Verified measurement-based quantum computing with hypergraph states

Tomoyuki Morimae,^{1,*} Yuki Takeuchi,^{2,†} and Masahito Hayashi^{3,4,‡}

¹ASRLD Unit, Gunma University, 1-5-1 Tenjincho Kiryushi Gunma, 376-0052, Japan
²Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan
³Graduate School of Mathematics, Nagoya University, Furocho, Chikusaku, Nagoya, 464-8602, Japan
⁴Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542, Singapore

Hypergraph states are generalizations of graph states where controlled-Z gates on edges are replaced with generalized controlled-Z gates on hyperedges. Hypergraph states have several advantages over graph states. For example, certain hypergraph states, such as the Union Jack states, are universal resource states for measurement-based quantum computing with only Pauli measurements, while graph state measurement-based quantum computing needs non-Clifford basis measurements. Furthermore, it is impossible to classically efficiently sample measurement results on hypergraph states with a constant L1-norm error unless the polynomial hierarchy collapses to the third level. Although several protocols have been proposed to verify graph states with only sequential single-qubit Pauli measurements, there was no verification method for hypergraph states. In this paper, we propose a method for verifying hypergraph states with only sequential single-qubit Pauli measurements. As applications, we consider verified blind quantum computing with hypergraph states, and quantum supremacy demonstrations with hypergraph states.

Many-point correlations in quantum many-body systems are one of the most essential ingredients in condensed-matter physics and statistical physics. Correlations of sequential single-qubit measurements on quantum states are also important drive forces for quantum information processing. For example, measurement-based quantum computing [1], which is nowadays one of the standard quantum computing models, enables universal quantum computing with only adaptive single-qubit measurements on certain quantum states, such as graph states [1] and other condensed-matter-physically motivated states including the AKLT state [2–17]. Furthermore, not only adaptive but also non-adaptive singlequbit measurements on graph states can demonstrate a quantumness which cannot be classically efficiently simulated: it is known that if probability distributions of nonadaptive sequential single-qubit measurements on graph states are classically efficiently sampled, then the polynomial hierarchy collapses to the third level [18–20] or the second level [21]. The polynomial hierarchy is a hierarchy of complexity classes generalizing P and NP, and it is not believed to collapse in computer science. It is an example of recently well studied "quantum supremacies" of sub-universal quantum computing models, which are expected to be easier to experimentally implement, but can outperform classical computing. (For details, see Refs. [18–24] and their supplementary materials.)

For practical implementations of measurement-based quantum computing and experimental demonstrations of the quantum supremacy, verifying graph states is essential, since in reality a generated state cannot be the ideal graph state due to some experimental noises. The problem becomes more serious if we consider delegated secure quantum computing, so called blind quantum computing [25, 26]. It is known that the ability of sequentially measuring single qubits is enough to secretly delegate

quantum computing to a remote server [27, 28]. The honest server sends each qubit of a graph state one by one to the user, and user can realize any quantum computing with only sequential single-qubit measurements. If the server is malicious, however, a completely wrong state might be sent to the user. The user therefore needs to test the state sent from the server. In such a quantum cryptographic scenario, the situation is worse than the singleparty laboratory experiments, since the noises on the given state are caused by malicious servers and therefore not necessarily physically natural ones. Several methods of verifying graph states with only sequential single-qubit Pauli measurements have been proposed [28, 29]. (If more than two non-communicating servers are available, a completely classical user can verify stabilizer states [30– 32].) In the protocol of Ref. [28], the user does a test so called the stabilizer test on some parts of the state sent from the server. The stabilizer test can be done with only sequential single-qubit Pauli measurements. If the user passes the test, the remaining state is guaranteed to be close to the ideal graph state.

Since the protocol of Ref. [28] makes no assumption (such as the i.i.d. sample or physically natural noises) on the given state, the verification method can be used in quantum cryptographic contexts. In particular, verified blind quantum computing and verified quantum supremacy demonstrations can be realized with graph states verified through the protocol. There are, however, two problems. First, in the verified blind protocol of Ref. [28], the user needs non-Clifford basis measurements for computing (the verification itself can be done with only Pauli measurements). It would be better if both the verification and the computation can be done with only Pauli measurements [33]. Second, the quantum supremacy demonstration with graph states [18], which needs only non-adaptive measurements, requires some-

how a strict approximation, namely a multiplicative-error approximation.

Recently, two breakthroughs that solve these drawbacks of graph states have been done. These results use hypergraph states [34–38] in stead of graph states. (For the definition of hypergraph states and their properties, see below.) First, certain hypergraph states, such as the Union Jack states, are universal resource states for measurement-based quantum computing with only Pauli measurements [39]. This result solves the first problem, namely, the requirement of non-Clifford basis measurements for the user. Therefore, by using the hypergraph states, the one-way secure delegated quantum computing is possible for the user who can do only Pauli measurements. Ref. [39] also pointed out that hypergraph states are important in the study of symmetry-protected topological orders. Second, it was shown in Ref. [19] that if hypergraph states are considered, the multiplicative error requirement can be replaced with an L1-norm one, which is more relaxed. This result solves the second problem.

In short, hypergraph states are promising novel resource states for many quantum information processing tasks. Unfortunately, however, there was no verification method for hypergraph states. In particular, we did not know how to test a given hypergraph state with only sequential single-qubit Pauli measurements. It was a huge obstacle for practical applications of hypergraph states in quantum information and condensed matter physics.

In this paper, we propose a method for verifying hypergraph states with only sequential single-qubit Pauli measurements. As in the case of the graph state verification [28], the user does a certain test on some parts of the state sent from the server. If the user passes the test, then the remaining state is guaranteed to be close to the ideal hypergraph state. As applications, we consider verified blind quantum computing with hypergraph states, and verified quantum supremacy demonstrations with hypergraph states.

Hypergraph states.— We first define hypergraph states, and explain their properties. A hypergraph $G \equiv (V, E)$ is a pair of a set V of vertices and a set E of hyperedges, where $n \equiv |V|$. A hyperedge may link more than two vertices. For simplicity, in this paper, we assume that $2 \leq |e| \leq 3$ for all $e \in E$, where |e| is the number of vertices linked to the hyperedge e. (Generalizations to other cases would be possible.) Let

$$|G\rangle \equiv \Big(\prod_{e \in E} \widetilde{CZ}_e\Big)|+\rangle^{\otimes n}$$

be the hypergraph state corresponding to the hypergraph G, where $\widehat{CZ}_e \equiv \bigotimes_{i \in e} I_i - 2 \bigotimes_{i \in e} |1\rangle\langle 1|_i$ is the generalized CZ gate acting on vertices in the hyperedge e. Here, I is the two-dimensional identity operator. For example, if |e| = 2, it is nothing but the standard CZ gate. If |e| = 3, it is the CCZ gate, $CCZ \equiv (I^{\otimes 2} - |11\rangle\langle 11|) \otimes I + |11\rangle\langle 11| \otimes Z$.

The stabilizer g_i of $|G\rangle$ associated with the vertex i is defined by

$$\begin{split} g_i &\equiv \Big(\prod_{e \in E} \widetilde{CZ}_e\Big) X_i \Big(\prod_{e \in E} \widetilde{CZ}_e\Big) \\ &= X_i \Big(\prod_{j \in W_i^Z} Z_j\Big) \Big(\prod_{(j,k) \in W_i^{CZ}} CZ_{j,k}\Big), \end{split}$$

where

$$\begin{split} W_i^Z & \equiv & \{j \in V \mid (i,j) \in E\}, \\ W_i^{CZ} & \equiv & \{(j,k) \in V \times V \mid (i,j,k) \in E\}. \end{split}$$

It is easy to check that the following properties are satisfied: $[g_i,g_j]=0$ for all $i,j\in V$. $g_i|G\rangle=|G\rangle$ for all $i\in V$. $g_i^2=I^{\otimes n}$ for all $i\in V$. $\prod_{i=1}^n\frac{I^{\otimes n}+g_i}{2}=|G\rangle\langle G|$. Stabilizer test for g_i .— Before introducing our verifi-

Stabilizer test for g_i .— Before introducing our verification protocol, we define the stabilizer test for each g_i , which is an essential ingredient of the protocol. Note that $CZ_{j,k} = \frac{1}{2}(I_j \otimes I_k + I_j \otimes Z_k + Z_j \otimes I_k - Z_j \otimes Z_k)$. Therefore

$$g_{i} = X_{i} \left(\prod_{j \in W_{i}^{Z}} Z_{j} \right) \left(\frac{1}{2^{r}} \sum_{t \in \{1,2,3,4\}^{r}} \prod_{(j,k) \in W_{i}^{CZ}} \sigma_{j,k}(t_{j,k}) \right)$$
$$= \frac{1}{2^{r}} \sum_{t \in \{1,2,3,4\}^{r}} s_{t},$$

where $r \equiv |W_i^{CZ}|$, $t \equiv \{t_{j,k}\}_{(j,k)\in W_i^{CZ}}$, $\sigma_{j,k}(1) \equiv I_j \otimes I_k$, $\sigma_{j,k}(2) \equiv I_j \otimes Z_k$, $\sigma_{j,k}(3) \equiv Z_j \otimes I_k$, $\sigma_{j,k}(4) \equiv -Z_j \otimes Z_k$, and

$$s_t \equiv X_i \Big(\prod_{j \in W_i^Z} Z_j \Big) \Big(\prod_{(j,k) \in W_i^{CZ}} \sigma_{j,k}(t_{j,k}) \Big).$$

Let us define a bit $\alpha_t \in \{0,1\}$ and a subset $D_t \subseteq V$ such that

$$s_t = (-1)^{\alpha_t} X_i \Big(\prod_{j \in D_t} Z_j \Big).$$

Note that α_t and D_t can be calculated in polynomial time. In fact, α_t can be calculated in the following way. We first set $\alpha_t = 0$. If $t_{j,k} = 4$, we flip α_t . We do it for all $(j,k) \in W_i^{CZ}$. Since $|W_i^{CZ}| \leq {n-1 \choose 2} = O(n^2)$, it takes at most polynomial time. Furthermore, D_t can be calculated in the following way. We first set $D_t = W_i^Z$. We then update D_t according to $t_{j,k}$ for each $(j,k) \in W_i^{CZ}$. Again, $|W_i^{CZ}| \leq O(n^2)$ means that it takes at most polynomial time.

Let ρ be an *n*-qubit state. We define the "stabilizer test for g_i on ρ " as the following Alice's action:

- 1. Alice randomly generates $t \in \{1, 2, 3, 4\}^r$.
- 2. She measures ith vertex of ρ in X, and jth vertex of ρ in Z for all $j \in D_t$.

Let $x \in \{+1, -1\}$ be the measurement result of the X measurement, and $z_j \in \{+1, -1\}$ be that of the Z measurement on vertex $j \in D_t$. We say that Alice passes the stabilizer test for g_i on ρ if $x \prod_{j \in D_t} z_j = (-1)^{\alpha_t}$.

The probability $p_{\text{test},i}$ that Alice passes the stabilizer test for g_i on ρ is [40]

$$p_{\text{test},i} \equiv \frac{1}{4^r} \sum_{t \in \{1,2,3,4\}^r} \text{Tr}\left(\rho \frac{I^{\otimes n} + s_t}{2}\right) = \frac{1}{2} + \frac{\text{Tr}(\rho g_i)}{2^{r+1}}.$$

Verification protocol.— We now explain our verification protocol. Bob sends Alice an n(nk + 1 + m)-qubit state Ψ , where $k = 2^{2r+3}n^7$ and $m \ge 2n^7k^2\ln 2$. The state Ψ consists of nk + 1 + m registers (Fig. 1). Each register stores n qubits. (If Bob is honest, every register is in the state $|G\rangle$. If Bob is malicious, on the other hand, Ψ can be any n(nk+1+m)-qubit entangled state.) Alice randomly permutes registers and discards m registers. (As we will see later, this random permutation and discarding of some registers are necessary to guarantee that the remaining state is close to an i.i.d. sample by using the quantum de Finetti theorem [41].) Let Ψ' be the remaining state. The state Ψ' consists of nk+1 registers. She chooses one register from Ψ' , which is used for the measurement-based quantum computing. We call the register computing register. The remaining nk registers of Ψ' are divided into n groups. Each group consists of k registers. The stabilizer test for q_i is performed on every register in the ith group for i = 1, 2, ..., n. (Note that Alice does not need to do the permutation "physically", which requires a quantum memory. Bob just sends each qubit of Ψ one by one to Alice, and Alice randomly chooses her action from the test, discarding, or computation.)

Let K_i be the number of times that Alice passes the stabilizer test for g_i , i.e. the random variable to describe the number of Alice's observation of the event $\frac{1}{4^r}\sum_t \frac{I^{\otimes n}+s_t}{2}$. If $\frac{K_i}{k}\geq \frac{1}{2}+\frac{1-\epsilon}{2^{r+1}}$, we say that the *i*th group passes the test. Here, $\epsilon=\frac{1}{2n^3}$. If all groups pass the test, we say that Alice accepts Bob.

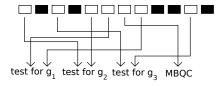


FIG. 1: An example for n=3, k=2, m=5. Each square represents a register that stores n qubits. Registers represented by black squares are discarded.

The main results of the present paper are the following two items:

1. Completeness: if every register of Ψ is in the state $|G\rangle$, then the probability that Alice accepts Bob is larger than $1-ne^{-n}$.

2. Soundness: if Alice accepts Bob, the state ρ_{comp} of the computing register satisfies $\langle G|\rho_{\text{comp}}|G\rangle \geq 1 - \frac{1}{n}$ with a probability larger than $1 - \frac{1}{n}$.

Proof of the completeness.— We first show the completeness. If every register of Ψ is in the state $|G\rangle$, then $p_{\text{test},i} = \frac{1}{2} + \frac{1}{2^{r+1}}$ for all i = 1, 2, ..., n. From the union bound and the Hoeffding inequality,

$$\begin{split} \Pr[\text{Alice accepts Bob}] &= \Pr\Big[\bigwedge_{i=1}^n \Big(\frac{K_i}{k} \geq \frac{1}{2} + \frac{1-\epsilon}{2^{r+1}}\Big)\Big] \\ &\geq 1 - \sum_{i=1}^n \Pr\Big[\frac{K_i}{k} < \frac{1}{2} + \frac{1-\epsilon}{2^{r+1}}\Big] \\ &= 1 - \sum_{i=1}^n \Pr\Big[\frac{K_i}{k} < p_{\text{test},i} - \frac{\epsilon}{2^{r+1}}\Big] \\ &\geq 1 - ne^{-2\frac{\epsilon^2}{2^{2r+2}}k}. \end{split}$$

Proof of the soundness.—We next show the soundness. We define the n-qubit projection operator $\Pi_G^{\perp} \equiv I^{\otimes n} - |G\rangle\langle G|$. Let T be the POVM element corresponding to the event that Alice accepts Bob. We can show that for any n-qubit state ρ ,

$$\operatorname{Tr}\left[(T \otimes \Pi_G^{\perp})\rho^{\otimes nk+1}\right] \leq \frac{1}{2n^2}.$$
 (1)

Its proof is given later. Due to the quantum de Finetti theorem (for the one-way LOCC norm version) [41],

$$\operatorname{Tr}\left[(T \otimes \Pi_{G}^{\perp})\Psi'\right] \leq \operatorname{Tr}\left[(T \otimes \Pi_{G}^{\perp}) \int d\mu(\rho) \rho^{\otimes nk+1}\right] + \frac{1}{2} \sqrt{\frac{2n^{2}k^{2}n \ln 2}{m}}$$

$$\leq \frac{1}{2n^{2}} + \frac{1}{2} \sqrt{\frac{2n^{3}k^{2} \ln 2}{2n^{7}k^{2} \ln 2}} = \frac{1}{n^{2}}.$$

We have $\operatorname{Tr}[(T \otimes \Pi_G^{\perp})\Psi'] = \operatorname{Tr}(\Pi_G^{\perp}\rho_{\operatorname{comp}})\operatorname{Tr}[(T \otimes I)\Psi']$. Therefore, if $\operatorname{Tr}(\Pi_G^{\perp}\rho_{\operatorname{comp}}) > \frac{1}{n}$, then $\operatorname{Tr}[(T \otimes I)\Psi'] < \frac{1}{n}$, which means that if Alice accepts Bob, $\langle G|\rho_{\operatorname{comp}}|G\rangle \geq 1 - \frac{1}{n}$ with a probability larger than $1 - \frac{1}{n}$.

Proof of Eq. (1).— First, let us assume that $\text{Tr}(\rho g_i) \geq 1 - \delta$ for all i = 1, 2, ..., n, where $\delta = \frac{1}{n^3}$. Due to the union bound,

$$1 - \langle G|\rho|G\rangle = 1 - \text{Tr}\Big(\prod_{i=1}^{n} \frac{I^{\otimes n} + g_i}{2}\rho\Big)$$

$$\leq \sum_{i=1}^{n} \left[1 - \text{Tr}\Big(\rho \frac{I^{\otimes n} + g_i}{2}\Big)\right] \leq \frac{n\delta}{2}.$$

Therefore,

$$\operatorname{Tr}\left[(T\otimes\Pi_{G}^{\perp})\rho^{\otimes nk+1}\right] = \operatorname{Tr}(T\rho^{\otimes nk})\operatorname{Tr}(\Pi_{G}^{\perp}\rho)$$

$$\leq 1 \times \frac{n\delta}{2} = \frac{1}{2n^{2}}.$$
(2)

Next let us assume that $Tr(\rho g_i) < 1 - \delta$ for at least one *i*. In this case,

$$p_{\text{test},i} = \frac{1}{2} + \frac{\text{Tr}(\rho g_i)}{2^{r+1}} < \frac{1}{2} + \frac{1-\delta}{2^{r+1}}$$

for the i. Then, due to the Hoeffding inequality,

$$\begin{split} \operatorname{Tr}[(T \otimes I) \rho^{\otimes nk+1}] & \leq & \operatorname{Pr}[\operatorname{group} i \text{ passes the test}] \\ & = & \operatorname{Pr}\Big[\frac{K_i}{k} \geq \frac{1}{2} + \frac{1-\epsilon}{2^{r+1}}\Big] \\ & = & \operatorname{Pr}\Big[\frac{K_i}{k} \geq \frac{1}{2} + \frac{1-\delta}{2^{r+1}} + \frac{\delta-\epsilon}{2^{r+1}}\Big] \\ & \leq & \operatorname{Pr}\Big[\frac{K_i}{k} > p_{\operatorname{test},i} + \frac{\delta-\epsilon}{2^{r+1}}\Big] \\ & \leq & e^{-2\frac{(\delta-\epsilon)^2}{2^{2r+2}}k} = e^{-n}. \end{split}$$

Hence

$$\operatorname{Tr}[(T \otimes \Pi_G^{\perp})\rho^{\otimes nk+1}] = \operatorname{Tr}(T\rho^{\otimes nk})\operatorname{Tr}(\Pi_G^{\perp}\rho)$$

$$\leq e^{-n} \times 1. \tag{3}$$

From Eqs. (2) and (3), for any state ρ ,

$$\operatorname{Tr}[(T \otimes \Pi_G^{\perp}) \rho^{\otimes nk+1}] \leq \max\left(\frac{1}{2n^2}, e^{-n}\right) = \frac{1}{2n^2}.$$

Applications.— To conclude this paper, we finally discuss two applications of our results. First, our verification protocol can be used in verified blind quantum computing. In the protocol of Ref. [28], the user needs non-Clifford basis measurements to implement quantum computing (the verification itself can be done with only Pauli measurements.) On the other hand, if the server generates the Union Jack states [39], for example, the user needs only Pauli measurements for both the verification and the computation.

Second, our protocol can be used for the verified quantum supremacy demonstration. It was shown in Ref. [19] that the following is true for several hypergraph states (assuming the so called "worst case vs average case" conjecture): if there exists a classical sampler that outputs z with probability q_z such that $\sum_{z \in \{0,1\}^n} |p_z - q_z| \le \frac{1}{192}$, then the polynomial hierarchy collapses to the third level. Here, p_z is the probability of obtaining the result $z \in \{0,1\}^n$ when certain single-qubit measurements are done on an n-qubit hypergraph state. This result means that if we can generate hypergraph states, we can demonstrate the quantum supremacy. However, what happens if we cannot have the ideal hypergraph state, and only the verified state ρ_{comp} is available? (For example, Alice, who can do only single-qubit measurements, might want untrusted Bob to send a hypergraph state.) We can show that the state ρ_{comp} is enough to demonstrate the same quantum supremacy. In fact, let us assume that there exists a classical sampler such that $\sum_{z} |p'_{z} - q_{z}| \leq \frac{1}{192}$,

where p'_z is the output probability distribution of the single-qubit measurements on ρ_{comp} . Then,

$$\sum_{z} |p_z - q_z| \leq \sum_{z} |p_z - p_z'| + \sum_{z} |p_z' - q_z|$$

$$\leq o(1) + \frac{1}{192},$$

which means that the classical sampler can also sample p_z with the $\sim 1/192~L1$ -norm error. For example, the hypergraph states naturally induced from the IQP circuits corresponding to the non-adaptive Union Jack state measurement-based quantum computing [39] can be used for that purpose. Since the non-adaptive Union Jack state measurement-based quantum computing is universal with postselections, a multiplicative error calculation of its output probability distribution is #P-hard [20]. If we assume the worst case hardness can be lifted to the average case one, we can show the hardness of the classical constant L1-norm error sampling.

TM is supported by the JST ACT-I, the JSPS Grantin-Aid for Young Scientists (B) No.26730003, and the MEXT JSPS Grant-in-Aid for Scientific Research on Innovative Areas No.15H00850. YT is supported by the Program for Leading Graduate Schools: Interactive Materials Science Cadet Program. MH is supported in part by Fund for the Promotion of Joint International Research (Fostering Joint International Research (Fostering Joint International Research (B) No.15KK0007, the JSPS MEXT Grant-in-Aid for Scientific Research (B) No.16KT0017, the Okawa Research Grant and Kayamori Foundation of Information Science Advancement.

- * Electronic address: morimae@gunma-u.ac.jp
- † Electronic address: takeuchi@qi.mp.es.osaka-u.ac.jp
- ‡ Electronic address: masahito@math.nagoya-u.ac.jp
- R. Raussendorf and H. J. Briegel, A one-way quantum computer. Phys. Rev. Lett. 86, 5188 (2001).
- [2] G. K. Brennen and A. Miyake, Measurement-based quantum computer in the gapped ground state of a two-body Hamiltonian. Phys. Rev. Lett. 101, 010502 (2008).
- [3] T. C. Wei, I. Affleck, and R. Raussendorf, Affleck-Kennedy-Lieb-Tasaki state on a honeycomb lattice is a universal quantum computational resource. Phys. Rev. Lett. 106, 070501 (2011).
- [4] A. Miyake, Quantum computational capability of a 2D valence bond solid phase. Ann. Phys. 326, 1656 (2011).
- [5] J. Cai, A. Miyake, W. Dür, and H. J. Briegel, Universal quantum computer from a quantum magnet. Phys. Rev. A 82, 052309 (2010).
- [6] A. Miyake, Quantum computation on the edge of a symmetry-protected topological order. Phys. Rev. Lett. 105, 040501 (2010).
- [7] A. C. Doherty and S. D. Bartlett, Identifying phases of quantum many-body systems that are universal for quantum computation. Phys. Rev. Lett. 103, 020506 (2009).

- [8] Y. Li, D. E. Browne, L. C. Kwek, R. Raussendorf, and T. C. Wei, Thermal states as universal resources for quantum computation with always-on interactions. Phys. Rev. Lett. 107, 060501 (2011).
- [9] D. V. Else, I. Schwarz, S. D. Bartlett, and A. C. Doherty, Symmetry-protected phases for measurement-based quantum computation. Phys. Rev. Lett. 108, 240505 (2012).
- [10] J. M. Cai, W. Dür, M. Van den Nest, A. Miyake, and H. J. Briegel, Quantum computation in correlation space and extremal entanglement. Phys. Rev. Lett. 103, 050503 (2009).
- [11] K. Fujii and T. Morimae, Topologically protected measurement-based quantum computation on the thermal state of a nearest-neighbor two-body Hamiltonian with spin-3/2 particles. Phys. Rev. A 85, 010304(R) (2012).
- [12] K. Fujii, Y. Nakata, M. Ozeki, and M. Murao, Measurement-based quantum computation on symmetry breaking thermal states. Phys. Rev. Lett. 110, 120502 (2013).
- [13] J. Miller and A. Miyake, Resource quality of a symmetryprotected topologically ordered phase for quantum computation. Phys. Rev. Lett. 114, 120506 (2015).
- [14] T. Griffin and S. D. Bartlett, Spin lattices with two-body Hamiltonians for which the ground state encodes a cluster state. Phys. Rev. A 78, 062306 (2008).
- [15] A. S. Darmawan, G. K. Brennen, and S. D. Bartlett, Measurement-based quantum computation in a twodimensional phase of matter. New J. Phys. 14, 013023 (2012).
- [16] D. Jennings, A. Dragan, S. D. Barrett, S. D. Bartlett, and T. Rudolph, Quantum computation via measurements on the low-temperature state of a many-body system. Phys. Rev. A 80, 032328 (2009).
- [17] D. Gross and J. Eisert, Novel schemes for measurement-based quantum computation. Phys. Rev. Lett. 98, 220503 (2007).
- [18] M. J. Bremner, R. Jozsa, and D. J. Shepherd, Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. Proc. R. Soc. A 467, 459 (2011).
- [19] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Average-case complexity versus approximate simulation of commuting quantum computations. Phys. Rev. Lett. 117, 080501 (2016).
- [20] K. Fujii and T. Morimae, Quantum commuting circuits and complexity of Ising partition functions. arXiv:1311.2128
- [21] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, Power of quantum computation with few clean qubits. Proceedings of 43rd International Colloquium on Automata, Languages, and Programming (ICALP2016), pp.13:1-13:14 (2016).
- [22] S. Aaronson and A. Arkhipov, The computational complexity of linear optics. Theory of Computing 9, 143 (2013).
- [23] A. P. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. L. O'Brien, and T. C. Ralph, Boson sampling from a Gaussian state. Phys. Rev. Lett. 113, 100502 (2014).
- [24] T. Morimae, K. Fujii, and J. F. Fitzsimons, Hardness of classically simulating the one clean qubit model. Phys. Rev. Lett. 112, 130502 (2014).
- [25] A. Broadbent, J. F. Fitzsimons, and E. Kashefi, Univer-

- sal blind quantum computation. Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, 517 (2009).
- [26] J. F. Fitzsimons and E. Kashefi, Unconditionally verifiable blind computation. arXiv:1203.5217
- [27] T. Morimae and K. Fujii, Blind quantum computation protocol in which Alice only makes measurements. Phys. Rev. A 87, 050301(R) (2013).
- [28] M. Hayashi and T. Morimae, Verifiable measurementonly blind quantum computing with stabilizer testing. Phys. Rev. Lett. 115, 220502 (2015).
- [29] T. Morimae, D. Nagaj, and N. Schuch, Quantum proofs can be verified using only single qubit measurements. Phys. Rev. A 93, 022326 (2016).
- [30] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems. Nature 496, 456 (2013).
- [31] M. McKague, Interactive proofs for BQP via self-tested graph states. Theory of Computing 12, 1 (2016).
- [32] Z. Ji, Classical verification of quantum proofs. arXiv:1505.07432
- [33] If a BQP problem is mapped to a local Hamiltonian problem, Pauli measurements are enough to do the verified computation. However, there are two problems for the idea. First, the server needs to generate somehow complicated states, so called Kitaev-Feynmann history states. Second, it is no longer blind, since the server has to know the program and input to generate Kitaev-Feynmann history states. Another idea would be to embed magic states in the graph state in advance. Pauli measurements are enough for universal quantum computing on such "magic-state-embedded" graph states. However, the verification of them seems to be more complicated, since we have to verify both the graph state and magic states at the same time.
- [34] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, Quantum hypergraph states. New J. Phys. 15, 113022 (2013).
- [35] M. Gachechiladze, C. Budroni, and O. Gühne, Extreme violation of local realism in quantum hypergraph states. Phys. Rev. Lett. 116, 070401 (2016).
- [36] O. Gühne, M. Cuquet, F. E. S. Steinhoff, T. Moroder, M. Rossi, D. Bruß, B. Kraus, and C. Macchiavello, Entanglement and nonclassical properties of hypergraph states. J. Phys. A: Math. Theor. 47, 335303 (2014).
- [37] X. Chen and L. Wang, Locally inequivalent four-qubit hypergraph states. J. Phys. A: Math. Theor. 47, 415304 (2014).
- [38] D. W. Lyons, D. J. Upchurch, S. N. Walck, and C. D. Yetter, Local unitary symmetries of hypergraph states. J. Phys. A: Math. Theor. 48, 095301 (2015).
- [39] J. Miller and A. Miyake, Hierarchy of universal entanglement in 2D measurement-based quantum computation. npj Quantum Information 2, 16036 (2016).
- [40] If r = poly, then $p_{\text{test},i} = \frac{1}{2} + O(2^{-poly})$, which means that exponentially many measurements are required to gain useful information about $\text{Tr}(\rho g_i)$. Therefore, our verification method cannot be used if r = poly. For many applications, however, r = const., such as the Union Jack states. It is an open problem whether we can verify hypergraph states with r = poly.
- [41] K. Li and G. Smith, Quantum de Finetti theorem under fully-one-way adaptive measurements. Phys. Rev. Lett. 114, 160503 (2015).