Fidelity-estimation method for graph states with depolarizing noise

Tomonori Tanizawa,[1] Yuki Takeuchi [ORCID],[2,3,*] Shion Yamashika [ORCID],[1] Ryosuke Yoshii,[4] and Shunji Tsuchiya [ORCID][1,†]

[1]*Department of Physics, Chuo University, 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan*

[2]*NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[3]*Research Center for Theoretical Quantum Information, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*

[4]*Center for Liberal Arts and Sciences, Sanyo-Onoda City University, 1-1-1 Daigaku-Dori, Sanyo-Onoda, Yamaguchi 756-0884, Japan*

Graph states are entangled states that are useful for several quantum information processing tasks, such as measurement-based quantum computation and quantum metrology. As the size of graph states realized in experiments increases, it becomes more essential to devise efficient methods for estimating the fidelity between the ideal graph state and an experimentally realized actual state. Any efficient fidelity-estimation method, in general, must use multiple experimental settings, i.e., needs to switch between at least two measurements. Recently, it has been shown that a single measurement is sufficient if the noise can be modeled as the phase-flip error. Since the bit-flip error should also occur in several experiments, it is desired to extend this simplest method to noise models that include phase and bit-flip errors. However, it seems to be nontrivial because their result strongly depends on properties of the phase-flip error. In this paper, by analyzing effects of the bit-flip error on stabilizer operators of graph states, we achieve the extension to the depolarizing noise, which is a major noise model including phase and bit-flip errors. We also numerically evaluate our simplest method for noise models interpolating between the phase-flip and depolarizing noises.

I. INTRODUCTION

Graph states [1] are entangled states that are useful for several quantum information processing tasks, such as measurement-based quantum computation (MBQC) [2], quantum metrology [3], and quantum communication [4]. Given this versatility, tremendous theoretical [5–9] and experimental [10–18] efforts have been devoted to increase the size of graph states. As the size n of graph states realized in experiments increases, it becomes more essential to devise efficient methods estimating the fidelity $\langle G|\rho|G\rangle$ between the ideal n-qubit graph state $|G\rangle$ and an experimentally realized actual state $\rho \equiv \mathcal{E}(|G\rangle\langle G|)$ that suffers from some noise $\mathcal{E}$. This fidelity estimation is also called the verification of graph states. Several efficient verification methods have been proposed for graph states [19–30]. These methods proceed as follows: (i) Each qubit of N_c copies of ρ is given to a verifier one by one. (ii) The verifier randomly chooses a measurement basis from N_m kinds of measurements and measures the received state ρ in this basis, repeating the same procedure for all copies of ρ. (iii) By processing all measurement outcomes with a classical computer, the verifier outputs an estimated value of (or a lower bound on) the fidelity $\langle G|\rho|G\rangle$. In most cases, to reduce the burden on the verifier as much as possible, only nonadaptive single-qubit projective measurements and efficient classical operations are required for the verifier. In this paper, we consider the same restriction on the verifier.

In the evaluation of verification protocols, two parameters N_c and N_m are usually considered. So far, several attempts to reduce the number N_c of copies have been done, and Zhu and Hayashi finally constructed an optimal verification protocol [27] such that $N_c = \Theta(\epsilon^{-1} \ln \delta^{-1})$ to guarantee $\langle G|\rho|G\rangle \geqslant 1 - \epsilon$ with significance level δ. As a remarkable property, the number N_c in their optimal protocol does not depend on the size n of the graph state $|G\rangle$.

On the other hand, the optimality of the number N_m of measurement settings is less explored. In many practical cases, the switching of measurement settings could be slow and, in some cases, it may be demanding or impossible (e.g., see Ref. [31]). Furthermore, since the measurement error is the most dominant in some state-of-the-art experiments [32], the reduction of the number of measurement settings should be helpful to realize verification protocols with high accuracy. Therefore, it is important to reduce N_m (ultimately to one) under the assumption that the verifier can perform only nonadaptive single-qubit projective measurements. However, under this assumption, it has been shown that at least two measurement settings are required for the verification of any bipartite pure entangled state if $\mathcal{E}$ is an arbitrary noise [31]. Since bipartite pure entangled states include a subclass of graph states, their result prevents the possibility of $N_m = 1$ for general noises. Even if adaptive measurements are allowed for the verifier, at least two measurement settings are still necessary [27]. Indeed, although several verification protocols were proposed for graph states [19–30], they require multiple measurement bases.

*yuki.takeuchi@ntt.com

†tsuchiya@phys.chuo-u.ac.jp

Recently, by restricting the noise model (i.e., by fixing $\mathcal{E}$), a verification protocol achieving $N_m = 1$ has been constructed [33]. In this protocol, $\mathcal{E}$ is assumed to be the phase-flip error, and they have achieved the optimal number of N_m by using properties of the phase-flip error. More precisely, from the commutation relations between Pauli operators and the phase-flip error, they have shown that measurements of a single stabilizer operator of $|G\rangle$ are sufficient to estimate a lower bound on the fidelity with high accuracy. Therefore, it is nontrivial whether $N_m = 1$ can be achieved for other noise models including bit-flip errors.

In this paper, we propose a verification protocol achieving $N_m = 1$ for graph states in the presence of the depolarizing noise [see also Eq. (4)]. Since the depolarizing noise is a major noise model used in several theoretical analyses of quantum error correction [34–36] and error mitigation [37–39], our protocol should also be compatible with other methods handling errors. To construct our protocol, we analyze the effect of depolarizing noise on the fidelity $\langle G|\rho|G\rangle$. As a well-known fact, the depolarizing noise on n qubits can be written as a classical mixture of Pauli noises [40]. We observe that Pauli noises definitely reduce the fidelity if and only if they do not coincide with any stabilizer operator of $|G\rangle$. From this observation, we obtain a single measurement from which we can obtain an approximate value of the fidelity. By using this measurement, we propose a verification protocol for graph states with the depolarizing noise that satisfies $N_c = \Theta(\epsilon^{-2} \ln \delta^{-1})$ and $N_m = 1$. As concrete applications, we apply our verification protocol to n-qubit fully connected graph states, which can be converted to n-qubit Greenberger-Horne-Zeilinger (GHZ) states by local Clifford operations [41], and cluster states. Since cluster states are resource states of universal MBQC, and GHZ states can be used to perform quantum sensing achieving the Heisenberg limit [42] and nonadaptive MBQC with linear side-processing (NMQC$_\oplus$) [43], our protocol can be used to make these protocols verifiable.

We also evaluate our protocol for noise models other than the depolarizing noise. First, we consider the noise model where the phase-flip or depolarizing noise is randomly applied. We show that although it is unknown which noise is applied, our protocol works well for some cluster states. Then we consider noise models interpolating between the phase-flip and depolarizing noises. We numerically evaluate how well our protocol works for these noise models. Lastly, we compare our protocol with previous protocols.

The rest of this paper is organized as follows: In Sec. II, we introduce graph states and the depolarizing noise. In Sec. III, we propose our verification protocol using only a single stabilizer measurement. In Sec. IV, as concrete examples, we apply our protocol in Sec. III to fully connected graph states and cluster states. We also evaluate our protocol in noise models other than the depolarizing noise. In Sec. V, we compare our protocol with previous protocols. Section VI is devoted to the Conclusion and Discussion. In Appendices A–D, we give a proof of Lemma 1, derivation of Eq. (22), proof of Theorem 1, and derivation of Eq. (31), respectively.

II. GRAPH STATES IN THE DEPOLARIZING CHANNEL

In this section, we introduce graph states in the depolarizing channel. To this end, we first define graph states [1]. A graph $G \equiv (V, E)$ is a pair of the set V of n vertices and the set E of edges. The n-qubit graph state $|G\rangle$ that corresponds to the graph G is defined as

$$|G\rangle \equiv \left(\prod_{(i,j) \in E} CZ_{i,j} \right) |+\rangle^{\otimes n}, \quad (1)$$

where $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ with $|0\rangle$ and $|1\rangle$ being, respectively, eigenstates of the Pauli-Z operator with eigenvalues $+1$ and -1, and $CZ_{i,j}$ is the controlled-Z (CZ) gate applied on the ith and jth qubits. The stabilizer generators $\{g_i\}_{i=1}^{n}$ for $|G\rangle$ are defined as

$$g_i \equiv X_i \left(\prod_{j: (i,j) \in E} Z_j \right). \quad (2)$$

Here, X_i and Z_j are the Pauli-X and Z operators for the ith and jth qubits, respectively, and the product of Z_j is taken over all vertices j such that $(i, j) \in E$. For any i and j, two stabilizer generators commute, i.e., $[g_i, g_j] = 0$. The graph state $|G\rangle$ is the unique common eigenstate of $\{g_i\}_{i=1}^{n}$ with eigenvalue $+1$, i.e., $g_i|G\rangle = |G\rangle$ for any i.

A stabilizer S_ℓ is a product of stabilizer generators such that $S_\ell \equiv \prod_{i=1}^{n} g_i^{\ell_i}$, where $\ell \equiv \ell_1 \ell_2 \ldots \ell_n \in \{0, 1\}^n$. It is a tensor product of n single-qubit operators. More precisely, by using $s \in \{0, 1\}$ and $\tau_i \in \{I, X, Y, Z\}$, where I and $Y = iXZ$ are the two-dimensional (2D) identity operator and Pauli-Y operator, respectively, it can be written as

$$S_\ell = (-1)^s \bigotimes_{i=1}^{n} \tau_i. \quad (3)$$

For any ℓ, the equality $S_\ell|G\rangle = |G\rangle$ can be easily checked from Eqs. (1) and (2).

The depolarizing channel is represented by the superoperator [40]

$$\mathcal{E}(\cdot) \equiv (1 - p)I(\cdot)I + \frac{p}{3}[X(\cdot)X + Y(\cdot)Y + Z(\cdot)Z]. \quad (4)$$

It operates independently on each qubit, where bit-flip (Pauli-X error), phase-flip (Pauli-Z error), and bit-phase-flip errors (Pauli-Y error) occur with equal probability $p/3$. The depolarizing channel is a major noise model that is used in several analyses as explained in Sec. I.

Let $\boxed{|\psi\rangle} \equiv |\psi\rangle\langle\psi|$ for any pure state $|\psi\rangle$. The density operator $\rho \equiv \mathcal{E}^{\otimes n}(|G\rangle\langle G|)$ for the graph state in the depolarizing channel can be written as

$$\rho = (1 - p)^n \boxed{|G\rangle} + (1 - p)^{n-1}\frac{p}{3}\sum_{i=1}^{n}\sum_{\mu=1}^{3}\boxed{\sigma_{\mu i}|G\rangle}$$

$$+ (1 - p)^{n-2}\left(\frac{p}{3}\right)^2 \sum_{1 \leqslant i < j \leqslant n}\sum_{\substack{1 \leqslant \mu \leqslant 3 \\ 1 \leqslant \nu \leqslant 3}}\boxed{\sigma_{\mu i}\sigma_{\nu j}|G\rangle} + \ldots$$

$$= (1 - p)^n \boxed{|G\rangle} + \sum_{m=1}^{n}(1 - p)^{n-m}\left(\frac{p}{3}\right)^m$$

$$\times \sum_{\substack{1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant n \\ \mu_1\mu_2\ldots\mu_m \in \{1,2,3\}^m}}\boxed{\left(\prod_{k=1}^{m}\sigma_{\mu_k i_k}\right)|G\rangle}, \quad (5)$$

where $\sigma_{1i} \equiv X_i$, $\sigma_{2i} \equiv Y_i$, and $\sigma_{3i} \equiv Z_i$.

We define the fidelity between two states ρ_1 and ρ_2 as

$$F \equiv \left(\text{Tr}\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right)^2. \tag{6}$$

Note that the fidelity is defined as $\sqrt{F}$ in Ref. [40]. For ease of our argument, we use the definition in Eq. (6). Therefore, the fidelity between the graph state ρ in the depolarizing channel and the ideal state $|G\rangle\langle G|$ can be written as

$$F = \langle G|\rho|G\rangle$$
$$= (1-p)^n + \sum_{m=1}^n (1-p)^{n-m}\left(\frac{p}{3}\right)^m$$
$$\times \sum_{\substack{i_1 < \ldots < i_m \\ \mu_1 \ldots \mu_m}} \langle G|\left(\prod_{k=1}^m \sigma_{\mu_k i_k}\right)|G\rangle^2. \tag{7}$$

The following lemma is useful for evaluation of Eq. (7).

Lemma 1. Suppose $|G\rangle$ is any n-qubit graph state, and $\sigma_{\mu i}$ is the μ component of the Pauli operator for the ith qubit. Then, for any natural number $m(\leqslant n)$,

$$\langle G|\left(\prod_{k=1}^m \sigma_{\mu_k i_k}\right)|G\rangle^2 = 1, \tag{8}$$

if and only if one of $\pm\prod_{k=1}^m \sigma_{\mu_k i_k}$ coincides with a stabilizer of $|G\rangle$. Otherwise, it vanishes.

Although Lemma 1 can be straightforwardly obtained from basic properties of graph states (e.g., see Ref. [44]), we give a proof of Lemma 1 in Appendix A for the completeness of our paper. From Lemma 1,

$$\sum_{\substack{i_1 < \ldots < i_m \\ \mu_1 \ldots \mu_m}} \langle G|\left(\prod_{k=1}^m \sigma_{\mu_k i_k}\right)|G\rangle^2 \tag{9}$$

is equal to the number of the stabilizers that are products of m Pauli operators. Since the number of stabilizers increases exponentially with n, in general, it would be hard to derive the exact value of F for large n. However, in Sec. IV A, we show that F can be represented by a simple formula [Eq. (28)] for fully connected graph states.

We can assume, without loss of generality, that the graph states we consider in this paper have no isolated single qubits because verification of isolated single qubits can be performed independently of other connected qubits. Each stabilizer of a connected graph state is a product of at least two Pauli operators, so the first-order error term ($m = 1$) in Eq. (7) vanishes. The second-order error term ($m = 2$) also vanishes for any graph state that has no stabilizers consisting of two Pauli operators, such as a 2D cluster state with $n > 4$.

Using the identity

$$|G\rangle\langle G| = \prod_{i=1}^n \frac{g_i + I_i}{2} = \frac{1}{2^n}\sum_\ell S_\ell, \tag{10}$$

the fidelity can also be written as

$$F = \text{Tr}(\rho|G\rangle\langle G|) = \frac{1}{2^n}\sum_\ell \text{Tr}(\rho S_\ell). \tag{11}$$

Equation (11) indicates that the fidelity can be estimated exactly from the average of all the stabilizers $\{S_\ell\}_{\ell \in \{0,1\}^n}$, that is, 2^n kinds of measurement settings are required. Note that only a polynomial number of them are chosen uniformly at random and performed in actual experiments. However, since chosen measurements vary in each experiment, the estimation of the fidelity requires the ability of performing any measurement in the 2^n stabilizer measurements.

III. FIDELITY ESTIMATION BY MEASURING A SINGLE STABILIZER

In this section, we discuss the idea employed in constructing our simplest fidelity-estimation protocol for graph states in the depolarizing channel. The average of the stabilizer is given as

$$\text{Tr}(\rho S_\ell) = (1-p)^n + \sum_{m=1}^n (1-p)^{n-m}\left(\frac{p}{3}\right)^m$$
$$\times \left[\sum_{\substack{i_1 < \ldots < i_m \\ \mu_1 \ldots \mu_m}} \langle G|\left(\prod_{k=1}^m \sigma_{\mu_k i_k}\right)S_\ell\left(\prod_{k=1}^m \sigma_{\mu_k i_k}\right)|G\rangle\right]. \tag{12}$$

Since the first-order error term vanishes in Eq. (7), the fidelity can be well approximated by the average of a stabilizer without the first-order error term when $p \ll 1$. By comparing Eqs. (7) and (12), for $p \ll 1$, we expect that the fidelity can be accurately estimated by measuring a single stabilizer for which the first-order error term vanishes.

Let us investigate the condition under which the first-order error term in Eq. (12) vanishes. Recall that τ_i is a single-qubit operator for the ith qubit of S_ℓ. τ_i commutes with each of X, Y, and Z in the case of $\tau_i = I$, while it commutes with only one of them and anticommutes with the others in the case of $\tau_i \in \{X, Y, Z\}$. We thus obtain

$$\sum_{\mu=1}^3 \langle G|\sigma_{\mu i}S_\ell\sigma_{\mu i}|G\rangle = \begin{cases} 3 & (\tau_i = I) \\ -1 & (\tau_i \in \{X, Y, Z\}). \end{cases} \tag{13}$$

Using this relation, we obtain

$$\sum_{i=1}^n \sum_{\mu=1}^3 \langle G|\sigma_{\mu i}S_\ell\sigma_{\mu i}|G\rangle = 3n_I - (n - n_I)$$
$$= 4n_I - n, \tag{14}$$

where n_I denotes the number of I in S_ℓ. Hence, the condition for the first-order error term to vanish is

$$n_I = \frac{n}{4}. \tag{15}$$

Generalizing the calculation of the first-order error term, the average of a stabilizer can be calculated, in general, as

$$\text{Tr}(\rho S_\ell) = \sum_{m=0}^n C(m)(1-p)^{n-m}\left(\frac{p}{3}\right)^m, \tag{16}$$

where $C(0) \equiv 1$. $C(m)$ $(m \geqslant 1)$ is given as

$$C(m) \equiv \sum_{\substack{i_1 < \ldots < i_m \\ \mu_1 \ldots \mu_m}} \langle G | \left(\prod_{k=1}^{m} \sigma_{\mu_k i_k} \right) S_\ell \left(\prod_{k=1}^{m} \sigma_{\mu_k i_k} \right) | G \rangle$$

$$= \sum_{j=w(\ell,m,n)}^{f(\ell,m)} (-1)^{m-j} 3^j \binom{n_I}{j} \binom{n-n_I}{m-j}, \qquad (17)$$

where $f(\ell, m) \equiv \min\{m, n_I\}$ and $w(\ell, m, n) \equiv \max\{0, m + n_I - n\}$. We have assumed $\binom{0}{0} = 1$.

$C(m)$ $(m \geqslant 1)$ corresponds to the sum of the averages of S_ℓ in the case of m errors. The term $\binom{n_I}{j} \binom{n-n_I}{m-j}$ expresses the number of cases in which j errors occur among the n_I qubits for which $\tau_i = I$, while the other $(m - j)$ errors occur on $(n - n_I)$ qubits for which $\tau_i \in \{X, Y, Z\}$.

From Eq. (17), the coefficient $C(2)$ is given as

$$C(2) = 8n_I^2 - 4(n+1)n_I + \frac{n(n-1)}{2}. \qquad (18)$$

By comparing the second-order error terms $(m = 2)$ in Eqs. (7) and (16), it should be preferable to set $C(2)$ as a non-negative number for the verification with high accuracy. Particularly in the case of cluster states, $C(2) = 0$ is desirable. However, in the case that the first-order error term vanishes, substituting $n_I = n/4$ in Eq. (18), we find that the second-order error term is negative as $C(2) = -3n/2$.

From Eq. (17), one finds that $C(m)$ is equivalent to the coefficient of the term $x^{n-m} y^m$ in the expansion of the polynomial $(x + 3y)^{n_I}(x - y)^{n-n_I}$. Then, substituting $x = 1 - p$ and $y = p/3$ in $(x + 3y)^{n_I}(x - y)^{n-n_I}$, we finally obtain a simple analytical expression for the average of the stabilizer as follows:

$$\text{Tr}(\rho S_\ell) = \left[(1-p) + 3\frac{p}{3} \right]^{n_I} \left[(1-p) - \frac{p}{3} \right]^{n-n_I} \qquad (19)$$

$$= \left(1 - \frac{4}{3}p \right)^{n-n_I}. \qquad (20)$$

It is clear from Eq. (20) that for fixed n and p, $\text{Tr}(\rho S_\ell)$ is determined solely by the number of I in S_ℓ. The average of the stabilizer decreases from unity as p increases in Eq. (20) because the eigenstates of S_ℓ with eigenvalue -1 are mixed to the pure graph state $|G\rangle\langle G|$ by the depolarizing noise. $\text{Tr}(\rho S_\ell)$ becomes negative when $p > 3/4$ in the case of odd $n - n_I$.

Equation (20) can be derived using an alternative approach, recognizing the tensor structure of both the stabilizer operator and the depolarizing noise. Using this approach, the average of a stabilizer under the general noise model

$$\mathcal{E}(\cdot) = (1 - p_x - p_y - p_z)(\cdot)$$
$$+ [p_x X(\cdot)X + p_y Y(\cdot)Y + p_z Z(\cdot)Z] \qquad (21)$$

can be derived as

$$\text{Tr}(\rho S_\ell) = (1 - 2p_y - 2p_z)^{n_X} (1 - 2p_z - 2p_x)^{n_Y}$$
$$\times (1 - 2p_x - 2p_y)^{n_Z}. \qquad (22)$$

Here, n_X, n_Y, and n_Z are the numbers of X, Y, and Z in the stabilizer S_ℓ, respectively. Equation (22) reduces to Eq. (20) when $p_x = p_y = p_z = p/3$. We provide a detailed description of the derivation of Eq. (22) in Appendix B.

Equations (11) and (20) lead to a simple expression for the fidelity

$$F = \frac{1}{2^n} \sum_{\ell \in \{0,1\}^n} \left(1 - \frac{4}{3}p \right)^{n-n_I(\ell)}, \qquad (23)$$

where $n_I(\ell)$ denotes the number of I in the stabilizer S_ℓ.

We have shown that $C(1) = 0$ when $n_I = n/4$ in Eq. (14). In fact, setting $n_I = n/4$ in Eqs. (19) and (20), we obtain

$$\text{Tr}(\rho S_\ell) = \left(1 - \frac{4}{3}p \right)^{3n/4}$$
$$= \left[(1-p)^4 - \frac{2}{3}p^2(1-p)^2 \right.$$
$$\left. + \frac{8}{27}p^3(1-p) - \frac{1}{27}p^4 \right]^{n/4}. \qquad (24)$$

Expanding the final expression and comparing with Eq. (7), it is clear that there is no first-order error term $(m = 1)$ in Eq. (24).

From this observation, we expect that the fidelity can be well estimated by measuring a single stabilizer that satisfies the condition Eq. (15). In fact, the following theorem holds.

Theorem 1. Let $|G\rangle$ be an n-qubit ideal graph state with $n = 4k$ for some natural number k. Let $\mathcal{A}$ be the set of stabilizers S of $|G\rangle$ such that $S = (-1)^s \otimes_{i=1}^{n} \tau_i$, where $\tau_i \in \{X, Y, Z\}$ for $3k$ kinds of i's, $\tau_i = I$ for other i's, and $s \in \{0, 1\}$. Let $F \equiv \langle G|\rho|G\rangle$ be the fidelity between $|G\rangle$ and an n-qubit graph state ρ [Eq. (5)] in the depolarizing channel with the error probability p. The fidelity $\tilde{F} = (1 - p)^{4k}$ up to the first-order error can be approximated by the expectation value $F_{\text{est}} \equiv \text{Tr}(\rho S) = (1 - 4p/3)^{3k}$ of any single stabilizer S in the set $\mathcal{A}$, such that

$$0 \leqslant \tilde{F} - F_{\text{est}} < \frac{2}{3k} \qquad (25)$$

for $0 \leqslant p \leqslant 3/4$.

Figures 1(a) and 1(b) illustrate examples of the stabilizers S_ℓ in the set $\mathcal{A}$ for 2D cluster states. They satisfy the condition $\text{wt}(\ell) \equiv \sum_{i=1}^{n} \ell_i = 3k$ and $\tau_i = I$ for arbitrary qubit i for which $\ell_i = 0$, namely, S_ℓ consists of $3k$ generators, and arbitrary qubit unoccupied by a generator is connected to occupied qubits with an even number of edges. Another example of such stabilizers is given in Sec. IV for fully connected graph states.

Our main contribution is to derive Eq. (20), from which Theorem 1 can be immediately obtained. A rigorous proof of Theorem 1 is given in Appendix C. Note that Theorem 1 holds for any graph state with $n = 4k$ under the condition that the graph state has no isolated single qubits, and the set $\mathcal{A}$ is not empty. Theorem 1 implies that as the number n of qubits increases, the precision of the estimation of $\tilde{F}$ by F_{est} improves. When the second-order error term in Eq. (7) vanishes, the fidelity up to the second-order error is also $\tilde{F}$. Consequently, the estimation of F by F_{est} improves further. This is the case for 2D cluster states, as we demonstrate it in the next section.

Based on Theorem 1, our verification protocol runs as follows:

(1) A quantum computer generates N graph states $\rho^{\otimes N}$ in the depolarizing channel and sends them to a verifier.

(2) The verifier measures S_ℓ that satisfies the condition in Eq. (15) on each received state ρ.
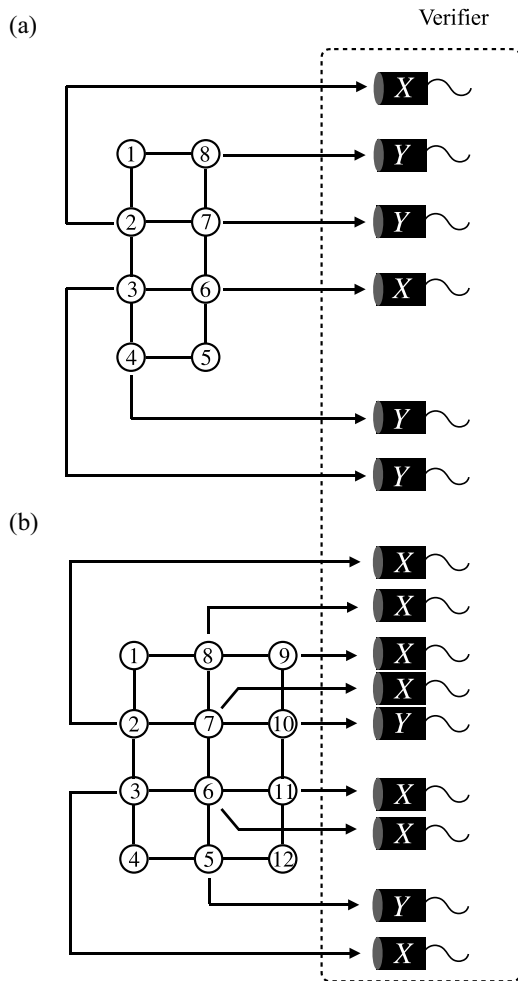
FIG. 1. Schematic diagram of our simplest verification protocol. A quantum computer generates graph states ρ in the depolarizing channel and sends each qubit one by one. A verifier just measures a single stabilizer S_ℓ, which has $3n/4$ Pauli operators, for each received state ρ by using only single-qubit Pauli measurements. No quantum memory is required for the verifier.

(3) The verifier outputs

$$\tilde{F}_{est} \equiv \frac{\sum_{i=1}^{N} o_i}{N} \qquad (26)$$

as an estimated value of the fidelity, where $o_i \in \{+1, -1\}$ denotes the ith outcome for $1 \leqslant i \leqslant N$.

$\tilde{F}_{est}$ converges to F_{est} in the limit of large N. In fact, the Hoeffding inequality [45] guarantees that when $N = \lceil 2/\epsilon^2 \ln (2/\delta) \rceil$, the inequality

$$|F_{est} - \tilde{F}_{est}| \leqslant \epsilon \qquad (27)$$

holds with probability at least $1 - \delta$. Here, $\lceil \cdot \rceil$ is the ceiling function.

The measurement of S_ℓ in step 2 can be realized by single-qubit Pauli measurements because S_ℓ is a tensor product of Pauli operators. Furthermore, by sequentially sending qubits one by one in step 1, no quantum memory is required for the verifier. To illustrate our protocol, we give concrete examples in Fig. 1.
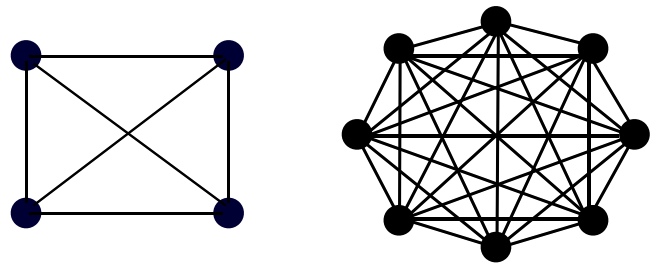

FIG. 2. Fully connected graphs with four (left) and eight vertices (right). The black dots and the solid lines are vertices and edges, respectively.

While the constraint in our protocol on the number of qubits, which must be a multiple of 4, may seem restrictive, we point out that it does not limit its practical applications. The central goal of our protocol is to verify high fidelity for graph states. Once high fidelity has been established for a graph state using our protocol, the number of qubits of the graph state can be changed by measurements in the Z basis because measuring a qubit in the Z basis results in breaking the edges and disconnecting the qubit from the graph.

IV. APPLICATIONS

In this section, we first discuss the estimation of the fidelity for fully connected graph states and cluster states. Particularly, cluster states are important resource states for MBQC, which allow universal quantum computation. Theorem 1 just guarantees that our simplest verification protocol outputs the estimated value that is close to the true value F of the fidelity only when p is sufficiently small. We numerically show that F_{est} becomes precise approximations for any $0 \leqslant p \leqslant 1/2$ in the case of fully connected graph and cluster states. Then, we evaluate our protocol for noise models other than the depolarizing noise.

A. Fully connected graph states

We consider fully connected graphs, in which each of the vertices is connected with all the other vertices by the edges, as shown in Fig. 2. Before applying Theorem 1 to fully connected graph states with $n = 4k$ ($k \in \mathbb{N}$) qubits, we first evaluate the fidelity of fully connected graph states. According to Eq. (23), since $n_I(\ell)$ for all ℓ's are required to evaluate the fidelity, it should not be easy to derive it in general. For fully connected graph states, however, Eq. (23) can be easily evaluated.

In the case of even $\mathrm{wt}(\ell) = \sum_{i=1}^{n} \ell_i$, i.e., S_ℓ is a product of even g_i's, we obtain $n_I(\ell) = n - \mathrm{wt}(\ell)$, because $\tau_i = I$ for $\ell_i = 0$, and $\tau_i = X$ or Y for $\ell_i = 1$. Meanwhile, $n_I = 0$ in the case of odd $\mathrm{wt}(\ell)$, because $\tau_i = Z$ for $\ell_i = 0$, and $\tau_i = X$ or Y for $\ell_i = 1$. We thus obtain

$$2^n F = \sum_{\mathrm{wt:\ even}} \binom{n}{\mathrm{wt}} \left(1 - \frac{4}{3}p\right)^{\mathrm{wt}} + \sum_{\mathrm{wt:\ odd}} \binom{n}{\mathrm{wt}} \left(1 - \frac{4}{3}p\right)^{n}$$

$$= 2^{n-1} \left[\left(1 - \frac{2}{3}p\right)^n + \left(\frac{2}{3}p\right)^n + \left(1 - \frac{4}{3}p\right)^n \right]. \qquad (28)$$
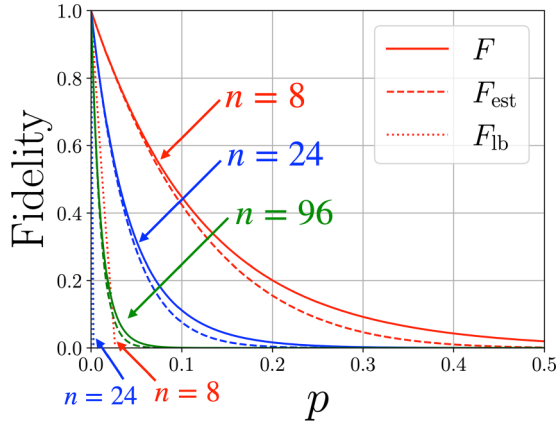
FIG. 3. Comparison of F (solid lines) and F_{est} (dashed lines) as functions of the error probability p for the fully connected graph states with $n = 8$, 24, and 96 qubits. The dotted lines represent F_{lb} in Eq. (42) for $n = 8$ and 24 qubits.

Here, we have used the following relations:

$$\sum_{j:\text{ even}} \binom{n}{j} x^j = \frac{1}{2}[(1+x)^n + (1-x)^n], \qquad (29)$$

$$\sum_{j:\text{ odd}} \binom{n}{j} = 2^{n-1}. \qquad (30)$$

Now we discuss the estimation of the fidelity for fully connected graph states with $n = 4k$ qubits. In the case of even k, any stabilizer S_ℓ with $\text{wt} = 3k$ satisfies the condition $n_I = n/4 = k$, because $\tau_i = I$ for $\ell_i = 0$, and $\tau_i = X$ or Y for $\ell_i = 1$. Meanwhile, in the case of odd k, any fully connected graph state with $n = 4k$ qubits has no stabilizers that satisfy the condition $n_I = n/4 = k$ because any stabilizer S_ℓ with $\text{wt} = 3k$ has $\tau_i = Z$ for $\ell_i = 0$, and $\tau_i = X$ or Y for $\ell_i = 1$. Theorem 1 can be thus applied to any fully connected graph state with $n = 8k$ ($k \in \mathbb{N}$) qubits.

Figure 3 shows the comparison of F in Eq. (28) and $F_{\text{est}} = (1 - 4p/3)^{6k}$ for the fully connected graph states with $n = 8k$ qubits. It demonstrates that the estimation of the fidelity F by F_{est} improves as n increases. The upper bound on $F - F_{\text{est}}$ for $0 \leqslant p \leqslant 3/4$ can be derived as

$$0 \leqslant F - F_{\text{est}}$$
$$< \frac{1}{2}\left(1 - \frac{1}{8k}\right)\left(1 - \frac{1}{4k}\right)^{8k-2} + \frac{1}{2}\left(\frac{2}{3}\right)^{8k} + \frac{1}{3k}. \quad (31)$$

The derivation is given in Appendix D. The upper bound in Eq. (31) monotonically decreases as k increases and converges to $1/(2e^2)$ in the limit of $k \to \infty$.

The second-order error term $F^{(2)}$ in Eq. (7) is nonzero for fully connected graph states. Since any stabilizer with $\text{wt} = 2$ consists of two Pauli operators, it can be written as

$$F^{(2)} = \binom{n}{2}(1-p)^{n-2}\left(\frac{p}{3}\right)^2. \qquad (32)$$

The relatively large deviation of F_{est} from F in Fig. 3 reflects the presence of $F^{(2)}$.

In the case of fully connected graph states, the other error terms can also be derived. First, from Eq. (7), we obtain

$$F = \sum_{\ell \in \{0,1\}^n} (1-p)^{n_I(\ell)} \left(\frac{p}{3}\right)^{n-n_I(\ell)}. \qquad (33)$$

Then, by following the similar argument as used to derive Eq. (32) and using Eq. (30), we calculate Eq. (33) as follows:

$$F = (1-p)^n + \sum_{k=1}^{\lfloor n/2 \rfloor} \binom{n}{2k}(1-p)^{n-2k}\left(\frac{p}{3}\right)^{2k}$$
$$+ 2^{n-1}\left(\frac{p}{3}\right)^n, \qquad (34)$$

where $\lfloor \cdot \rfloor$ is the floor function. Taking the summation over k as in Eq. (16), we can derive the analytical expression of the fidelity in Eq. (28) from Eq. (34).

B. Two-dimensional cluster states

We discuss the estimation of the fidelity of 2D cluster states, which are universal resource states for MBQC. Here, we focus on the rectangular cluster states with $n = q \times r$ ($q, r \in \mathbb{N}$, $q \neq r$) qubits because they suffice for universal quantum computation in MBQC.

In contrast to fully connected graph states, it should be difficult to derive a general expression for the fidelity of 2D cluster states. Meanwhile, the fidelity up to the third-order error term can be easily obtained. In the case of $q, r > 2$, the cluster states have no second-order error terms because they have no stabilizers that consist of two Pauli operators. As for the third-order error terms, the four generators on the corners of the corresponding rectangular are the only stabilizers that consist of three Pauli operators. Thus, the fidelity up to the third-order error can be written as

$$F' = (1-p)^n + 4(1-p)^{n-3}\left(\frac{p}{3}\right)^3. \qquad (35)$$

The fidelity of the cluster state with 2×4 qubits up to the third-order error is given as

$$F' = (1-p)^8 + 8(1-p)^5\left(\frac{p}{3}\right)^3. \qquad (36)$$

Since F has no second-order error terms in both cases, it is expected that F can be well estimated by F_{est}. Figure 4 shows the comparison of the fidelity F and F_{est} for the cluster states with 2×4 and 3×4 qubits. The stabilizers that satisfy the condition $n_I = n/4$ are shown in Figs. 1(a) and 1(b). Here, F is evaluated numerically by taking the average of all the stabilizers. It also demonstrates that the estimation of F by F_{est} improves as n increases. Compared with Fig. 3, the deviation of F_{est} from F is smaller than that for the fully connected graph states.

C. Fidelity estimation for cluster states in the presence of either phase-flip or depolarizing noise

So far, we have restricted the noise model and fixed $\mathcal{E}$ to the depolarizing channel. This restriction can be justified in the case where we can specify the noise model based on knowledge of how the cluster state provided to a verifier is generated in an experiment. In this subsection, we relax
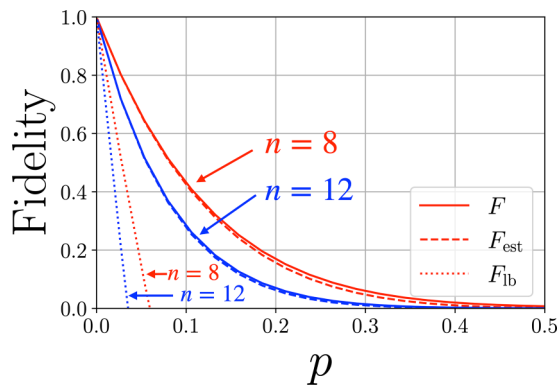
FIG. 4. Comparison of F (solid lines) and F_{est} (dashed lines) as functions of the error probability p for the rectangular cluster states of 2×4 and 3×4 qubits. The dotted lines represent F_{lb} in Eq. (44).

this restriction and consider the possibility of estimating the fidelity of a 2D cluster state by measuring a single stabilizer in the presence of either phase-flip or depolarizing noise. It may be useful in the case where the phase-flip or depolarizing noise is randomly applied. It may also be useful in cases where the noise model cannot be determined between the phase-flip and depolarizing noises due to a lack of knowledge about the experimental setups.

We first consider the cluster state of 2×4 qubits. In the presence of the phase-flip error, the fidelity of an n-qubit graph state can be estimated by measuring a single stabilizer S_ℓ that satisfies $\text{wt}(\ell) = n/2$ [33]. Then, the stabilizer

$$S_\ell = g_1 g_3 g_5 g_7 = X_1 Z_2 X_3 I_4 X_5 Z_6 X_7 I_8 \tag{37}$$

satisfies both the conditions $\text{wt}(\ell) = n/2$ and $n_I = n/4$, where the indices of qubits in Eq. (37) correspond to those in Fig. 1(a). Thus, the fidelity can be estimated by measuring it in the presence of either phase-flip or depolarizing noise.

Extending the above argument, the fidelity of a large cluster state with $n = 4q \times 2r$ qubits can be estimated by measuring a single stabilizer. For example, choosing generators every 4×2 qubits analogously to Eq. (37) as shown in Fig. 5, the stabilizer obtained as their product satisfies both the conditions $\text{wt}(\ell) = n/2$ and $n_I = n/4$.
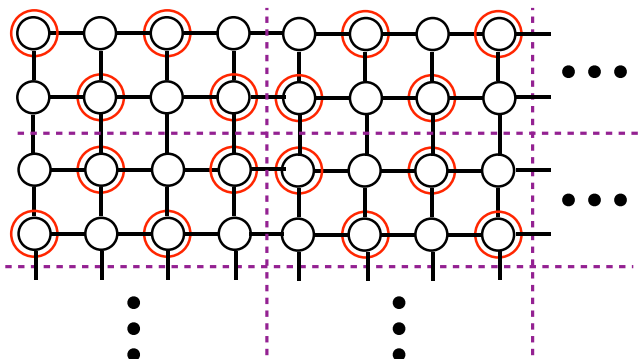

FIG. 5. Cluster state of $n = 4q \times 2r$ qubits. The fidelity of it in the presence of either the phase-flip or the depolarizing noise can be estimated by a stabilizer that is a product of the generators indicated by the red circles.
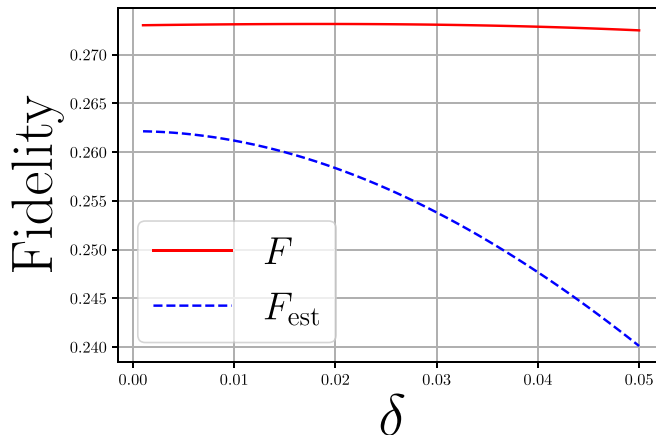

FIG. 6. Comparison of F and F_{est} for the (2×4)-qubit cluster state in the presence of the noise model in Eq. (21) as functions of the parameter δ. We set $p = 0.15$.

Furthermore, the fidelity of the same cluster state can be estimated by measuring the same stabilizer even in the presence of a more general noise model Eq. (21) with $p_x = p_y = p/3 - \delta$ and $p_z = p/3 + 2\delta$. This noise model interpolates the phase-flip and depolarizing noises; it reduces to the depolarizing (phase-flip) noise when $\delta = 0$ ($\delta = p/3$).

From Eq. (22), the average of a stabilizer under this noise model can be obtained as

$$\text{Tr}(\rho S_\ell) = \left(1 - \tfrac{4}{3}p - 2\delta\right)^{\text{wt}(\ell)} \left(1 - \tfrac{4}{3}p + 4\delta\right)^{n_Z}, \tag{38}$$

where $n_X + n_Y = \text{wt}(\ell)$ and $n_Z = n - n_I - \text{wt}(\ell)$. Thus, setting $\text{wt}(\ell) = n/2$ and $n_I = n/4$ in Eq. (38), F_{est} for the stabilizer Eq. (37) is

$$F_{\text{est}}(\delta) = \left(1 - \tfrac{4}{3}p - 2\delta\right)^{n/2} \left(1 - \tfrac{4}{3}p + 4\delta\right)^{n/4}. \tag{39}$$

The above expression interpolates $F_{\text{est}} = (1 - 4p/3)^{3n/4}$ for the depolarizing noise ($\delta = 0$) and $F_{\text{est}} = (1 - 2p)^{n/2}$ for the phase-flip noise ($\delta = p/3$) [33].

Figure 6 shows a comparison of the fidelity $F(\delta)$ and $F_{\text{est}}(\delta)$ for the (2×4)-qubit cluster state in the presence of the noise Eq. (21) with $p_x = p_y = p/3 - \delta$ and $p_z = p/3 + 2\delta$. From $\partial F_{\text{est}}/\partial \delta \leqslant 0$ in the case of $0 \leqslant 2\delta \leqslant 1 - 4p/3$, $F_{\text{est}}(\delta)$ monotonically decreases, as shown in Fig. 6. When $0 \leqslant p \leqslant 1/2$, therefore, $F_{\text{est}}(\delta)$ is a lower bound on $F(\delta)$ for any δ as

$$F_{\text{est}}(0 \leqslant \delta \leqslant p/3) \leqslant F_{\text{est}}(\delta = 0) = \left(1 - \tfrac{4}{3}p\right)^{3n/4}$$
$$\leqslant \tilde{F} = (1 - p)^n < F(\delta), \tag{40}$$

where we use Theorem 1 in the second inequality. Consequently, a lower bound on the fidelity of a large cluster state with $n = 4q \times 2r$ qubits can also be estimated by measuring the stabilizer specified in Fig. 5 when $0 \leqslant p \leqslant 1/2$.

V. COMPARISON WITH PREVIOUS PROTOCOLS

Several verification protocols exist for graph states that work for any type of error [19–21,24–28]. The lower bound of the fidelity obtained in some of them becomes loose in general. It has been shown that the necessary number of measurement settings can be improved to n from 2^n by using

the union bound [24], where the obtained lower bound of the fidelity is given as

$$F_{\rm lb} = 1 - \sum_{i=1}^{n} \left\{ 1 - \mathrm{Tr}\left[\rho\left(\frac{I^{\otimes n} + g_i}{2} \right) \right] \right\} \qquad (41)$$

in the limit of large N.

For any n-qubit fully connected graph state, using $\mathrm{Tr}(\rho g_i) = (1 - 4p/3)^n$, the lower bound $F_{\rm lb}$ is calculated as

$$F_{\rm lb} = 1 - \frac{n}{2} + \frac{n}{2}\left(1 - \frac{4}{3}p \right)^n \qquad (42)$$

$$\simeq 1 - \frac{2}{3}n^2 p \quad (p \ll 1). \qquad (43)$$

For any $n = q \times r$ $(q, r \geqslant 2)$-qubit cluster state, the lower bound $F_{\rm lb}$ is calculated as

$$F_{\rm lb} = 1 - \frac{n}{2} + \frac{1}{2}\left[2(q + r - 4)\left(1 - \frac{4}{3}p \right)^4 + 4\left(1 - \frac{4}{3}p \right)^3 \right.$$

$$\left. + (q - 2)(r - 2)\left(1 - \frac{4}{3}p \right)^5 \right] \qquad (44)$$

$$\simeq 1 - \frac{2}{3}[5n - 2(q + r)]p \quad (p \ll 1). \qquad (45)$$

$F_{\rm lb}$ becomes loose as n increases in both types of graph states, which is in sharp contrast with the fact that $F_{\rm est}$ becomes tight as n increases. Figures 3 and 4 show that our estimated value $F_{\rm est}$ is close to the true value $F = \langle G|\rho|G \rangle$ even when the number n of qubits and p are large. Meanwhile, the deviation of $F_{\rm lb}$ from F increases as p increases as shown in Figs. 3 and 4.

VI. CONCLUSION AND DISCUSSION

We proposed a verification protocol for graph states assuming the depolarizing channel. A remarkable feature of our verification protocol is that the fidelity of an n-qubit graph state can be estimated by just measuring a single stabilizer S_ℓ that satisfies the condition $n_I = n/4$, where n_I denotes the number of identity operators in S_ℓ. Consequently, it requires only one measurement setting. Furthermore, we showed that the estimation improves as the number n of qubits increases. We also derived a simple analytic expression for the average of a stabilizer in the depolarizing channel. We applied our protocol to fully connected graph states and cluster states, demonstrating its usefulness. Furthermore, we evaluated our protocol for other noise models other than the depolarizing noise and compared it with the previous protocols. Our protocol should be useful even when it is unknown whether the actual physical noise model is the phase-flip or depolarizing noise.

We note the scope of applications of our protocol in the presence of the depolarizing noise. Our protocol, which estimates the fidelity of the graph state under the depolarizing noise, is specifically useful in the situation where we have almost no information about the actual physical noise channel for the following reason. For a single-qubit state, the depolarizing noise introduces a probabilistic mixture of the ideal state and the maximally mixed state with probability $4p/3$

[see Eq. (4)]. From Ref. [46], this noise model is valuable when knowledge about the underlying noise channel is quite limited. In essence, the depolarizing noise is used as a representative model due to the lack of detailed information about the specific noise model.

Introducing the step of estimating the parameter p could indeed be an approach. In the approach, to obtain an estimated value of the fidelity, Eq. (7) has to be calculated with the estimated value of p, which increases the required time for the estimation. On the other hand, our protocol can directly estimate the fidelity without calculating Eq. (7). More concretely, when state preparations and/or measurements are the most time consuming, it should be important to evaluate the required number of samples (i.e., the sample complexity) to determine the required time. The purpose of the verification is to obtain $\tilde{F}_{\rm est}$ such that $|F - \tilde{F}_{\rm est}| \leqslant \tilde{\epsilon}$ with probability at least $1 - \delta$. Under the condition that the target state is the 160-qubit fully connected graph state, the error probability p is 0.002, the desired accuracy is $\tilde{\epsilon} = 0.1$, and the desired confidence level is $1 - \delta = 0.99$, the sample complexity of our method is $N = 45\,630$ from Eqs. (27) and (31). On the other hand, an approach based on the estimation of p first prepares $|+\rangle$ in the depolarizing channel and then measures it in the X basis. Since the target state is the fully connected graph state, the fidelity Eq. (7) becomes Eq. (28). Therefore, p has to be estimated with the accuracy at least $\epsilon' = 0.000824205$ to achieve $\tilde{\epsilon} = 0.1$. Note that we obtain $\epsilon' = 0.000824205$ by numerically solving $F(160, 0.002) + 0.1 = F(160, 0.002 - \epsilon')$, where $F(n, p) \equiv [(1 - 2p/3)^n + (2p/3)^n + (1 - 4p/3)^n]/2$. From the Hoeffding inequality [45] and the fact that the probability of obtaining the measurement outcome $+1$ is $1 - 2p/3$, the sample complexity is $8\,774\,450$. Since our method uses 160 qubits in a single repetition, we assume that the approach based on the estimation of p uses $|+\rangle^{\otimes 160}$ rather than $|+\rangle$ in each repetition. As a result, we can reduce the sample complexity to $8\,774\,450/160 \simeq 54\,840$, but it is still larger than our sample complexity $45\,630$. In contrast, with respect to the experimental overhead, the approach based on the estimation of p outperforms our method in the sense that the approach based on the estimation of p does not require entangled states to estimate the fidelity. We leave the more thorough comparison as a future work.

As a future work, it would also be interesting to extend our results to correlated noises such as the global depolarizing noise

$$\mathcal{E}(\rho) = (1 - p)\rho + p\frac{I^{\otimes n}}{2^n}, \qquad (46)$$

where ρ is any n-qubit state and p is the error probability. Since this error model is observed in actual experiments such as the quantum supremacy experiment in Ref. [32], by doing so, we can make our results more practical.

APPENDIX A: PROOF OF LEMMA 1

Proof. Using Eq. (1), the expectation value $\langle G|(\prod_{k=1}^{m} \sigma_{\mu_k i_k})|G\rangle$ can be written as

$$\langle G|\left(\prod_{k=1}^{m} \sigma_{\mu_k i_k}\right)|G\rangle = \langle +|^{\otimes n} U_{CZ}^{\dagger}\left(\prod_{k=1}^{m} \sigma_{\mu_k i_k}\right) U_{CZ}|+\rangle^{\otimes n}, \tag{A1}$$

where $U_{CZ} \equiv \prod_{e \in E} CZ_e$. Given that CZ is a Clifford operator, $U_{CZ}^{\dagger}(\prod_{k=1}^{m} \sigma_{\mu_k i_k})U_{CZ}$ is also a tensor product of Pauli operators with a sign $+$ or $-$. A tensor product of Pauli operators averaged by $|+\rangle^{\otimes n}$ yields $+1$ if it is a tensor product of X and/or I and zero otherwise. Thus, we obtain $\langle G|(\prod_{k=1}^{m} \sigma_{\mu_k i_k})|G\rangle^2 = 0$ or 1. For $\langle G|(\prod_{k=1}^{m} \sigma_{\mu_k i_k})|G\rangle$ being nonzero, there must exist $s \in \{+1, -1\}$ and the set $A \subseteq \{1, 2, \ldots, n\}$ such that

$$U_{CZ}^{\dagger}\left(\prod_{k=1}^{m} \sigma_{\mu_k i_k}\right) U_{CZ} = s\left(\prod_{i \in A} X_i \prod_{j \in \bar{A}} I_j\right), \tag{A2}$$

$$s\left(\prod_{k=1}^{m} \sigma_{\mu_k i_k}\right) = U_{CZ}\left(\prod_{i \in A} X_i \prod_{j \in \bar{A}} I_j\right) U_{CZ}^{\dagger}, \tag{A3}$$

where $\bar{A}$ is the complement of A. When $\langle G|(\prod_{k=1}^{m} \sigma_{\mu_k i_k})|G\rangle$ is nonzero, thus, $\prod_{k=1}^{m} \sigma_{\mu_k i_k}$ or $-\prod_{k=1}^{m} \sigma_{\mu_k i_k}$ coincides with one of the stabilizers of $|G\rangle$.

APPENDIX B: DERIVATION OF EQ. (22)

In this Appendix, we derive Eq. (22) and provide an alternative derivation of Eq. (20). For convenience, we express the general noise model Eq. (21) as

$$\mathcal{E}(\cdot) = \sum_{\mu=0,1,2,3} p_\mu \sigma_\mu(\cdot)\sigma_\mu, \tag{B1}$$

where $p_1 = p_x$, $p_2 = p_y$, $p_3 = p_z$, and $p_0 = 1 - p_x - p_y - p_z$, $\sigma_0 = I$, $\sigma_1 = X$, $\sigma_2 = Y$, and $\sigma_3 = Z$.

Using the cyclic property of trace and the anticommuting property of the Pauli matrices, we can derive the following relation:

$$\text{Tr}[\sigma_\nu \mathcal{E}(\cdot)] = \sum_{\mu=0,1,2,3} p_\mu \text{Tr}[\sigma_\mu \sigma_\nu \sigma_\mu(\cdot)]$$
$$= f_\nu \text{Tr}[\sigma_\nu(\cdot)], \quad (\nu = 0, 1, 2, 3). \tag{B2}$$

Here, f_ν is given as

$$f_\nu = p_0 + \sum_{\mu=1,2,3} p_\mu(-1)^{1+\delta_{\mu,\nu}} \tag{B3}$$

in the case of $\nu = 1, 2, 3$, and $f_0 = 1$. Using the above relation, we obtain

$$\text{Tr}\left[\left(\bigotimes_{i=1}^{n} \tau_i\right) \mathcal{E}^{\otimes n}(\cdot)\right] = \text{Tr}_1 \cdots \text{Tr}_n\left[\left(\bigotimes_{i=1}^{n} \tau_i\right) \mathcal{E}^{\otimes n}(\cdot)\right]$$

$$= f_1^{n_X} f_2^{n_Y} f_3^{n_Z} \text{Tr}\left[\left(\bigotimes_{i=1}^{n} \tau_i\right)(\cdot)\right]. \tag{B4}$$

Thus, Eq. (22) can be obtained as

$$\text{Tr}(S_\ell \rho) = \text{Tr}\left[\left((-1)^s \bigotimes_{i=1}^{n} \tau_i\right) \mathcal{E}^{\otimes n}(|G\rangle\langle G|)\right]$$

$$= f_1^{n_X} f_2^{n_Y} f_3^{n_Z} \text{Tr}\left[\left((-1)^s \bigotimes_{i=1}^{n} \tau_i\right)(|G\rangle\langle G|)\right]$$

$$= f_1^{n_X} f_2^{n_Y} f_3^{n_Z} \langle G|S_\ell|G\rangle$$

$$= f_1^{n_X} f_2^{n_Y} f_3^{n_Z}, \tag{B5}$$

where $f_1 = 1 - 2p_y - 2p_z$, $f_2 = 1 - 2p_z - 2p_x$, and $f_3 = 1 - 2p_x - 2p_y$. For the depolarizing noise, setting $p_x = p_y = p_z = p/3$, we obtain

$$\text{Tr}(S_\ell \rho) = \left(1 - \tfrac{4}{3}p\right)^{n-n_I}, \tag{B6}$$

where we use $n_X + n_Y + n_Z = n - n_I$.

APPENDIX C: PROOF OF THEOREM 1

Proof. Let $X \equiv (1 - p)^4$ and $Y \equiv (1 - 4p/3)^3$, then $\tilde{F} = X^k$ and $F_{est} = Y^k$. Using $X \geqslant Y$ for $p \in [0, 1]$, and $X - Y = [(p - 22/27)^2 + 2/729]p^2$,

$$0 \leqslant \tilde{F} - F_{est} = X^k - Y^k$$

$$= (X - Y)(X^{k-1} + X^{k-2}Y + \cdots + XY^{k-2} + Y^{k-1})$$

$$\leqslant k(X - Y)X^{k-1}$$

$$\leqslant kp^2\left(-\frac{1}{2}p + \frac{2}{3}\right)(1 - p)^{4(k-1)} \tag{C1}$$

$$\leqslant kp_0^2\left(-\frac{1}{2}p_0 + \frac{2}{3}\right)(1 - p_0)^{4(k-1)} \leqslant \frac{2}{3}kp_0^2 < \frac{2}{3k}. \tag{C2}$$

Here, the right-hand side of Eq. (C1) takes its maximum value at p_0, which is given by

$$p_0 = \frac{16k + 1 - \sqrt{256k^2 - 352k + 97}}{6(4k - 1)}. \tag{C3}$$

The last inequality in Eq. (C2) can be obtained from the inequality $p_0 < 1/k$.

APPENDIX D: DERIVATION OF EQ. (31)

$F - F_{est}$ for the fully connected graph states with $n = 8k$ qubits can be written as

$$F - F_{est} = \frac{1}{2}\left\{\left[\left(1 - \tfrac{2}{3}p\right)^n - (1 - p)^n\right]\right.$$

$$\left. - \left[(1 - p)^n - \left(1 - \tfrac{4}{3}p\right)^n\right]\right\}$$

$$+ \frac{1}{2}\left(\tfrac{2}{3}p\right)^n + \left[(1 - p)^n - \left(1 - \tfrac{4}{3}p\right)^{6k}\right]. \tag{D1}$$

Note that $F - F_{\text{est}} \geqslant 0$ holds because $F \geqslant \tilde{F}$ from Eq. (7), and $\tilde{F} \geqslant F_{\text{est}}$ from Eq. (25). From the inequalities

$$\left(\tfrac{2}{3}p\right)^n \leqslant \left(\tfrac{2}{3}\right)^n, \tag{D2}$$

$$(1-p)^n - \left(1 - \frac{4}{3}p\right)^{6k} < \frac{1}{3k}, \tag{D3}$$

it is necessary to evaluate the upper bound of the terms inside the bracket $\{\cdot\}$ on the right-hand side of Eq. (D1). Note that Eq. (D3) holds due to Theorem 1. Let $s \equiv 1 - p$, $t \equiv 1 - (2/3)p$, and $u \equiv 1 - (4/3)p$. For $0 \leqslant p \leqslant 3/4$, it can be evaluated as

$$
\begin{aligned}
&(t^n - s^n) - (s^n - u^n) \\
&= (t-s)(t^{n-1} + t^{n-2}s + \cdots + s^{n-1}) \\
&\quad - (s-u)(s^{n-1} + s^{n-2}u + \cdots + u^{n-1}) \\
&\leqslant (t-s)nt^{n-1} - (s-u)ns^{n-1} = \frac{p}{3}n(t^{n-1} - s^{n-1})
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{p}{3}n(t-s)(t^{n-2} + t^{n-3}s + \cdots + ts^{n-3} + s^{n-2}) \\
&\leqslant \frac{n(n-1)}{9}p^2 t^{n-2} \\
&= \frac{n(n-1)}{9}p^2\left(1 - \frac{2}{3}p\right)^{n-2} \leqslant \left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right)^{n-2}.
\end{aligned}
\tag{D4}
$$

We use the relation $(t^{n-1} - t^{n-i}s^{i-1}) - (s^{n-1} - s^{n-i}u^{i-1}) \geqslant 0$ for integer $i \in [1, n]$, which can be easily proved by induction, for the first inequality. We also use the fact that $p^2(1 - (2/3)p)^{n-2}$ takes the maximum value at $p = 3/n$ for $0 \leqslant p \leqslant 3/4$ for the final inequality. Combining Eqs. (D2)–(D4), we obtain Eq. (31). The right-hand side of Eq. (D4) converges to $1/e^2$ due to the relation

$$\lim_{n \to \infty} \left(1 - \frac{2}{n}\right)^n = \frac{1}{e^2}. \tag{D5}$$

Therefore, the upper bound in Eq. (31) converges to $1/(2e^2)$.

---

[1] H. J. Briegel and R. Raussendorf, Persistent entanglement in arrays of interacting particles, Phys. Rev. Lett. **86**, 910 (2001).

[2] R. Raussendorf and H. J. Briegel, A one-way quantum computer, Phys. Rev. Lett. **86**, 5188 (2001).

[3] N. Shettell and D. Markham, Graph states as a resource for quantum metrology, Phys. Rev. Lett. **124**, 110502 (2020).

[4] K. Azuma, K. Tamaki, and H.-K. Lo, All-photonic quantum repeaters, Nat. Commun. **6**, 6787 (2015).

[5] S. Spilla, R. Migliore, M. Scala, and A. Napoli, GHZ state generation of three Josephson qubits in the presence of bosonic baths, J. Phys. B: At. Mol. Opt. Phys. **45**, 065501 (2012).

[6] K. L. Brown, C. Horsman, V. Kendon, and W. J. Munro, Layer-by-layer generation of cluster states, Phys. Rev. A **85**, 052305 (2012).

[7] C. Monroe, R. Raussendorf, A. Ruthven, K. R. Brown, P. Maunz, L.-M. Duan, and J. Kim, Large-scale modular quantum-computer architecture with atomic memory and photonic interconnects, Phys. Rev. A **89**, 022317 (2014).

[8] K. Inaba, Y. Tokunaga, K. Tamaki, K. Igeta, and M. Yamashita, High-fidelity cluster state generation for ultracold atoms in an optical lattice, Phys. Rev. Lett. **112**, 110501 (2014).

[9] M. Gimeno-Segovia, P. Shadbolt, D. E. Browne, and T. Rudolph, From three-photon Greenberger-Horne-Zeilinger states to ballistic universal quantum computation, Phys. Rev. Lett. **115**, 020502 (2015).

[10] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan, Experimental entanglement of six photons in graph states, Nat. Phys. **3**, 91 (2007).

[11] Y. Tokunaga, S. Kuwashiro, T. Yamamoto, M. Koashi, and N. Imoto, Generation of high-fidelity four-photon cluster state and quantum-domain demonstration of one-way quantum computing, Phys. Rev. Lett. **100**, 210501 (2008).

[12] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, Observation of eight-photon entanglement, Nat. Photonics **6**, 225 (2012).

[13] X.-C. Yao, T.-X. Wang, H.-Z. Chen, W.-B. Gao, A. G. Fowler, R. Raussendorf, Z.-B. Chen, N.-L. Liu, C.-Y. Lu, Y.-J. Deng, Y.-A. Chen, and J.-W. Pan, Experimental demonstration of topological error correction, Nature (London) **482**, 489 (2012).

[14] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, H. Lu, Y. Hu, X. Jiang, C.-Z. Peng, L. Li, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, and J.-W. Pan, Experimental ten-photon entanglement, Phys. Rev. Lett. **117**, 210502 (2016).

[15] X.-L. Wang, Y.-H. Luo, H.-L. Huang, M.-C. Chen, Z.-E. Su, C. Liu, C. Chen, W. Li, Y.-Q. Fang, X. Jiang, J. Zhang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, 18-qubit entanglement with six photons' three degrees of freedom, Phys. Rev. Lett. **120**, 260502 (2018).

[16] Y. Wang, Y. Li, Z.-Q. Yin, and B. Zeng, 16-qubit IBM universal quantum computer can be fully entangled, npj Quantum Inf. **4**, 46 (2018).

[17] M. Gong, M.-C. Chen, Y. Zheng, S. Wang, C. Zha, H. Deng, Z. Yan, H. Rong, Y. Wu, S. Li, F. Chen, Y. Zhao, F. Liang, J. Lin, Y. Xu, C. Guo, L. Sun, A. D. Castellano, H. Wang, C. Peng, C.-Y. Lu, X. Zhu, and J.-W. Pan, Genuine 12-qubit entanglement on a superconducting quantum processor, Phys. Rev. Lett. **122**, 110501 (2019).

[18] G. J. Mooney, C. D. Hill, and L. C. L. Hollenberg, Entanglement in a 20-qubit superconducting quantum computer, Sci. Rep. **9**, 13465 (2019).

[19] M. Hayashi and T. Morimae, Verifiable measurement-only blind quantum computing with stabilizer testing, Phys. Rev. Lett. **115**, 220502 (2015).

[20] T. Morimae, D. Nagaj, and N. Schuch, Quantum proofs can be verified using only single-qubit measurements, Phys. Rev. A **93**, 022326 (2016).

[21] K. Fujii and M. Hayashi, Verifiable fault tolerance in measurement-based quantum computation, Phys. Rev. A **96**, 030301(R) (2017).

[22] S. Pallister, N. Linden, and A. Montanaro, Optimal verification of entangled states with local measurements, Phys. Rev. Lett. **120**, 170502 (2018).

[23] M. Hayashi and M. Hajdušek, Self-guaranteed measurement-based quantum computation, Phys. Rev. A **97**, 052308 (2018).

[24] Y. Takeuchi and T. Morimae, Verification of many-qubit states, Phys. Rev. X **8**, 021060 (2018).

[25] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, Resource-efficient verification of quantum computing using Serfling's bound, npj Quantum Inf. **5**, 27 (2019).

[26] H. Zhu and M. Hayashi, Efficient verification of pure quantum states in the adversarial scenario, Phys. Rev. Lett. **123**, 260504 (2019).

[27] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario, Phys. Rev. A **100**, 062335 (2019).

[28] D. Markham and A. Krause, A simple protocol for certifying graph states and applications in quantum networks, Cryptography **4**, 3 (2020).

[29] N. Dangniam, Y.-G. Han, and H. Zhu, Optimal verification of stabilizer states, Phys. Rev. Res. **2**, 043323 (2020).

[30] Z. Li, H. Zhu, and M. Hayashi, Robust and efficient verification of measurement-based quantum computation, npj Quantum Inf. **9**, 115 (2023).

[31] Y. Li, H. Zhang, Z. Li, and H. Zhu, Minimum number of experimental settings required to verify bipartite pure states and unitaries, Phys. Rev. A **104**, 062439 (2021).

[32] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandràa, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Quantum supremacy using a programmable superconducting processor, Nature (London) **574**, 505 (2019).

[33] K. Akimoto, S. Tsuchiya, R. Yoshii, and Y. Takeuchi, Passive verification protocol for thermal graph states, Phys. Rev. A **106**, 012405 (2022).

[34] R. Raussendorf, J. Harrington, and K. Goyal, Topological fault-tolerance in cluster state quantum computation, New J. Phys. **9**, 199 (2007).

[35] D. S. Wang, A. G. Fowler, and L. C. L. Hollenberg, Surface code quantum computing with error rates over 1, Phys. Rev. A **83**, 020302(R) (2011).

[36] H. Bombin, R. S. Andrist, M. Ohzeki, H. G. Katzgraber, and M. A. Martin-Delgado, Strong Resilience of Topological Codes to Depolarization, Phys. Rev. X **2**, 021004 (2012).

[37] R. Takagi, S. Endo, S. Minagawa, and M. Gu, Fundamental limits of quantum error mitigation, npj Quantum Inf. **8**, 114 (2022).

[38] R. Takagi, H. Tajima, and M. Gu, Universal sampling lower bounds for quantum error mitigation, Phys. Rev. Lett. **131**, 210602 (2023).

[39] K. Tsubouchi, T. Sagawa, and N. Yoshioka, Universal cost bound of quantum error mitigation based on quantum estimation theory, Phys. Rev. Lett. **131**, 210601 (2023).

[40] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[41] M. Van den Nest, J. Dehaene, and B. D. Moor, Graphical description of the action of local Clifford transformations on graph states, Phys. Rev. A **69**, 022316 (2004).

[42] G. Tóth and I. Apellaniz, Quantum metrology from a quantum information science perspective, J. Phys. A: Math. Theor. **47**, 424006 (2014).

[43] M. J. Hoban, E. T. Campbell, K. Loukopoulos, and D. E. Browne, Non-adaptive measurement-based quantum computation and multi-party Bell inequalities, New J. Phys. **13**, 023014 (2011).

[44] L. Aolita, D. Cavalcanti, R. Chaves, C. Dhara, L. Davidovich, and A. Acín, Noisy evolution of graph-state entanglement, Phys. Rev. A **82**, 032317 (2010).

[45] W. Hoeffding, Probability inequalities for sums of bounded random variables, J. Am. Stat. Assoc. **58**, 13 (1963).

[46] M. M. Wilde, *Quantum Information Theory*, 2nd ed. (Cambridge University Press, Cambridge, 2017).