theorem 3. *Consider the class of circuits on $n+m$ qubits with input state $|0\rangle^{\otimes n}\otimes_{i=1}^m|\psi_i\rangle$, Clifford operation $\mathcal{C}$, and measurements on k qubits in the computational basis with $k\le n+m-\sum_{i=1}^m\log_2(\chi(\psi_i)/2)$ and $\chi(\psi_i)$ being the Pauli rank of ψ_i. Then for all $\alpha>0$, there exists a classical algorithm that when given a circuit from the above class, approximates the output probability up to l_1 norm δ in time $(n+m)^{O(1)}m^{O(\log(\sqrt{\alpha}/\delta)/\mu)}$ for at least a $1-\frac{2}{\alpha}$ fraction of Clifford circuits $\mathcal{C}$, where the Clifford operation $\mathcal{C}$ is uniformly randomly chosen, and $\mu:=\min_i\mu(\psi_i)$ and $\mu(\psi_i)$ is defined as* (2).

The proof is presented in Section D of the Supplementary Material [19]. If the parameters α, δ and μ are constants, then the running time is polynomial in n. The maximal number of allowed measured qubits in this algorithm decreases with the amount of the magic in the input states, which is quantified by the Pauli rank. A curious property of our algorithm is that its running time decreases with the amount of magic of the input states quantified by fidelity, contrary to the intuition that quantum circuits with more magic are harder to simulate. Similarly, if the quantum circuits are slightly beyond the Clifford circuits, for example, $\mathcal{C}=\mathcal{C}_1\circ V$ where the gates in $\mathcal{C}_1$ are Clifford gates in $\mathcal{C}l_{n+m}$ and V is some unitary gate in the third level of the Clifford Hierarchy $\mathcal{C}l_m^{(3)}$, then the result in Theorem 3 still holds.

Combining Theorem 1 and 3, we have the following corollary for any product input state:

Corollary 4. *Consider the class of circuits on $n+m_1+m_2$ qubits with input states $|0\rangle\langle 0|^{\otimes n}\otimes_{i=1}^{m_1}\rho_i\otimes_{j=1}^{m_2}|\psi_j\rangle\langle\psi_j|$, Clifford operation $\mathcal{C}$, and measurements on k qubits in the computational basis, where each ρ_i is a mixed state, each $|\psi_j\rangle$ is a pure nonstabilizer state, $k\le n+m_1+m_2-\sum_{j=1}^{m_2}\log_2(\chi(\psi_i)/2)$ and $\chi(\psi_i)$ is the Pauli rank of ψ_i. Then for all $\alpha>0$, there exists a classical algorithm that when given a circuit from the above class, approximates the output probability with respect to the l_1 norm δ in time $(n+m_1+m_2)^{O(1)}(m_1+m_2)^{O(\log(\sqrt{\alpha}/\delta)/\varepsilon)}$ for at least $1-\frac{2}{\alpha}$ fraction of Clifford circuits $\mathcal{C}$, where the Clifford operation $\mathcal{C}$ is uniformly randomly chosen, $\varepsilon=\min\{\lambda,\mu\}$ and $\lambda:=\min_i\lambda_i$, $\mu:=\min_j\mu(\psi_j)$.*

Now, let us apply our results to some restricted quantum computation models, such as Clifford circuits with solely magic state inputs (CM) and Pauli-based measurement (PBC), which gives an efficient simulation of $O(n)$ measurement with high probability.

Example 3—Theorem 3 implies the following result: for Clifford circuit $\mathcal{C}$ with input states $|T\rangle^{\otimes n}$ and measurement on k qubits in computational basis with $k\le(1-\log_2(3/2))n\approx 0.415n$, there exists a classical algorithm to approximate the output probability up to l_1 norm δ in time $n^{O((2+\sqrt{2})\log(\sqrt{\alpha}/\delta))}$ for at least $1-\frac{2}{\alpha}$ fraction of Clifford circuits $\mathcal{C}$, where $\mu(|T\rangle)=1-\frac{1}{\sqrt{2}}$ and $\chi(|T\rangle)=3$. If we choose the parameters α and δ to be constants, then the corresponding running time of this classical simulation is $poly(n)$, which implies that the Clifford circuit with magic input states and measurements on $0.415n$ qubits can be simulated efficiently on a classical computer with high probability. Note that our results do not contradict the hardness results given in [13], which are about the average-case hardness with measurements on n qubits.

Example 4—A Pauli-Based Computation (PBC) is defined as a sequence of measurement of some Pauli operators $P_i\in P^n$, where the measurement outcome is $(-1)^{\sigma_i}$ with $\sigma_i\in\{0,1\}$ and the Pauli operators $\{P_i\}$ are commuting with each other. Here, the initial state is $|T\rangle$ (or $|H\rangle=\cos\frac{\pi}{8}|0\rangle+\sin\frac{\pi}{8}|1\rangle$, which is equivalent to $|T\rangle$ up to Clifford unitary [32].). After k steps, the probability of outcome $P(\sigma_1,\dots,\sigma_k)=\langle T^{\otimes n}|\Pi|T^{\otimes n}\rangle$, where $\Pi=2^{-k}\prod_{i=1}^k(I+(-1)^{\sigma_i}P_i)$. Note that

PBC was considered in the fault-tolerant implementation of quantum computation based on stabilizer codes, where the stabilizer codes provide a simple realization of nondestructive Pauli measurements [33, 34]. Besides, it has been proved that the quantum computation based on Clifford+T circuits can be simulated by PBC [32]. Thus, this implies that the output probability $P(\sigma_1,\ldots,\sigma_k)$ is #P-hard to simulate. It has been shown that any PBC on n qubits can be classically simulated in $2^{cn}poly(n)$ time with $c\approx 0.94$ [32]. Here, Theorem 3 implies that if we choose α to be some constant and the measurement steps $k\leq(1-\log_2(3/2))n\approx 0.415n$, then there exists a classical algorithm to approximate the output probability up to l_1 norm δ in time $n^{O((2+\sqrt{2})\log(1/\delta))}$ for a large fraction of PBC. Moreover, if the approximation error δ is some constant, then the running time is $poly(n)$, which implies that the output probability of PBC after $0.415n$ measurement steps can be simulated efficiently on a classical computer with high probability.

At the end of this work, let us discuss the relationship between the Pauli rank we defined here and the stabilizer rank [29, 32]. Given a pure state $|\psi\rangle$, there are two ways to write the given pure state as a linear combination of stabilizer states: one is written in density matrix form and the other is written in vector state form. Thus, there are two definitions of stabilizer rank,

$$\chi_D(\psi)=\min\{R: |\psi\rangle\langle\psi|=\sum_{i=1}^{R}x_i|\phi_i\rangle\langle\phi_i|,\phi_i \text{ is a stabilizer state}\},$$
$$\chi_V(\psi)=\min\{R: |\psi\rangle=\sum_{i=1}^{R}x_i\ |\phi_i\rangle,\phi_i \text{ is a stabilizer state}\}.$$

Both stabilizer ranks χ_D and χ_V play an important role in the classical simulation of quantum circuits, which usually appears in the running time of classical algorithm [29, 32]. However, whether there exists an exponential lower bound for χ_D and χ_V for $|T^{\otimes n}\rangle$ is still unknown to our knowledge. Note that if this statement is false, then it follows that constant-depth Clifford+T circuits can be classically simulated in subexponential time [32]. Here, we find that the Pauli rank and stabilizer rank have the following relationship for any n-qubit pure state $|\psi\rangle$,

$$\chi_D(\psi)\geq\frac{\chi(\psi)}{2^n} \tag{3}$$

based on the Pauli rank of $|T^{\otimes n}\rangle$ is equal to 3^n, we can give an exponential lower bound $\chi_D(|T^{\otimes n}\rangle)\geq\left(\frac{3}{2}\right)^n$, see the Table I. The details of the proof is presented in Section D3 of the Supplementary Material [19].

$\lvert T^{\otimes n}\rangle$	χ_D	χ_V
Size	$\geq\left(\frac{3}{2}\right)^n$	$\overset{?}{\geq} 2^{\Omega(n)}$

TABLE I. Here we show that the stabilizer rank χ_D for $|T^{\otimes n}\rangle$ is lower bounded by $(\frac{3}{2})^n$. However, it is still unknown whether χ_V has an exponential lower bound.

III. CONCLUSION

In this work, we investigated the problem of evaluating the output probabilities of Clifford circuits with nonstabilizer input states. First, we provided an efficient classical algorithm to approximate the output probability of the Clifford circuits with mixed input states and showed that the running time scales with the increase in the purity of input states. Second, we showed that a modification of this algorithm gives an efficient classical simulation for pure nonstabilizer states, under some restriction on the number of measured qubits that is determined by the Pauli rank of the input states. The Pauli rank we introduced in this work can be regarded as a good candidate for a magic monotone. We showed that these two results have several implications in other restricted quantum computation models such as Clifford circuits with magic input states, Pauli-based computation and IQP circuits, which sheds new light on the classical simulation of these restricted quantum computational models. We also discuss the relationship between Pauli rank and stabilizer rank, and give an exponential lower bound on stabilizer rank χ_D for $|T^{\otimes n}\rangle$.

ACKNOWLEDGMENTS

K. B. thanks Xun Gao for introducing the tensor network representation of quantum circuits to him, and for fruitful discussions related to this topic. K.B. acknowledges the Templeton Religion Trust for the partial support of this research under grants TRT0159 and Zhejiang University for the support of an Academic Award for Outstanding Doctoral Candidates. D.E.K. is funded by EPiQC, an NSF Expedition in Computing, under grant CCF-1729369.

[1] P. W. Shor, FOCS **35**, 124 (1994).
[2] P. W. Shor, SIAM review **41**, 303 (1999).
[3] J. Preskill, Quantum **2**, 79 (2018).
[4] J. Preskill, arXiv:1203.5813.
[5] A. W. Harrow and A. Montanaro, Nature **549**, 203 (2017).
[6] S. Aaronson and A. Arkhipov, in *Proceedings of the forty-third annual ACM symposium on Theory of computing* (ACM, 2011) pp. 333–342.
[7] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[8] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Phys. Rev. Lett. **120**, 200502 (2018).
[9] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Proc. Roy. Soc. London Ser. A **467**, 459 (2010).
[10] T. Morimae, Y. Takeuchi, and H. Nishimura, Quantum **2**, 106 (2018).
[11] R. Jozsa and M. Van den Nest, Quantum Information & Computation **14**, 633 (2014).
[12] D. E. Koh, Quantum Information & Computation **17**, 0262 (2017).

[13] M. Yoganathan, R. Jozsa, and S. Strelchuk, arXiv:1806.03200.

[14] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Nature Physics **14**, 595 (2018).

[15] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, Nature Physics , 1 (2018).

[16] A. Bouland, J. F. Fitzsimons, and D. E. Koh, in *33rd Computational Complexity Conference (CCC 2018)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 102, edited by R. A. Servedio (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2018) pp. 21:1–21:25.

[17] D. Gottesman, Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics , 32 (1999).

[18] S. Aaronson and D. Gottesman, Phys. Rev. A **70**, 052328 (2004).

[19] See Supplementary Material [url] for the details of the proof, which includes Refs. [35–37].

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

[21] B. Zeng, X. Chen, and I. L. Chuang, Phys. Rev. A **77**, 042313 (2008).

[22] S. X. Cui, D. Gottesman, and A. Krishna, Phys. Rev. A **95**, 012329 (2017).

[23] X. Gao and L. Duan, arXiv:1810.03176.

[24] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Quantum **1**, 8 (2017).

[25] G. Kuperberg, Theory of Computing **11**, 183 (2015).

[26] K. Fujii and T. Morimae, New Journal of Physics **19**, 033003 (2017).

[27] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, Quantum **2**, 65 (2018).

[28] S. Bravyi, D. Browne, P. Calpin, E. Campbell, D. Gosset, and M. Howard, arXiv:1808.00128.

[29] S. Bravyi and D. Gosset, Phys. Rev. Lett. **116**, 250501 (2016).

[30] M. Howard and E. Campbell, Phys. Rev. Lett. **118**, 090501 (2017).

[31] V. Veitch, S. A. H. Mousavian, D. Gottesman, and J. Emerson, New Journal of Physics **16**, 013009 (2014).

[32] S. Bravyi, G. Smith, and J. A. Smolin, Phys. Rev. X **6**, 021043 (2016).

[33] D. Gottesman, Phys. Rev. A **57**, 127 (1998).

[34] A. M. Steane, Phys. Rev. Lett. **78**, 2252 (1997).

[35] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Phys. Rev. A **80**, 012304 (2009).

[36] T. Tao and V. H. Vu, *Additive combinatorics*, Vol. 105 (Cambridge University Press, 2006).

[37] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Phys. Rev. Lett. **117**, 080501 (2016).