



Efficient verification of two-colorable graph states

Qingshan Xu ¹, Xiaoqing Tan, ^{1,*} Yangwei Ou,¹ Daipengwei Bao,¹ and Rui Huang ²

¹College of Information Science and Technology, *Jinan University*, Guangzhou 510632, China

²School of Artificial Intelligence, *Shenzhen Polytechnic University*, Shenzhen 518055, China



(Received 25 January 2024; revised 12 June 2024; accepted 14 June 2024; published 8 July 2024)

Graph states known as the resource states for measurement-based quantum computation play an important role in quantum information processing. Verifying the correctness of graph states in an efficient way is crucial to scalable quantum computing. In this paper, we propose an efficient method for verifying two-colorable graph states with Pauli measurements, where the number of required measurement settings is a constant that is independent of the size of graph states. In addition, the number of required tests is less than the existing protocols. We also present several examples, such as the brickwork state and the two-dimensional square lattice state, to show how to get the specific verification strategy. Furthermore, we propose a robust verification of graph states for resisting the noise acting on the measurement device. Finally, based on the verification of two-colorable graph states in the adversarial scenario, we propose a verifiable blind quantum computing protocol, which can realize the less resource overhead.

DOI: [10.1103/PhysRevA.110.012606](https://doi.org/10.1103/PhysRevA.110.012606)

I. INTRODUCTION

Quantum computing is capable of accomplishing several tasks exponentially faster than classical computers, such as boson sampling [1] and integer factorization [2]. The rapid development of quantum technology has raised a question that how to verify the correctness of quantum computing. Quantum verification [3,4] can solve this task efficiently, which is regard as a method that returns accept if the functionality of the quantum device is correct and reject if the quantum device runs wrong.

One type of quantum verification is aimed at verifying the correctness of a quantum state produced by a quantum device. Various methods are proposed for the verification of quantum states, including state tomography [5], direct quantum-state certification [6], direct-fidelity estimation [7], and self-testing [8]. Another type of quantum verification is aimed at verifying the correctness of quantum processes, which contains direct quantum-process certification [9], randomized benchmarking [10], cross-entropy benchmarking [11], and verifiable delegated quantum computing [12–18].

Verifying quantum states with high fidelity is important to quantum information processing. Traditional methods require an overhead in resources that increases exponentially with the size of the quantum state. It has been an obstacle to scalable quantum computing. It is significant to design an efficient verification method such that the precision is high and the overhead is low. Recently, an efficient approach called quantum state verification (QSV) [19–22] has been proposed, which can realize an exponential improvement of the overhead in the number of tests with respect to the traditional quantum state tomography [23]. Existing QSV protocols can verify various quantum states with local projective

measurements, including bipartite pure states [19–21,24–27], Greenberger-Horne-Zeilinger (GHZ) states [28], graph states [18,19,29,30], hypergraph states [29], weighted graph states [31], and Dicke states [32].

In this work, we focus on the verification of graph states based on QSV. Towards the realization of quantum computing, there are mainly two models, i.e., quantum computing based on quantum circuits [33] and measurement-based quantum computing (MBQC) [34,35]. Graph states play an important role in MBQC, which are the resource states used to realize the universal quantum computation. In addition, the verification of graph states in the adversarial scenario can be used in many secure quantum information processing tasks, such as verifiable blind quantum computing [13,16,18], where the adversarial scenario means that the quantum states may be prepared by an untrusted device. Verifiable blind quantum computing allows a client with limited quantum ability (preparing or measuring single qubits) to delegate quantum computation tasks to a server with universal quantum ability while preserving the privacy and correctness of the computation, even in the face of an adversarial server.

Recently, Zhu *et al.* proposed a cover protocol [29] which can verify the graph states or hypergraph states efficiently with Pauli X and Pauli Z measurements. Furthermore, Zhu *et al.* constructed an optimal verification method of stabilizer states [30], where Pauli X , Pauli Y , and Pauli Z measurements are required. However this method relies on a search algorithm, which makes it is difficult to find all measurement settings when the number of qubits is large. Moreover, the number of measurement settings increases with the size of the quantum state. Our goal is to design a more effective and feasible verification method for the graph states.

Our contributions can be summarized as follows:

(1) We propose a verification protocol for verifying two-colorable symmetric graph states. Utilizing our method, finite measurement settings can be obtained easily, where the

*Contact author: ttxqx@jnu.edu.cn

total number of measurement settings is independent of the number of qubits. In addition, our verification method has a nice scalability, which can be extended from the case of low-dimensional graph states to the case of high-dimensional graph states. We also propose a verification protocol for verifying two-colorable asymmetric graph states, which is the general case of two-colorable symmetric graph states.

(2) We analyze the spectral gap of the verification strategy of our protocols, where this property has reflected the efficiency of verification method. Compared with the cover protocol, our protocols can achieve less overhead about the number of required tests. Additionally, we give several examples to show the specific verification strategy, including the brickwork state and the two-dimensional square lattice state.

(3) We consider the verification of graph states in the noisy scenario, where the measurement device is subject to noise. Moreover, we give the number of tests required for the verification in the noisy scenario.

(4) We consider the verification of two-colorable graph states in the adversarial scenario and apply it to the verification of blind quantum computing. Compared with the traditional protocols, our method has reduced the number of copies of the graph state from the quadratic scale to nearly linear scale.

The remainder of this paper is organized as follows. In Sec. II, we give some basic notations about quantum state verification. In Sec. III, we construct an efficient verification method for two-colorable graph states. In Sec. IV, we present the verification of graph states in the noisy scenario. In Sec. V, we give the verification of two-colorable graph states in the adversarial scenario. In Sec. VI, we conclude with some discussions and open problems.

II. PRELIMINARIES

A. Graph state

A graph $G = (V, E)$ consists of vertices $v_i \in V$ and edges $e(v_i, v_j) \in E$. A vertex is isolated if it has no neighbor. Two different vertices $v_i, v_j \in V$ are adjacent if $e(v_i, v_j) \in E$. Let the matrix A be the adjacency matrix of the graph G , where $A_{i,j} = 1$ if the vertex v_i and the vertex v_j are adjacent and $A_{i,j} = 0$ otherwise. The degree of a vertex $v_i \in V$ is the number of all vertices that are adjacent to the vertex v_i . A graph is called m -colorable if all vertices of the graph can be divided into at least m disjoint subsets S_1, S_2, \dots, S_m of vertices such that there is no edge connecting any pair of vertices in S_i for any $i \in \{1, 2, \dots, m\}$. We say that S_1, S_2, \dots, S_m are m divided sets of the m -colorable graph.

The n -qubit graph state $|G\rangle$ associated with the graph G is defined by

$$|G\rangle = \left(\prod_{e(v_i, v_j) \in E} U_{ij} \right) |+\rangle^{\otimes n}, \quad (1)$$

where U_{ij} is the controlled- Z gate $|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes Z$ acting on the qubits corresponding to the vertices v_i, v_j , and $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. There are n stabilizers $\{g_i\}_{i=1}^n$ for the graph state $|G\rangle$, where

$$g_i = X_i \prod_{v_j \in N(v_i)} Z_j. \quad (2)$$

Here, $N(v_i)$ is the set of neighbors of vertex v_i , X_i is the Pauli X operator acting on the qubit corresponding to the vertex v_i , and Z_j is the Pauli Z operator acting on the qubit corresponding to the vertex v_j .

B. Quantum state verification

Let $|\psi\rangle$ be a target state, which is supposed to be generated by a quantum device. In fact, the states generated by the device in N rounds could be $\rho_1, \rho_2, \dots, \rho_N$. The goal of quantum state verification is to ensure that the average infidelity $\bar{\epsilon} = \sum_{i=1}^N (1 - \langle \psi | \rho_i | \psi \rangle) / N$ is less than a given threshold ϵ . The verification is carried out by performing two-outcome measurements $\{P_i, 1 - P_i\}$ randomly from a set of projective measurements in each round, where the test operator P_i means passing the test. The target state $|\psi\rangle$ can pass all tests, i.e., $P_i |\psi\rangle = |\psi\rangle$. Assume that the test P_i is implemented with probability p_i . The verification operator can be written as $\Psi = \sum_i p_i P_i$. To guarantee the average infidelity $\bar{\epsilon} < \epsilon$ with significance level δ , the minimum number of tests satisfies [19]

$$N(\epsilon, \delta, \Psi) \leq \left\lceil \frac{\ln \delta^{-1}}{v(\Psi)\epsilon} \right\rceil, \quad (3)$$

where $v(\Psi) = 1 - \beta(\Psi)$ is the spectral gap of the operator Ψ and $\beta(\Psi)$ is the second-largest eigenvalue of the operator Ψ .

As for the verification of graph states, Ref. [30] has given a lower bound of $\beta(\Psi)$, i.e.,

$$\beta(\Psi) \geq \max_{i \in V_{\text{NI}}} \max \{p_i^X, p_i^Y, p_i^Z\} \geq 1/3, \quad (4)$$

where V_{NI} is the set of nonisolated vertices and p_i^X, p_i^Y, p_i^Z are probabilities that the i th qubit is measured in the Pauli X basis, Pauli Y basis, and Pauli Z basis, respectively. Let a symplectic vector $\mu = (\mu^X, \mu^Z) \in \mathbb{Z}_2^{2n}$ determine each measurement setting on an n -qubit graph state $|G\rangle$, where the i th qubit is measured in the Pauli $i^{\mu_i^X} \mu_i^Z X_i^{\mu_i^X} Z_i^{\mu_i^Z}$ basis. Let

$$\mathcal{A}_\mu = \text{diag}(\mu^X)A + \text{diag}(\mu^Z), \quad (5)$$

where $\text{diag}(\cdot)$ means a diagonal matrix, and the matrix A is the adjacency matrix of the graph G associated with the graph state $|G\rangle$. Define

$$a_{\mu, \bar{w}} = \begin{cases} 1, & \bar{w} \in \mathcal{R}(\mathcal{A}_\mu) \\ 0, & \text{otherwise,} \end{cases} \quad (6)$$

where the vector $\bar{w} \in \mathbb{Z}_2^{2n}$, $\bar{w} \neq 0$, and $\mathcal{R}(\mathcal{A}_\mu)$ is the row span of the matrix \mathcal{A}_μ . Let \bar{a}_μ be a test vector corresponding to test operator P_μ or the measurement setting μ , which consists of $2^n - 1$ elements $a_{\mu, \bar{w}}$. It is shown in Ref. [30] that all eigenvalues of $\Psi = \sum_\mu p_\mu P_\mu$ except the largest eigenvalue are contained in

$$\bar{\lambda} = \sum_\mu p_\mu \bar{a}_\mu. \quad (7)$$

III. EFFICIENT VERIFICATION OF TWO-COLORABLE GRAPH STATES

A. Verification of two-colorable symmetric graph states

In this section, we propose an efficient method for verifying two-colorable graph states. According to Eq. (3), the lower $\beta(\Psi)$ results in the less tests. From Eq. (4), in order to get a lower $\beta(\Psi)$, we need to construct a verification strategy satisfying $p_i^X \neq 0$, $p_i^Y \neq 0$, $p_i^Z \neq 0$ for any i . Otherwise, $\beta(\Psi) \geq 1/2$. Given a graph state $|G\rangle$ corresponding to a two-colorable graph $G = (V, E)$, let the sets S_1 and S_2 be two divided sets of G . The double degree for two adjacent vertices $v_1, v_2 \in V$ is defined by $d(v_1) + d(v_2) - 1$, where $d(\cdot)$ represents the degree of the vertex. Our verification protocol is described as follows:

Protocol 1: Verification of two-colorable symmetric graph states

(1) Perform two measurement settings (the first group of measurement settings) based on Pauli X and Z measurements, where each measurement setting is performed with probability p_{XZ} . In the first setting, one measures in the Pauli Z basis the qubits corresponding to the vertices of the set S_1 and measures in the Pauli X basis the qubits corresponding to the vertices of the set S_2 . In the second setting, one measures in the Pauli Z basis the qubits corresponding to the vertices of the set S_2 and measures in the Pauli X basis the qubits corresponding to the vertices of the set S_1 .

(2) Perform one measurement setting (the second group of measurement settings) based on Pauli X and Y measurements, where each measurement setting is performed with probability p_{XY} . One measures in the Pauli X basis the qubits corresponding to the vertices whose degree is even and measures in the Pauli Y basis the qubits corresponding to the vertices whose degree is odd.

(3) Find two adjacent vertices v', v'' whose double degree is the maximum. Denote the edges connecting the vertex v' or v'' by $e_1, \dots, e_{d(v') + d(v'') - 1}$. Perform $d(v') + d(v'')$ measurement settings (the third group of measurement settings) based on Pauli X , Y , and Z measurements, where each measurement setting is performed with probability p_{XYZ} . With the help of the Principles 1 and 2, ones can choose subsets $E_1, \dots, E_{d(v') + d(v'')}$ of the edge set E such that

$$E_1 \cup \dots \cup E_{d(v') + d(v'')} = E, \quad (8)$$

$$\left(\bigcup_{e(v_i, v_j) \in E_k} \{N(v_i)/\{v_j\}\} \right) \cap \left(\bigcup_{e(v_i, v_j) \in E_k} \{v_i, v_j\} \right) = \emptyset, \quad (9)$$

where the set E_k includes the edge e_k for $k = 1, 2, \dots, d(v') + d(v'') - 1$ and the set $E_{d(v') + d(v'')}$ does not contain the edges $e_1, \dots, e_{d(v') + d(v'') - 1}$. In other words, the set E_k consists of all fixed edges (red edges) derived from Principles 1 and 2 in the k th measurement setting. As for the k th measurement setting, $k = 1, \dots, d(v') + d(v'')$, one measures in the Pauli Y basis the qubits corresponding to the vertices connected by the edges of the set E_k . If the qubit is adjacent to a qubit measured in the Pauli Y basis, one measures it in the Pauli Z basis. One then measures in the Pauli X basis the qubits whose all adjacent qubits are measured in the Pauli Z basis. We denote by S_k^X (or S_k^Z or S_k^Y) the set of vertices corresponding to the qubits measured in the

Pauli X (or Z or Y) basis. There is a restrictive condition for the selection of subsets $E_1, \dots, E_{d(v') + d(v'')}$, i.e.,

$$\sum_{k=1}^{d(v') + d(v'')} f_k(v_i) \leq \frac{d(v') + d(v'')}{2} \quad (10)$$

holds for any vertex $v_i \in V$, where $f_k(v_i)$ is equal to one if and only if $v_i \in S_k^Z$.

In step 1 of Protocol 1, the first measurement setting means measuring all the stabilizer operators g_i for $i \in S_2$. The test projector corresponding to passing the test is written by

$$P_1 = \prod_{i \in S_2} \frac{\mathbb{I} + g_i}{2}. \quad (11)$$

Similarly, the second measurement setting means measuring all the stabilizer operators g_i for $i \in S_1$. The test projector corresponding to passing the test is

$$P_2 = \prod_{i \in S_1} \frac{\mathbb{I} + g_i}{2}. \quad (12)$$

In step 2 of Protocol 1, the measurement setting indicates measuring the products of all stabilizer operators g_i for $i \in V$. The test projector corresponding to passing the test is

$$P_3 = \frac{1}{2} \left(\mathbb{I} + \prod_{i \in V} g_i \right). \quad (13)$$

In step 3 of Protocol 1, the k th measurement setting indicates measuring the products of all stabilizer operators g_i for $i \in (\cup_{e(v_i, v_j) \in E_k} \{v_i, v_j\}) \cup S_k^X$. The test projector corresponding to passing the test is

$$P'_k = \frac{1}{2} \left(\mathbb{I} + \prod_{i \in (\cup_{e(v_i, v_j) \in E_k} \{v_i, v_j\}) \cup S_k^X} g_i \right). \quad (14)$$

Thus, the verification operator is characterized by

$$\Psi = p_{XZ} P_1 + p_{XZ} P_2 + p_{XY} P_3 + p_{XYZ} \sum_{k=1}^{d(v') + d(v'')} P'_k. \quad (15)$$

Since the target state $|G\rangle$ is stabilized by g_i for all $i \in V$, $|G\rangle$ can always pass the tests of steps 1–3. Note that our verification protocol needs just $3 + d(v') + d(v'')$ measurement settings, which is independent of the size of the graph state $|G\rangle$. Protocol 1 has considered the verification of two-colorable symmetric graph state, where the terminology “symmetric” means that $d(v') = d(v'')$.

Now we give three examples to illustrate our method. Here we consider the brickwork state, the two-dimensional square lattice state, and a four-qubit ring cluster state. The reason why we choose these examples is that $d(v') = d(v'') = 2$ holds for the four-qubit ring cluster state, $d(v') = d(v'') = 3$ holds for the brickwork state, and $d(v') = d(v'') = 4$ holds for the two-dimensional square lattice state. Moreover, the brickwork state and the two-dimensional square lattice state are two typical resource states for universal blind quantum computing.

Figure 1 shows a 27-qubit brickwork state. We first explain how to derive the verification strategy for a 10-qubit brickwork state, which consists of qubits denoted by numbers

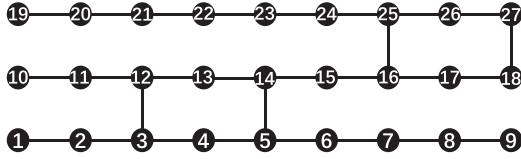


FIG. 1. A 27-qubit brickwork state.

1–5 and 10–14. Recall Protocol 1, the first measurement setting is performed by measuring in the Pauli X basis the qubits denoted by odd numbers and measuring in the Pauli Z basis the qubits denoted by even numbers. Similarly, the second measurement setting is performed by measuring in the Pauli X basis the qubits denoted by even numbers and measuring in the Pauli Z basis the qubits denoted by odd numbers. The third measurement setting is performed by measuring in the Pauli Y basis the qubits 1, 3, 10, 12, and measuring in the Pauli X basis the qubits 2, 4, 5, 11, 13, 14. As for the group of the Pauli measurements in the step 3, we find the double degree of the adjacent vertices v_3 and v_{12} is the largest, which is five. The six measurement settings based on Pauli X, Y and Z measurements are illustrated in Fig. 2. We have marked the selection of the subsets E_1, \dots, E_6 of the edge set E in red.

Principle 1.

- (1) We can fix one edge denoted by e_1 that connects one of two adjacent vertices that have maximum double degree. We then perform the Pauli Y measurements on two qubits corresponding to vertices connected by the fixed edge. We measure in the Pauli Z basis the qubits corresponding to vertices that are adjacent to the vertices on the edge.
- (2) We ignore the vertices whose corresponding qubits have determined measurement type, and ignore all edges connecting these vertices. We can obtain a subgraph $G' = (V', E')$. We then measure in the Pauli X basis the qubits corresponding to isolated vertices.
- (3) We fix one edge of set E' and measure in the Pauli Y basis the qubits corresponding to the vertices on this edge. We then measure in the Pauli Z basis the qubits corresponding to vertices that are adjacent to the vertices on this edge.

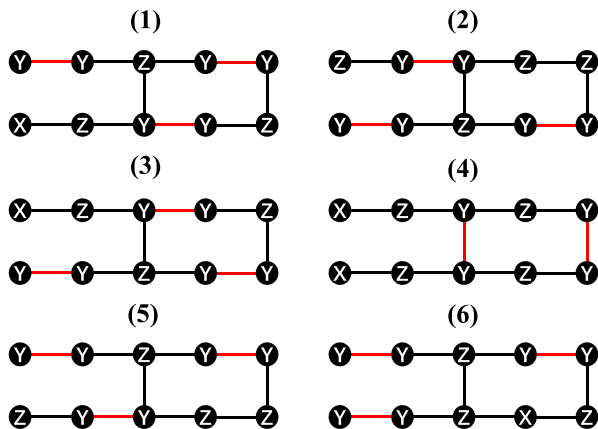


FIG. 2. The third group of measurement settings for a 10-qubit brickwork state.

(4) Repeat steps 2 and 3 until all qubits of the graph state $|G\rangle$ have determined measurement type, i.e., the first measurement setting of step 3 of Protocol 1 is done.

(5) The i th ($i = 2, \dots, d(v') + d(v'') - 1$) measurement setting of step 3 of Protocol 1 can be completed by the repetition of steps 1–4, where the fixed edge in step 1 is replaced with the edge e_i .

(6) We perform the Pauli Z measurements on two qubits corresponding to two adjacent vertices that have maximum double degree. Repeat steps 2 and 3 until all qubits of the graph state $|G\rangle$ have determined measurement type, i.e., the last measurement setting of step 3 of Protocol 1 is done.

(7) *Remark.* To satisfy the constraint of Protocol 1, the overlap degree of the selected edge of set E' between all measurement settings of step 3 of Protocol 1 should be as low as possible.

In the first measurement setting of Fig. 2, the edge $e_1 = e(v_3, v_4)$ is fixed, and the qubits 3 and 4 are measured in the Pauli Y basis. The qubits 2, 5, and 12 are measured in the Pauli Z basis. Then, a subgraph is obtained, which consists of $V' = \{v_1, v_{10}, v_{11}, v_{13}, v_{14}\}$ and $E' = \{e(v_{10}, v_{11}), e(v_{13}, v_{14})\}$. Qubit 1 is measured in the Pauli X basis. Next, the edge $e(v_{10}, v_{11})$ is selected from the set E' , and the qubits 10 and 11 are measured in the Pauli Y basis. Afterward, a new subgraph is obtained, which consists of $V' = \{v_{13}, v_{14}\}$ and $E' = \{e(v_{13}, v_{14})\}$. Finally, the edge $e(v_{13}, v_{14})$ is selected from the set E' , and the qubits 13 and 14 are measured in the Pauli Y basis. The remaining measurement settings in Fig. 2 is obtained similarly, where $e_2 = e(v_{11}, v_{12})$, $e_3 = e(v_{12}, v_{13})$, $e_4 = e(v_3, v_{12})$, and $e_5 = e(v_2, v_3)$.

Our method has a great scalability. We now show how to expand the scheme for the selection of the edge sets to higher dimensional situations. The new principle about selection is as follows:

Principle 2.

- (1) As for the subgraph with the same structure, we adopt the same measurements obtained by Principle 1. The qubits measured in the Pauli X basis need to be assigned to new measurement types by subsequent steps.
- (2) We measure in the Pauli Z basis the qubits which are adjacent to the qubits measured in the Pauli Y basis.
- (3) Repeat steps 2 and 3 of Principle 1 until all qubits of the graph state $|G\rangle$ have determined measurement type.
- (4) To get the remaining measurement settings, we repeat steps 1–3.

(5) If the graph has many pairs of adjacent qubits, which have the largest double degree, we need to ensure that for any edge connecting one of such adjacent qubits there is one measurement setting performing Pauli Y measurements on the qubits on this edge. In addition, we need to ensure that there is one measurement setting performing Pauli Z measurements on such adjacent qubits. Therefore, we need to adjust some measurement settings to satisfy these conditions and get the ultimate measurement settings.

According to Principle 1, if the qubits on the edge $e_i \in E_i$ are chosen to be measured in the Pauli Y basis, then there is at least one qubit on any edge e_j for $j \neq i$ and it is measured in the Pauli Z basis. Thus, the edge set E_i will not contain e_j for $j \neq i$. To cover all edges e_k for $k = 1, 2, \dots, d(v') + d(v'') - 1$, it is necessary to select $d(v') + d(v'') - 1$ edge

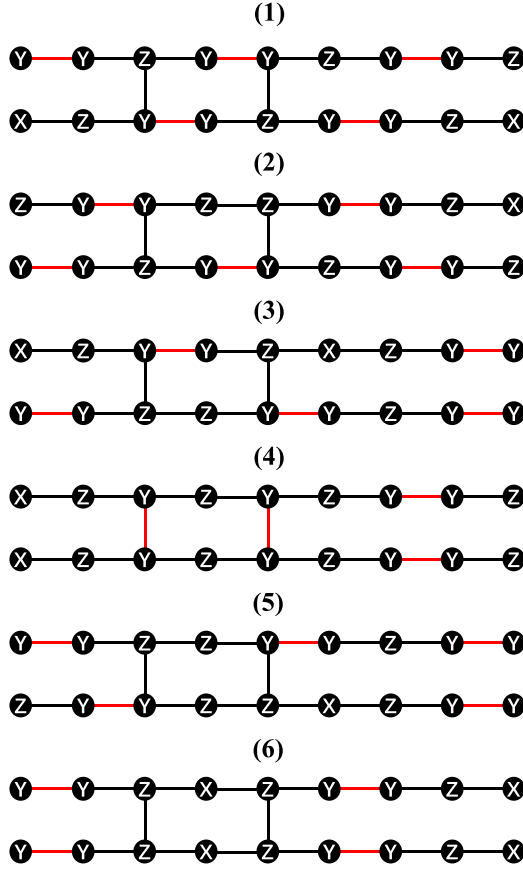


FIG. 3. The third group of measurement settings for an 18-qubit brickwork state.

sets, i.e., $E_1, E_2, \dots, E_{d(v') + d(v'') - 1}$. Since for any edge $e \in E$, where $e \notin \{e_1, e_2, \dots, e_{d(v') + d(v'') - 1}\}$, the double degree of two vertices on the edge e is less than the maximum double degree, i.e., $d(v') + d(v'') - 1$. This property ensures that the edge e can be selected and included in at least one edge set E_k , $k \in \{1, 2, \dots, d(v') + d(v'') - 1\}$. As for the extension to higher-dimensional two-colorable graph states, let edge set E' consist of all edges connecting any one of two vertices with the maximum double degree. Principle 2 has guaranteed that, for any edge $e' \in E'$, there is one measurement setting measuring in the Pauli Y basis the qubits on the edge e' . It means that the edge e' is included in only one edge set E_k , $k \in \{1, 2, \dots, d(v') + d(v'') - 1\}$. For any edge $e'' \notin E'$, the double degree of two vertices on the edge e'' is less than the maximum double degree, this property ensures that the edge e'' can be selected and included in at least one edge set E_k , $k \in \{1, 2, \dots, d(v') + d(v'') - 1\}$. To sum up, for any edge $e \in E$, we have $e \in E_1 \cup \dots \cup E_{d(v') + d(v'') - 1}$. Therefore, Eq. (8) always holds.

Consider an 18-qubit brickwork state consisting of qubits denoted by numbers 1–18. Using Principle 2, we can obtain the measurement settings of step 3 of Protocol 1 for such an 18-qubit brickwork state, as shown in Fig. 3. As for the first measurement setting, the subgraph represents the graph corresponding to a 10-qubit brickwork state of Fig. 2. We apply the first measurement setting of Fig. 2 to the subgraph. Excluding

the qubit measured in the Pauli X basis, i.e., qubit 1, we can determine the measurement type of qubits 2–5 and 10–14. The qubit 15 is adjacent to the qubit 14 measured in the Pauli Y basis. We then measure qubit 15 in the Pauli Z basis. As a result, a subgraph is obtained, which consists of $V' = \{v_1, v_6, v_7, v_8, v_9, v_{16}, v_{17}, v_{18}\}$ and $E' = \{e(v_6, v_7), e(v_7, v_8), e(v_8, v_9), e(v_{16}, v_{17}), e(v_{17}, v_{18})\}$. Qubit 1 is measured in the Pauli X basis. Next, the edge $e(v_6, v_7)$ is selected from the set E' , and qubits 6 and 7 are measured in the Pauli Y basis. Qubit 8 is measured in the Pauli Z basis. As a result, a subgraph is obtained, which consists of $V' = \{v_9, v_{16}, v_{17}, v_{18}\}$ and $E' = \{e(v_{16}, v_{17}), e(v_{17}, v_{18})\}$. Qubit 9 is measured in the Pauli X basis. The edge $e(v_{16}, v_{17})$ is selected from the set E' , and qubits 16 and 17 are measured in the Pauli Y basis. Qubit 18 is measured in the Pauli Z basis. The remaining five measurement settings can be obtained in a similar way.

We can find that there is no measurement setting performing Pauli Y measurements on the both qubits on the edge $e(v_5, v_6)$ or $e(v_{14}, v_{15})$. In addition, there is no measurement setting performing Pauli Z measurements on the both qubits on the edge $e(v_5, v_{14})$. Recall step 5 of Principle 2, we first modify the third measurement setting. We measure in the Pauli Y basis the qubits on the edge $e(v_5, v_6)$. Qubits 4, 7, 14 that are adjacent to qubits 5, 6 are measured in the Pauli Z basis. The measurement type of remaining qubits that belong to a 10-qubit brickwork state of Fig. 2 is invariant. As a result, one subgraph consists of $V' = \{v_8, v_9, v_{15}, v_{16}, v_{17}, v_{18}\}$ and $E' = \{e(v_8, v_9), e(v_{15}, v_{16}), e(v_{16}, v_{17}), e(v_{17}, v_{18})\}$. Repeating steps 2 and 3 of Principle 1 can result in one ultimate measurement setting. Similarly, the fifth measurement setting is altered, where the qubits on the edge $e(v_{14}, v_{15})$ are measured in the Pauli Y basis. Finally, we modify the last measurement setting. We measure in the Pauli Z basis the qubits on the edge $e(v_5, v_{14})$. The measurement type of remaining qubits that belong to a 10-qubit brickwork state of Fig. 2 is invariant, except that qubit 13 whose all adjacent qubits are measured in the Pauli Z basis should be measured in the Pauli X basis. Repeating steps 2 and 3 of Principle 1 can obtain one ultimate measurement setting.

Now we return to the verification of a 27-qubit brickwork state in Fig. 1. According to Principles 1 and 2, we can derive the measurement settings of step 3 of Protocol 1 for such a 27-qubit brickwork state, as shown in Fig. 4. In the graph corresponding to the 27-qubit brickwork state, there are three pairs of adjacent vertices that have the largest double degree, i.e., (v_3, v_{12}) , (v_5, v_{14}) , and (v_{16}, v_{25}) . The edge set \tilde{E}_1 consists of edges that are associated with a pair of adjacent vertices (v_3, v_{12}) . The edge sets \tilde{E}_2 and \tilde{E}_3 are defined in the similar way.

$$\begin{aligned} \tilde{E}_1 &= \{(v_2, v_3), (v_3, v_4), (v_3, v_{12}), (v_{11}, v_{12}), (v_{12}, v_{13})\}, \\ \tilde{E}_2 &= \{(v_4, v_5), (v_5, v_6), (v_5, v_{14}), (v_{13}, v_{14}), (v_{14}, v_{15})\}, \\ \tilde{E}_3 &= \{(v_{15}, v_{16}), (v_{16}, v_{17}), (v_{16}, v_{25}), \\ &\quad (v_{24}, v_{25}), (v_{25}, v_{26})\}. \end{aligned} \quad (16)$$

One can check that for any edge $\tilde{e} \in \tilde{E}_1 \cup \tilde{E}_2 \cup \tilde{E}_3$, there is one measurement setting such that all qubits on this edge are measured in the Pauli Y basis. In addition, it is guaranteed

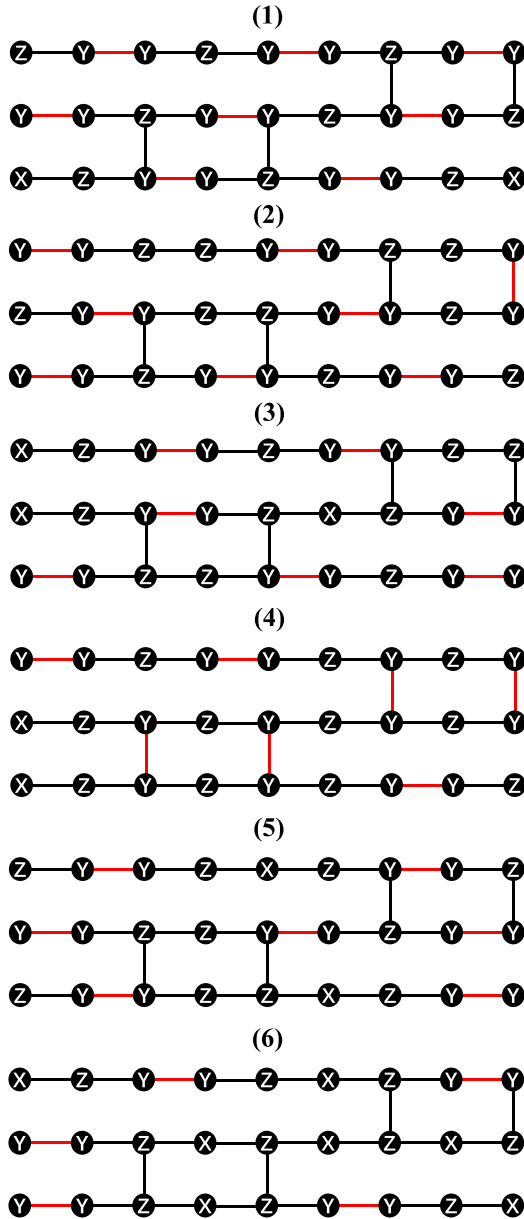


FIG. 4. The third group of measurement settings for the 27-qubit brickwork state.

that there is one measurement setting such that both qubits corresponding to vertices (v_3, v_{12}) or (v_5, v_{14}) or (v_{16}, v_{25}) are measured in the Pauli Z basis.

In the special case of a 16-qubit two-dimensional square lattice state, as shown in Fig. 5, we find the double degree of

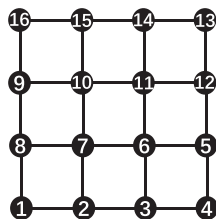


FIG. 5. A 16-qubit two-dimensional square lattice state.

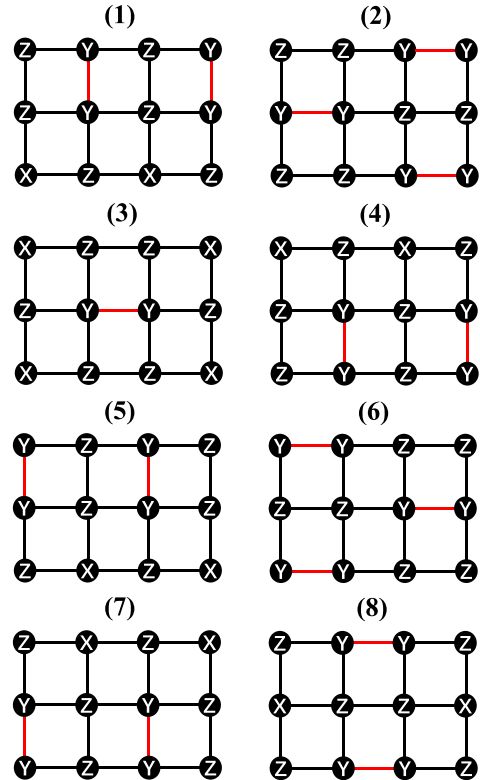


FIG. 6. The third group of measurement settings for a 12-qubit two-dimensional square lattice state.

the adjacent vertices 6 and 7 is the largest, which is 7. In the first measurement setting of Protocol 1, the qubits denoted by the odd number are measured in the Pauli X basis, and the qubits denoted by the even number are measured in the Pauli Z basis. In the second measurement setting of Protocol 1, the qubits denoted by even numbers are measured in the Pauli X basis, and the qubits denoted by odd numbers are measured in the Pauli Z basis. In the third measurement setting of Protocol 1, qubits 1, 4, 6, 7, 10, 11, 13, 16 are measured in the Pauli X basis, and qubits 2, 3, 5, 8, 9, 12, 14, 15 are measured in the Pauli Y basis. We first consider the verification strategy of step 3 of Protocol 1 for a 12-qubit state that consists of qubits 1–12. Utilizing Principle 1, we can get eight measurement settings, as shown in Fig. 6. Using Principle 2, we can extend the verification from such a 12-qubit state to the 16-qubit two-dimensional square lattice state, where the eight measurement settings of step 3 of Protocol 1 are demonstrated in Fig. 7.

A 4-qubit ring cluster state is shown in Fig. 8(a), where the double degree of the adjacent vertices v_1 and v_2 is the largest. According to Principle 1, two measurement settings required for the step 1 of Protocol 1 are illustrated in Fig. 8(b), one measurement settings required for step 2 of Protocol 1 is illustrated in Fig. 8(c), and four measurement settings required for step 3 of Protocol 1 are illustrated in Fig. 8(d).

B. Analysis of the property for the verification strategy of Protocol 1

To characterize the performance of verification protocol, we show how to compute the spectral gap of the verification

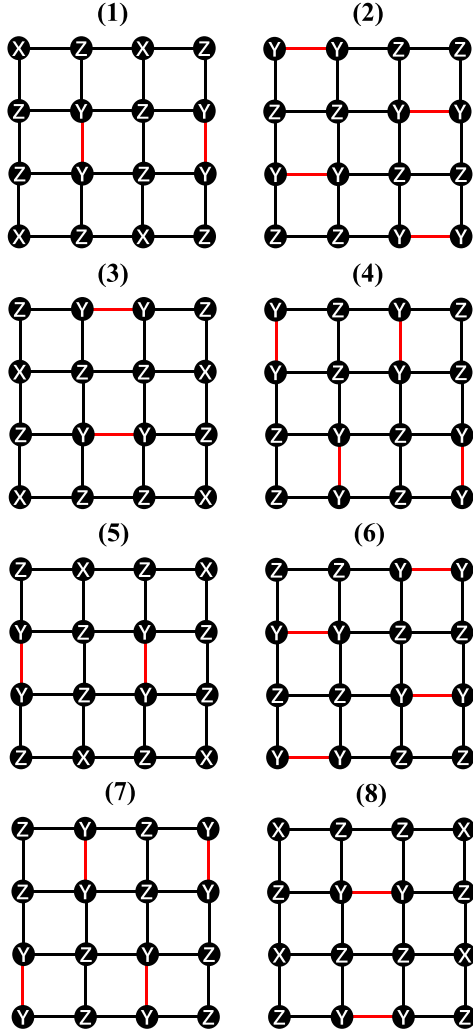


FIG. 7. The third group of measurement settings for the 16-qubit two-dimensional square lattice state.

operator, where a higher spectral gap means a higher efficiency of verification.

For any two-colorable symmetric graph state $|G\rangle$, without loss of generality, we assume that $d(v') = d(v'') = \xi$. Theorem III B gives the spectral gap of the verification operator for the general two-colorable symmetric graph state.

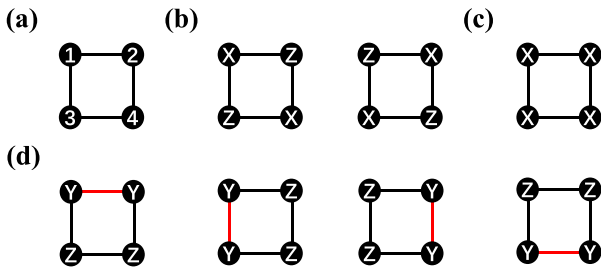


FIG. 8. The example of a 4-qubit ring cluster state. (a) A 4-qubit ring cluster state. (b) The first group of measurement settings. (c) The second group of measurement settings. (d) The third group of measurement settings.

Theorem 1. The second largest eigenvalue and spectral gap of the verification operator Ψ of Protocol 1 for the two-colorable symmetric graph state $|G\rangle$ are

$$\beta(\Psi) = \frac{2\xi + 1}{4\xi + 3}, \quad v(\Psi) = \frac{2\xi + 2}{4\xi + 3}. \quad (17)$$

Proof. We call matrix \mathcal{A}_μ corresponding to the measurement setting μ by the measurement matrix. From the definition of the matrix \mathcal{A}_μ , we present a scheme in order to calculate the value of each element of the matrix \mathcal{A}_μ quickly. Consider the i th row of matrix \mathcal{A}_μ . If the qubit denoted by number i is measured in the Pauli X basis, let the set Δ_X consist of the numbers corresponding to the qubits which are adjacent to qubit i . If the number $j \in \Delta_X$, then the element of the i th row and the j th column of the matrix \mathcal{A}_μ is one. Otherwise, the value is zero. If the qubit denoted by number i is measured in the Pauli Y basis, let the set Δ_Y consist of the number i and numbers corresponding to the qubits adjacent to qubit i . If the number $j \in \Delta_Y$, then the element of the i th row and the j th column of the matrix \mathcal{A}_μ is one. Otherwise, the value is zero. If the qubit denoted by number i is measured in the Pauli Z basis, then the element of the i th row and the i th column of the matrix \mathcal{A}_μ is one, and the remaining elements of the i th row of the matrix \mathcal{A}_μ are zero. Let $\{\mu_1, \mu_2, \dots, \mu_{3+d(v')+d(v'')}\}$ be all measurement settings. Then the corresponding probabilities $\{p_{\mu_i}\}_i$ are $\{p_{XZ}, p_{XZ}, p_{XY}, p_{XYZ}, \dots, p_{XYZ}\}$.

Let

$$\vec{\lambda}(\vec{w}) = \sum_{\mu} p_{\mu} a_{\mu, \vec{w}}. \quad (18)$$

Note that the set $\{\vec{\lambda}(\vec{w}) | \vec{w} \in \mathbb{Z}_2^n, \vec{w} \neq 0\}$ contains all eigenvalues of Ψ except the first largest eigenvalue. To solve the second largest eigenvalue of Ψ , we need to solve the following optimization problem, where $f_{\max}(\cdot)$ is a function that finds the maximum element in a set.

$$\begin{aligned} \min & f_{\max}(\{\vec{\lambda}(\vec{w}) | \vec{w} \in \mathbb{Z}_2^n, \vec{w} \neq 0\}) \\ \text{s.t.} & \sum_{\mu} p_{\mu} = 1, \quad 0 \leq p_{\mu} \leq 1, \quad \forall \mu. \end{aligned} \quad (19)$$

We can pick out all elements that may be the maximum value of the set $\{\vec{\lambda}(\vec{w}) | \vec{w} \in \mathbb{Z}_2^n, \vec{w} \neq 0\}$ as follows. By Eq. (18), if the vector \vec{w} belongs to the row span of as many measurement matrices as possible, then the element $\vec{\lambda}(\vec{w})$ can be a candidate. Hence, we need to consider seven situations. Recall that $\mathcal{R}(\mathcal{A}_{\mu_i})$ is the row span of the measurement matrix \mathcal{A}_{μ_i} . It means that each element of $\mathcal{R}(\mathcal{A}_{\mu_i})$ is one linear combination of all rows of \mathcal{A}_{μ_i} , where the operator is the modulo two addition.

Let the three groups of measurement settings of Protocol 1 be expressed by $\mathcal{E}_1 = \{1, 2\}$, $\mathcal{E}_2 = \{3\}$, $\mathcal{E}_3 = \{4, \dots, 3 + d(v') + d(v'')\}$. The first situation needs to find one vector \vec{w} such that the Eq. (20) is maximum.

$$\left\| \left\{ i | \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}), \vec{w} \notin \bigcup_{j \in \mathcal{E}_2 \cup \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_j}), i \in \mathcal{E}_1 \right\} \right\|, \quad (20)$$

where $|\cdot|$ means the size of a set. The second situation needs to find one vector \vec{w} such that Eq. (21) is maximum:

$$\left| \left\{ i | \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}), \vec{w} \notin \bigcup_{j \in \mathcal{E}_1 \cup \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_j}), i \in \mathcal{E}_2 \right\} \right|. \quad (21)$$

The third situation needs to find one vector \vec{w} such that Eq. (22) is maximum:

$$\left| \left\{ i | \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}), \vec{w} \notin \bigcup_{j \in \mathcal{E}_1 \cup \mathcal{E}_2} \mathcal{R}(\mathcal{A}_{\mu_j}), i \in \mathcal{E}_3 \right\} \right|. \quad (22)$$

The fourth situation needs to find one vector \vec{w} such that Eq. (23) is maximum:

$$\left| \left\{ (i, j) | \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}), \vec{w} \notin \bigcup_{k \in \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_k}), i \in \mathcal{E}_1, j \in \mathcal{E}_2 \right\} \right|. \quad (23)$$

The fifth situation needs to find one vector \vec{w} such that Eq. (24) is maximum:

$$\left| \left\{ (i, j) | \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}), \vec{w} \notin \bigcup_{k \in \mathcal{E}_2} \mathcal{R}(\mathcal{A}_{\mu_k}), i \in \mathcal{E}_1, j \in \mathcal{E}_3 \right\} \right|. \quad (24)$$

The sixth situation needs to find one vector \vec{w} such that Eq. (25) is maximum:

$$\left| \left\{ (i, j) | \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}), \vec{w} \notin \bigcup_{k \in \mathcal{E}_1} \mathcal{R}(\mathcal{A}_{\mu_k}), i \in \mathcal{E}_2, j \in \mathcal{E}_3 \right\} \right|. \quad (25)$$

The last situation needs to find one vector \vec{w} such that Eq. (26) is maximum:

$$\left| \left\{ (i, j, k) | \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}) \cap \mathcal{R}(\mathcal{A}_{\mu_k}), i \in \mathcal{E}_1, j \in \mathcal{E}_2, k \in \mathcal{E}_3 \right\} \right|. \quad (26)$$

As for the first situation, since the intersection of $\mathcal{R}(\mathcal{A}_{\mu_1})$ and $\mathcal{R}(\mathcal{A}_{\mu_2})$ is an empty set, the upper bound of Eq. (20) is one. As a result, the element $\vec{\lambda}(\vec{w}) = p_{XZ}$ is a candidate. As for the second situation, since only one measurement matrix \mathcal{A}_{μ_3} is considered, the upper bound of Eq. (21) is one. Moreover, the element $\vec{\lambda}(\vec{w}) = p_{XY}$ is a candidate. As for the third situation, the upper bound of Eq. (22) is $d(v') + d(v'')$. The element $\vec{\lambda}(\vec{w}) = [d(v') + d(v'')]p_{XYZ}$ is a candidate. As for the fourth candidate, the upper bound of Eq. (23) is one. Thus, the element $\vec{\lambda}(\vec{w}) = p_{XZ} + p_{XY}$ is a candidate.

As for the fifth situation, if one nonzero vector \vec{w} satisfies

$$\vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}), \vec{w} \notin \bigcup_{k \in \mathcal{E}_2} \mathcal{R}(\mathcal{A}_{\mu_k}), i \in \mathcal{E}_1, \quad (27)$$

it means that the amount of ones in the vector $\vec{w} = (w_1, \dots, w_n)$ is odd and $\text{supp}(\vec{w}) \in S_i$, where

$$\text{supp}(\vec{w}) = \{l | w_l = 1\}. \quad (28)$$

In addition, for $i \in \mathcal{E}_1, j \in \mathcal{E}_3$, if two nonzero vectors \vec{w}_1 and \vec{w}_2 that have an odd number of ones satisfy

$$\text{supp}(\vec{w}_1) \in S_i, \quad \text{supp}(\vec{w}_2) \in S_i, \quad \text{supp}(\vec{w}_1) \subseteq \text{supp}(\vec{w}_2), \quad (29)$$

then

$$\vec{w}_2 \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}) \quad (30)$$

leads to

$$\vec{w}_1 \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}). \quad (31)$$

To clarify Eq. (31), let us focus on Eq. (30). The condition $\vec{w}_2 \in \mathcal{R}(\mathcal{A}_{\mu_i})$ means that for any $l \in \text{supp}(\vec{w}_2)$ the measurement setting μ_i ($i \in \mathcal{E}_1$) measures in the Pauli Z basis the qubit denoted by the number l . Combining $\vec{w}_2 \in \mathcal{R}(\mathcal{A}_{\mu_i})$ with $\vec{w}_2 \in \mathcal{R}(\mathcal{A}_{\mu_j})$ implies that, for any $l \in \text{supp}(\vec{w}_2)$, the measurement setting μ_j ($j \in \mathcal{E}_3$) measures in the Pauli Z basis the qubit denoted by the number l . Note that if the measurement setting μ_j measures in the Pauli X basis qubit l , then $l \notin \text{supp}(\vec{w}_2)$ results in a contradiction. If the measurement setting μ_j measures in the Pauli Y basis qubit l , then $l \in \text{supp}(\vec{w}_2) \in S_i$ leads to $l' \in \text{supp}(\vec{w}_2)$, where $l' \notin S_i$. It reflects a contradiction. From the condition $\text{supp}(\vec{w}_1) \subseteq \text{supp}(\vec{w}_2)$, we can know that for any $l \in \text{supp}(\vec{w}_1)$ both measurement settings μ_i and μ_j measure in the Pauli Z basis the qubit denoted by the number l . According to the definition of $\mathcal{R}(\mathcal{A}_{\mu_i})$, the conditions $\vec{w}_1 \in \mathcal{R}(\mathcal{A}_{\mu_i})$ and $\vec{w}_1 \in \mathcal{R}(\mathcal{A}_{\mu_j})$ are established.

So we just need to find a vector \vec{w} satisfying $\sum_{l=1}^n w_l = 1$ and $\text{supp}(\vec{w}) \in S_i, i \in \mathcal{E}_1$ such that the following Eq. (32) is maximum.

$$|\{j | \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_j}), j \in \mathcal{E}_3\}|. \quad (32)$$

In other words, in the third group of measurement settings we need to find as many measurement settings as possible which perform the Pauli Z measurement on one fixed qubit. There are at most ξ measurement settings that measure in the Pauli Z basis the same qubit due to the restrictive condition of step 3 of Protocol 1. The upper bound of Eq. (24) is ξ . The element $p_{XZ} + \xi p_{XYZ}$ is a candidate.

As for the sixth situation, the upper bound of Eq. (25) is 2ξ . Thus, the element $p_{XY} + 2\xi p_{XYZ}$ is a candidate.

As for the seventh situation, if one nonzero vector \vec{w} satisfies

$$\vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}), i \in \mathcal{E}_1, j \in \mathcal{E}_2, \quad (33)$$

it means that the amount of ones in the vector $\vec{w} = (w_1, \dots, w_n)$ is even and $\text{supp}(\vec{w}) \in S_i$. In addition, for $i \in \mathcal{E}_1, j \in \mathcal{E}_2, k \in \mathcal{E}_3$, if two nonzero vectors \vec{w}_1 and \vec{w}_2 that have an even number of ones satisfy Eq. (29) then

$$\vec{w}_2 \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}) \cap \mathcal{R}(\mathcal{A}_{\mu_k}) \quad (34)$$

leads to

$$\bar{w}_1 \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}) \cap \mathcal{R}(\mathcal{A}_{\mu_k}). \quad (35)$$

So we just need to find a vector \bar{w} satisfying $\sum_{l=1}^n w_l = 2$ and $\text{supp}(\bar{w}) \in S_i, i \in \mathcal{E}_1$ such that the following Eq. (36) is maximum.

$$|\{k | \bar{w} \in \mathcal{R}(\mathcal{A}_{\mu_k}), k \in \mathcal{E}_3\}|. \quad (36)$$

In other words, in the third group of measurement settings we have to find as many measurement settings as possible, where two fixed qubits corresponding to two vertices of the set S_1 or S_2 are all measured in the Pauli Z basis. Since the number of measurement settings that measure two qubits with the same color in the Pauli Z basis is not more than the number of measurement settings that measure one qubit in the Pauli Z basis. In addition, by the principles of the selection of edge sets, if there are ξ measurement settings that measure in the Pauli Z basis the qubit corresponding to one vertex v_i , then there is no other vertex v_j such that all these ξ measurement settings measure in the Pauli Z basis the qubit corresponding to the vertex v_j . It means that the number of measurement settings that measure two qubits with the same color in the Pauli Z basis is not more than $\xi - 1$. Therefore, the element $p_{XZ} + p_{XY} + (\xi - 1)p_{XYZ}$ is a candidate.

Our verification strategy has several remarkable properties. Let us consider a vector $\bar{w} \in \mathcal{R}(\mathcal{A}_{\mu_i})$ for $i \in \mathcal{E}_3$. If $v_j \in S_{i-3}^Y$ and $j \in \text{supp}(\bar{w})$, where S_{i-3}^Y means the set of vertices corresponding to the qubits measured in the Pauli Y basis in the measurement setting μ_i , then there is a vertex v_k adjacent to the vertex v_j such that $k \in \text{supp}(\bar{w})$. It implies that $\bar{w} \notin \mathcal{R}(\mathcal{A}_{\mu_1}) \cup \mathcal{R}(\mathcal{A}_{\mu_2})$. Furthermore, for any $i \in \mathcal{E}_1$, if there is a vertex v_j satisfying $v_j \in S_{i \oplus 1}$, where the symbol \oplus represents modulo two addition, then each vector $\bar{w} \in \mathcal{R}(\mathcal{A}_{\mu_i})$ satisfies $j \notin \text{supp}(\bar{w})$. Similarly, for any $i \in \mathcal{E}_3$, if there is a vertex v_j satisfying $v_j \in S_{i-3}^X$, then each vector $\bar{w} \in \mathcal{R}(\mathcal{A}_{\mu_i})$ satisfies $j \notin \text{supp}(\bar{w})$.

Let Φ consist of all the vectors $\bar{w} \in \mathbb{Z}_2^n$ having an even number of ones. Note that $\mathcal{R}(\mathcal{A}_{\mu_3})$ belongs to Φ , i.e., $\mathcal{R}(\mathcal{A}_{\mu_3}) \subseteq \Phi$. We have already replaced $\mathcal{R}(\mathcal{A}_{\mu_3})$ with Φ in this paper. The candidates obtained by Φ are greater than or equal to the candidates obtained by $\mathcal{R}(\mathcal{A}_{\mu_3})$. It indicates the worst case for the spectral gap $v(\Psi)$ of the verification operator Ψ .

Based on the above analysis, all candidates that may be the maximum value of the set $\{\vec{\lambda}(\bar{w}) | \bar{w} \in \mathbb{Z}_2^n, \bar{w} \neq 0\}$ are

$$\{p_{XZ}, p_{XY}, 2\xi p_{XYZ}, p_{XZ} + p_{XY}, p_{XZ} + \xi p_{XYZ}, p_{XY} + 2\xi p_{XYZ}, p_{XZ} + p_{XY} + (\xi - 1)p_{XYZ}\}. \quad (37)$$

To solve the maximum value, we just need to consider the last three candidates. Therefore, the optimization problem can be written as

$$\begin{aligned} \min \quad & f_{\max}(\Theta) \\ \text{s.t.} \quad & \Theta = \{p_{XZ} + \xi p_{XYZ}, p_{XY} + 2\xi p_{XYZ}, \\ & p_{XZ} + p_{XY} + (\xi - 1)p_{XYZ}, \\ & 2p_{XZ} + p_{XY} + 2\xi p_{XYZ} = 1, \\ & p_{XZ}, p_{XY}, p_{XYZ} \in [0, 1]. \end{aligned} \quad (38)$$

The analytical solution is obtained when three candidates are equal, which implies

$$\begin{aligned} p_{XZ} &= \frac{\xi + 1}{4\xi + 3}, \quad p_{XY} = \frac{1}{4\xi + 3}, \\ p_{XYZ} &= \frac{1}{4\xi + 3}, \quad \beta(\Psi) = \frac{2\xi + 1}{4\xi + 3}. \end{aligned} \quad (39)$$

Thus, the spectral gap of the verification operator Ψ is $v(\Psi) = 1 - \beta(\Psi) = (2\xi + 2)/(4\xi + 3)$. ■

The value $v(\Psi)$ with regard to the graph state with special structures can be further improved, such as the 4-qubit ring cluster state and the two-dimensional square lattice state. Theorem 2 gives the spectral gap of the verification operator when the graph state is a 4-qubit ring cluster state.

Theorem 2. The second largest eigenvalue and spectral gap of the verification operator Ψ of Protocol 1 for the 4-qubit ring cluster state are

$$\beta(\Psi) = 3/7, \quad v(\Psi) = 4/7. \quad (40)$$

Proof. Let $\{\mu_1, \mu_2, \dots, \mu_7\}$ be the measurement settings of Fig. 8. Then the corresponding probabilities $\{p_{\mu_i}\}_{i=1}^7$ are $\{p_{XZ}, p_{XZ}, p_{XY}, p_{XYZ}, p_{XYZ}, p_{XYZ}, p_{XYZ}\}$. According to the definition of the matrix of \mathcal{A}_{μ} , we have

$$\begin{aligned} \mathcal{A}_{\mu_1} &= \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \mathcal{A}_{\mu_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \\ \mathcal{A}_{\mu_3} &= \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad \mathcal{A}_{\mu_4} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \\ \mathcal{A}_{\mu_5} &= \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{A}_{\mu_6} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \\ \mathcal{A}_{\mu_7} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}. \end{aligned} \quad (41)$$

Similarly, the first three candidates are p_{XZ} , p_{XY} , and $4p_{XYZ}$. As for the fourth situation, there is one vector $\bar{w} = (0, 1, 1, 0)$ that belongs to $\mathcal{R}(\mathcal{A}_{\mu_1}) \cap \mathcal{R}(\mathcal{A}_{\mu_3})$ and is not a part of $\bigcup_{k \in \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_k})$. The maximum value of Eq. (23) can be attained, which is one. Thus, the element $\vec{\lambda}(\bar{w}) = p_{XZ} + p_{XY}$ is a candidate. As for the fifth situation, we can find that the first measurement setting, the fifth measurement setting, and the seventh measurement setting measure in the Pauli Z basis the qubit denoted by the number two. So the vector $\bar{w} = (0, 1, 0, 0)$ belongs to $\mathcal{R}(\mathcal{A}_{\mu_1}) \cap \mathcal{R}(\mathcal{A}_{\mu_5}) \cap \mathcal{R}(\mathcal{A}_{\mu_7})$ and is not a part of $\mathcal{R}(\mathcal{A}_{\mu_3})$. The maximum value of Eq. (24) can be attained, which is two. The element $\vec{\lambda}(\bar{w}) = p_{XZ} + 2p_{XYZ}$ is a candidate. As for the sixth situation, there is one vector $\bar{w} = (1, 1, 1, 1)$ that belongs to $\mathcal{R}(\mathcal{A}_{\mu_3}) \cap (\bigcap_{j \in \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_j}))$ and is not a part of $\bigcup_{k \in \mathcal{E}_1} \mathcal{R}(\mathcal{A}_{\mu_k})$. The maximum value of Eq. (25) can be attained, which is four. Thus, the element

$\vec{\lambda}(\vec{w}) = p_{XY} + 4p_{XYZ}$ is a candidate. Let us consider the seventh situation. If we choose a pair of vertices from the set S_1 , i.e., (v_2, v_3) , then there is no measurement setting in step 3 of Protocol 1 measuring in the Pauli Z basis both qubits denoted by the numbers two and three. If we choose a pair of vertices from the set S_2 , i.e., (v_1, v_4) , then there is no measurement settings in step 3 of Protocol 1 measuring in the Pauli Z basis both qubits denoted by the numbers one and four. As a result, The maximum value of Eq. (26) can be attained, which is zero. The element $\vec{\lambda}(\vec{w}) = p_{XZ} + p_{XY} + 0p_{XYZ}$ is a candidate.

Therefore, the optimization problem can be written as

$$\begin{aligned} \min f_{\max}(\{p_{XZ} + 2p_{XYZ}, p_{XY} + 4p_{XYZ}, p_{XZ} + p_{XY}\}) \\ \text{s.t.} \quad 2p_{XZ} + p_{XY} + 4p_{XYZ} = 1, \\ p_{XZ}, p_{XY}, p_{XYZ} \in [0, 1]. \end{aligned} \quad (42)$$

The analytical solution is obtained when three candidates are equal, i.e., $p_{XZ} + 2p_{XYZ} = p_{XY} + 4p_{XYZ} = p_{XZ} + p_{XY}$. It implies that $p_{XY} = 2p_{XYZ}$ and $p_{XZ} = 4p_{XYZ}$. Bringing these into the condition $2p_{XZ} + p_{XY} + 4p_{XYZ} = 1$ leads to

$$p_{XZ} = \frac{2}{7}, \quad p_{XY} = \frac{1}{7}, \quad p_{XYZ} = \frac{1}{14}, \quad \beta(\Psi) = \frac{3}{7}. \quad (43)$$

Using Matlab, we can obtain the numerical solution, which is the same as the analytical solution. Thus, the spectral gap of the verification operator Ψ is $v(\Psi) = 1 - \beta(\Psi) = 4/7$. ■

Theorem 3 gives the spectral gap of the verification operator when the graph state is a 27-qubit brickwork state. Theorem 3 also holds for higher-dimensional brickwork states.

Theorem 3. The second largest eigenvalue and spectral gap of the verification operator Ψ of Protocol 1 for the 27-qubit brickwork state are

$$\beta(\Psi) = 7/15, \quad v(\Psi) = 8/15. \quad (44)$$

Proof. Let $\{\mu_1, \mu_2\}$ be the first group of measurement settings, $\{\mu_3\}$ be the second group of measurement settings, and $\{\mu_4, \mu_5, \dots, \mu_9\}$ be the third group of measurement settings, as illustrated in Fig. 4. Then the corresponding probabilities $\{p_{\mu_i}\}_{i=1}^9$ are $\{p_{XZ}, p_{XZ}, p_{XY}, p_{XYZ}, p_{XYZ}, p_{XYZ}, p_{XYZ}, p_{XYZ}, p_{XYZ}\}$. Let $\mathcal{E}_1 = \{1, 2\}$, $\mathcal{E}_2 = \{3\}$, $\mathcal{E}_3 = \{4, 5, 6, 7, 8, 9\}$ label the three groups of measurement settings.

The first three candidates are p_{XZ} , p_{XY} , $6p_{XYZ}$. As for the fourth candidate, the upper bound of Eq. (23) is one. Thus, the element $\vec{\lambda}(\vec{w}) = p_{XZ} + p_{XY}$ is a candidate. As for the fifth candidate, the measurement settings $\{\mu_5, \mu_6, \mu_7\}$ measure in the Pauli Z basis the qubit denoted by the number 26. Let the vector \vec{w} satisfy $w_l = 1$ for $l = 26$ and $w_l = 0$ for $l \neq 26$. Therefore, the vector \vec{w} belongs to $\mathcal{R}(\mathcal{A}_{\mu_1}) \cap \mathcal{R}(\mathcal{A}_{\mu_5}) \cap \mathcal{R}(\mathcal{A}_{\mu_6}) \cap \mathcal{R}(\mathcal{A}_{\mu_7})$ and is not a part of $\mathcal{R}(\mathcal{A}_{\mu_3})$. The maximum value of Eq. (24) can be attained, which is three. The element $\vec{\lambda}(\vec{w}) = p_{XZ} + 3p_{XYZ}$ is a candidate. As for the sixth candidate, the upper bound of Eq. (25) is six. Thus, the element $\vec{\lambda}(\vec{w}) = p_{XY} + 6p_{XYZ}$ is a candidate. As for the last candidate, we choose a pair of vertices (v_6, v_{26}) . Then the measurement settings $\{\mu_5, \mu_7\}$ perform Pauli Z measurements on both qubits denoted by the numbers six and 26. Therefore the maximum value of Eq. (26) can be attained,

which is two. Thus, the element $\vec{\lambda}(\vec{w}) = p_{XZ} + p_{XY} + 2p_{XYZ}$ is a candidate.

Therefore, the optimization problem can be written as

$$\begin{aligned} \min f_{\max}(\Theta) \\ \text{s.t.} \quad \Theta = \{p_{XZ} + 3p_{XYZ}, p_{XY} + 6p_{XYZ}, \\ p_{XZ} + p_{XY} + 2p_{XYZ}, \\ 2p_{XZ} + p_{XY} + 6p_{XYZ} = 1, \\ p_{XZ}, p_{XY}, p_{XYZ} \in [0, 1]. \end{aligned} \quad (45)$$

Similarly, we can obtain the analytical solution as follows:

$$p_{XZ} = \frac{4}{15}, \quad p_{XY} = \frac{1}{15}, \quad p_{XYZ} = \frac{1}{15}, \quad \beta(\Psi) = \frac{7}{15}. \quad (46)$$

Thus, the spectral gap of the verification operator Ψ is $v(\Psi) = 1 - \beta(\Psi) = 8/15$. ■

Theorem 4 has given the spectral gap of the verification operator when the graph state is a 16-qubit two-dimensional square lattice state.

Theorem 4. The second largest eigenvalue and spectral gap of the verification operator Ψ of Protocol 1 for the 16-qubit two-dimensional square lattice state are

$$\beta(\Psi) = 3/7, \quad v(\Psi) = 4/7. \quad (47)$$

Proof. Let $\{\mu_1, \mu_2\}$ be the first group of measurement settings, $\{\mu_3\}$ be the second group of measurement settings, and $\{\mu_4, \mu_5, \dots, \mu_{11}\}$ be the third group of measurement settings, as shown in Fig. 7. Then the corresponding probabilities $\{p_{\mu_i}\}_{i=1}^{11}$ are $\{p_{XZ}, p_{XZ}, p_{XY}, p_{XYZ}, p_{XYZ}, p_{XYZ}, p_{XYZ}, p_{XYZ}, p_{XYZ}, p_{XYZ}, p_{XYZ}\}$. Let the three groups of measurement settings be labeled by $\mathcal{E}_1 = \{1, 2\}$, $\mathcal{E}_2 = \{3\}$, $\mathcal{E}_3 = \{4, 5, 6, 7, 8, 9, 10, 11\}$.

Similarly, the first two candidates are p_{XZ} , p_{XY} , and the fourth candidate is $p_{XZ} + p_{XY}$. As for the third candidate, we just need to find a vector \vec{w} such that the following Eq. (48) is maximum.

$$|\{i | \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}), i \in \mathcal{E}_3\}|, \quad (48)$$

where \vec{w} has an odd number of ones and satisfies

$$\begin{aligned} \{\text{supp}(\vec{w}) / \{\text{supp}(\vec{w}) \cap S_1\}\} \cap S_2 \neq \emptyset, \\ \{\text{supp}(\vec{w}) / \{\text{supp}(\vec{w}) \cap S_2\}\} \cap S_1 \neq \emptyset. \end{aligned} \quad (49)$$

The vector $\vec{w} = (1, 1, 1, 0, 0, \dots, 0)$ can be chosen to reach the maximum value of Eq. (22). It is easy to check that

$$\begin{aligned} \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_9}) \cap \mathcal{R}(\mathcal{A}_{\mu_{11}}), \\ \vec{w} \notin \mathcal{R}(\mathcal{A}_{\mu_1}) \cup \mathcal{R}(\mathcal{A}_{\mu_2}) \cup \mathcal{R}(\mathcal{A}_{\mu_3}). \end{aligned} \quad (50)$$

As a result, we obtain the third candidate $2p_{XYZ}$. Recall Fig. 7. In the measurement settings μ_9 , the qubits 1 and 2 are measured in the Pauli Y basis, and qubits 3, 7, and 8 (which are adjacent to qubits 1 and 2) are measured in the Pauli Z basis. According to the definition of the matrix of \mathcal{A}_{μ} , the first row of \mathcal{A}_{μ_9} is $r_1 = (1, 1, 0, 0, 0, 0, 0, 1, 0, \dots, 0)$. The second row of \mathcal{A}_{μ_9} is $r_2 = (1, 1, 1, 0, 0, 0, 1, 0, 0, \dots, 0)$. The third row of \mathcal{A}_{μ_9} is $r_3 = (0, 0, 1, 0, 0, 0, 0, 0, 0, \dots, 0)$. The seventh row of \mathcal{A}_{μ_9} is $r_7 = (0, 0, 0, 0, 0, 0, 1, 0, 0, \dots, 0)$. The eighth row of \mathcal{A}_{μ_9} is $r_8 = (0, 0, 0, 0, 0, 0, 0, 1, 0, \dots, 0)$. Adding the rows r_1, r_3, r_8 , i.e., $r_1 \oplus r_3 \oplus r_8$, (or adding the

rows r_2, r_7) leads to the vector $(1, 1, 1, 0, 0, 0, 0, 0, \dots, 0)$, which is one element of \mathcal{A}_{μ_9} . In the measurement settings $\mathcal{A}_{\mu_{11}}$, qubits 2 and 3 are measured in the Pauli Y basis, and qubits 1, 4, 6, and 7 (which are adjacent to qubits 2 and 3) are measured in the Pauli Z basis. In a similar way, the vector $(1, 1, 1, 0, 0, 0, 0, 0, \dots, 0)$ belongs to $\mathcal{A}_{\mu_{11}}$.

We now consider the fifth candidate. The measurement settings $\{\mu_4, \mu_5, \mu_6, \mu_{10}\}$ measure in the Pauli Z basis the qubit denoted by the number two. Let the vector \vec{w} satisfy $w_l = 1$ for $l = 2$ and $w_l = 0$ for $l \neq 2$. Then

$$\begin{aligned} \vec{w} &\in \mathcal{R}(\mathcal{A}_{\mu_1}) \cap \mathcal{R}(\mathcal{A}_{\mu_4}) \cap \mathcal{R}(\mathcal{A}_{\mu_5}) \cap \mathcal{R}(\mathcal{A}_{\mu_6}) \cap \mathcal{R}(\mathcal{A}_{\mu_{10}}), \\ \vec{w} &\notin \mathcal{R}(\mathcal{A}_{\mu_3}). \end{aligned} \quad (51)$$

The maximum value of Eq. (24) can be attained, which is four. The element $\vec{\lambda}(\vec{w}) = p_{XZ} + 4p_{XYZ}$ is a candidate.

As for the sixth candidate, we just need to find a vector \vec{w} that has the even number of ones and satisfies Eq. (49), such that Eq. (25) is maximum. Let the vector \vec{w} satisfy $w_l = 1$ for $l \in \{6, 7, 10, 11\}$ and $w_l = 0$ for $l \notin \{6, 7, 10, 11\}$. Then the vector \vec{w} can reach the maximum value of Eq. (25). We get the sixth candidate $p_{XY} + 4p_{XYZ}$ due to

$$\begin{aligned} \vec{w} &\in \mathcal{R}(\mathcal{A}_{\mu_3}) \cap \mathcal{R}(\mathcal{A}_{\mu_4}) \cap \mathcal{R}(\mathcal{A}_{\mu_6}) \cap \mathcal{R}(\mathcal{A}_{\mu_8}) \cap \mathcal{R}(\mathcal{A}_{\mu_{11}}), \\ \vec{w} &\notin \mathcal{R}(\mathcal{A}_{\mu_1}) \cup \mathcal{R}(\mathcal{A}_{\mu_2}). \end{aligned} \quad (52)$$

For the convenience of calculation, we have replaced the set $\mathcal{R}(\mathcal{A}_{\mu_3})$ with the set Φ . Thus, the vector $(0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, \dots, 0)$ that has the even number of ones belongs to $\mathcal{R}(\mathcal{A}_{\mu_3})$.

As for the seventh candidate, we choose a pair of vertices (v_7, v_{11}) . Then the measurement settings $\{\mu_9, \mu_{10}\}$ perform Pauli Z measurements on both qubits denoted by the numbers seven and eleven. Therefore the maximum value of Eq. (26) can be attained, which is two. Thus, the element $\vec{\lambda}(\vec{w}) = p_{XZ} + p_{XY} + 2p_{XYZ}$ is a candidate.

Therefore, the optimization problem can be written as

$$\begin{aligned} \min \quad & f_{\max}(\Theta) \\ \text{s.t. } \Theta = & \{p_{XZ} + 4p_{XYZ}, p_{XY} + 4p_{XYZ}, \\ & p_{XZ} + p_{XY} + 2p_{XYZ}\}, \\ & 2p_{XZ} + p_{XY} + 8p_{XYZ} = 1, \\ & p_{XZ}, p_{XY}, p_{XYZ} \in [0, 1]. \end{aligned} \quad (53)$$

Similarly, we can obtain the analytical solution as follows:

$$p_{XZ} = \frac{1}{7}, \quad p_{XY} = \frac{1}{7}, \quad p_{XYZ} = \frac{1}{14}, \quad \beta(\Psi) = \frac{3}{7}. \quad (54)$$

Thus, the spectral gap of the verification operator Ψ is $v(\Psi) = 1 - \beta(\Psi) = 4/7$. ■

Theorem 4 also holds for large-scale two-dimensional square lattice states. As for any two-dimensional square lattice state with a larger scale, the third group of measurement settings can be obtained by the extension of measurement settings of Fig. 7. For example, given a $4n$ -qubit two-dimensional square lattice state (including n rows and four columns), the measurement setting μ_4 is constructed as follows: The remaining measurement settings $\{\mu_5, \mu_6, \mu_7, \mu_8, \mu_9, \mu_{10}, \mu_{11}\}$ can be derived in the similar way.

If $n = 4k$, where $k \geq 2$ is a positive integer, then the measurement setting μ_4 measures in the Pauli Y basis each qubit

located in row $4l + 2$ and column 2 or located in row $4l + 3$ and column 2 or located in row $4l + 2$ and column 4 or located in row $4l + 3$ and column 4, where $l = 0, \dots, k - 1$. In addition, the measurement setting μ_4 measures in the Pauli Y basis the each qubit located in row $4l + 4$ and column 1 or located in row $4l + 5$ and column 1 or located in row $4l + 4$ and column 3 or located in row $4l + 5$ and column 3, where $l = 0, \dots, k - 2$. Each qubit located in row 1 and column 1 or located in row 1 and column 3 or located in row $4k$ and column 1 or located in row $4k$ and column 3 is measured in the Pauli X basis. The remaining qubits are measured in the Pauli Z basis.

If $n = 4k + 1$, then the measurement setting μ_4 measures in the Pauli Y basis each qubit located in row $4l + 2$ and column 2 or located in row $4l + 3$ and column 2 or located in row $4l + 2$ and column 4 or located in row $4l + 3$ and column 4, where $l = 0, \dots, k - 1$. In addition, the measurement setting μ_4 measures in the Pauli Y basis the each qubit located in row $4l + 4$ and column 1 or located in row $4l + 5$ and column 1 or located in row $4l + 4$ and column 3 or located in row $4l + 5$ and column 3, where $l = 0, \dots, k - 1$. Each qubit located in row 1 and column 1 or located in row 1 and column 3 is measured in the Pauli X basis. The remaining qubits are measured in the Pauli Z basis.

If $n = 4k + 2$, then the measurement setting μ_4 measures in the Pauli Y basis each qubit located in row $4l + 2$ and column 2 or located in row $4l + 3$ and column 2 or located in row $4l + 2$ and column 4 or located in row $4l + 3$ and column 4, where $l = 0, \dots, k - 1$. In addition, the measurement setting μ_4 measures in the Pauli Y basis the each qubit located in row $4l + 4$ and column 1 or located in row $4l + 5$ and column 1 or located in row $4l + 4$ and column 3 or located in row $4l + 5$ and column 3, where $l = 0, \dots, k - 1$. Each qubit located in row 1 and column 1 or located in row 1 and column 3 or located in row $4k + 2$ and column 2 or located in row $4k + 2$ and column 4 is measured in the Pauli X basis. The remaining qubits are measured in the Pauli Z basis.

If $n = 4k + 3$, then the measurement setting μ_4 measures in the Pauli Y basis each qubit located in row $4l + 2$ and column 2 or located in row $4l + 3$ and column 2 or located in row $4l + 2$ and column 4 or located in row $4l + 3$ and column 4, where $l = 0, \dots, k$. In addition, the measurement setting μ_4 measures in the Pauli Y basis the each qubit located in row $4l + 4$ and column 1 or located in row $4l + 5$ and column 1 or located in row $4l + 4$ and column 3 or located in row $4l + 5$ and column 3, where $l = 0, \dots, k - 1$. Each qubit located in row 1 and column 1 or located in row 1 and column 3 is measured in the Pauli X basis. The remaining qubits are measured in the Pauli Z basis.

To solve the spectral gap, we only need to consider the fifth candidate, the sixth candidate, and the seventh candidate. According to the construction of the third group of measurement settings, there are at most four measurement settings that measure the same qubit in the Pauli Z basis. It implies the fifth candidate is $p_{XZ} + 4p_{XYZ}$. In addition, for any higher dimensional cluster state, we can find a subgraph corresponding to an 4-qubit ring cluster state. There is always one measurement setting that measures in the Pauli Y basis qubits on one edge of such a ring graph. It implies the sixth candidate is $p_{XY} + 4p_{XYZ}$. Moreover, there are at

most two measurement settings that measure in the Pauli Z basis two fixed qubits with the same color. It shows that the seventh candidate is $p_{XZ} + p_{XY} + 2p_{XYZ}$. Therefore, the optimization problem has no change and the spectral gap is identical.

C. Verification of two-colorable asymmetric graph states

In this section, we present an efficient verification of two-colorable asymmetric graph states. Consider a graph state $|G\rangle$ corresponding to a graph $G = (V, E)$. the terminology ‘‘asymmetric’’ means that $d(v') \neq d(v'')$, where v' and v'' are two adjacent vertices of the graph G that have the maximum double degree. Our verification protocol is described as follows:

Protocol 2: Verification of two-colorable asymmetric graph states

(1) Perform the measurement settings of step 1 of Protocol 1, where the first measurement setting is performed with probability p'_{XZ} and the second measurement setting is performed with probability p''_{XZ} .

(2) Follow step 2 of Protocol 1.

(3) Follow step 3 of Protocol 1. Assume that $v' \in S_2$, $v'' \in S_1$. The restrictive condition is rewritten as

$$\begin{aligned} \sum_{k=1}^{d(v')+d(v'')} f_k(v_i) &\leq d(v'), \quad \forall v_i \in S_1, \\ \sum_{k=1}^{d(v')+d(v'')} f_k(v_i) &\leq d(v''), \quad \forall v_i \in S_2. \end{aligned} \quad (55)$$

The verification operator of Protocol 2 is

$$\Psi = p'_{XZ}P_1 + p''_{XZ}P_2 + p_{XY}P_3 + p_{XYZ} \sum_{k=1}^{d(v')+d(v'')} P_k. \quad (56)$$

To derive Eq. (55), recall step 3 of Protocol 1. The edge sets $E_1, E_2, \dots, E_{d(v')+d(v'')-1}$ contain the edges $e_1, e_2, \dots, e_{d(v')+d(v'')-1}$, respectively. Let $e_1^{v'}, \dots, e_{d(v')-1}^{v'}$ be the edges, which connect the vertex $v' \in S_2$ and do not connect the vertex $v'' \in S_1$. Let $e_1^{v''}, \dots, e_{d(v'')-1}^{v''}$ be the edges, which connect the vertex v'' and do not connect the vertex v' . As a result, $\{e_1, e_2, \dots, e_{d(v')+d(v'')-1}\} = \{e_1^{v'}, \dots, e_{d(v')-1}^{v'}, e_1^{v''}, \dots, e_{d(v'')-1}^{v''}\}$. For any edge $e \in \{e_1^{v'}, \dots, e_{d(v')-1}^{v'}\}$, there is one measurement setting that measures in the Pauli Y basis the qubits on the edge e . It implies that in the first $d(v') + d(v'') - 1$ measurement settings of the third group of measurement settings, there are $d(v') - 1$ measurement settings that measure in the Pauli Z basis the qubit corresponding to the vertex v'' . Note that the last measurement setting of the third group of measurement settings measure the Pauli Z basis the qubits on the edge $e(v', v'')$. Thus, we can know that there are $d(v')$ measurement settings that measure in the Pauli Z basis the qubit corresponding to the vertex v'' in total, which leads to the first inequality of Eq. (55). The second inequality of Eq. (55) can be obtained in the same way. In addition, if we set $d(v') = d(v'')$, then Eq. (55) becomes Eq. (10) of Protocol 1.

For any two-colorable asymmetric graph state $|G\rangle$, without loss of generality, we assume that $d(v') = \xi_1$,

$d(v'') = \xi_2$. Theorem 5 has given the spectral gap of the verification operator for the general two-colorable asymmetric graph state.

Theorem 5. The second-largest eigenvalue and spectral gap of the verification operator Ψ of protocol 2 for the two-colorable asymmetric graph state $|G\rangle$ are

$$\beta(\Psi) = \frac{\xi_1 + \xi_2 + 1}{2(\xi_1 + \xi_2) + 3}, \quad v(\Psi) = \frac{\xi_1 + \xi_2 + 2}{2(\xi_1 + \xi_2) + 3}. \quad (57)$$

Proof. Similar to the proof of Theorem 1, the proof is as follows: Let $\mathcal{E}'_1 = \{1\}$, $\mathcal{E}''_1 = \{2\}$, $\mathcal{E}_1 = \{1, 2\}$, $\mathcal{E}_2 = \{3\}$, $\mathcal{E}_3 = \{4, \dots, 3 + d(v') + d(v'')\}$. The first situation needs to find one vector \bar{w} such that Eq. (58) is maximum:

$$\left| \left\{ i \mid \bar{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}), \bar{w} \notin \bigcup_{j \in \mathcal{E}_2 \cup \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_j}), i \in \mathcal{E}'_1 \right\} \right|. \quad (58)$$

The second situation needs to find one vector \bar{w} such that Eq. (59) is maximum:

$$\left| \left\{ i \mid \bar{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}), \bar{w} \notin \bigcup_{j \in \mathcal{E}_2 \cup \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_j}), i \in \mathcal{E}''_1 \right\} \right|. \quad (59)$$

The third situation is just the second situation of the proof of Theorem 2. The fourth situation is just the third situation of the proof of Theorem 2. The fifth situation needs to find one vector \bar{w} such that Eq. (60) is maximum:

$$\left| \left\{ (i, j) \mid \bar{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}), \bar{w} \notin \bigcup_{k \in \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_k}), i \in \mathcal{E}'_1, j \in \mathcal{E}_2 \right\} \right|. \quad (60)$$

The sixth situation needs to find one vector \bar{w} such that Eq. (61) is maximum:

$$\left| \left\{ (i, j) \mid \bar{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}), \bar{w} \notin \bigcup_{k \in \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_k}), i \in \mathcal{E}''_1, j \in \mathcal{E}_2 \right\} \right|. \quad (61)$$

The seventh situation needs to find one vector \bar{w} such that Eq. (62) is maximum:

$$\left| \left\{ (i, j) \mid \bar{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}), \bar{w} \notin \bigcup_{k \in \mathcal{E}_2} \mathcal{R}(\mathcal{A}_{\mu_k}), i \in \mathcal{E}'_1, j \in \mathcal{E}_3 \right\} \right|. \quad (62)$$

The eighth situation needs to find one vector \vec{w} such that Eq. (63) is maximum:

$$\left\{ \begin{array}{l} (i, j) \mid \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}), \\ \vec{w} \notin \bigcup_{k \in \mathcal{E}_3} \mathcal{R}(\mathcal{A}_{\mu_k}), i \in \mathcal{E}'_1, j \in \mathcal{E}_3 \end{array} \right\}. \quad (63)$$

The ninth situation is just the sixth situation of the proof of Theorem 2. The tenth situation needs to find one vector \vec{w} such that Eq. (64) is maximum:

$$\left\{ (i, j, k) \mid \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}) \cap \mathcal{R}(\mathcal{A}_{\mu_k}), \right. \\ \left. i \in \mathcal{E}'_1, j \in \mathcal{E}_2, k \in \mathcal{E}_3 \right\}. \quad (64)$$

The last situation needs to find one vector \vec{w} such that Eq. (65) is maximum:

$$\left\{ (i, j, k) \mid \vec{w} \in \mathcal{R}(\mathcal{A}_{\mu_i}) \cap \mathcal{R}(\mathcal{A}_{\mu_j}) \cap \mathcal{R}(\mathcal{A}_{\mu_k}), \right. \\ \left. i \in \mathcal{E}'_1, j \in \mathcal{E}_2, k \in \mathcal{E}_3 \right\}. \quad (65)$$

Similarly, the first six candidates are p'_{XZ} , p''_{XZ} , p_{XY} , $(\xi_1 + \xi_2)p_{XYZ}$, $p'_{XZ} + p_{XY}$, $p''_{XZ} + p_{XY}$. We just need to consider the last five candidates. Let us focus on the third group of measurement settings. First, there are at most ξ_1 measurement settings that measure in the Pauli Z basis the same qubit whose corresponding vertex belongs to the set S_1 due to Eq. (55) of step 3 of Protocol 2. The upper bound of Eq. (62) is ξ_1 . The element $p'_{XZ} + \xi_1 p_{XYZ}$ is a candidate. Second, there are at most ξ_2 measurement settings that measure in the Pauli Z basis the same qubit whose corresponding vertex belongs to the set S_2 due to Eq. (55) of step 3 of Protocol 2. The upper bound of Eq. (63) is ξ_2 . The element $p''_{XZ} + \xi_2 p_{XYZ}$ is a candidate. Third, the upper bound of Eq. (25) is $\xi_1 + \xi_2$. Thus, the element $p_{XY} + (\xi_1 + \xi_2)p_{XYZ}$ is a candidate. Since the number of measurement settings that measure two qubits of the set S_1 in the Pauli Z basis is not more than the number of measurement settings that measure one qubit of the set S_1 in the Pauli Z basis. In addition, by the principles of the selection of edge sets, if there are ξ_1 measurement settings that measure in the Pauli Z basis the qubit corresponding to one vertex v_i of the set S_1 , then ones cannot find another vertex v_j from the set S_1 such that all these ξ_1 measurement settings measure in the Pauli Z basis the qubit corresponding to the vertex v_j . It means that the number of measurement settings that measure two qubits of the set S_1 in the Pauli Z basis is not more than $\xi_1 - 1$. Therefore, the element $p'_{XZ} + p_{XY} + (\xi_1 - 1)p_{XYZ}$ is a candidate. Similarly, there are at most $\xi_2 - 1$ measurement settings that measure in the Pauli Z basis two fixed qubits whose corresponding vertices belong to the set S_2 . Therefore, the element $p''_{XZ} + p_{XY} + (\xi_2 - 1)p_{XYZ}$ is a candidate.

The optimization problem can be written as

$$\begin{aligned} \min & \quad f_{\max}(\Theta) \\ \text{s.t.} & \quad \Theta = \{p'_{XZ} + \xi_1 p_{XYZ}, p''_{XZ} + \xi_2 p_{XYZ}, \\ & \quad p_{XY} + (\xi_1 + \xi_2)p_{XYZ}, \\ & \quad p'_{XZ} + p_{XY} + (\xi_1 - 1)p_{XYZ}, \end{aligned}$$

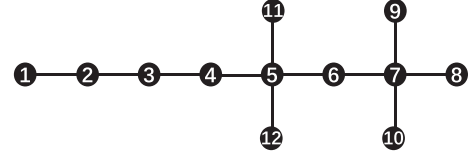


FIG. 9. The example of a 12-qubit asymmetric graph state.

$$\begin{aligned} & p'_{XZ} + p_{XY} + (\xi_2 - 1)p_{XYZ}, \\ & p'_{XZ} + p''_{XZ} + p_{XY} + (\xi_1 + \xi_2)p_{XYZ} = 1, \\ & p'_{XZ}, p''_{XZ}, p_{XY}, p_{XYZ} \in [0, 1]. \end{aligned} \quad (66)$$

Similarly, we can obtain the analytical solution as follows:

$$\begin{aligned} p'_{XZ} &= \frac{\xi_2 + 1}{2(\xi_1 + \xi_2) + 3}, & p''_{XZ} &= \frac{\xi_1 + 1}{2(\xi_1 + \xi_2) + 3}, \\ p_{XY} &= \frac{1}{2(\xi_1 + \xi_2) + 3}, & p_{XYZ} &= \frac{1}{2(\xi_1 + \xi_2) + 3}, \\ \beta(\Psi) &= \frac{\xi_1 + \xi_2 + 1}{2(\xi_1 + \xi_2) + 3}. \end{aligned} \quad (67)$$

Thus, the spectral gap of the verification operator Ψ is $v(\Psi) = 1 - \beta(\Psi) = (\xi_1 + \xi_2 + 2)/(2(\xi_1 + \xi_2) + 3)$. ■

Note that if we substitute $d(v') = \xi_1$, $d(v'') = \xi_2$ with $d(v') = d(v'') = \xi$, then Theorem 5 will be converted to Theorem 1. It means that the verification of two-colorable symmetric graph states is a special case for the verification of two-colorable asymmetric graph states.

Consider the 12-qubit two-colorable asymmetric graph state illustrated in Fig. 9, where $v' = v_6$, $v'' = v_5$, and $d(v') = 2$, $d(v'') = 4$. In the first measurement setting of Protocol 2, the qubits denoted by the numbers 1, 3, 5, 7 are measured in the Pauli Z basis, and the remaining qubits are measured in the Pauli X basis. In the second measurement setting of Protocol 2, the qubits denoted by the numbers 2, 4, 6, 8, 9, 10, 11, 12 are measured in the Pauli Z basis, and the remaining qubits are measured in the Pauli X basis. In the third measurement setting of Protocol 2, the qubits denoted by the numbers 1, 8, 9, 10, 11, 12 are measured in the Pauli Y basis, and the remaining qubits are measured in the Pauli X basis. Utilizing Principles 1 and 2, we can get six measurement settings (the third group of measurement settings), as shown in Fig. 10. Note that the second condition of step 5 of Principle 2 is not required for Protocol 2. It is easy to check that

$$\begin{aligned} \sum_{k=1}^6 f_k(v_i) &\leq 4, \quad \forall v_i \in \{v_2, v_4, v_6, v_8, v_9, v_{10}, v_{11}, v_{12}\}, \\ \sum_{k=1}^6 f_k(v_i) &\leq 2, \quad \forall v_i \in \{v_1, v_3, v_5, v_7\}. \end{aligned} \quad (68)$$

This implies that the restrictive condition of step 3 of Protocol 2 is satisfied.

Theorem 6 has given the spectral gap of the verification operator when the graph state is the 12-qubit asymmetric graph state illustrated in Fig. 9.

Theorem 6. The second largest eigenvalue and spectral gap of the verification operator Ψ of Protocol 2 for the 12-qubit

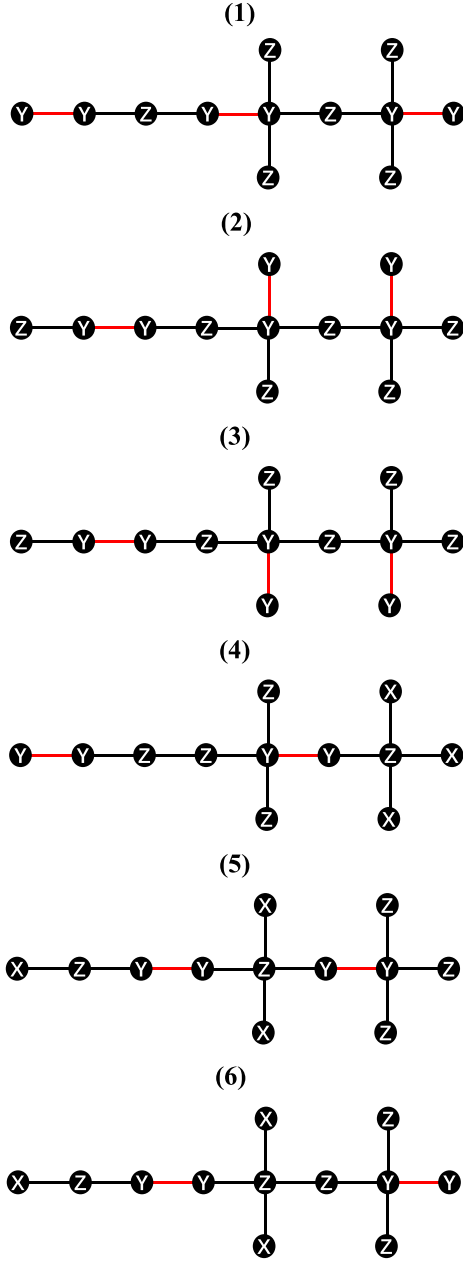


FIG. 10. The third group of measurement settings for the 12-qubit asymmetric graph state.

two-colorable asymmetric graph state are

$$\beta(\Psi) = 7/15, \quad v(\Psi) = 8/15. \quad (69)$$

Proof. The first six candidates are invariant. As for the seventh candidate, in the third group of measurement settings we need to find as many measurement settings as possible, which perform the Pauli Z measurement on one fixed qubit corresponding to a vertex that belongs to the set S_1 . Note that the measurement settings $\{\mu_8, \mu_9\}$ measure in the Pauli Z basis the qubit denoted by the number five. Let the vector \vec{w} satisfy $w_l = 1$ for $l = 5$ and $w_l = 0$ for $l \neq 5$. Then

$$\begin{aligned} \vec{w} &\in \mathcal{R}(\mathcal{A}_{\mu_1}) \cap \mathcal{R}(\mathcal{A}_{\mu_8}) \cap \mathcal{R}(\mathcal{A}_{\mu_9}), \\ \vec{w} &\notin \mathcal{R}(\mathcal{A}_{\mu_3}). \end{aligned} \quad (70)$$

The maximum value of Eq. (62) can be attained, which is two. The element $\vec{\lambda}(\vec{w}) = p'_{XZ} + 2p_{XYZ}$ is a candidate. The eighth candidate can be obtained in a similar way, where the set S_1 is replaced with the set S_2 . Note that the measurement settings $\{\mu_4, \mu_6, \mu_8, \mu_9\}$ measure in the Pauli Z basis the qubit denoted by the number nine. Let the vector \vec{w} satisfy $w_l = 1$ for $l = 9$ and $w_l = 0$ for $l \neq 9$. Then

$$\begin{aligned} \vec{w} &\in \mathcal{R}(\mathcal{A}_{\mu_2}) \cap \mathcal{R}(\mathcal{A}_{\mu_4}) \cap \mathcal{R}(\mathcal{A}_{\mu_6}) \cap \mathcal{R}(\mathcal{A}_{\mu_8}) \cap \mathcal{R}(\mathcal{A}_{\mu_9}), \\ \vec{w} &\notin \mathcal{R}(\mathcal{A}_{\mu_3}). \end{aligned} \quad (71)$$

The maximum value of Eq. (63) can be attained, which is four. The element $\vec{\lambda}(\vec{w}) = p''_{XZ} + 4p_{XYZ}$ is a candidate. The ninth candidate is $p_{XY} + 6p_{XYZ}$.

As for the tenth candidate, in the third group of measurement settings we need to find as many measurement settings as possible, where two fixed qubits corresponding to two vertices of the set S_1 are all measured in the Pauli Z basis. Here, we choose a pair of vertices (v_3, v_7) . Then the measurement setting μ_7 performs Pauli Z measurements on both qubits denoted by the numbers three and seven. Therefore the maximum value of Eq. (64) can be attained, which is one. Thus, the element $\vec{\lambda}(\vec{w}) = p'_{XZ} + p_{XY} + p_{XYZ}$ is a candidate. The last candidate can be obtained in a similar way, where the set S_1 is replaced with the set S_2 . Here, we choose a pair of vertices (v_6, v_{10}) . Then the measurement settings $\{\mu_4, \mu_5, \mu_9\}$ perform Pauli Z measurements on both qubits denoted by the numbers six and ten. Therefore the maximum value of Eq. (65) can be attained, which is three. Thus, the element $\vec{\lambda}(\vec{w}) = p''_{XZ} + p_{XY} + 3p_{XYZ}$ is a candidate.

Therefore, the optimization problem can be written as

$$\begin{aligned} \min & \quad f_{\max}(\Theta) \\ \text{s.t. } \Theta &= \{p'_{XZ} + 2p_{XYZ}, p''_{XZ} + 4p_{XYZ}, p_{XY} + 6p_{XYZ}, \\ & p'_{XZ} + p_{XY} + p_{XYZ}, p''_{XZ} + p_{XY} + 3p_{XYZ}\}, \\ & p'_{XZ} + p''_{XZ} + p_{XY} + 6p_{XYZ} = 1, \\ & p'_{XZ}, p''_{XZ}, p_{XY}, p_{XYZ} \in [0, 1]. \end{aligned} \quad (72)$$

Similarly, we can obtain the analytical solution as follows:

$$\begin{aligned} p'_{XZ} &= \frac{5}{15}, \quad p''_{XZ} = \frac{3}{15}, \quad p_{XY} = \frac{1}{15}, \\ p_{XYZ} &= \frac{1}{15}, \quad \beta(\Psi) = \frac{7}{15}. \end{aligned} \quad (73)$$

Thus, the spectral gap of the verification operator Ψ is $v(\Psi) = 1 - \beta(\Psi) = 8/15$. ■

D. Comparison with previous protocols

Figure 11 has demonstrated the spectral gap $v(\Psi)$ of the verification operator of our protocols, which is a function of $d(v')$ and $d(v'')$. It shows that $v(\Psi) > 0.5$ and $v(\Psi)$ approaches 0.5 when $d(v')$ or $d(v'')$ becomes larger. The cover protocol of Ref. [29] can achieve $v(\Psi) = 0.5$. To verify a two-colorable graph state $|G\rangle$ within infidelity ϵ and significance level δ , by Eq. (3), the number of tests required for our protocols is

$$N = \left\lceil \frac{\ln \delta}{\ln \left(1 - \frac{d(v') + d(v'') + 2}{2(d(v') + d(v'')) + 3} \epsilon \right)} \right\rceil \leq \left\lceil \frac{\ln \delta^{-1}}{\frac{d(v') + d(v'') + 2}{2(d(v') + d(v'')) + 3} \epsilon} \right\rceil. \quad (74)$$

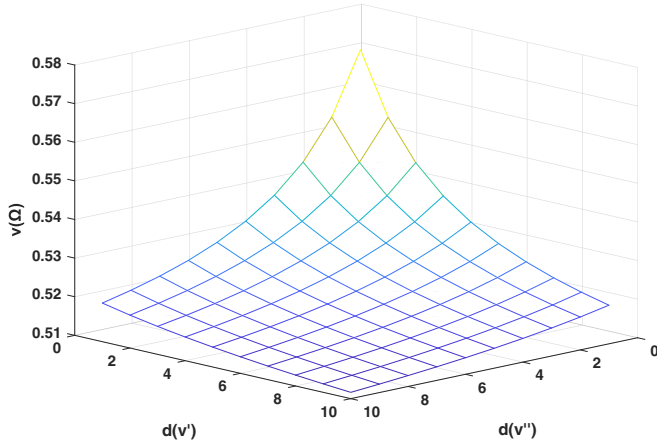


FIG. 11. The spectral gap $v(\Psi)$ of our verification operator as a function of $d(v')$ and $d(v'')$.

The number of tests required for the cover protocol of Ref. [29] is

$$N = \left\lceil \frac{\ln \delta}{\ln(1 - \frac{1}{2}\epsilon)} \right\rceil \leq \left\lceil \frac{2 \ln \delta^{-1}}{\epsilon} \right\rceil. \quad (75)$$

The left plot of Fig. 12 has shown the number of tests required for different protocols as a function of the significance level δ when the infidelity is $\epsilon = 0.001$. The right plot of Fig. 12 has shown the number of tests required for different protocols as a function of the infidelity ϵ when the significance level is $\delta = 0.001$. Here, our protocol with $v(\Psi) = 6/11$ means our verification method for a two-colorable graph state satisfying $d(v') + d(v'') = 4$. Our protocol with $v(\Psi) = 8/15$ means our verification method for a two-colorable graph state satisfying $d(v') + d(v'') = 6$. Our protocol with $v(\Psi) = 10/19$ means our verification method for a two-colorable graph state satisfying $d(v') + d(v'') = 8$. Figure 12 indicates that our protocols are more efficient than the cover protocol of Ref. [29].

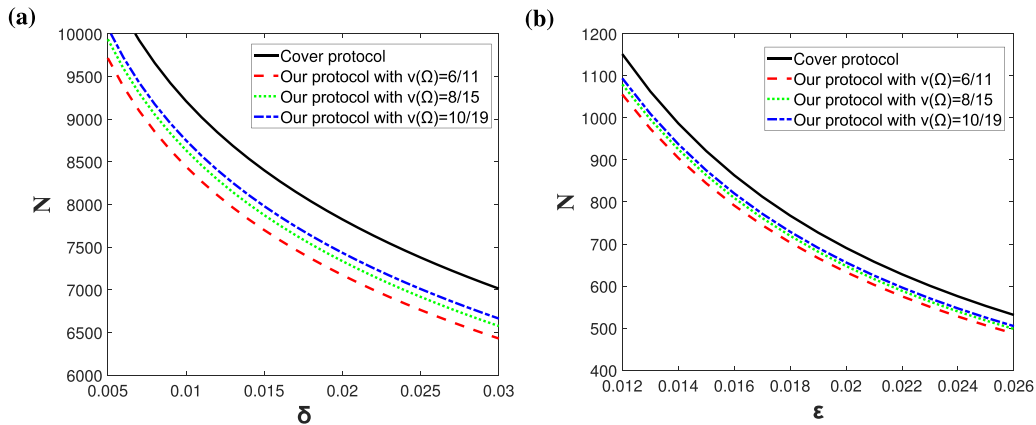


FIG. 12. A comparison of the number of tests in our protocols and the cover protocol. (a) To verify the graph state within infidelity $\epsilon = 0.001$, the number N of tests is a function of the significance level δ . (b) To verify the graph state within significance level $\delta = 0.001$, the number N of tests is a function of the infidelity ϵ .

IV. VERIFICATION OF GRAPH STATES IN THE NOISY SCENARIO

In this section, we propose a method that verifies graph states in a realistic experimental scenario where the measurements are subject to noise. Existing methods [19,29,30] using quantum state verification (QSV) need perfect measurements to verify graph states. Here, we extend QSV to the case where the measurement devices are noisy.

In previous works [18,36–38] on fault tolerant quantum verification, the purpose and method are different. The verification framework of Fujii *et al.* [36] has used the technology of topological protection to verify three-dimensional two-colorable graph states. Hayashi *et al.* [37] have utilized self-testing to verify three-colorable graph states, where the prior-trusted devices for performing measurements or preparing entangled states are not needed. The verification protocol of Takeuchi *et al.* [38] has used Serfling's bound to verify multiple quantum states (including qudit graph states and hypergraph states), where the noisy robustness just considered slightly noisy graph states. Li *et al.* [18] have realized the robust verification of graph states under the framework of QSV, where fault tolerance is based on the design of threshold for the permitted number of failed tests. Here, our fault tolerant verification protocol has settled the robust verification of two-colorable graph states by overcoming the effect of noisy measurement device on the QSV technology.

If the measurement devices are perfect, the verification operator is

$$\Psi = \sum_i p_i P_i. \quad (76)$$

We start by introducing a noise parameter $\eta \in [0, 1]$. If the measurements corresponding to the projector P_i are noisy, we denote the projector onto the pass eigenspace as

$$\eta P_i + (1 - \eta) \frac{\mathbb{I}}{2}. \quad (77)$$

It means that each measurement proceeds perfectly with probability η , and each measurement randomly gives either a ± 1 outcome with probability $1 - \eta$. Thus, the verification

operator in the noisy scenario is written as

$$\Psi' = \sum_i p_i \left[\eta P_i + (1 - \eta) \frac{\mathbb{I}}{2} \right] = \eta \Psi + (1 - \eta) \frac{\mathbb{I}}{2}. \quad (78)$$

When the infidelity of one quantum state σ is at least ϵ , i.e., $\langle G|\sigma|G \rangle \leq 1 - \epsilon$, the maximum average probability that σ can pass a test is given by

$$\begin{aligned} \max_{\langle G|\rho|G \rangle \leq 1 - \epsilon} \text{Tr}(\Psi' \rho) &= \max_{\langle G|\rho|G \rangle \leq 1 - \epsilon} \eta \text{Tr}(\Psi \rho) + \frac{1 - \eta}{2} \\ &= \eta(1 - v(\Psi)\epsilon) + \frac{1 - \eta}{2}. \end{aligned} \quad (79)$$

The probability that all states $\rho_1, \rho_2, \dots, \rho_N$ in N tests are passed is

$$\begin{aligned} \prod_{i=1}^N \text{Tr}(\Psi' \rho_i) &\leq \prod_{i=1}^N \left[\eta(1 - v(\Psi)\epsilon_i) + \frac{1 - \eta}{2} \right] \\ &\leq \left[\eta(1 - v(\Psi)\bar{\epsilon}) + \frac{1 - \eta}{2} \right]^N, \end{aligned} \quad (80)$$

where $\bar{\epsilon} = \sum_i \epsilon_i / N$ with $\epsilon_i = 1 - \langle G|\rho_i|G \rangle$ is the average infidelity. If N tests are passed, the condition $\bar{\epsilon} < \epsilon$ holds with significance level

$$\delta = \left[\eta(1 - v(\Psi)\epsilon) + \frac{1 - \eta}{2} \right]^N. \quad (81)$$

Therefore, the number of tests required for verifying quantum states within infidelity ϵ and significance level δ is

$$N(\epsilon, \delta, \Psi, \eta) = \left\lceil \frac{\ln \delta}{\ln \left[\eta(1 - v(\Psi)\epsilon) + \frac{1 - \eta}{2} \right]} \right\rceil. \quad (82)$$

V. VERIFICATION OF TWO-COLORABLE GRAPH STATES IN THE ADVERSARIAL SCENARIO

Section III has accomplished the verification of two-colorable graph states in the nonadversarial scenario, where all quantum states $\rho_1, \rho_2, \dots, \rho_N$ prepared in N tests are independent of each other. However, the device in adversarial scenario may be controlled by any malicious adversary and prepare an arbitrary entangled state. The verification of graph states in the adversarial scenario is important to secure quantum computing, such as blind quantum computing [15,39,40]. In this section, we extend our verification protocols to the adversarial scenario and apply it to verifiable blind quantum computing.

A general method of Refs. [41,42] has considered the verification of pure quantum states in the adversarial scenario. It indicates that, in order to verify the target state $|\Psi\rangle$ within infidelity ϵ and significance level δ , the number of tests required by the verification operator Ψ in the adversarial scenario is

$$N \leq \left\lceil \frac{1 - \delta}{v(\Psi)\delta\epsilon} \right\rceil. \quad (83)$$

As for the cover protocol of Ref. [29], the number of tests required for verifying the graph state $|G\rangle$ within infidelity

ϵ and significance level δ is

$$N \leq \left\lceil \frac{2(1 - \delta)}{\delta\epsilon} \right\rceil. \quad (84)$$

As for our verification protocols for two-colorable graph states, the number of tests required for verifying the graph state $|G\rangle$ within infidelity ϵ and significance level δ is

$$N \leq \left\lceil \frac{1 - \delta}{\frac{d(v') + d(v'') + 2}{2(d(v') + d(v'') + 3)} \delta\epsilon} \right\rceil. \quad (85)$$

To reduce the overhead of the number of tests in the adversarial scenario, we can construct a new verification protocol referred to the hedged protocol as follows. The hedged verification operator is written as

$$\Psi_\gamma = (1 - \gamma)\Psi + \gamma\mathbb{I}, \quad (86)$$

where $\gamma \in [0, 1]$. It means that the verification protocol performs the verification operator Ψ with probability $1 - \gamma$ and performs the trivial test with probability γ . According to Ref. [42]. If $\gamma = v(\Psi)/e$, then the number of tests required for verifying the graph state $|G\rangle$ within infidelity ϵ and significance level δ is

$$N \leq \frac{[1 + ev(\Psi) - v(\Psi)] \ln(F\delta)^{-1}}{v(\Psi)\epsilon}, \quad (87)$$

where $F = 1 - \epsilon$. To verify $|G\rangle$ within infidelity ϵ and significance level δ , the number of tests required for the hedged cover protocol of Ref. [29] is

$$N \leq \frac{(1 + e) \ln(F\delta)^{-1}}{\epsilon}. \quad (88)$$

To verify $|G\rangle$ within infidelity ϵ and significance level δ , the number of tests required for our hedged protocol is

$$N \leq \left(\frac{2[d(v') + d(v'')] + 3}{d(v') + d(v'') + 2} + e - 1 \right) \frac{\ln(F\delta)^{-1}}{\epsilon}. \quad (89)$$

According to above analysis, it indicates that in the adversarial scenario, our verification protocols for two-colorable graph states are more efficient than the cover protocol of Ref. [29].

Since the adversarial scenario has considered that the device may prepare an arbitrary entangled state ρ on the system $\mathcal{H}^{\otimes(N+1)}$ and is aimed at keeping the infidelity of the reduced state on the remaining system less than ϵ by performing N tests on N systems which are chosen uniformly at random. In each test, one verification strategy Ψ is performed on one system. The state on the remaining system is accepted if and only if all N tests are passed. Therefore, bring our verification strategy Ψ [see Eqs. (15) and (56)] for two-colorable graph states into above adversarial scenario results in the sampling complexity of Eq. (85) or Eq. (89).

The relation of our verification strategy to homogeneous strategy is explained as follows: Here, a verification strategy for the graph state $|G\rangle$ is homogeneous if the verification operator Ψ can be written as the following form:

$$\Psi = |G\rangle\langle G| + t(I - |G\rangle\langle G|), \quad (90)$$

where $0 \leq t < 1$. All eigenvalues of the homogeneous verification strategy are equal to t except for the largest one. In addition, the homogeneous verification strategy means that

the verification protocol performs the test $|G\rangle\langle G|$ with probability $1 - t$ and the trivial test with probability t . Since the projector onto $|G\rangle$ reads

$$|G\rangle\langle G| = \prod_{i \in V} \frac{I + g_i}{2}, \quad (91)$$

our verification operator [see Eqs. (15) and (56)] cannot be characterized by above form. It indicates that our verification strategy is not homogeneous. Readers can refer to Ref. [42] for the sample complexity of homogeneous strategies in the adversarial scenario. The homogeneous strategy can be implemented by local projective measurements when t is sufficiently large [19]. However, our verification strategy can be realized by Pauli X , Pauli Y , and Pauli Z measurements.

Now we show how to apply our verification protocols for two-colorable graph states in the adversarial scenario to the verification of blind quantum computation. The two-colorable graph states used to achieve blind quantum computation are mainly the brickwork state and the two-dimensional square lattice state. According to Eqs. (44) and (87), the number of tests required for verifying the brickwork state in the adversarial scenario within infidelity ϵ and significance level δ is

$$N \leq (7/8 + e) \frac{\ln(F\delta)^{-1}}{\epsilon}. \quad (92)$$

Similarly, from Eqs. (47) and (87), the number of tests required for verifying the two-dimensional square lattice state in the adversarial scenario within infidelity ϵ and significance level δ is

$$N \leq (3/4 + e) \frac{\ln(F\delta)^{-1}}{\epsilon}. \quad (93)$$

Recall our verification strategy for the two-dimensional square lattice state. There are 11 measurement settings needed to achieve efficient verification, i.e., $v(\Psi) > 1/2$. In the following, we propose a new verification strategy for the two-dimensional square lattice state, which requires less measurement settings and satisfies $v(\Psi) > 1/2$. Consider a verification operator which is characterized by

$$\Psi = p_{XZ}P_1 + p_{XZ}P_2 + p_{XY}P_3 + p_{XYZ} \sum_{k=1}^{d(v')+d(v'')-1} P'_k. \quad (94)$$

It means that the verification strategy does not contain the measurement setting that performs the Pauli Z measurements on two qubits corresponding to two adjacent vertices v' , v'' that have maximum double degree. Thus the new verification strategy for the two-dimensional square lattice state is the same as before except that the last measurement setting of Fig. 7 is removed. Similarly, the seven candidates remain unchanged, i.e., Eq. (53). Therefore, solving the second largest eigenvalue of the verification operator Ψ is equal to solving the following optimization problem:

$$\begin{aligned} \min \quad & f_{\max}(\Theta) \\ \text{s.t. } \Theta = \{ & p_{XZ} + 4p_{XYZ}, p_{XY} + 4p_{XYZ}, \\ & p_{XZ} + p_{XY} + 2p_{XYZ}, \\ & 2p_{XZ} + p_{XY} + 7p_{XYZ} = 1, \\ & p_{XZ}, p_{XY}, p_{XYZ} \in [0, 1]. \end{aligned} \quad (95)$$

Similarly, we can obtain the analytical solution as follows:

$$p_{XZ} = \frac{2}{13}, \quad p_{XY} = \frac{2}{13}, \quad p_{XYZ} = \frac{1}{13}, \quad v(\Psi) = \frac{7}{13}. \quad (96)$$

According to Eqs. (87) and (96), the number of tests required for verifying the two-dimensional square lattice state in the adversarial scenario within infidelity ϵ and significance level δ is

$$N \leq (6/7 + e) \frac{\ln(F\delta)^{-1}}{\epsilon}. \quad (97)$$

Verifiable blind quantum computing is a secure quantum computing, where a client Alice can delegate a computational task to a quantum server Bob while keeping the privacy and correctness of the computation. Our verification protocol for blind quantum computing is shown as follows:

Protocol 3: Efficient verification of blind quantum computation

(1) Alice asks Bob to prepare $N + 1$ copies of an n -qubit graph state $|G\rangle$ and send all copies to Alice. If the used graph state is the brickwork state, then the number N is set to be the maximum value of Eq. (92). If the used graph state is the two-dimensional square lattice state, then the number N is set to be the maximum value of Eq. (93) [or Eq. (97)]. However, an adversarial Bob will generate an arbitrary state that may be entangled.

(2) Alice uniformly and randomly chooses N copies for testing. For each copy, Alice chooses one measurement setting and performs corresponding measurements on this copy. As for the case of the brickwork state, each measurement setting of the first group of measurement settings is chosen with probability $4/15$, each measurement setting of the second group of measurement settings and Fig. 4 is chosen with probability $1/15$. As for the case of the two-dimensional square lattice state, each measurement setting of the first group and the second group of measurement settings is chosen with probability $1/7$, each measurement setting of Fig. 7 is chosen with probability $1/14$. Otherwise, Alice can adopt the verification strategy corresponding to Eq. (94), i.e., each measurement setting of the first group and the second group of measurement settings is chosen with probability $2/13$, each measurement setting of the first seven measurement settings of Fig. 7 is chosen with probability $1/13$.

(3) The remaining copy is used to accomplish the computational task, where we assume the state is ρ_{tgt} .

(4) If all tests are passed, Alice accepts the result of the computation performed on the last copy.

According to Eqs. (92), (93), and (97), we have the following theorem:

Theorem 7. In Protocol 3, if all tests are passed with the significance level δ , we can ensure that the state ρ_{tgt} satisfies $\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - \epsilon$.

Recently, the protocol of Ref. [16] has given a verification method of graph states without the use of QSV. To verify an n -qubit two-colorable graph state $|G\rangle$, Ref. [16] needs $[n^2 \ln n]$ copies of the graph state to guarantee that if all tests are passed with the significance level $4n^{-\lambda/2}$, the state ρ_{tgt} of the copy

TABLE I. Performance of our verification protocol compared with existing protocols, including the total number Σ of measurement settings, the spectral gap $v(\Psi)$ of the verification operator, the coloring type of verifiable graph states.

Method	Σ	$v(\Psi)$	m -colorable graph states
Optimal verification protocol [30]	Uncertain	$2/3$	$m \geq 2$
Cover protocol [29]	m	$1/m$	$m \geq 2$
Minimax optimal measurement protocol [19]	2^n	$\frac{2^n - 2^{n-1}}{2^n - 1}$	$m \geq 2$
Our protocol	$d(v') + d(v'') + 3$	$\frac{d(v') + d(v'') + 2}{2(d(v') + d(v'')) + 3}$	$m = 2$

used for computation satisfies

$$\langle G | \rho_{\text{tgt}} | G \rangle \geq 1 - \frac{1 + 4\sqrt{\lambda}}{n}, \quad (98)$$

where λ is an arbitrary constant satisfying $\log_n 16 < \lambda < (n-1)^2/16$. To compare our verification protocol of blind quantum computing with Ref. [16], if we require our Protocol 3 to satisfy the same infidelity and the same significance as the protocol of Ref. [16], i.e.,

$$\epsilon = \frac{1 + 4\sqrt{\lambda}}{n}, \quad \delta = 4n^{-\lambda/2}, \quad (99)$$

then the number of copies of the graph state required for Protocol 3 is

$$\begin{aligned} N + 1 &\leq \frac{1}{\epsilon} \left(\frac{1}{v(\Psi)} + e - 1 \right) \ln [(1 - \epsilon)\delta]^{-1} + 1 \\ &\approx \frac{1}{1 + 4\sqrt{\lambda}} \left(\frac{1}{v(\Psi)} + e - 1 \right) n \ln n^{\lambda/2} \\ &= O(n \ln n). \end{aligned} \quad (100)$$

It shows that our method of verifiable blind quantum computing can reduce the resource overhead from the quadratic scale to the nearly linear scale.

VI. CONCLUSION

To verify two-colorable graph states with high precision and low resource overhead, we have proposed a verification protocol for the symmetric case and the asymmetric case, respectively. Using our method, the verification strategy of the high-dimensional graph states can be obtained from the verification strategy of the low-dimensional graph states. Table I has compared the performance of our verification protocol with existing protocols [19,29,30]. The results indicate that for the verification of the two-colorable graph states, our protocol needs less measurement settings than the optimal verification protocol [30] and the minimax optimal measurement protocol [19] and needs more measurement settings than the cover

protocol [29]. Note that the number of measurement settings in our protocol is a constant that is not related to the size n of the graph state. However, the verification strategy of optimal verification protocol [30] is unknown, which depends on a classical algorithm. Therefore, our method is more feasible in practice. In addition, the spectral gap $v(\Psi)$ of the verification operator of our protocol is more than the cover protocol [29] and the minimax optimal measurement protocol [19] and is less than the optimal verification protocol [30]. It reflects that our verification protocol is efficient. We have given several examples, such as the brickwork state and the two-dimensional square lattice state, to demonstrate how to obtain concrete verification strategies.

We have extended the verification of graph states to the noisy scenario. In this scenario, the measurement device is not perfect. It is significant to the quantum verification of noisy intermediate-scale quantum (NISQ) [43] era. In addition, we have extended the verification of two-colorable graph states to the adversarial scenario. One important application of our verification method is the verifiable blind quantum computing, which has achieved the quadratic improvement over the resource overhead than the known best approach [16] that is not based on the QSV technology.

In the future, one can consider how to construct an efficient verification method for m -colorable graph states when $m > 2$. Moreover, the ultimate purpose is to realize the higher spectral gap of the verification operator with the less measurement settings. Finally, one can consider a robust verification of graph states, where the noise on measurement device is in a more complex form.

ACKNOWLEDGMENTS

This work is partly supported by Guangdong Basic and Applied Basic Research Foundation under Grant No. 2024A1515013066, the National Natural Science Foundation of China under Grant No. 62302318, and Shenzhen Science and Technology Program under Grant No. 20231124122522001.

- [1] S. Aaronson and A. Arkhipov, *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing (STOC)* (ACM, New York, 2011), p. 333.
[2] P. W. Shor, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE Computer Society Press, Los Alamitos, 1994), p. 124.

- [3] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, *Nat. Rev. Phys.* **2**, 382 (2020).
[4] M. Kliesch and I. Roth, *PRX Quantum* **2**, 010201 (2021).
[5] Z. Hradil, *Phys. Rev. A* **55**, R1561(R) (1997).
[6] D. Hangleiter, M. Kliesch, M. Schwarz, and J. Eisert, *Quantum Sci. Technol.* **2**, 015004 (2017).

- [7] S. T. Flammia and Y.-K. Liu, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [8] I. Šupić and J. Bowles, *Quantum* **4**, 337 (2020).
- [9] Y.-C. Liu, J. Shang, X.-D. Yu, and X. Zhang, *Phys. Rev. A* **101**, 042315 (2020).
- [10] E. Magesan, J. M. Gambetta, and J. Emerson, *Phys. Rev. Lett.* **106**, 180504 (2011).
- [11] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, *Nat. Phys.* **14**, 595 (2018).
- [12] J. F. Fitzsimons and E. Kashefi, *Phys. Rev. A* **96**, 012303 (2017).
- [13] M. Hayashi and T. Morimae, *Phys. Rev. Lett.* **115**, 220502 (2015).
- [14] U. Mahadev, *Proceedings of the 59th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE Computer Society Press, Paris, 2018), p. 259.
- [15] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, *Theory Comput. Syst.* **63**, 715 (2019).
- [16] Q. Xu, X. Tan, R. Huang, and M. Li, *Phys. Rev. A* **104**, 042412 (2021).
- [17] D. Leichtle, L. Music, E. Kashefi, and H. Ollivier, *PRX Quantum* **2**, 040302 (2021).
- [18] Z. Li, H. Zhu, and M. Hayashi, *npj Quantum Inf.* **9**, 115 (2023).
- [19] S. Pallister, N. Linden, and A. Montanaro, *Phys. Rev. Lett.* **120**, 170502 (2018).
- [20] M. Hayashi, K. Matsumoto, and Y. Tsuda, *J. Phys. A: Math. Gen.* **39**, 14427 (2006).
- [21] M. Hayashi, *New J. Phys.* **11**, 043028 (2009).
- [22] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, *Nat. Commun.* **6**, 8498 (2015).
- [23] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, *Phys. Rev. Lett.* **105**, 150401 (2010).
- [24] H. Zhu and M. Hayashi, *Phys. Rev. A* **99**, 052346 (2019).
- [25] Z. Li, Y.-G. Han, and H. Zhu, *Phys. Rev. A* **100**, 032316 (2019).
- [26] K. Wang and M. Hayashi, *Phys. Rev. A* **100**, 032315 (2019).
- [27] X.-D. Yu, J. Shang, and O. Gühne, *npj Quantum Inf.* **5**, 112 (2019).
- [28] Z. Li, Y.-G. Han, and H. Zhu, *Phys. Rev. Appl.* **13**, 054002 (2020).
- [29] H. Zhu and M. Hayashi, *Phys. Rev. Appl.* **12**, 054047 (2019).
- [30] N. Dangniam, Y.-G. Han, and H. Zhu, *Phys. Rev. Res.* **2**, 043323 (2020).
- [31] M. Hayashi and Y. Takeuchi, *New J. Phys.* **21**, 093060 (2019).
- [32] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang, *Phys. Rev. Appl.* **12**, 044020 (2019).
- [33] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Phys. Rev. Lett.* **101**, 060401 (2008).
- [34] H. J. Briegel, D. E. Browne, W. Dur, R. Raussendorf, and M. Van den Nest, *Nat. Phys.* **5**, 19 (2009).
- [35] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
- [36] K. Fujii and M. Hayashi, *Phys. Rev. A* **96**, 030301(R) (2017).
- [37] M. Hayashi and M. Hajdusek, *Phys. Rev. A* **97**, 052308 (2018).
- [38] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, *npj Quantum Inf.* **5**, 27 (2019).
- [39] Y. Takeuchi and T. Morimae, *Phys. Rev. X* **8**, 021060 (2018).
- [40] S. Ma, C. Zhu, X. Liu, H. Li, and S. Li, *Phys. Rev. A* **109**, 012606 (2024).
- [41] H. Zhu and M. Hayashi, *Phys. Rev. Lett.* **123**, 260504 (2019).
- [42] H. Zhu and M. Hayashi, *Phys. Rev. A* **100**, 062335 (2019).
- [43] J. Preskill, *Quantum* **2**, 79 (2018).