

Verification of Many-Qubit States


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

¹*Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*

²*Department of Computer Science, Gunma University,
1-5-1 Tenjin-cho, Kiryu-shi, Gunma 376-0052, Japan*

³*JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama 332-0012, Japan*

⁴*Yukawa Institute for Theoretical Physics, Kyoto University,
Kitashirakawa Oiwakecho, Sakyo-ku, Kyoto 606-8502, Japan*

 (Received 2 October 2017; revised manuscript received 9 February 2018; published 7 June 2018)

Verification is a task to check whether a given quantum state is close to an ideal state or not. In this paper, we show that a variety of many-qubit quantum states can be verified with only sequential single-qubit measurements of Pauli operators. First, we introduce a protocol for verifying ground states of Hamiltonians. We next explain how to verify quantum states generated by a certain class of quantum circuits. We finally propose an adaptive test of stabilizers that enables the verification of all polynomial-time-generated hypergraph states, which include output states of the Bremner-Montanaro-Shepherd-type instantaneous quantum polynomial time (IQP) circuits. Importantly, we do not make any assumption that the identically and independently distributed copies of the same states are given: Our protocols work even if some highly complicated entanglement is created among copies in any artificial way. As applications, we consider the verification of the quantum computational supremacy demonstration with IQP models, and verifiable blind quantum computing.

DOI: [10.1103/PhysRevX.8.021060](https://doi.org/10.1103/PhysRevX.8.021060)

Subject Areas: Quantum Physics,
Quantum Information

I. INTRODUCTION

Quantum computing is expected to solve several problems exponentially faster than classical computing, and therefore, realizing universal quantum computers is one of the most central goals in modern quantum information science. Output states of even simpler quantum circuits are also useful. For example, quantum circuits consisting of only Clifford gates, which are actually classically simulatable [1], can generate important resources for quantum metrology [2] and measurement-based quantum computing (MBQC) [3]. Furthermore, it has recently been shown that output states of several subuniversal circuits, such as boson sampling, instantaneous quantum polynomial time (IQP), and deterministic quantum computation with one quantum bit (DQC1), can generate certain probability distributions that cannot be classically efficiently sampled unless the polynomial-time hierarchy collapses [4–21]. Other quantum advantages have also been actively studied [22,23].

Moreover, ground states of Hamiltonians are important. Generating ground states of local Hamiltonians is, in general, quantum Merlin-Arthur (QMA)-hard [24] (which suggests that it is much harder than polynomial-time quantum computing), but several local Hamiltonians offer important quantum abilities with their ground states, such as topologically protected quantum memory [25], adiabatic quantum computing [26], and MBQC [3,27–42]. In this way, many-qubit quantum states are essential resources for quantum information processing.

When an experimentalist generates these many-qubit resource states in his or her own laboratory [Fig. 1(a)], or when a client of cloud quantum computing receives these resource states from a remote server [Fig. 1(b)], it is important to check the correctness of given states [43]. More precisely, let us consider the following game between two people, the verifier and the prover [44]. The prover sends a certain quantum state Φ to the verifier claiming that it is the tensor product of many copies $\rho^{\otimes k}$ of a many-qubit state ρ . The state ρ is an important resource state for the verifier. For example, ρ is a ground state of a Hamiltonian or a resource state of MBQC. However, the prover is not necessarily trusted, and therefore, the verifier has to check the correctness of the given state.

If Φ is guaranteed to be at least the tensor product of many copies $\sigma^{\otimes k}$ of the same state σ , i.e., the states are

*takeuchi@qi.mp.es.osaka-u.ac.jp

†tomoyuki.morimae@yukawa.kyoto-u.ac.jp

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

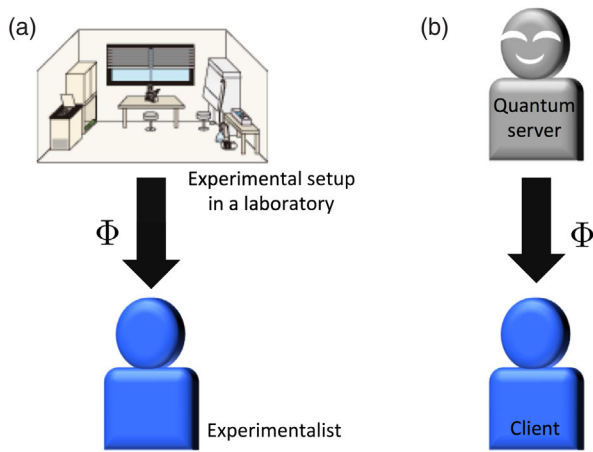


FIG. 1. The prover-verifier game considered in this paper. (a) An experimentalist (verifier) wants to verify the correctness of a state Φ from the experimental setup (prover). (b) In cloud quantum computing of the type of Ref. [45], a client (verifier) asks a remote server (prover) to generate and send a certain quantum many-qubit state Φ . The client wants to verify the correctness of the state sent from the server.

independent and identically distributed (i.i.d.), and if the size of σ is small, the quantum tomography [46] is enough. However, useful resource states are often large-size quantum states, and therefore, the quantum tomography suffers from the exponential blowup. The exponential increase of parameters is somehow mitigated by using the compressed sensing idea, especially for low-rank quantum states [47], but the scaling is, in general, exponential. If we are interested only in the fidelity, by direct fidelity estimation [48] and by using fidelity witnesses [49], we achieve the goal without reconstructing the full state, which is more efficient than quantum tomography.

However, these protocols also assume the i.i.d. property of quantum states. In reality, such an i.i.d. property does not hold. Because of environmental noises, the generated state in a laboratory is not a tensor product of the same states. In cloud quantum computing, moreover, the situation is worse because a malicious prover might generate highly complicated entanglement among samples to fool the verifier. In other words, what the verifier actually receives is not $\rho^{\otimes k}$ but $\mathcal{E}(\rho^{\otimes k})$ with a completely positive and trace-preserving (CPTP) map \mathcal{E} . If $\mathcal{E}(\rho^{\otimes k})$ is a state generated by a well-controlled experimental setup, \mathcal{E} is a time evolution generated by a physically natural Hamiltonian describing the interaction between the system and the environment. If $\mathcal{E}(\rho^{\otimes k})$ is a state given by the server of cloud quantum computing, \mathcal{E} can be any CPTP map [50].

In addition to the non-i.i.d. property of samples, another realistic assumption in verifications is that the verifier's ability is severely limited. (In fact, otherwise the verification task would be trivial. For example, if the verifier can generate the correct state by his or herself, the verification is straightforward by doing the SWAP test between the given state and the correct state generated by him or her [51].) If

the verifier is severely restrictive, the verification is a highly nontrivial problem. For example, can the verifier verify a highly entangled many-qubit state by measuring each qubit individually?

In summary, a verification protocol should satisfy the following three conditions:

- (i) It runs in polynomial time.
- (ii) The i.i.d. property of samples is not assumed.
- (iii) No entangling operation is required for the verifier.

Verification protocols that satisfy these three conditions have been proposed for some specific classes of states, such as graph states [52,53] and hypergraph states with low connectivity [54], including the Union Jack state [55]. Here, hypergraph states are generalizations of graph states by replacing the controlled-Z (CZ) gates of graph states with generalized CZ gates. A generalized CZ gate is a unitary gate that flips the phase ± 1 if and only if all qubits are $|1\rangle$. (See Sec. IV A for the definition of hypergraph states.) We say that a hypergraph state has a low connectivity if the connectivity

$$\xi \equiv \max_{v \in V} \xi_v \quad (1)$$

is constant with respect to $|V|$, where ξ_v is the number of generalized CZ gates acting on the vertex v , V is the set of vertices, and $|V|$ is the size of V .

These protocols, Refs. [52–54], satisfy all the above conditions (i)–(iii). In particular, in these protocols, the verifier only needs sequential single-qubit measurements of Pauli operators. However, these protocols leave the following two problems open:

- (1) Are there other more general classes of states that are verifiable with only sequential single-qubit measurements of Pauli operators? For example, can we verify ground states of Hamiltonians and states generated by general quantum circuits with sequential single-qubit measurements of Pauli operators?
- (2) Can we verify hypergraph states with high connectivity by using only sequential single-qubit measurements of Pauli operators?

Here, high connectivity means that Eq. (1) is polynomial with respect to $|V|$. The second open problem is important for the verification of the quantum computational supremacy demonstration because output states of the Bremner-Montanaro-Shepherd-type IQP circuits [12] are hypergraph states with high connectivity. (See Sec. V for details.)

In this paper, we solve the two open problems by proposing three verification protocols. We first introduce a protocol for verifying ground states of Hamiltonians (Sec. II). We next show a protocol for verifying quantum states generated by a certain class of quantum circuits (Sec. III). As a common technique used in these two verification protocols, we decompose an operator such as a Hamiltonian or a generalized stabilizer into Pauli operators and estimate overlaps between the verified state and Pauli

operators. A similar technique was used in the direct fidelity estimation [48]. We finally explain a verification protocol for hypergraph states with high connectivity (Sec. IV). For the construction of the third protocol, we propose a novel test, which we call the adaptive stabilizer test, by combining the stabilizer test of Ref. [52] with adaptive classical processing. This adaptivity is the key that enables the verification of hypergraph states with high connectivity. The previous protocol [54] is not enough to verify hypergraph states with high connectivity. The adaptive classical processing we introduce in Secs. IV B and IV C is the key idea to realize a verification protocol for hypergraph states with high connectivity.

The validness of our protocols is demonstrated by showing their completeness and soundness. Roughly speaking, if the verifier accepts the ideal quantum state with high probability, we say that the verification protocol has the completeness. On the other hand, if the protocol guarantees that a quantum state passing the verification protocol is close to the ideal state with high probability, we say that the protocol has the soundness. The precise statements are given later as theorems.

In Sec. V, we discuss applications of our protocols to the verification of quantum computational supremacy demonstrations with the IQP model and its variants. We also consider an application to verifiable blind quantum computing. Sections VI and VII are devoted to the discussion and the conclusion, respectively.

Note that in addition to Refs. [52–54] and the present paper, other papers have proposed verification protocols for quantum computational supremacy demonstrations. Hangleiter *et al.* have proposed a polynomial-time verification protocol for ground states of frustration-free Hamiltonians [56]. A disadvantage of this protocol when it is used for the verification of quantum computing is that the Feynman-Kitaev history state [24,57] corresponding to the quantum circuit, which is more complicated than the mere output state of the circuit, has to be generated. Furthermore, their verification protocol requires multiqubit measurements. Based on the verification protocol of Ref. [56], Gao *et al.* [14] and Bermejo-Vega *et al.* [15] have proposed verification protocols for quantum computational supremacy demonstrations of their architectures. Miller *et al.* [16] have proposed a polynomial-time verification protocol for the output states of the Bremner-Montanaro-Shepherd-type IQP circuits [12]. Their protocol is a special case of our third protocol when the target state is restricted to hypergraph states. With respect to the boson sampling model [4], a verification protocol has already been proposed [58], but this protocol requires at most exponentially many copies of a verified quantum state. As a common drawback of all these protocols [14–16,56,58], they assume the i.i.d. property of samples.

All verification protocols introduced above and our present protocols require the ability of the verifier to make

measurements. On the other hand, there are complement protocols where a verifier is required to prepare quantum states [59,60]. The protocol in Ref. [59] uses trap qubits [61,62] to perform verified quantum computational supremacy demonstrations for an Ising sampler [14] or an IQP circuit [10–12], and does not assume the i.i.d. property. The protocol in Ref. [60] can verify that the server has the ability to sample from an IQP circuit. For some experimental setups, measurements are easier than preparations, and vice versa for other experimental setups. Therefore, at this moment, we do not know which approach is better.

II. VERIFICATION OF GROUND STATES OF HAMILTONIANS

In this section, we explain our verification protocol for ground states of Hamiltonians. In Sec. II A, we define a test. In Sec. II B, we explain how to verify ground states by using the test.

A. Test

Let H be an N -qubit Hamiltonian. We want to verify its ground state corresponding to the ground energy E_0 . Let $\Delta (> 0)$ be a lower bound of the energy gap, i.e., $E_1 - E_0 \geq \Delta$, where E_1 is the first excitation energy. From H , we define a rescaled Hamiltonian

$$H' \equiv \frac{H - E_0 I^{\otimes N}}{\Delta}. \quad (2)$$

Since H' is Hermitian, if we decompose H' in the Pauli basis as

$$H' = \sum_{i=0}^h c_i \tau_i, \quad (3)$$

c_i is a real number, where $h = 4^N - 1$,

$$\tau_i \equiv \bigotimes_{j=1}^N \sigma_{ij},$$

$\sigma_{ij} \in \{I, X, Y, Z\}$, and $\tau_0 \equiv I^{\otimes N}$. From Eq. (2), the ground energy of H' is 0. Accordingly,

$$c_0 = c_0 \frac{\text{Tr}[I^{\otimes N}]}{2^N} + \sum_{i=1}^h c_i \frac{\text{Tr}[\tau_i]}{2^N} = \text{Tr} \left[H' \frac{I^{\otimes N}}{2^N} \right] \geq 0. \quad (4)$$

Hereafter, we consider Hamiltonians that satisfy the following three conditions:

- (i) The probability distribution from $\{|c_i|/R\}_{i=0}^h$ can be sampled exactly in polynomial time. Here, $R \equiv \sum_{i=0}^h |c_i|$.
- (ii) $R = O(\text{poly}(N))$.

(iii) R is known or can be computed in polynomial time. Condition (i) is necessary to perform the test defined in the next paragraph. Condition (ii) is required to extract the information of $\text{Tr}[\rho H']$ from p_{pass} in Eq. (5) using only the polynomial number of quantum states ρ . Condition (iii) is needed to define the accept or reject criteria in Eq. (6). Note that it is obvious that for the usual Hamiltonians in condensed matter physics, such as Ising models and Heisenberg models, these conditions are satisfied if the energy gap is constant or polynomially decays. On the other hand, if the energy gap exponentially decays, then condition (ii) is not satisfied. In fact, for a Hamiltonian $H = \sum_{i=1}^h d_i \tau_i$ with $|d_i| \leq \text{const}$ and $h = O(\text{poly}(N))$,

$$R = \frac{\sum_{i=1}^h |d_i| + |E_0|}{\Delta} \geq \frac{\sum_{i=1}^h |d_i|}{\Delta} = O(2^{\text{poly}(N)}).$$

The test on an N -qubit quantum state ρ is defined as follows: The verifier selects i with probability $|c_i|/R$. If the verifier selects i , the verifier measures the j th qubit of ρ in the Pauli basis σ_{ij} . Let $m_j \in \{1, -1\}$ be the outcome of the measurement on the j th qubit. Note that if $\sigma_{ij} = I$, the verifier sets $m_j = 1$. We say that the verifier passes the test on ρ if

$$\prod_{j=1}^N m_j = \text{sgn}(c_i).$$

Here, $\text{sgn}(\cdot)$ is the sign function.

The expected probability p_{pass} that the verifier passes the test on ρ , where the expectation is taken over the sampling of i , is

$$\begin{aligned} p_{\text{pass}} &= \frac{|c_0|}{R} + \sum_{i=1}^h \frac{|c_i|}{R} \text{Tr} \left[\rho \frac{I^{\otimes N} + \text{sgn}(c_i) \tau_i}{2} \right] \\ &= \frac{|c_0|}{R} \text{Tr} \left[\rho \frac{I^{\otimes N} + \text{sgn}(c_0) I^{\otimes N}}{2} \right] \\ &\quad + \sum_{i=1}^h \frac{|c_i|}{R} \text{Tr} \left[\rho \frac{I^{\otimes N} + \text{sgn}(c_i) \tau_i}{2} \right] \\ &= \frac{1}{2} + \frac{\text{Tr}[\rho H']}{2R}, \end{aligned} \quad (5)$$

where we have used Eqs. (4) and (3) to derive the second and the last equalities, respectively. Note that in order to relate p_{pass} to $\text{Tr}[\rho H']$, $i = 0$ is included in the test.

B. Verification

In this subsection, we propose a verification protocol for ground states based on the test explained in the previous subsection. Our protocol runs as follows:

- (1) The prover sends the verifier an $N(k+m+1)$ -qubit state ρ_B [see Fig. 2(a)]. The state ρ_B consists of

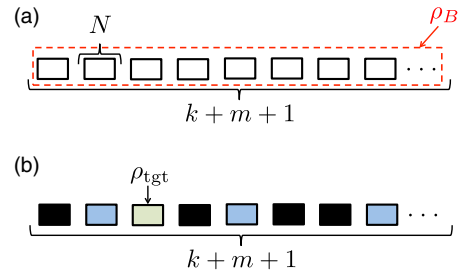


FIG. 2. (a) The quantum state ρ_B in step 1. Each rectangle represents a register that stores N qubits, and ρ_B consists of $k+m+1$ registers. If the prover is honest, the state of each register is the ideal quantum state. On the other hand, if the prover is malicious, registers may be entangled with each other. (b) A quantum state in step 2. Randomly chosen black registers are discarded, and then the remaining m blue registers and one green register become close to i.i.d. samples because of the quantum de Finetti theorem [63]. Randomly chosen m blue registers are used for the test. The green register is the target state ρ_{tgt} .

$k+m+1$ registers, and each register stores N qubits. If the prover is honest, the prover sends the tensor product of the ideal state. On the other hand, if the prover is malicious, the prover sends an $N(k+m+1)$ -qubit, completely arbitrary, quantum state instead of the tensor product of the ideal state.

- (2) The verifier chooses m registers uniform randomly and discards them to guarantee that the remaining $N(k+1)$ -qubit state ρ'_B is close to an i.i.d. sample by using the quantum de Finetti theorem [63]. Next, the verifier chooses one register—which we call the target register, whose state is ρ_{tgt} —uniform randomly and uses it for the verifier's purpose. The verifier performs the test on each of the remaining k registers [see Fig. 2(b)]. Let K_{pass} be the number of times that the verifier passes the test. If

$$\frac{K_{\text{pass}}}{k} \leq \frac{1}{2} + \frac{\epsilon}{2R}, \quad (6)$$

we say that the verifier accepts the prover, where $0 < \epsilon < 1$ is specified later.

Note that since the random selection is equivalent to random permutation of registers, ρ_B becomes permutation invariant after the random selection in step 2. Accordingly, we can use the quantum de Finetti theorem [63]. This idea comes from Ref. [54]. Hereafter, we consider the case where $\epsilon = 1/(4N^2)$, $m \geq 2N^5 k^2 \log 2$, and $k \geq 32R^2 N^5$ are satisfied. In this case, the following theorems hold.

Theorem 1 (Completeness). If the prover is honest, i.e., the state of each register is a ground state of H , the probability that the verifier accepts the prover is larger than $1 - e^{-N}$.

Proof.—When the state of each register is a ground state of H , $p_{\text{pass}} = 1/2$. Because of the Hoeffding inequality,

$\Pr[\text{the verifier accepts the prover}]$

$$\begin{aligned} &= 1 - \Pr\left[\frac{K_{\text{pass}}}{k} > \frac{1}{2} + \frac{\epsilon}{2R}\right] \\ &= 1 - \Pr\left[\frac{K_{\text{pass}}}{k} > p_{\text{pass}} + \frac{\epsilon}{2R}\right] \\ &\geq 1 - e^{-2\epsilon^2 k / (4R^2)} \\ &\geq 1 - e^{-N}. \quad \blacksquare \end{aligned}$$

Theorem 2 (Soundness). If the verifier accepts the prover, the state ρ_{tgt} of the target register satisfies

$$\text{Tr}[\Pi \rho_{\text{tgt}}] \geq 1 - \frac{1}{N}$$

with a probability larger than $1 - 1/N$. Here, Π is the projector onto the ground-energy eigenspace of H , and we consider the case where $N \neq 2$.

Proof.—Let $\Pi^\perp \equiv I^{\otimes N} - \Pi$, and T be the positive-operator-valued-measure (POVM) element corresponding to the event where the verifier accepts the prover. When $N \neq 2$, we can show that for any N -qubit state ρ ,

$$\text{Tr}[(T \otimes \Pi^\perp) \rho^{\otimes k+1}] \leq \frac{1}{2N^2}. \quad (7)$$

Its proof is given later. Because of the quantum de Finetti theorem [for the fully one-way local operations and classical communication (LOCC) norm] [63] and Eq. (7),

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp) \rho'_B] &\leq \text{Tr}\left[(T \otimes \Pi^\perp) \int d\mu \rho^{\otimes k+1}\right] \\ &\quad + \frac{1}{2} \sqrt{\frac{2Nk^2 \log 2}{m}} \\ &\leq \frac{1}{2N^2} + \frac{1}{2N^2} = \frac{1}{N^2}. \end{aligned}$$

Here, μ is a probability measure on ρ . We have

$$\text{Tr}[(T \otimes \Pi^\perp) \rho'_B] = \text{Tr}[(T \otimes I) \rho'_B] \text{Tr}[\Pi^\perp \rho_{\text{tgt}}].$$

Therefore, if

$$\text{Tr}[\Pi^\perp \rho_{\text{tgt}}] > \frac{1}{N},$$

then

$$\text{Tr}[(T \otimes I) \rho'_B] < \frac{1}{N}.$$

This means that if the verifier accepts the prover,

$$\text{Tr}[\Pi \rho_{\text{tgt}}] \geq 1 - \frac{1}{N}$$

with a probability larger than $1 - 1/N$.

To complete the proof, we show Eq. (7). First, we consider the case where $\text{Tr}[H'\rho] \leq 2\epsilon$. Let $\{|E'_i\rangle, E'_i\}_i$ be

the set of excited eigenstates of H' and their eigenvalues. Since $E'_i \geq 1$,

$$\begin{aligned} \text{Tr}[\Pi^\perp \rho] &= \sum_i \langle E'_i | \rho | E'_i \rangle \\ &\leq \sum_i E'_i \langle E'_i | \rho | E'_i \rangle \\ &= \text{Tr}[H'\rho] \leq 2\epsilon. \end{aligned}$$

Therefore,

$$\text{Tr}[(T \otimes \Pi^\perp) \rho^{\otimes k+1}] = \text{Tr}[T \rho^{\otimes k}] \text{Tr}[\Pi^\perp \rho] \leq \frac{1}{2N^2}. \quad (8)$$

Next, we consider the case where $\text{Tr}[\rho H'] > 2\epsilon$. In this case,

$$p_{\text{pass}} = \frac{1}{2} + \frac{\text{Tr}[\rho H']}{2R} > \frac{1}{2} + \frac{\epsilon}{R}.$$

Therefore, because of the Hoeffding inequality,

$$\begin{aligned} \text{Tr}[T \rho^{\otimes k}] &= \Pr\left[\frac{K_{\text{pass}}}{k} \leq \frac{1}{2} + \frac{\epsilon}{2R}\right] \\ &\leq \Pr\left[\frac{K_{\text{pass}}}{k} < p_{\text{pass}} - \frac{\epsilon}{2R}\right] \\ &\leq e^{-2\epsilon^2 k / (4R^2)} \\ &\leq e^{-N}. \end{aligned}$$

Hence,

$$\text{Tr}[(T \otimes \Pi^\perp) \rho^{\otimes k+1}] = \text{Tr}[T \rho^{\otimes k}] \text{Tr}[\Pi^\perp \rho] \leq e^{-N}. \quad (9)$$

From Eqs. (8) and (9), when $N \neq 2$,

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp) \rho^{\otimes k+1}] &\leq \max\left(\frac{1}{2N^2}, e^{-N}\right) \\ &= \frac{1}{2N^2}. \quad \blacksquare \end{aligned}$$

III. VERIFICATION OF QUANTUM STATES GENERATED BY A CERTAIN CLASS OF QUANTUM CIRCUITS

In this section, we explain our second verification protocol, namely, the protocol for quantum states generated by a certain class of quantum circuits. In Sec. III A, we explain a stabilizer test. In Sec. III B, we show the verification protocol based on the stabilizer test.

A. Stabilizer test

Let us assume that we want to verify the quantum state $|\psi\rangle \equiv U|+\rangle^{\otimes N}$, where $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$, and U is a certain N -qubit unitary operator whose properties are specified later. The i th stabilizer g_i of $|\psi\rangle$ is defined by

$$g_i \equiv UX_iU^\dagger, \quad (10)$$

where X_i is performed on the i th qubit of $|\psi\rangle$. Note that g_i is not necessarily a tensor product of Pauli operators, and therefore, it should be considered as a ‘‘generalized stabilizer.’’ From Eq. (10),

$$\prod_{i=1}^N \frac{I^{\otimes N} + g_i}{2} = |\psi\rangle\langle\psi|.$$

Since g_i is Hermitian, if we decompose g_i in the Pauli basis as

$$g_i = \sum_j c_j^{(i)} \tau_j,$$

$c_j^{(i)}$ is a real number, where

$$\tau_j \equiv \bigotimes_{k=1}^N \sigma_{j|k},$$

and $\sigma_{j|k} \in \{I, X, Y, Z\}$. Hereafter, we consider the U that satisfies the following three conditions:

- (i) The probability distribution from $\{|c_j^{(i)}|/R_i\}_j$ can be sampled exactly in polynomial time. Here, $R_i \equiv \sum_j |c_j^{(i)}|$.
- (ii) $R \equiv \max(R_1, \dots, R_N) = O(\text{poly}(N))$.
- (iii) R_i is known or can be computed in polynomial time for all i .

Condition (i) is necessary to perform the stabilizer test defined in the next paragraph. Condition (ii) is required to extract the information of $\text{Tr}[\rho g_i]$ from $p_{\text{pass}}(i)$ in Eq. (11) using only the polynomial number of quantum states ρ . Condition (iii) is needed to define the accept or reject criteria in Eq. (12).

The stabilizer test for g_i on ρ is defined as follows: The verifier selects j with probability $|c_j^{(i)}|/R_i$. The verifier measures the k th qubit of ρ in the Pauli basis $\sigma_{j|k}$. Let $m_k \in \{1, -1\}$ be the outcome of the measurement on the k th qubit. Note that if $\sigma_{j|k} = I$, the verifier sets $m_k = 1$. We say that the verifier passes the stabilizer test for g_i on ρ if

$$\prod_{k=1}^N m_k = \text{sgn}(c_j^{(i)}).$$

Since quantum states satisfying the above three properties include graph states and hypergraph states with low

connectivity as special cases, our stabilizer test can be considered as a generalization of previous stabilizer tests [52,54].

The expected probability $p_{\text{pass}}(i)$ that the verifier passes the stabilizer test for g_i on ρ , where the expectation is taken over the sampling of j , is

$$\begin{aligned} p_{\text{pass}}(i) &= \sum_j \frac{|c_j^{(i)}|}{R_i} \text{Tr} \left[\rho \frac{I^{\otimes N} + \text{sgn}(c_j^{(i)}) \tau_j}{2} \right] \\ &= \frac{1}{2} + \frac{\text{Tr}[\rho g_i]}{2R_i}. \end{aligned} \quad (11)$$

B. Verification

In this subsection, we propose a verification protocol for $|\psi\rangle = U|+\rangle^{\otimes N}$. Our protocol runs as follows:

- (1) The prover sends the verifier an $N(Nk + m + 1)$ -qubit state ρ_B . The state ρ_B consists of $Nk + m + 1$ registers, and each register stores N qubits. If the prover is honest, the prover sends $|\psi\rangle^{\otimes Nk+m+1}$. On the other hand, if the prover is malicious, the prover sends an $N(Nk + m + 1)$ -qubit, completely arbitrary, quantum state instead of $|\psi\rangle^{\otimes Nk+m+1}$.
- (2) The verifier chooses m registers uniform randomly and discards them to guarantee that the remaining $N(Nk + 1)$ -qubit state ρ'_B is close to an i.i.d. sample by using the quantum de Finetti theorem [63]. Next, the verifier chooses one register—which we call the target register, whose state is ρ_{tgt} —uniform randomly and uses it for the verifier’s purpose. The remaining Nk registers are divided into N groups such that which register is assigned to the i th group is uniformly random. The verifier performs the stabilizer test for g_i on every register in the i th group. Let K_i be the number of times that the verifier passes the stabilizer test for g_i . If

$$\frac{K_i}{k} \geq \frac{1}{2} + \frac{1 - \epsilon}{2R_i}, \quad (12)$$

we say that the verifier passes the stabilizer test for the i th group, where $0 < \epsilon < 1$ is specified later. If the verifier passes the stabilizer test for all i , we say that the verifier accepts the prover.

Hereafter, we consider the case where $\epsilon = 1/(2N^3)$, $m \geq 2N^7 k^2 \log 2$, and $k \geq 8R^2 N^7$ are satisfied. In this case, the following theorems hold.

Theorem 3 (Completeness). If the prover is honest, i.e., the state of each register is $|\psi\rangle$, the probability that the verifier accepts the prover is larger than $1 - Ne^{-N}$.

Proof.—When the state of each register is $|\psi\rangle$,

$$p_{\text{pass}}(i) = \frac{1}{2} + \frac{1}{2R_i}.$$

Because of the union bound and the Hoeffding inequality,

$$\begin{aligned} & \Pr[\text{the verifier accepts the prover}] \\ &= \Pr\left[\bigwedge_{i=1}^N \left(\frac{K_i}{k} \geq \frac{1}{2} + \frac{1-\epsilon}{2R_i}\right)\right] \\ &\geq 1 - \sum_{i=1}^N \Pr\left[\frac{K_i}{k} < p_{\text{pass}}(i) - \frac{\epsilon}{2R_i}\right] \\ &\geq 1 - \sum_{i=1}^N e^{-2\epsilon^2 k / (4R_i^2)} \\ &\geq 1 - N e^{-2\epsilon^2 k / (4R^2)} \\ &\geq 1 - N e^{-N}. \quad \blacksquare \end{aligned}$$

Theorem 4 (Soundness). If the verifier accepts the prover, the state ρ_{tgt} of the target register satisfies

$$\langle \psi | \rho_{\text{tgt}} | \psi \rangle \geq 1 - \frac{1}{N}$$

with a probability larger than $1 - 1/N$. Here, we consider the case where $N \neq 2$.

Proof.—Let Π^\perp be the N -qubit projector $I^{\otimes N} - |\psi\rangle\langle\psi|$, and T be the POVM element corresponding to the event where the verifier accepts the prover. When $N \neq 2$, we can show that for any N -qubit state ρ ,

$$\text{Tr}[(T \otimes \Pi^\perp) \rho^{\otimes Nk+1}] \leq \frac{1}{2N^2}. \quad (13)$$

Its proof is given later. Because of the quantum de Finetti theorem (for the fully one-way LOCC norm) [63] and Eq. (13),

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp) \rho'_B] &\leq \text{Tr}\left[(T \otimes \Pi^\perp) \int d\mu \rho^{\otimes Nk+1}\right] \\ &\quad + \frac{1}{2} \sqrt{\frac{2N^3 k^2 \log 2}{m}} \\ &\leq \frac{1}{2N^2} + \frac{1}{2N^2} = \frac{1}{N^2}. \end{aligned}$$

Here, μ is a probability measure on ρ . We have

$$\text{Tr}[(T \otimes \Pi^\perp) \rho'_B] = \text{Tr}[(T \otimes I) \rho'_B] \text{Tr}[\Pi^\perp \rho_{\text{tgt}}].$$

Therefore, if

$$\text{Tr}[\Pi^\perp \rho_{\text{tgt}}] > \frac{1}{N},$$

then

$$\text{Tr}[(T \otimes I) \rho'_B] < \frac{1}{N}.$$

This means that if the verifier accepts the prover,

$$\langle \psi | \rho_{\text{tgt}} | \psi \rangle \geq 1 - \frac{1}{N}$$

with a probability larger than $1 - 1/N$.

To complete the proof, we show Eq. (13). First, we consider the case where $\text{Tr}[g_i \rho] \geq 1 - 2\epsilon$ is satisfied for all i . From the union bound,

$$\begin{aligned} 1 - \langle \psi | \rho | \psi \rangle &= 1 - \text{Tr}\left[\rho \prod_{i=1}^N \frac{I^{\otimes N} + g_i}{2}\right] \\ &\leq \sum_{i=1}^N \left(1 - \text{Tr}\left[\rho \frac{I^{\otimes N} + g_i}{2}\right]\right) \\ &\leq N\epsilon. \end{aligned}$$

Therefore,

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp) \rho^{\otimes Nk+1}] &= \text{Tr}[T \rho^{\otimes Nk}] \text{Tr}[\Pi^\perp \rho] \\ &\leq \frac{1}{2N^2}. \end{aligned} \quad (14)$$

Next, we consider the case where $\text{Tr}[g_i \rho] < 1 - 2\epsilon$ is satisfied for at least one i . In this case, for the i' that satisfies $\text{Tr}[g_{i'} \rho] < 1 - 2\epsilon$,

$$p_{\text{pass}}(i') = \frac{1}{2} + \frac{\text{Tr}[g_{i'} \rho]}{2R_{i'}} < \frac{1}{2} + \frac{1 - 2\epsilon}{2R_{i'}}.$$

Therefore, because of the Hoeffding inequality,

$$\begin{aligned} \text{Tr}[T \rho^{\otimes Nk}] &\leq \Pr\left[\frac{K_{i'}}{k} \geq \frac{1}{2} + \frac{1-\epsilon}{2R_{i'}}\right] \\ &\leq \Pr\left[\frac{K_{i'}}{k} > p_{\text{pass}}(i') + \frac{\epsilon}{2R_{i'}}\right] \\ &\leq e^{-2\epsilon^2 k / (4R_{i'}^2)} \\ &\leq e^{-2\epsilon^2 k / (4R^2)} \\ &\leq e^{-N}. \end{aligned}$$

Hence,

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp) \rho^{\otimes Nk+1}] &= \text{Tr}[T \rho^{\otimes Nk}] \text{Tr}[\Pi^\perp \rho] \\ &\leq e^{-N}. \end{aligned} \quad (15)$$

From Eqs. (14) and (15), when $N \neq 2$,

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp)\rho^{\otimes Nk+1}] &\leq \max\left(\frac{1}{2N^2}, e^{-N}\right) \\ &= \frac{1}{2N^2}. \quad \blacksquare \end{aligned}$$

IV. VERIFICATION OF HYPERGRAPH STATES

Although the verification protocol proposed in Sec. III can verify hypergraph states with low connectivity, it cannot verify hypergraph states with high connectivity. To verify hypergraph states with high connectivity, we now explain our third protocol, which uses a new adaptive stabilizer test. In Sec. IV A, we review the definition of hypergraph states. In Sec. IV B, we explain our basic idea with a simple example. In Sec. IV C, we define the adaptive stabilizer test in a general form. In Sec. IV D, we explain how to verify hypergraph states with high connectivity by using the adaptive stabilizer test.

A. Hypergraph states

In this subsection, we review the definition of hypergraph states [64] and their properties. A hypergraph $G \equiv (V, E)$ is a pair of a set V of vertices and a set E of hyperedges, where a hyperedge is a set of vertices. We define $N \equiv |V|$. The hypergraph state $|G\rangle$ corresponding to the hypergraph G is defined by

$$|G\rangle \equiv \left(\prod_{e \in E} \widetilde{CZ}_e \right) |+\rangle^{\otimes N},$$

where \widetilde{CZ}_e is the generalized CZ gate acting on vertices in e ; i.e., it is the gate that flips the phase ± 1 if all qubits in e are $|1\rangle$. Since a hypergraph has at most $2^N - 1$ hyperedges, the time required to generate a hypergraph state is at most $O(2^N)$. However, in many quantum-information processing protocols, only quantum states that can be generated in polynomial time are used. To focus on such efficiently generatable quantum states, we assume that $2 \leq |e| \leq c$ for all $e \in E$, where $|e|$ is the size of e . Here, $c (\geq 3)$ is a constant integer. The size $|E|$ of E is then polynomially upper bounded:

$$|E| \leq \sum_{k=2}^c \binom{N}{k} = O(N^c).$$

The i th stabilizer g_i of $|G\rangle$ ($i = 1, 2, \dots, N$) is defined by

$$g_i \equiv \left(\prod_{e \in E} \widetilde{CZ}_e \right) X_i \left(\prod_{e \in E} \widetilde{CZ}_e \right), \quad (16)$$

where X_i is the Pauli- X operator acting on the i th qubit. We can show the useful relation

$$\prod_{i=1}^N \frac{I^{\otimes N} + g_i}{2} = |G\rangle\langle G|,$$

which is derived by applying $\prod_{e \in E} \widetilde{CZ}_e$ from both the right and the left on both sides of the trivial equation

$$\prod_{i=1}^N \frac{I + X_i}{2} = |+\rangle\langle +|^{\otimes N},$$

and by using Eq. (16).

B. Simple example

Before introducing the general formalism of our adaptive stabilizer test, here we briefly explain our basic idea with a simple example. Let us consider the three-qubit hypergraph state,

$$\begin{aligned} |G\rangle &= \widetilde{CZ}_{1,2,3} |+\rangle^{\otimes 3} \\ &= \frac{(|00\rangle + |01\rangle + |10\rangle)_{1,2} |+\rangle_3 + |11\rangle_{1,2} |-\rangle_3}{2}, \end{aligned}$$

where $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$. From the definition Eq. (16), its stabilizers are calculated as

$$\begin{aligned} g_1 &= \sum_{a \in \{0,1\}} X \otimes |a\rangle\langle a| \otimes Z^a, \\ g_2 &= \sum_{a \in \{0,1\}} |a\rangle\langle a| \otimes X \otimes Z^a, \\ g_3 &= \sum_{a \in \{0,1\}} |a\rangle\langle a| \otimes Z^a \otimes X. \end{aligned}$$

The adaptive stabilizer test for g_1 on a three-qubit quantum state ρ proceeds as follows:

- (1) The verifier measures the first qubit of ρ in the X basis. Let $x_1 \in \{1, -1\}$ be the measurement result.
- (2) The verifier measures the second and third qubits in the Z bases. Let $z_j \in \{1, -1\}$ ($j = 2, 3$) be the measurement result for the j th qubit.
- (3) If $z_2 = 1$ and $x_1 = 1$, the verifier accepts. If $z_2 = -1$ and $x_1 z_3 = 1$, the verifier accepts. Otherwise, the verifier rejects.

It is easy to check that the acceptance probability p_{pass} of this test is

$$p_{\text{pass}} = \text{Tr} \left[\rho \frac{I^{\otimes 3} + g_1}{2} \right].$$

(The intuitive idea is illustrated in Fig. 3. When $z_2 = 1$, the three-qubit hypergraph state $|G\rangle$ becomes $|+\rangle_1 \otimes |+\rangle_3$. When $z_2 = -1$, it becomes the two-qubit graph state that is stabilized by $X_1 Z_3$.) Therefore, the correct state $|G\rangle$ passes the test with probability 1. We will see later that the

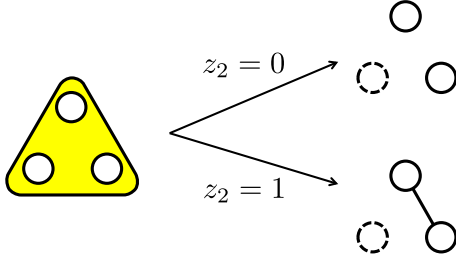


FIG. 3. A quantum state after the Z_2 -basis measurement on $|G\rangle$. Solid-line and dashed-line circles represent $|+\rangle$ and a measured qubit, respectively. The yellow triangle and the black solid line represent $\widetilde{CZ}_{1,2,3}$ and $\widetilde{CZ}_{1,3}$, respectively.

estimation of p_{pass} (and therefore the estimation of $\text{Tr}[g_1\rho]$) is possible in our verification protocol. With respect to g_2 and g_3 , a similar argument holds.

C. Adaptive stabilizer test

For general polynomial-time-generated hypergraph states, we define the adaptive stabilizer test for g_i using the idea explained above. Let $V = \{v_1, v_2, \dots, v_N\}$ and $E = \{e_1, e_2, \dots, e_{|E|}\}$. The generalized CZ gate acting on vertices $\{v_1^{(j)}, v_2^{(j)}, \dots, v_{|e_j|}^{(j)}\}$ that are connected by the j th hyperedge e_j can be written as

$$\begin{aligned} \widetilde{CZ}_{e_j} \equiv & \left(\prod_{k=1}^{|e_j|-1} I_{v_k^{(j)}} - \prod_{k=1}^{|e_j|-1} \overline{1}_{v_k^{(j)}} \right) I_{v_{|e_j|}^{(j)}} \\ & + \left(\prod_{k=1}^{|e_j|-1} \overline{1}_{v_k^{(j)}} \right) Z_{v_{|e_j|}^{(j)}}, \end{aligned} \quad (17)$$

where $\overline{a} \equiv |a\rangle\langle a|$ ($a \in \{0, 1\}$). From Eq. (16), the i th stabilizer g_i of $|G\rangle$ can be calculated as

$$g_i = X_{v_i} \left(\prod_{v_{i'} \in W_Z^{(i)}} Z_{v_{i'}} \right) \left(\prod_{\tilde{v}^{(j)} \in W_{CZ}^{(i)}} \widetilde{CZ}_{\tilde{v}^{(j)}} \right), \quad (18)$$

where

$$W_Z^{(i)} \equiv \{v_{i'} \in V | (v_i, v_{i'}) \in E\},$$

$$W_{CZ}^{(i)} \equiv \cup_{e_j \in E'} W_{CZ}^{(i,j)},$$

$$W_{CZ}^{(i,j)} \equiv \{\tilde{v}^{(j)} | (v_i, \tilde{v}^{(j)}) = e_j\}.$$

Here, $E' (\subseteq E)$ is a set of hyperedges that connect more than two vertices, and $\tilde{v}^{(j)} \equiv \tilde{v}_1^{(j)}, \dots, \tilde{v}_{|e_j|-1}^{(j)}$ is a shorthand notation. By substituting Eq. (17) into Eq. (18),

$$\begin{aligned} g_i &= X_{v_i} \left(\prod_{v_{i'} \in W_Z^{(i)}} Z_{v_{i'}} \right) \left[\prod_{\tilde{v}^{(j)} \in W_{CZ}^{(i)}} \sum_{\mathbf{a}^{(j)} \in \{0,1\}^{|e_j|-2}} \left(\prod_{k=1}^{|e_j|-2} \overline{a_{\tilde{v}_k^{(j)}}} \right) Z_{\tilde{v}_{|e_j|-1}^{(j)}}^{f(\mathbf{a}^{(j)} \cup \{a_{\tilde{v}_{|e_j|-1}^{(j)}}\})} \right] \\ &= \sum_{\mathbf{a} \in \{0,1\}^{|W_P^{(i)}|}} (-1)^{\alpha^{(i,\mathbf{a})}} X_{v_i} \left(\prod_{v_{i'} \in \tilde{W}_Z^{(i,\mathbf{a})}} Z_{v_{i'}} \right) \left(\prod_{v_{i'} \in \tilde{W}_P^{(i)}} \overline{a_{v_{i'}}} \right), \end{aligned} \quad (19)$$

where

$$\tilde{W}_P^{(i)} \equiv \cup_{\tilde{v}^{(j)} \in W_{CZ}^{(i)}} \{\tilde{v}^{(j)}\} \setminus \{\tilde{v}_{|e_j|-1}^{(j)}\}, \quad (20)$$

$$\begin{aligned} & (-1)^{\alpha^{(i,\mathbf{a})}} \left(\prod_{v_{i'} \in \tilde{W}_Z^{(i,\mathbf{a})}} Z_{v_{i'}} \right) \left(\prod_{v_{i'} \in \tilde{W}_P^{(i)}} \overline{a_{v_{i'}}} \right) \\ \equiv & \left(\prod_{v_{i'} \in W_Z^{(i)}} Z_{v_{i'}} \right) \left[\prod_{\tilde{v}^{(j)} \in W_{CZ}^{(i)}} \sum_{\mathbf{a}^{(j)} \in \{0,1\}^{|e_j|-2}} \left(\prod_{k=1}^{|e_j|-2} \overline{a_{\tilde{v}_k^{(j)}}} \right) Z_{\tilde{v}_{|e_j|-1}^{(j)}}^{f(\mathbf{a}^{(j)} \cup \{a_{\tilde{v}_{|e_j|-1}^{(j)}}\})} \right] \left(\prod_{v_{i'} \in \tilde{W}_P^{(i)}} \overline{a_{v_{i'}}} \right). \end{aligned} \quad (21)$$

Here, $\mathbf{a}^{(j)} \equiv \{a_{\tilde{v}_1^{(j)}}, \dots, a_{\tilde{v}_{|e_j|-2}^{(j)}}\}$, $\mathbf{a} \equiv \cup_{\tilde{v}^{(j)} \in W_{CZ}^{(i)}} \mathbf{a}^{(j)}$, $\alpha^{(i,\mathbf{a})} \in \{0, 1\}$, and $f(\mathbf{a}^{(j)} \cup \{a_{\tilde{v}_{|e_j|-1}^{(j)}}\})$ is a function, where it is equal to 1 if and only if all elements of $\{a_{\tilde{v}_1^{(j)}}, \dots, a_{\tilde{v}_{|e_j|-1}^{(j)}}\}$ are 1, and it is equal to 0 in other cases. Note that $\alpha^{(i,\mathbf{a})}$ and $\tilde{W}_Z^{(i,\mathbf{a})}$ are defined by Eq. (21), and $\tilde{W}_Z^{(i,\mathbf{a})} \cap \tilde{W}_P^{(i)} = \emptyset$. From Eq. (20), the time required to derive $\tilde{W}_P^{(i)}$ is at most $O(N^{c-1})$. When the

values of all elements of \mathbf{a} are given and $\tilde{W}_P^{(i)}$ is known, the time required to calculate the rhs of Eq. (21) is at most $O(N^{c-1})$. Accordingly, we can derive $\alpha^{(i,\mathbf{a})}$, $\tilde{W}_Z^{(i,\mathbf{a})}$, and $\tilde{W}_P^{(i)}$ in classical polynomial time.

The adaptive stabilizer test for g_i on an N -qubit quantum state ρ is defined as follows: The verifier measures the i th qubit of ρ that corresponds to the vertex v_i in the X basis, and each of the other qubits of ρ in the Z basis, respectively. Let $x_i \in \{1, -1\}$ be the outcome of the X -basis measurement, and $z_{i'} \in \{1, -1\}$ be the outcome of the Z -basis measurement on the i' th qubit. Then, the verifier calculates $\tilde{W}_P^{(i)}$. From $\tilde{W}_P^{(i)}$ and measurement outcomes, the verifier knows the values of \mathbf{a} . We say that the verifier passes the adaptive stabilizer test for g_i on ρ if

$$(-1)^{\alpha^{(i,\mathbf{a})}} x_i \prod_{v_{i'} \in \tilde{W}_Z^{(i,\mathbf{a})}} z_{i'} = 1.$$

Note that the adaptiveness is not needed in the special case of graph states because $W_{CZ}^{(i)} = \emptyset$.

The expected probability $p_{\text{pass}}(i)$ that the verifier passes the adaptive stabilizer test for g_i on ρ , where the expectation is taken over the sampling of \mathbf{a} , is

$$\begin{aligned} p_{\text{pass}}(i) &= \sum_{\mathbf{a}: p(\mathbf{a}) \neq 0} p(\mathbf{a}) \text{Tr} \left[\frac{P^{(i,\mathbf{a})} \rho P^{(i,\mathbf{a})} I^{\otimes |\tilde{W}_Z^{(i,\mathbf{a})|+1} + S^{(i,\mathbf{a})}}{p(\mathbf{a}) \cdot 2} \right] \\ &= \frac{1}{2} \sum_{\mathbf{a}: p(\mathbf{a}) \neq 0} (\text{Tr}[\rho P^{(i,\mathbf{a})}] + \text{Tr}[\rho P^{(i,\mathbf{a})} S^{(i,\mathbf{a})}]) \\ &= \frac{1}{2} \sum_{\mathbf{a} \in \{0,1\}^{|\tilde{W}_P^{(i)}|}} (\text{Tr}[\rho P^{(i,\mathbf{a})}] + \text{Tr}[\rho P^{(i,\mathbf{a})} S^{(i,\mathbf{a})}]) \\ &= \frac{1}{2} \left(1 + \text{Tr} \left[\rho \sum_{\mathbf{a} \in \{0,1\}^{|\tilde{W}_P^{(i)}|}} P^{(i,\mathbf{a})} S^{(i,\mathbf{a})} \right] \right) \\ &= \frac{1}{2} (1 + \text{Tr}[\rho g_i]), \end{aligned} \quad (22)$$

where

$$\begin{aligned} p(\mathbf{a}) &\equiv \text{Tr} \left[\rho P^{(i,\mathbf{a})} \right], \\ P^{(i,\mathbf{a})} &\equiv \prod_{v_{i'} \in \tilde{W}_P^{(i)}} \overline{a_{v_{i'}}} X_{v_{i'}}, \\ S^{(i,\mathbf{a})} &\equiv (-1)^{\alpha^{(i,\mathbf{a})}} X_{v_i} \left(\prod_{v_{i'} \in \tilde{W}_Z^{(i,\mathbf{a})}} Z_{v_{i'}} \right). \end{aligned}$$

We have used Eq. (19) to derive the last equality.

Let us explain why our adaptive stabilizer test can verify hypergraph states with high connectivity, while our second protocol (Sec. III) and the previous protocol [54] cannot. For the nonadaptive stabilizer test (Sec. III), the probability $p_{\text{pass}}(i)$ of passing the stabilizer test for g_i is given in Eq. (11). If $R_i = O(\exp(N))$, exponentially many tests are required to distinguish $p_{\text{pass}}(i)$ from $1/2$, which means that no polynomial-time verification is possible. On the other hand, since R_i does not appear in Eq. (22), such a problem does not occur for the adaptive stabilizer test.

D. Verification

In this subsection, we propose a verification protocol for hypergraph states based on the adaptive stabilizer test explained in the previous subsection. Our protocol runs as follows:

- (1) The prover sends the verifier an $N(Nk + m + 1)$ -qubit state ρ_B . The state ρ_B consists of $Nk + m + 1$ registers, and each register stores N qubits. If the prover is honest, the prover sends $|G\rangle^{\otimes Nk+m+1}$. On the other hand, if the prover is malicious, the prover sends an $N(Nk + m + 1)$ -qubit, completely arbitrary, quantum state instead of $|G\rangle^{\otimes Nk+m+1}$.
- (2) The verifier chooses m registers uniformly randomly and discards them to guarantee that the remaining $N(Nk + 1)$ -qubit state ρ'_B is close to an i.i.d. sample by using the quantum de Finetti theorem [63]. Next, the verifier chooses one register—which we call the target register, whose state is ρ_{tgt} —uniformly randomly and uses it for the verifier's purpose. The remaining Nk registers are divided into N groups such that which register is assigned to the i th group is uniformly random. The verifier performs the adaptive stabilizer test for g_i on every register in the i th group. Let K_i be the number of times that the verifier passes the adaptive stabilizer test for g_i . If

$$\frac{K_i}{k} \geq 1 - \epsilon, \quad (23)$$

we say that the verifier passes the adaptive stabilizer test for the i th group, where $0 < \epsilon < 1$ is specified later. If the verifier passes the adaptive stabilizer test for all i , we say that the verifier accepts the prover.

When the prover is honest, i.e., the prover sends $|G\rangle^{\otimes Nk+m+1}$ to the verifier, the verifier accepts him with probability 1, which is obvious from Eq. (22). This means that our verification protocol has the completeness. Hereafter, we consider the case where $\epsilon = 1/(4Nk^{2/7})$, $m \geq 2N^3 k^{18/7} \log 2$, and $k \geq (4N)^7$ are satisfied. In this case, the following theorem holds.

Theorem 5 (Soundness). If the verifier accepts the prover, the state ρ_{tgt} of the target register satisfies

$$\langle G|\rho_{\text{tgt}}|G\rangle \geq 1 - k^{-1/7}$$

with a probability larger than $1 - k^{-1/7}$.

Proof.—Let Π^\perp be the N -qubit projector $I^{\otimes N} - |G\rangle\langle G|$, and T be the POVM element corresponding to the event where the verifier accepts the prover. We can show that for any N -qubit state ρ ,

$$\text{Tr}[(T \otimes \Pi^\perp)\rho^{\otimes Nk+1}] \leq \frac{1}{2k^{2/7}}. \quad (24)$$

Its proof is given later. Because of the quantum de Finetti theorem (for the fully one-way LOCC norm) [63] and Eq. (24),

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp)\rho'_B] &\leq \text{Tr}\left[(T \otimes \Pi^\perp) \int d\mu \rho^{\otimes Nk+1}\right] \\ &\quad + \frac{1}{2} \sqrt{\frac{2N^3 k^2 \log 2}{m}} \\ &\leq \frac{1}{2k^{2/7}} + \frac{1}{2k^{2/7}} = \frac{1}{k^{2/7}}. \end{aligned}$$

Here, μ is a probability measure on ρ . We have

$$\text{Tr}[(T \otimes \Pi^\perp)\rho'_B] = \text{Tr}[(T \otimes I)\rho'_B] \text{Tr}[\Pi^\perp \rho_{\text{tgt}}].$$

Therefore, if

$$\text{Tr}[\Pi^\perp \rho_{\text{tgt}}] > k^{-1/7},$$

then

$$\text{Tr}[(T \otimes I)\rho'_B] < k^{-1/7}.$$

This means that if the verifier accepts the prover,

$$\langle G|\rho_{\text{tgt}}|G\rangle \geq 1 - k^{-1/7}$$

with a probability larger than $1 - k^{-1/7}$.

To complete the proof, we show Eq. (24). First, we consider the case where $\text{Tr}[g_i \rho] \geq 1 - 4\epsilon$ for all i . Because of the union bound,

$$\begin{aligned} \text{Tr}[\Pi^\perp \rho] &= 1 - \text{Tr}\left[\prod_{i=1}^N \frac{I^{\otimes N} + g_i}{2} \rho\right] \\ &\leq \sum_{i=1}^N \left(1 - \text{Tr}\left[\frac{I^{\otimes N} + g_i}{2} \rho\right]\right) \\ &\leq 2N\epsilon \\ &= \frac{1}{2k^{2/7}}. \end{aligned}$$

Therefore,

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp)\rho^{\otimes Nk+1}] &= \text{Tr}[T\rho^{\otimes Nk}] \text{Tr}[\Pi^\perp \rho] \\ &\leq \frac{1}{2k^{2/7}}. \end{aligned} \quad (25)$$

Next, we consider the case where $\text{Tr}[g_i \rho] < 1 - 4\epsilon$ is satisfied for at least one i . In this case, for the i' that satisfies $\text{Tr}[g_{i'} \rho] < 1 - 4\epsilon$,

$$p_{\text{pass}}(i') = \frac{1 + \text{Tr}[g_{i'} \rho]}{2} < 1 - 2\epsilon.$$

Therefore, because of the Hoeffding inequality,

$$\begin{aligned} \text{Tr}[(T \otimes I)\rho^{\otimes Nk+1}] &\leq \Pr\left[\frac{K_{i'}}{k} \geq 1 - \epsilon\right] \\ &\leq \Pr\left[\frac{K_{i'}}{k} > p_{\text{pass}}(i') + \epsilon\right] \\ &\leq e^{-2\epsilon^2 k} \\ &= e^{-k^{3/7}/(8N^2)} \\ &\leq e^{-2k^{1/7}}. \end{aligned}$$

Hence,

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp)\rho^{\otimes Nk+1}] &= \text{Tr}[T\rho^{\otimes Nk}] \text{Tr}[\Pi^\perp \rho] \\ &\leq e^{-2k^{1/7}}. \end{aligned} \quad (26)$$

From, Eqs. (25) and (26),

$$\begin{aligned} \text{Tr}[(T \otimes \Pi^\perp)\rho^{\otimes Nk+1}] &\leq \max\left(\frac{1}{2k^{2/7}}, e^{-2k^{1/7}}\right) \\ &= \frac{1}{2k^{2/7}}. \end{aligned} \quad \blacksquare$$

V. APPLICATIONS

In this section, we discuss applications of our protocols to the verification of quantum computational supremacy demonstrations with IQP circuits and its variants, and verifiable blind quantum computing.

First, we discuss the verification of quantum computational supremacy demonstrations with IQP circuits. An N -qubit IQP circuit is the following restricted quantum circuit:

- (i) The initial state is $|0\rangle^{\otimes N}$.
- (ii) The N -qubit unitary $H^{\otimes N} D H^{\otimes N}$ is applied, where H is the Hadamard gate, and D is a quantum circuit consisting of a polynomial number of Z -diagonal gates, such as Z , CZ , and $e^{i\theta Z}$.
- (iii) Finally, each qubit is measured in the computational basis.

The IQP model does not seem to be universal, but it is known that the output probability distributions of the IQP

model cannot be classically efficiently sampled with a constant multiplicative error unless the polynomial-time hierarchy (PH) collapses to the third level [11] or the second level [8]. Here, we say that a probability distribution $\{p_z\}_z$ is sampled with a multiplicative error ϵ if

$$|p_z - q_z| \leq \epsilon p_z$$

for all z , where q_z is the probability that the classical sampler outputs z .

Recently, Bremner, Montanaro, and Shepherd [12] have shown that, assuming a certain unproven conjecture, the no-go result can be generalized to the l_1 -norm error sampling, which is more realistic. Here, we say that a probability distribution $\{p_z\}_z$ is sampled with an l_1 -norm error ϵ if

$$\sum_z |p_z - q_z| \leq \epsilon,$$

where q_z is the probability that the classical sampler outputs z . More precisely, they have shown the following theorem.

Theorem 6 (Ref. [12]). Assume the below conjecture is true. If it is possible to classically sample from the output probability distribution of any IQP circuit in polynomial time, up to an error of $1/192$ in l_1 norm, then there is a BPP^{NP} algorithm to solve any problem in $\text{P}^{\#\text{P}}$. Hence, the PH would collapse to its third level.

Conjecture 1 (Ref. [12]). Let $f: \{0, 1\}^N \rightarrow \{0, 1\}$ be a uniformly random degree-3 polynomial over \mathbb{F}_2 . Then, it is $\#\text{P}$ -hard to approximate $(\text{gap}(f)/2^N)^2$ up to a multiplicative error of $1/4 + o(1)$ for a $1/24$ fraction of polynomials f . Here, $\text{gap}(f) \equiv |\{x: f(x)=0\}| - |\{x: f(x)=1\}|$.

Here, complexity classes BPP , NP , P , and $\#\text{P}$ are abbreviations of bounded-error probabilistic polynomial time, nondeterministic polynomial time, polynomial time, and sharp P , respectively.

Importantly, the theorem holds for the IQP model that uses only Z , CZ , and CCZ gates, where CCZ is the controlled-controlled- Z gate defined as

$$CCZ = I^{\otimes 3} - 2|111\rangle\langle 111|.$$

The theorem therefore shows the hardness for the sampling of the probability distribution of the X -basis measurement outcomes on hypergraph states. In other words, if the verifier generates a hypergraph state in his or her laboratory or receives it from a remote server, the verifier can demonstrate the quantum computational supremacy. However, one problem is that what the verifier receives deviates from the ideal hypergraph state because of the experimental imperfections or the server's dishonesty. The verifier therefore has to verify the correctness of the state, where the verification task becomes important.

In Ref. [12], all gates, Z , CZ , and CCZ , are applied uniformly random. The anticoncentration lemma, which is essential for their proof, is satisfied when Z and CZ gates are applied uniformly random, but Conjecture 1, which is often called ‘‘average case vs worst case hardness conjecture,’’ seems to be more plausible when the application of CCZ gates is also uniformly random. In other words, the hypergraph states generated by the IQP circuits of Ref. [12] can have high connectivity.

Our third protocol can verify such hypergraph states with high connectivity. From Theorem 5, we can guarantee that

$$\frac{1}{2} \|\rho_{\text{tgt}} - |G\rangle\langle G|\| \leq \sqrt{1 - \langle G | \rho_{\text{tgt}} | G \rangle} \leq \frac{1}{\text{poly}(k)},$$

which means

$$\begin{aligned} \frac{1}{2} \sum_x |\text{Tr}[M_x \rho_{\text{tgt}}] - \langle G | M_x | G \rangle| &\leq \frac{1}{2} \|\rho_{\text{tgt}} - |G\rangle\langle G|\| \\ &\leq \frac{1}{\text{poly}(k)} \end{aligned}$$

for any POVM $\{M_x\}_x$. Here, $\|\cdot\|$ is the trace norm. In particular, if we take the POVM as the X -basis measurements,

$$\sum_z |p_z - p'_z| \leq \frac{1}{\text{poly}(k)},$$

where p_z is the probability of obtaining the outcome z ($\in \{0, 1\}^N$) when $|G\rangle$ is measured in the X bases, and p'_z is the probability of obtaining the outcome z when ρ_{tgt} is measured in the X bases:

$$\begin{aligned} p_z &= |\langle z | H^{\otimes N} | G \rangle|^2, \\ p'_z &= \langle z | H^{\otimes N} \rho_{\text{tgt}} H^{\otimes N} | z \rangle. \end{aligned}$$

Assume that $\{p'_z\}_z$ is classically efficiently sampled with the l_1 -norm error $1/193$:

$$\sum_z |p'_z - q_z| \leq \frac{1}{193},$$

where q_z is the probability that a classical sampler outputs z . Then,

$$\begin{aligned} \sum_z |p_z - q_z| &\leq \sum_z |p_z - p'_z| + \sum_z |p'_z - q_z| \\ &\leq \frac{1}{\text{poly}(k)} + \frac{1}{193} \leq \frac{1}{192}, \end{aligned}$$

which causes the collapse of the PH according to Theorem 6. In conclusion, the probability distribution of the X -basis measurement outcomes on the verified state ρ_{tgt} through our

third protocol cannot be classically efficiently sampled with the l_1 -norm error. Similarly, our third protocol can also be used to verify variants of the IQP model such as those introduced in Refs. [13–16,23].

Recently, several other verification protocols for IQP circuits have also been proposed. For example, Hangleiter *et al.* have proposed a polynomial-time verification protocol [56] using the Feynman-Kitaev history state [24,57]

$$\frac{1}{\sqrt{L+1}} \sum_{i=0}^L \left(\prod_{i=0}^i U_i |\phi_0\rangle \right) \otimes |t\rangle$$

corresponding to the quantum circuit $\prod_{i=1}^L U_i$ with an initial state $|\phi_0\rangle$, where $U_0 = I$. In their protocol, the prover sends the Feynman-Kitaev history state to the verifier. Since the Feynman-Kitaev history state is, in general, more complicated than the mere output state $(\prod_{i=1}^L U_i)|\phi_0\rangle$, their protocol is more demanding for the prover than ours. Their protocol is also more demanding for the verifier because multiqubit measurements are necessary for the verifier. Moreover, their protocol assumes the i.i.d. property of samples unlike ours. Miller *et al.* have proposed another polynomial-time verification protocol for IQP circuits [16]. Although the prover in their protocol only has to generate hypergraph states like our protocol, their protocol also assumes the i.i.d. property of samples. A verification protocol proposed in Ref. [54] does not assume any i.i.d. property of samples, but the protocol cannot be used for hypergraph states with high connectivity because exponentially many quantum states are required to distinguish the probability of passing a test from $1/2$, which means that no polynomial-time verification is possible. Accordingly, this protocol cannot be used to verify the Bremner-Montanaro-Shepherd-type IQP circuits of Ref. [12].

As another application, our verification protocol for hypergraph states can also be used to construct a verifiable blind quantum computing protocol in a similar way to Ref. [54]. Since the Union Jack state [55], which is a hypergraph state, is a universal resource state for MBQC with only adaptive single-qubit measurements of Pauli operators, the client is required to perform only single-qubit Pauli measurements.

VI. DISCUSSION

We have seen that if the honest prover sends the correct state to the verifier, the verifier accepts it with high probability. However, in reality, it is not easy for the verifier to receive the perfectly ideal state: Imperfections in the prover's machine and noises in the channel from the prover to the verifier change the state even if the prover is honest. In this section, we point out that even if the state is slightly deviated from the ideal one, the verifier still accepts with high probability. In other words, our protocols are

robust to some extent. We also discuss possibilities of using the quantum error correction.

To understand our argument, let us consider a simple example. Assume that the verifier receives the slightly deviated state

$$[(1 - \epsilon')|G\rangle\langle G| + \epsilon'\eta]^{\otimes Nk+m+1} \quad (27)$$

instead of $|G\rangle\langle G|^{\otimes Nk+m+1}$, where $0 < \epsilon' < 1$, $|G\rangle$ is the ideal hypergraph state, and η is any state. The trace distance between the deviated state and the ideal state is

$$\frac{1}{2} \|(1 - \epsilon')|G\rangle\langle G| + \epsilon'\eta - |G\rangle\langle G|\| \leq \sqrt{\epsilon'},$$

and therefore, if $\epsilon' = O(1/\text{poly})$, the deviated state is still useful for the quantum computational supremacy demonstration. This means that the deviated state should also be accepted by the verifier with high probability. In fact, our protocol accepts it with high probability. From Eq. (22),

$$\begin{aligned} p_{\text{pass}}(i) &= \frac{1 + \text{Tr}[\rho g_i]}{2} \\ &= 1 - \frac{\epsilon'}{2} (1 - \text{Tr}[\eta g_i]) \end{aligned}$$

for each $i = 1, 2, \dots, N$. Therefore, the probability that the verifier accepts the deviated state is

$$\begin{aligned} \text{Pr}[\text{verifier accepts}] &= \text{Pr} \left[\bigwedge_{i=1}^N \left(\frac{K_i}{k} \geq 1 - \epsilon \right) \right] \\ &\geq 1 - \sum_{i=1}^N \text{Pr} \left[\frac{K_i}{k} < 1 - \epsilon \right] \\ &\geq 1 - N e^{-2(\epsilon' - \epsilon)^2 k}. \end{aligned}$$

Since $k \geq (4N^7)$, if $\epsilon' - \epsilon = O(N^{-3})$, $1 - N e^{-2(\epsilon' - \epsilon)^2 k}$ approaches 1 asymptotically.

For simplicity, in the above example, we have considered the tensor product of the same states, Eq. (27), but it is easy to confirm that a similar argument holds even if the tensor product state is replaced with a slightly entangled state.

In this way, we have seen that our protocols are robust to some extent. However, we have to mention that our protocols are not perfectly fault tolerant. For example, let us consider the state

$$(Z_1 \otimes I^{\otimes N-1})|G\rangle,$$

where only the first qubit of the ideal hypergraph state is phase flipped. Such a state should also be accepted with high probability because such a tiny error can be easily corrected with a quantum error correction; thus, the corrected state is a useful resource state for the verifier. However, it is also easy to check that our protocols cannot

accept such a state with high probability because such a state is stabilized by $-g_1$, where g_1 is the first stabilizer of the ideal state $|G\rangle$.

A solution to the problem is to ask the prover to send the encoded version of $|G\rangle$ with the Calderbank-Shor-Steane (CSS) code [65,66]. (This means that the prover encodes each qubit of $|G\rangle$ into a logical qubit with the CSS code.) A great advantage of our protocols is that only Pauli measurements are required for the verifier. Since in the CSS code logical Pauli measurements can be done with the transversal physical Pauli measurements, the verifier can do the verification and the syndrome measurements with only physical single-qubit Pauli measurements; i.e., no entangling gate is required for the verifier.

In Refs. [67,68], more elaborated methods have been proposed. Instead of physically encoding states, the prover sends special states, such as the Raussendorf-Harrington-Goyal (RHG) topological graph state [69], so that the verifier can do the topological quantum error correction with only physical single-qubit Pauli measurements. Unfortunately, such a scheme is known only for graph states, and at this moment, we do not know how to generalize it to hypergraph states. If a similar scheme is found for hypergraph states, we can apply it to our verification protocols so that the verifier can accept a broad class of deviated but topologically correctable states with high probability.

With respect to other verification protocols for ground states of Hamiltonians and output states of quantum circuits, a similar argument holds from Eqs. (6) and (12).

VII. CONCLUSION

In this paper, we have proposed verification protocols for ground states of Hamiltonians, quantum states generated by a certain class of quantum circuits, and all polynomial-time-generated hypergraph states. As applications of our verification protocols, we have considered the verification of IQP circuits and its variants, and verifiable blind quantum computing.

As an outlook, let us finally provide several open problems. First, our verification protocol for ground states of Hamiltonians requires knowledge of, for example, the ground energy and energy gap. It is, in general, QMA-hard to know these quantities, and therefore, it is an important open problem whether or not a protocol that does not use this knowledge exists. If it exists, it is desirable to invent such a protocol. More precisely, it is unknown whether or not the conditions (i)–(iii) for the Hamiltonian in Sec. II can be relaxed. Related to this open problem, it is interesting to consider the physical relevance of the conditions. This is also the case for our second verification protocol, namely, the verification protocol for quantum circuits. It is an important open problem to find physical meaning of conditions (i)–(iii) for the circuit and to relax these conditions.

Second, it would be useful to consider verification protocols for other quantum states such as weighted graph states,

$$\left(\prod_{(i,j) \in E} e^{i\theta_{ij}Z_i Z_j} \right) |+\rangle^{\otimes N},$$

and higher-dimensional quantum states including the continuous-variable ones. Here, E is a set of edges, and $\theta_{ij} \in \mathbb{R}$. Those states are important resources in quantum information and condensed matter physics [27,70].

Finally, with respect to the verification of quantum computational supremacy demonstrations, it would be interesting to explore good verification protocols for sub-universal circuits other than the IQP, such as the DQC1 model [6–9], the boson sampling model [4], the depth-four model [71], the Fourier sampling model [17], and the conjugated Clifford model [21].

ACKNOWLEDGMENTS

We thank anonymous referees for valuable comments. Y. T. is supported by the Program for Leading Graduate Schools: Interactive Materials Science Cadet Program and JSPS Grant-in-Aid for JSPS Research Fellow No. JP17J03503. T. M. is supported by JST ACT-I No. JPMJPR16UP, the JSPS Grant-in-Aid for Young Scientists (B) No. 17K12637, and JST, PRESTO, No. JPMJPR176A.

-
- [1] D. Gottesman, *The Heisenberg Representation of Quantum Computers*, in *Group 22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics* (International Press, Cambridge, MA, 1999).
 - [2] J. J. Bollinger, W. M. Itano, D. J. Wineland, and D. J. Heinzen, *Optimal Frequency Measurements with Maximally Correlated States*, *Phys. Rev. A* **54**, R4649(R) (1996).
 - [3] R. Raussendorf and H. J. Briegel, *A One-Way Quantum Computer*, *Phys. Rev. Lett.* **86**, 5188 (2001).
 - [4] S. Aaronson and A. Arkhipov, *The Computational Complexity of Linear Optics*, *Theory Comput.* **9**, 143 (2013).
 - [5] D. J. Brod, *Complexity of Simulating Constant-Depth Boson Sampling*, *Phys. Rev. A* **91**, 042316 (2015).
 - [6] E. Knill and R. Laflamme, *Power of One Bit of Quantum Information*, *Phys. Rev. Lett.* **81**, 5672 (1998).
 - [7] T. Morimae, K. Fujii, and J. F. Fitzsimons, *Hardness of Classically Simulating the One-Clean-Qubit Model*, *Phys. Rev. Lett.* **112**, 130502 (2014).
 - [8] K. Fujii, H. Kobayashi, T. Morimae, H. Nishimura, S. Tamate, and S. Tani, *Power of Quantum Computation with Few Clean Qubits*, in *Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming (EATCS, Rixenart, 2016)*, pp. 13:1–13:14.
 - [9] T. Morimae, *Hardness of Classically Sampling the One-Clean-Qubit Model with Constant Total Variation Distance Error*, *Phys. Rev. A* **96**, 040302(R) (2017).

- [10] D. Shepherd and M. J. Bremner, *Temporally Unstructured Quantum Computation*, *Proc. R. Soc. A* **465**, 1413 (2009).
- [11] M. Bremner, R. Jozsa, and D. Shepherd, *Classical Simulation of Commuting Quantum Computations Implies Collapse of the Polynomial Hierarchy*, *Proc. R. Soc. A* **467**, 459 (2011).
- [12] 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).
- [13] Y. Takeuchi and Y. Takahashi, *Ancilla-Driven Instantaneous Quantum Polynomial Time Circuit for Quantum Supremacy*, *Phys. Rev. A* **94**, 062336 (2016).
- [14] X. Gao, S.-T. Wang, and L.-M. Duan, *Quantum Supremacy for Simulating a Translation-Invariant Ising Spin Model*, *Phys. Rev. Lett.* **118**, 040502 (2017).
- [15] J. Bermejo-Vega, D. Hangleiter, M. Schwarz, R. Raussendorf, and J. Eisert, *Architectures for Quantum Simulation Showing a Quantum Speedup*, *Phys. Rev. X* **8**, 021010 (2018).
- [16] J. Miller, S. Sanders, and A. Miyake, *Quantum Supremacy in Constant-Time Measurement-Based Computation: A Unified Architecture for Sampling and Verification*, *Phys. Rev. A* **96**, 062320 (2017).
- [17] B. Fefferman and C. Umans, *The Power of Quantum Fourier Sampling*, [arXiv:1507.05592](https://arxiv.org/abs/1507.05592).
- [18] A. Bouland, L. Mančinska, and X. Zhang, *Complexity Classification of Two-qubit Commuting Hamiltonians*, [arXiv:1602.04145](https://arxiv.org/abs/1602.04145).
- [19] K. Fujii, *Noise Threshold of Quantum Supremacy*, [arXiv:1610.03632](https://arxiv.org/abs/1610.03632).
- [20] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, *Anti-Concentration Theorems for Schemes Showing a Quantum Speedup*, [arXiv:1706.03786](https://arxiv.org/abs/1706.03786).
- [21] A. Bouland, J. F. Fitzsimons, and D. E. Koh, *Quantum Advantage from Conjugated Clifford Circuits*, [arXiv:1709.01805](https://arxiv.org/abs/1709.01805).
- [22] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, *Characterizing Quantum Supremacy in Near-Term Devices*, [arXiv:1608.00263](https://arxiv.org/abs/1608.00263).
- [23] S. Bravyi, D. Gosset, and R. Koenig, *Quantum Advantage with Shallow Circuits*, [arXiv:1704.00690](https://arxiv.org/abs/1704.00690).
- [24] A. Y. Kitaev, A. H. Shen, and M. N. Vyalys, *Classical and Quantum Computation* (AMS, Boston, 2002).
- [25] A. Yu. Kitaev, *Fault-Tolerant Quantum Computation by Anyons*, *Ann. Phys. (Amsterdam)* **303**, 2 (2003).
- [26] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, *A Quantum Adiabatic Evolution Algorithm Applied to Random Instances of an NP-Complete Problem*, *Science* **292**, 472 (2001).
- [27] D. Gross and J. Eisert, *Novel Schemes for Measurement-Based Quantum Computation*, *Phys. Rev. Lett.* **98**, 220503 (2007).
- [28] 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).
- [29] 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).
- [30] 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).
- [31] 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).
- [32] 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).
- [33] A. Miyake, *Quantum Computation on the Edge of a Symmetry-Protected Topological Order*, *Phys. Rev. Lett.* **105**, 040501 (2010).
- [34] J. Cai, A. Miyake, W. Dür, and H. J. Briegel, *Universal Quantum Computer from a Quantum Magnet*, *Phys. Rev. A* **82**, 052309 (2010).
- [35] 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).
- [36] A. Miyake, *Quantum Computational Capability of a 2D Valence Bond Solid Phase*, *Ann. Phys. (Amsterdam)* **326**, 1656 (2011).
- [37] Y. Li, D. E. Browne, L. C. Kwak, R. Raussendorf, and T. C. Wei, *Thermal States as Universal Resources for Quantum Computation with Always-on Interactions*, *Phys. Rev. Lett.* **107**, 060501 (2011).
- [38] A. S. Darmawan, G. K. Brennen, and S. D. Bartlett, *Measurement-Based Quantum Computation in a Two-Dimensional Phase of Matter*, *New J. Phys.* **14**, 013023 (2012).
- [39] 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).
- [40] 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).
- [41] K. Fujii, Y. Nakata, M. Ozeki, and M. Muraio, *Measurement-Based Quantum Computation on Symmetry Breaking Thermal States*, *Phys. Rev. Lett.* **110**, 120502 (2013).
- [42] J. Miller and A. Miyake, *Resource Quality of a Symmetry-Protected Topologically Ordered Phase for Quantum Computation*, *Phys. Rev. Lett.* **114**, 120506 (2015).
- [43] When resource states are used to solve a decision problem in nondeterministic polynomial time (NP), we do not have to verify the correctness of the resource states because the correctness of outputs can be classically verified. However, since the relationship between bounded-error quantum polynomial time (BQP) and NP is not well known, such a classical verification method cannot always be used for decision problems in BQP.
- [44] From the model theoretical perspective, it is preferable to call these procedures “certification.” However, in this paper, we use “verification” instead because we are also interested in the interactive proof setup such as verifiable blind quantum computing.

- [45] T. Morimae and K. Fujii, *Blind Quantum Computation Protocol in which Alice Only Makes Measurements*, *Phys. Rev. A* **87**, 050301(R) (2013).
- [46] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, *Measurement of Qubits*, *Phys. Rev. A* **64**, 052312 (2001).
- [47] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, *Quantum State Tomography via Compressed Sensing*, *Phys. Rev. Lett.* **105**, 150401 (2010).
- [48] S. T. Flammia and Y.-K. Liu, *Direct Fidelity Estimation from Few Pauli Measurements*, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [49] M. Gluza, M. Kliesch, J. Eisert, and L. Aolita, *Fidelity Witnesses for Fermionic Quantum Simulations*, [arXiv:1703.03152](https://arxiv.org/abs/1703.03152).
- [50] Not all CPTP maps can be implemented in quantum polynomial time. However, in cloud quantum computing, i.e., verifiable blind quantum computing [45,52], the security is guaranteed for any CPTP map performed by the malicious server. Therefore, we assume that \mathcal{E} is any CPTP map. This situation is similar to quantum key distribution, where an eavesdropper is assumed to be able to perform any CPTP map as an attack.
- [51] Here, we assume that the correct state to be verified is pure. If it is not pure, the SWAP test is not enough. Actually, distinguishing mixed states is quantum-statistical zero-knowledge (QSZK) complete.
- [52] M. Hayashi and T. Morimae, *Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing*, *Phys. Rev. Lett.* **115**, 220502 (2015).
- [53] T. Morimae, D. Nagaj, and N. Schuch, *Quantum Proofs Can Be Verified Using Only Single-Qubit Measurements*, *Phys. Rev. A* **93**, 022326 (2016).
- [54] T. Morimae, Y. Takeuchi, and M. Hayashi, *Verification of Hypergraph States*, *Phys. Rev. A* **96**, 062321 (2017).
- [55] J. Miller and A. Miyake, *Hierarchy of Universal Entanglement in 2D Measurement-Based Quantum Computation*, *npj Quantum Inf.* **2**, 16036 (2016).
- [56] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, *Direct Certification of a Class of Quantum Simulations*, *Quantum Sci. Tech.* **2**, 015004 (2017).
- [57] R. P. Feynman, *Quantum Mechanical Computers*, *Found. Phys.* **16**, 507 (1986).
- [58] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, *Reliable Quantum Certification of Photonic State Preparations*, *Nat. Commun.* **6**, 8498 (2015).
- [59] T. Kapourniotis and A. Datta, *Nonadaptive Fault-Tolerant Verification of Quantum Supremacy with Noise*, [arXiv:1703.09568](https://arxiv.org/abs/1703.09568).
- [60] D. Mills, A. Pappa, T. Kapourniotis, and E. Kashefi, *Information Theoretically Secure Hypothesis Test for Temporally Unstructured Quantum Computation*, [arXiv:1704.01998](https://arxiv.org/abs/1704.01998).
- [61] D. Aharonov, M. Ben-Or, and E. Eban, in *Proceedings of Innovations in Computer Science 2010* (Tsinghua University Press, Beijing, China, 2010), p. 453.
- [62] J. F. Fitzsimons and E. Kashefi, *Unconditionally Verifiable Blind Quantum Computation*, *Phys. Rev. A* **96**, 012303 (2017).
- [63] K. Li and G. Smith, *Quantum de Finetti Theorem under Fully-One-Way Adaptive Measurements*, *Phys. Rev. Lett.* **114**, 160503 (2015).
- [64] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, *Quantum Hypergraph States*, *New J. Phys.* **15**, 113022 (2013).
- [65] A. R. Calderbank and P. W. Shor, *Good Quantum Error-Correcting Codes Exist*, *Phys. Rev. A* **54**, 1098 (1996).
- [66] A. M. Steane, *Multiple-Particle Interference and Quantum Error Correction*, *Proc. R. Soc. A* **452**, 2551 (1996).
- [67] K. Fujii and M. Hayashi, *Verifiable Fault Tolerance in Measurement-Based Quantum Computation*, *Phys. Rev. A* **96**, 030301(R) (2017).
- [68] T. Morimae, K. Fujii, and H. Nishimura, *Quantum Merlin-Arthur with Noisy Channel*, [arXiv:1608.04829](https://arxiv.org/abs/1608.04829).
- [69] R. Raussendorf, J. Harrington, and K. Goyal, *Topological Fault-Tolerance in Cluster State Quantum Computation*, *New J. Phys.* **9**, 199 (2007).
- [70] L. Hartmann, J. Calsamiglia, W. Dür, and H. J. Briegel, *Weighted Graph States and Applications to Spin Chains, Lattices and Gases*, *J. Phys. B* **40**, S1 (2007).
- [71] B. M. Terhal and D. P. DiVincenzo, *Adaptive Quantum Computation, Constant Depth Quantum Circuits and Arthur-Merlin Games*, *Quantum Inf. Comput.* **4**, 134 (2004).