Quantum Supremacy for Simulating a Translation-Invariant Ising Spin Model

Xun Gao,[1] Sheng-Tao Wang,[2] and L.-M. Duan[2,1]

[1]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*
[2]*Department of Physics, University of Michigan, Ann Arbor, Michigan 48109, USA*

(Received 19 July 2016; revised manuscript received 16 November 2016; published 27 January 2017)

We introduce an intermediate quantum computing model built from translation-invariant Ising-interacting spins. Despite being nonuniversal, the model cannot be classically efficiently simulated unless the polynomial hierarchy collapses. Equipped with the intrinsic single-instance-hardness property, a single fixed unitary evolution in our model is sufficient to produce classically intractable results, compared to several other models that rely on implementation of an ensemble of different unitaries (instances). We propose a feasible experimental scheme to implement our Hamiltonian model using cold atoms trapped in a square optical lattice. We formulate a procedure to certify the correct functioning of this quantum machine. The certification requires only a polynomial number of local measurements assuming measurement imperfections are sufficiently small.

DOI: 10.1103/PhysRevLett.118.040502

A universal quantum computer is believed to be able to solve certain tasks exponentially faster than the current computers [1,2]. Over the past several decades, there has been tremendous progress in both theoretical and experimental developments of a quantum computer. In theory, pioneering quantum algorithms, including Shor's factorization [3] and an algorithm for linear systems of equations [4], achieve exponential speedup compared with the best-known classical algorithms. However, formidable experimental challenges still lie ahead in building a universal quantum computer large enough to demonstrate quantum supremacy. This calls for simpler tasks to demonstrate exponential quantum speedup without the need for a universal machine.

Several intermediate computing models have been developed recently for this purpose. Examples include boson sampling [5], quantum circuits with commuting gates (IQP) [6,7], sparse and "fault-tolerant" IQP [8,9], the one-clean-qubit model [10,11], evolution of two-qubit commuting Hamiltonians [12], quantum approximate optimization algorithm [13], and random or universal quantum circuit [14,15]. These models fall into the category of sampling problems: the task of simulating the distribution sampled from the respective quantum system is believed to be classically intractable. In particular, if a classical computer can efficiently simulate the distribution to multiplicative errors, the polynomial hierarchy, a generalization of P and NP classes, will have to collapse to the third level [16,17], which is believed to be unlikely in complexity theory. Several experiments (e.g. [20,21]) have been reported for realization of boson sampling in small quantum systems using photons. However, the system size is still limited, which prohibits demonstration of quantum supremacy beyond classical tractability.

In this paper, we report three advancements towards demonstration of exponential quantum speedup in intermediate computing models. First, we formulate a new sampling model built from translation-invariant Ising-interacting spins, with strong connection to simulation of natural quantum many-body systems [22–25]. Our model only requires nearest-neighbor Ising-type interactions. The state preparation, the Hamiltonian, and measurements are all constructed to be translation invariant. Similar to Refs. [5,7], we prove the distribution sampled from our model cannot be classically efficiently simulated based on complexity theory results under reasonable conjectures [6,26–28]. An additional desirable feature of our model, which we call the "single-instance-hardness" property, is that a single fixed circuit and measurement pattern are sufficient to produce a classically hard distribution once the system size is fixed. This differs from typical sampling problems, where an ensemble of instances (unitaries) with a large number of parameters is demanded for the hardness result to hold [5–15]. This feature offers a significant simplification for experiments since proof of quantum supremacy for this model requires implementation of only a single Hamiltonian and measurement pattern instead of a range of different realizations (typically an exponential number or even an infinite number). Reference [5] also discussed the single-instance-hardness possibility in an abstract quantum circuit language, but no explicit circuit has been given thus far. Second, we propose a feasible experimental scheme to realize our model with cold atoms in optical lattices. The state preparation, engineering of time evolution, and measurement techniques are achievable with the state-of-the-art technology. Unlike photonic systems, cold atomic systems are much easier to scale up and reach a system size intractable to classical machines. Finally, we devise a scheme to certify our proposed quantum machine based on extension of the techniques developed in Refs. [29,30]. Certification of functionality is critically important for a sampling quantum machine as a correct sampling is hard to be verified. Our certification scheme only requires a polynomial number of local measurements, assuming the measurement imperfections are sufficiently small.

Before introducing our model, let us make more precise the two different error requirements used in this paper. Suppose the distribution $\{q_x\}$ is sampled from the quantum system with q_x being the probability of measuring the result x. Simulating $\{q_x\}$ to multiplicative errors translates to finding another distribution $\{p_x\}$ such that

$$\forall x, |p_x - q_x| \leq \gamma q_x \tag{1}$$

with $\gamma < 1/2$. This requirement seems too stringent for a classical sampler [5,6]: even the quantum device may not achieve such a physically unrealistic precision. A more sensible choice is the variation distance error [5,7,31]

$$\sum_x |p_x - q_x| \leq \epsilon. \tag{2}$$

Other than physical motivation, another reason to use this quantification of error lies in the equivalence between search and sampling problems under the variation distance bound [32]: the separation between classical and quantum samplers under this error requirement will permit the quantum device to solve classically intractable search problems [5]. This will have broad practical applications due to the ubiquity of search problems. For our Ising spin model, we will prove that the distribution produced by the quantum sampler can be certified by local measurements to variation distance errors, assuming the measurement imperfections are sufficiently small.

Our model can be regarded as a special type of IQP with a constant circuit depth. A general IQP [6,7] consists of Ising interactions between any pairs of spins and with varying strengths, while the sparse IQP [9] has $O(\sqrt{n}\log n)$ depth. Note that we are able to achieve such a low depth while maintaining classical hardness with variation distance errors [Eq. (2)] because we use a different complexity conjecture of average-case hardness. Reference [8] proposed another type of IQP in constant circuit depth on the Raussendorf-Harrington-Goyal (RHG) lattice [33]. In their model, the classical hardness result is guaranteed with multiplicative errors under some local noise below a threshold. Their Hamiltonian is also translation-invariant but the measurements are not. Thus, this model and the general IQP do not have the single-instance-hardness property. The general interactions in IQP and the three-dimensional structure of the RHG lattice may be difficult to realize in experiments.

Translation-invariant Ising model.—Our main construction is based on measurement-based quantum computing models [34–36]. We first introduce a translation-invariant nonadaptive measurement-based quantum computation model with only one measurement basis required. With postselection, we show that it can simulate universal quantum computation. Next, we reinterpret the measurement-based model as a sampling model based on quantum simulation of two-dimensional (2D) spins with translation-invariant Ising interactions and local magnetic fields. It has been known that if a sampling model with postselection can simulate universal quantum computation, it will be hard to simulate classically with multiplicative error bounds unless the polynomial hierarchy collapses to the third level [6,10,12]. We therefore conclude that our quantum Ising model will be classically intractable if the polynomial hierarchy does not collapse [17].

Consider the brickwork state shown in Fig. 1(a), which has been used for universal blind quantum computation [37]. Each circle represents a qubit prepared in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. A line connecting two neighboring circles denotes a controlled-Z operation on the qubits. As illustrated in Fig. 1(b), a measurement on one qubit in X basis with measurement result s implements a gate $HZ^s R_z(\theta)$, where H is the Hadamard gate and $R_z(\theta) = e^{-i\theta Z/2}$ denotes a rotation on a single qubit. Reference [37] proved that the model supports universal quantum computation given proper rotation angles θ and measurement results s (see Supplemental Material [17] for details). An important attribute of this model is that the graph structure and measurement patterns are independent of the computation. We further improve the model by making the angles θ translation invariant. In terms of the sampling problem, this modification gives rise to the advantage of the single-instance-hardness property. It differs from other existing sampling problems, such as boson sampling, wherein an average over random quantum circuits is needed for the classical hardness result to hold.

To fix the angle pattern, we use seven qubits to replace one white circle [Fig. 1(c)]. The primary goal is to encode

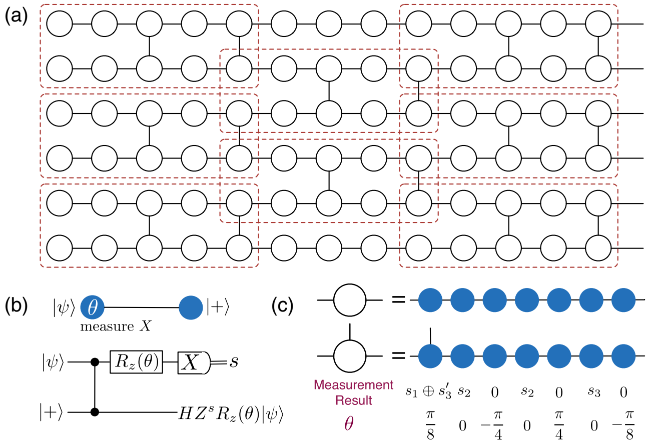
(a)
(b)
$|\psi\rangle$
θ
measure X
$|+\rangle$
$|\psi\rangle$
$R_z(\theta)$
X
s
$|+\rangle$
$HZ^s R_z(\theta)|\psi\rangle$
(c)
=
=
Measurement Result
θ
$s_1 \oplus s_3'$ s_2 0 s_2 0 s_3 0
$\frac{\pi}{8}$ 0 $-\frac{\pi}{4}$ 0 $\frac{\pi}{4}$ 0 $-\frac{\pi}{8}$

FIG. 1. (a) The brickwork state. Each circle represents a $|+\rangle$ state and each line denotes a CZ operation. (b) Propagation of the gate by measuring a qubit. (c) Each white circle with varying rotation angles is replaced by seven physical qubits with fixed rotation angles. The variation in the overall angle is encoded into different measurement outcomes.

rotation angle values into measurement outcomes, so that measurement postselection effectively realizes all necessary rotation angles. The basic building block is

$$HZ^sHR_z\left(-\frac{\theta}{2}\right)HZ^sHR_z\left(\frac{\theta}{2}\right) = R_z^s(\theta) \qquad (3)$$

which can be realized by measuring four connecting qubits in X basis with rotation angles $\theta/2, 0, -\theta/2, 0$ and postselecting the results to be $0, s, 0, s$. This equality furnishes a mechanism to conditionally perform the rotation $R_z(\theta)$ based on the measurement result s. Because of the Solovey-Kitaev theorem [38], it is sufficient to implement $HR_z(k\pi/4), k \in \{0, \ldots, 7\}$ for universal computation [17]. Writing $k = s_1s_2s_3, s_i \in \{0, 1\}$ in binary form, we have

$$\begin{aligned} Z^{s_3}HR_z\left(\frac{k\pi}{4}\right)Z^{s_3'} &= Z^{s_3}HR_z^{s_1}(\pi)R_z^{s_2}\left(\frac{\pi}{2}\right)R_z^{s_3}\left(\frac{\pi}{4}\right)Z^{s_3'} \\ &= HR_z\left(-\frac{\pi}{8}\right)HZ^{s_3}HR_z\left(\frac{\pi}{4}\right)HZ^{s_2} \\ &\quad \times HR_z\left(-\frac{\pi}{4}\right)HZ^{s_2}HZ^{s_1+s_3'}R_z\left(\frac{\pi}{8}\right). \end{aligned}$$

The extra term Z^{s_3} can be absorbed into the following gate and $Z^{s_3'}$ is left from the previous gate. Postselecting the measurement results as $s_1 \oplus s_3', s_2, 0, s_2, 0, s_3, 0$ with rotation angles $\pi/8, 0, -\pi/4, 0, \pi/4, 0, -\pi/8$, we can implement the gates $HR_z(k\pi/4)$ with $k = s_1s_2s_3$.

We now recast the nonadaptive measurement-based computation model as a sampling problem. A distribution can be sampled by measuring each spin in Fig. 1 in the X basis. The above procedure is only used to prove the universality of the nonadaptive measurement-based model with a fixed circuit under postselection. We remark that neither postselection nor adaptive measurements are required for sampling the distribution. The circuit can be implemented by a unitary time evolution under a local Hamiltonian

$$\mathcal{H} = -\sum_{\langle i,j\rangle} JZ_iZ_j + \sum_i B_iZ_i \qquad (4)$$

starting from the initial state $|+\rangle^{\otimes m\times n}$, with $m \times n$ being the number of spins. The second term imprints local rotation angles since $e^{-iB_iZ_i} = R_z(\theta_i)$, where $B_i = \theta_i/2$ characterizes the local Zeeman field strength on spin i. The evolution time and the reduced Planck constant $\hbar$ are set to unity. The first term performs the controlled-z operations with $J = \pi/4$, where $\langle i, j\rangle$ represents nearest-neighbor pairs connected by a line in Fig. 1. This can be seen as

$$\begin{aligned} CZ_{ij} &= e^{i\pi|1\rangle\langle 1|_i\otimes|1\rangle\langle 1|_j} = e^{i\pi/4(I_i-Z_i)\otimes(I_j-Z_j)} \\ &= e^{i\pi/4}e^{-i\pi/4I_i\otimes Z_j}e^{-i\pi/4Z_i\otimes I_j}e^{i\pi/4Z_i\otimes Z_j}. \end{aligned} \qquad (5)$$

The two local magnetic field terms in the equation above can be absorbed into rotation angles, without changing Fig. 1(c) (see Supplemental Material [17]). The distribution sampled from this fixed 2D Ising model cannot be simulated by a classical computer in polynomial time to multiplicative errors unless the polynomial hierarchy collapses.

Implementation proposal with cold atoms.—The Hamiltonian in Eq. (4) exhibits a few properties that make it amenable for experimental implementation. First of all, it only consists of commuting terms, so in experiment one can choose to break up the Hamiltonian and apply simpler terms in sequence. Second, the state preparation, the Hamiltonian and measurements are all translation invariant. This may greatly simplify the implementation for setups that can engineer the required unit cell. Another merit of our model originates from the single-instance-hardness feature. It ensures the sampling distribution after a single fixed unitary operation is already hard to simulate classically.

Here, we put forward a feasible experimental scheme based on cold atoms in optical lattices. A major difficulty arises from the special geometry required in the brickwork state. We propose to circumvent this problem by starting from the 2D cluster state (square lattice geometry) and reducing it to the brickwork state. In theory, this can be achieved by the "break" and "bridge" operations with measurement postselection as shown in Fig. 2 (see Supplemental Material [17] for more details). In experiment, postselection is again unnecessary with regard to sampling, but one incurs an additional cost of measuring in both X and Z basis (the measurement pattern is still translation invariant though). As a by-product, this procedure offers a concrete single-instance-hardness protocol to produce classically nonsimulatable distribution from the cluster state.

A complete experimental procedure is as follows. First, create a Mott-insulator state of cold atoms in 2D optical lattices with a central core of unit filling. One atom with two relevant atomic levels (e.g., $|F = 1, m_F = -1\rangle$ and $|F = 2, m_F = -2\rangle$ hyperfine levels of ^{87}Rb atoms) can be trapped in each site forming a square lattice of qubits. A 2D cluster state can be created in a single operational step by controlled collisional interaction [39,40]. The basic idea involves entangling neighboring atoms by spin-dependent transport together with controlled on-site collisions, which has been realized in experiment [40]. After generating the

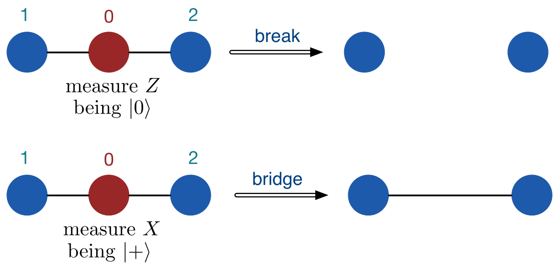

FIG. 2. Break and bridge operations. Qubit 0 is first rotated by $R_z(\pi/2)$ before measured in the Z and X basis, respectively, to perform the break and bridge operations.

cluster state, one needs to impose the rotation angle pattern onto each qubit. This requires the ability to address individual atoms with diffraction-limited performance. Single-site addressing is currently one of the state-of-the-art quantum control techniques in cold atom experiments [41,42]. In particular, by using a digital micro-mirror device, it is possible to engineer holographic beam shaping with arbitrary amplitude and phase control [42]. To imprint the individual phases, one can make use of spin-dependent ac Stark shifts [41] with beam amplitude patterns given by the rotation angles. The amplitude hologram controls the strength B_i and realizes the second term in the Hamiltonian in Eq. (4). Finally, spin measurements can be performed on each site, with single-site-resolved imaging techniques [43,44]. Because some spins have to be measured in the Z basis, they should be rotated by individual addressing techniques before all atoms can be measured in the X basis.

Simulation and certification with variation distance errors.—So far, we have shown that our Ising spin model is classically intractable with multiplicative error bounds. Similar to what have been attained in boson sampling [5] and IQP [7], we can also prove classical hardness to variation distance error bounds if we assume the "worst-case" hardness result can be extended to "average-case." More specifically, let us define the partition function of

$$\mathcal{H}_x = \mathcal{H} + \frac{\pi}{2}\sum_i x_i Z_i, \quad \text{where } x_i \in \{0, 1\} \tag{6}$$

to be $\mathcal{Z}_x = \mathrm{tr}(e^{-\beta\mathcal{H}_x})$, setting the imaginary temperature unit as $\beta \equiv 1/k_B T = i$. In the Supplemental Material [17], we prove that approximating $|\mathcal{Z}_x|^2/2^{mn}$ by $|\widetilde{\mathcal{Z}_x}|^2/2^{mn}$ to a mixture of multiplicative and additive errors such that

$$\left|\frac{|\widetilde{\mathcal{Z}_x}|^2}{2^{mn}} - \frac{|\mathcal{Z}_x|^2}{2^{mn}}\right| \le \frac{1}{\mathrm{poly}(n)}\frac{|\mathcal{Z}_x|^2}{2^{mn}} + \frac{\epsilon}{\delta}[1 + o(1)] \tag{7}$$

with $\epsilon/\delta < 1/2$ is #P-hard in the worst case. Our classical intractability result requires lifting the #P-hardness of the estimation from the worst case to the average-case: picking any $1-\delta$ fraction of instances x, it is still #P-hard. This conjecture is similar to the one used in Ref. [7] except that they reduced the mixture of errors to simply multiplicative errors. All the known classically intractable quantum sampling models with variation distance errors require a similar average-case complexity conjecture.

Thus, with reasonable assumptions, our Ising spin model is also classically intractable with variation distance bounds. Using techniques similar to those in Refs. [29,30], we can in addition certify the correct functioning of a quantum device, with only a polynomial number of local measurements. Suppose $\{q'_x\}$ is the distribution sampled from our quantum device with the final state ρ' (state before measurement); the ideal ones are denoted as $\{q_x\}$ and ρ. The total variation distance between distributions $\{q_x\}$ and $\{q'_x\}$ can be bounded by [1]

$$\sum_x |q_x - q'_x| \le D(\rho, \rho'), \tag{8}$$

where $D(\rho, \rho') = \mathrm{tr}(|\rho - \rho'|)/2$ is the trace distance between states ρ and ρ'. Hence, if we can bound the trace distance $D(\rho, \rho') < \epsilon$, we can also bound the total variation distance. Note, however, this does not allow us to estimate q_x in experiment: statistical errors always kick in to thwart any polynomial-time efforts to estimate the distribution due to the exponential suppression of some q_x. We bypass statistical errors by assuming the correctness of quantum mechanics. To sample from $\{q'_x\}$ in experiment though, measurement imperfections may cause deviations in variation distance. However, if measurement imperfections on each spin are local and bounded by $O(\epsilon/(mn))$ [17], we can still correctly certify the quantum device. Below, we show how to bound $D(\rho, \rho')$ by a polynomial number of local measurements.

As a graph state, the brickwork state in Figs. 1(a) and 1(c) is the unique ground state of the 4-local Hamiltonian

$$H_{\mathrm{brickwork}} = \sum_i \frac{I - X_i \prod_{j\in \mathrm{neighbor\ of}\, i} Z_j}{2}. \tag{9}$$

Each qubit i is connected to at most three neighboring ones, and the energy gap from the ground state is 1. The ideal state ρ is the brickwork state acted by some single qubit rotations $R_z(\theta_i)$. It is therefore the unique ground state of the Hamiltonian

$$\begin{aligned} H'_{\mathrm{brickwork}} &= \prod_i R_z(\theta_i) H_{\mathrm{brickwork}} \prod_j R_z^\dagger(\theta_j) \\ &= \sum_i \frac{I - R_z(\theta_i) X_i R_z^\dagger(\theta_i) \prod_{j\in \mathrm{neighbor\ of}\, i} Z_j}{2}. \end{aligned}$$

This Hamiltonian is still 4-local, with ground state energy gap 1. Using the weak-membership quantum state certification protocol in Ref. [29], one can measure each local term of $H'_{\mathrm{brickwork}}$ by a polynomial number of times to obtain a good estimation of $\langle H'_{\mathrm{brickwork}}\rangle$ averaged over ρ'. The estimation will be efficient due to Hoeffding's bound and the finite norm of each local term. Since the ground state energy gap is constant, $\langle H'_{\mathrm{brickwork}}\rangle > 0$ implies a finite component of excited states is present in ρ'. Conversely, a small $\langle H'_{\mathrm{brickwork}}\rangle$ will be able to bound $D(\rho, \rho')$. More quantitatively, we show in the Supplemental Material [17] that with confidence level $1–2^{-O(r)}$, using $O(m^2 n^2 r/\epsilon^4)$ measurements on each local term is sufficient to certify $\sum_x |q_x - q'_x| \le \epsilon$, provided the measurement imperfections on each spin are bounded by $O[\epsilon/(mn)]$. Similar hardness and certification results hold if we start from the cluster state as in our experimental proposal [17]. In that case, 5-local measurements are needed.

The IQP certification protocol developed in Ref. [29] requires a much stronger quantum simulator than the IQP simulator itself since they need to generate all the history states [45]. In contrast, our certification protocol only requires preparing the state ρ' itself. This is relevant in light of demonstrating quantum supremacy [46] using practical quantum many-body systems, instead of resorting to a universal quantum simulation device.

Discussion.—In summary, we have introduced a translation-invariant Ising spin model and shown that it is classically intractable unless the polynomial hierarchy collapses. Because our average-case conjecture bypasses the anticoncentration property used in Refs. [5,7,9], the classical simulability result under constant-strength local noise [9] may not apply to our model. Whether our model is robust to noise requires further analysis. There is also a natural connection between our model and sampling models of random quantum circuits such as the one in Ref. [14]: measurement on qubits in the first $n-1$ columns in our model corresponds to choosing one instance of a random circuit due to the relation between our model and measurement-based quantum computing. With the advantageous single-instance-hardness property, the amenability to experimental implementation and certification of the quantum machine, we develop a full picture of using our model to demonstrate quantum supremacy. This may shed light on the likely exponential gap in computational power between a classical and a quantum machine.

X. G. is grateful to Man-Hong Yung and Mingji Xia for helpful discussions that inspire this work. S. T. W. thanks Ruichao Ma for useful discussions related to the experimental proposal. We also thank Michael J. Bremner and Ashley Montanaro for insightful discussions and suggestions. This work was supported by the Ministry of Education of China and Tsinghua University. L. M. D. and S. T. W. acknowledge, in addition, support from the AFOSR MURI program and the IARPA program.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2010).

[2] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, Nature (London) **464**, 45 (2010).

[3] P. W. Shor, in *1994 Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994*, pp. 124–134, http://ieeexplore.ieee.org/document/365700/.

[4] A. W. Harrow, A. Hassidim, and S. Lloyd, Phys. Rev. Lett. **103**, 150502 (2009).

[5] S. Aaronson and A. Arkhipov, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing, STOC '11* (ACM, New York, 2011), pp. 333–342.

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

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

[8] K. Fujii and S. Tamate, Sci. Rep. **6**, 25598 (2016).

[9] M. J. Bremner, A. Montanaro, and D. J. Shepherd, arXiv:1610.01808.

[10] T. Morimae, K. Fujii, and J. F. Fitzsimons, Phys. Rev. Lett. **112**, 130502 (2014).

[11] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, arXiv:1409.6777.

[12] A. Bouland, L. Mančinska, and X. Zhang, arXiv:1602.04145.

[13] E. Farhi and A. W. Harrow, arXiv:1602.07674.

[14] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, J. M. Martinis, and H. Neven, arXiv:1608.00263.

[15] K. Fujii, arXiv:1610.03632.

[16] S. Arora and B. Barak, *Computational Complexity: A Modern Approach* (Cambridge University Press, Cambridge, England, 2009).

[17] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.118.040502, which includes Refs. [18,19], for more details on the proof of the hardness result and the simulation and certification with variation distance errors.

[18] L. Stockmeyer, SIAM J. Comput. **14**, 849 (1985).

[19] C. E. Porter and R. G. Thomas, Phys. Rev. **104**, 483 (1956).

[20] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, Science **339**, 794 (2013).

[21] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, J. C. Gates, B. J. Smith, P. G. R. Smith, and I. A. Walmsley, Science **339**, 798 (2013).

[22] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[23] S. Lloyd, Science **273**, 1073 (1996).

[24] I. Buluta and F. Nori, Science **326**, 108 (2009).

[25] J. I. Cirac and P. Zoller, Nat. Phys. **8**, 264 (2012).

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

[27] Y. Han, L. A. Hemaspaandra, and T. Thierauf, SIAM J. Comput. **26**, 59 (1997).

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

[29] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, arXiv:1602.00703.

[30] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Nat. Commun. **1**, 149 (2010).

[31] B. Fefferman and C. Umans, arXiv:1507.05592.

[32] S. Aaronson, Theor. Comp. Sys. **55**, 281 (2014).

[33] R. Raussendorf, J. Harrington, and K. Goyal, Ann. Phys. (Amsterdam) **321**, 2242 (2006).

[34] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, Nat. Phys. **5**, 19 (2009).

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

[36] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68**, 022312 (2003).

[37] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *50th Annual IEEE Symposium on Foundations of Computer Science, 2009, FOCS '09* (2009), pp. 517–526, http://ieeexplore.ieee.org/document/5438603/.

[38] A. Y. Kitaev, Russ. Math. Surv. **52**, 1191 (1997).

[39] D. Jaksch, H.-J. Briegel, J. I. Cirac, C. W. Gardiner, and P. Zoller, Phys. Rev. Lett. **82**, 1975 (1999).

[40] O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hansch, and I. Bloch, Nature (London) **425**, 937 (2003).

[41] C. Weitenberg, M. Endres, J. F. Sherson, M. Cheneau, P. Schausz, T. Fukuhara, I. Bloch, and S. Kuhr, Nature (London) **471**, 319 (2011).

[42] P. Zupancic, P. M. Preiss, R. Ma, A. Lukin, M. E. Tai, M. Rispoli, R. Islam, and M. Greiner, Opt. Express **24**, 13881 (2016).

[43] W. S. Bakr, A. Peng, M. E. Tai, R. Ma, J. Simon, J. I. Gillen, S. Fölling, L. Pollet, and M. Greiner, Science **329**, 547 (2010).

[44] J. F. Sherson, C. Weitenberg, M. Endres, M. Cheneau, I. Bloch, and S. Kuhr, Nature (London) **467**, 68 (2010).

[45] A. Y. Kitaev, A. Shen, and M. N. Vyalyi, *Classical and Quantum Computation* (American Mathematical Society, Providence, RI, 2002), Vol. 47.

[46] J. Preskill, arXiv:1203.5813.