

Quantum Subspace Verification for Error Correction Codes

Junjie Chen¹,¹ Pei Zeng,² Qi Zhao,³ Xiongfeng Ma,¹ and You Zhou^{4,5,*}

¹Center for Quantum Information, Institute for Interdisciplinary Information Sciences, *Tsinghua University*, Beijing 100084, China

²Pritzker School of Molecular Engineering, *The University of Chicago*, Illinois 60637, USA

³QICI Quantum Information and Computation Initiative, School of Computing and Data Science, *The University of Hong Kong*, Pokfulam Road, Hong Kong SAR, China

⁴Key Laboratory for Information Science of Electromagnetic Waves (Ministry of Education), *Fudan University*, Shanghai 200433, China

⁵*Hefei National Laboratory*, Hefei 230088, China



(Received 12 March 2025; revised 28 May 2025; accepted 10 November 2025; published 3 December 2025)

Quantum error correction is pivotal in advancing toward large-scale quantum computation, and efficient verification is crucial for ensuring the high fidelity of code states. Traditional methodologies, such as state tomography, direct fidelity estimation, and state verification, either fall short in measurement efficiency, especially for large-scale systems, or are restricted to some specific states. In this work, we introduce a general framework for quantum subspace verification, enabling efficient and measurement-noise-robust fidelity estimation between a given state and the target subspace with a specified confidence level. By integrating the proposed subspace verification with direct fidelity estimation, we develop a composite protocol that significantly improves the efficiency of verifying the fidelity of general magic logical states, as demonstrated by intuitive numerical results. This improvement stems from the use of subspace verification, which leverages the knowledge of code subspaces to significantly reduce measurement costs. Additionally, we detail the construction of verification operators for typical error correction codes, including general stabilizer codes and quantum low-density parity-check codes, enabling their efficient implementation using practical local measurements. Notably, for certain codes, such as the Calderbank-Shor-Steane codes and quantum low-density parity-check stabilizer codes, we reduce the number of required measurement settings and sample complexity to a constant level using graphical methods. Our approach facilitates efficient and feasible verification of error correction codes and generic magic logical states, advancing their practical implementations on quantum platforms.

DOI: [10.1103/fyw6-lq11](https://doi.org/10.1103/fyw6-lq11)

I. INTRODUCTION

Quantum information processing and quantum computing have emerged as important technologies, offering potential advantages in areas ranging from simulation [1] to cryptography [2]. Despite notable theoretical and experimental progress [3–5], the practical realization of large-scale quantum computing remains difficult due to the disturbance of noise. Fault-tolerant quantum computing [6,7], facilitated by the framework of quantum error correction (QEC) codes, is the essential pathway

toward achieving large-scale quantum computing. Various QEC codes have been developed, including surface codes [5,8–10], high-quality quantum low-density parity-check (QLDPC) codes [7,11,12], and random stabilizer codes [13]. As the logical fidelity improves, the number of qubits in physical states also increases significantly, making efficient and accurate verification of these QEC states a fundamental challenge.

Conventional methods such as state tomography [14–16] and fidelity estimation [17–19] are known to be resource-intensive with respect to the system size. Although recent advances such as shadow tomography [20–22] have shown improvements in efficiency, they require some global unitary rotations that are difficult to realize. Essentially, these protocols do not adequately address the state verification problem because they fail to utilize prior knowledge about the quantum states. In contrast, quantum state verification [23–25], as an efficient

*Contact author: you_zhou@fudan.edu.cn

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

framework introduced to leverage such prior knowledge, thus significantly reducing the measurement resources [26–32]. In particular, all stabilizer states [33] can be efficiently verified using only local measurements [28,34].

However, efficient verification protocols for more general quantum states beyond stabilizer ones, particularly the logical magic state [35–37], which plays a critical role in the realization of fault-tolerant quantum computing, are still missing [38]. In many early fault-tolerant setups, the code state to be verified is usually not a stabilizer state, such as a small rotation on the logical $|\bar{0}\rangle$ state [39,40]. Moreover, suppose one is only interested in the fidelity between the prepared state and the QEC code subspace, the previous state verification framework [23,25] would complicate the situation, as it generally needs to tailor various protocols for different target physical states in the subspace.

In this work, to fill the gaps, we develop a general framework for quantum subspace verification, extending the traditional approach from the quantum state scenario. Notably, our framework goes beyond the conventional hypothesis testing setup [25,26] by tolerating measurement failures, making it robust against measurement noise.

Furthermore, it enables the estimation of fidelity ranges to chosen subspaces of interest directly from the collected measurement data. Building on this framework, we introduce a composite scheme termed Subspace-Verification-Assisted Fidelity Estimation (SVAFE) (shown in Fig. 1), which facilitates the verification of generic stabilizer code states with a significantly reduced sample complexity compared to previous methods [17,23]. SVAFE first uses the proposed subspace verification to constrain the potential parameters of the quantum states, thereby enhancing the efficiency of the subsequent direct fidelity estimation (DFE) [17] in the logical subspace. In other words, it becomes sufficient to measure only logical Pauli operators in the second step, which could be implemented fault-tolerantly using techniques like lattice surgery [41].

The subspace verification scheme plays a central role in SVAFE, as DFE-related protocols are well-established. For subspace verification, the design of the measurement strategy—essentially, the corresponding verification operator—is crucial, as both the sample complexity and the accuracy of estimated fidelity are intrinsically related to its spectral properties. In this work, we investigate the construction of verification operators for two prevalent

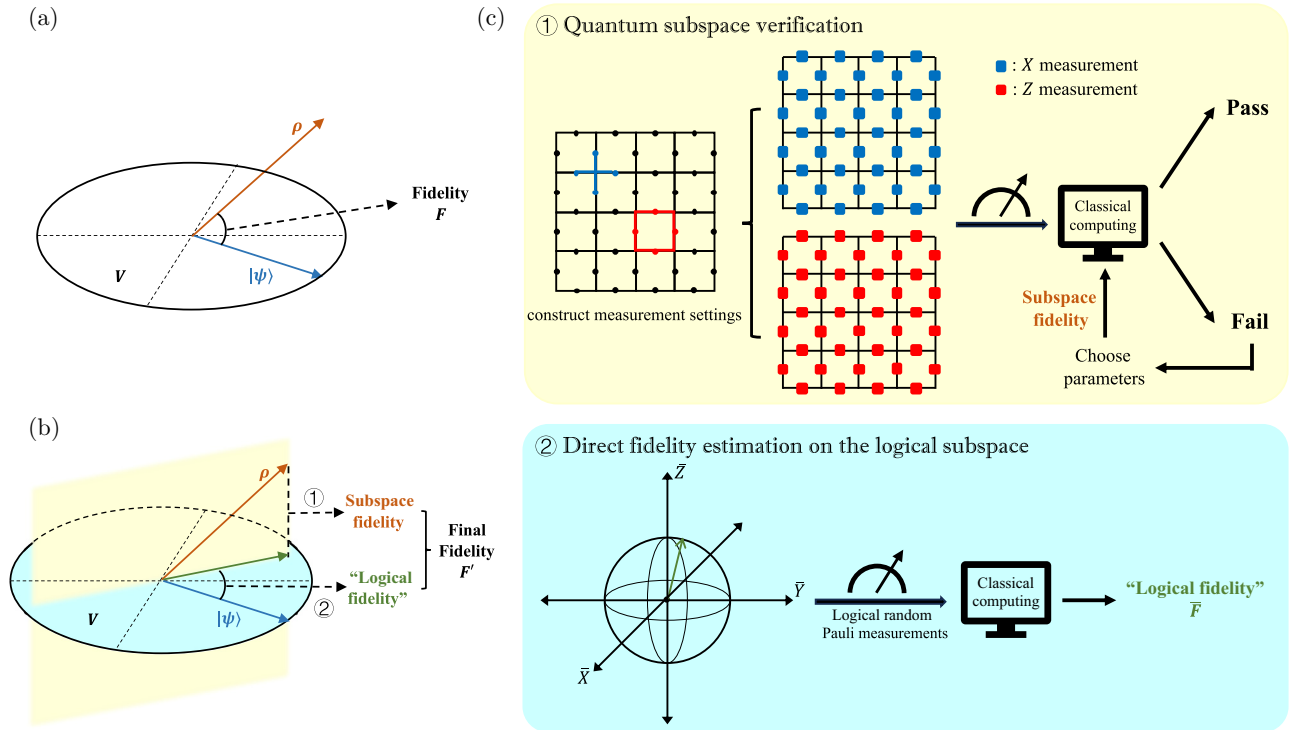


FIG. 1. (a) Illustration of the task of fidelity estimation or state verification. (b) Illustration of the proposed Subspace-Verification-Assisted Fidelity Estimation scheme. The first step involves subspace verification (denoted as ①) to verify the subspace fidelity between the given state ρ (orange vector) and the code subspace V . The second step applies direct fidelity estimation within the logical subspace (denoted as ②) to ascertain the “logical fidelity.” By combining both of them, one can obtain the final fidelity. (c) Application example for a toric code state. Subspace verification is employed first to verify the subspace fidelity with parameters ϵ_1 and δ_1 . It is followed by the assessment of “logical fidelity” through DFE in the code subspace with parameters ϵ_2 and δ_2 . Here, we assume all the measurements can be realized fault-tolerantly. By combining these two steps, one can derive the overall fidelity with parameters ϵ and δ .

classes of QEC codes: stabilizer codes and generic QLDPC codes, with graphical methods, utilizing local measurements to enable practical implementations in physical systems [5,12]. In this context, we employ a generalized concept of QLDPC codes, defined based on projectors, and do not necessarily conform to traditional stabilizer codes. Notably, for Calderbank-Shor-Steane (CSS) codes [42,43] and QLDPC stabilizer codes [7,11], the number of local measurement settings and the sample complexity can be significantly reduced, potentially to a constant level.

Consequently, our work enables efficient and feasible verification of QEC code subspaces and generic magic logical states, which are crucial for the current early fault-tolerant era. In Sec. II, we introduce the framework for subspace verification, covering both the hypothesis testing and fidelity estimation scenarios. Sections III and IV detail the construction of verification operators for stabilizer codes and QLDPC codes, respectively. The protocol of SSAFE is presented in Sec. V.

II. FRAMEWORK OF SUBSPACE VERIFICATION

Verifying whether a state is in the code subspace is a common task in quantum error correction. Although measuring the stabilizers or projectors of the code subspace using ancillary qubits is a fundamental method, its practical use remains limited because such an approach inherently propagates measurement errors through interactions with ancillary qubits and requires additional hardware overhead. Furthermore, in some physical platforms such as photonic systems, implementing stabilizer or projector measurements is challenging due to difficulties in applying control gates. As a result, destructive state verification usually becomes the default measurement paradigm in verification problems. It requires no ancilla and only local measurement, matching native measurement capabilities across major platforms (photonic, superconducting qubits via demolition readout, trapped ions via state fluorescence), where nondestructive parity checks often require complex ancillary architectures.

In this section, we present a framework for subspace verification. It is important to note that this framework applies to any quantum subspace verification and is not solely restricted to QEC code subspaces.

Given a quantum device that should produce quantum states in a specific subspace $\mathcal{V}$, our objective is to verify whether it works correctly. Suppose the device always produces quantum states independently and identically (i.i.d. assumption). Denote the projector to the target subspace $\mathcal{V}$ as $\mathcal{P}$ and denote the expected quantum states produced by the device as ρ . We can use the fidelity between ρ and $\mathcal{P}$ defined as

$$F(\mathcal{P}, \rho) := \text{Tr}(\mathcal{P}\rho) \quad (1)$$

to characterize the overlap between a quantum state and the target subspace [26,32]. Then, the verification problem can be described by the following hypothesis testing problem [44].

- (1) The device is “good”: The quantum states ρ generated by it satisfy $F(\mathcal{P}, \rho) \geq 1 - \tau\epsilon$.
- (2) The device is “bad”: The quantum states ρ generated by it satisfy $F(\mathcal{P}, \rho) \leq 1 - \epsilon$.

Notice that a gap characterized by $\tau < 1$ is introduced to tolerate imperfect verification strategy design and measurement result fluctuation. Ideally, one would like to minimize this gap, approaching $\tau \rightarrow 1$. However, while measurement result fluctuations can be reduced to any small positive constant with sufficient samples, the impact of an imperfect verification strategy design cannot be disregarded. We will later provide an upper bound for τ , taking these considerations into account.

To achieve this task, a strategy analogous to that in quantum state verification can be adopted [25,26]. To be specific, one can adopt a series of two-outcome positive-operator-valued measurements (POVMs) $\{E_l, \mathbb{I} - E_l\}_l$. If the measurement outcome corresponds to E_l , it is considered to have passed the test; otherwise, it is deemed to have failed. These POVMs should be designed such that any state ρ within the subspace $\mathcal{V}$ will always pass the test, i.e., $\text{Tr}(E_l\rho) = 1, \forall \rho \in \mathcal{V}$. In each verification round, we choose a POVM $\{E_l, \mathbb{I} - E_l\}$ from a probability distribution p_l with $\sum_l p_l = 1$. Define

$$\Omega = \sum_l p_l E_l \quad (2)$$

as the verification operator. By construction, one thus has $\text{Tr}(\Omega\sigma) = \sum_l p_l \text{Tr}(E_l\sigma) = 1$ for any $\sigma \in \mathcal{V}$. The following fact, analogous to that in [25,26], gives the spectral decomposition of Ω .

Fact 1. The verification operator Ω for the subspace $\mathcal{V}$ shows the following spectral decomposition:

$$\Omega = \mathcal{P} + \sum_{j=d_{\mathcal{V}}+1}^d \lambda_j |\psi_j\rangle\langle\psi_j|, \quad (3)$$

where $\mathcal{P}$ is the projector of $\mathcal{V}$ and $\{|\psi_j\rangle\}_{k=d_{\mathcal{V}}+1}^d$ is a set of basis for the orthogonal complement $\mathcal{V}^\perp$. d and $d_{\mathcal{V}}$ are the dimensions of the Hilbert space and the subspace $\mathcal{V}$, respectively. The eigenvalues are arranged in descending order.

Note that the largest eigenvalue of Ω is 1. We denote the spectral gap between the largest eigenvalue and the second largest one as $\Delta_{\min}(\Omega) = 1 - \lambda_{d_{\mathcal{V}}+1}$, and the spectral gap between the largest eigenvalue and the smallest

one as $\Delta_{\max}(\Omega) = 1 - \lambda_d$, and it is clear that $\Delta_{\max}(\Omega) \geq \Delta_{\min}(\Omega)$.

Note that even a “good” device can occasionally fail a test; therefore, we should not classify a device as “good” only if it passes every single test. Now, define $r := \Delta_{\min}(\Omega)/\tau \Delta_{\max}(\Omega)$ and $\tilde{\epsilon} := \Delta_{\min}(\Omega)\epsilon$ for short. Denote

$$p_0 = \frac{\ln r}{\ln r + \ln \frac{1-\tilde{\epsilon}/r}{1-\tilde{\epsilon}}} \quad (4)$$

as the solution to the equation $D[p_0 \| 1 - \tilde{\epsilon}] = D[p_0 \| 1 - \tilde{\epsilon}/r]$, where $D[p \| q] := p \log(p/q) + (1-p) \log(1-p)/(1-q)$ stands for the Kullback-Leibler divergence for Bernoulli distribution.

Suppose we adopt the verification tests for N times and N_{pass} of them pass. To assess the performance of the quantum device, we evaluate whether $N_{\text{pass}} > p_0 N$. If this condition is met, we categorize it as “good”; otherwise, we categorize it as “bad.” The subsequent theorem shows the number of required verification tests for this assessment strategy.

Theorem 1. For the verification problem described by parameters ϵ , δ , τ , and the verification operator Ω , if $\tau \Delta_{\max}(\Omega) < \Delta_{\min}(\Omega)$ (i.e., $r > 1$), one can reach confidence $1 - \delta$ with

$$N = \frac{\ln 1/\delta}{D[p_0 \| 1 - \tilde{\epsilon}]} \quad (5)$$

rounds of tests. More specifically, suppose we adopt the verification tests for N times and N_{pass} of them pass. The type 1 error, i.e., the probability of getting $N_{\text{pass}} \leq p_0 N$ when the device is “good” is upper-bounded by

$$\Pr(N_{\text{pass}} \leq p_0 N) \leq \delta = e^{-D[p_0 \| 1 - \tilde{\epsilon}/r]N}. \quad (6)$$

The type 2 error, i.e., the probability of getting $N_{\text{pass}} \geq p_0 N$ when the device is “bad” is upper-bounded by

$$\Pr(N_{\text{pass}} \geq p_0 N) \leq \delta = e^{-D[p_0 \| 1 - \tilde{\epsilon}]N}. \quad (7)$$

Here the parameters r , $\tilde{\epsilon}$, and p_0 are defined around Eq. (4).

One can prove it by bounding the passing probability, i.e., $\mathbb{E}[N_{\text{pass}}/N]$, with $1 - \tilde{\epsilon}$ and $1 - \tilde{\epsilon}/r$ and using the Chernoff-Hoeffding theorem. The detailed proof is given in Appendix A. When ϵ is sufficiently small, we can simplify Eq. (5) to the first order in ϵ ,

$$N \sim f(r) \frac{\ln 1/\delta}{\Delta_{\min}(\Omega)\epsilon}, \quad (8)$$

where $f(r) := (1 + (1/\ln r)(1 - (1/r))(\ln(1/\ln r(1 - (1/r))))^{-1}$ is some constant as a function of r . Notably, the scaling of N with respect to ϵ is

$N = O(1/\epsilon)$, which deviates significantly from the typical scaling of $N = O(1/\epsilon^2)$ found in fidelity estimation [17,19,45]. This distinct scaling behavior is closely associated with the property of hypothesis testing that “good” states invariably pass the test. Specifically, the verification operator can be expressed as outlined in Eq. (3), where the coefficient of $\mathcal{P}$ is 1.

It is also noteworthy that our framework diverges from previous state verification frameworks [25,26]. Traditional frameworks require the “good” case of the hypothesis testing problem to satisfy $F(\mathcal{P}, \rho) = 1$, implying that the device is judged to be “good” only if all tests are passed. However, physical states are invariably noisy, and it is unrealistic to expect that they will consistently pass every test, rendering these frameworks less effective when there is non-negligible measurement error or the fidelity is not exceptionally high. Our framework modifies the “good” case to be $F(\mathcal{P}, \rho) \geq 1 - \tau\epsilon$, thereby accommodating scenarios where fidelity may not reach such ideal levels. Notably, when $\tau \rightarrow 0$, the equation $D[p_0 \| 1 - \tilde{\epsilon}] = D[p_0 \| 1 - \tilde{\epsilon}/r]$ cannot hold since r is singular. In this case, if we simply let $p_0 = 1$, the type 2 error is always 0 and the type 1 error gives $N = \ln(1/\delta)/D[p_0 \| 1 - \tilde{\epsilon}] = \ln(1/\delta)/(-\ln(1 - \tilde{\epsilon})) \approx \ln(1/\delta)/\Delta_{\min}(\Omega)\epsilon$ according to Eq. (5), which degenerates to the result of previous frameworks [25,26].

Based on Theorem 1, we can give the following proposition, which considers an estimation scenario rather than a hypothesis testing scenario. We want to derive a bound for the infidelity of the input state ρ with the ratio of passed tests.

Proposition 1. Suppose we adopt the verification tests for N times, and N_{pass} of them pass. Denote $p = N_{\text{pass}}/N$ as the passing frequency observed in the verification, the estimated infidelity can be bounded in the interval

$$\max \left\{ \frac{1-p-\xi}{\Delta_{\max}(\Omega)}, 0 \right\} \leq \epsilon_\rho \leq \min \left\{ \frac{1-p+\xi}{\Delta_{\min}(\Omega)}, 1 \right\} \quad (9)$$

with approximate confidence level $1 - \delta$. Here $\xi = z(1 - (\delta/2))\sqrt{p(1-p)/N}$ with $z(x)$ standing for the inverse of the cumulative distribution function of the standard normal distribution at x .

The proof is given in Appendix B. The physical interpretation of Eq. (9) is straightforward. The term ξ arises from statistical fluctuations, proportional to the square root of N , and approaches zero as $N \rightarrow \infty$. The factors $1/\Delta_{\max}(\Omega)$ and $1/\Delta_{\min}(\Omega)$ result from imperfect verification operator design. They will equal 1 if Ω is ideally designed, i.e., $\lambda_{d_V+1} = \lambda_d = 0$. The remaining term, $1 - p$, represents the expected infidelity. Notice that in Eq. (9), the uncertainty of ϵ is proportional to $1/\sqrt{N}$ rather than $1/N$. This distinction indicates that the specific scaling of sample complexity only appears in the hypothesis testing scenario.

Given parameters ϵ , δ , and τ , our goal of minimizing the net sample complexity N involves optimizing the construction of the verification operator Ω . In the subsequent two sections, we will focus on developing verification operators for two typical QEC codes: stabilizer codes and QLDPC codes. The main concern is to improve the spectral gaps and reduce the number of different measurement settings, which will be introduced in the next section.

III. VERIFICATION OF STABILIZER CODE SUBSPACE

Stabilizer codes play an essential role in the design of quantum error correction codes, primarily because the stabilizer formalism facilitates the adaptation of some classical codes into quantum codes. For an $[[n, k, d]]$ stabilizer code, the code subspace $\mathcal{V}$ is characterized by its stabilizer group $\mathbb{S} = \langle S_i \rangle_{i=1}^m$ where $m = n - k$. The projector onto the code subspace $\mathcal{V}$ can be expressed as

$$\mathcal{P} = \prod_{i=1}^m \frac{\mathbb{I} + S_i}{2} = \frac{1}{2^m} \sum_{S \in \mathbb{S}} S. \quad (10)$$

If there is no restriction on the measurement, one can directly adopt $\{\mathcal{P}, \mathbb{I} - \mathcal{P}\}$ as the POVM, i.e., the projector itself, to do the verification. In this way, the verification operator is actually $\Omega = \mathcal{P}$ with the spectral gaps $\Delta_{\min}(\mathcal{P}) = \Delta_{\max}(\mathcal{P}) = 1$. Although the performance is optimal, implementing multiqubit measurements on real quantum devices presents substantial challenges. Therefore, our focus shifts to the verification operator constructed from s -local measurements with constant s , which can be implemented using the tensor product of at most s -qubit measurements. Specifically, when $s = 1$, indicating the use of only single-qubit measurements, we refer to these as local measurements in subsequent discussions. The number of local measurement settings required to realize Ω is a critical parameter in the design of the verification operator.

As all the stabilizers are Pauli operators that can be measured with local measurements, a natural construction is to measure all the stabilizers S in $\mathbb{S}$ with local measurements with equal probability. The verification operator is

$$\Omega_{\text{all}} = \frac{1}{2^m} \sum_{S \in \mathbb{S}} \frac{\mathbb{I} + S}{2} = \frac{\mathbb{I} + \mathcal{P}}{2}. \quad (11)$$

The spectral gaps are $\Delta_{\min}(\Omega_{\text{all}}) = \Delta_{\max}(\Omega_{\text{all}}) = 1/2$, suggesting that the number of verification tests required scales as $O(\ln(1/\delta)/\epsilon)$, independent of m . Nevertheless, each $S \in \mathbb{S}$ corresponds to a local measurement setting. The number of measurement settings required scales exponentially with m , potentially complicating experimental implementation.

To reduce the number of measurement settings, one can turn to measure all the stabilizer generators S_i of the subspace with equal probability. It needs at most m different measurement settings. The verification operator becomes

$$\Omega_{\text{gen}} = \frac{1}{m} \sum_{i=1}^m \frac{\mathbb{I} + S_i}{2} = \frac{1}{2} \left(\mathbb{I} + \frac{1}{m} \sum_{i=1}^m S_i \right). \quad (12)$$

The spectral gaps are given by $\Delta_{\min}(\Omega_{\text{gen}}) = 1/m$ and $\Delta_{\max}(\Omega_{\text{gen}}) = 1$, which will be proven in Appendix C. Due to the nonconstant spectral gap, the number of verification tests required scales as $O(\ln(1/\delta)/\epsilon m)$, which hinders the performance of the strategy for a large m .

We further introduce a new construction of Ω to improve the spectral gap and reduce the number of measurement settings. Our method is inspired by the chromatic property of the graph state [46–49]. We start by defining the concept of bitwise commutativity of stabilizers and the corresponding graph.

Definition 1. Two stabilizers on the same system, S and S' , bitwise commute with each other iff their reduced operators on any qubit l commute, $[S(l), S'(l)] = 0$.

The bitwise commutativity graph G_S associated with a stabilizer generator set $\mathcal{S} := \{S_1, S_2, \dots, S_m\}$ is defined as follows: The vertex set $V = \{v_i\}_{i=1}^m$ represents the stabilizer generators, and the edge set $E = \{e_{ij}\}$ contains an edge e_{ij} iff S_i and S_j do not bitwise commute.

We remark that if one focuses on the typical class of stabilizer states, the graph states, the introduced bitwise commutativity graph becomes the corresponding graph of graph states as one considers the generator associated with each vertex [50].

If S_i and S_j bitwise commute, there should be $S_i(l) = \mathbb{I}$ or $S_j(l) = \mathbb{I}$ or $S_i(l) \cdot S_j(l) = \mathbb{I}$. As a result, one can measure them and their product $S_i S_j$ simultaneously. Take an independent set $\mathcal{I}$ of vertices in G_S , any two stabilizers corresponding to the vertices in $\mathcal{I}$ should bitwise commute, i.e., S_i and S_j bitwise commute if $v_i, v_j \in \mathcal{I}$. Now, construct a Pauli operator $M_{\mathcal{I}}$: $M_{\mathcal{I}}(l) = S_i(l)$ if there exists $v_i \in \mathcal{I}$ such that $S_i(l) \neq \mathbb{I}$; otherwise, $M_{\mathcal{I}}(l) = \mathbb{I}$. One can find that any S_i corresponding to $v_i \in \mathcal{I}$ or their product is a reduced operator of $M_{\mathcal{I}}$. Therefore, all of the stabilizers whose corresponding vertices are in $\mathcal{I}$ and their product can be measured simultaneously with just a single measurement setting $M_{\mathcal{I}}$. Here, a measurement setting $M_{\mathcal{I}}$ means to assign the measurement basis according to the single qubit Pauli operators of $M_{\mathcal{I}}$. Furthermore, the POVM $\{\mathcal{P}_{\mathcal{I}}, \mathbb{I} - \mathcal{P}_{\mathcal{I}}\}$ where

$$\mathcal{P}_{\mathcal{I}} = \prod_{v_i \in \mathcal{I}} \frac{\mathbb{I} + S_i}{2} \quad (13)$$

can be realized by local measurement setting $M_{\mathcal{I}}$ and postprocessing (2).

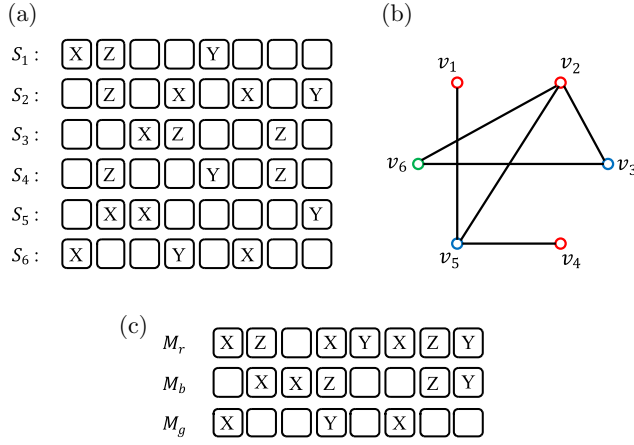


FIG. 2. Construction of $\Omega_{\text{chr}}(\mathcal{S})$: (a) an example set of stabilizer generators; (b) the corresponding bitwise commutativity graph of stabilizers in (a); (c) measurement settings according to the chromatic method in (b).

An optimal coloring method $\{\mathcal{I}_u\}_{u=1}^{\chi(G_S)}$ of G_S divides vertices into a minimal number of independent sets, i.e., $V = \bigcup_{u=1}^{\chi(G_S)} \mathcal{I}_u$ and $\mathcal{I}_u \cap \mathcal{I}_v = \emptyset$ for $u \neq v$. $\chi(G_S)$ stands for the chromatic number of G_S . We can construct a verification operator as

$$\Omega_{\text{chr}}(\mathcal{S}) = \frac{1}{\chi(G_S)} \sum_{u=1}^{\chi(G_S)} \mathcal{P}_{\mathcal{I}_u} = \frac{1}{\chi(G_S)} \sum_{u=1}^{\chi(G_S)} \prod_{v_i \in \mathcal{I}_u} \frac{\mathbb{I} + S_i}{2}. \quad (14)$$

An example illustrating the construction of $\Omega_{\text{chr}}(\mathcal{S})$ is shown in Fig. 2. It is clear that $\Omega_{\text{chr}}(\mathcal{S})$ is a legal verification operator and can be measured with $\chi(G_S)$ measurement settings. The spectral gaps show $\Delta_{\min}(\Omega_{\text{chr}}(\mathcal{S})) = 1/\chi(G_S)$ and $\Delta_{\max}(\Omega_{\text{chr}}(\mathcal{S})) = 1$, which will be proved in Appendix C.

Notice that the construction of $\Omega_{\text{chr}}(\mathcal{S})$ is uniquely determined by the set of stabilizer generators $\mathcal{S}$ rather than the stabilizer group $\mathbb{S}$. As there are different choices of $\mathcal{S}$ given $\mathbb{S}$, one can further optimize the construction of $\Omega_{\text{chr}}(\mathcal{S})$ by choosing $\mathcal{S}$ such that the chromatic number $\chi(G_S)$ is minimal. Denote the optimal set of stabilizer generators as $\mathcal{S}^*$ and the corresponding chromatic number as χ^* . The optimal choice of $\Omega_{\text{chr}}(\mathcal{S})$ is thus

$$\Omega_{\text{chr}}^* = \frac{1}{\chi^*} \sum_{u=1}^{\chi^*} \mathcal{P}_{\mathcal{I}_u}, \quad (15)$$

with χ^* measurement settings and spectral gaps $\Delta_{\min}(\Omega_{\text{chr}}^*) = 1/\chi^*$, $\Delta_{\max}(\Omega_{\text{chr}}^*) = 1$.

Compared with Ω_{gen} , the verification operator Ω_{chr}^* reduces the number of measurement setting required from m to χ^* and improve the spectral gap $\Delta_{\min}(\Omega)$ from $1/m$

to $1/\chi^*$. For large-scale QEC codes, the optimal chromatic number χ^* usually scales much slower than m and often remains constant. For example, CSS code [42,43], including many practical QEC architectures such as surface codes [9], toric codes [8], and hypergraph-product codes [51], is an important code family that supports transversal CNOT gates and maintains a close connection to classical linear codes. All CSS codes share the optimal chromatic number $\chi^* = 2$. Besides, for QLDPC stabilizer codes [7,11,12], which are valued for efficient syndrome measurement and will be discussed in the next section, the chromatic number χ^* is also bounded by a constant. By contrast, stabilizer codes with a large chromatic number are generally impractical, lacking convenient transversal gates and incurring prohibitive overhead in fault-tolerant quantum computing [7], highlighting the practical advantages of our construction [46,48].

IV. VERIFICATION OF QLDPC CODE SUBSPACE

QLDPC codes with a constant encoding rate have been demonstrated to reduce the overhead of fault-tolerant quantum computation to a constant level [7]. This significant reduction positions them as a promising candidate for fault-tolerant quantum computing. For an $[[n, k, d]]$ QLDPC code, the code subspace $\mathcal{V}$ is uniquely determined by $m = n - k$ pairwise commuting projectors $\Pi = \{\pi_i\}_{i=1}^m$, such that any quantum state $|\psi\rangle \in \mathcal{V}$ should satisfies $\pi_i |\psi\rangle = |\psi\rangle$ for all $i \in [m]$. The projector onto the QLDPC code subspace $\mathcal{V}$ is given by $\mathcal{P} = \prod_{i=1}^m \pi_i$, analogous to stabilizer codes. We denote a subsystem $A = \text{supp}(O)$ as the nontrivial support of any operator O iff O can be decomposed as $O = O_A \otimes \mathbb{I}_{\bar{A}}$, and one cannot find a smaller subsystem $A' \subset A$ such that $O = O_{A'} \otimes \mathbb{I}_{\bar{A}'}$. The sparsity of Π is defined as $s := \max_i |\text{supp}(\pi_i)|$. For QLDPC codes, s should be some constant independent of n .

We can also define a support graph, analog to the previously introduced Definition 1 for stabilizer states.

Definition 2. The support graph G_Π associated with the set of projectors $\Pi = \{\pi_i\}_{i=1}^m$ is defined as follows: The vertex set $V = \{v_i\}_{i=1}^m$ represents the projectors, and the edge set $E = \{e_{ij}\}$ contains an edge e_{ij} iff $\text{supp}(\pi_i) \cap \text{supp}(\pi_j) \neq \emptyset$.

The QLDPC condition requires that each qubit appears in no more than s supports of the projectors. Combining with the fact that each projector acts nontrivially on at most s qubits, the support of any projector intersects with at most s^2 other supports, which implies that the degree of G_Π is at most s^2 . Consequently, the support graph G_Π of any QLDPC code with sparsity s can be colored with no more than s^2 colors.

If s -local measurements are permitted, verification operators similar to those discussed in the previous section can

be constructed, as each POVM $\{\pi_i, \mathbb{I} - \pi_i\}$ can be realized with a single s -local measurement. To be specific, by measuring each projector with equal probability, we can construct

$$\Omega_{\text{gen}}^{(s)} = \frac{1}{m} \sum_{i=1}^m \pi_i, \quad (16)$$

with spectral gaps $\Delta_{\min}(\Omega_{\text{gen}}^{(s)}) = 1/m$ and $\Delta_{\max}(\Omega_{\text{gen}}^{(s)}) = 1$. Here, the superscript (s) implies s -local measurements are used. It is not hard to find that $\Omega_{\text{gen}}^{(s)}$ can be realized with m different s -local measurement settings. Moreover, with a coloring method of the support graph G_{Π} , we can construct

$$\Omega_{\text{chr}}^{(s)} = \frac{1}{\chi(G_{\Pi})} \sum_{u=1}^{\chi(G_{\Pi})} \prod_{v_i \in \mathcal{I}_u} \pi_i, \quad (17)$$

with spectral gaps $\Delta_{\min}(\Omega_{\text{chr}}^{(s)}) = 1/\chi(G_{\Pi}) \geq 1/s^2$ and $\Delta_{\max}(\Omega_{\text{chr}}^{(s)}) = 1$. Each $\prod_{v_i \in \mathcal{I}_u} \pi_i$ can be measured with a single measurement setting since different π_i in the same independent set act on different supports, which indicates that $\Omega_{\text{chr}}^{(s)}$ can be realized with $\chi(G_{\Pi}) \leq s^2$ different measurement settings.

For QLDPC stabilizer codes [7,11,12], since all the s -local projectors are $+1$ projectors of Pauli operators, they can be measured with one-local measurements and postprocessing. However, in general, $\{\pi_i, \mathbb{I} - \pi_i\}$ cannot be directly implemented by a single local measurement setting and postprocessing. The implementation of s -local measurements often faces practical challenges due to the geometric limitations of the qubits. Consequently, there is a continued need to develop methodologies that utilize one-local measurements.

To address this problem, we decompose the projectors π_i into Pauli measurements that are feasible to implement. We also present the associated verification operator along with its spectral information. Further details and proofs are provided in Appendix D.

Let $T_i = 2\pi_i - \mathbb{I}$ as the measurement operator of $\{\pi_i, \mathbb{I} - \pi_i\}$. One can decompose $T_i = \sum_{P_j \in \mathbb{P}_n} t_{ij} P_j$ where $t_{ij} = \text{Tr}(T_i P_j)$ are positive numbers and $\mathbb{P}_n = \{\mathbb{I}, X, Y, Z\}^{\otimes n}$ denotes the n -qubit Pauli group with only ± 1 phase. All the P_j with nonzero coefficient t_{ij} should act on the sub-supports of A_i , which is the support of T_i (or π_i). Denote each set of Pauli operators with nonzero t_{ij} with $\mathcal{T}_i$, and let $a_i = \sum_j t_{ij}$, $p_{ij} = t_{ij}/a_i$ for simplicity. Therefore, $\{p_{ij}\}_j$ can be regarded as a probability distribution. Since $t_{ij} \in [0, 1]$ and $1/2^n \text{Tr}(T_i) = \sum_j t_{ij}^2 = 1$, we can obtain $1 \leq a_i \leq \sqrt{|\mathcal{T}_i|} \leq 2^s$. The decomposition can be written as $T_i = a_i \sum_{P_{ij} \in \mathcal{T}_i} p_{ij} P_{ij}$. Based on the decomposition, the

verification operator can be constructed as

$$\begin{aligned} \Omega_{\text{gen}}^{(1)} &= \frac{1}{m} \sum_i \left(\frac{1}{a_i} \pi_i + \left(1 - \frac{1}{a_i}\right) \frac{\mathbb{I}}{2} \right) \\ &= \frac{1}{m} \sum_i \left(\frac{1}{2} \sum_{P_{ij} \in \mathcal{T}_i} p_{ij} P_{ij} + \frac{\mathbb{I}}{2} \right) \\ &= \frac{1}{m} \sum_i \sum_{P_{ij} \in \mathcal{T}_i} p_{ij} \frac{\mathbb{I} + P_{ij}}{2}. \end{aligned} \quad (18)$$

The corresponding spectral gaps are given by

$$\Delta_{\min}(\Omega_{\text{gen}}^{(1)}) = \frac{1}{m \cdot \max_i a_i}, \quad \Delta_{\max}(\Omega_{\text{gen}}^{(1)}) = \frac{1}{m} \sum_i \frac{1}{a_i}. \quad (19)$$

Since $1 \leq a_i \leq \sqrt{|\mathcal{T}_i|} \leq 2^s$, the spectral gaps $\Delta_{\min}(\Omega_{\text{gen}}^{(1)}) \geq 1/2^s m$ and $\Delta_{\max}(\Omega_{\text{gen}}^{(1)}) \geq 1/2^s$. Meanwhile, since $\{p_{ij}\}_j$ can be regarded as a probability distribution, such a verification operator can be realized by measuring P_{ij} with probability p_{ij} , totally no more than $\sum_i |\mathcal{T}_i| \leq m \cdot 4^s$ measurement settings.

Importantly, note that $\Omega_{\text{gen}}^{(1)}$ does not have the maximum eigenvalue $+1$ anymore, as shown in Appendix D, which implies that perfect QLDPC code states might not pass the test. This indicates that the analysis in Theorem 1 no longer applies. Therefore, we give the following refined treatment, which would be of independent interest.

Proposition 2. For the verification problem described by parameters ϵ , δ , τ , and the verification operator Ω , suppose the verification operator Ω has the maximum eigenvalue $\lambda < 1$, i.e., $\Omega = \lambda \mathcal{P} + \sum_{j=d_V+1}^d \lambda_j |\psi_j\rangle\langle\psi_j|$. If $\tau \Delta_{\max}(\Omega) < \Delta_{\min}(\Omega)$, one can reach confidence $1 - \delta$ with the judgement passing frequency p'_0 given in Eq. (E3) as a function of λ , τ , ϵ and spectral gaps of Ω , and

$$N \sim \frac{8\lambda(1-\lambda) \ln 1/\delta}{(\Delta_{\min}(\Omega) - \Delta_{\max}(\Omega)\tau)^2 \epsilon^2} \quad (20)$$

rounds of tests. In other words, if $N_{\text{pass}} \geq p'_0 N$, we categorize the device as “good”; otherwise, we categorize it as “bad.”

The proof is analogous to that of Theorem 1 and given in Appendix E. If one regards λ as a constant for general case, $N = O(\ln(1/\delta)/\Delta_{\min}^2(\Omega)\epsilon^2)$ scales differently as that in Theorem 1. This difference comes from the condition that the maximum eigenvalue of Ω is no longer 1, i.e., the states in the target subspace may also fail to pass the test.

For $\Omega_{\text{gen}}^{(1)}$, the maximum eigenvalue, denoted as λ , is calculated as $\lambda = \frac{1}{2} (1 + (1/m) \sum_i 1/a_i)$, where it is trivially

bounded within the interval $[\frac{1}{2}, 1]$. Consequently, λ can be considered a constant, and the number of tests required scales $N = O(m^2 \ln(1/\delta)/\epsilon^2)$. The quadratic relation to m and ϵ comes from the inexistence of a local operator such that the code space is a subspace of its $+1$ eigenspace for general QLDPC codes.

One may expect the enhancement construction of $\Omega_{\text{chr}}^{(1)}$, analogous to that in Eq. (17), which can be implemented with one-local measurement settings. However, such construction typically results in exponentially small eigenvalues, making it ineffective for verification tasks. Detailed discussion is given in Appendix D.

V. FIDELITY ESTIMATION OF LOGICAL STATES

A common challenge in quantum information processing and quantum computing involves estimating the fidelity between a quantum state ρ and a target state $|\psi\rangle$. Two prevalent methods, quantum state verification [23,25–27] and DFE [17–19,45], exhibit specific constraints respectively. Quantum state verification, while relatively efficient, typically relies on the stabilizer structure of the target state $|\psi\rangle$, making it difficult to develop efficient protocols for general magic states [38]. Conversely, DFE offers broader applicability across various quantum states but demands substantial resources, especially for magic states. The sample complexity of this method scales exponentially with the number of qubits n , specifically $O((1/\epsilon^2\delta) + (2^n/\epsilon^2) \ln 1/\delta)$, rendering it unsuitable for large systems. We first briefly introduce it before starting our protocol.

The main idea of DFE to avoid full quantum-state tomography is to measure only a small random subset of Pauli observables and to combine them into an unbiased fidelity estimator. Suppose the target state can be decomposed as $|\psi\rangle\langle\psi| = 1/2^n \sum_{P \in \mathbb{P}_n} \alpha_P P$ with $\alpha_P = \text{Tr}(P|\psi\rangle\langle\psi|)$. In each step, one can select a random Pauli operator P according to the probability distribution $(1/2^n)\alpha_P^2$ over all Pauli operators (due to the purity condition $1/2^n \sum_P \alpha_P^2 = 1$) and measure its expectation value on ρ . Ideally, one would obtain $\text{Tr}(P\rho)$ with probability $(1/2^n)\alpha_P^2$. If we construct the estimator as $\text{Tr}(P\rho)/\alpha_P$, the expectation gives

$$\mathbb{E}\left[\frac{\text{Tr}(P\rho)}{\alpha_P}\right] = \sum_P \frac{1}{2^n} \alpha_P \text{Tr}(P\rho) = \text{Tr}(|\psi\rangle\langle\psi|\rho). \quad (21)$$

Consequently, $\text{Tr}(P\rho)/\alpha_P$ is an unbiased estimator of $F(\rho, |\psi\rangle)$. Detailed error analysis [17] shows that only $l = \lceil 1/\epsilon^2\delta \rceil$ Pauli observables need to be measured to estimate $F(\rho, |\psi\rangle)$ with an error ϵ and confidence level $1 - \delta$, i.e., we only need to measure a constant number of distinct observables. However, the Pauli observable should be measured for $m_P = \lceil 2 \log(2/\delta)/(\alpha_P^2 l \epsilon^2) \rceil$ times, which could be exponentially large depending on α_P . The

expected number of sample complexity shows $\mathbb{E}[m_P] = O((1/\epsilon^2\delta) + 2^n \log(1/\delta)/\epsilon^2)$, which remains exponential in the number of qubits n .

By integrating quantum subspace verification with DFE, we propose a composite protocol, SVAFE, for estimating the fidelity between a state ρ and a stabilizer code state $|\psi\rangle$ as follows, where $|\psi\rangle$ could be any magic state in the code space. Crucially, the subspace verification step certifies that the prepared state lies within the code subspace, and this certification is essential for reducing the effective Hilbert space dimension. Without it, direct fidelity estimation would still operate over the full physical Hilbert space of dimension 2^n , leading to prohibitive costs. With subspace verification in place, DFE can instead be applied on the logical subspace of dimension 2^k , thereby achieving a substantial reduction in resource cost for fidelity estimation.

We first adopt the subspace verification protocol to ensure that the given state ρ lies close to the code subspace $\mathcal{V}$, i.e., the fidelity satisfies $\text{Tr}(\mathcal{P}_{\mathcal{V}}\rho) \geq 1 - \epsilon_1$ with confidence $1 - \delta_1$. Specifically, based on Eq. (7) in Theorem 1, one has

$$\Pr(N_{\text{pass}} \geq p_0 N_1 | \text{Tr}(\mathcal{P}_{\mathcal{V}}\rho) \leq 1 - \epsilon_1) \leq \delta_1. \quad (22)$$

After confirming that ρ is close to the verified subspace $\mathcal{V}$ (within the above confidence), we implement the DFE scheme on the logical qubits to evaluate the “logical fidelity” between ρ and the ideal logical state $|\psi\rangle$,

$$\bar{F} := \frac{1}{2^k} \sum_{\bar{P}} \text{Tr}(\bar{P}|\psi\rangle\langle\psi|) \cdot \text{Tr}(\bar{P}\rho), \quad (23)$$

where the sum runs over physical operators $\bar{P}$ that represent the logical Pauli operators P on the k -qubit logical subspace. As an example, for a $[[7, 1, 3]]$ CSS code, $\bar{X} = X^{\otimes 7}$ and $\bar{Z} = Z^{\otimes 7}$. Notice that the choice of physical representative $\bar{P}$ for a logical operator P is not unique; for any stabilizer S , the operator $\bar{P}S$ is an equivalent representative. Consequently, the definition of $\bar{F}$ is only fixed once a specific set of representatives is chosen. However, the following results are unaffected by this ambiguity, as they hold for any consistent choice of $\bar{P}$. Finally, we emphasize that the logical fidelity $\bar{F}$ is meaningful only when ρ is close to the code subspace $\mathcal{V}$, highlighting the necessity of the preceding subspace verification step.

For stabilizer codes, $\bar{P}$ should always be a tensor product of physical Pauli operators. Thus, measuring logical Pauli operators P can be replaced by measuring physical operators $\bar{P}$, which can still be done with local measurements. Following DFE, we construct an unbiased estimator Y such that $\mathbb{E}[Y] = \bar{F}$, and by Chebyshev’s inequality [17],

$$\Pr(Y \geq \mathbb{E}[Y] + \epsilon_2) \leq \delta_2. \quad (24)$$

Detailed illustrations are given in Appendix F.

We emphasize that the step of subspace verification is indispensable. For example, in the repetition code where $|\bar{0}\rangle = |000\rangle$ and $|\bar{1}\rangle = |111\rangle$, consider the physical operators $\bar{X} = XXX$, $\bar{Y} = YXX$, and $\bar{Z} = ZII$. The erroneous state $|001\rangle$ yields identical measurement outcomes for $\bar{X}$, $\bar{Y}$, and $\bar{Z}$ as the valid logical state $|\bar{0}\rangle$, despite being outside the code space. Therefore, without prior subspace verification step, logical DFE alone is unable to detect such errors.

The integration of the previous two steps can return an estimation of the target fidelity, and the following theorem shows the net sample complexity of SVAFE protocol for the fidelity estimation.

Theorem 2. Suppose one applies the SVAFE protocol to estimate the fidelity between the prepared state ρ with the target state $|\psi\rangle$ in the code subspace, namely $\text{Tr}(|\psi\rangle\langle\psi|\rho)$. Assume that in the initial step, the input states ρ pass the subspace verification using N_1 samples with verification operator Ω , i.e., $N_{\text{pass}} \geq p_0 N_1$, under parameters ϵ and δ . In the subsequent step, one obtains the estimator Y using N_2 samples under the same parameters. It can be concluded that the fidelity $\text{Tr}(|\psi\rangle\langle\psi|\rho) \geq Y - 2\epsilon$ with a confidence level of $1 - 2\delta$. The overall sample complexity is given by $N = N_1 + N_2 = O(\ln(1/\delta)/\Delta_{\min}(\Omega)\epsilon) + O((1/\epsilon^2\delta) + 2^k \ln(1/\delta)/\epsilon^2)$.

The proof is given in Appendix F. As shown in Sec. III, Ω can be constructed such that $\Delta_{\min}(\Omega) \geq 1/m$ for stabilizer codes with $m = n - k$. As a result, in most cases, the second term is the leading term. The sample complexity of our protocol is reduced by 2^m times compared to that of DFE, making it much more efficient than directly applying that method. For CSS codes and QLDPC stabilizer codes, $\Delta_{\min}(\Omega)$ could be a constant, which implies that the sample complexity is only related to the logical qubit number, independent of the physical qubit number.

In applications requiring precise preparation of states with small phases, such as phase estimation and calibration of single-qubit gates, fidelity estimation is crucial. Currently, there is no dedicated state verification protocol for these small phase states, and DFE becomes resource-intensive as the phase decreases. We have numerically demonstrated that our protocol significantly reduces the sample complexity required to estimate the fidelity of the logical state $|\psi(\theta)\rangle = \frac{1}{2}(|\bar{0}\rangle + e^{i\theta}|\bar{1}\rangle)^{\otimes 2}$, for toric codes with $n = 2d^2$ physical qubits, where the code distance d ranges from 2 to 7. This improvement is depicted in Fig. 3. In the first subspace verification step of our protocol, we only need to measure X operators and Z operators on all the qubits respectively based on the CSS code construction stated in Sec. III, followed by classical post-processing to bound the fidelity to the code subspace. In the second fidelity estimation step, we honestly execute the direct fidelity estimation on the logical space,

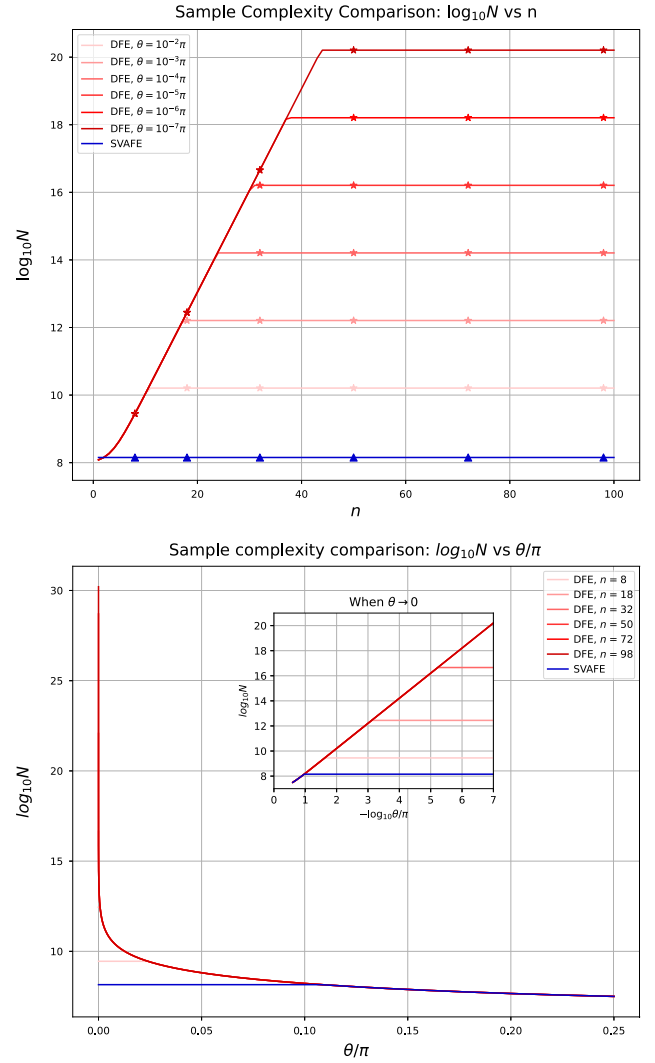


FIG. 3. Comparison of sample complexity: The task is to verify the code state $(\cos \theta/2 |\bar{0}\rangle + \sin \theta/2 |\bar{1}\rangle)^{\otimes 2}$ of the toric code with physical qubit number n . The parameters are given by $\delta = 10^{-2}$ and $\epsilon = 10^{-3}$. The red lines are sample complexities of directly applying DFE. The blue line is the sample complexity of our method: SVAFE. Since it is hard to see the difference in the sample complexities of our method between different n or θ , we only draw a single blue curve in the figures. These two figures are the relation between (a) $\log_{10} N$ and qubit number n and (b) $\log_{10} N$ and the angle θ [or $-\log_{10}(\theta/\pi)$ in the subfigure].

specifically, measure the logical Pauli operators $\bar{P}$ for $m_{\bar{P}} = 4d \log(4/\delta)/(\langle\psi(\theta)|\bar{P}|\psi(\theta)\rangle^2)$ times with probability $1/2^n \langle\psi(\theta)|\bar{P}|\psi(\theta)\rangle^2$ and repeat the procedure for $8/\epsilon^2\delta$ times. (The parameters should be $\epsilon/2$ and $\delta/2$ in each step based on Theorem 2.) Notably, the sample complexity of our protocol is nearly independent of both the angle θ and the number of physical qubits n . In contrast, the sample complexity of DFE escalates sharply as θ diminishes based on the protocol for “well-conditioned”

states [17,19]. This distinct advantage underscores the efficacy of our approach.

VI. CONCLUSION AND DISCUSSION

In this work, we expand the concept of quantum state verification by proposing a framework for quantum subspace verification. This framework can be used to address the challenge of the verification of logical states. Our theoretical analysis reveals that the spectral gaps of the verification operator play a critical role in determining the number of measurements required. We construct various verification operators for two widely used types of QEC codes: stabilizer codes and QLDPC codes. The verification process can be efficiently realized with $O(m \ln(1/\delta)/\epsilon)$ and $O(m^2 \ln(1/\delta)/\epsilon^2)$ local measurements for generic stabilizer codes and QLDPC codes, respectively. Remarkably, for specific codes such as CSS codes and QLDPC stabilizer codes, the number of required local measurements does not depend on m . These developments enable us to propose a composite protocol named SSAFE for fidelity estimation of stabilizer code states. This hybrid approach facilitates efficient fidelity estimation between ρ and any stabilizer code state $|\psi\rangle$.

We should note that our protocol differs fundamentally from logical randomized benchmarking [52]. While logical randomized benchmarking estimates the average fidelity over all logical states and improves efficiency by evaluating the decoded k -qubit state instead of the encoded n -qubit state, our method targets specific magic logical states and employs subspace verification to restrict the Hilbert space from 2^n to 2^k . Thus, both the objective and mechanism are entirely distinct.

Subsequent efforts may focus on extending our constructions of verification operators to encompass a broader array of QEC codes. A promising direction is to adapt our framework for continuous-variable quantum systems, specifically to verify QEC codes such as Gottesman-Kitaev-Preskill codes [53,54] within these systems. Additionally, exploring the integration of our subspace verification approach with approximate QEC codes [55,56] presents an intriguing possibility. These codes are pivotal in fault-tolerant quantum computing, benefiting from their capacity to support universal transversal gates. Furthermore, it remains crucial to determine whether almost all QEC subspaces that exhibit good performance can be efficiently verified using local measurements, as demonstrated for quantum state verification [44].

The current work mainly discusses the combination of quantum subspace verification and DFE. It is thus intriguing to explore the further application of quantum subspace verification on general quantum state and subspace learning problems [57–59]. While subspace verification is a powerful technique for reducing the effective Hilbert space

dimension, its trivial composition with other state learning protocols is insufficient. Since the primary advantage of subspace verification over full fault-tolerant error correction is its realizability through local measurements, any subsequent state learning protocol must also be realizable under the same constraint. For stabilizer codes, this condition requires that the protocol employ only Pauli measurements. Moreover, for those existing protocols that rely on specific subspace assumptions [60], subspace verification can be directly applied to efficiently verify these assumptions, thereby enhancing their robustness and making the protocols more assumption-independent.

To broaden the applicability of our framework, it is also crucial to extend it to adversarial scenarios, which would relax the i.i.d. assumption of the input states. Techniques employed in the framework of quantum state verification might be used to address the problem [25]. In addition, the extension to the quantum process is also interesting [61–63].

While finalizing our manuscript, we note that a contemporaneous work also introduces the concept of subspace verification [64]. Compared with theirs, our framework utilizes a more general hypothesis testing scheme better suited for noisy physical states, rather than merely extending the existing quantum state verification frameworks to include subspace. Additionally, our research focuses on a broader range of quantum error correction codes, including generic stabilizer and QLDPC codes, rather than specific codes. Furthermore, we introduce SSAFE that leverages quantum subspace verification for quantum state learning, illustrating a practical application of our theoretical advancements.

ACKNOWLEDGMENTS

We thank Zihao Li, Guoding Liu, Zhenhuan Liu, Yuxuan Yan, Huangjun Zhu, and Xingjian Zhang for their useful discussions. J.C. and X.M. acknowledge the support of the National Natural Science Foundation of China Grant No. 12174216 and Quantum Science and Technology-National Science and Technology Major Project Grants No. 2021ZD0300804 and No. 2021ZD0300702. Q.Z. acknowledges funding from Quantum Science and Technology-National Science and Technology Major Project No. 2024ZD0301900, National Natural Science Foundation of China (NSFC) via Projects No. 12347104 and No. 12305030, Guangdong Basic and Applied Basic Research Foundation via Project No. 2023A1515012185, Hong Kong Research Grant Council (RGC) via No. 27300823, N_HKU718/23, and R6010-23, Guangdong Provincial Quantum Science Strategic Initiative No. GDZX2303007. Y.Z. acknowledges the support from the Quantum Science and Technology-National Science and Technology Major Project Grants No. 2024ZD0301900 and No. 2021ZD0302000, the National

Natural Science Foundation of China (NSFC) Grants No. 12205048 and No. 12575012, the Shanghai Municipal Commission of Science and Technology with Grant No. 25511103200, the Shanghai Science and Technology Innovation Action Plan Grant No. 24LZ1400200, Shanghai Pilot Program for Basic Research—Fudan University 21TQ1400100 (25TQ003), the CCF-Quantum CTeK Superconducting Quantum Computing Special Project Research Activities CCF-QC2025006.

DATA AVAILABILITY

No data were created or analyzed in this study.

APPENDIX A: PROOF OF THEOREM 1

First, the following lemma gives the range of the passing probability $\text{Tr}(\Omega\rho)$ of a single test.

Lemma A1. The passing probability of ρ of a single test satisfies

$$1 - \Delta_{\max}(\Omega)\epsilon_\rho \leq \text{Tr}(\Omega\rho) \leq 1 - \Delta_{\min}(\Omega)\epsilon_\rho, \quad (\text{A1})$$

where $\epsilon_\rho := 1 - F(\mathcal{P}, \rho)$ is the infidelity of ρ to subspace $\mathcal{V}$.

Proof. For simplicity, we only prove the upper bound. The lower bound can be proved in the same way. By definition and the decomposition in Eq. (3),

$$\begin{aligned} \text{Tr}(\Omega\rho) &= \text{Tr}(\mathcal{P}\rho) + \text{Tr}\left(\sum_{j=d_{\mathcal{V}}+1}^d \lambda_j |\phi_j\rangle\langle\phi_j|\right) \\ &\leq 1 - \epsilon_\rho + \lambda_{d_{\mathcal{V}}+1} \sum_{j=d_{\mathcal{V}}+1}^d \text{Tr}(|\phi_j\rangle\langle\phi_j|\rho) \\ &= 1 - \epsilon_\rho + \lambda_{d_{\mathcal{V}}+1}\epsilon_\rho = 1 - \Delta_{\min}(\Omega)\epsilon_\rho. \end{aligned} \quad (\text{A2})$$

Here we use the fact that $\sum_{j=d_{\mathcal{V}}+1}^d |\phi_j\rangle\langle\phi_j| = \mathbb{I} - \mathcal{P}$ is the projector on $\mathcal{V}^\perp$. Note that the inequality can be saturated as all the nonzero $\text{Tr}(|\phi_j\rangle\langle\phi_j|\rho)$ corresponds to eigenvalues equaling to $\lambda_{d_{\mathcal{V}}+1}$. ■

Based on the former lemma, the expected total number of passed tests satisfies

$$\mathbb{E}[N_{\text{pass}}] \in [(1 - \Delta_{\max}(\Omega)\epsilon_\rho)N, (1 - \Delta_{\min}(\Omega)\epsilon_\rho)N]. \quad (\text{A3})$$

If the device is “good,” there should be $\epsilon_\rho \leq \tau\epsilon$. By adopting the Chernoff-Hoeffding theorem, we can derive

$$\begin{aligned} \Pr(N_{\text{pass}} \leq p_0 N) &= \Pr\left(\frac{N_{\text{pass}}}{N} \leq \frac{\mathbb{E}[N_{\text{pass}}]}{N} - \frac{\mathbb{E}[N_{\text{pass}}] - p_0 N}{N}\right) \\ &\leq e^{-D[p_0 \| \frac{\mathbb{E}[N_{\text{pass}}]}{N}]} N \\ &\leq e^{-D[p_0 \| 1 - \tilde{\epsilon}/r]N} = \delta. \end{aligned} \quad (\text{A4})$$

The third line is based on

$$\frac{\mathbb{E}[N_{\text{pass}}]}{N} \geq 1 - \Delta_{\max}(\Omega)\epsilon_\rho \geq 1 - \tilde{\epsilon}/r \geq p_0. \quad (\text{A5})$$

Since p_0 is the solution to the equation $D[p_0 \| 1 - \tilde{\epsilon}/r] = D[p_0 \| 1 - \tilde{\epsilon}]$, it should be between $1 - \tilde{\epsilon}$ and $1 - \tilde{\epsilon}/r$. The final inequality in Eq. (A5) comes from $1 - \tilde{\epsilon} \leq p_0 \leq 1 - \tilde{\epsilon}/r$ when $r > 1$.

If the device is “bad,” there should be $\epsilon_\rho \geq \epsilon$. We can similarly derive

$$\begin{aligned} \Pr(N_{\text{pass}} \geq p_0 N) &= \Pr\left(\frac{N_{\text{pass}}}{N} \geq \frac{\mathbb{E}[N_{\text{pass}}]}{N} + \frac{p_0 N - \mathbb{E}[N_{\text{pass}}]}{N}\right) \\ &\leq e^{-D[p_0 \| \frac{\mathbb{E}[N_{\text{pass}}]}{N}]} N \\ &\leq e^{-D[p_0 \| 1 - \tilde{\epsilon}]N} = \delta. \end{aligned} \quad (\text{A6})$$

The third line is based on

$$\frac{\mathbb{E}[N_{\text{pass}}]}{N} \leq 1 - \Delta_{\min}(\Omega)\epsilon_\rho \leq 1 - \tilde{\epsilon} \leq p_0. \quad (\text{A7})$$

APPENDIX B: PROOF OF PROPOSITION 1

First, we can give an interval estimator of the passing probability $\mathbb{E}[N_{\text{pass}}]/N$ based on the simplified confidence interval of the Bernoulli model,

$$p - \xi \leq \frac{\mathbb{E}[N_{\text{pass}}]}{N} \leq p + \xi, \quad (\text{B1})$$

with approximate confidence level $1 - \delta$.

From Lemma A1, $\mathbb{E}[N_{\text{pass}}]/N = \text{Tr}(\Omega\rho) \in [1 - \Delta_{\max}(\Omega)\epsilon_\rho, 1 - \Delta_{\min}(\Omega)\epsilon_\rho]$. By combining these two conditions, with approximate confidence level $1 - \delta$ we need $1 - \Delta_{\max}(\Omega)\epsilon_\rho \leq p + \xi$ and $1 - \Delta_{\min}(\Omega)\epsilon_\rho \geq p - \xi$, from which we can solve that

$$\frac{1 - p - \xi}{\Delta_{\max}(\Omega)} \leq \epsilon_\rho \leq \frac{1 - p + \xi}{\Delta_{\min}(\Omega)}. \quad (\text{B2})$$

By combining it with $0 \leq \epsilon_\rho \leq 1$, we can derive the proposition.

APPENDIX C: SPECTRAL GAPS OF VERIFICATION OPERATORS OF STABILIZER CODES

We can write $\Omega_{\text{all}} = (\mathbb{I} + \mathcal{P})/2 = \mathcal{P} + \frac{1}{2}\mathcal{P}^\perp$, where $\mathcal{P}^\perp$ represents the projector onto the subspace orthogonal to $\mathcal{V}$. This expression is just a diagonalization of Ω_{all} , showing that the second largest and smallest eigenvalues are both $\frac{1}{2}$. Thus, the spectral gaps are $\Delta_{\min}(\Omega_{\text{all}}) = \Delta_{\max}(\Omega_{\text{all}}) = \frac{1}{2}$.

For Ω_{gen} , consider the subspace $\mathcal{V}_{\vec{r}}$ with projector

$$\mathcal{P}_{\vec{r}} = \prod_{i=1}^m \frac{\mathbb{I} + (-1)^{\vec{r}(i)} S_i}{2} \quad (\text{C1})$$

characterized by a binary vector $\vec{r} = (\dots, \vec{r}(i), \dots)$ of dimension m . It is clear that the code subspace $\mathcal{V}$ corresponds to $\vec{r} = \vec{0}$. One can verify their orthogonality by

$$\mathcal{P}_{\vec{r}} \mathcal{P}_{\vec{r}'} = \delta(\vec{r}, \vec{r}') \mathcal{P}_{\vec{r}}, \quad (\text{C2})$$

where $\delta(a, b) = 1$ if $a = b$ and $\delta(a, b) = 0$ otherwise. Since $S_i \mathcal{P}_{\vec{r}} = (-1)^{\vec{r}(i)} \mathcal{P}_{\vec{r}}$, we can derive

$$\Omega_{\text{gen}} \mathcal{P}_{\vec{r}} = \frac{1}{m} \sum_{i=1}^m \frac{\mathbb{I} + S_i}{2} \mathcal{P}_{\vec{r}} = \left(1 - \frac{1}{m} \sum_{i=1}^m \vec{r}(i) \right) \mathcal{P}_{\vec{r}}. \quad (\text{C3})$$

Here, the calculation of $\sum_{i=1}^m \vec{r}(i)$ is performed on the field of $\mathbb{R}$ rather than $\mathbb{Z}_2$.

For different $\vec{r}$, the eigenstates in subspace $\mathcal{P}_{\vec{r}}$ are always eigenstates of $\Omega_{\text{chr}}(\mathcal{S})$ with eigenvalues $1 - (1/m) \sum_{i=1}^m \vec{r}(i)$. There are 2^m different $\vec{r}$, corresponding to 2^m orthogonal subspace $\mathcal{V}_{\vec{r}}$ of the whole Hilbert space. Each of them has dimension 2^k . Therefore, $1 - (1/m) \sum_{i=1}^m \vec{r}(i)$ are all the possible eigenvalues. The largest eigenvalue is 1, corresponding to $\vec{r} = \vec{0}$ with degeneracy 2^k . The second largest and smallest eigenvalues are $1 - (1/m)$ and 0. The spectral gaps are $\Delta_{\min}(\Omega_{\text{gen}}) = 1/m$ and $\Delta_{\max}(\Omega_{\text{gen}}) = 1$.

For $\Omega_{\text{chr}}(\mathcal{S})$ in Eq. (14), we still consider the subspace $\mathcal{V}_{\vec{r}}$ with projector $\mathcal{P}_{\vec{r}}$

$$\begin{aligned} \mathcal{P}_{\vec{r}} &= \prod_{i=1}^m \frac{\mathbb{I} + (-1)^{\vec{r}(i)} S_i}{2} \\ &= \prod_{u=1}^{\chi(G_S)} \prod_{v_i \in \mathcal{I}_u} \frac{\mathbb{I} + (-1)^{\vec{r}(i)} S_i}{2} = \prod_{u=1}^{\chi(G_S)} \mathcal{P}_{\mathcal{I}_u, \vec{r}_u}, \end{aligned} \quad (\text{C4})$$

where $\mathcal{P}_{\mathcal{I}_u, \vec{r}_u}$ is defined as

$$\mathcal{P}_{\mathcal{I}_u, \vec{r}_u} = \prod_{v_i \in \mathcal{I}_u} \frac{\mathbb{I} + (-1)^{r_u(i)} S_i}{2} \quad (\text{C5})$$

depending on the restricted vector on the index of $\mathcal{I}_u$, i.e., $\vec{r}_u = \sum_{v_i \in \mathcal{I}_u} r(i) \vec{e}_i$ with $\sum_{u=1}^{\chi(G_S)} \vec{r}_u = \vec{r}$. Then, one has

$$\mathcal{P}_{\mathcal{I}_u, \vec{r}_u} \cdot \mathcal{P}_{\mathcal{I}_u} = \delta(\vec{r}_u, \vec{0}) \mathcal{P}_{\mathcal{I}_u}, \quad (\text{C6})$$

where $\mathcal{P}_{\mathcal{I}_u}$ is defined in Eq. (13) for the all-zero vector. As a result,

$$\begin{aligned} \Omega_{\text{chr}}(\mathcal{S}) \mathcal{P}_{\vec{r}} &= \frac{1}{\chi(G_S)} \sum_{u=1}^{\chi(G_S)} \mathcal{P}_{\mathcal{I}_u} \mathcal{P}_{\vec{r}} \\ &= \frac{1}{\chi(G_S)} \sum_{u=1}^{\chi(G_S)} \delta(\vec{r}_u, \vec{0}) \mathcal{P}_{\vec{r}}. \end{aligned} \quad (\text{C7})$$

For different $\vec{r}$, the eigenstates in subspace $\mathcal{P}_{\vec{r}}$ are always eigenstates of $\Omega_{\text{chr}}(\mathcal{S})$ and their eigenvalue are

$$\lambda_{\vec{r}} = \frac{\sum_{u=1}^{\chi(G_S)} \delta(\vec{r}_u, \vec{0})}{\chi(G_S)}. \quad (\text{C8})$$

There are 2^m different $\vec{r}$, corresponding to 2^m orthogonal subspace $\mathcal{V}_{\vec{r}}$ of the whole Hilbert space. Each of them has dimension 2^k . Therefore, $\lambda_{\vec{r}}$ are all the eigenvalues of $\Omega_{\text{chr}}(\mathcal{S})$. Only when all the $\vec{r}_u = \vec{0}$, i.e., $\vec{r} = \vec{0}$ and $\mathcal{V}_{\vec{r}}$ is the code subspace, we have $\lambda_{\vec{r}} = 1$. The second largest and smallest eigenvalues are $1 - (1/\chi(G_S))$ and 0. The spectral gaps are $\Delta_{\min}(\Omega_{\text{chr}}(\mathcal{S})) = 1/\chi(G_S)$ and $\Delta_{\max}(\Omega_{\text{chr}}(\mathcal{S})) = 1$.

APPENDIX D: SPECTRAL GAPS OF VERIFICATION OPERATORS OF QLDPC CODES

By replacing S_i with T_i in the analysis of Ω_{gen} and $\Omega_{\text{chr}}(\mathcal{S})$ in Appendix C, one can similarly derive the spectral gaps of $\Omega_{\text{gen}}^{(s)}$ and $\Omega_{\text{chr}}^{(s)}$.

For $\Omega_{\text{gen}}^{(1)}$ given in Eq. (18), we can rewrite it as

$$\begin{aligned} \Omega_{\text{gen}}^{(1)} &= \frac{1}{m} \sum_i \left(\frac{1}{a_i} \pi_i + \left(1 - \frac{1}{a_i} \right) \frac{\mathbb{I}}{2} \right) \\ &= \frac{1}{2m} \sum_i \left(\mathbb{I} + \frac{1}{a_i} T_i \right). \end{aligned} \quad (\text{D1})$$

With a similar construction of $\mathcal{P}_{\vec{r}}$ as that in Appendix C, we can derive its eigenvalues

$$\lambda_{\vec{r}} = \frac{1}{2m} \sum_{i=1}^m \left(1 + \frac{(-1)^{\vec{r}(i)}}{a_i} \right) = \frac{1}{2} + \frac{1}{2m} \sum_{i=1}^m \frac{(-1)^{\vec{r}(i)}}{a_i}. \quad (\text{D2})$$

Since $a_i > 0$ for all i , the largest eigenvalue should be $\frac{1}{2} + (1/2m) \sum_{i=1}^m 1/a_i$, the second largest eigenvalue should be $\frac{1}{2} + (1/2m) (\sum_{i=1}^m (1/a_i) - (2/\max_i a_i))$, and

the smallest eigenvalue should be $\frac{1}{2} - (1/2m) \sum_{i=1}^m (1/a_i)$. Thus, the spectral gaps are $\Delta_{\min}(\Omega_{\text{gen}}^{(1)}) = 1/m \cdot \max_i a_i$ and $\Delta_{\max}(\Omega_{\text{gen}}^{(1)}) = 1/m \sum_{i=1}^m 1/a_i$.

Furthermore, we can construct

$$\begin{aligned}\Omega_{\text{chr}}^{(1)} &= \frac{1}{\chi(G_{\Pi})} \sum_{u=1}^{\chi(G_{\Pi})} \prod_{v_i \in \mathcal{I}_u} \left(\frac{1}{a_i} \pi_i + \left(1 - \frac{1}{a_i}\right) \frac{\mathbb{I}}{2} \right) \\ &= \frac{1}{\chi(G_{\Pi})} \sum_{u=1}^{\chi(G_{\Pi})} \prod_{v_i \in \mathcal{I}_u} \sum_{P_{ij} \in \mathcal{I}_i} p_{ij} \frac{\mathbb{I} + P_{ij}}{2},\end{aligned}\quad (\text{D3})$$

as we did in the construction of $\Omega_{\text{chr}}(\mathcal{S})$ for stabilizer codes. However, with a similar analysis, we can find that the maximum eigenvalue

$$\lambda(\Omega_{\text{chr}}^{(1)}) = \frac{1}{\chi(G_{\Pi})} \sum_{u=1}^{\chi(G_{\Pi})} \prod_{v_i \in \mathcal{I}_u} \frac{1}{2} \left(1 + \frac{1}{a_i}\right) \quad (\text{D4})$$

and the spectral gaps

$$\Delta_{\min}(\Omega_{\text{chr}}^{(1)}) = \frac{1}{\chi(G_{\Pi})} \min_{i_0} \left(\frac{1}{a_{i_0}} \prod_{\substack{i: \\ v_i \in \mathcal{I}_u, i \neq i_0}} \frac{1}{2} \left(1 + \frac{1}{a_i}\right) \right), \quad (\text{D5})$$

$$\begin{aligned}\Delta_{\max}(\Omega_{\text{chr}}^{(1)}) &= \frac{1}{\chi(G_{\Pi})} \sum_{u=1}^{\chi(G_{\Pi})} \left(\prod_{v_i \in \mathcal{I}_u} \frac{1}{2} \left(1 + \frac{1}{a_i}\right) \right. \\ &\quad \left. - \prod_{v_i \in \mathcal{I}_u} \frac{1}{2} \left(1 - \frac{1}{a_i}\right) \right). \end{aligned} \quad (\text{D6})$$

Roughly speaking, as long as $a_i > 1$ for most of i , $\lambda(\Omega_{\text{chr}}^{(1)})$, $\Delta_{\min}(\Omega_{\text{chr}}^{(1)})$, and $\Delta_{\max}(\Omega_{\text{chr}}^{(1)})$ go exponentially small with m . In general, since $\Delta_{\min}(\Omega_{\text{chr}}^{(1)}) \leq 1/\chi(G_{\Pi}) \min_u \prod_{v_i \in \mathcal{I}_u} \frac{1}{2} (1 + (1/a_i)) \leq (1/\chi(G_{\Pi})) \lambda(\Omega_{\text{chr}}^{(1)})$,

$$\begin{aligned}N &\sim \frac{8\lambda(\Omega_{\text{chr}}^{(1)})(1 - \lambda(\Omega_{\text{chr}}^{(1)})) \ln 1/\delta}{(\Delta_{\min}(\Omega_{\text{chr}}^{(1)}) - \Delta_{\max}(\Omega_{\text{chr}}^{(1)})\tau)^2 \epsilon^2} \\ &\geq \frac{8\lambda(\Omega_{\text{chr}}^{(1)})}{(\Delta_{\min}(\Omega_{\text{chr}}^{(1)}))^2} \cdot \frac{(1 - \lambda(\Omega_{\text{chr}}^{(1)})) \ln 1/\delta}{\epsilon^2} \\ &\geq \frac{8\chi(G_{\Pi})}{\Delta_{\min}(\Omega_{\text{chr}}^{(1)})} \cdot \frac{(1 - \lambda(\Omega_{\text{chr}}^{(1)})) \ln 1/\delta}{\epsilon^2}.\end{aligned}\quad (\text{D7})$$

Therefore, N will scale exponentially with m as long as $\Delta_{\min}(\Omega_{\text{chr}}^{(1)})$ goes exponentially small with m and $\lambda(\Omega_{\text{chr}}^{(1)})$ is not negligible, which indicates that the construction of $\Omega_{\text{chr}}^{(1)}$ is usually useless.

APPENDIX E: PROOF OF PROPOSITION 2

First, one can obtain the passing probability

$$\lambda - \Delta_{\max}(\Omega)\epsilon_{\rho} \leq \text{Tr}(\Omega\rho) \leq \lambda - \Delta_{\min}(\Omega)\epsilon_{\rho} \quad (\text{E1})$$

as we have done in Lemma A1. Consequently, the expected passing number shows

$$\mathbb{E}[N_{\text{pass}}] \in [(\lambda - \Delta_{\max}(\Omega)\epsilon_{\rho})N, (\lambda - \Delta_{\min}(\Omega)\epsilon_{\rho})N]. \quad (\text{E2})$$

Let p'_0 be the solution to the equation $e^{-D[p'_0\|\lambda - \tau\Delta_{\max}(\Omega)]N} = e^{-D[p'_0\|\lambda - \Delta_{\min}(\Omega)]N}$. One can solve it to obtain

$$p'_0 = \frac{\ln \frac{1 - \lambda + \Delta_{\max}(\Omega)\tau\epsilon}{1 - \lambda + \Delta_{\min}(\Omega)\epsilon}}{\ln \frac{1 - \lambda + \Delta_{\max}(\Omega)\tau\epsilon}{1 - \lambda + \Delta_{\min}(\Omega)\epsilon} + \ln \frac{\lambda - \Delta_{\min}(\Omega)\epsilon}{\lambda - \Delta_{\max}(\Omega)\tau\epsilon}}. \quad (\text{E3})$$

If the device is “good,” there should be $\epsilon_{\rho} \leq \tau\epsilon$. By adopting the Chernoff-Hoeffding theorem, we can derive

$$\Pr(N_{\text{pass}} \leq p'_0 N) \leq e^{-D[p'_0\|\lambda - \tau\Delta_{\max}(\Omega)\epsilon]N} \quad (\text{E4})$$

based on

$$\frac{\mathbb{E}[N_{\text{pass}}]}{N} \geq \lambda - \Delta_{\max}(\Omega)\epsilon_{\rho} \geq \lambda - \tau\Delta_{\max}(\Omega)\epsilon \geq p'_0. \quad (\text{E5})$$

One can check the final inequality in Eq. (E5) given p'_0 in Eq. (E3) when $r > 1$.

If the device is “bad,” there should be $\epsilon_{\rho} \geq \epsilon$. We can similarly derive

$$\Pr(N_{\text{pass}} \geq p'_0 N) \leq e^{-D[p'_0\|\lambda - \Delta_{\min}(\Omega)\epsilon]N} \quad (\text{E6})$$

based on

$$\frac{\mathbb{E}[N_{\text{pass}}]}{N} \leq \lambda - \Delta_{\min}(\Omega)\epsilon_{\rho} \leq \lambda - \Delta_{\min}(\Omega)\epsilon \leq p'_0. \quad (\text{E7})$$

The final inequality can also be derived with p'_0 in Eq. (E3) when $r > 1$.

Finally, the definition of δ gives $\delta = e^{-D[p'_0\|\lambda - \tau\Delta_{\max}(\Omega)]N} = e^{-D[p'_0\|\lambda - \Delta_{\min}(\Omega)]N}$. Therefore,

$$N = \frac{\ln 1/\delta}{D[p'_0\|\lambda - \Delta_{\min}(\Omega)\epsilon]}. \quad (\text{E8})$$

When ϵ is sufficiently small, we can simplify it to the second order in ϵ ,

$$N \sim \frac{8\lambda(1 - \lambda) \ln 1/\delta}{(\Delta_{\min}(\Omega) - \Delta_{\max}(\Omega)\tau)^2 \epsilon^2}. \quad (\text{E9})$$

APPENDIX F: DETAILS OF DFE AND PROOF OF THEOREM 2

To construct an unbiased estimator Y for $1/2^k \sum_{\bar{P}} \text{Tr}(\bar{P}|\psi\rangle\langle\psi|) \cdot \text{Tr}(\bar{P}\rho)$, we start by establishing that the quantity $p(\bar{P}) := 1/2^k (\text{Tr}(\bar{P}|\psi\rangle\langle\psi|))^2$ satisfies the condition $\sum_{\bar{P}} p(\bar{P}) = 1$. Consequently, $p(\bar{P})$ can be treated as a probability distribution. Also, define $l := 8/\epsilon_2^2 \delta_2$. The first step is to sample l logical Pauli operators $\{\bar{P}_i\}_{i=1}^l$ according to the probability distribution $p(\bar{P})$. For each sampled Pauli operator $\bar{P}_i$, define $m_i := \delta_2 \log(4/\delta_2)/2^k p(\bar{P})$. We then measure the corresponding operator $\bar{P}_i$ on the input states m_i times, obtaining measurement outcomes, denoted as A_{ij} . The estimator Y is a postprocessing on the measurement outcomes,

$$Y = \frac{1}{l} \sum_i \left(\frac{1}{\text{Tr}(\bar{P}_i|\psi\rangle\langle\psi|)} \cdot \frac{1}{2^{k/2} m_i} \sum_j A_{ij} \right). \quad (\text{F1})$$

Note that $\mathbb{E}_{j,A_{ij}} = 2^{k/2} \text{Tr}(\bar{P}_i \rho)$. One can check that Y is unbiased since

$$\begin{aligned} \mathbb{E}_{i,j}[Y] &= \sum_{\bar{P}} p(\bar{P}) \left(\frac{1}{\text{Tr}(\bar{P}|\psi\rangle\langle\psi|)} \cdot \frac{1}{2^{k/2} m_i} \cdot m_i \cdot 2^{k/2} \text{Tr}(\bar{P} \rho) \right) \\ &= \frac{1}{2^k} \sum_{\bar{P}} \text{Tr}(\bar{P}|\psi\rangle\langle\psi|) \cdot \text{Tr}(\bar{P} \rho). \end{aligned} \quad (\text{F2})$$

Since $(\mathbb{I} - \mathcal{P}_V)\rho(\mathbb{I} - \mathcal{P}_V) = \mathcal{P}_{V^\perp}\rho\mathcal{P}_{V^\perp}$ is non-negative, it could be composed to $(\mathbb{I} - \mathcal{P}_V)\rho(\mathbb{I} - \mathcal{P}_V) = \sum_j \lambda_j |\phi_j\rangle\langle\phi_j|$ with $\sum_j \lambda_j = 1 - \text{Tr}(\mathcal{P}_V \rho)$. Thus, if $\text{Tr}(\mathcal{P}_V \rho) \geq 1 - \epsilon_1$,

$$\begin{aligned} &\left| \text{Tr}(|\psi\rangle\langle\psi|\rho) - \frac{1}{2^k} \sum_{\bar{P}} \text{Tr}(\bar{P}|\psi\rangle\langle\psi|) \cdot \text{Tr}(\bar{P} \rho) \right| \\ &= \left| \frac{1}{2^k} \text{Tr} \left(\sum_{\bar{P}} \text{Tr}(\bar{P}|\psi\rangle\langle\psi|) \bar{P} \cdot (\mathbb{I} - \mathcal{P}_V) \rho (\mathbb{I} - \mathcal{P}_V) \right) \right| \\ &= \left| \frac{1}{2^k} \sum_{\bar{P}} \text{Tr}(\bar{P}|\psi\rangle\langle\psi|) \text{Tr} \left(\bar{P} \sum_j \lambda_j |\phi_j\rangle\langle\phi_j| \right) \right| \\ &\leq \frac{1}{2^k} \sum_j \lambda_j \left| \sum_{\bar{P}} \text{Tr}(\bar{P}|\psi\rangle\langle\psi|) \text{Tr}(\bar{P}|\phi_j\rangle\langle\phi_j|) \right| \\ &\leq \frac{1}{2^k} \sum_j \lambda_j \left(\sum_{\bar{P}} (\text{Tr}(\bar{P}|\psi\rangle\langle\psi|))^2 \cdot \sum_{\bar{P}} (\text{Tr}(\bar{P}|\phi_j\rangle\langle\phi_j|))^2 \right)^{1/2} \\ &\leq \frac{1}{2^k} \epsilon_1 \cdot (2^k \cdot 2^k)^{1/2} = \epsilon_1. \end{aligned} \quad (\text{F3})$$

The second line is based on the decomposition

$$|\psi\rangle\langle\psi| = \mathcal{P}_V \frac{1}{2^k} \cdot \sum_{\bar{P}} \text{Tr}(\bar{P}|\psi\rangle\langle\psi|) \bar{P}, \quad (\text{F4})$$

and the fact that $(\mathbb{I} - \mathcal{P}_V)^2 = \mathbb{I} - \mathcal{P}_V$. The fifth line is directly applying Cauchy-Schwarz inequality. The final line can be derived from the following fact.

Fact F1. Suppose $\bar{P}$ are logical Pauli operators of an $[[n, k, d]]$ QEC code, it can be transformed to Pauli operators of the first k qubits with a decoding unitary U . To be specific, there exists a unitary U such that $U\bar{P}U^\dagger = P_k \otimes \mathbb{I}_{n-k}$ where P_k is a k -qubit Pauli operator. Therefore, for any n -qubit pure state $|\phi\rangle$,

$$\begin{aligned} \sum_{\bar{P}} (\text{Tr}(\bar{P}|\phi\rangle\langle\phi|))^2 &= \sum_{\bar{P}} (\text{Tr}(U\bar{P}U^\dagger U|\phi\rangle\langle\phi|U^\dagger))^2 \\ &= \sum_{P_k} (\text{Tr}(P_k \otimes \mathbb{I} \cdot U|\phi\rangle\langle\phi|U^\dagger))^2 \\ &= \sum_{P_k} (\text{Tr}(P_k \rho_k))^2 \\ &= 2^k \text{Tr}(\rho_k^2) \leq 2^k, \end{aligned} \quad (\text{F5})$$

where $\rho_k = \text{Tr}_{n-k}(U|\phi\rangle\langle\phi|U^\dagger)$.

For simplicity, we denote $N_{\text{pass}} \geq p_0 N$ as event A , $\text{Tr}(\mathcal{P}_V \rho) \leq 1 - \epsilon_1$ as event B , $1/2^k \sum_{\bar{P}} \text{Tr}(\bar{P}|\psi\rangle\langle\psi|) \cdot \text{Tr}(\bar{P} \rho) \leq Y - \epsilon_2$ as event C , and $\text{Tr}(|\psi\rangle\langle\psi|\rho) \leq Y - \epsilon_1 - \epsilon_2$ as event D . Equation (F3) shows that if both B and C are false, D should also be false, which implies $\Pr(D) \leq \Pr(B \vee C)$. Therefore, we can conclude that $\Pr(A \wedge D) \leq \Pr(A \wedge (B \vee C)) \leq \Pr(A \wedge B) + \Pr(A \wedge C) \leq \Pr(A|B) + \Pr(C) \leq \delta_1 + \delta_2$, i.e.,

$$\Pr(N_{\text{pass}} \geq p_0 N, \text{Tr}(|\psi\rangle\langle\psi|\rho) \leq Y - \epsilon_1 - \epsilon_2) \leq \delta_1 + \delta_2. \quad (\text{F6})$$

Suppose $\delta_1 = \delta_2 = \delta$ and $\epsilon_1 = \epsilon_2 = \epsilon$. Equation (F6) shows that if the quantum states ρ pass the subspace verification, we can conclude that $\text{Tr}(|\psi\rangle\langle\psi|\rho) \leq Y - 2\epsilon$ with confidence $1 - 2\delta$. The sample complexity $N = N_1 + N_2 = O(\ln(1/\delta)/\Delta_{\min}(\Omega)\epsilon) + O((1/\epsilon^2\delta) + 2^k \ln(1/\delta)/\epsilon^2)$.

-
- [1] R. P. Feynman, Simulating physics with computers, *Int. J. Theor. Phys.* **21**, 467 (1982).
 - [2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).

- [3] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
- [4] Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, *et al.*, Strong quantum computational advantage using a superconducting quantum processor, *Phys. Rev. Lett.* **127**, 180501 (2021).
- [5] R. Acharya, L. Aghababaie-Beni, I. Aleiner, T. I. Andersen, M. Ansmann, F. Arute, K. Arya, A. Asfaw, N. Astrakhantsev, J. Atalaya, *et al.*, Quantum error correction below the surface code threshold, *Nature* **638**, 920 (2025).
- [6] P. W. Shor, Fault-tolerant quantum computation, [arXiv:quant-ph/9605011](https://arxiv.org/abs/quant-ph/9605011).
- [7] D. Gottesman, Fault-tolerant quantum computation with constant overhead, [arXiv:1310.2984](https://arxiv.org/abs/1310.2984).
- [8] A. Kitaev, Fault-tolerant quantum computation by anyons, *Ann. Phys. (N.Y.)* **303**, 2 (2003).
- [9] S. B. Bravyi and A. Y. Kitaev, Quantum codes on a lattice with boundary, [arXiv:quant-ph/9811052](https://arxiv.org/abs/quant-ph/9811052).
- [10] Y. Zhao, Y. Ye, He L. Huang, Y. Zhang, D. Wu, H. Guan, Q. Zhu, Z. Wei, T. He, S. Cao, *et al.*, Realization of an error-correcting surface code with superconducting qubits, *Phys. Rev. Lett.* **129**, 030501 (2022).
- [11] P. Panteleev and G. Kalachev, in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2022* (Association for Computing Machinery, New York, NY, 2022), p. 375.
- [12] Q. Xu, J. P. Bonilla Ataides, C. A. Pattison, N. Raveendran, D. Bluvstein, J. Wurtz, B. Vasić, M. D. Lukin, L. Jiang, and H. Zhou, Constant-overhead fault-tolerant quantum computation with reconfigurable atom arrays, *Nat. Phys.* **20**, 1084 (2024).
- [13] Michael J. Gullans, S. Krastanov, David A. Huse, L. Jiang, and Steven T. Flammia, Quantum coding with low-depth random circuits, *Phys. Rev. X* **11**, 031066 (2021).
- [14] M. Cramer, M. B. Plenio, S. T. Flammia, R. Somma, D. Gross, S. D. Bartlett, O. Landon-Cardinal, D. Poulin, and Y.-K. Liu, Efficient quantum state tomography, *Nat. Commun.* **1**, 149 (2010).
- [15] D. Gross, Yi K. Liu, Steven T. Flammia, S. Becker, and J. Eisert, Quantum state tomography via compressed sensing, *Phys. Rev. Lett.* **105**, 150401 (2010).
- [16] A. I. Lvovsky and M. G. Raymer, Continuous-variable optical quantum-state tomography, *Rev. Mod. Phys.* **81**, 299 (2009).
- [17] Steven T. Flammia and Yi K. Liu, Direct fidelity estimation from few Pauli measurements, *Phys. Rev. Lett.* **106**, 230501 (2011).
- [18] A. Seshadri, M. Ringbauer, J. Spainhour, R. Blatt, T. Monz, and S. Becker, Versatile fidelity estimation with confidence, *Phys. Rev. Lett.* **133**, 020402 (2024).
- [19] M. Kliesch and I. Roth, Theory of quantum system certification, *PRX Quantum* **2**, 010201 (2021).
- [20] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nat. Phys.* **16**, 1050 (2020).
- [21] S. Chen, W. Yu, P. Zeng, and Steven T. Flammia, Robust shadow estimation, *PRX Quantum* **2**, 030348 (2021).
- [22] Y. Zhou and Z. Liu, A hybrid framework for estimating nonlinear functions of quantum states, *npj Quantum Inf.* **10**, 62 (2024).
- [23] S. Pallister, N. Linden, and A. Montanaro, Optimal verification of entangled states with local measurements, *Phys. Rev. Lett.* **120**, 170502 (2018).
- [24] M. Hayashi, K. Matsumoto, and Y. Tsuda, A study of LOCC-detection of a maximally entangled state using hypothesis testing, *J. Phys. A: Math. Gen.* **39**, 14427 (2006).
- [25] H. Zhu and M. Hayashi, Efficient verification of pure quantum states in the adversarial scenario, *Phys. Rev. Lett.* **123**, 260504 (2019).
- [26] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario, *Phys. Rev. A* **100**, 062335 (2019).
- [27] X.-D. Yu, J. Shang, and O. Gühne, Optimal verification of general bipartite pure states, *npj Quantum Inf.* **5**, 1 (2019).
- [28] Ye C. Liu, Xiao D. Yu, J. Shang, H. Zhu, and X. Zhang, Efficient verification of Dicke states, *Phys. Rev. Appl.* **12**, 044020 (2019).
- [29] Ye C. Liu, J. Shang, R. Han, and X. Zhang, Universally optimal verification of entangled states with nondemolition measurements, *Phys. Rev. Lett.* **126**, 090504 (2021).
- [30] H. Zhu, Y. Li, and T. Chen, Efficient verification of ground states of frustration-free Hamiltonians, *Quantum* **8**, 1221 (2024).
- [31] T. Chen, Y. Li, and H. Zhu, Efficient verification of Affleck-Kennedy-Lieb-Tasaki states, *Phys. Rev. A* **107**, 022616 (2023).
- [32] K. Fujii and M. Hayashi, Verifiable fault tolerance in measurement-based quantum computation, *Phys. Rev. A* **96**, 030301(R) (2017).
- [33] D. Gottesman, Stabilizer codes and quantum error correction, [arXiv:quant-ph/9705052](https://arxiv.org/abs/quant-ph/9705052).
- [34] N. Dangniam, Yun G. Han, and H. Zhu, Optimal verification of stabilizer states, *Phys. Rev. Res.* **2**, 043323 (2020).
- [35] S. Bravyi and A. Kitaev, Universal quantum computation with ideal Clifford gates and noisy ancillas, *Phys. Rev. A* **71**, 022316 (2005).
- [36] S. Bravyi and J. Haah, Magic-state distillation with low overhead, *Phys. Rev. A* **86**, 052329 (2012).
- [37] Y. Ye, T. He, He L. Huang, Z. Wei, Y. Zhang, Y. Zhao, D. Wu, Q. Zhu, H. Guan, S. Cao, *et al.*, Logical magic state preparation with fidelity beyond the distillation threshold on a superconducting quantum processor, *Phys. Rev. Lett.* **131**, 210603 (2023).
- [38] H. Zhu and M. Hayashi, Efficient verification of hypergraph states, *Phys. Rev. Appl.* **12**, 054047 (2019).
- [39] Y. Akahoshi, K. Maruyama, H. Oshima, S. Sato, and K. Fujii, Partially fault-tolerant quantum computing architecture with error-corrected Clifford gates and space-time efficient analog rotations, *PRX Quantum* **5**, 010337 (2024).
- [40] H. Choi, F. T. Chong, D. Englund, and Y. Ding, Fault tolerant non-Clifford state preparation for arbitrary rotations, [arXiv:2303.17380](https://arxiv.org/abs/2303.17380).
- [41] D. Horsman, A. G. Fowler, S. Devitt, and R. V. Meter, Surface code quantum computing by lattice surgery, *New J. Phys.* **14**, 123011 (2012).

- [42] A. R. Calderbank and Peter W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A* **54**, 1098 (1996).
- [43] A. Steane, Multiple-particle interference and quantum error correction, *Proc. R. Soc. London, A* **452**, 2551 (1996).
- [44] H.-Y. Huang, J. Preskill, and M. Soleimanifar, Certifying almost all quantum states with few single-qubit measurements, *Nat. Phys.* **21**, 1834 (2025).
- [45] O. Gühne, Chao Y. Lu, Wei B. Gao, and Jian W. Pan, Toolbox for entanglement detection and fidelity estimation, *Phys. Rev. A* **76**, 030305(R) (2007).
- [46] G. Tóth and O. Gühne, Detecting genuine multipartite entanglement with two local measurements, *Phys. Rev. Lett.* **94**, 060501 (2005).
- [47] G. Tóth and O. Gühne, Entanglement detection in the stabilizer formalism, *Phys. Rev. A* **72**, 022340 (2005).
- [48] Y. Zhou, Q. Zhao, X. Yuan, and X. Ma, Detecting multipartite entanglement structure with minimal resources, *npj Quantum Inf.* **5**, 83 (2019).
- [49] Q. Zhao and Y. Zhou, Constructing multipartite bell inequalities from stabilizers, *Phys. Rev. Res.* **4**, 043215 (2022).
- [50] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. V. den Nest, and H. J. Briegel, Entanglement in graph states and its applications, [arXiv:quant-ph/0602096](https://arxiv.org/abs/quant-ph/0602096).
- [51] J.-P. Tillich and G. Zémor, Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength, *IEEE Trans. Inf. Theory* **60**, 1193 (2014).
- [52] J. Combes, C. Granade, C. Ferrie, and S. T. Flammia, Logical randomized benchmarking, [arXiv:1702.03688](https://arxiv.org/abs/1702.03688).
- [53] D. Gottesman, A. Kitaev, and J. Preskill, Encoding a qubit in an oscillator, *Phys. Rev. A* **64**, 012310 (2001).
- [54] Ye C. Liu, J. Shang, and X. Zhang, Efficient verification of entangled continuous-variable quantum states with local measurements, *Phys. Rev. Res.* **3**, L042004 (2021).
- [55] Debbie W. Leung, M. A. Nielsen, Isaac L. Chuang, and Y. Yamamoto, Approximate quantum error correction can lead to better codes, *Phys. Rev. A* **56**, 2567 (1997).
- [56] P. Hayden and G. Penington, Approximate quantum error correction revisited: Introducing the alpha-bit, *Commun. Math. Phys.* **374**, 369 (2020).
- [57] A. Anshu and S. Arunachalam, A survey on the complexity of learning quantum states, *Nat. Rev. Phys.* **6**, 59 (2024).
- [58] V. Gebhart, R. Santagati, A. A. Gentile, E. M. Gauger, D. Craig, N. Ares, L. Banchi, F. Marquardt, L. Pezzè, and C. Bonato, Learning quantum systems, *Nat. Rev. Phys.* **5**, 141 (2023).
- [59] T. Wagner, H. Kampermann, D. Bruß, and M. Kliesch, Learning logical Pauli noise in quantum error correction, *Phys. Rev. Lett.* **130**, 200601 (2023).
- [60] K. He, M. Yuan, Y. Wong, S. Chakram, A. Seif, L. Jiang, and D. I. Schuster, Efficient multimode Wigner tomography, *Nat. Commun.* **15**, 4138 (2024).
- [61] Ye C. Liu, J. Shang, Xiao D. Yu, and X. Zhang, Efficient verification of quantum processes, *Phys. Rev. A* **101**, 042315 (2020).
- [62] H. Zhu and H. Zhang, Efficient verification of quantum gates with local operations, *Phys. Rev. A* **101**, 042316 (2020).
- [63] P. Zeng, Y. Zhou, and Z. Liu, Quantum gate verification and its application in property testing, *Phys. Rev. Res.* **2**, 023306 (2020).
- [64] C. Zheng, X. Yu, Z. Zhang, P. Xu, and K. Wang, Efficient verification of stabilizer code subspaces with local measurements, [arXiv:2409.19699](https://arxiv.org/abs/2409.19699).