# Efficient verification of pure quantum states with applications to hypergraph states

Huangjun Zhu[1, 2, 3, 4, 5, *] and Masahito Hayashi[6, 7, 8]

[1] *Department of Physics and Center for Field Theory and Particle Physics, Fudan University, Shanghai 200433, China*
[2] *State Key Laboratory of Surface Physics, Fudan University, Shanghai 200433, China*
[3] *Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China*
[4] *Collaborative Innovation Center of Advanced Microstructures, Nanjing 210093, China*
[5] *Institute for Theoretical Physics, University of Cologne, Cologne 50937, Germany*
[6] *Graduate School of Mathematics, Nagoya University, Nagoya, 464-8602, Japan*
[7] *Shenzhen Institute for Quantum Science and Engineering,*
*Southern University of Science and Technology, Shenzhen, 518055, China*
[8] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542, Singapore*

(Dated: February 27, 2019)

Bipartite and multipartite entangled states are of central interest in quantum information processing and foundational studies. Efficient verification of these states, especially in the adversarial scenario, is a key to various applications, such as blind measurement-based quantum computation and quantum networks. Here we offer a general recipe to constructing efficient verification protocols for the adversarial scenario from protocols devised for the nonadversarial scenario. With this recipe, arbitrary pure states can be verified in the adversarial scenario with almost the same efficiency as in the nonadversarial scenario. In addition, we propose a simple protocol for verifying hypergraph states which requires only two distinct Pauli measurements for each party, yet its efficiency is comparable to the best protocol based on entangling measurements. For a given state, the overhead is bounded by the chromatic number and degree of the underlying hypergraph. Our protocol is dramatically more efficient than all known candidates based on local measurements, including tomography and direct fidelity estimation. It enables the verification of hypergraph states and genuine multipartite entanglement of thousands of qubits even in the adversarial scenario.

## I. INTRODUCTION

Entanglement is the characteristic feature of quantum theory and a key resource in quantum information processing [1, 2]. For example, bipartite entangled states, especially maximally entangled states, are crucial to quantum teleportation, dense coding, and quantum cryptography. As an archetypal example of quantum states with genuine multipartite entanglement (GME), graph states are of central interest to (blind) quantum computation [3–7], quantum error correction [8, 9], quantum networks [10–12], and foundational studies on nonlocality [13–15]. Hypergraph states [16–20], as a generalization of graph states, are equally useful in these research areas [21–25]. In addition, certain hypergraph states, like Union Jack states, are universal for measurement-based quantum computation (MBQC) under only Pauli measurements [21, 22, 25, 26], which is impossible for graph states. Moreover, hypergraph states are attractive for demonstrating quantum supremacy [23, 27]. Recently, multipartite entangled states, such as tensor-network states, also found extensive applications in other research areas, including condensed matter physics [28, 29].

The applications of entangled states in quantum information processing rely crucially on our ability to verify them with local measurements that are accessible in the lab. However, the resource required in traditional tomography increases exponentially with the number of qubits. The same is true for popular alternatives, such as compressed sensing [30] and direct fidelity estimation (DFE) [31]. So far efficient verification protocols are known only for bipartite pure states [32–37], stabilizer states (including graph states) [7, 12, 38–40], and weighted graph states [41]; many of these results are posted after the first version of this paper.

The situation is much worse in the adversarial scenario, in which the states to be verified are controlled by the adversary or an untrusted party. State verification in this adversarial scenario is crucial to many quantum information processing tasks that entail high security conditions, such as blind MBQC [6, 7, 26, 38, 39] and quantum networks [10–12]. However, no efficient method is known for addressing the adversarial scenario in general. For example, although several papers have studied the verification of hypergraph states [23, 42], to verify the simplest nontrivial hypergraph states (say of three qubits) already requires astronomical number of measurements. In addition, known verification protocols only apply to qubit hypergraph states, but not qudit hypergraph states, not to say more general quantum states.

In this paper we initiate a systematic study of pure-state verification in the adversarial scenario. In particular, we provide a general recipe to constructing efficient verification protocols for the adversarial scenario from verification protocols for the nonadversarial scenario. With this recipe, pure states can be verified in the adversarial scenario with almost the same efficiency as in the nonadversarial scenario. For high-precision verification, the overhead in the number of tests is at most three times. In this way, pure-state verification in the

[*] zhuhuangjun@fudan.edu.cn

adversarial scenario can be greatly simplified since it suffices to focus on the nonadversarial scenario and then apply our recipe. Surprisingly, optimal protocols constructed in this way are already nearly optimal among the most general protocols given the same restriction on the accessible measurements. In the course of our study, we determine the precision that can be reached given the resource available, and vice versa. Our study also reveals that entangling measurements are less helpful and often unnecessary in improving the efficiency for the adversarial scenario, which is counterintuitive at first sight. After the first version of this paper was posted, our results have found fruitful applications in the verification of bipartite pure states [34, 35] and weighted graph states [41].

In addition, we propose a simple method for verifying general (qubit and qudit) hypergraph states which requires only two distinct Pauli measurements for each party. To verify an $n$-qubit hypergraph state, our protocol requires at most $m = n$ (potential) measurement settings and $m \ln \delta^{-1}/\epsilon$ tests in total, where $\epsilon$ and $\delta$ denote the the infidelity and significance level, which characterize the precision required. For a given hypergraph state, $m$ can be replaced by the chromatic number or degree of the underlying hypergraph. The efficiency of our protocol has a simple graph theoretic interpretation. For many interesting families of graph and hypergraph states, including cluster states and Union Jack states, the number of measurement settings and that of tests in total do not increase with the number of qubits. For example, Union Jack states can be verified with only three measurement settings and $3 \ln \delta^{-1}/\epsilon$ tests in total.

Our protocol for verifying hypergraph states is dramatically more efficient than known candidates, including tomography and DFE [31], as well as recent verification protocols tailored for hypergraph states [23, 42]. This protocol enables efficient verification of hypergraph states and GME of thousands of qubits, which are more than enough for demonstrating quantum supremacy. By contrast, it would take the age of the universe to achieve the same task with protocols known in the literature. Thanks to the general recipe mentioned above, a simple variant of the protocol can be applied to the verification of hypergraph states in the adversarial scenario and achieves almost the same efficiency. Now the advantage over previous approaches is even more dramatic. In the special case of graph states and stabilizer states, our approach is also much more efficient than known candidates, although this problem has been well studied. Therefore, our approach is particularly appealing to blind MBQC, quantum networks, and many other applications in which security requirements are high.

The rest of this paper is organized as follows. In Sec. II we review the basic framework of pure-state verification in the nonadversarial scenario and derive a lower bound on the minimal number of measurement settings for each party. In Sec. III we study systematically pure-state verification in the adversarial scenario and propose a general recipe for constructing efficient verification protocols for the adversarial scenario by virtue of protocols devised for the nonadversarial scenario. In Sec. IV, we review hypergraph and hypergraph states and derive a few graph theoretic results in preparation for later study. In Sec. V we propose simple and efficient protocols for verifying general hypergraph states in both nonadversarial scenario and adversarial scenario. Applications of these protocols to the detection of GME are discussed in Sec. VI. Generalization to qudit hypergraph states is discussed in Sec. VII. To streamline the presentation, most technical proofs are relegated to the appendix.

## II. VERIFICATION OF PURE STATES: NONADVERSARIAL SCENARIO

In this section we review the basic framework of pure-state verification in the nonadversarial scenario. The main results presented here are known before [40], but we have simplified the derivation. These results will serve as a benchmark for understanding pure-state verification in the adversarial scenario, which is a main focus of this paper. In addition, we determine the minimal number of measurement settings required by each party to verify generic multipartite pure states.

### A. Setting the stage

Consider a device that is supposed to produce the target state $|\Psi\rangle$ in the (generally multipartite) Hilbert space $\mathcal{H}$. In practice, the device may actually produce $\sigma_1, \sigma_2, \dots, \sigma_N$ in $N$ runs. We assume that the fidelity $\langle\Psi|\sigma_j|\Psi\rangle$ is either 1 for all $j$ or satisfies $\langle\Psi|\sigma_j|\Psi\rangle \leq 1-\epsilon$ for all $j$ [40]. Now the task is to determine which is the case. This conclusion is useful if we assume that the next state $\sigma_{N+1}$ produced by the device has the same behavior as the previous ones.

To achieve this task we can perform two-outcome measurements from a set of accessible measurements. Here we are interested in local projective measurements that are most relevant in practice. Each two-outcome projective measurement $\{P_l, 1-P_l\}$ is specified by a projector $P_l$, which corresponds to passing the test, and is performed with probability $\mu_l$. Here we assume that the target state $|\Psi\rangle$ always passes the test, that is, $P_l|\Psi\rangle = |\Psi\rangle$ for all $P_l$. When $\langle\Psi|\sigma_j|\Psi\rangle \leq 1-\epsilon$, by contrast, the maximal probability that $\sigma_j$ can pass the test is given by [40] (see also Appendix A)

$$\max_{\langle\Psi|\sigma|\Psi\rangle\leq 1-\epsilon} \operatorname{tr}(\Omega\sigma) = 1 - [1-\beta(\Omega)]\epsilon = 1 - \nu(\Omega)\epsilon, \quad (1)$$

where $\Omega := \sum_l \mu_l P_l$ is referred to as a verification operator and a strategy, $\beta(\Omega)$ is the second largest eigenvalue of $\Omega$, and $\nu(\Omega) := 1 - \beta(\Omega)$ is the spectral gap from the maximal eigenvalue.

After $N$ runs, $\sigma_j$ in the bad case can pass all tests with probability at most $[1-\nu(\Omega)\epsilon]^N$. Solving the equation $\delta=[1-\nu(\Omega)\epsilon]^N$ yields $\epsilon=(1-\delta^{1/N})/\nu(\Omega)\leq-\frac{\ln\delta}{N\nu(\Omega)}$, assuming $\delta>0$. If all $N$ tests are passed, with significance level $\delta$, we can guarantee that the state $\sigma_{N+1}$ satisfies

$$\langle\Psi|\sigma_{N+1}|\Psi\rangle>1-\frac{1-\delta^{1/N}}{\nu(\Omega)}\geq1-\frac{\ln\delta^{-1}}{N\nu(\Omega)}. \quad (2)$$

Note that the significance level is the maximum passing probability when the state $\sigma_{N+1}$ does not satisfy Eq. (2). Hence, to guarantee the condition $\langle\Psi|\sigma_{N+1}|\Psi\rangle>1-\epsilon$ with significance level $\delta$, the minimal number of tests is given by [40]

$$N_{\mathrm{NA}}(\epsilon,\delta,\Omega)=\left\lceil\frac{1}{\ln[1-\nu(\Omega)\epsilon]}\ln\delta\right\rceil\leq\left\lceil\frac{1}{\nu(\Omega)\epsilon}\ln\delta^{-1}\right\rceil. \quad (3)$$

The optimal protocol is obtained by maximizing the spectral gap $\nu(\Omega)$. If there is no restriction on the measurements, then the optimal protocol is composed of the projective measurement $\{|\Psi\rangle\langle\Psi|,1-|\Psi\rangle\langle\Psi|\}$, in which case $\Omega=|\Psi\rangle\langle\Psi|$, $\nu(\Omega)=1$, and $N\approx\frac{1}{\epsilon}\ln\delta^{-1}$. This efficiency cannot be improved further even if we can perform collective measurements. In practice, however, $|\Psi\rangle$ is usually entangled, and it is too difficult to perform such entangling measurements. It is therefore crucial to devise efficient protocols based on local projective measurements, which is a focus of this paper.

When all $\sigma_j$ are identical to $\sigma$, let $F=\langle\Psi|\sigma|\Psi\rangle$; then $F\leq\operatorname{tr}(\Omega\sigma)\leq\nu(\Omega)F+1-\nu(\Omega)$, which implies that

$$1-\operatorname{tr}(\Omega\sigma)\leq1-F\leq\nu(\Omega)^{-1}[1-\operatorname{tr}(\Omega\sigma)]. \quad (4)$$

So the passing probability $\operatorname{tr}(\Omega\sigma)$ provides upper and lower bounds for the infidelity (and fidelity). In general, Eq. (4) still holds if $F$ and $\operatorname{tr}(\Omega\sigma)$ are replaced by the average over all $\sigma_j$.

Here, we compare the approach presented above with the preceding papers Refs. [32, 33]. In mathematical statistics, we often discuss hypothesis testing with the framework of uniformly most powerful test among a certain class of tests. In this case, we fix a certain set of states $\mathcal{S}_0$, and impose to our test the condition that the probability of erroneously supporting states in $\mathcal{S}_0$ is upper bounded by a certain value $\delta'\geq0$. Under this condition, we maximize the probability of detecting a state $\sigma$ in $\mathcal{S}^c$. Since the detecting probability depends on the state $\sigma$, in general there is no test to maximize the probability uniformly. In this paper, $\mathcal{S}_0$ and $\delta'$ are chosen to be $\{|\Psi\rangle\}$ and 0, respectively. We consider the case when we apply the same strategy $\Omega$ $N$ times. Since we support the state $|\Psi\rangle$ only when all our outcomes correspond to the pass eigenspace of $\Omega$, our test is uniformly most powerful under this case. When the set $\mathcal{S}_0$ is chosen as $\{\sigma|\langle\Psi|\sigma|\Psi\rangle\geq1-\epsilon'\}$, and $\delta'$ is a non-zero value, the problem is more complicated. Such a setting arises when we allow a certain amount of error. The preceding papers Refs. [32, 33] discussed several optimization problems and investigated their asymptotic behaviors when $|\Psi\rangle$ is a maximally entangled state.

### B. Minimal requirements for verifying multipartite pure states

As a first step towards understanding the limitation of local measurements, it is instructive to study the minimal number of measurement settings for each party required to verify a general multipartite pure state that is genuinely multipartite entangled (GME). Recall that a multipartite pure state is GME if it cannot be expressed as the product of two pure states [2]. Here is the scenario of interest: in each test, each party performs a local projective measurement, and the test is passed for a certain subset of the outcomes; the measurement of one party may depend on the measurement outcome of another party. The following proposition sets a fundamental lower bound for the number of measurement settings for each party.

*Proposition* 1. To verify any multipartite pure state that is GME with local projective measurements, each party needs at least two measurement settings.

*Proof.* Let $|\Psi\rangle$ be any multipartite pure state that is GME. Suppose on the contrary that $|\Psi\rangle$ can be verified by a strategy $\Omega$ for which party $j$ performs only one projective measurement associated with the basis $\{|\varphi_1\rangle,|\varphi_2\rangle,\dots,|\varphi_d\rangle\}$ where $d$ is the dimension of the Hilbert space for party $j$. Let $P_k=|\varphi_k\rangle\langle\varphi_k|$ be the corresponding rank-1 projectors and $|\tilde{\Psi}_k\rangle=\langle\varphi_k|\Psi\rangle$ be states on the remaining parties, which are not normalized. Then each test projector has the form $\sum_{k=1}^d P_k\otimes Q_k$, where $Q_k$ for $k=1,2,\dots,d$ are projectors acting on the Hilbert space for the remaining parties and satisfy $Q_k|\tilde{\Psi}_k\rangle=|\tilde{\Psi}_k\rangle$, so that the target state $|\Psi\rangle$ can always pass the test. Since $|\Psi\rangle$ is GME by assumption, $|\tilde{\Psi}_k\rangle$ is nonzero for at least two different values of $k$, say 1 and 2. Let $|\Psi_k\rangle=|\tilde{\Psi}_k\rangle/\sqrt{\langle\tilde{\Psi}_k|\tilde{\Psi}_k\rangle}$ for $k=1,2$. Then $|\varphi_k\rangle\otimes|\Psi_k\rangle$ for $k=1,2$ belong to the support of each test projector and thus the pass eigenspace of $\Omega$. Consequently, the pass eigenspace of $\Omega$ has dimension at least 2, which means $\nu(\Omega)=0$, so $|\Psi\rangle$ cannot be verified reliably. This contradiction completes the proof. □

According to the same reasoning presented above, to verify any multipartite pure state, each party needs at least two measurement settings unless the party is not entangled with other parties, in which case the reduced state of the party is a pure state and the party needs to perform only one projective measurement with the pure state as a basis state.

## III. VERIFICATION OF PURE STATES: ADVERSARIAL SCENARIO

Now we turn to the adversarial scenario in which the device for generating quantum states is controlled by a potentially malicious adversary. Efficient verification of quantum states in such adversarial scenario is crucial to many quantum information-processing tasks that entail high security requirements, such as blind quantum computation [6, 7, 26, 38, 39] and quantum networks [10–12]. However, little is known about this problem in the literature. Most previous studies only focus on specific families of states, such as graph states [7, 12, 38, 39] and hypergraph states [23, 42]. In addition, known protocols are not so efficient, especially for hypergraph states for which the best protocols known in the literature require astronomical number of tests even in the simplest nontrivial scenario.

In this section we initiate a systematic study of pure-state verification in the adversarial scenario and settle three key problems. First, we determine the precision that can be reached given the resource available (the number of copies of the state available for verification or the number of tests). Second, we determine the resource required for achieving a given precision. Third, we provide a general recipe to constructing efficient verification protocols for the adversarial scenario from verification protocols for the nonadversarial scenario. With this recipe, arbitrary pure states can be verified in the adversarial scenario with almost the same efficiency as in the nonadversarial scenario. For high-precision verification, the overhead in the number of tests is at most three times.

### A. Formulation

In the adversarial scenario, the device is controlled by a potentially malicious adversary and may produce an arbitrary state $\rho$ on the whole system $\mathcal{H}^{\otimes(N+1)}$. Our task is to ensure that the reduced state on one system has infidelity less than $\epsilon$ by performing $N$ tests on other systems. To verify the state produced by the device, we randomly choose $N$ systems and apply certain strategy $\Omega$ to each system chosen. Since $N$ systems are chosen randomly, without loss of generality, we may assume that $\rho$ is permutation invariant.

Suppose the strategy $\Omega$ is applied to the first $N$ systems, then the probability that $\rho$ can pass $N$ tests reads

$$p_\rho = \operatorname{tr}[(\Omega^{\otimes N} \otimes 1)\rho]. \tag{5}$$

The reduced state on system $N+1$ (assuming $p_\rho > 0$) is given by

$$\sigma_{N+1} = \frac{\operatorname{tr}_{1,2,\ldots,N}[(\Omega^{\otimes N} \otimes 1)\rho]}{p_\rho}, \tag{6}$$

where $\operatorname{tr}_{1,2,\ldots,N}$ means the partial trace over the systems $1, 2, \ldots, N$. The fidelity between $\sigma_{N+1}$ and $|\Psi\rangle$ reads

$$F_\rho = \langle\Psi|\sigma_{N+1}|\Psi\rangle = \frac{f_\rho}{p_\rho}, \tag{7}$$

where

$$f_\rho = \operatorname{tr}[(\Omega^{\otimes N} \otimes |\Psi\rangle\langle\Psi|)\rho]. \tag{8}$$

To characterize the performance of the strategy $\Omega$ applied to the adversarial scenario, here we introduce four figures of merit. Define

$$F(N,\delta,\Omega) := \min_\rho \{p_\rho^{-1} f_\rho \,|\, p_\rho \geq \delta\}, \quad 0 < \delta \leq 1, \tag{9a}$$

$$\mathcal{F}(N,f,\Omega) := \min_\rho \{p_\rho^{-1} f_\rho \,|\, f_\rho \geq f\}, \quad 0 < f \leq 1, \tag{9b}$$

$$\zeta(N,\delta,\Omega) := \min_\rho \{f_\rho \,|\, p_\rho \geq \delta\}, \quad 0 \leq \delta \leq 1, \tag{9c}$$

$$\eta(N,f,\Omega) := \max_\rho \{p_\rho \,|\, f_\rho \leq f\}, \quad 0 \leq f \leq 1, \tag{9d}$$

where $N$ is a positive integer. The four figures of merit are closely related to each other, as we shall see later. In practice $F(N,\delta,\Omega)$ is a main figure of merit of interest; it denotes the minimal fidelity of the state on the remaining party (with the target state), assuming that $\rho$ can pass $N$ tests with significance level at least $\delta$. By definition $F(N,\delta,\Omega)$ and $\zeta(N,\delta,\Omega)$ are nondecreasing in $\delta$, while $\mathcal{F}(N,f,\Omega)$ and $\eta(N,f,\Omega)$ are nondecreasing in $f$.

The four figures of merit defined in Eq. (9a)-(9d) are tied to the two-dimensional region composed of all the points $(p_\rho, f_\rho)$ for density matrices $\rho$, that is,

$$R_{N,\Omega} := \{(p_\rho, f_\rho)|\forall\rho\}. \tag{10}$$

This geometric picture will be very helpful to understanding state verification in the adversarial scenario. By definition the region $R_{N,\Omega}$ is convex since the state space is convex, and $p_\rho, f_\rho$ are both linear in $\rho$. What is not so obvious at the moment is that the region $R_{N,\Omega}$ is actually a convex polygon.

In addition to characterizing the verification precision that is achievable for a given number $N$ of tests, it is equally important to determine the number of tests required to reach a given precision. To this end, we define $N(\epsilon,\delta,\Omega)$ as the minimum value of $N$ that satisfies the condition $F(N,\delta,\Omega) \geq 1-\epsilon$; in other words,

$$N(\epsilon,\delta,\Omega) := \min\{N \,|\, F(N,\delta,\Omega) \geq 1-\epsilon\}. \tag{11}$$

### B. Computation of the verification precision

In this section we develop a general method for computing the figures of merit defined in Eq. (9), which characterize the verification precision in the adversarial scenario. We also clarify the properties of these figures of merit in preparation for latter study. Both algebraic derivation and geometric pictures will be helpful in our analysis.

Suppose the verification operator $\Omega$ for the target state $|\Psi\rangle \in \mathcal{H}$ has spectral decomposition $\Omega = \sum_{j=1}^{D} \lambda_j \Pi_j$, where $\lambda_j$ are the eigenvalues of $\Omega$ arranged in decreasing order $1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_D$, and $\Pi_j$ are mutually orthogonal rank-1 projectors with $\Pi_1 = |\Psi\rangle\langle\Psi|$. Here the second largest eigenvalue $\beta := \lambda_2$ and the smallest eigenvalue $\tau := \lambda_D$ deserve special attention because they determine the performance of $\Omega$ to a large extent, as we shall see later. Suppose the adversary produces the state $\rho$ on the whole system $\mathcal{H}^{\otimes(N+1)}$, which is permutation invariant (cf. Sec. III A). Without loss of generality, we may assume that $\rho$ is diagonal in the product basis constructed from the eigenbasis of $\Omega$ (as determined by the projectors $\Pi_j$), since $p_\rho$, $f_\rho$, and $F_\rho$ only depend on the diagonal elements of $\rho$.

Let $\mathbf{k} = (k_1, k_2, \ldots, k_D)$ be a sequence of $D$ nonnegative integers that sum up to $N+1$, that is, $\sum_j k_j = N+1$. Let $\mathscr{S}$ be the set of all such sequences. For each $\mathbf{k}$, we can define a permutation-invariant diagonal density matrix $\rho_{\mathbf{k}}$ as the uniform mixture of all permutations of $\Pi_1^{\otimes k_1} \otimes \Pi_2^{\otimes k_2} \otimes \cdots \otimes \Pi_D^{k_D}$. Then any permutation-invariant diagonal density matrix $\rho$ can be expressed as $\rho = \sum_{\mathbf{k}} c_{\mathbf{k}} \rho_{\mathbf{k}}$, where $c_{\mathbf{k}}$ form a probability distribution on $\mathscr{S}$. Accordingly,

$$p_\rho = \sum_{\mathbf{k}} c_{\mathbf{k}} \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \quad f_\rho = \sum_{\mathbf{k}} c_{\mathbf{k}} \zeta_{\mathbf{k}}(\boldsymbol{\lambda}), \tag{12}$$

$$F_\rho = \frac{f_\rho}{p_\rho} = \frac{\sum_{\mathbf{k}} c_{\mathbf{k}} \zeta_{\mathbf{k}}(\boldsymbol{\lambda})}{\sum_{\mathbf{k}} c_{\mathbf{k}} \eta_{\mathbf{k}}(\boldsymbol{\lambda})}, \tag{13}$$

where $\boldsymbol{\lambda} := (\lambda_1, \lambda_2, \ldots, \lambda_D)$ and

$$\begin{aligned} \eta_{\mathbf{k}}(\boldsymbol{\lambda}) &:= p_{\rho_{\mathbf{k}}} = \sum_{i|k_i \geq 1} \frac{k_i}{(N+1)} \lambda_i^{k_i - 1} \prod_{j \neq i|k_j \geq 1} \lambda_j^{k_j}, \\ \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) &:= f_{\rho_{\mathbf{k}}} = \frac{k_1}{N+1} \prod_{i|k_i \geq 1} \lambda_i^{k_i}. \end{aligned} \tag{14}$$

Here we set $\lambda_i^0 = 1$ even if $\lambda_i = 0$.

The assumption $1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_D = \tau$ implies that $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \leq \eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leq 1$; the second inequality is saturated iff $\mathbf{k} = \mathbf{k}_0 := (N+1, 0, \ldots, 0)$, in which case both inequalities are saturated, that is, $\zeta_{\mathbf{k}_0}(\boldsymbol{\lambda}) = \eta_{\mathbf{k}_0}(\boldsymbol{\lambda}) = 1$. As an implication, we have $f_\rho \leq p_\rho \leq 1$, and the second inequality is saturated iff $\rho = \rho_{\mathbf{k}_0} = (|\Psi\rangle\langle\Psi|)^{\otimes(N+1)}$, in which case $f_\rho = p_\rho = 1$. This observation implies that

$$F(N, \delta = 1, \Omega) = \zeta(N, \delta = 1, \Omega) = 1, \tag{15}$$

$$\mathcal{F}(N, f = 1, \Omega) = \eta(N, f = 1, \Omega) = 1. \tag{16}$$

By contrast, $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) \geq \tau^N$, and the lower bound is saturated when $\mathbf{k} = (0, \ldots, 0, N+1)$. Accordingly, $p_\rho \geq \tau^N$, and the lower bound is saturated when $\rho = \Pi_D^{\otimes(N+1)}$.

In view of the above discussion, the region $R_{N,\Omega}$ defined in Eq. (10) is the convex hull of $(\eta_{\mathbf{k}}(\boldsymbol{\lambda}), \zeta_{\mathbf{k}}(\boldsymbol{\lambda}))$ for all $\mathbf{k} \in \mathscr{S}$, which is a polygon, as illustrated in Fig. 1. It should be emphasized that $R_{N,\Omega}$ only depends on the distinct eigenvalues of $\Omega$, but not on their degeneracies (though $\lambda_1$ is not degenerate by assumption). The same conclusion also applies to the figures of merit $F(N, \delta, \Omega)$, $\mathcal{F}(N, f, \Omega)$, $\zeta(N, \delta, \Omega)$, and $\eta(N, f, \Omega)$ defined in Eq. (9) given that they are completely determined by the region $R_{N,\Omega}$. For example, $F(N, \delta, \Omega)$ corresponds to the lower boundary of the intersection of $R_{N,\Omega}$ and the vertical line $p_\rho = \delta$ as long as $\delta \geq \tau^N$. This geometric picture is very helpful to understanding the properties of $F(N, \delta, \Omega)$, although in general it is not easy to find an explicit analytical formula. As $N$ increases, the region $R_{N,\Omega}$ concentrates more and more around the diagonal defined by the equation $f = p$ as illustrated in Fig. 1, which means $F(N, \delta, \Omega)$ approaches 1 as $N$ increases.

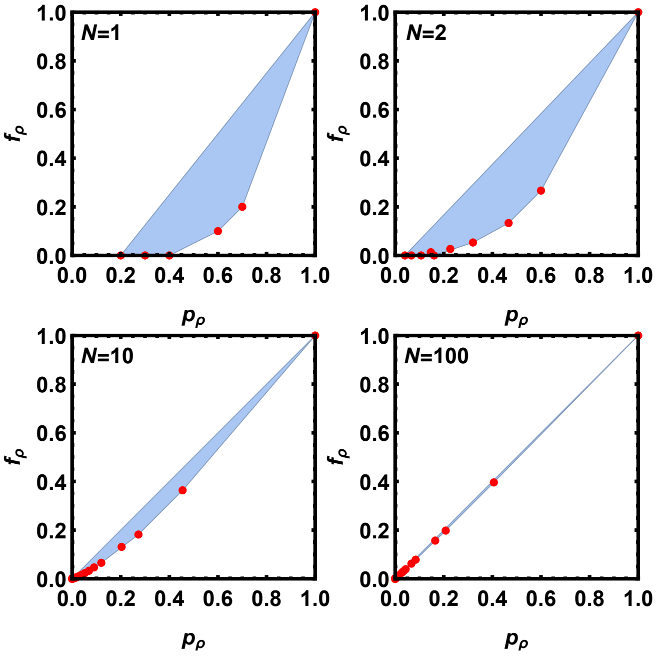

FIG. 1. (color online) The region $R_{N,\Omega}$ composed of $(p_\rho, f_\rho)$ as defined in Eq. (10). This region is the convex hull of points $(\eta_{\mathbf{k}}(\boldsymbol{\lambda}), \zeta_{\mathbf{k}}(\boldsymbol{\lambda}))$ for $\mathbf{k} \in \mathscr{S}$, which are highlighted as red dots. Here $\Omega$ has three distinct eigenvalues, namely, 1, 0.4, and 0.2.

Denote by $\sigma(\Omega)$ the set of distinct eigenvalues of $\Omega$. If $\Omega'$ is another verification operator for $|\Psi\rangle$ with $\beta(\Omega') < 1$ and $\sigma(\Omega') \subset \sigma(\Omega)$. Then $\Omega'$ is more efficient than $\Omega$ in the sense that

$$F(N, \delta, \Omega') \geq F(N, \delta, \Omega), \ N(\epsilon, \delta, \Omega') \leq N(\epsilon, \delta, \Omega). \tag{17}$$

This observation is instructive to constructing efficient verification protocols, as we shall see in Sec. III C.

In the rest of this section we summarize the main properties of the four figures of merit $F(N, \delta, \Omega)$, $\mathcal{F}(N, f, \Omega)$, $\zeta(N, \delta, \Omega)$, and $\eta(N, f, \Omega)$; the proofs are relegated to Appendix B. We also show that these figures of merit can be computed by linear programming.

To start with, we determine $\eta(N, 0, \Omega)$, the maximum of $p_\rho$ under the condition $f_\rho = 0$.

*Lemma* 1. $\eta(N,0,\Omega)=\delta_{\rm c}$, where

$$\delta_{\rm c}:=\begin{cases}\beta^N & \tau>0,\\ \max\{\beta^N,1/(N+1)\} & \tau=0.\end{cases} \tag{18}$$

Lemma 1 has implications for the figures of merit $F(N,\delta,\Omega)$ and $\zeta(N,\delta,\Omega)$ as well,

$$F(N,\delta,\Omega)=\zeta(N,\delta,\Omega)=0,\quad 0<\delta\leq\delta_{\rm c}, \tag{19}$$

$$F(N,\delta,\Omega)>0,\quad \zeta(N,\delta,\Omega)>0,\quad \delta_{\rm c}<\delta\leq 1. \tag{20}$$

Next, we introduce alternative definitions of the figures of merit defined in Eq. (9), which are easier to analyze. Define

$$\tilde{F}(N,\delta,\Omega):=\begin{cases}\delta^{-1}\min\limits_{\rho}\{f_\rho\,|\,p_\rho=\delta\} & \delta_{\rm c}\leq\delta\leq 1,\\ 0 & 0<\delta\leq\delta_{\rm c};\end{cases} \tag{21a}$$

$$\tilde{\mathcal{F}}(N,f,\Omega):=f\min_{\rho}\left\{p_\rho^{-1}\,|\,f_\rho=f\right\}\quad 0<f\leq 1; \tag{21b}$$

$$\tilde{\zeta}(N,\delta,\Omega):=\begin{cases}\min_\rho\left\{f_\rho\,|\,p_\rho=\delta\right\} & \delta_{\rm c}\leq\delta\leq 1,\\ 0 & 0\leq\delta\leq\delta_{\rm c};\end{cases} \tag{21c}$$

$$\tilde{\eta}(N,f,\Omega):=\max_{\rho}\left\{p_\rho\,|\,f_\rho=f\right\},\quad 0\leq f\leq 1. \tag{21d}$$

By definition $\tilde{F}(N,\delta,\Omega)=\tilde{\zeta}(N,\delta,\Omega)/\delta$ for $0<\delta\leq 1$ and $\tilde{\mathcal{F}}(N,f,\Omega)=f/\tilde{\eta}(N,f,\Omega)$ for $0<f\leq 1$.

*Lemma* 2. Suppose $0<\delta,f\leq 1$. Then

$$F(N,\delta,\Omega)=\tilde{F}(N,\delta,\Omega), \tag{22a}$$

$$\mathcal{F}(N,f,\Omega)=\tilde{\mathcal{F}}(N,f,\Omega), \tag{22b}$$

$$\zeta(N,\delta,\Omega)=\tilde{\zeta}(N,\delta,\Omega), \tag{22c}$$

$$\eta(N,f,\Omega)=\tilde{\eta}(N,f,\Omega). \tag{22d}$$

Lemma 2 implies that

$$F(N,\delta,\Omega)=\frac{\tilde{\zeta}(N,\delta,\Omega)}{\delta}=\frac{\zeta(N,\delta,\Omega)}{\delta},\ 0<\delta\leq 1, \tag{23}$$

$$\mathcal{F}(N,f,\Omega)=\frac{f}{\tilde{\eta}(N,f,\Omega)}=\frac{f}{\eta(N,f,\Omega)},\ 0<f\leq 1. \tag{24}$$

To compute $F(N,\delta,\Omega)$ and $\mathcal{F}(N,f,\Omega)$, it suffices to compute $\zeta(N,\delta,\Omega)$ and $\eta(N,f,\Omega)$. By virtue of Eq. (12) and Lemma 2, $\zeta(N,\delta,\Omega)$ with $\delta_{\rm c}\leq\delta\leq 1$ and $\eta(N,f,\Omega)$ with $0\leq f\leq 1$ can be computed via linear programming,

$$\zeta(N,\delta,\Omega)=\min_{\{c_{\mathbf{k}}\}}\left\{\sum_{\mathbf{k}\in\mathscr{S}}c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda})\middle|\sum_{\mathbf{k}\in\mathscr{S}}c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda})=\delta\right\}, \tag{25a}$$

$$\eta(N,f,\Omega)=\max_{\{c_{\mathbf{k}}\}}\left\{\sum_{\mathbf{k}\in\mathscr{S}}c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda})\middle|\sum_{\mathbf{k}\in\mathscr{S}}c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda})=f\right\}. \tag{25b}$$

Here the minimum in Eq. (25a) can be attained at a distribution $\{c_{\mathbf{k}}\}$ that is supported on at most two points in $\mathscr{S}$; a similar conclusion holds for the maximum in Eq. (25b). These conclusions are tied to the geometric fact that any boundary point of $R_{N,\Omega}$ lies on a line segment that connects two extremal points. This observation can greatly simplify the computation of $F(N,\delta,\Omega)$ and $\mathcal{F}(N,f,\Omega)$ as well as $\zeta(N,\delta,\Omega)$ and $\eta(N,f,\Omega)$. In addition to the computational value, Eq. (25) implies that $\zeta(N,\delta,\Omega)$ and $\eta(N,f,\Omega)$ are piecewise linear functions, whose turning points correspond to the extremal points of the region $R_{N,\Omega}$ and have the form $(\eta_{\mathbf{k}}(\boldsymbol{\lambda}),\zeta_{\mathbf{k}}(\boldsymbol{\lambda}))$ for some $\mathbf{k}\in\mathscr{S}$; cf. Lemma 13 in Appendix B.

*Lemma* 3. The following statements hold.

1. $\zeta(N,\delta,\Omega)$ is convex in $\delta$ for $0\leq\delta\leq 1$ and is strictly increasing in $\delta$ for $\delta_{\rm c}\leq\delta\leq 1$.

2. $\eta(N,f,\Omega)$ is concave and strictly increasing in $f$ for $0\leq f\leq 1$.

3. $F(N,\delta,\Omega)$ is strictly increasing in $\delta$ for $\delta_{\rm c}\leq\delta\leq 1$.

4. $\mathcal{F}(N,f,\Omega)$ is strictly increasing in $f$ for $0<f\leq 1$.

Note that the two functions $\zeta(N,\delta,\Omega)$ and $F(N,\delta,\Omega)$ are nondecreasing in $\delta$ over the whole interval $0<\delta\leq 1$, given that they are nonnegative and that $F(N,\delta,\Omega)=\zeta(N,\delta,\Omega)=0$ for $0<\delta\leq\delta_{\rm c}$. This conclusion also follows from the definitions in Eq. (9).

*Lemma* 4. Suppose $0\leq\delta,f\leq 1$. Then

$$\eta(N,\zeta(N,\delta,\Omega),\Omega)=\max\{\delta,\delta_{\rm c}\}, \tag{26}$$

$$\zeta(N,\eta(N,f,\Omega),\Omega)=f. \tag{27}$$

*Lemma* 5. Suppose $N\geq 2$ and $0<\delta,f\leq 1$. Then

$$\zeta(N,\delta,\Omega)\geq\zeta(N-1,\delta,\Omega), \tag{28a}$$

$$F(N,\delta,\Omega)\geq F(N-1,\delta,\Omega), \tag{28b}$$

$$\eta(N,f,\Omega)\leq\eta(N-1,f,\Omega), \tag{28c}$$

$$\mathcal{F}(N,f,\Omega)\geq\mathcal{F}(N-1,f,\Omega). \tag{28d}$$

The first two inequalities are saturated iff $\delta\leq\delta_{\rm c}$ or $\delta=1$. The last two inequalities are saturated iff $f=1$.

Finally, we present a few results about $N(\epsilon,\delta,\Omega)$ defined in Eq. (11). As an implication of Lemma 3, $N(\epsilon,\delta,\Omega)$ increases monotonically with $1/\epsilon$ and $1/\delta$ as expected. The following lemma provides several equivalent ways for computing $N(\epsilon,\delta,\Omega)$.

*Lemma* 6. Suppose $0<\epsilon,\delta<1$. Then

$$N(\epsilon,\delta,\Omega)=\min\{N\,|\,\zeta(N,\delta,\Omega)\geq\delta(1-\epsilon)\} \tag{29}$$

$$=\min\{N\,|\,\eta(N,\delta(1-\epsilon),\Omega)\leq\delta\} \tag{30}$$

$$=\min\{N\,|\,\mathcal{F}(N,\delta(1-\epsilon),\Omega)\geq(1-\epsilon)\}. \tag{31}$$

### C. Homogeneous strategies

A strategy (or verification operator) $\Omega$ for $|\Psi\rangle$ is *homogeneous* if it has the form

$$\Omega=|\Psi\rangle\langle\Psi|+\lambda(1-|\Psi\rangle\langle\Psi|), \tag{32}$$

where $0 \leq \lambda < 1$. In this case, all eigenvalues of $\Omega$ are equal to $\lambda$ except for the largest one, so we have $\beta = \tau = \lambda$, $\nu = 1 - \lambda$, and

$$\delta_{\mathrm{c}} = \begin{cases} \lambda^N & \lambda > 0, \\ 1/(N+1) & \lambda = 0. \end{cases} \tag{33}$$

In the nonadversarial scenario, a smaller $\lambda$ achieves a better performance among homogeneous strategies. Here, we clarify what $\lambda$ is optimal in the adversarial scenario, which turns out to be very different from the nonadversarial scenario. Incidentally, the homogeneous strategy $\Omega$ can always be realized by performing the test $P = |\Psi\rangle\langle\Psi|$ with probability $1-\lambda$ and the trivial test with probability $\lambda$. By "trivial test" we mean the test projector is equal to the identity operator. For bipartite pure states [32–35] and stabilizer states [40], the homogeneous strategy can also be realized by virtue of local projective measurements when $\lambda$ is sufficiently large.

Given that the homogeneous strategy $\Omega$ in Eq. (32) is determined by the parameter $\lambda$, it is more informative to express the figures of merit in Eqs. (9) and (11) as follows,

$$F(N,\delta,\lambda) := F(N,\delta,\Omega), \tag{34a}$$
$$\mathcal{F}(N,f,\lambda) := \mathcal{F}(N,f,\Omega), \tag{34b}$$
$$\zeta(N,\delta,\lambda) := \zeta(N,\delta,\Omega), \tag{34c}$$
$$\eta(N,f,\lambda) := \eta(N,f,\Omega), \tag{34d}$$
$$N(\epsilon,\delta,\lambda) := N(\epsilon,\delta,\Omega). \tag{34e}$$

Suppose $\tilde{\Omega}$ is an arbitrary verification operator with eigenvalues $1 = \tilde{\lambda}_1 > \tilde{\lambda}_2 \geq \cdots \geq \tilde{\lambda}_D$. Then we have $F(N,\delta,\tilde{\lambda}_j) \geq F(N,\delta,\tilde{\Omega})$ for $2 \leq j \leq D$ according to Eq. (17). Therefore, the optimal performance can always be achieved by a homogeneous strategy if there is no restriction on the accessible measurements. This observation reveals the importance of homogeneous strategies in studying quantum state verification in the adversarial scenario.

In preparation for the following discussions, we need to introduce a few more notations. Denote by $\mathbb{Z}$ and $\mathbb{Z}^{\geq 0}$ the set of integers and the set of nonnegative integers, respectively. For $k \in \mathbb{Z}^{\geq 0}$, define

$$\begin{aligned} \eta_k(\lambda) &:= \frac{(N+1-k)\lambda^k + k\lambda^{k-1}}{N+1}, \\ \zeta_k(\lambda) &:= \frac{(N+1-k)\lambda^k}{N+1}. \end{aligned} \tag{35}$$

We take the convention that $\lambda^0 = \eta_0(\lambda) = \zeta_0(\lambda) = 1$ even if $\lambda = 0$. Note that

$$\eta_k(\lambda) = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \quad \zeta_k(\lambda) = \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \tag{36}$$

when $k \in \{0,1,\ldots,N+1\}$, where $\mathbf{k} = (N+1-k,k)$, $\boldsymbol{\lambda} = (1,\lambda)$, and $\eta_{\mathbf{k}}(\boldsymbol{\lambda})$, $\zeta_{\mathbf{k}}(\boldsymbol{\lambda})$ are defined in Eq. (14). The extension of the definitions of $\eta_k(\lambda)$ and $\zeta_k(\lambda)$ to the set $\mathbb{Z}^{\geq 0}$ will be useful in proving several important results on homogeneous strategies.

### 1. The singular homogeneous strategy

When $\lambda = 0$, the verification operator $\Omega = |\Psi\rangle\langle\Psi|$ is singular, and Eq. (35) reduces to

$$\eta_k(\lambda) = \begin{cases} 1 & k = 0, \\ (N+1)^{-1} & k = 1, \\ 0 & k \geq 2. \end{cases} \quad \zeta_k(\lambda) = \begin{cases} 1 & k = 0, \\ 0 & k \geq 1. \end{cases} \tag{37}$$

According to Lemma 2, we have

$$\zeta(N,\delta,\lambda=0) = \begin{cases} 0 & \delta \leq (N+1)^{-1}, \\ \frac{(N+1)\delta-1}{N} & \delta > (N+1)^{-1}; \end{cases} \tag{38}$$

$$F(N,\delta,\lambda=0) = \begin{cases} 0 & \delta \leq (N+1)^{-1}, \\ \frac{(N+1)\delta-1}{N\delta} & \delta > (N+1)^{-1}. \end{cases} \tag{39}$$

In addition, we can determine the minimal number $N(\epsilon,\delta,\lambda=0)$ of tests required to verify the pure state $|\Psi\rangle$ within infidelity $\epsilon$ and significance level $\delta$ as defined in Eq. (11), with the result

$$N(\epsilon,\delta,\lambda=0) = \left\lceil \frac{1-\delta}{\epsilon\delta} \right\rceil. \tag{40}$$

Here the scaling with $1/\delta$ is suboptimal although the strategy is optimal for the nonadversarial scenario; cf. Sec. II A. Fortunately, nonsingular homogeneous strategies can achieve a better scaling behavior, as we shall see shortly.

### 2. Nonsingular homogeneous strategies

Here we assume $0 < \lambda < 1$, so the homogeneous strategy defined in Eq. (32) is nonsingular. In this case, $\eta_k(\lambda)$ decreases strictly monotonically with $k$ for $k \in \mathbb{Z}^{\geq 0}$, and $\zeta_k(\lambda)$ decreases strictly monotonically with $k$ for $k \in \{0,1,\ldots,N+1\}$. Define

$$c_k(\delta,\lambda) := \frac{\delta - \eta_{k+1}(\lambda)}{\eta_k(\lambda) - \eta_{k+1}(\lambda)}, \tag{41}$$

$$\begin{aligned} \zeta(N,\delta,\lambda,k) :=& c_k(\delta,\lambda)\zeta_k(\lambda) + [1 - c_k(\delta,\lambda)]\zeta_{k+1}(\lambda) \\ =& \frac{\lambda\{\delta[1+(N-k)(1-\lambda)] - \lambda^k\}}{(1-\lambda)[k+(N-k)\lambda]}. \end{aligned} \tag{42}$$

The following theorem clarifies the precision that can be achieved by a given number of tests; see Appendix C 2 for a proof.

*Theorem* 1. Suppose $0 < \lambda < 1$ and $0 < \delta \leq 1$. Then we have $F(N,\delta,\lambda) = \zeta(N,\delta,\lambda)/\delta$ with

$$\zeta(N,\delta,\lambda) = \begin{cases} 0 & \delta \leq \lambda^N, \\ \zeta(N,\delta,\lambda,k_*) & \delta > \lambda^N, \end{cases} \tag{43}$$

where $k_*$ is the largest integer $k$ that satisfies $\eta_k(\lambda) \geq \delta$.

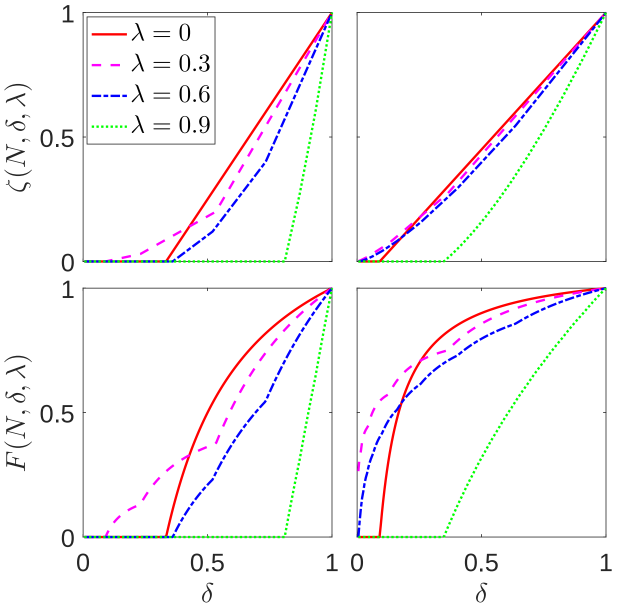

FIG. 2. (color online) Variations of $\zeta(N,\delta,\lambda)$ and $F(N,\delta,\lambda)$ with $\delta$ and $\lambda$ for $N = 2$ (left plots) and $N = 10$ (right plots).

The dependences of $\zeta(N,\delta,\lambda)$ and $F(N,\delta,\lambda)$ on $\delta$ and $\lambda$ are illustrated in Fig. 2. The choice of the parameter $k_*$ in Theorem 1 guarantees that $0 < c_{k_*}(\delta,\lambda) \leq 1$. Given the assumption $\lambda^N < \delta \leq 1$, we can deduce from Eq. (35) that $k_*$ is equal to either $k_+$ or $k_-$, where

$$k_+ :=\lceil \log_\lambda \delta \rceil, \quad k_- := \lfloor \log_\lambda \delta \rfloor. \tag{44}$$

When $k \in \{0, 1, \ldots, N\}$, Theorem 1 implies that

$$F(N, \delta = \lambda^k, \lambda) = \frac{(N-k)\lambda}{k + (N-k)\lambda}, \tag{45}$$

which decreases monotonically with $k$. In particular we have $F(N, \delta = 1, \lambda) = 1$ as expected; cf. Eq. (15). When $\delta = \eta_k(\lambda)$ with $k \in \{0, 1, \ldots, N+1\}$, we have

$$F(N, \delta = \eta_k(\lambda), \lambda) = \frac{\zeta_k(\lambda)}{\eta_k(\lambda)} = \frac{(N+1-k)\lambda}{k + (N+1-k)\lambda}, \tag{46}$$

which also decreases monotonically with $k$.

*Corollary* 1. Suppose $0 < \lambda < 1$ and $0 < \delta \leq 1$. Then

$$\zeta(N,\delta,\lambda) = \max\Big\{0, \max_{k\in\mathbb{Z}^{\geq 0}} \zeta(N,\delta,\lambda,k)\Big\} \tag{47}$$

$$= \max\{0, \zeta(N,\delta,\lambda,k_+), \zeta(N,\delta,\lambda,k_-\}. \tag{48}$$

Corollary 1 follows from Theorem 1 above and Lemma 16 in Appendix C. Equation (47) provides a family of lower bounds for $\zeta(N,\delta,\lambda)$, namely,

$$\zeta(N,\delta,\lambda) \geq \zeta(N,\delta,\lambda,k), \quad k \in \mathbb{Z}^{\geq 0}. \tag{49}$$

*Corollary* 2. Suppose $N \geq 1$, $0 < \lambda < 1$, and $\lambda^N \leq \delta < 1$. Then $F(N,\delta,\lambda)$ increases strictly monotonically with $\delta$ and $N$. In particular, $F(N+1,\delta,\lambda) > F(N,\delta,\lambda)$.

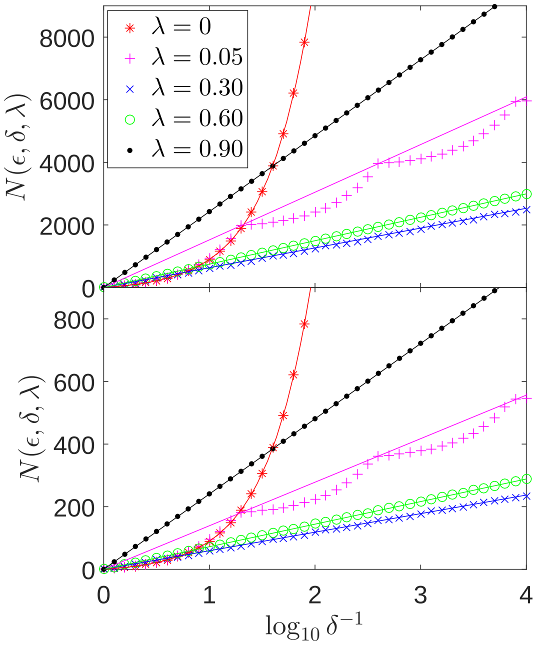

FIG. 3. (color online) Minimal numbers of tests required to verify a pure state with five different homogeneous strategies. Here $\epsilon = 0.01$ in the upper plot and $\epsilon = 0.1$ in the lower plot. In each plot, the red curve represents the approximate formula $(1-\delta)/(\epsilon\delta)$ when $\lambda = 0$; cf. Eq. (40). The four lines represent the approximate formula $(F + \lambda\epsilon)\log_{10}\delta/(\lambda\epsilon\log_{10}\lambda)$; cf. Eq. (64).

*Corollary* 3. Suppose $0 < \lambda < 1$ and $\lambda^N \leq \delta \leq 1$. Then

$$\frac{(N-k_+)\lambda}{k_+ + (N-k_+)\lambda} \leq F(N,\delta,\lambda) \leq \frac{(N-k_-)\lambda}{k_- + (N-k_-)\lambda}. \tag{50}$$

Corollary 2 follows from Theorem 1; the monotonicity with $\delta$ also follows from Lemma 3. Corollary 3 follows from Corollary 2 and Eq. (45).

Now, we are ready to determine the minimal number of tests required to verify the pure state $|\Psi\rangle$ within infidelity $\epsilon$ and significance level $\delta$. Theorems 2 and 3 below are proved in Appendix C 2. The results are illustrated in Figs. 3 and 4.

*Theorem* 2. Suppose $0 < \epsilon, \delta, \lambda < 1$. Then

$$N(\epsilon,\delta,\lambda) = \Big\lceil \min_{k\in\mathbb{Z}^{\geq 0}} \tilde{N}(\epsilon,\delta,\lambda,k) \Big\rceil = \lceil \tilde{N}(\epsilon,\delta,\lambda,k^*) \rceil, \tag{51}$$

where

$$\tilde{N}(\epsilon,\delta,\lambda,k) := \frac{k\nu^2\delta F + \lambda^{k+1} + \lambda\delta(k\nu - 1)}{\lambda\nu\delta\epsilon}, \tag{52}$$

with $F = 1-\epsilon$, $\nu = 1-\lambda$, and $k^*$ is the largest integer $k$ that satisfies $\delta \leq \lambda^k/(F\nu + \lambda) = \lambda^k/(F + \lambda\epsilon)$.

Suppose $k$ is a positive integer, then it is straightforward to verify that $\tilde{N}(\epsilon,\delta,\lambda,k) \leq \tilde{N}(\epsilon,\delta,\lambda,k-1)$ iff

$\delta \le \lambda^k/(F+\lambda\epsilon)$. In addition, we have

$$\frac{\lambda^{k_+ +1}}{F+\lambda\epsilon} < \delta < \frac{\lambda^{k_-}}{F+\lambda\epsilon} \tag{53}$$

given that $\lambda < F+\lambda\epsilon < 1$, which means $k^*$ in Eq. (51) is equal to either $k_+$ or $k_-$. Therefore, $N(\epsilon,\delta,\lambda)$ can also be expressed as follows,

$$N(\epsilon,\delta,\lambda) = \left\lceil \min\{\tilde{N}_+(\epsilon,\delta,\lambda), \tilde{N}_-(\epsilon,\delta,\lambda)\} \right\rceil \tag{54}$$

$$= \begin{cases} \lceil \tilde{N}_-(\epsilon,\delta,\lambda) \rceil & \delta \ge \frac{\lambda^{k_+}}{F+\lambda\epsilon}, \\ \lceil N_+(\epsilon,\delta,\lambda) \rceil & \delta \le \frac{\lambda^{k_+}}{F+\lambda\epsilon}, \end{cases} \tag{55}$$

where

$$\tilde{N}_\pm(\epsilon,\delta,\lambda) := \tilde{N}(\epsilon,\delta,\lambda,k_\pm). \tag{56}$$

The following corollary is an easy consequence of Theorem 2.

*Corollary* 4. Suppose $0<\epsilon,\delta,\lambda<1$. Then

$$N(\epsilon,\delta,\lambda) \le \lceil \tilde{N}(\epsilon,\delta,\lambda,k) \rceil \quad k \in \mathbb{Z}^{\ge 0}, \tag{57}$$

where the upper bound for a given $k$ is saturated when $\lambda^{k+1}/(F+\lambda\epsilon) \le \delta \le \lambda^k/(F+\lambda\epsilon)$.

The two cases $k=0,1$ in Eq. (57) are of special interest,

$$N(\epsilon,\delta,\lambda) \le \lceil \tilde{N}(\epsilon,\delta,\lambda,0) \rceil = \left\lceil \frac{1-\delta}{\nu\epsilon\delta} \right\rceil, \tag{58}$$

$$N(\epsilon,\delta,\lambda) \le \lceil \tilde{N}(\epsilon,\delta,\lambda,1) \rceil = \left\lceil \frac{\nu^2\delta F + \lambda^2 - \lambda^2\delta}{\lambda\nu\delta\epsilon} \right\rceil. \tag{59}$$

If $\lambda/(F+\lambda\epsilon) \le \delta < 1$, then Eq. (58) is saturated, so we have

$$N(\epsilon,\delta,\lambda) = \left\lceil \frac{1-\delta}{\nu\epsilon\delta} \right\rceil. \tag{60}$$

This result also holds when $\lambda = 0$ (as long as $0<\delta<1$) according to Eq. (40). If $\lambda^2/(F+\lambda\epsilon) \le \delta \le \lambda/(F+\lambda\epsilon)$, then Eq. (59) is saturated, so we have

$$N(\epsilon,\delta,\lambda) = \left\lceil \frac{\nu^2\delta F + \lambda^2 - \lambda^2\delta}{\lambda\nu\delta\epsilon} \right\rceil \ge \frac{2\sqrt{(1-\delta)F}}{\epsilon\sqrt{\delta}}, \tag{61}$$

where the lower bound is proved in Appendix C 2. Equations (60) and (61) show that homogeneous strategies with small $\lambda$, say $\lambda \le 0.1$, are not efficient when $\epsilon,\delta \le 0.1$, as reflected in Fig. 4.

The following theorem provides informative bounds for $N(\epsilon,\delta,\lambda)$, which complement the analytical formula in Theorem 2.

*Theorem* 3. Suppose $0<\epsilon,\delta,\lambda<1$. Then

$$k_- + \left\lceil \frac{k_- F}{\lambda\epsilon} \right\rceil \le N(\epsilon,\delta,\lambda) \le k_+ + \left\lceil \frac{k_+ F}{\lambda\epsilon} \right\rceil, \tag{62}$$

$$N(\epsilon,\delta,\lambda) \le \left\lceil \frac{\log_\lambda \delta}{\lambda\epsilon} - \frac{\nu k_-}{\lambda} \right\rceil = \left\lceil \frac{\ln\delta}{\lambda\epsilon\ln\lambda} - \frac{\nu k_-}{\lambda} \right\rceil. \tag{63}$$

All three bounds in Eqs. (62) and (63) are saturated when $\log_\lambda \delta$ is an integer.

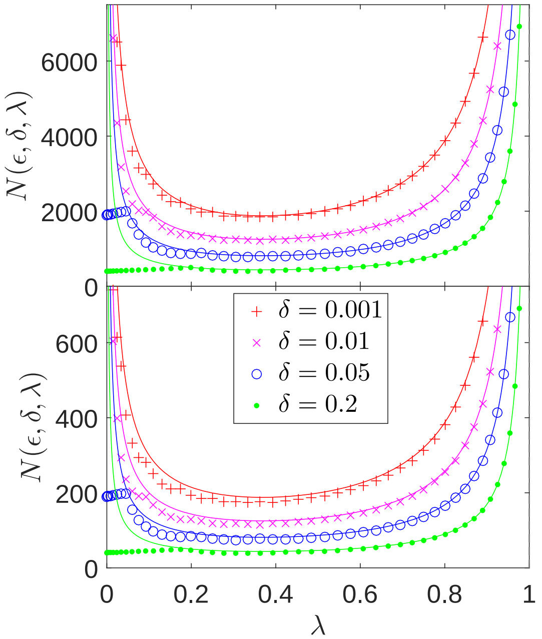

FIG. 4. (color online) Variation of $N(\epsilon,\delta,\lambda)$ with $\lambda$ and $\delta$. Here $\epsilon = 0.01$ in the upper plot and $\epsilon = 0.1$ in the lower plot. The four curves in each plot represent the approximate formula $\ln\delta/(\lambda\epsilon\ln\lambda)$; cf. Eqs. (66) and (68).

By virtue of Eq. (62), we can derive

$$\lim_{\delta\to 0} \frac{N(\epsilon,\delta,\lambda)}{\ln\delta^{-1}} = \frac{F+\lambda\epsilon}{\lambda\epsilon\ln\lambda^{-1}}, \tag{64}$$

$$\frac{k_-}{\lambda} \le \lim_{\epsilon\to 0} \epsilon N(\epsilon,\delta,\lambda) \le \frac{k_+}{\lambda}, \tag{65}$$

$$\lim_{\epsilon,\delta\to 0} \frac{\epsilon N(\epsilon,\delta,\lambda)}{\ln\delta^{-1}} = \frac{1}{\lambda\ln\lambda^{-1}}. \tag{66}$$

The exact value of $\lim_{\epsilon\to 0}\epsilon N(\epsilon,\delta,\lambda)$ can be derived from Eq. (55), with the result

$$\lim_{\epsilon\to 0}\epsilon N(\epsilon,\delta,\lambda) = \lim_{\epsilon\to 0}\epsilon\tilde{N}_-(\epsilon,\delta,\lambda) = \frac{k_-}{\lambda} + \frac{\lambda^{k_-}-\delta}{\nu\delta}, \tag{67}$$

note that the inequality $\delta \ge \lambda^{k_+}/(F+\lambda\epsilon)$ is always satisfied in the limit $\epsilon \to 0$ if $\log_\lambda \delta$ is not an integer.

### *3. Optimal homogeneous strategies*

In the adversarial scenario, the optimal performance can always be achieved by a homogeneous strategy if there is no restriction on the measurements. However, the value of $\lambda$ that minimizes $N(\epsilon,\delta,\lambda)$ depends on the target precision, as characterized by $\epsilon$ and $\delta$. We cannot find a homogeneous strategy that is optimal for all $\epsilon$ and $\delta$, unlike the nonadversarial scenario. Here we are mostly interested in the high precision limit, which means $\epsilon,\delta \to 0$.

In view of the above analysis, in the high-precision limit, the minimum number of tests can be approximated as follows,

$$N(\epsilon,\delta,\lambda)\approx(\lambda\epsilon)^{-1}\log_\lambda\delta=(\lambda\epsilon\ln\lambda)^{-1}\ln\delta. \tag{68}$$

To understand the condition of this approximation, note that $k_\pm\approx\log_\lambda\delta$ if $\delta\ll\lambda$, which is usually the case in high-precision verification. If in addition $\epsilon\ll 1$, then the ratio of the lower bound over the upper bound in Eq. (62) is close to 1, so that the two bounds are nearly tight with respect to relative deviation. In this case, Eq. (68) is a good approximation. Furthermore, numerical calculation shows that Eq. (68) is quite accurate for most parameter range of interest, as illustrated in Figs. 3 and 4. When $\lambda$ is very small, the approximation in Eq. (68) is not so good. On the other hand, homogeneous strategies with small $\lambda$, say $\lambda\leq 0.1$, are not efficient when $\epsilon,\delta\leq 0.1$ according to Eqs. (60) and (61), as illustrated in Fig. 4. Such strategies are not so important due to the reasons explained in Sec. III E.

Thanks to Theorems 2 and 3, the number of tests required by any nonsingular homogeneous strategy can achieve the same scaling behaviors with $\epsilon$ and $\delta$ as the counterparts in the nonadversarial scenario for high-precision state verification. In the limit $\epsilon,\delta\to 0$, the efficiency is characterized by the function $(\lambda\ln\lambda^{-1})^{-1}$. Analysis shows that the function $(\lambda\ln\lambda^{-1})^{-1}$ is convex for $0<\lambda<1$ and attains the minimum e when $\lambda=1/\mathrm{e}$, with e being the base of the natural logarithm. It is strictly decreasing in $\lambda$ when $0<\lambda<1/\mathrm{e}$ and strictly increasing when $1/\mathrm{e}<\lambda<1$; cf. Fig. 4. In particular, the homogeneous strategy with $\lambda=1/\mathrm{e}$, that is, $\nu=1-(1/\mathrm{e})$, is optimal in the high-precision limit $\epsilon,\delta\to 0$, in which case the number of tests reads

$$N(\epsilon,\delta,\lambda=\mathrm{e}^{-1})\approx\mathrm{e}\epsilon^{-1}\ln\delta^{-1}. \tag{69}$$

Compared with the minimum number $\epsilon^{-1}\ln\delta^{-1}$ for the nonadversarial scenario, the overhead is only e times.

Although we cannot find a value of $\lambda$ that is optimal for all $\epsilon$ and $\delta$, the optimal value usually lies in a neighborhood, say $[0.32,0.38]$, of $1/\mathrm{e}$ for the values of $\epsilon$ and $\delta$ that are of practical interest, say $\epsilon,\delta\leq 0.1$. In addition, $N(\epsilon,\delta,\lambda)$ varies quite slowly with $\lambda$ in this neighborhood, as illustrated in Fig. 4. So the choice $\lambda=1/\mathrm{e}$ is nearly optimal even if it is not optimal.

The above analysis shows that the optimal strategies for the adversarial scenario are very different from the counterpart for the nonadversarial scenario. Entangling measurements are less helpful and often unnecessary for realizing the optimal strategies. Consider bipartite pure states for example, the optimal strategies for high-precision verification can always be realized by virtue of local projective measurements [32–35].

In the rest of this section, we discuss briefly the scenario in which $\delta\to 0$, but $\epsilon$ is not necessarily so small, which is relevant to entanglement detection [34]. According to Eq. (64), in this case, the performance of the homogeneous strategy $\Omega$ is characterized by

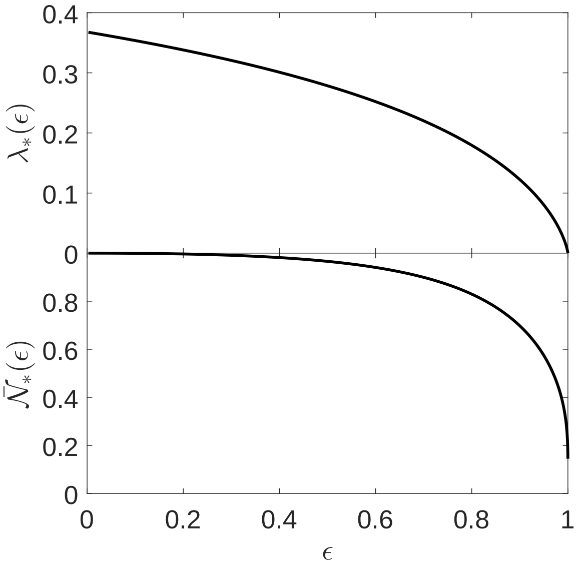

FIG. 5. Optimal homogeneous strategy in the limit $\delta\to 0$. Here $\lambda_*(\epsilon)$ denotes the value of $\lambda$ that minimizes $\mathcal{N}(\epsilon,\lambda)$ defined in Eq. (70), which determines the number of required tests. $\bar{\mathcal{N}}_*(\epsilon)$ denotes the number of tests normalized with respect to the benchmark, as defined in Eq. (76).

$$\mathcal{N}(\epsilon,\lambda):=\lim_{\delta\to 0}\frac{N(\epsilon,\delta,\lambda)}{\ln\delta^{-1}}=\frac{F+\lambda\epsilon}{\lambda\epsilon\ln\lambda^{-1}}, \tag{70}$$

where $F=1-\epsilon$. The partial derivative of $\mathcal{N}(\epsilon,\lambda)$ over $\lambda$ reads

$$\frac{\mathcal{N}(\epsilon,\lambda)}{\partial\lambda}=\frac{F+\lambda\epsilon+F\ln\lambda}{\lambda^2\epsilon(\ln\lambda)^2}. \tag{71}$$

For a given $\epsilon$ or $F$, the minimum of $\mathcal{N}(\epsilon,\lambda)$ is denoted by $\mathcal{N}_*(\epsilon)$. It is attained when $\lambda=\lambda_*(\epsilon)$, where $\lambda_*(\epsilon)$ is the unique solution of the equation

$$F+\lambda\epsilon+F\ln\lambda=0, \tag{72}$$

which amounts to

$$F=\frac{\lambda}{\ln\lambda^{-1}+\lambda-1}. \tag{73}$$

It is not difficult to verify that $\lambda_*(\epsilon)=0$ when $\epsilon=1$ ($F=0$) and $\lambda_*(\epsilon)=1/\mathrm{e}$ when $\epsilon=0$ ($F=1$); in addition, $\lambda_*(\epsilon)$ decreases monotonically with $\epsilon$ and is concave in $\epsilon$, as illustrated in Fig. 5. Therefore,

$$\mathrm{e}^{-1}F\leq\lambda_*(\epsilon)\leq\mathrm{e}^{-1}. \tag{74}$$

Next, we compare the efficiencies of different homogeneous strategies. As a benchmark, we take the homogeneous strategy with $\lambda=1/\mathrm{e}$, in which case we have

$$\mathcal{N}(\epsilon,\lambda=\mathrm{e}^{-1})=\frac{\mathrm{e}F+\epsilon}{\epsilon}. \tag{75}$$

Define

$$\bar{\mathcal{N}}(\epsilon,\lambda):=\frac{\mathcal{N}(\epsilon,\lambda)}{\mathcal{N}(\epsilon,\mathrm{e}^{-1})},\quad \bar{\mathcal{N}}_*(\epsilon):=\frac{\mathcal{N}_*(\epsilon)}{\mathcal{N}(\epsilon,\mathrm{e}^{-1})}. \tag{76}$$

Straightforward calculation shows that

$$\bar{\mathcal{N}}(\epsilon,\lambda)=\frac{F+\lambda\epsilon}{(\mathrm{e}F+\epsilon)\lambda\ln\lambda^{-1}}. \tag{77}$$

When $\lambda<1/\mathrm{e}$, $\bar{\mathcal{N}}(\epsilon,\lambda)$ decreases monotonically with $\epsilon$, so we have

$$\frac{1}{\ln\lambda^{-1}}\leq\bar{\mathcal{N}}(\epsilon,\lambda)\leq\frac{1}{\mathrm{e}\lambda\ln\lambda^{-1}}. \tag{78}$$

A homogeneous strategy $\Omega$ with a small $\beta(\Omega)$ could be significantly more efficient than the benchmark when $\epsilon$ is large ($F$ is small). When $\lambda>1/\mathrm{e}$, by contrast, $\bar{\mathcal{N}}(\epsilon,\lambda)$ increases monotonically with $\epsilon$, so we have

$$\frac{1}{\mathrm{e}\lambda\ln\lambda^{-1}}\leq\bar{\mathcal{N}}(\epsilon,\lambda)\leq\frac{1}{\ln\lambda^{-1}}. \tag{79}$$

In addition, calculation shows that

$$\bar{\mathcal{N}}_*(\epsilon):=\frac{1}{\mathrm{e}\lambda_*(\epsilon)-\ln\lambda_*(\epsilon)-1}. \tag{80}$$

According to the analysis on $\lambda_*(\epsilon)$, we can deduce that $\bar{\mathcal{N}}_*(\epsilon)$ decreases monotonically with $\epsilon$; it approaches 1 in the limit $\epsilon\to0$, while it approaches 0 (quite slowly) in the limit $\epsilon\to1$. Although $\bar{\mathcal{N}}_*(\epsilon)$ could be arbitrarily small when $\epsilon$ is large, it is close to 1 when $\epsilon$ is not too large, as illustrated in Fig. 5. For example, $\bar{\mathcal{N}}_*(\epsilon)\geq0.965$ when $\epsilon\leq0.5$ and $\bar{\mathcal{N}}_*(\epsilon)\geq0.999$ when $\epsilon\leq0.1$. Therefore, the homogeneous strategy $\Omega$ with $\beta(\Omega)=1/\mathrm{e}$ is nearly optimal for most parameter range of practical interest, as pointed out earlier.

### D. Efficiencies of general verification strategies

In this section we present our main results on the efficiencies of general verification strategies. The proofs are relegated to Appendices D and E to streamline the discussions. As we shall see shortly, the efficiency of a general verification operator $\Omega$ of a pure state $|\Psi\rangle$ is mainly determined by its second largest eigenvalue $\beta$ (or equivalently $\nu=1-\beta$) and the smallest eigenvalue $\tau$.

Define

$$\delta^*:=\frac{1+N\beta}{N+1}=\frac{1+N(1-\nu)}{N+1}. \tag{81}$$

Lemma 7 and Theorem 4 below are proved in Appendix D.

*Lemma* 7. Suppose $\Omega$ is a singular verification operator and $1/(N+1)\leq\delta\leq\delta^*$. Then

$$F(N,\delta,\Omega)\leq1-\frac{1}{\delta(N+1)}. \tag{82}$$

*Theorem* 4. Suppose $0<\delta\leq1$ and $0<\nu\leq1$. Then

$$F(N,\delta,\Omega)\geq1-\frac{1-\delta}{N\delta\nu}, \tag{83}$$

and the inequality is saturated when $\delta\geq\delta^*$. If $\nu\geq1/2$, then

$$F(N,\delta,\Omega)\geq1-\frac{1}{\delta(N+1)}, \tag{84}$$

and the inequality is saturated if $\Omega$ is singular and $\delta$ satisfies $1/(N+1)\leq\delta\leq\delta^*$.

The bound in Eq. (83) is positive if $\delta>1/(N\nu+1)$, while the one in Eq. (84) is positive if $\delta>1/(N+1)$. The two bounds coincide when $\delta=\delta^*$. Equation (83) is optimal when $\delta\geq\delta^*$, while Eq. (84) is better when $\delta<\delta^*$. The lower bound in Eq. (84) under the condition $\nu\geq1/2$ was also given in Ref. [7] under a slightly different situation. According to Lemma 7 and Theorem 4, if $\Omega$ is singular, then

$$F(N,\delta,\Omega)\leq\max\biggl\{0,1-\frac{1-\delta}{N\delta\nu},1-\frac{1}{\delta(N+1)}\biggr\}. \tag{85}$$

If $\nu\geq1/2$, by contrast, then the above inequality is reversed,

$$F(N,\delta,\Omega)\geq\max\biggl\{0,1-\frac{1-\delta}{N\delta\nu},1-\frac{1}{\delta(N+1)}\biggr\}. \tag{86}$$

If $\Omega$ is singular and meanwhile $\nu\geq1/2$, then the inequalities in Eqs. (85) and (86) are saturated.

*Corollary* 5. Suppose $0<\epsilon,\delta<1$ and $0<\nu\leq1$. Then

$$N(\epsilon,\delta,\Omega)\leq\biggl\lceil\frac{1-\delta}{\nu\delta\epsilon}\biggr\rceil. \tag{87}$$

If $\Omega$ is singular, then

$$N(\epsilon,\delta,\Omega)\geq\min\biggl\{\biggl\lceil\frac{1-\delta}{\nu\delta\epsilon}\biggr\rceil,\ \biggl\lceil\frac{1}{\delta\epsilon}-1\biggr\rceil\biggr\}, \tag{88}$$

If $\nu\geq1/2$, then

$$N(\epsilon,\delta,\Omega)\leq\min\biggl\{\biggl\lceil\frac{1-\delta}{\nu\delta\epsilon}\biggr\rceil,\ \biggl\lceil\frac{1}{\delta\epsilon}-1\biggr\rceil\biggr\}. \tag{89}$$

Corollary 5 is an easy consequence of Theorem 4 and Eqs. (85), (86). If $\Omega$ is singular and meanwhile $\nu\geq1/2$, then the inequalities in Eqs. (88) and (89) are saturated, and we have

$$N(\epsilon,\delta,\Omega)=\min\biggl\{\biggl\lceil\frac{1-\delta}{\nu\delta\epsilon}\biggr\rceil,\ \biggl\lceil\frac{1}{\delta\epsilon}-1\biggr\rceil\biggr\}, \tag{90}$$

which generalizes Eq. (40). The number of tests characterized by the upper bound in Eq. (87) is much smaller than what can be achieved by previous approaches that are based on quantum de Finetti theorem [23, 42]. Nevertheless, the scaling with $1/\delta$ is still suboptimal compared with the counterpart for the nonadversarial scenario.

In the rest of this section we shall provide an even better bound on the number of tests when $\Omega$ is nonsingular. Lemma 8 and Theorem 5 below are proved in Appendix E.

*Lemma* 8. Suppose $\Omega$ is positive definite. Then

$$\mathcal{F}(N,f,\Omega)\geq\frac{N+1-(\ln\beta)^{-1}\ln f}{N+1-(\ln\beta)^{-1}\ln f-h\ln f},\tag{91}$$

where

$$\begin{aligned}h=h(\Omega)&:=\max_{j\geq2}\bigl(\lambda_j\ln\lambda_j^{-1}\bigr)^{-1}\\&=\bigl[\min\{\beta\ln\beta^{-1},\tau\ln\tau^{-1}\}\bigr]^{-1}.\end{aligned}\tag{92}$$

Define

$$\tilde{\beta}:=\begin{cases}\beta, & \beta\ln\beta^{-1}\leq\tau\ln\tau,\\ \tau, & \beta\ln\beta^{-1}>\tau\ln\tau.\end{cases}\tag{93}$$

Then we have $h=\bigl(\tilde{\beta}\ln\tilde{\beta}^{-1}\bigr)^{-1}$. Note that the lower bound in Eq. (91) increases monotonically with $N$ as expected. Lemma 8 is very useful to studying quantum state verification in the adversarial scenario. It should be pointed out that many results derived for homogeneous strategies can not be applied directly to general strategies, so here we have to resort to a different approach.

*Theorem* 5. Suppose $\Omega$ is positive definite. Then

$$N(\epsilon,\delta,\Omega)\geq N(\epsilon,\delta,\lambda_j)\geq k_-(\lambda_j)+\left\lfloor\frac{k_-(\lambda_j)F}{\lambda_j\epsilon}\right\rfloor,\quad j=2,3,\ldots,D,\tag{94}$$

$$k_-(\tilde{\beta})+\left\lfloor\frac{k_-(\tilde{\beta})F}{\tilde{\beta}\epsilon}\right\rfloor\leq N(\epsilon,\delta,\Omega)\leq\left\lceil\frac{hF\ln(F\delta)^{-1}}{\epsilon}+\frac{\ln(F\delta)}{\ln\beta}-1\right\rceil<\frac{h\ln(F\delta)^{-1}}{\epsilon},\tag{95}$$

where $\lambda_j$ are the eigenvalues of $\Omega$, $F=1-\epsilon$, $k_-(\lambda_j)=\lfloor\ln\delta/\ln\lambda_j\rfloor$ for $j=2,3,\ldots,D$, $k_-(\tilde{\beta})=\lfloor\ln\delta/\ln\tilde{\beta}\rfloor$, and $h=\bigl(\tilde{\beta}\ln\tilde{\beta}^{-1}\bigr)^{-1}$, with $\tilde{\beta}$ defined in Eq. (93).

Suppose $\tau(\Omega)$ is bounded from below by a positive constant. Then the ratio of the lower bound over the upper bound in Eq. (95) approaches 1 in the high-precision limit $\epsilon,\delta\to0$, so the two bounds are nearly tight, as in the case of homogeneous strategies. Therefore, $N(\epsilon,\delta,\Omega)$ can be approximated as follows,

$$N(\epsilon,\delta,\Omega)\approx\frac{h\ln(\delta^{-1})}{\epsilon}=\frac{\ln\delta}{\epsilon\tilde{\beta}\ln\tilde{\beta}}.\tag{96}$$

The number of tests has the same scaling behavior with $\epsilon^{-1}$ and $\delta^{-1}$ as the number for the nonadversarial scenario presented in Eq. (3), except for an overhead characterized by $\nu h$. In addition, $\Omega$ is not efficient when $\tau(\Omega)$ is small compared with $\epsilon,\delta$ according to Eq. (94) and the discussion on homogeneous strategies in Sec. III C 2. Also, the scaling behavior with $\delta^{-1}$ is worse when $\Omega$ is singular according to Eq. (88).

The above analysis can be extended to the scenario in which we want to verify whether the support of the resultant state belongs to a certain subspace $\mathcal{K}$. In this case, we need to replace the projector $|\Psi\rangle\langle\Psi|$ by the projector $P$ onto the subspace $\mathcal{K}$, impose the condition $P_lP=P$, and redefine $f_\rho$ as $\operatorname{tr}[(\Omega^{\otimes N}\otimes P)\rho]$. Such extension is useful when we want to verify whether the resultant state is correctable in a fault-tolerant way [38].

### E. Power of the trivial test

According to Sec. III D, the number $N(\epsilon,\delta,\Omega)$ of tests required to verify a pure state in the adversarial scenario has the same scaling behavior with $\epsilon^{-1}$ and $\delta^{-1}$ as the number for the nonadversarial scenario as long as the verification operator $\Omega$ is nonsingular, and its smallest eigenvalue $\tau$ is bounded from below by a positive constant. However, the scaling behavior of $N(\epsilon,\delta,\Omega)$ with $\delta$ is suboptimal when $\Omega$ is singular, that is, $\tau=0$. Similarly, the efficiency is limited when $\tau$ is nonzero, but very small. Here we provide a simple recipe to reducing the number of tests significantly, so that pure states can be verified in the adversarial scenario with high precision and with almost the same efficiency as in the nonadversarial scenario. Surprisingly, all we need to do is to perform the trivial test with a suitable probability. By "trivial test" we mean the test whose test projector $P$ is equal to the identity operator, that is $P=1$, so that all the states can pass the test with certainty. Our main task in the rest of this section is to determine the optimal probability for performing the trivial test.

Suppose $\Omega$ is a verification operator for the pure state $|\Psi\rangle$. Based on $\Omega$, we can construct a new verification operator as follows,

$$\Omega_p=(1-p)\Omega+p,\quad 0\leq p<1,\tag{97}$$

which means the trivial test is performed with probability $0\leq p<1$ and $\Omega$ is performed with probability $1-p$.

Denote by $\beta_p$ and $\tau_p$ the second largest eigenvalue a the smallest eigenvalue of $\Omega_p$, respectively. Then

$$\beta_p=(1-p)\beta+p,\quad \tau_p=(1-p)\tau+p,$$ (9

where $\beta$ and $\tau$ are the second largest eigenvalue a smallest eigenvalue of $\Omega$, respectively, which satisfy t inequality $\tau\leq\beta$. Here we view $\beta_p$ as a function $\nu=1-\beta$ and $p$.

According to Sec. II A, the trivial test can only decrea the efficiency in the nonadversarial scenario. In hig precision verification for example, the number of tes required by $\Omega_p$ is about $1/(1-p)$ times the number r quired by $\Omega$ according to Eq. (3). In sharp contrast, t trivial test can increase the efficiency in the adversar scenario by hedging the influence of small eigenvalues $\Omega$. Therefore, $\Omega_p$ is called a *hedged verification operat* of $\Omega$.

According to Eq. (95), to verify $|\Psi\rangle$ within infidelity and significance level $\delta$, the number of tests required the strategy $\Omega_p$ (assuming $\tau_p>0$) satisfies

$$N(\epsilon,\delta,\Omega_p)<\frac{h(p,\nu,\tau)\ln(F\delta)^{-1}}{\epsilon},$$ (9

where $F=1-\epsilon$ and

$$h(p,\nu,\tau)=h(\Omega_p)=\left[\min\left\{\beta_p\ln\beta_p^{-1},\tau_p\ln\tau_p^{-1}\right\}\right]^{-1}. \tag{100}$$

Compared with the number in Eq. (3) for the nonadversarial scenario, the overhead is upper bounded as follows,

$$\frac{N(\epsilon,\delta,\Omega_p)}{N_{\mathrm{NA}}(\epsilon,\delta,\Omega)}<\nu h(p,\nu,\tau)\frac{\ln[(F\delta)^{-1}]\ln(1-\nu\epsilon)}{\nu\epsilon\ln\delta}. \tag{101}$$

It is straightforward to verify that this bound decreases monotonically with $1/\epsilon$ and $1/\delta$. It turns out that the bound also decreases monotonically with $1/\nu$ according to Lemmas 9 and 10 below. When $\epsilon$ and $\delta$ approach zero, the bound in Eq. (99) becomes tight (with respect to relative deviation) according to Eq. (95), so we have

$$\lim_{\epsilon,\delta\to0,}\frac{N(\epsilon,\delta,\Omega_p)}{N_{\mathrm{NA}}(\epsilon,\delta,\Omega)}=\nu h(p,\nu,\tau). \tag{102}$$

This equation corroborates the significance of the function $\nu h(p,\nu,\tau)$ for characterizing the overhead of high-precision state verification in the adversarial scenario.

To achieve high performance, we need to choose a suitable value of $p$ so as to minimize $h(p,\nu,\tau)$. To this end, it is instructive to recall that the function $x\ln x^{-1}$ is concave for $0\leq x\leq1$ and is strictly increasing in $x$ when $0\leq x<1/\mathrm{e}$, while it is strictly decreasing when $1/\mathrm{e}<x\leq1$; it attains the maximum $1/\mathrm{e}$ when $x=1/\mathrm{e}$. Accordingly, $h(p,\nu,\tau)$ has a tight lower bound,

$$h(p,\nu,\tau)\geq\mathrm{e}, \tag{103}$$

and the bound can be saturated only if $\tau=1-\nu\leq1/\mathrm{e}$ and $p=(\mathrm{e}\nu-\mathrm{e}+1)/(\mathrm{e}\nu)$; cf. Eqs. (105) and (106) below.

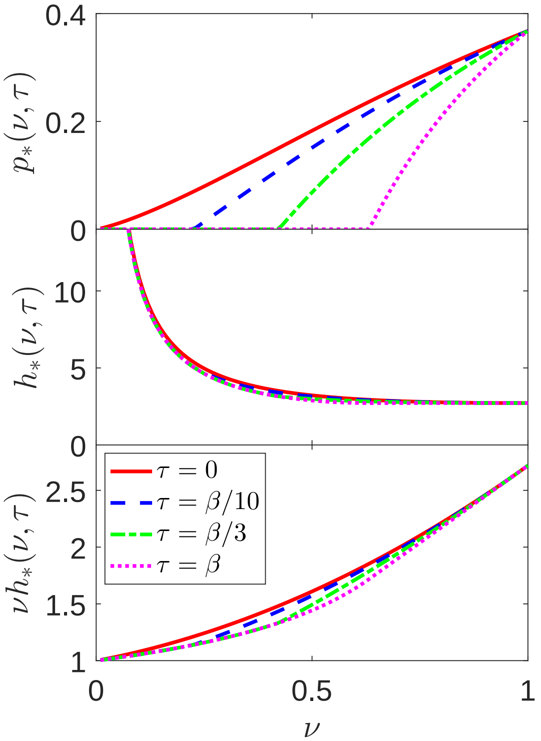

FIG. 6. (color online) The optimal probability $p_*(\nu,\tau)$ for performing the trivial test (upper plot), the prefactor $h_*(\nu,\tau)$ (middle plot), and the overhead $\nu h_*(\nu,\tau)$ (lower plot) for high-precision state verification in the adversarial scenario.

Given the value of $\nu=1-\beta$ and $\tau$ with $\nu+\tau\leq1$, $h(p,\nu,\tau)$ has a unique minimizer in $p$, which is denoted by $p_*(\nu,\tau)$ or $p_*$ henceforth; cf. Fig. 6. By definition we have

$$h(p_*,\nu,\tau)=h_*(\nu,\tau):=\min_{0\leq p<1}h(p,\nu,\tau). \tag{104}$$

In addition, $p_*$ is the smallest value of $p\geq0$ such that $(\tau_p\ln\tau_p^{-1})^{-1}\leq(\beta_p\ln\beta_p^{-1})^{-1}$, that is, $\tau_p\ln\tau_p^{-1}\geq\beta_p\ln\beta_p^{-1}$. This observation implies that $\beta_{p_*}\geq1/\mathrm{e}$; by contrast, $\tau_{p_*}\leq1/\mathrm{e}$ if $\tau\leq1/\mathrm{e}$.

When the strategy $\Omega$ is homogeneous, that is, when $\tau=\beta=1-\nu$, it is straightforward to derive the following result

$$p_*(\nu,1-\nu)=\begin{cases}0 & 0<\nu\leq1-\frac{1}{\mathrm{e}},\\ \frac{\mathrm{e}\nu-\mathrm{e}+1}{\mathrm{e}\nu} & 1-\frac{1}{\mathrm{e}}\leq\nu\leq1;\end{cases} \tag{105}$$

$$h_*(\nu,1-\nu)=\begin{cases}(\beta\ln\beta^{-1})^{-1} & 0<\nu\leq1-\frac{1}{\mathrm{e}},\\ \mathrm{e} & 1-\frac{1}{\mathrm{e}}\leq\nu\leq1.\end{cases} \tag{106}$$

In this case $\Omega_p$ is also homogeneous, so the results presented in Sec. III C can be applied directly.

*Lemma* 9. Suppose $0<\nu\leq1$. Then $p_*(\nu,1-\nu)$ is nondecreasing in $\nu$, $h_*(\nu,1-\nu)$ is nonincreasing in $\nu$, and $\nu h_*(\nu,1-\nu)$ is strictly increasing in $\nu$. Meanwhile, $\nu h_*(\nu,1-\nu)>1$ and $\lim_{\nu\to0}\nu h_*(\nu,1-\nu)=1$. If in addition $0 \le p < 1$ and $1-\nu+p\nu > 0$, then $\nu h(p,\nu,1-\nu)$ is strictly increasing in $\nu$.

*Lemma* 10. Suppose $\nu$ and $\tau$ satisfy the following conditions $0 < \nu \le 1$, $0 \le \tau < 1$, and $\nu + \tau \le 1$. Then

1. $p_*(\nu,\tau)$ is nondecreasing in $\nu$ and nonincreasing in $\tau$.
2. $h_*(\nu,\tau)$ is nonincreasing in both $\nu$ and $\tau$.
3. $\nu h_*(\nu,\tau) > 1$.
4. $\lim_{\nu\to 0} \nu h_*(\nu,\tau) = 1$.
5. $\nu h_*(\nu,\tau)$ is strictly increasing in $\nu$.

If in addition $0 \le p < 1$ and $\tau_p = (1-p)\tau + p > 0$, then

6. $h(p,\nu,\tau)$ is nonincreasing in both $\nu$ and $\tau$.
7. $\nu h(p,\nu,\tau)$ is strictly increasing in $\nu$.

Lemmas 9 and 10 are proved in Appendix F. In Lemma 10 we assume that $\nu$ and $\tau$ can vary independently, which means the dimension of the Hilbert space $\mathcal{H}$ on which $\Omega$ acts has dimension at least 3. Incidentally, if $\mathcal{H}$ has dimension 2, then $\Omega$ is always homogeneous and $\tau = 1-\nu$. Lemmas 9 and 10 summarize the main properties of $p_*(\nu,\tau)$, $h(p,\nu,\tau)$, and $h_*(\nu,\tau)$, which are very instructive to understanding quantum state verification in the adversarial scenario. In particular Lemma 10 reveals that the overhead $\nu h_*(\nu,\tau)$ in the number of tests becomes negligible when $\nu$ approaches 0, as illustrated in Fig. 6. To be concrete, calculation shows that $\nu h_*(\nu,\tau) \le 1.09, 1.19, 1.31, 1.45, 1.61$ when $\nu \le 0.1, 0.2, 0.3, 0.4, 0.5$, respectively.

Lemma 10 also implies that

$$h_*(\nu,1-\nu) \le h(p,\nu,\tau) \le h_*(\nu) \tag{107}$$

as long as $p_*(\nu,\tau) \le p \le p_*(\nu)$, where $p_*(\nu) := p_*(\nu,0)$ and $h_*(\nu) := h_*(\nu,0)$. When $p = p_*(\nu)$, we have a stronger conclusion, namely,

$$h(p_*(\nu),\nu,\tau) = h_*(\nu). \tag{108}$$

Lemma 10 and Eq. (105) together yield an upper bound for $p_*(\nu,\tau)$,

$$p_*(\nu,\tau) \le 1/\mathrm{e}, \tag{109}$$

and the bound is saturated iff $\nu = 1$, $\tau = 0$. As a consequence, we have $1/[1-p_*(\nu,\tau)] \le \mathrm{e}/(\mathrm{e}-1) < 1.6$, so the number of tests required by $\Omega_{p_*}$ is at most 60% more than the number required by $\Omega$ for high-precision verification in the nonadversarial scenario although here we are mainly interested in the adversarial scenario. By contrast, Lemma 10 and Eq. (106) yield a lower bound for $h_*(\nu,\tau)$,

$$h_*(\nu,\tau) \ge \begin{cases} (\beta \ln \beta^{-1})^{-1} & 0 < \nu \le 1 - \frac{1}{\mathrm{e}}, \\ \mathrm{e} & 1 - \frac{1}{\mathrm{e}} < \nu < 1. \end{cases} \tag{110}$$

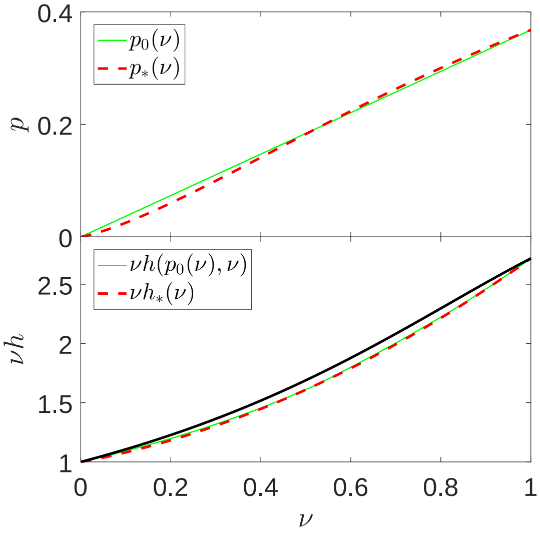

FIG. 7. (color online) The optimal probability $p_*(\nu,\tau)$ for performing the trivial test in high-precision state verification and a pretty-good approximation $p_0(\nu)$ (upper plot). Variations of $\nu h_*(\nu)$ and its upper bound $\nu h(p_0(\nu),\nu)$ with $\nu$ (lower plot). The black solid line represents an upper bound for $\nu h(p_0(\nu),\nu)$ presented in Eq. (115).

When $\tau > 0$ and $\tau \ln \tau^{-1} \ge \beta \ln \beta^{-1}$, we have

$$p_*(\nu,\tau) = 0, \quad h_*(\nu,\tau) = (\beta \ln \beta^{-1})^{-1}. \tag{111}$$

So there is no need to perform the trivial test. When $\tau \ln \tau^{-1} < \beta \ln \beta^{-1}$ (including the case $\tau = 0$), which implies that $\tau < 1/\mathrm{e}$, the probability $p_*(\nu,\tau)$ happens to be the unique solution of the equation

$$\beta_p \ln \beta_p = \tau_p \ln \tau_p, \quad 0 < p < 1. \tag{112}$$

In this case, it is beneficial to perform the trivial test with a suitable probability. The inequality $\tau \ln \tau^{-1} < \beta \ln \beta^{-1}$ is thus an indication that $\tau$ is too small. It is not easy to derive an analytical formula for $p_*$, but it is very easy to determine $p_*$ numerically.

In view of Lemma 10, singular verification operator $\Omega$ with $\tau = 0$ is of special interest because the overhead $\nu h_*(\nu,\tau)$ for a given $\nu$ is maximized when $\tau = 0$. In this case, we can provide a pretty good approximation for $p_*(\nu) = p_*(\nu,0)$, namely,

$$p_0 = p_0(\nu) = \frac{\nu}{\mathrm{e}} = \frac{1-\beta}{\mathrm{e}}, \tag{113}$$

which is exact when $\nu = 1$, as illustrated in Fig. 7.

*Lemma* 11. Suppose $0 < \nu \leq 1$ and let $h(p_0, \nu) := h(p_0, \nu, 0)$. Then

$$h_*(\nu) \leq h(p_0, \nu) \leq \Big[\Big(1 - \nu + \frac{\nu^2}{\mathrm{e}}\Big)\nu\Big]^{-1} \leq \frac{1}{\nu} + (\mathrm{e} - 1) \leq \frac{\mathrm{e}}{\nu}, \tag{114}$$

$$\nu h_*(\nu) \leq \nu h(p_0, \nu) \leq \Big(1 - \nu + \frac{\nu^2}{\mathrm{e}}\Big)^{-1} \leq 1 + (\mathrm{e} - 1)\nu \leq \mathrm{e}. \tag{115}$$

Lemma 11 is proved in Appendix F. Calculation shows that the difference between $\nu h(p_0, \nu)$ and $\nu h_*(\nu)$ is less than 2% (cf. Fig. 7); therefore, $p_0$ is indeed a good approximation for $p_*(\nu)$. According to Lemma 10, $h_*(\nu)$ is an upper bound for $h_*(\nu, \tau)$ and $h(p, \nu, \tau)$ with $p_*(\nu, \tau) \leq p \leq p_*(\nu)$, while $h(p_0(\nu), \nu)$ is an upper bound for $h(p_0(\nu), \nu, \tau)$. So Lemma 11 has implications for all verification operators. The following theorem is an implication of Lemma 11 and Eq. (99).

*Theorem* 6. Suppose $\Omega$ is a verification operator for $|\Psi\rangle$, $\nu = \nu(\Omega)$, and $\tau = \tau(\Omega)$. If $p = \nu/\mathrm{e}$, then

$$N(\epsilon, \delta, \Omega_p) < \frac{h(p, \nu, \tau)\ln(F\delta)^{-1}}{\epsilon} \leq \frac{h(p, \nu)\ln(F\delta)^{-1}}{\epsilon} \leq \frac{\ln[(F\delta)^{-1}]}{\nu(1 - \nu + \mathrm{e}^{-1}\nu^2)\epsilon} \leq \frac{(1 + \mathrm{e}\nu - \nu)\ln[(F\delta)^{-1}]}{\nu\epsilon}, \tag{116}$$

where $F = 1 - \epsilon$. If $p_*(\nu, \tau) \leq p \leq p_*(\nu)$, then

$$N(\epsilon, \delta, \Omega_p) < \frac{h(p, \nu, \tau)\ln(F\delta)^{-1}}{\epsilon} \leq \frac{h_*(\nu)\ln(F\delta)^{-1}}{\epsilon} \leq \frac{\ln[(F\delta)^{-1}]}{\nu(1 - \nu + \mathrm{e}^{-1}\nu^2)\epsilon} \leq \frac{(1 + \mathrm{e}\nu - \nu)\ln[(F\delta)^{-1}]}{\nu\epsilon}. \tag{117}$$

In conjunction with Eq. (3) or Eq. (101), Theorem 6 sets a general upper bound on the overhead of state verification in the adversarial scenario. If $p = \nu/\mathrm{e}$ or $p_*(\nu, \tau) \leq p \leq p_*(\nu)$ for example, then

$$\frac{N(\epsilon, \delta, \Omega_p)}{N_{\mathrm{NA}}(\epsilon, \delta, \Omega)} < \nu h(p, \nu, \tau)\frac{\ln[(F\delta)^{-1}]\ln(1 - \nu\epsilon)}{\nu\epsilon\ln\delta} \leq \frac{\ln[(F\delta)^{-1}]\ln(1 - \nu\epsilon)}{(1 - \nu + \mathrm{e}^{-1}\nu^2)\nu\epsilon\ln\delta} \leq \frac{(1 + \mathrm{e}\nu - \nu)\ln[(F\delta)^{-1}]\ln(1 - \nu\epsilon)}{\nu\epsilon\ln\delta}. \tag{118}$$

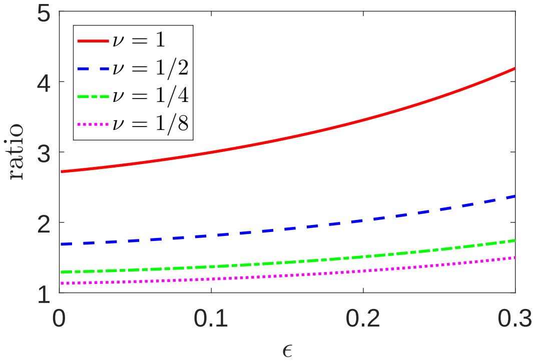

FIG. 8. (color online) Upper bound on the ratio of $N(\epsilon, \delta, \Omega_{p_*})$ over $N_{\mathrm{NA}}(\epsilon, \delta, \Omega)$, which characterizes the overhead of state verification in the adversarial scenario. Here $\delta = \epsilon$ and $\tau = 0$.

By virtue of Lemmas 9 and 10, it is straightforward to verify that all three bounds in Eq. (118) decrease monotonically with $1/\epsilon$, $1/\delta$, and $1/\nu$, as illustrated in Figs. 6 and 8. Theorem 6 has profound implications for state verification in the adversarial scenario. With the help of the trivial test, the number of tests can achieve the same scaling behavior with $\epsilon^{-1}$ and $\delta^{-1}$ as the number for the nonadversarial scenario presented in Eq. (3). The overhead is at most four times when $\epsilon, \delta \leq 1/4$ and three times when $\epsilon, \delta \leq 1/10$; furthermore, the overhead becomes negligible when $\nu, \epsilon, \delta$ approach zero. Therefore, pure states can be verified in the adversarial scenario with almost the same efficiency as in the nonadversarial scenario.

Although the performance of $\Omega$ is very sensitive to the smallest eigenvalue $\tau$, surprisingly, the performance of $\Omega_{p_*}$ is not sensitive to $\tau$ at all. According to Lemma 10, the difference between $h_*(\nu, \tau_1)$ and $h_*(\nu, \tau_2)$ for a given $\nu$ is maximized when $\tau_1 = 0$ (cf. Eq. (114)) and $\tau_2 = 1 - \nu$ (cf. Eq. (106)). Calculation shows that the difference between $h_*(\nu)$ and $h_*(\nu, 1 - \nu)$ is less than 12%, and it is even smaller when $\nu$ is close to zero or close to 1, as illustrated in Fig. 6. Therefore, the influence of $\tau$ on the performance of $\Omega_{p_*}$ can be neglected to a large extent. Moreover, the probability $p$ for performing the trivial test can be chosen without even knowing the value of $\tau$, while achieving nearly optimal performance. Actually, the choices $p = p_*(\nu)$ and $p = p_0(\nu) = \nu/\mathrm{e}$ are both nearly optimal. These observations are very helpful to constructing efficient verification protocols because we can focus on $\nu$ without worrying about the impact of $\tau$ or even knowing the value of $\tau$. Suppose $\Omega$ is a verification operator with the largest possible $\nu$ (under given conditions), then $\Omega_p$ is guaranteed to be nearly optimal, where $p$ can be chosen to be $p_*(\nu, \tau)$, $p_*(\nu)$, or $p_0(\nu) = \nu/\mathrm{e}$. Without this insight, it would be much more difficult to devise efficient verification protocols.

## IV. HYPERGRAPHS AND HYPERGRAPH STATES

In preparation for later study, here we briefly review hypergraphs and hypergraph states [17, 18]. In addition, we introduce the concepts of independence cover and cover strength together with a number of graph theoretic results, which will play important roles in the verification of hypergraph states.

### A. Hypergraphs

A hypergraph $G = (V, E)$ is characterized by a set of vertices $V = \{1, 2, \ldots, n\}$ and a set of hyperedges $E \subset \mathscr{P}(V)$, where $\mathscr{P}(V)$ is the power set of $V$ [17, 18]; see Fig. 9 for some examples. The order of a hyperedge is the number of vertices it connects, and the order of a hypergraph is the maximal order of its hyperedges. A graph is a special hypergraph in which all hyperedges have order 2 as ordinary edges. Two distinct vertices of $G$ are adjacent if they are connected by a hyperedge. The degree $\deg(j)$ of a vertex $j$ is the number of vertices that are adjacent to it; the degree $\Delta(G)$ of $G$ is the maximal vertex degree. A subset of the vertex set $V$ is a clique if every two vertices in the set are adjacent. The clique number $\varpi(G)$ of $G$ is the maximal number of vertices over all cliques. By contrast, a subset is an independent set if no two vertices are adjacent. The independence number $\alpha(G)$ of $G$ is the maximal number of vertices over all independent sets.

A set $\mathscr{A} = \{A_1, A_2, \ldots, A_m\}$ of independent sets of $G$ is an independence cover if $\cup_{l=1}^m A_l = V$. The cover $\mathscr{A}$ also defines a coloring of $G$ with $m$ colors when $\mathscr{A}$ forms a partition of $V$, that is, when $A_l$ are pairwise disjoint (assuming no $A_l$ is empty). A hypergraph $G$ is $k$-colorable if its vertices can be colored using $k$ different colors such that any two adjacent vertices are assigned with different colors. A 2-colorable graph is also called a bipartite graph. The chromatic number $\chi(G)$ of $G$ is the minimal number of colors in any coloring of $G$ or, equivalently, the minimal number of elements in any independence cover of $G$.

A weighted independence cover $(\mathscr{A}, \mu)$ of $G$ is a cover together with weights $\mu_l$ for $A_l \in \mathscr{A}$. Throughout this paper, we assume that $\mu_l$ form a probability distribution, that is, $\mu_l \geq 0$ and $\sum_l \mu_l = 1$. The cover strength of the cover $(\mathscr{A}, \mu)$ is defined as

$$s(\mathscr{A}, \mu) = \min_{j\in V} \sum_{l|A_l \ni j} \mu_l. \tag{119}$$

The independence degree $\gamma(G)$ of $G$ is the maximum of $s(\mathscr{A}, \mu)$ over all weighted independence covers. As we shall see in Sec. V, any weighted independence cover of $G$ can be used to construct a verification protocol for the hypergraph state associated with $G$ in which the cover strength determines the spectral gap and thus the verification efficiency (cf. Theorem 7 below). The degrees $\Delta(G)$, clique numbers $\varpi(G)$, independence numbers $\alpha(G)$, chromatic numbers $\chi(G)$, and independence degrees $\gamma(G)$ of common graphs and hypergraphs are displayed in Table I.

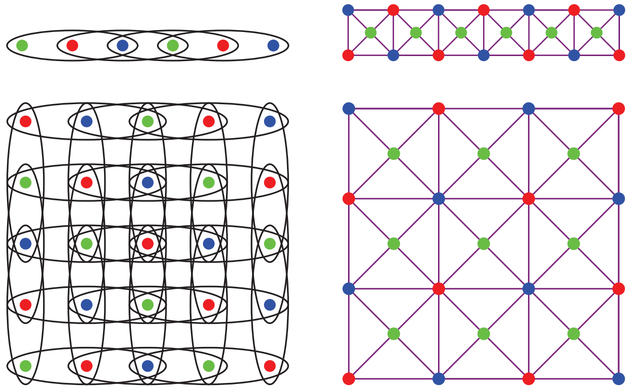

FIG. 9. (color online) Examples of hypergraphs and associated hypergraph states. Left plot: 1D and 2D order-3 cluster states; every three neighboring vertices on a row or column are connected by an order-3 hyperedge. Right plot: Union Jack states on a chain and on a 2D lattice, respectively; the three vertices of each elementary triangle are connected by an order-3 hyperedge [21]. All four hypergraphs are 3-colorable as illustrated.

TABLE I. Degrees $\Delta(G)$, clique numbers $\varpi(G)$, independence numbers $\alpha(G)$, chromatic numbers $\chi(G)$, and independence degrees $\gamma(G)$ of common graphs and hypergraphs of $n$ vertices. A graph is complete if every two vertices are adjacent. Note that the odd cycle of three vertices is complete. Here we assume that each 2-colorable graph has at least one edge, while each 3-colorable hypergraph has at least one hyperedge of order 3, as illustrated in Fig. 9.

| hypergraphs $G$ | $\Delta(G)$ | $\varpi(G)$ | $\alpha(G)$ | $\chi(G)$ | $\gamma(G)$ |
|---|---|---|---|---|---|
| square lattice | 4 | 2 | $\lceil n/2 \rceil$ | 2 | 1/2 |
| cubic lattice in dimension $k$ | $2k$ | 2 | $\lceil n/2 \rceil$ | 2 | 1/2 |
| triangular lattice | 6 | 3 | $\geq n/3$ | 3 | 1/3 |
| even cycle | 2 | 2 | $n/2$ | 2 | 1/2 |
| odd cycle ($n \geq 5$) | 2 | 2 | $(n-1)/2$ | 3 | $(n-1)/(2n)$ |
| complete graph | $n-1$ | $n$ | 1 | $n$ | $1/n$ |
| 2-colorable graph | - | 2 | $\geq n/2$ | 2 | 1/2 |
| 3-colorable hypergraph | - | 3 | $\geq n/3$ | 3 | 1/3 |

In view of the significance of cover strength and independence degree, it is not surprising that the following proposition will play an important role in studying the verification of hypergraph states.

*Proposition* 2. Any hypergraph $G = (V, E)$ satisfies

$$\frac{1}{\Delta(G)+1} \leq \frac{1}{\chi(G)} \leq \gamma(G) \leq \min\left\{\frac{\alpha(G)}{|V|}, \frac{1}{\varpi(G)}\right\}. \tag{120}$$

*Proof.* The inequality $\frac{1}{\Delta(G)+1} \leq \frac{1}{\chi(G)}$, that is, $\chi(G) \leq \Delta(G)+1$, follows from a well-known greedy algorithm which produces a coloring of $G$ with no more than $\Delta(G)+1$ colors. Let $v_1, v_2, \ldots, v_n$ be the vertices of $G$ whose degrees are in decreasing order. Use natural numbers to represent colors and assign color 1 to $v_1$. The colors of other vertices are assigned inductively as follows. Suppose the colors of $v_1, v_2, \ldots, v_{j-1}$ for $j \leq n$ have been assigned. Then the color number of $v_j$ is the smallest natural number that is different from the color numbers of those vertices in the set $\{v_1, v_2, \ldots, v_{j-1}\}$ that are adjacent to $v_j$. Since $v_j$ has at most $\min\{\deg(v_j), j-1\}$ neighbors in this set, where $\deg(v_j)$ is the degree of $v_j$, it follows that the color number of $j$ is at most $\min\{\deg(v_j)+1, j\}$. Therefore,

$$\chi(G) \leq \max_j \min\{\deg(v_j)+1, j\} \leq \Delta(G)+1. \tag{121}$$

The inequality $\gamma(G) \geq 1/\chi(G)$ follows from the observation that any independence cover (or coloring) of $G$ with $\chi(G)$ elements and uniform weights has cover strength $1/\chi(G)$.

To prove the inequality $\gamma(G) \leq \alpha(G)/|V|$, let $(\mathscr{A}, \mu)$ be an arbitrary independence cover. Then

$$\begin{aligned} |V| s(\mathscr{A}, \mu) &= |V| \min_{j\in V} \sum_{l|A_l \ni j} \mu_l \leq \sum_j \sum_{l|A_l\ni j} \mu_l \\ &= \sum_l \mu_l |A_l| \leq \alpha(G) \sum_l \mu_l = \alpha(G), \end{aligned} \tag{122}$$

which implies that $\gamma(G) \leq \alpha(G)/|V|$. To prove the inequality $\gamma(G) \leq 1/\varpi(G)$, let $V_{\mathrm{C}}$ be a subset of $\varpi(G)$ vertices in $V$ that forms a clique. Then

$$\begin{aligned} \varpi(G) s(\mathscr{A}, \mu) &= \varpi(G) \min_{j\in V} \sum_{l|A_l\ni j} \mu_l \leq \sum_{j\in V_{\mathrm{C}}} \sum_{l|A_l\ni j} \mu_l \\ &\leq \sum_l \mu_l = 1, \end{aligned} \tag{123}$$

where the second inequality follows from the fact that each $A_l$ can contain at most one vertex in $V_{\mathrm{C}}$ because $V_{\mathrm{C}}$ forms a clique, while $A_l$ is an independent set. □

As an implication of Proposition 2, $\gamma(G) \geq 1/n$ for any hypergraph of $n$ vertices since $\Delta(G) \leq n-1$ and $\chi(G) \leq n$. In addition, $\gamma(G) = 1/m$ if the hypergraph $G$ has chromatic number and clique number both equal to $m$. In particular, $\gamma(G)$ can attain the maximum 1 iff $G$ has no nontrivial hyperedges. Here a hyperedge is nontrivial if its order is larger than or equal to 2. Any 2-colorable graph $G$ with at least one nontrivial edge has $\gamma(G) = 1/2$. For example $\gamma(G) = 1/2$ when $G$ is a square lattice (or analogs in higher dimensions) or an even cycle; $\gamma(G) = 1/3$ when $G$ is a triangular lattice; see Table I.

### B. Cover strengths of colorings and minimal covers

Let $G = (V, E)$ be a hypergraph and $(\mathscr{A}, \mu)$ a weighted independence cover constructed from a coloring $\mathscr{A}$, assuming that no independent set in $\mathscr{A}$ is empty (note that empty independent sets cannot increase the cover strength). Then each vertex of $V$ is contained in only one independent set in $\mathscr{A}$, which implies that

$$s(\mathscr{A}, \mu) = \min_l \mu_l \leq |\mathscr{A}|^{-1} \leq \chi(G)^{-1}. \tag{124}$$

Here the first inequality is saturated iff all weights $\mu_l$ are equal, and the second inequality is saturated iff the coloring $\mathscr{A}$ is optimal in the sense that no other coloring of $G$ requires fewer colors.

Next, let $(\mathscr{A}, \mu)$ be a weighted independence cover of $G$ constructed from a minimal cover $\mathscr{A}$. By "minimal" we mean that any proper subset $\mathscr{A}'$ of $\mathscr{A}$ is not a cover of $G$ because the union of sets in $\mathscr{A}'$ does not coincide with the vertex set $V$. In other words, for any $A_l$ in $\mathscr{A}$, there exists a vertex $j \in V$ such that $j \in A_l$ and $j \notin A_k$ for all $k \neq l$. Therefore,

$$s(\mathscr{A}, \mu) = \min_l \mu_l \leq |\mathscr{A}|^{-1} \leq \chi(G)^{-1} \tag{125}$$

as in Eq. (124). Again the first inequality is saturated iff all weights $\mu_l$ are equal; the second inequality is saturated iff $|\mathscr{A}| = \chi(G)$, in which case an optimal coloring of $G$ can be constructed from $\mathscr{A}$ by deleting some vertices in some independent sets if $\mathscr{A}$ is not yet a coloring.

In view of the above discussion, to maximize the cover strength it is always beneficial to choose equal weights when $\mathscr{A}$ is a coloring or minimal independence cover. In addition, the cover strength of any such cover is upper bounded by $1/\chi(G)$, which can be saturated.

### C. Independence degrees of odd cycles

Here we determine the independence degrees of odd cycles, which indicate that overcomplete covers of some hypergraph $G$ can have cover strengths larger than $1/\chi(G)$ and that the inequality $\gamma(G) \geq 1/\chi(G)$ in Proposition 2 is in general strict.

Let $C_n$ be a cycle with $n$ vertices, where $n$ is an odd integer. Then we have $\alpha(C_n) = (n-1)/2$, so that $\gamma(C_n) \leq (n-1)/(2n)$ according to Proposition 2. This upper bound can be saturated by the equal-weight cover composed of the $n$ sets

$$A_j = \{j, j+2, \ldots, j+n-3\}, \quad j = 1, 2, \ldots, n. \tag{126}$$

Here vertex labels $j$ and $j+n$ are taken to be the same. Therefore, the independence degree of the odd cycle $C_n$ is given by

$$\gamma(C_n) = \frac{n-1}{2n} = \frac{1}{2} - \frac{1}{2n}, \tag{127}$$

which increases monotonically with $n$. By contrast, the cover strength of any coloring or minimal cover of $C_n$ is upper bounded by $1/3$ given that $\chi(C_n) = 3$. So it is indeed advantageous to consider independence covers beyond colorings for some hypergraphs. These observations are of interest to constructing efficient verification protocols for hypergraph states, as we shall see later.

### D. Hypergraph states

The Pauli group for a qubit is generated by the following two Pauli matrices

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{128}$$

The Pauli matrices for the $j$th qubit are indexed by the subscript $j$. Given any hypergraph $G$ with $n$ vertices, we can construct an $n$-qubit hypergraph state $|G\rangle$ as follows: prepare the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ (eigenstate of $X$ with eigenvalue 1) for each vertex of $G$ and apply the generalized controlled-$Z$ operation $CZ_e$ on the vertices of each hyperedge $e$ [17, 18], that is,

$$|G\rangle = \biggl(\prod_{e\in E} CZ_e\biggr)|+\rangle^{\otimes n}. \tag{129}$$

Here

$$CZ_e = \bigotimes_{j\in e} 1_j - 2\bigotimes_{j\in e} |1\rangle\langle 1|_j, \tag{130}$$

which acts trivially on $V \setminus e$. When $e$ contains a single vertex, $CZ_e$ reduces to the Pauli operator $Z$ on the vertex, which is local. In addition, $CZ_e$ is the familiar controlled-$Z$ operation when $e$ connects two vertices.

Alternatively, the hypergraph state $|G\rangle$ is the unique eigenstate (up to a global phase factor) of the $n$ commuting (nonlocal) stabilizer operators [17, 18]

$$K_j = X_j \otimes \prod_{e\in E\,|\, e\ni j} CZ_{e\setminus\{j\}}, \quad j = 1, 2, \ldots, n. \tag{131}$$

This alternative definition will play a key role in the verification of hypergraph states. The definition of hypergraph states can also be generalized to the qudit setting [19, 20]; see Sec. VII for more details.

Hypergraph states enjoy a number of merits that are particularly appealing. For example, any hypergraph state of a connected hypergraph is GME [17]. Certain hypergraph states, like Union Jack states shown in Fig. 9, are universal for measurement-based quantum computation (MBQC) under only Pauli measurements [21, 22, 25], which is impossible for graph states. What is more, hypergraph states are found recently that are universal for MBQC under only $X$ and $Z$ measurements [26]. In addition, certain hypergraph states possess symmetry-protected topological orders, which are a focus of ongoing research [21, 22, 43]. Furthermore, hypergraph states are attractive for demonstrating quantum supremacy [23, 27]. When $G$ is an ordinary graph, $|G\rangle$ reduces to a graph state. All stabilizer states are equivalent to graph states under local Clifford transformations (LC) [44, 45]. Meanwhile, any graph state of a 2-colorable graph can be turned into a Calderbank-Shor-Steane (CSS) state under LC, and vice versa [46].

The order of a hypergraph state is defined as the order of the underlying hypergraph; similar convention applies to many other graph theoretic quantities, such as the degree, clique number, chromatic number, independence number, and independence degree. For example $\gamma(G) = 1/2$ for graph states $|G\rangle$ associated with nontrivial 2-colorable graphs (with at least one edge), including cluster states (of any dimension); $\gamma(G) = 1/3$ for hypergraph states associated with nontrivial 3-colorable hypergraphs (with at least one hyperedge of order 3): including order-3 cluster states (of any dimension) and Union Jack states; cf. Table I.

## V. EFFICIENT VERIFICATION OF HYPERGRAPH STATES

Before introducing a verification protocol for hypergraph states, it is instructive to determine the minimal number of measurement settings for each party required to verify a general hypergraph state, suppose we can only perform local projective measurements. The following corollary is a direct consequence of Proposition 1 and the fact that any connected hypergraph state is GME [17].

*Corollary* 6. To verify a connected hypergraph state with local projective measurements, each party needs at least two measurement settings.

If a vertex in a hypergraph is isolated, then the reduced state of the hypergraph state corresponding to the vertex is an eigenstate of $X$. To verify the hypergraph state, the party corresponding to the isolated vertex can measure $X$ alone. By contrast, any party corresponding to a non-isolated vertex needs at least two measurement settings. Surprisingly, two measurement settings for each party are also sufficient for verifying any hypergraph state, as we shall see shortly.

### A. Construction of tests for hypergraph states

Let $G = (V, E)$ be a hypergraph with $n$ vertices and $|G\rangle$ the associated hypergraph state. Then $|G\rangle$ is the unique eigenstate of the stabilizer operators $K_j$ for $j = 1, 2, \ldots, n$, as defined in Eq. (131). With this observation in mind, given any nonempty independent set $A$ of $G$, we can devise a test for $|G\rangle$ based on two types of Pauli measurements. The test consists in measuring $X_j$ for all $j \in A$ and measuring $Z_k$ for all $k \in \overline{A}$, where $\overline{A} := V \setminus A$ is the complement of $A$ in $V$. The measurement outcome on the $a$th qubit for $a = 1, 2, \ldots, n$ can be written as $(-1)^{o_a}$, where the Boolean variable $o_a$ is either 0 or 1. Since $A$ is an independent set, $X_j$ and $Z_k$ commute with $K_i$ for all $i, j \in A$ and $k \in \overline{A}$. In addition, the joint eigenstate of $X_j$ and $Z_k$ corresponding to the outcome $\{o_a\}$ is an eigenstate of $K_i$, whose eigenvalue is $(-1)^{t_i}$

with

$$t_i = o_i + \sum_{e\in E|e\ni i}\prod_{k\in e, k\neq i} o_k \tag{132}$$

according to Eq. (131).

Now we set the criterion that the test is passed iff $(-1)^{t_i}=1$ for all $i\in A$, then the test effectively measures all the stabilizer operators $K_i$ for $i\in A$. The projector onto the pass eigenspace reads

$$P=\prod_{i\in A}\frac{1+K_i}{2}. \tag{133}$$

A state $\rho$ can pass the test with certainty iff it is supported on the common eigenspace of $K_i$ with eigenvalue 1 for all $i\in A$. In particular, the target state $|G\rangle$ can always pass the test. Denote by $\mathscr{N}(A)$ the neighborhood of $A$ in the graph $G$, that is , the set of vertices in $G$ that are adjacent to at least one vertex in $A$. Then the complement $\overline{A}$ appearing above can be replaced by $\mathscr{N}(A)\setminus A$ since Eq. (132) only involves measurement outcomes associated with vertices in $A\cup\mathscr{N}(A)$.

The rank of the test projector $P$ in Eq. (133) is

$$\operatorname{rank}(P)=\operatorname{tr}(P)=2^{n-|A|}, \tag{134}$$

where $|A|$ denotes the cardinality of the set $A$; the larger is $|A|$, the smaller is $\operatorname{rank}(P)$. In view of this observation, it is desirable to choose large independent sets for constructing test projectors for the hypergraph state $|G\rangle$. In particular, the independence set $A$ can be enlarged when $A\cup\mathscr{N}(A)$ is a proper subset of the vertex set $V$. On the other hand, if $A\cup\mathscr{N}(A)=V$, then $\mathscr{N}(A)\setminus A=\overline{A}$, and $A$ cannot be contained in any larger independent set. Incidentally, the cardinality $|A|$ is upper bounded by the independence number $\alpha(G)$. Suppose $G$ has at least one nontrivial hyperedge or edge; then $\alpha(G)\leq n-1$, which implies that $\operatorname{rank}(P)\geq 2$. So at least two distinct tests are necessary to verify $|G\rangle$ as expected.

### B. The cover protocol

Let $\mathscr{A}=\{A_1,A_2,\dots,A_m\}$ be an independence cover of $G$ that is composed of $m$ nonempty independent sets, then we can devise a verification protocol for $|G\rangle$ with $m$ distinct tests (measurement settings). For each independent set $A_l$, we can construct a test by virtue of the method described in Sec. V A, with the test projector given by

$$P_l=\prod_{i\in A_l}\frac{1+K_i}{2}. \tag{135}$$

A state can pass all $m$ tests iff it is stabilized by $K_i$ for all $i\in\cup_{l=1}^m A_l=V$. So only the target state $|G\rangle$ can pass all tests with certainty as desired. This verification protocol will be referred to as the *cover protocol* since it is based on an independence cover.

Suppose the $l$th test (associated with $A_l$) is applied with probability $\mu_l$. Then the cover protocol can be specified by the weighted independence cover $(\mathscr{A},\mu)$. Its efficiency is determined by the spectral gap of the verification operator

$$\Omega(\mathscr{A},\mu)=\sum_{l=1}\mu_l P_l=\sum_l\mu_l\prod_{i\in A_l}\frac{1+K_i}{2}. \tag{136}$$

Note that the common eigenbasis of $K_i$ for $i\in V$ also forms an eigenbasis of $\Omega(\mathscr{A},\mu)$. Each eigenstate $|\Psi_x\rangle$ in this basis is specified by an $n$ bit string $x\in\{0,1\}^n$ and satisfies the equation $K_i|\Psi_x\rangle=(-1)^{x_i}|\Psi_x\rangle$. The corresponding eigenvalue of $\Omega(\mathscr{A},\mu)$ reads

$$\lambda_x=\sum_{l|\operatorname{supp}(x)\subset\overline{A}_l}\mu_l, \tag{137}$$

where $\operatorname{supp}(x):=\{i\,|\,x_i\neq 0\}$. To attain the second largest eigenvalue of $\Omega(\mathscr{A},\mu)$, it suffices to consider the case in which $x$ has only one bit equal to 1, which means

$$\beta(\Omega(\mathscr{A},\mu))=\max_{i\in V}\sum_{l|\overline{A}_l\ni i}\mu_l, \tag{138}$$

$$\nu(\Omega(\mathscr{A},\mu))=\min_{i\in V}\sum_{l|A_l\ni i}\mu_l=s(\mathscr{A},\mu). \tag{139}$$

Similarly, the smallest eigenvalue of $\Omega(\mathscr{A},\mu)$ is attained when all bits of $x$ are equal to 1, in which case we have $\lambda_x=0$. So the verification operator $\Omega(\mathscr{A},\mu)$ is always singular. These observations confirm the following theorem.

*Theorem* 7. Let $(\mathscr{A},\mu)$ be a weighted independence cover of $G$. Then

$$\nu(\Omega(\mathscr{A},\mu))=s(\mathscr{A},\mu),\quad \tau(\Omega(\mathscr{A},\mu))=0, \tag{140}$$

$$\max_{(\mathscr{A},\mu)}\nu(\Omega(\mathscr{A},\mu))=\gamma(G). \tag{141}$$

When $A_1,A_2,\dots,A_m$ are pairwise disjoint, $\mathscr{A}$ defines a coloring of $G$, in which case the verification protocol $(\mathscr{A},\mu)$ presented above is also called a *coloring protocol.* Each test of the coloring protocol is associated with a color (cf. Fig. 9): $X$ measurement is performed on all qubits associated with a given color, while $Z$ measurement is performed on all qubits associated with other colors. The number of distinct tests is equal to the number of colors. For example, three distinct tests are enough for all hypergraph states associated with hypergraphs displayed in Fig. 9.

According to Theorem 7 and Eq. (124), the efficiency of the coloring protocol $(\mathscr{A},\mu)$ admits a simple formula,

$$\nu(\Omega(\mathscr{A},\mu))=\min_l\mu_l\leq|\mathscr{A}|^{-1}\leq\chi(G)^{-1}. \tag{142}$$

Here the first inequality is saturated iff all weights $\mu_l$ are equal; the second one is saturated iff $|\mathscr{A}|=\chi(G)$, in

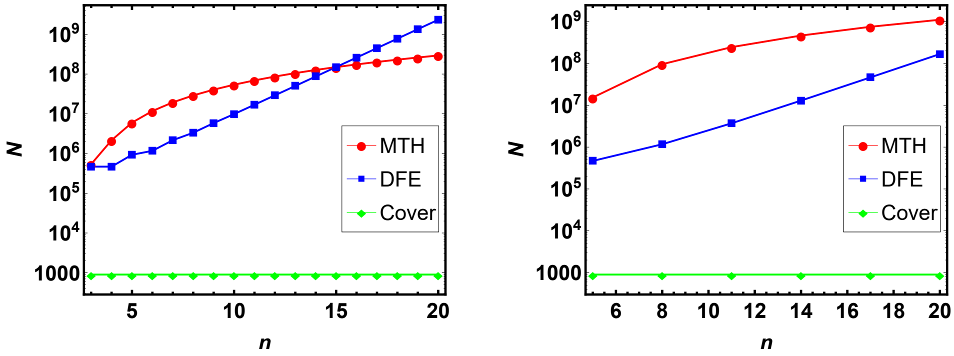

FIG. 10. (color online) Resource costs for verifying hypergraph states in the nonadversarial scenario. Left plot: 1D order-3 cluster states; right plot: Union Jack states on a chain. Here $n$ is the number of qubits of the hypergraph state, and $N$ is the (expected) number of tests required to verify the state within infidelity $\epsilon = 0.01$ and significance level $\delta = 0.05$. In the case of the MTH protocol proposed in Ref. [23], only a lower bound for $N$ is given (cf. Appendix I 3). The lines are guides for the eye. Our cover protocol dramatically outperforms direct fidelity estimation (DFE) [31] and the MTH protocol (cf. Appendix I).

which case the coloring $\mathscr{A}$ is optimal in the sense that no other coloring of $G$ requires fewer colors. In view of the above observation, by a coloring protocol, we usually assume that all weights $\mu_l$ are equal, that is, all distinct tests are performed with an equal probability, except when stated otherwise. Then the coloring protocol $(\mathscr{A},\mu)$ is also referred by $\mathscr{A}$. Similar conclusions and convention also apply to the cover protocol based on a minimal cover according to Sec. IV B. For a coloring protocol $\mathscr{A}$, it is straightforward to verify that all distinct eigenvalues of $\Omega(\mathscr{A})$ are given by $j/m$ for $j = 0, 1, \dots, m$, where $m = |\mathscr{A}|$ is the number of colors used in the coloring.

Theorem 7 reveals operational meanings of cover strength and independence degree in the verification of hypergraph states. Given a cover protocol $(\mathscr{A},\mu)$ with cover strength $s(\mathscr{A},\mu) > 0$, to verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$, the number of required tests is only

$$N = \left\lceil \frac{\ln \delta}{\ln[1 - s(\mathscr{A},\mu)\epsilon]} \right\rceil \leq \left\lceil \frac{\ln \delta^{-1}}{s(\mathscr{A},\mu)\epsilon} \right\rceil \tag{143}$$

according to Eq. (3). This number is minimized when the weighted independence cover $(\mathscr{A},\mu)$ is optimal, in which case we have $s(\mathscr{A},\mu) = \gamma(G)$, so that

$$N = \left\lceil \frac{\ln \delta}{\ln[1 - \gamma(G)\epsilon]} \right\rceil \leq \left\lceil \frac{\ln \delta^{-1}}{\gamma(G)\epsilon} \right\rceil. \tag{144}$$

According to Proposition 2,

$$N \leq \left\lceil \frac{\chi(G)}{\epsilon} \ln \frac{1}{\delta} \right\rceil \leq \left\lceil \frac{\Delta(G)+1}{\epsilon} \ln \frac{1}{\delta} \right\rceil \leq \left\lceil \frac{n}{\epsilon} \ln \frac{1}{\delta} \right\rceil, \tag{145}$$

where the first upper bound can be achieved by an optimal coloring protocol. In general, it is not easy to find an optimal independence cover, coloring, or even to compute $\chi(G)$ and $\gamma(G)$. Fortunately, the rightmost bound in Eq. (145) is very easy to compute and can be achieved by a coloring constructed from a simple greedy algorithm as presented in the proof of Proposition 2. By virtue of Eq. (4), we can also provide upper and lower bounds for the infidelity between the state prepared and the target state. In addition, Theorem 7 applies to qudit hypergraph states, as shown in Sec. VII later.

The above analysis shows that any hypergraph state $|G\rangle$ can be verified with at most $m = \Delta(G) + 1$ measurement settings in which each party performs either $X$ or $Z$ measurement. Note that $m$ is upper bounded by the number $n$ of qubits. The total number of tests scales as $m \ln \delta^{-1}/\epsilon$ and is at most $m$ times as large as the number for the best protocol based on entangling measurements. The cover protocol for verifying hypergraph states is dramatically more efficient than protocols known before [23, 31], as illustrated in Fig. 10 and discussed in detail in Appendix I. Consider the protocol of Ref. [23] for example, both the number of measurement settings and the total number of tests increase exponentially with $\Delta(G)$; in addition, the total number of tests scales as $1/\epsilon^2$ instead of $1/\epsilon$.

For many interesting families of hypergraph states, the chromatic numbers do not grow with the number of qubits. Most hypergraph states of practical interest are generated by short-range interactions, so their degrees and chromatic numbers are upper bounded by small constants. In this case, the cover protocol can achieve the optimal scaling behavior as the best protocol based on entangling measurements. For example, only two measurement settings are necessary for all graph states of 2-colorable graphs, including GHZ states, cluster states (of arbitrary dimensions), CSS states (up to LC), tree graph states, and graph states associated with even cycles. Only three measurement settings are necessary for order-3 cluster states and Union Jack states (cf. Table I).

For stabilizer states, which are equivalent to graph states under LC [44, 45], several methods are available in the literature [31, 40]. The protocol introduced by Pallister, Linden, and Montanaro (PLM) [40] is particularly efficient in terms of the total number of tests. To be specific, the PLM protocol measures all $2^n-1$ nontrivial stabilizer operators of $|G\rangle$ in the Pauli group with equal probability. The resulting verification operator reads

$$\Omega_{\mathrm{PLM}}=|G\rangle\langle G|+\frac{2^{(n-1)}-1}{2^n-1}(1-|G\rangle\langle G|), \tag{146}$$

which is homogeneous with

$$\beta(\Omega_{\mathrm{PLM}})=\frac{2^{(n-1)}-1}{2^n-1},\quad \nu(\Omega_{\mathrm{PLM}})=\frac{2^{(n-1)}}{2^n-1}. \tag{147}$$

To verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$, this protocol requires about

$$\lceil 2^{1-n}(2^n-1)\epsilon^{-1}\ln\delta^{-1}\rceil\leq\lceil 2\epsilon^{-1}\ln\delta^{-1}\rceil \tag{148}$$

tests, which is smaller than the number $\lceil\chi(G)\epsilon^{-1}\ln\delta^{-1}\rceil$ required by our coloring protocol [cf. Eq. (145)]. However, the number of potential measurement settings of the PLM protocol increases exponentially with the number $n$ of qubits. When $n$ is large, this protocol will be impractical if it is costly or time consuming to switch measurement settings. By contrast, our coloring protocol requires at most $n$ potential measurement settings. In addition, when the chromatic number $\chi(G)$ of $G$ is small (in particular when $G$ is 2-colorable), the total number of tests required is comparable to the PLM protocol. Furthermore, the PLM protocol requires $Y=\mathrm{i}XZ$ measurement because it is necessary to measure all nontrivial stabilizer operators of $|G\rangle$, while our protocol requires only $X$ and $Z$ measurements.

Incidentally, Ref. [40] introduced another protocol for verifying the graph state $|G\rangle$ by measuring $n$ stabilizer generators of $|G\rangle$ with equal probability. The resulting verification operator $\Omega$ can achieve $\nu(\Omega)=1/n$. This protocol requires $\lceil n\epsilon^{-1}\ln\delta^{-1}\rceil$ tests in total, which corresponds to the performance of our coloring protocol in the worst case in which the graph is complete (contains all possible edges). In general, the coloring protocol requires much fewer measurement settings and tests in total.

### C. The cover protocol for the adversarial scenario

Thanks to Theorem 4 and Corollary 5, the cover protocol can also be applied to verifying hypergraph states in the adversarial scenario, which is very important to many quantum information processing tasks that entail high-security requirements, such as blind MBQC. Let $\Omega=\Omega(\mathscr{A},\mu)$ be the verification operator associated with the cover protocol $(\mathscr{A},\mu)$, then $\nu(\Omega)=s(\mathscr{A},\mu)$ and $\tau(\Omega)=0$ according to Theorem 7. By Corollary 5, the number of tests required to verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$ satisfies

$$\min\left\{\left\lceil\frac{1-\delta}{\nu(\Omega)\delta\epsilon}\right\rceil,\ \left\lceil\frac{1}{\delta\epsilon}-1\right\rceil\right\}\leq N\leq\left\lceil\frac{1-\delta}{\nu(\Omega)\delta\epsilon}\right\rceil. \tag{149}$$

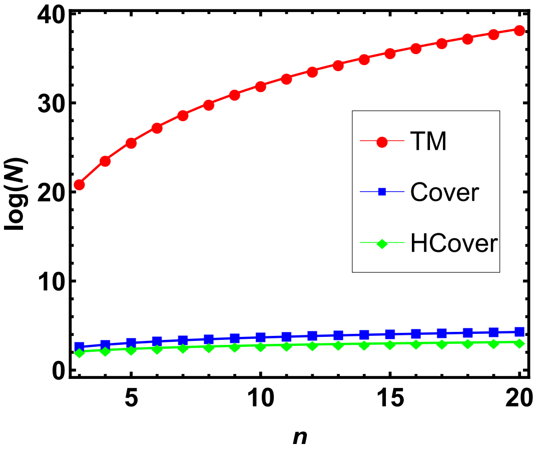

FIG. 11. (color online) Resource costs for verifying 3-colorable hypergraph states in the adversarial scenario. Here $n$ is the number of qubits, and $N$ is the number of tests required to verify the state within infidelity $\epsilon=1/(4n)$ and significance level $\delta=1/(4n)$; here "log" has base 10. The lines are guides for the eye. Our cover protocol (Cover) and hedged cover protocol (HCover) outperform the TM protocol proposed in Ref. [42] by at least 18 orders of magnitude.

For the optimal coloring protocol with $\nu(\Omega)=1/\chi(G)$, we have

$$N\leq\left\lceil\frac{\chi(G)(1-\delta)}{\delta\epsilon}\right\rceil\leq\left\lceil\frac{\Delta(G)+1}{\delta\epsilon}\right\rceil\leq\left\lceil\frac{n}{\delta\epsilon}\right\rceil. \tag{150}$$

If in addition $G$ is a 2-colorable graph, then $\nu(\Omega)=1/2$ and the lower bound in Eq. (149) is saturated according to Eq. (89).

Since $\Omega(\mathscr{A},\mu)$ is singular according to Theorem 7, the suboptimal scaling of $N$ with $\delta$ in Eq. (149) cannot be improved without modifying the protocol. Fortunately, it is easy to improve the scaling behavior by performing the trivial test with a suitable probability according to Sec. III E. Instead of $(\mathscr{A},\mu)$, here we propose the *hedged cover protocol* $(\mathscr{A},\mu)_p$ as characterized by the following verification operator

$$\Omega_p=(1-p)\Omega+p. \tag{151}$$

The name "hedged cover protocol" reflects the fact that the trivial test is introduced to hedge the influence of small eigenvalues of the operator $\Omega=\Omega(\mathscr{A},\mu)$. When $p=p_*(\nu)=p_*(\nu,0)$ is the optimal probability determined by Eq. (104) in Sec. III E, the hedged cover protocol $(\mathscr{A},\mu)_p$ is also denoted by $(\mathscr{A},\mu)_*$, where $\nu=\nu(\Omega)=s(\mathscr{A},\mu)$ depends on the specific cover protocol. The hedged cover protocol $(\mathscr{A},\mu)_p$ for the hypergraph state $|G\rangle$ is also called the *hedged coloring protocol* when $\mathscr{A}$ is a coloring of $G$, in which case it is natural to set $\mu_l=1/m$ for $l=1,2,\ldots,m$, where $m=|\mathscr{A}|$ denotes the number of colors.

Thanks to Theorem 6, by virtue of the hedged cover protocol $(\mathscr{A},\mu)_*$, that is, $(\mathscr{A},\mu)_p$ with $p=p_*(\nu)$, the number of tests in Eq. (149) can be reduced to

$$N=\left\lfloor\frac{h_*(\nu)\ln(F\delta)^{-1}}{\epsilon}\right\rfloor\leq\frac{\ln[(F\delta)^{-1}]}{\nu(1-\nu+\mathrm{e}^{-1}\nu^2)\epsilon}$$
$$\leq\frac{(1+\mathrm{e}\nu-\nu)\ln[(F\delta)^{-1}]}{\nu\epsilon}\leq\frac{\mathrm{e}\ln[(F\delta)^{-1}]}{\nu\epsilon},\qquad(152)$$

where $\nu=s(\mathscr{A},\mu)$, $F=1-\epsilon$, and e is the base of the natural logarithm. Here the three upper bounds also apply if we choose $p=\nu/\mathrm{e}$. If $(\mathscr{A},\mu)$ denotes the optimal cover protocol, then $\nu=\gamma(G)$. If $(\mathscr{A},\mu)$ denotes the optimal coloring protocol, then $\nu=1/\chi(G)$ and the number of tests required by $(\mathscr{A},\mu)_*$ satisfies

$$N\leq\frac{[\chi(G)+\mathrm{e}-1]\ln[(F\delta)^{-1}]}{\epsilon}\leq\frac{[\Delta(G)+\mathrm{e}]\ln[(F\delta)^{-1}]}{\epsilon}$$
$$\leq\frac{(n+\mathrm{e}-1)\ln[(F\delta)^{-1}]}{\epsilon}.\qquad(153)$$

The second bound still applies if the optimal coloring is replaced by a coloring with $\chi(G)+1$ colors. Although in general it is not easy to find an optimal coloring of the hypergraph $G$, it is easy to find a coloring with $\chi(G)+1$ colors by virtue of the greedy algorithm (see the proof of Proposition 2). Therefore, the hedged cover (or coloring) protocol can achieve the same optimal scaling behavior in the number $N$ of tests with $\epsilon^{-1}$ and $\delta^{-1}$ as the counterpart in the nonadversarial scenario; cf. Eq. (145). Accordingly, all the conclusions presented in Sec. V B can easily be adapted for the adversarial scenario. For many hypergraph states of practical interest, $\chi(G)$ is upper bounded by a small constant, so the number of tests required by the hedged cover protocol is comparable to the best protocol based on entangling measurements.

To illustrate the advantage of the cover protocol and hedged cover protocol, consider the verification of $n$-qubit 3-colorable hypergraph states (including order-3 cluster states and Union Jack states) in the adversarial scenario. To achieve infidelity $\epsilon=1/(4n)$ and significance level $\delta=1/(4n)$, the protocol proposed by Takeuchi and Morimae in a recent paper [42] requires at least $9.5\times10^{10}n^{21}$ tests (cf. Appendix I 5), which is already astronomical in the simplest nontrivial scenario. By contrast, the optimal cover or coloring protocol with $\nu(\Omega)=\gamma(G)=1/\chi(G)=1/3$ requires at most $12n(4n-1)$ tests according to Eq. (149), which outperforms Ref. [42] by at least 18 orders of magnitude even when $n=3$, and the advantage increases rapidly with the number $n$ of qubits. According to Eq. (152), the hedged cover protocol can further reduce the number to

$$\left\lfloor16.3n\ln\frac{16n^2}{4n-1}\right\rfloor,\qquad(154)$$

given that $h_*(\nu=1/3)<4.06$, which can be verified by straightforward calculation (cf. Sec. III E).

Even for graph states, our cover protocol and hedged cover protocol can significantly outperform previous approaches. Suppose $|G\rangle$ is a graph state associated with an $m$-colorable graph $G$. To verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$, the protocol proposed in a recent paper Ref. [39] requires $\lceil m^3/(\delta\epsilon)\rceil$ tests (cf. Appendix I 4). By contrast, the cover protocol requires only $\lceil m(1-\delta)/(\delta\epsilon)\rceil$ tests. Thanks to Eq. (152), the hedged cover or coloring protocol can further reduce the number of tests to

$$N=\left\lfloor\frac{h_*(1/m)\ln(F\delta)^{-1}}{\epsilon}\right\rfloor\leq\frac{(m+\mathrm{e}-1)\ln[(F\delta)^{-1}]}{\epsilon}$$
$$\approx\frac{(m+\mathrm{e}-1)\ln\delta^{-1}}{\epsilon},\qquad(155)$$

where $F=1-\epsilon$. When $m=3$ and $\epsilon=\delta=0.01$ for example, the protocol of Ref. [39] requires 270000 tests, while the hedged cover protocol requires only 1874 tests, which is smaller by 144 times.

For a graph state or stabilizer state, the number of tests can be reduced further by virtue of the PLM protocol introduced in Ref. [40] (only for the nonadversarial scenario originally) and the general method for addressing the adversarial scenario presented in Sec. III. According to Eq. (146) and Theorem 2, now the number of tests is given by $N(\epsilon,\delta,\lambda)$ with $\lambda=\beta(\Omega_{\mathrm{PLM}})$, which satisfies $1/3\leq\lambda\leq1/2$ according to Eq. (147). By Eq. (63) this number can be bounded from above as follows,

$$N(\epsilon,\delta,\lambda)\leq\left\lceil\frac{\ln\delta}{\lambda\epsilon\ln\lambda}\right\rceil\leq\left\lceil\frac{2\ln\delta^{-1}}{(\ln2)\epsilon}\right\rceil<\left\lceil\frac{2.9\ln\delta^{-1}}{\epsilon}\right\rceil.\qquad(156)$$

The second bound is independent of the number of qubits and is comparable to the counterpart $\lceil\mathrm{e}\ln\delta^{-1}/\epsilon\rceil$ for the best protocol based on entangling measurements. When $\epsilon=\delta=0.01$ for example, the bound is equal to 1329 (the exact value of $N(\epsilon,\delta,\lambda)$ is slightly smaller), which is about 71% of the number for the hedged cover protocol. Entangling measurements can further reduce the number of tests only a little bit (about 6%). The price for applying $\Omega_{\mathrm{PLM}}$ is that the number of potential measurement settings increases exponentially with the number of qubits. In addition, no generalization to hypergraph states is known.

## VI. DETECTION OF GENUINE MULTIPARTITE ENTANGLEMENT

Here we show that the cover protocol and the hedged cover protocol can also be applied to detecting GME of hypergraph states, although it is not necessarily optimized for this purpose. Recall that a multipartite pure state is GME if it is not biseparable, that is, if it cannot be written as a tensor product of two pure states. A mixed state is GME if it cannot be written as a convex mixture of biseparable states [2].

### A. Nonadversarial scenario

*Theorem* 8. Let $G$ be a connected order-$k$ hypergraph and $|G\rangle$ the corresponding hypergraph state. If a state $\rho$ satisfies $\langle G|\rho|G\rangle > 1-2^{1-k}$, then $\rho$ is GME.

This theorem was proved in Ref. [47]; see Appendix G for an independent proof. Note that the conclusion is independent of the number $n$ of qubits. When $|G\rangle$ is a graph state, Theorem 8 is known much earlier [2, 48, 49], in which case $\rho$ is GME if its fidelity with $|G\rangle$ is larger than one half. In general, to certify GME of the hypergraph state $|G\rangle$ with significance level $\delta$, we need to guarantee $\langle G|\rho|G\rangle > 1-2^{1-k}$ with significance level $\delta$. Given a verification strategy $\Omega$, then it suffices to perform

$$N=\left\lceil\frac{1}{\ln[1-2^{1-k}\nu(\Omega)]}\ln\delta\right\rceil \leq \left\lceil\frac{2^{k-1}}{\nu(\Omega)}\ln\delta^{-1}\right\rceil \qquad (157)$$

tests according to Eq. (3). If $\Omega$ corresponds to the cover protocol $(\mathscr{A},\mu)$, then $\nu(\Omega)$ is equal to the cover strength $s(\mathscr{A},\mu)$ according to Theorem 7. If we choose the optimal cover protocol, then $\nu(\Omega)$ is equal to the independence degree $\gamma(G)$, so the number of tests reduces to

$$\begin{aligned}N&=\left\lceil\frac{1}{\ln[1-2^{1-k}\gamma(G)]}\ln\delta\right\rceil \leq \left\lceil 2^{k-1}\chi(G)\ln\delta^{-1}\right\rceil\\&\leq \left\lceil 2^{k-1}[\Delta(G)+1]\ln\delta^{-1}\right\rceil \leq \left\lceil 2^{k-1}n\ln\delta^{-1}\right\rceil, \qquad (158)\end{aligned}$$

note that $1/\gamma(G)\leq\chi(G)\leq\Delta(G)+1\leq n$ according to Proposition 2. For a given $\delta$, this number is upper bounded by a constant that is independent of the number of qubits as long as $\gamma(G)$, $\chi(G)$, or $\Delta(G)$ is bounded. For example, we have $N\leq 3\times 2^{k-1}\chi(G)$ when $\delta=0.05$. In addition, GME of 2-colorable graph states (with $k=2$ and $\gamma(G)=1/\chi(G)=1/2$) can be certified with only $\lceil\ln\delta/\ln(3/4)\rceil$ tests (11 tests when $\delta=0.05$); for order-3 cluster states and Union jack states (with $k=3$ and $\gamma(G)=1/\chi(G)=1/3$), it suffices to perform $\lceil\ln\delta/\ln(11/12)\rceil$ tests (35 tests when $\delta=0.05$).

### B. Adversarial scenario

Next, consider the detection of GME of hypergraph states in the adversarial scenario. Given the cover protocol $(\mathscr{A},\mu)$ with verification operator $\Omega$, to certify the GME of $|G\rangle$ with significance level $\delta$, the minimal number of tests is determined by Eq. (149) with $\epsilon=2^{1-k}$, that is,

$$N\leq\left\lceil\frac{2^{k-1}(1-\delta)}{\nu(\Omega)\delta}\right\rceil, \qquad (159)$$

where $\nu(\Omega)=s(\mathscr{A},\mu)$ depends on the specific cover protocol. For example, $\nu(\Omega)=\gamma(G)$ for the optimal cover protocol and $\nu(\Omega)=1/\chi(G)$ for the optimal coloring protocol. When $\nu(\Omega)\geq 1/2$, the lower bound in Eq. (149) can be saturated, so the number of tests reduces to

$$N=\min\left\{\left\lceil\frac{2^{k-1}(1-\delta)}{\nu(\Omega)\delta}\right\rceil,\ \left\lceil\frac{2^{k-1}}{\delta}-1\right\rceil\right\}. \qquad (160)$$

To improve the scaling of $N$ with $1/\delta$, we can apply the hedged cover protocol $(\mathscr{A},\mu)_*$ as proposed in Sec. V C. Then the number of required tests is given by Eq. (152) with $\epsilon=2^{1-k}$, that is,

$$\begin{aligned}N&=\left\lfloor 2^{k-1}h_*(\nu)\ln(F\delta)^{-1}\right\rfloor \leq \frac{2^{k-1}\ln[(F\delta)^{-1}]}{\nu(1-\nu+\mathrm{e}^{-1}\nu^2)}\\&\leq\frac{2^{k-1}(1+\mathrm{e}\nu-\nu)\ln[(F\delta)^{-1}]}{\nu}\leq\frac{2^{k-1}\mathrm{e}\ln[(F\delta)^{-1}]}{\nu},\end{aligned} \qquad (161)$$

where $\nu=s(\mathscr{A},\mu)$ and $F=1-\epsilon=1-2^{1-k}$. If $(\mathscr{A},\mu)$ denotes the optimal coloring protocol, then $\nu=1/\chi(G)$, and the number of tests required by the protocol $(\mathscr{A},\mu)_*$ satisfies

$$\begin{aligned}N&\leq 2^{k-1}[\chi(G)+\mathrm{e}-1]\ln[(1-2^{1-k})^{-1}\delta^{-1}]\\&\leq 2^{k-1}[\Delta(G)+\mathrm{e}]\ln[(1-2^{1-k})^{-1}\delta^{-1}]. \qquad (162)\end{aligned}$$

These bounds are close to the counterparts for the nonadversarial scenario presented in Eq. (158), especially when $k$, $\chi(G)$, and $\Delta(G)$ are large. Therefore, GME of hypergraph states can be certified efficiently even in the adversarial scenario as long as the order $k$ is bounded. For example, GME of 2-colorable graph states can be certified in the adversarial scenario with only $\lfloor 6.44\ln(2/\delta)\rfloor$ tests (23 tests when $\delta=0.05$) according to Eq. (161). Incidentally, efficient entanglement (not GME) verification of cluster states was also studied in Ref. [50]. For order-3 cluster states and Union jack states, which are 3-colorable, it suffices to perform $\lceil 16.3\ln(4/3\delta)\rceil$ tests (53 tests when $\delta=0.05$).

Although detection of GME has been discussed in many works, our approach is appealing for at least four reasons. First, our approach is based on state verification, which can provide more precise information about the state than entanglement detection usually based on witness operators. Such information is crucial to many practical applications, such as MBQC. Second, our approach requires much fewer measurement settings and tests than most previous works on the detection of GME. Third, given a significance level, we can determine the number of required tests explicitly, which is not the case for most previous works. Fourth, our approach can be applied to both nonadversarial scenario and adversarial scenario. In addition, protocols devised on the nonadversarial scenario can easily be adapted for the adversarial scenario according to the general recipe presented in Sec. III E, while retaining almost the same efficiency.

## VII. VERIFICATION OF QUDIT HYPERGRAPH STATES

Most previous verification protocols only apply to qubit hypergraph states [23, 42]. Here we show that the cover protocol for verifying hypergraph states can also be applied to qudit hypergraph states with minor modifications, and most conclusions presented in Sec. V remain the same. This merit is appealing to both theoretical studies and practical applications.

### A. Qudit hypergraphs

In the case of qudit, we need to revise the definition of hypergraphs to take into account multiplicities of hyperedges. Now a hypergraph $G = (V, E, m_E)$ (also known as multihypergraph in the literature) is characterized by a set of vertices $V$ and a set of hyperedges $E \subset \mathscr{P}(V)$ together with multiplicities specified by $m_E = (m_e)_{e\in E}$, where $m_e \in \mathbb{Z}_d$ with $m_e \neq 0$ and $\mathbb{Z}_d$ is the ring of integers modulo $d$ [19, 20]. Nevertheless, almost all graph theoretic concepts considered in this work do not depend on the multiplicity vector $m_E$ and are defined in the same way as in the qubit case. To be specific, these concepts include the order of a hyperedge and the hypergraph, the adjacency relation, the degree of a vertex and the hypergraph, clique and clique number, independent set and independence number, (weighted) independence cover, cover strength, and independence degree. Therefore, Proposition 2 and its proof are applicable without any modification.

### B. Qudit hypergraph states

The qudit Pauli group (also known as the Heisenberg-Weyl group) is generated by the following two generalized Pauli operators

$$X = \sum_{j\in\mathbb{Z}_d} |j+1\rangle\langle j|, \quad Z = \sum_{j\in\mathbb{Z}_d} \omega^j |j\rangle\langle j|, \tag{163}$$

where $\omega = \mathrm{e}^{2\pi\mathrm{i}/d}$ is a primitive $d$th root of unity. Given any qudit hypergraph $G = (V, E, m_E)$ with $n$ vertices, we can construct an $n$-qudit hypergraph state $|G\rangle$ as follows: prepare the quantum state $|+\rangle := \frac{1}{\sqrt{d}}\sum_{j\in\mathbb{Z}_d}|j\rangle$ (eigenstate of $X$ with eigenvalue 1) for each vertex of $G$ and apply $m_e$ times the generalized controlled-$Z$ operation $CZ_e$ on the vertices of each hyperedge $e$ [19, 20], that is,

$$|G\rangle = \left(\prod_{e\in E} CZ_e^{m_e}\right)|+\rangle^{\otimes n}. \tag{164}$$

To simplify the notation, here we only give the expression of $CZ_e$ when $e = \{1, 2, \dots, k\}$, in which case we have

$$CZ_e := \sum_{j_1,j_2,\dots,j_k\in\mathbb{Z}_d} \omega^{j_1 j_2\dots j_k} |j_1, j_2, \dots, j_k\rangle\langle j_1, j_2, \dots, j_k|; \tag{165}$$

the general case is defined analogously. Alternatively, $|G\rangle$ is the unique eigenstate (up to a global phase factor) of the $n$ commuting (nonlocal) stabilizer operators [19, 20]

$$K_j = X_j \otimes \prod_{e\in E|\, e\ni j} CZ_{e\setminus\{j\}}^{m_e}, \quad j = 1, 2, \dots, n, \tag{166}$$

which satisfy $K_j^d = 1$. As in the qubit case, graph theoretic concepts related to the hypergraph $G$ also apply to the corresponding state $|G\rangle$.

### C. Verification of qudit hypergraph states

The following protocol for verifying qudit hypergraph states is a simple variation of the cover protocol for verifying qubit hypergraph states presented in Sec. V.

Let $G = (V, E, m_E)$ be a qudit hypergraph and $|G\rangle$ the associated hypergraph state. Choose an independence cover $\mathscr{A} = \{A_1, A_2, \dots\}$ of $G$ and let $\overline{A}_l := V \setminus A_l$ be the complement of $A_l$ in $V$. Then we can construct a verification protocol with $|\mathscr{A}|$ distinct tests (measurement settings): the $l$th test consists in measuring $X_j$ for all $j \in A_l$ and measuring $Z_k$ for all $k \in \overline{A}_l$. By measuring $X_j$ $(Z_k)$ we mean the measurement on the eigenbasis of $X_j$ $(Z_k)$. The measurement outcome on the $a$th qubit for $a = 1, 2, \dots, n$ can be written as $\omega^{o_a}$, where $o_a \in \mathbb{Z}_d$. Note that $X_j$ and $Z_k$ commute with $K_i$ for all $i, j \in A_l$ and $k \in \overline{A}_l$. In addition, the joint eigenstate of $X_j$ and $Z_k$ corresponding to the outcome $\{o_a\}$ is an eigenstate of $K_i$, whose eigenvalue is given by $\omega^{t_i}$ with

$$t_i = o_i + \sum_{e\in E|e\ni i} m_e \prod_{k\in e, k\neq i} o_k \tag{167}$$

according to Eq. (166). The test is passed if $\omega^{t_i} = 1$ for all $i \in A_l$. The projector onto the pass eigenspace associated with the $l$th test reads

$$P_l = \prod_{i\in A_l}\left(\frac{1}{d}\sum_{b\in\mathbb{Z}_d} K_i^b\right). \tag{168}$$

A state can pass all tests iff it is stabilized by $K_i$ for all $i \in V$. So only the target state $|G\rangle$ can pass all tests with certainty as desired.

Suppose the $l$th test is applied with probability $\mu_l$. The efficiency of the resulting protocol is determined by the spectral gap of $\Omega(\mathscr{A}, \mu) = \sum_{l=1} \mu_l P_l$. Here the common eigenbasis of $K_i$ for $i \in V$ also form an eigenbasis of $\Omega(\mathscr{A}, \mu)$. Each eigenstate $|\Psi_x\rangle$ in this basis is specified by a string $x \in \mathbb{Z}_d^n$ and satisfies $K_i|\Psi_x\rangle = \omega^{x_i}|\Psi_x\rangle$. The corresponding eigenvalue of $\Omega(\mathscr{A},\mu)$ reads

$$\lambda_x = \sum_{l|\mathrm{supp}(x)\subset\overline{A}_l} \mu_l, \tag{169}$$

where $\mathrm{supp}(x) := \{i\,|\,x_i \neq 0\}$. The second largest eigenvalue of $\Omega(\mathscr{A},\mu)$ can be attained when $x_i = 0$ for all $i \in V$ except for one of them, so that

$$\beta(\Omega(\mathscr{A},\mu)) = \max_{i\in V} \sum_{l|\overline{A}_l\ni i} \mu_l, \tag{170}$$

$$\nu(\Omega(\mathscr{A},\mu)) = \min_{i\in V} \sum_{l|A_l\ni i} \mu_l = s(\mathscr{A},\mu), \tag{171}$$

as in the case of qubit hypergraph states. Similarly, the smallest eigenvalue of $\Omega(\mathscr{A},\mu)$ is attained when all bits of $x$ are nonzero, in which case we have $\lambda_x = 0$. Again, the verification operator $\Omega(\mathscr{A},\mu)$ is always singular. Therefore, Theorem 7 as well as Eqs. (142)-(145) in Sec. V B and Eqs. (149)-(153) in Sec. V C are also applicable in the qudit case.

## VIII. SUMMARY

We presented a comprehensive study of pure-state verification in the adversarial scenario. In particular, we proposed a general recipe to constructing efficient verification protocols for the adversarial scenario based on verification protocols for the nonadversarial scenario. With this recipe, arbitrary pure states can be verified in the adversarial scenario with almost the same efficiency as in the nonadversarial scenario. For high-precision verification, the overhead in the number of tests is at most three times. In this way, pure-state verification in the adversarial scenario is reduced to the much simpler problem of verification in the nonadversarial scenario.

In addition, we introduced a simple method for verifying (qubit and qudit) hypergraph states which requires only two distinct Pauli measurements for each party. Our protocol is dramatically more efficient than all known candidates based on local measurements and is comparable to the best protocols based on entangling measurements. In general, the overhead is bounded by the chromatic number and degree of the underlying hypergraph. This protocol enables the verification of hypergraph states and GME of thousands of qubits, which will be instrumental in quantum information processing and in demonstrating quantum supremacy. Moreover, this protocol can be applied to the adversarial scenario and is thus particularly appealing to blind MBQC and quantum networks.

Our recipe to addressing the adversarial scenario is also very useful to the verification of bipartite pure states, weighted graph states, and various other multipartite pure states of practical interest. Besides quantum information processing, our work and its generalization may find potential applications in a number of different research areas, such as many-body physics.

## ACKNOWLEDGEMENTS

HZ is grateful to Zhibo Hou and Jiangwei Shang for discussions. This work is supported by the National Natural Science Foundation of China (Grant No. 11875110). HZ acknowledges financial support from the Excellence Initiative of the German Federal and State Governments Zukunftskonzept (ZUK 81) and the Deutsche Forschungsgemeinschaft (DFG) in the early stage of this work. MH was supported in part by Fund for the Promotion of Joint International Research (Fostering Joint International Research) Grant No. 15KK0007, Japan Society for the Promotion of Science (JSPS) Grant-in-Aid for Scientific Research (A) No. 17H01280, (B) No. 16KT0017, and Kayamori Foundation of Informational Science Advancement.

## APPENDIX

In this Appendix, we prove many results presented in the main text, including Theorems 1-5 and Lemmas 1-11 in particular. We also present a simpler proof of Eq. (1) (originally proved in Ref. [40]) and an independent proof of Theorem 8 (originally proved in Ref. [47]). In addition, we provide more details on the cover protocol and hedged cover protocol applied to GHZ states. Finally, we compare our approach with existing works.

### Appendix A: Proof of Eq. (1)

Here we present a simpler proof of Eq. (1), which was originally proved in Ref. [40].

*Proof.* Suppose the verification operator $\Omega$ has spectral decomposition $\Omega = \sum_{j=1}^{D} \lambda_j \Pi_j$, where $D$ is the dimension of the Hilbert space, $\lambda_j$ are the eigenvalues of $\Omega$ arranged in decreasing order $1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_D$, and $\Pi_j$ are mutually orthogonal rank-1 projectors with $\Pi_1 = |\Psi\rangle\langle\Psi|$. Without loss of generality, we may assume that $\sigma$ is diagonal in the eigenbasis of $\Omega$ because both $\mathrm{tr}(\Omega\sigma)$ and $\langle\Psi|\sigma|\Psi\rangle$ only depend on the diagonal elements of $\sigma$ in this basis. Suppose $\sigma = \sum_{j=1}^{D} x_j \Pi_j$ with $x_j \geq 0$ and $\sum_j x_j = 1$. Then

$$\langle\Psi|\sigma|\Psi\rangle = x_1, \quad \mathrm{tr}(\Omega\sigma) = \sum_j \lambda_j x_j. \tag{A1}$$

Therefore,

$$\begin{aligned}\max_{\langle\Psi|\sigma|\Psi\rangle\leq 1-\epsilon} \operatorname{tr}(\Omega\sigma) &= \max_{x_j\geq 0,\,\sum_j x_j=1,\,x_1\leq 1-\epsilon} \sum_j \lambda_j x_j \\ &= \max_{0\leq x_1\leq 1-\epsilon} x_1+\lambda_2(1-x_1) = 1-\nu(\Omega)\epsilon, \qquad \text{(A2)}\end{aligned}$$

where $\nu(\Omega) := 1-\beta = 1-\lambda_2$. The maximum can be attained when $\sigma = (1-\epsilon)(|\Psi\rangle\langle\Psi|)+\epsilon\Pi_2$. □

## Appendix B: Proofs of Lemmas 1 to 6

*Proof of Lemma 1.* Let $\rho$ be an arbitrary permutation-invariant diagonal density matrix with decomposition $\rho = \sum_{\mathbf{k}} c_{\mathbf{k}}\rho_{\mathbf{k}}$, where $c_{\mathbf{k}} \geq 0$. If $f_\rho = 0$, then $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0$ whenever $c_{\mathbf{k}} > 0$. Therefore,

$$\eta(N,0,\Omega) = \max_{\mathbf{k}\in\mathscr{S}}\{\eta_{\mathbf{k}}(\boldsymbol{\lambda})\,|\,\zeta_{\mathbf{k}}(\boldsymbol{\lambda})=0\}, \qquad \text{(B1)}$$

where $\mathscr{S}$ is the set of all sequences $\mathbf{k} = (k_1, k_2, \ldots, k_D)$ of $D$ nonnegative integers that sum up to $N+1$, that is, $\sum_j k_j = N+1$.

To compute $\eta(N,0,\Omega)$, we need to determine those $\mathbf{k}\in\mathscr{S}$ at which $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0$. According to Eq. (14), this condition is satisfied iff $k_1 = 0$, or $\lambda_i = 0$ and $k_i \geq 1$ for some $2 \leq i \leq D$. In the first case, $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leq \beta^N$, and the inequality is saturated when $\mathbf{k} = (0, N+1, 0, \ldots, 0)$. In the second case,

$$\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \frac{k_i\lambda_i^{k_i-1}}{N+1}\prod_{j\neq i,k_j\geq 1}\lambda_j^{k_j} \leq \frac{1}{N+1}, \qquad \text{(B2)}$$

and the inequality is saturated when $\mathbf{k} = (N, 0, \ldots, 0, 1)$. If $\tau > 0$, then only the first case can occur, so we have $\eta(N,0,\Omega) = \beta^N$. If $\tau = 0$, then both cases can occur, so $\eta(N,0,\Omega) = \max\{\beta^N, 1/(N+1)\}$. In conclusion, we have $\eta(N,0,\Omega) = \delta_{\mathrm{c}}$, which confirms Lemma 1. □

Next, consider the proofs of Lemmas 2 and 3. From the definitions in Eqs. (9) and (21) we can deduce the following equalities.

$$F(N,\delta,\Omega) = \min_{\delta'\geq\delta}\tilde{F}(N,\delta',\Omega), \qquad \text{(B3a)}$$

$$\mathcal{F}(N,f,\Omega) = \min_{f'\geq f}\tilde{\mathcal{F}}(N,f',\Omega), \qquad \text{(B3b)}$$

$$\zeta(N,\delta,\Omega) = \min_{\delta'\geq\delta}\tilde{\zeta}(N,\delta',\Omega), \qquad \text{(B3c)}$$

$$\eta(N,f,\Omega) = \max_{f'\leq f}\tilde{\eta}(N,f',\Omega). \qquad \text{(B3d)}$$

Therefore, Lemmas 2 and 3 are immediate consequences of Lemma 12 below.

*Lemma* 12. The following statements hold.

1. $\tilde{\zeta}(N,\delta,\Omega)$ is convex in $\delta$ for $0\leq\delta\leq 1$ and is strictly increasing in $\delta$ for $\delta_{\mathrm{c}}\leq\delta\leq 1$.
2. $\tilde{\eta}(N,f,\Omega)$ is concave and strictly increasing in $f$ for $0\leq f\leq 1$.
3. $\tilde{F}(N,\delta,\Omega)$ is strictly increasing in $\delta$ for $\delta_{\mathrm{c}}\leq\delta\leq 1$.
4. $\tilde{\mathcal{F}}(N,f,\Omega)$ is strictly increasing in $f$ for $0 < f \leq 1$.

Lemma 12 implies that the two functions $\tilde{\zeta}(N,\delta,\Omega)$ and $\tilde{F}(N,\delta,\Omega)$ are nondecreasing in $\delta$ for $0 < \delta \leq 1$, given that the two functions are nonnegative and that $\tilde{F}(N,\delta,\Omega) = \tilde{\zeta}(N,\delta,\Omega) = 0$ for $0 < \delta \leq \delta_{\mathrm{c}}$. The convexity of $\tilde{\zeta}(N,\delta,\Omega)$ means

$$\tilde{\zeta}(N,\delta,\Omega) \leq (1-s)\tilde{\zeta}(N,\delta_1,\Omega)+s\tilde{\zeta}(N,\delta_2,\Omega) \qquad \text{(B4)}$$

for $\delta = (1-s)\delta_1+s\delta_2$ and $0\leq s,\delta_1,\delta_2\leq 1$. Note that this inequality is trivial when $\delta_1 = \delta_2$ or $s = 0, 1$. The concavity of $\tilde{\eta}(N,f,\Omega)$ means

$$\tilde{\eta}(N,(1-s)f_1+sf_2,\Omega) \geq (1-s)\tilde{\eta}(N,f_1,\Omega)+s\tilde{\eta}(N,f_2,\Omega) \qquad \text{(B5)}$$

for $0\leq s, f_1, f_2\leq 1$.

*Proof of Lemma 12.* The convexity of $\tilde{\zeta}(N,\delta,\Omega)$ in $\delta$ follows from its definition based on minimization in Eq. (21). Suppose $0\leq\delta_1<\delta_2\leq 1$ and $0 < s < 1$; let $\delta = (1-s)\delta_1+s\delta_2$. In the case $\delta_1 > \delta_{\mathrm{c}}$, suppose the minimum in the definition of $\tilde{\zeta}(N,\delta_1,\Omega)$ is attained at $\rho_1$ and that of $\tilde{\zeta}(N,\delta_2,\Omega)$ is attained at $\rho_2$, that is,

$$\begin{aligned} p_{\rho_1} &= \delta_1, & f_{\rho_1} &= \tilde{\zeta}(N,\delta_1,\Omega), \\ p_{\rho_2} &= \delta_2, & f_{\rho_2} &= \tilde{\zeta}(N,\delta_2,\Omega). \end{aligned} \qquad \text{(B6)}$$

Let $\rho = (1-s)\rho_1+s\rho_2$; then

$$p_\rho = (1-s)\delta_1+s\delta_2 = \delta, \qquad \text{(B7)}$$

so that

$$\tilde{\zeta}(N,\delta,\Omega) \leq f_\rho = (1-s)\tilde{\zeta}(N,\delta_1,\Omega)+s\tilde{\zeta}(N,\delta_2,\Omega). \qquad \text{(B8)}$$

If $\delta_1\leq\delta_{\mathrm{c}}$ and $\delta\leq\delta_{\mathrm{c}}$, then $\tilde{\zeta}(N,\delta,\Omega) = \tilde{\zeta}(N,\delta_1,\Omega) = 0$, while $\tilde{\zeta}(N,\delta_2,\Omega)\geq 0$, so Eq. (B4) holds.

If $\delta_1\leq\delta_{\mathrm{c}}$ and $\delta > \delta_{\mathrm{c}}$, then $\tilde{\zeta}(N,\delta_1,\Omega) = 0$. Let $\rho_{\mathrm{c}}$ be a quantum state that satisfies $p_{\rho_{\mathrm{c}}} = \delta_{\mathrm{c}}$ and $f_{\rho_{\mathrm{c}}} = 0$. Let $s'$ be the solution of the equation $\delta = (1-s')\delta_{\mathrm{c}}+s'\delta_2$, which satisfies $s'\leq s$. Let $\rho = (1-s')\rho_{\mathrm{c}}+s'\rho_2$. Then $p_\rho = \delta$, so that

$$\begin{aligned}\tilde{\zeta}(N,\delta,\Omega) &\leq f_\rho = s'\tilde{\zeta}(N,\delta_2,\Omega) \leq s\tilde{\zeta}(N,\delta_2,\Omega) \\ &= (1-s)\tilde{\zeta}(N,\delta_1,\Omega)+s\tilde{\zeta}(N,\delta_2,\Omega), \qquad \text{(B9)}\end{aligned}$$

which confirms Eq. (B4) again. Therefore, $\tilde{\zeta}(N,\delta,\Omega)$ is convex in $\delta$ for $0\leq\delta\leq 1$.

To prove the monotonicity of of $\tilde{\zeta}(N,\delta,\Omega)$, let $\delta_1,\delta_2$ be arbitrary real numbers that satisfy $\delta_{\mathrm{c}}\leq\delta_1<\delta_2\leq 1$, so that $\tilde{\zeta}(N,\delta_2,\Omega) > 0$. If $\delta_1 = \delta_{\mathrm{c}}$, then $\tilde{\zeta}(N,\delta_1,\Omega) = 0 < \tilde{\zeta}(N,\delta_2,\Omega)$. If $\delta_1 > \delta_{\mathrm{c}}$, suppose the minimum in the definition of $\tilde{\zeta}(N,\delta_2,\Omega)$ is attained $\rho_2$. Let $s$ be the solution to the equation $\delta_1=(1-s)\delta_{\mathrm{c}}+s\delta_2$; note that $0<s<1$ because of the assumption $\delta_{\mathrm{c}}<\delta_1<\delta_2$. Let $\rho=(1-s)\rho_{\mathrm{c}}+s\rho_2$; then $p_\rho=\delta_1$, so that

$$\tilde{\zeta}(N,\delta_1,\Omega)\leq f_\rho=s\tilde{\zeta}(N,\delta_2,\Omega)<\tilde{\zeta}(N,\delta_2,\Omega). \tag{B10}$$

It follows that $\tilde{\zeta}(N,\delta,\Omega)$ is strictly increasing in $\delta$ when $\delta\geq\delta_{\mathrm{c}}$. As a corollary, $\tilde{\zeta}(N,\delta,\Omega)$ is nondecreasing in $\delta$ for $0\leq\delta\leq1$ given that $\tilde{\zeta}(N,\delta,\Omega)=0$ for $0\leq\delta\leq\delta_{\mathrm{c}}$.

Next, consider statement 2 in Lemma 12. The concavity of $\tilde{\eta}(N,f,\Omega)$ follows from a similar reasoning that leads to Eq. (B8).

To prove the monotonicity of $\tilde{\eta}(N,f,\Omega)$, let $0\leq f_1<f_2\leq1$. Suppose the maximum in the definition of $\tilde{\eta}(N,f_1,\Omega)$ is attained at $\rho_1$. Let $\varrho=(|\Psi\rangle\langle\Psi|)^{\otimes(N+1)}$; then $f_\varrho=p_\varrho=1$. Let $s$ be the solution to the equation $f_2=(1-s)f_1+s$; note that $0<s\leq1$ because of the assumption $f_1<f_2\leq1$. Let $\rho_2=(1-s)\rho_1+s\varrho$; then $f_{\rho_2}=f_2$, so that

$$\tilde{\eta}(N,f_2,\Omega)\geq p_{\rho_2}=(1-s)\tilde{\eta}(N,f_1,\Omega)+s>\tilde{\eta}(N,f_1,\Omega). \tag{B11}$$

Here the second inequality follows from the facts that $0<s\leq1$ and that $\tilde{\eta}(N,f_1,\Omega)<1$. To verify the inequality $\tilde{\eta}(N,f_1,\Omega)<1$, suppose on the contrary that $\tilde{\eta}(N,f_1,\Omega)=1$. Then $p_{\rho_1}=1$, so that $\rho_1=(|\Psi\rangle\langle\Psi|)^{\otimes(N+1)}$ and $f_1=f_{\rho_1}=1$, which contradicts the assumption $f_1<f_2\leq1$.

Next, consider statement 3 in Lemma 12. Suppose $\delta_1$ and $\delta_2$ are arbitrary real numbers that satisfy $\delta_{\mathrm{c}}\leq\delta_1<\delta_2\leq1$. Then $\tilde{F}(N,\delta_2,\Omega)>0$ given that $\delta_2>\delta_{\mathrm{c}}$. Suppose the minimum in the definition of $\tilde{F}(N,\delta_2,\Omega)$ is attained at $\rho_2$, that is, $p_{\rho_2}=\delta_2$ and $f_{\rho_2}=\delta_2\tilde{F}(N,\delta_2,\Omega)$. By assumption, $\delta_1$ can be expressed as a convex combination of $\delta_2$ and $\delta_{\mathrm{c}}$, that is, $\delta_1=s\delta_2+(1-s)\delta_{\mathrm{c}}$ with $0\leq s<1$. Let $\rho_1=s\rho_2+(1-s)\rho_{\mathrm{c}}$, then

$$p_{\rho_1}=s\delta_2+(1-s)\delta_{\mathrm{c}}=\delta_1,\quad f_{\rho_1}=sf_{\rho_2}=s\delta_2\tilde{F}(N,\delta_2,\Omega), \tag{B12}$$

so that

$$\tilde{F}(N,\delta_1,\Omega)\leq\frac{f_{\rho_1}}{p_{\rho_1}}=\frac{s\delta_2\tilde{F}(N,\delta_2,\Omega)}{s\delta_2+(1-s)\delta_{\mathrm{c}}}<\tilde{F}(N,\delta_2,\Omega). \tag{B13}$$

Therefore, $\tilde{F}(N,\delta,\Omega)$ is strictly increasing in $\delta$ whenever $\delta_{\mathrm{c}}\leq\delta\leq1$.

Finally, consider statement 4 in Lemma 12. Suppose $f_1$ and $f_2$ are real numbers that satisfy $0<f_1<f_2\leq1$. Let $s=f_1/f_2$, then $0<s<1$. Suppose the minimum in the definition of $\tilde{\mathcal{F}}(N,f_2,\Omega)$ is attained at $\rho_2$, that is, $f_{\rho_2}=f_2$ and $p_{\rho_2}=f_2/\tilde{\mathcal{F}}(N,f_2,\Omega)$. Let $\rho_1=s\rho_2+(1-s)\rho_{\mathrm{c}}$; then

$$f_{\rho_1}=sf_2=f_1,\quad p_{\rho_1}=sp_{\rho_2}+(1-s)\delta_{\mathrm{c}}, \tag{B14}$$

so that

$$\tilde{\mathcal{F}}(N,f_1,\Omega)\leq\frac{sf_2}{sp_{\rho_2}+(1-s)\delta_{\mathrm{c}}}<\frac{f_2}{p_{\rho_2}}=\tilde{\mathcal{F}}(N,f_2,\Omega). \tag{B15}$$

Therefore, $\tilde{\mathcal{F}}(N,f,\Omega)$ increases strictly monotonically with $f$ when $0<f\leq1$. □

*Proof of Lemma 4.* To prove Eq. (26), let $f_1=\zeta(N,\delta,\Omega)$ and $\delta_1=\eta(N,f_1,\Omega)$. If $\delta$ satisfies $0\leq\delta\leq\delta_{\mathrm{c}}$, then $f_1=0$ and $\delta_1=\delta_{\mathrm{c}}$ according to Lemma 1, which confirms Eq. (26).

Now suppose $\delta_{\mathrm{c}}<\delta\leq1$; then $\max\{\delta,\delta_{\mathrm{c}}\}=\delta$. In addition, there exists a quantum state $\rho$ on $\mathcal{H}^{\otimes(N+1)}$ such that $p_\rho=\delta$ and $f_\rho=f_1$, which implies that $\delta_1=\eta(N,f_1,\Omega)\geq\delta$. Meanwhile, there exists a state $\rho'$ such that $f_{\rho'}=f_1$ and $p_{\rho'}=\delta_1$, which implies that $\zeta(N,\delta_1,\Omega)\leq f_1=\zeta(N,\delta,\Omega)$. Since $\zeta(N,\delta,\Omega)$ is strictly increasing in $\delta$ for $\delta_{\mathrm{c}}\leq\delta\leq1$ according to Lemma 3, we conclude that $\delta_1\leq\delta$. This observation implies that $\delta_1=\delta$ and confirms Eq. (26) given the opposite inequality derived above.

Next, consider Eq. (27). Let $\delta_1=\eta(N,f,\Omega)$ and $f_1=\zeta(N,\delta_1,\Omega)$. Then there exists a quantum state $\rho$ on $\mathcal{H}^{\otimes(N+1)}$ such that $p_\rho=\delta_1$ and $f_\rho=f$, which implies that $f_1=\zeta(N,\delta_1,\Omega)\leq f$. Meanwhile, there exists a state $\rho'$ such that $f_{\rho'}=f_1$ and $p_{\rho'}=\delta_1$, which implies that $\eta(N,f_1,\Omega)\geq\delta_1=\eta(N,f,\Omega)$. Since $\eta(N,\delta,\Omega)$ is strictly increasing in $f$ for $0\leq f\leq1$ according to Lemma 3, we conclude that $f_1\geq f$. This observation implies that $f_1=f$ and confirms Eq. (27) given the opposite inequality derived above. □

*Proof of Lemma 5.* Recall that $\zeta(N,\delta,\Omega)$ is convex and nondecreasing in $\delta$ according to Lemma 3. In addition, $\zeta(N,\delta,\Omega)$ is a piecewise-linear function of $\delta$, and each turning point is equal to $\eta_{\mathbf{k}}$ for some $\mathbf{k}\in\mathscr{S}$ at which $\zeta(N,\delta=\eta_{\mathbf{k}},\Omega)=\zeta_{\mathbf{k}}$ (cf. Lemma 13 below). Here $\eta_{\mathbf{k}}$ and $\zeta_{\mathbf{k}}$ are shorthands for $\eta_{\mathbf{k}}(\boldsymbol{\lambda})$ and $\zeta_{\mathbf{k}}(\boldsymbol{\lambda})$, respectively, which are defined in Eq. (14). To prove Eq. (28a), it suffices to prove the inequality $\zeta_{\mathbf{k}}\geq\zeta(N-1,\eta_{\mathbf{k}},\Omega)$ for each turning point.

If $k_1=0$, then $\zeta_{\mathbf{k}}=0$, which implies that $\eta_{\mathbf{k}}\leq\delta_{\mathrm{c}}$ according to Lemma 1, so that $\zeta(N-1,\eta_{\mathbf{k}},\Omega)=0\leq\zeta_{\mathbf{k}}$.

If $k_1\geq1$, let $\mathbf{k}'=(k_1-1,k_2,\dots,k_D)$. Then

$$\eta_{\mathbf{k}',N-1}\geq\eta_{\mathbf{k}},\quad\zeta_{\mathbf{k}',N-1}\leq\zeta_{\mathbf{k}}, \tag{B16}$$

where $\eta_{\mathbf{k}',N-1}$ and $\zeta_{\mathbf{k}',N-1}$ are given in Eq. (14) with $N$ replaced by $N-1$ and $\mathbf{k}$ replaced by $\mathbf{k}'$. In conjunction with Lemma 3 we conclude that

$$\begin{aligned}\zeta(N-1,\eta_{\mathbf{k}},\Omega)\leq\zeta(N-1,\eta_{\mathbf{k}',N-1},\Omega)&\leq\zeta_{\mathbf{k}',N-1}\\ &\leq\zeta_{\mathbf{k}},\end{aligned} \tag{B17}$$

which implies Eq. (28a) as desired. If $\delta\leq\delta_{\mathrm{c}}$ then we have $\zeta(N,\delta,\Omega)=\zeta(N-1,\delta,\Omega)=0$. If $\delta=1$ by contrast, then $\zeta(N,\delta,\Omega)=\zeta(N-1,\delta,\Omega)=1$. So the inequality in Eq. (28a) is saturated in both cases.

If the upper bound in Eq. (B17) is saturated, then $\zeta_{\mathbf{k}',N-1}=\zeta_{\mathbf{k}}$, which implies that $\zeta_{\mathbf{k}}=0$ (which means $\eta_{\mathbf{k}}\leq\delta_{\mathrm{c}}$) or $\zeta_{\mathbf{k}}=1$ (which means $\eta_{\mathbf{k}}=1$). So the upper bound in Eq. (B17) cannot be saturated whenever the turning point satisfies $\delta_{\mathrm{c}}<\eta_{\mathbf{k}}<1$. In conjunction with

Eqs. (19) and (20), this observation implies that the inequality in Eq. (28a) is saturated iff $\delta \leq \delta_c$ or $\delta = 1$. According to Lemma 2, Eq. (28b) and Eq. (28a) are equivalent, so the same conclusion also applies to Eq. (28b).

Equations (28c) and (28d) can be proved by a similar reasoning as presented above. □

*Proof of Lemma 6.* Lemma 6 follows from the definition of $N(\epsilon, \delta, \Omega)$ in Eq. (11) and the fact that the following four inequalities are equivalent,

$$F(N, \delta, \Omega) \geq 1 - \epsilon, \tag{B18}$$

$$\zeta(N, \delta, \Omega) \geq \delta(1 - \epsilon), \tag{B19}$$

$$\eta(N, \delta(1 - \epsilon), \Omega) \leq \delta, \tag{B20}$$

$$\mathcal{F}(N, \delta(1 - \epsilon), \Omega) \geq (1 - \epsilon). \tag{B21}$$

Here the equivalence of the first two inequalities is a corollary of Lemma 2; so is the equivalence of the last two inequalities. The equivalence of the middle two inequalities follows from Lemmas 3 and 4, note that $\delta \geq \delta_c$ if either inequality is satisfied. □

By Eq. (25) in the main text, $\zeta(N, \delta, \Omega)$ and $\eta(N, f, \Omega)$ are piecewise linear functions, whose turning points correspond to the extremal points of the region $R_{N,\Omega}$, which have the form $(\eta_{\mathbf{k}}(\boldsymbol{\lambda}), \zeta_{\mathbf{k}}(\boldsymbol{\lambda}))$ for certain $\mathbf{k} \in \mathscr{S}$. In conjunction with the monotonicity and convexity (concavity) of $\zeta(N, \delta, \Omega)$ ($\eta(N, f, \Omega)$) stated in Lemma 3 (see also Lemma 4), we can deduce the following conclusion. Here $\delta_c$ is defined in Eq. (18).

*Lemma* 13. $\zeta(N, \delta, \Omega)$ for $\delta_c \leq \delta \leq 1$ and $\eta(N, f, \Omega)$ for $0 \leq f \leq 1$ can be expressed as follows,

$$\zeta(N, \delta, \Omega) = \frac{a_{j+1} - \delta}{a_{j+1} - a_j} b_j + \frac{\delta - a_j}{a_{j+1} - a_j} b_{j+1}, \tag{B22}$$

$$\eta(N, f, \Omega) = \frac{b_{l+1} - f}{b_{l+1} - b_l} a_l + \frac{f - b_l}{b_{l+1} - b_l} a_{l+1}, \tag{B23}$$

where $j$ and $l$ are chosen so that $a_j \leq \delta \leq a_{j+1}$ and $b_l \leq f \leq b_{l+1}$. Here $a_j = \eta_{\mathbf{k}^{(j)}}(\boldsymbol{\lambda})$ and $b_j = \zeta_{\mathbf{k}^{(j)}}(\boldsymbol{\lambda})$ with $\mathbf{k}^{(j)} \in \mathscr{S}$ for $j = 0, 1, \ldots, m$, which satisfy the following conditions

$$\delta_c = a_0 < a_1 < \ldots < a_{m-1} < a_m = 1, \tag{B24}$$

$$0 = b_0 < b_1 < \ldots < b_{m-1} < b_m = 1, \tag{B25}$$

$$0 = \frac{b_0}{a_0} < \frac{b_1}{a_1} < \ldots < \frac{b_{m-1}}{a_{m-1}} < \frac{b_m}{a_m} = 1. \tag{B26}$$

For example, when $\Omega$ is a nonsingular homogeneous strategy defined in Eq. (32), then $\delta_c = \lambda^N$, $m = N + 1$, $a_j = \eta_{N+1-j}(\lambda)$, and $b_j = \zeta_{N+1-j}(\lambda)$.

Lemma 13 is very helpful to understanding the properties of $\zeta(N, \delta, \Omega)$ and $\eta(N, f, \Omega)$, although, in general, it is not easy to determine the values of $m$, $\mathbf{k}^{(j)}$, $a_j$, and $b_j$. Geometrically, $(a_j, b_j)$ happen to be the extremal points of the region $R_{N,\Omega}$. When $\delta_c = \tau^N$, which can happen iff $\tau = \beta > 0$, $R_{N,\Omega}$ has no other extremal point; when $\delta_c > \tau^N$, $R_{N,\Omega}$ has only one additional extremal point, namely $(\tau^N, 0)$.

## Appendix C: Homogeneous strategies

### 1. Additional results on homogeneous strategies

Before proving the results on homogeneous strategies presented in the main text, we need to introduce a few auxiliary results. For $k, j \in \mathbb{Z}^{\geq 0}$, define

$$g_{kj}(\lambda) := \frac{\zeta_k(\lambda) - \zeta_j(\lambda)}{\eta_k(\lambda) - \eta_j(\lambda)}, \quad j \neq k, \tag{C1}$$

$$g_k(\lambda) := g_{k(k+1)}(\lambda) = \frac{\zeta_k(\lambda) - \zeta_{k+1}(\lambda)}{\eta_k(\lambda) - \eta_{k+1}(\lambda)}, \tag{C2}$$

where $\eta_k(\lambda)$ and $\zeta_k(\lambda)$ are defined in Eq. (35), assuming that $N$ is a positive integer. To simplify the notations, we shall use $\eta_k$, $\zeta_k$, $g_k$, $g_{kj}$ as shorthands for $\eta_k(\lambda)$, $\zeta_k(\lambda)$, $g_k(\lambda)$, $g_{kj}(\lambda)$ if there is no danger of confusions.

*Lemma* 14. Suppose $0 < \lambda < 1$ and $j, k \in \mathbb{Z}^{\geq 0}$ with $k < j$. Then $g_k(\lambda)$ decreases strictly monotonically with $k$, and $g_{kj}(\lambda)$ decreases strictly monotonically with $j, k$.

*Lemma* 15. Let $0 \leq \lambda < 1$ and $k \in \{1, 2, \ldots, N + 1\}$. Then

$$\frac{1}{1 - \lambda^N} \leq \frac{1 - \zeta_k(\lambda)}{1 - \eta_k(\lambda)} \leq \frac{1 + N(1 - \lambda)}{N(1 - \lambda)} = \frac{1 + N\nu}{N\nu}. \tag{C3}$$

The first inequality is saturated only if $k = N + 1$, or $k \geq 2$ and $\lambda = 0$; the second inequality is saturated only if $k = 1$.

Lemma 15 in particular implies that

$$\frac{1}{1 - \lambda^N} < \frac{1 + N\nu}{N\nu}, \tag{C4}$$

which in turn implies that

$$\lambda^N < \frac{1}{N\nu + 1}, \tag{C5}$$

recall that $N$ is a positive integer.

*Lemma* 16. Suppose $0 < \lambda < 1$ and $0 < \delta \leq 1$. Then

$$\max_{k \in \mathbb{Z}^{\geq 0}} \zeta(N, \delta, \lambda, k) = \zeta(N, \delta, \lambda, k_*), \tag{C6}$$

$$\begin{aligned} &\max\{0, \zeta(N, \delta, \lambda, k_*)\} \\ &= \max\{0, \zeta(N, \delta, \lambda, k_+), \zeta(N, \delta, \lambda, k_-)\}. \end{aligned} \tag{C7}$$

where $k_*$ is the largest integer $k$ that satisfies $\eta_k \geq \delta$, $k_+ = \lceil \log_\lambda \delta \rceil$, and $k_- = \lfloor \log_\lambda \delta \rfloor$. In addition

$$\zeta(N, \delta, \lambda, k_*) \leq 0, \quad 0 \leq \delta \leq \lambda^N, \tag{C8}$$

$$\zeta(N, \delta, \lambda, k_*) > 0, \quad \lambda^N < \delta \leq 1. \tag{C9}$$

*Lemma* 17. Suppose $0 < \epsilon, \delta, \lambda < 1$. Then

$$\tilde{N}_-(\epsilon, \delta, \lambda) \leq \frac{F\nu + \lambda}{\lambda\epsilon} k_- + \frac{\log_\lambda \delta - k_-}{\lambda\epsilon} = \frac{\log_\lambda \delta}{\lambda\epsilon} - \frac{\nu k_-}{\lambda}, \tag{C10}$$

where $F = 1 - \epsilon$, $\nu = 1 - \lambda$, and $k_- = \lfloor \log_\lambda \delta \rfloor$. The inequality is saturated when $\log_\lambda \delta$ is an integer.

*Proof of Lemma 14.* From the definitions of $\eta_k(\lambda)$ and $\zeta_k(\lambda)$ in Eq. (35) we can derive

$$g_k(\lambda) = \frac{\lambda[1+(N-k)\nu]}{\nu(N\lambda+k\nu)}, \tag{C11}$$

$$g_k(\lambda) - g_{k+1}(\lambda) = \frac{(N+1)\lambda}{[N\lambda+(k+1)\nu](N\lambda+k\nu)} > 0, \tag{C12}$$

which shows that $g_k(\lambda)$ decreases strictly monotonically with $k$ for $k \in \mathbb{Z}^{\geq 0}$.

Simple analysis shows that $g_{kj}(\lambda)$ can be expressed as a weighted average of $g_m(\lambda)$ for $m = k, k+1, \ldots, j-1$, namely,

$$g_{kj}(\lambda) = \sum_{m=k}^{j-1} \frac{\eta_m(\lambda)-\eta_{m+1}(\lambda)}{\eta_k(\lambda)-\eta_j(\lambda)} g_m(\lambda), \tag{C13}$$

where the weight for each $g_m(\lambda)$ is strictly positive. So $g_j(\lambda) < g_{j-1}(\lambda) < g_{kj}(\lambda) < g_k(\lambda)$ when $k+1 < j$. In addition, $g_{k(j+1)}(\lambda)$ is a convex sum of $g_{kj}(\lambda)$ and $g_j(\lambda)$, that is,

$$g_{k(j+1)} = \frac{(\eta_k-\eta_j)g_{kj} + (\eta_j-\eta_{j+1})g_j}{\eta_k-\eta_{j+1}}, \tag{C14}$$

which implies that $g_{k(j+1)}(\lambda) < g_{kj}(\lambda)$; by the same token we can prove $g_{(k+1)j}(\lambda) < g_{kj}(\lambda)$ when $k+1 < j$. Therefore, $g_{kj}(\lambda)$ decreases strictly monotonically with $k$ and $j$. □

*Proof of Lemma 15.* When $0 < \lambda < 1$, Lemma 15 is an immediate consequence of Lemma 14 given that

$$\eta_0(\lambda) = \zeta_0(\lambda) = 1,\ \eta_{N+1}(\lambda) = \lambda^N,\ \zeta_{N+1}(\lambda) = 0, \tag{C15}$$

$$\eta_1(\lambda) = \frac{1+N\lambda}{N+1}, \quad \zeta_1(\lambda) = \frac{N\lambda}{N+1}, \tag{C16}$$

so that

$$g_{0k}(\lambda) = \frac{1-\zeta_k(\lambda)}{1-\eta_k(\lambda)} = \begin{cases} \frac{1+N(1-\lambda)}{N(1-\lambda)} & k=1, \\ \frac{1}{1-\lambda^N} & k=N+1. \end{cases} \tag{C17}$$

When $\lambda = 0$, we have $\zeta_0 = \eta_0 = 1$, $\eta_1 = 1/(N+1)$, $\eta_k = 0$ for $k = 2, 3, \ldots, N+1$, and $\zeta_k = 0$ for $k = 1, 2, \ldots, N+1$, in which case Lemma 15 can be verified explicitly. □

*Proof of Lemma 16.* By the definition of $\zeta(N,\delta,\lambda,k)$ in Eq. (42), we can derive

$$\begin{aligned} &\zeta(N,\delta,\lambda,k) - \zeta(N,\delta,\lambda,k-1) \\ &\quad= \frac{\lambda^k[k+(N+1-k)\lambda] - (N+1)\lambda\delta}{(k\nu+N\lambda)[k\nu+(N+1)\lambda-1]}. \end{aligned} \tag{C18}$$

So $\zeta(N,\delta,\lambda,k) \geq \zeta(N,\delta,\lambda,k-1)$ iff $\delta \leq \eta_k$ and the inequality is saturated only when $\delta = \eta_k$. Therefore, the maximum of $\zeta(N,\delta,\lambda,k)$ over $k \in \mathbb{Z}^{\geq 0}$ is attained when $k$ is the largest integer that satisfies $\eta_k \geq \delta$, which confirms Eq. (C6).

Before proving Eq. (C7), we first prove Eqs. (C8) and (C9). According to Eq. (42) in the main text and the definition of $k_*$, $\zeta(N,\delta,\lambda,k_*)$ is a convex sum of $\zeta_{k_*}(\lambda)$ and $\zeta_{k_*+1}(\lambda)$ in which the weight of $\zeta_{k_*}(\lambda)$ is nonzero. If $0 < \delta \leq \lambda^N$, then we have $k_* \geq N+1$, which implies that $\zeta_{k_*}(\lambda) \leq 0$ and $\zeta_{k_*+1}(\lambda) < 0$. Therefore, $\zeta(N,\delta,\lambda,k_*) \leq 0$, which confirms Eq. (C8). Conversely, if $\lambda^N < \delta \leq 1$, then $k_* \leq N$, which implies that $\zeta_{k_*}(\lambda) > 0$ and $\zeta_{k_*+1}(\lambda) \geq 0$. So $\zeta(N,\delta,\lambda,k_*) > 0$, which confirms Eq. (C9).

Alternatively, to prove Eq. (C8), we can prove that $\zeta(N,\delta,\lambda,k) \leq 0$ for $k \in \mathbb{Z}^{\geq 0}$. Given that $\zeta(N,\delta,\lambda,k)$ is a linear function of $\delta$, it suffices to prove the result when $\delta = 0$ and $\delta = \lambda^N$. According to Eq. (42),

$$\zeta(N,\delta=0,\lambda,k) = -\frac{\lambda^{k+1}}{(1-\lambda)[k+(N-k)\lambda]} < 0. \tag{C19}$$

In addition,

$$\zeta(N,\delta=\lambda^N,\lambda,k) = \frac{\lambda\{\lambda^N[1+(N-k)(1-\lambda)] - \lambda^k\}}{(1-\lambda)[k+(N-k)\lambda]}. \tag{C20}$$

To prove the inequality $\zeta(N,\delta=\lambda^N,\lambda,k) \leq 0$, it suffices to prove the following inequality

$$1 + j(1-\lambda) - \lambda^{-j} \leq 0, \quad j \in \mathbb{Z}, \quad 0 < \lambda < 1. \tag{C21}$$

This inequality can be verified by noting that the left-hand side is equal to 0 when $\lambda = 1$ and that its derivative over $\lambda$ is nonnegative,

$$-j(1-\lambda^{-j-1}) \geq 0. \tag{C22}$$

In conjunction with Eq. (C19), this observation confirms Eq. (C8).

Now we can prove Eq. (C7). If $0 < \delta \leq \lambda^N$, then the equality holds because both sides are equal to zero according to Eq. (C8). On the other hand, if $\lambda^N < \delta \leq 1$, then $0 \leq k_+ \leq N$ and $0 \leq k_- \leq N-1$; in addition, $\eta_{k_-}(\lambda) \geq \delta$ and $\eta_{1+k_+}(\lambda) < \delta$. Therefore, $k_*$ is equal to either $k_+$ or $k_-$, so that

$$\zeta(N,\delta,\lambda,k_*) = \max\{\zeta(N,\delta,\lambda,k_+), \zeta(N,\delta,\lambda,k_-)\}, \tag{C23}$$

which confirms Eq. (C7). □

*Proof of Lemma 17.* The equality in Eq. (C10) can be verified by straightforward calculation given the equality $F\nu + \lambda = 1 - \nu\epsilon$. According to Theorem 2,

$$\begin{aligned} \tilde{N}_-(\epsilon,\delta,\lambda) &= \frac{k_-\nu^2\delta F + \lambda^{k_-+1} + \lambda\delta(k_-\nu-1)}{\lambda\nu\delta\epsilon} \\ &= \frac{F\nu+\lambda}{\lambda\epsilon}k_- + \frac{\lambda^{k_-+1}-\lambda\delta}{\lambda\nu\delta\epsilon} \\ &= \frac{F\nu+\lambda}{\lambda\epsilon}k_- + \frac{\lambda^{k_- - \log_\lambda\delta + 1}-\lambda}{\lambda\nu\epsilon}. \end{aligned} \tag{C24}$$

To prove the inequality in Eq. (C10), it is equivalent to prove the following inequality

$$\lambda^{1-a} - \lambda - \nu a \leq 0, \tag{C25}$$

where $a = \log_\lambda \delta - \lfloor \log_\lambda \delta \rfloor$, which satisfies $0 \leq a < 1$. Equation (C25) holds because the function $\lambda^{1-a} - \lambda - \nu a$ is convex in $a$ and is equal to 0 when $a = 0$ and $a = 1$. This observation completes the proof of Eq. (C10).

When $\log_\lambda \delta$ is an integer, we have $a = 0$, so the inequality in Eq. (C25) and that in (C10) are saturated. □

### 2. Proofs of Theorems 1-3 and Eq. (61)

*Proof of Theorem 1.* According to Lemma 2, we have $F(N, \delta, \lambda) = \zeta(N, \delta, \lambda)/\delta$, where $\zeta(N, \delta, \lambda) = 0$ if $\delta \leq \delta_\mathrm{c} = \lambda^N$. If $\delta \geq \lambda^N$, then

$$\zeta(N, \delta, \lambda) = \min_{0 \leq k < j \leq N+1} [c_j \zeta_j + c_k \zeta_k], \tag{C26}$$

where $\zeta_j, \zeta_k$ are shorthands for $\zeta_j(\lambda), \zeta_k(\lambda)$, and the parameters $k, j$ are restricted by the requirements $\eta_k \geq \delta$ and $\eta_j < \delta$. The coefficients $c_j, c_k$ are determined by the conditions

$$c_j + c_k = 1, \quad c_j \eta_j + c_k \eta_k = \delta, \tag{C27}$$

which yield

$$c_j = \frac{\eta_k - \delta}{\eta_k - \eta_j}, \quad c_k = \frac{\delta - \eta_j}{\eta_k - \eta_j}. \tag{C28}$$

Therefore,

$$\begin{aligned} c_j \zeta_j + c_k \zeta_k &= \frac{\eta_k - \delta}{\eta_k - \eta_j} \zeta_j + \frac{\delta - \eta_j}{\eta_k - \eta_j} \zeta_k \\ &= \zeta_j + g_{kj}(\delta - \eta_j) = \zeta_k + g_{kj}(\delta - \eta_k), \end{aligned} \tag{C29}$$

where $g_{kj} = g_{kj}(\lambda)$ is defined in Eq. (C1).

If $j > k + 1$, then $\eta_{j-1} < \delta$ or $\eta_{k+1} \geq \delta$, so we can decrease the value of $c_j \zeta_j + c_k \zeta_k$ by replacing $j$ with $j - 1$ or $k$ with $k + 1$ according to Lemma 14. Therefore, the minimum in Eq. (C26) can be attained when $j = k + 1$ and $\eta_{k+1} < \delta \leq \eta_k$, in which case $k = k_*$ is the largest integer that satisfies the condition $\eta_k \geq \delta$. In this case, $c_k = c_k(\delta, \lambda)$, $c_j = 1 - c_k(\delta, \lambda)$, so that

$$c_j \zeta_j + c_k \zeta_k = \zeta(N, \delta, \lambda, k_*), \tag{C30}$$

which confirms Eq. (43). □

*Proof of Theorem 2.* By definition $N(\epsilon, \delta, \lambda)$ is the minimum value of positive integer $N$ under the condition $F(N, \delta, \lambda) \geq F$ with $F = 1 - \epsilon$, that is,

$$\zeta(N, \delta, \lambda) \geq F\delta, \tag{C31}$$

where $F\delta > 0$. According to Corollary 1 in the main text, Eq. (C31) is equivalent to

$$\max_{k \in \mathbb{Z}^{\geq 0}} \zeta(N, \delta, \lambda, k) \geq F\delta. \tag{C32}$$

From the definition of $\zeta(N, \delta, \lambda, k)$ in Eq. (42) we can deduce that the inequality $\zeta(N, \delta, \lambda, k) \geq F\delta$ is satisfied iff

$$N \geq \tilde{N}(\epsilon, \delta, \lambda, k) = \frac{k\nu^2 \delta F + \lambda^{k+1} + \lambda\delta(k\nu - 1)}{\lambda\nu\delta\epsilon}. \tag{C33}$$

So Eq. (C31) is satisfied iff

$$N \geq \min_{k \in \mathbb{Z}^{\geq 0}} \tilde{N}(\epsilon, \delta, \lambda, k). \tag{C34}$$

Therefore,

$$N(\epsilon, \delta, \lambda) = \left\lceil \min_{k \in \mathbb{Z}^{\geq 0}} \tilde{N}(\epsilon, \delta, \lambda, k) \right\rceil, \tag{C35}$$

which confirms the first equality in Eq. (51).

Calculation shows that

$$\begin{aligned} &\tilde{N}(\epsilon, \delta, \lambda, k) - \tilde{N}(\epsilon, \delta, \lambda, k-1) \\ &= \frac{\nu\delta(F\nu + \lambda) + \lambda^{k+1} - \lambda^k}{\lambda\nu\delta\epsilon} = \frac{\delta(F + \lambda\epsilon) - \lambda^k}{\lambda\delta\epsilon}, \end{aligned} \tag{C36}$$

so $\tilde{N}(\epsilon, \delta, \lambda, k) \leq \tilde{N}(\epsilon, \delta, \lambda, k-1)$ iff $\delta \leq \lambda^k/(F + \lambda\epsilon)$. The minimum in Eq. (C35) is attained when $k$ is the largest integer that satisfies $\delta \leq \lambda^k/(F + \lambda\epsilon)$, that is $k = k^*$. Therefore, $N(\epsilon, \delta, \lambda) = \lceil \tilde{N}(\epsilon, \delta, \lambda, k^*) \rceil$, which confirms Eq. (51)

Alternatively, Eq. (C31) is satisfied iff

$$\max\bigl\{\zeta(N, \delta, \lambda, k_+), \zeta(N, \delta, \lambda, k_-)\bigr\} \geq F\delta. \tag{C37}$$

Note that

$$\max_{k \in \mathbb{Z}^{\geq 0}} \zeta(N, \delta, \lambda, k) = \max\bigl\{\zeta(N, \delta, \lambda, k_+), \zeta(N, \delta, \lambda, k_-)\bigr\} \tag{C38}$$

whenever one side of the equation is known to be positive by Corollary 1 in the main text. Based on this observation, we can derive

$$N(\epsilon, \delta, \lambda) = \bigl\lceil \min\{\tilde{N}_+(\epsilon, \delta, \lambda), \tilde{N}_-(\epsilon, \delta, \lambda)\} \bigr\rceil, \tag{C39}$$

which confirms Eq. (54) and implies Eq. (55) given Eq. (C36). □

*Proof of Eq.* (61). The equality in Eq. (61) follows from Theorem 2. To prove the lower bound, we first compute the derivative of $\tilde{N}(\epsilon, \delta, \lambda, 1)$ over $\lambda$, with the result

$$\frac{\partial \tilde{N}(\epsilon, \delta, \lambda, 1)}{\partial \lambda} = \frac{(1 - \delta)\lambda^2 - \delta F \nu^2}{\lambda^2 \nu^2 \epsilon\delta}. \tag{C40}$$

The minimum of $\tilde{N}(\epsilon, \delta, \lambda, 1)$ over the interval $0 < \lambda < 1$ is attained when $\lambda/(1 - \lambda) = \sqrt{\delta F/(1 - \delta)}$, that is,

$$\lambda = \lambda_* := \frac{\sqrt{\delta F}}{\sqrt{1 - \delta} + \sqrt{\delta F}}. \tag{C41}$$

Therefore,

$$N(\epsilon, \delta, \lambda) \geq \tilde{N}(\epsilon, \delta, \lambda, 1) \geq \tilde{N}(\epsilon, \delta, \lambda_*, 1) = \frac{2\sqrt{(1 - \delta)F}}{\epsilon\sqrt{\delta}}, \tag{C42}$$

which confirms the lower bound in Eq. (61). □

*Proof of Theorem 3.* Let $N = k_+ + \lceil \frac{k_+F}{\lambda\epsilon} \rceil$. According to Corollary 3, we have

$$\begin{aligned} F(N,\delta,\lambda) &\ge \frac{(N-k_+)\lambda}{k_+ + (N-k_+)\lambda} = \frac{\lceil\frac{k_+F}{\lambda\epsilon}\rceil\lambda}{k_+ + \lceil\frac{k_+F}{\lambda\epsilon}\rceil\lambda} \\ &\ge \frac{\frac{k_+F}{\epsilon}}{k_+ + \frac{k_+F}{\epsilon}} = F = 1-\epsilon, \end{aligned} \tag{C43}$$

which implies that $N(\epsilon,\delta,\lambda) \le N$ and confirms the upper bound in Eq. (62).

Next, let $N = k_- + \lceil \frac{k_-F}{\lambda\epsilon} \rceil$. If $k_- = 0$, then $N = 0 < N(\epsilon,\delta,\lambda)$. If $k_- \ge 1$, then $N - 1 \ge k_- \ge 1$. According to Corollary 3, we have

$$\begin{aligned} F(N-1,\delta,\lambda) &\le \frac{(N-1-k_-)\lambda}{k_- + (N-1-k_-)\lambda} \\ &= \frac{(\lceil\frac{k_-F}{\lambda\epsilon}\rceil - 1)\lambda}{k_- + (\lceil\frac{k_-F}{\lambda\epsilon}\rceil - 1)\lambda} < \frac{\frac{k_-F}{\epsilon}}{k_- + \frac{k_-F}{\epsilon}} = 1-\epsilon, \end{aligned} \tag{C44}$$

which implies that $N(\epsilon,\delta,\lambda) \ge N$ and confirms the lower bound in Eq. (62). If $\log_\lambda \delta$ is an integer, then $k_+ = k_-$, so the lower bound and the upper bound in Eq. (62) coincide, which means both of them are saturated. Alternatively, this fact can be verified by virtue of Theorem 2.

Finally, let us prove Eq. (63). According to Theorem 2 in the main text and Lemma 17,

$$\begin{aligned} N(\epsilon,\delta,\lambda) &= \lceil \min\{\tilde{N}_+(\epsilon,\delta,\lambda), \tilde{N}_-(\epsilon,\delta,\lambda)\}\rceil \\ &\le \lceil \tilde{N}_-(\epsilon,\delta,\lambda)\rceil \le \left\lceil \frac{\log_\lambda \delta}{\lambda\epsilon} - \frac{\nu k_-}{\lambda} \right\rceil, \end{aligned} \tag{C45}$$

which confirms Eq. (63). If $\log_\lambda \delta$ is an integer, then both inequalities are saturated, so the bound in Eq. (63) is saturated. □

## Appendix D: Proofs of Lemma 7 and Theorem 4

*Proof of Lemma 7.* To prove the inequality in Eq. (82), it suffices to find a state $\rho$ on $\mathcal{H}^{\otimes(N+1)}$ such that $p_\rho = \delta$ and

$$f_\rho = p_\rho - \frac{1}{N+1} \tag{D1}$$

for $1/(N+1) \le \delta \le \delta^*$. Since $p_\rho$ and $f_\rho$ are linear in $\rho$, it suffices to find such a state in the two cases $\delta = 1/(N+1)$ and $\delta = \delta^*$, respectively. When $\delta = 1/(N+1)$, we can choose the state $\rho = \rho_{\mathbf{k}}$ with $\mathbf{k} = (N, 0, \ldots, 0, 1)$, in which case we have $p_\rho = 1/(N+1)$ and $f_\rho = 0$ as desired, note that $\Omega$ is singular, that is, $\tau = 0$ by assumption.

In the case $\delta = \delta^*$, we can choose $\rho = \rho_{\mathbf{k}_1}$, where $\mathbf{k}_1 := (N, 1, 0, \ldots, 0)$ and

$$\begin{aligned} \eta_{\mathbf{k}_1}(\boldsymbol{\lambda}) &= \frac{1+N\beta}{N+1} = \frac{1+N(1-\nu)}{N+1} = \delta^*, \\ \zeta_{\mathbf{k}_1}(\boldsymbol{\lambda}) &= \frac{N\beta}{N+1} = \frac{N(1-\nu)}{N+1} \end{aligned} \tag{D2}$$

according to Eq. (14). Then we have $p_\rho = \eta_{\mathbf{k}_1}(\boldsymbol{\lambda})$ and $f_\rho = \zeta_{\mathbf{k}_1}(\boldsymbol{\lambda})$, so that

$$p_\rho - f_\rho = \eta_{\mathbf{k}_1}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}_1}(\boldsymbol{\lambda}) = \frac{1}{N+1}. \tag{D3}$$

This observation completes the proof of Lemma 7. □

*Proof of Theorem 4.* To prove the inequality in Eq. (83), Let $\rho = \sum_{\mathbf{k}} c_{\mathbf{k}}\rho_{\mathbf{k}}$. If $p_\rho = 1$, then we have $c_{\mathbf{k}} = \delta_{\mathbf{k},\mathbf{k}_0}$, where $\mathbf{k}_0 := (N+1, 0, \ldots, 0)$. Therefore, $F_\rho = f_\rho = 1$, $F(N, \delta = 1, \Omega) = 1$, and Eq. (83) holds. If $0 < p_\rho < 1$, then $c_{\mathbf{k}_0} < 1$ and

$$\begin{aligned} \frac{1-p_\rho}{1-f_\rho} &= \frac{1-\sum_{\mathbf{k}} c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-\sum_{\mathbf{k}} c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda})} = \frac{1-c_{k_0}-\sum_{\mathbf{k}\in\mathscr{S}^*} c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-c_{k_0}-\sum_{\mathbf{k}\in\mathscr{S}^*} c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda})} \\ &= \frac{1-\sum_{\mathbf{k}\in\mathscr{S}^*} c'_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-\sum_{\mathbf{k}\in\mathscr{S}^*} c'_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda})} = \frac{\sum_{\mathbf{k}\in\mathscr{S}^*} c'_{\mathbf{k}}[1-\eta_{\mathbf{k}}(\boldsymbol{\lambda})]}{\sum_{\mathbf{k}\in\mathscr{S}^*} c'_{\mathbf{k}}[1-\zeta_{\mathbf{k}}(\boldsymbol{\lambda})]}, \end{aligned} \tag{D4}$$

where $\mathscr{S}^* := \mathscr{S} \setminus \{\mathbf{k}_0\}$ is the subset of $\mathscr{S}$ with the vector $\mathbf{k}_0 := (N+1, 0, \ldots, 0)$ deleted, and $c'_{\mathbf{k}} := c_{\mathbf{k}}/(1-c_{\mathbf{k}_0})$ form a probability distribution on $\mathscr{S}^*$. By virtue of Lemma 19 below, we can deduce that

$$\frac{1-p_\rho}{1-f_\rho} \ge \min_{\mathbf{k}\in\mathscr{S}^*} \frac{1-\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-\zeta_{\mathbf{k}}(\boldsymbol{\lambda})} = \frac{1-\eta_{\mathbf{k}_1}(\boldsymbol{\lambda})}{1-\zeta_{\mathbf{k}_1}(\boldsymbol{\lambda})} = \frac{N\nu}{N\nu+1}, \tag{D5}$$

where $\mathbf{k}_1 = (N, 1, 0, \ldots, 0)$. Therefore,

$$f_\rho \ge p_\rho - \frac{1-p_\rho}{N\nu}, \tag{D6}$$

so that

$$F_\rho = \frac{f_\rho}{p_\rho} \ge 1 - \frac{1-p_\rho}{Np_\rho\nu}. \tag{D7}$$

In view of Eq. (9a), we conclude that

$$F(N,\delta,\Omega) \ge 1 - \frac{1-\delta}{N\delta\nu}. \tag{D8}$$

Incidentally, the above bound is negative and thus trivial when $\delta \le \beta^N$ since $\beta^N < 1/(N\nu+1)$ according to Eq. (C5).

Now we show that the inequality in Eq. (83) [that is, Eq. (D8)] is saturated when $\delta \ge \delta^* = \eta_{\mathbf{k}_1}(\boldsymbol{\lambda})$. To this end, it suffices to show that the inequality in Eq. (D6) can be saturated when $p_\rho \ge \eta_{\mathbf{k}_1}(\boldsymbol{\lambda})$. When $c_{\mathbf{k}} = \delta_{\mathbf{k},\mathbf{k}_0}$, that is, $\rho = \rho_{\mathbf{k}_0} = (|\Psi\rangle\langle\Psi|)^{\otimes(N+1)}$, we have $p_\rho = 1$ and $f_\rho = 1$, so Eq. (D6) is saturated. When $c_{\mathbf{k}} = \delta_{\mathbf{k},\mathbf{k}_1}$, that is, $\rho = \rho_{\mathbf{k}_1}$, we have $p_\rho = \eta_{\mathbf{k}_1}(\boldsymbol{\lambda})$ and $f_\rho = \zeta_{\mathbf{k}_1}(\boldsymbol{\lambda})$, so Eq. (D6) is also saturated. Since both $p_\rho$ and $f_\rho$ are linear in $\rho$, it follows that the inequality in Eq. (D6) can be saturated by a convex combination of $\rho_{\mathbf{k}_0}$ and $\rho_{\mathbf{k}_1}$ whenever $p_\rho \ge \eta_{\mathbf{k}_1}(\boldsymbol{\lambda})$.

Next, we prove Eq. (84) when $\nu \ge 1/2$. To this end, note that

$$\begin{aligned} p_\rho - f_\rho &= \sum_{\mathbf{k}} c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \sum_{\mathbf{k}} c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \\ &= \sum_{\mathbf{k}} c_{\mathbf{k}}[\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}}(\boldsymbol{\lambda})] \le \frac{1}{N+1}, \end{aligned} \tag{D9}$$

where the last inequality follows from Lemma 18 below. Therefore,

$$F_\rho \geq 1 - \frac{1}{(N+1)p_\rho}, \tag{D10}$$

which implies that

$$F(N,\delta,\Omega) \geq 1 - \frac{1}{(N+1)\delta} \tag{D11}$$

and confirms Eq. (84). If $\Omega$ is singular and $\delta$ satisfies $1/(N+1) \leq \delta \leq \delta^*$, then this bound is saturated according to Lemma 7. □

### 1. Auxiliary lemmas

*Lemma* 18. $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \leq 1/(N+1)$ for all $\mathbf{k} \in \mathscr{S}$ if $\nu(\Omega) \geq 1/2$.

*Proof.* If $\mathbf{k} = \mathbf{k}_0$, then $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 1$, so we have $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0 \leq 1/(N+1)$. If $\mathbf{k} \neq \mathbf{k}_0$, then

$$\begin{aligned}\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) &= \sum_{i\geq 2|k_i\geq 1} \frac{k_i}{(N+1)}\lambda_i^{k_i-1} \prod_{j\neq i|k_j\geq 1} \lambda_j^{k_j} \\ \leq \frac{N+1-k_1}{N+1}\lambda_2^{N-k_1} &\leq \frac{N+1-k_1}{N+1}\Bigl(\frac{1}{2}\Bigr)^{N-k_1} \leq \frac{1}{N+1}.\end{aligned} \tag{D12}$$

Here the second last inequality follows from the assumption $\nu(\Omega) \geq 1/2$, which means $\lambda_2 \leq 1/2$. □

Define

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) := \frac{1-\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-\zeta_{\mathbf{k}}(\boldsymbol{\lambda})}, \quad \mathbf{k} \in \mathscr{S}^*. \tag{D13}$$

*Lemma* 19. For any $\mathbf{k} \in \mathscr{S}^*$, we have

$$\frac{N\nu}{N\nu+1} \leq \xi_{\mathbf{k}}(\boldsymbol{\lambda}) \leq 1 - \tau^N, \tag{D14}$$

where $\nu = 1 - \beta$ with $\beta = \lambda_2$ and $\tau = \lambda_D$, assuming that $\lambda_1 = 1$ and $\lambda_j$ are arranged in decreasing order.

The lower bound in Eq. (D14) can be expressed as

$$\frac{N\nu}{N\nu+1} = \frac{1-\eta_{\mathbf{k}_1}(\boldsymbol{\lambda})}{1-\zeta_{\mathbf{k}_1}(\boldsymbol{\lambda})}, \tag{D15}$$

where $\mathbf{k}_1 := (N, 1, 0, \dots, 0)$.

*Proof.* Note that $\sum_j k_j = N+1$ and $k_1 \leq N$ by the assumption $\mathbf{k} \in \mathscr{S}^*$. According to Lemma 20 below,

$$\begin{aligned}\xi_{\mathbf{k}}(\boldsymbol{\lambda}) &\geq \xi_{\mathbf{k}}(1,\beta,\dots,\beta) = \xi_{(k_1,N-k_1+1)}(1,\beta) \\ &= \frac{1-\eta_{N-k_1+1}(\beta)}{1-\zeta_{N-k_1+1}(\beta)} \geq \frac{N\nu}{N\nu+1},\end{aligned} \tag{D16}$$

where the second inequality follows from Lemma 15 in Appendix C. Note that the definition of $\xi_{\mathbf{k}}(\boldsymbol{\lambda})$ (as well as that of $\eta_{\mathbf{k}}(\boldsymbol{\lambda})$ and $\zeta_{\mathbf{k}}(\boldsymbol{\lambda})$) can be extended as long as $\mathbf{k}$ and $\boldsymbol{\lambda}$ have the same number of components.

By the same token, we have

$$\begin{aligned}\xi_{\mathbf{k}}(\boldsymbol{\lambda}) &\leq \xi_{\mathbf{k}}(1,\tau,\dots,\tau) = \xi_{(k_1,N-k_1+1)}(1,\tau) \\ &= \frac{1-\eta_{N-k_1+1}(\tau)}{1-\zeta_{N-k_1+1}(\tau)} \leq 1-\tau^N,\end{aligned} \tag{D17}$$

where the two inequalities follow from Lemma 20 and Lemma 15, respectively. □

It is instructive to take a look at the special scenario in which $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0$ (cf. the proof of Lemma 1 in Appendix B), which means $k_1 = 0$, or $\lambda_i = 0$ and $k_i \geq 1$ for some $2 \leq i \leq D$. In the first case, we have $\tau^N \leq \eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leq \beta^N$, so that

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) = 1 - \eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leq 1 - \tau^N, \tag{D18}$$

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) \geq 1 - \beta^N = 1 - (1-\nu)^N \geq \frac{N\nu}{N\nu+1}. \tag{D19}$$

In the second case, we have $\tau = 0$ and

$$\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \frac{k_i\lambda_i^{k_i-1}}{N+1} \prod_{j\neq i,k_j\geq 1} \lambda_j^{k_j} \leq \frac{1}{N+1}, \tag{D20}$$

which implies that

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) = 1 - \eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leq 1 = 1 - \tau^N, \tag{D21}$$

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) \geq \frac{N}{N+1} \geq \frac{N\nu}{N\nu+1}. \tag{D22}$$

These results are compatible with Lemma 19 as expected.

*Lemma* 20. Suppose $\mathbf{k} = (k_1, k_2, \dots, k_m)$ is a sequence of $m$ nonnegative integers that satisfies $\sum_j k_j = N+1$ and $k_1 \leq N$. Let $\boldsymbol{u}, \boldsymbol{v}$ be two $m$-component vectors that satisfy $0 \leq \boldsymbol{u} \leq \boldsymbol{v} \leq 1$ and $u_1 = v_1 = 1$. Then we have $\xi_{\mathbf{k}}(\boldsymbol{u}) \geq \xi_{\mathbf{k}}(\boldsymbol{v})$.

The inequality $0 \leq \boldsymbol{u} \leq \boldsymbol{v} \leq 1$ in the above lemma means $0 \leq u_j \leq v_j \leq 1$ for all $j = 1, 2, \dots, m$.

*Proof.* By the assumption $0 \leq \boldsymbol{u} \leq \boldsymbol{v} \leq 1$ and Eq. (14), we have $\zeta_{\mathbf{k}}(\boldsymbol{u}) \leq \zeta_{\mathbf{k}}(\boldsymbol{v}) \leq k_1/(N+1) < 1$. According to Eq. (D13), $\xi_{\mathbf{k}}(\boldsymbol{u})$ is continuous in $\boldsymbol{u}$ for $0 \leq \boldsymbol{u} \leq 1$. So it suffices to prove the lemma in the case $0 < \boldsymbol{u} \leq \boldsymbol{v} \leq 1$.

For $j \geq 2$, calculation shows that

$$\begin{aligned}\frac{\partial \eta_{\mathbf{k}}(\boldsymbol{u})}{\partial u_j} &= \theta\biggl(\frac{k_j}{u_j}\sum_i \frac{k_i}{u_i} - \frac{k_j}{u_j^2}\biggr), \\ \frac{\partial \zeta_{\mathbf{k}}(\boldsymbol{u})}{\partial u_j} &= \theta\frac{k_1 k_j}{u_j},\end{aligned} \tag{D23}$$

where $\theta := \bigl(\prod_i u_i^{k_i}\bigr)/(N+1)$. These derivatives have well-defined limits when some components $u_i$ go to zero; this fact would be clearer if we insert the expression of $\theta$

and adopt lengthier expressions for these derivatives. In addition,

$$\frac{\partial \xi_{\mathbf{k}}(\boldsymbol{u})}{\partial u_j} = -\frac{\theta k_j u_j \sum_{i>1}\frac{k_i}{u_i} - \theta k_j + k_1 k_j \theta^2}{(1-k_1\theta)^2 u_j^2} < 0, \tag{D24}$$

note that $1 - k_1\theta \geq 1/(N+1)$. Therefore, $\xi_{\mathbf{k}}(\boldsymbol{u})$ is monotonically decreasing in $u_j$ for $j \geq 2$; in other words, $\xi_{\mathbf{k}}(\boldsymbol{u}) \geq \xi_{\mathbf{k}}(\boldsymbol{v})$ whenever $0 < \boldsymbol{u} \leq \boldsymbol{v} \leq 1$ and $u_1 = v_1 = 1$. The condition $0 < \boldsymbol{u} \leq \boldsymbol{v} \leq 1$ can be relaxed to $0 \leq \boldsymbol{u} \leq \boldsymbol{v} \leq 1$ by continuity. □

## Appendix E: Proofs of Lemma 8 and Theorem 5

Before proving Lemma 8 and Theorem 5, wee need to introduce a few auxiliary notations and results.

When $\Omega$ is positive definite, that is, $\tau(\Omega) > 0$, we can extend the definition of $\eta_{\mathbf{k}}(\boldsymbol{\lambda})$ and $\zeta_{\mathbf{k}}(\boldsymbol{\lambda})$ to the convex hull of $\mathscr{S}$, denoted by $\bar{\mathscr{S}}$, which is composed of vectors $\mathbf{k} = (k_1, k_2, \ldots, k_D)$ that satisfy $\sum_{j=1}^{D} k_j = N+1$ and $k_j \geq 0$ for $j = 1, 2, \ldots D$. The following analogs of $\zeta(N,\delta,\Omega)$ and $\eta(N,\delta,\Omega)$ will play important roles in proving Lemma 8 and Theorem 5. Define

$$\bar{\zeta}(N,\delta,\Omega) := \begin{cases} \min\limits_{\mathbf{k}\in\bar{\mathscr{S}}}\bigl\{\zeta_{\mathbf{k}}(\boldsymbol{\lambda})\big|\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \delta\bigr\} & \delta_{\mathrm{c}} < \delta \leq 1, \\ 0 & 0 \leq \delta \leq \delta_{\mathrm{c}}; \end{cases} \tag{E1}$$

$$\bar{\eta}(N,f,\Omega) := \max_{\mathbf{k}\in\bar{\mathscr{S}}}\bigl\{\eta_{\mathbf{k}}(\boldsymbol{\lambda})\big|\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = f\bigr\} \quad 0 \leq f \leq 1, \tag{E2}$$

where $\eta_{\mathbf{k}}(\boldsymbol{\lambda})$ and $\zeta_{\mathbf{k}}(\boldsymbol{\lambda})$ are defined in Eq. (14). By assumption all eigenvalues of $\Omega$ are positive, that is, $\lambda_j > 0$ for $j = 1, 2, \ldots, D$, so $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) > 0$ for all $\mathbf{k} \in \bar{\mathscr{S}}$.

*Lemma* 21. Suppose $\Omega$ is positive definite; then

$$\zeta(N,\delta,\Omega) \geq \bar{\zeta}(N,\delta,\Omega), \tag{E3}$$

$$\eta(N,f,\Omega) \leq \bar{\eta}(N,f,\Omega). \tag{E4}$$

*Proof of Lemma 21.* When $\delta$ satisfies $0 \leq \delta \leq \delta_{\mathrm{c}}$, we have $\bar{\zeta}(N,\delta,\Omega) = 0 \leq \zeta(N,\delta,\Omega)$ by definition, so Eq. (E3) holds in this case.

When $\delta > \delta_{\mathrm{c}}$, according to Lemma 13, we can find two vectors $\mathbf{q}_0, \mathbf{q}_1 \in \mathscr{S}$ such that $\eta_0 \leq \delta \leq \eta_1$ and $\zeta(N,\delta,\Omega) = c_0\zeta_0 + c_1\zeta_1$, where $\eta_j = \eta_{\mathbf{q}_j}(\boldsymbol{\lambda})$ and $\zeta_j = \zeta_{\mathbf{q}_j}(\boldsymbol{\lambda})$ for $j = 0, 1$; here $c_0$ and $c_1$ are nonnegative coefficients determined by the requirements $c_0 + c_1 = 1$ and $c_0\eta_0 + c_1\eta_1 = \delta$, that is,

$$c_0 = \frac{\eta_1 - \delta}{\eta_1 - \eta_0}, \quad c_1 = \frac{\delta - \eta_0}{\eta_1 - \eta_0}. \tag{E5}$$

Let $F_j = \zeta_j/\eta_j$ for $j = 0, 1$, then $F_0 < F_1$ by Lemma 13. Geometrically, the point $(\delta, \zeta(N,\delta,\Omega))$ lies on the line segment that connects the two points $(\eta_0, \zeta_0)$ and $(\eta_1, \zeta_1)$, which has slope $(\zeta_1 - \zeta_0)/(\eta_1 - \eta_0)$. If $\delta = \eta_0$ or $\delta = \eta_1$, then Eq. (E3) follows from the fact that $\mathscr{S} \in \bar{\mathscr{S}}$. So it remains to consider the scenario $\eta_0 < \delta < \eta_1$, in which case $0 < c_0, c_1 < 1$.

For $0 \leq t \leq 1$, let

$$\mathbf{k}(t) = \mathbf{q}_0(1-t) + \mathbf{q}_1 t = \mathbf{q}_0 + (\mathbf{q}_1 - \mathbf{q}_0)t, \tag{E6}$$

$$\eta(t) = \eta_{\mathbf{k}(t)}(\boldsymbol{\lambda}), \quad \zeta(t) = \zeta_{\mathbf{k}(t)}(\boldsymbol{\lambda}), \tag{E7}$$

$$F(t) = \frac{\zeta(t)}{\eta(t)} = \frac{k_1(t)}{\sum_j \frac{k_j(t)}{\lambda_j}}. \tag{E8}$$

Note that $\mathbf{k}(t) \in \bar{\mathscr{S}}$ for $0 \leq t \leq 1$; in addition, $\eta(0) = \eta_0$, $\zeta(0) = \zeta_0$, $F(0) = F_0$, while $\eta(1) = \eta_1$, $\zeta(1) = \zeta_1$, $F(1) = F_1$. So Eq. (E7) defines a parametric curve $(\eta(t), \zeta(t))$ that connects $(\eta_0, \zeta_0)$ and $(\eta_1, \zeta_1)$. Let $t_\delta$ be the smallest value of $t$ such that $\eta(t) = \delta$. Then $\bar{\zeta}(N,\delta,\Omega) \leq \zeta(t_\delta)$. So it remains to prove $\zeta(t_\delta) \leq \zeta(N,\delta,\Omega)$ in order to prove Eq. (E3).

To achieve our goal, we shall prove that the parametric curve $(\eta(t), \zeta(t))$ for $0 \leq t \leq t_\delta$ lies below the line segment passing the two points $(\eta_0, \zeta_0)$ and $(\eta_1, \zeta_1)$. To this end, we need to analyze the convexity (or concavity) property of the curve, which depends on the second derivative

$$\frac{d\zeta(t)^2}{d\eta(t)^2} = \frac{\zeta''(t)\eta'(t) - \eta''(t)\zeta'(t)}{\eta'(t)^3}. \tag{E9}$$

Here the derivatives with respect to $t$ can be computed explicitly by virtue of Eq. (14), with the result

$$\eta'(t) = \frac{d\eta(t)}{dt} = \eta(t)\sum_j (q_{1j} - q_{0j})\ln\lambda_j + \theta(t)\frac{q_{1j} - q_{0j}}{\lambda_j} = \eta(t)\Bigl[\ln\frac{\theta_1}{\theta_0} + \frac{\theta(t)}{\eta(t)}\Bigl(\frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0}\Bigr)\Bigr], \tag{E10}$$

$$\zeta'(t) = \frac{d\zeta(t)}{dt} = \zeta(t)\sum_j (q_{1j} - q_{0j})\ln\lambda_j + \theta(t)(q_{11} - q_{01}) = \theta(t)\Bigl[k_1(t)\ln\frac{\theta_1}{\theta_0} + (q_{11} - q_{01})\Bigr], \tag{E11}$$

$$\eta''(t) = \frac{d^2\eta(t)}{dt^2} = \eta(t)\Bigl(\ln\frac{\theta_1}{\theta_0}\Bigr)\Bigl[\ln\frac{\theta_1}{\theta_0} + \frac{2\theta(t)}{\eta(t)}\Bigl(\frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0}\Bigr)\Bigr], \tag{E12}$$

$$\zeta''(t) = \frac{d^2\zeta(t)}{dt^2} = \theta(t)\Bigl(\ln\frac{\theta_1}{\theta_0}\Bigr)\Bigl[k_1(t)\ln\frac{\theta_1}{\theta_0} + 2(q_{11} - q_{01})\Bigr], \tag{E13}$$

where

$$\theta(t)=\frac{1}{N+1}\prod_j \lambda_j^{k_j(t)},\quad \theta_0=\theta(t=0)=\frac{1}{N+1}\prod_j \lambda_j^{q_{0j}},\quad \theta_1=\theta(t=1)=\frac{1}{N+1}\prod_j \lambda_j^{q_{1j}}. \tag{E14}$$

Note that

$$\eta(t)=\theta(t)\sum_j \frac{k_j(t)}{\lambda_j},\quad \zeta(t)=\theta(t)k_1(t). \tag{E15}$$

Therefore,

$$\begin{aligned}\zeta''(t)\eta'(t)-\eta''(t)\zeta'(t)&=\theta(t)^2\Big(\ln\frac{\theta_1}{\theta_0}\Big)^2\Big[(q_{11}-q_{01})\frac{\eta(t)}{\theta(t)}-\Big(\frac{\eta_1}{\theta_1}-\frac{\eta_0}{\theta_0}\Big)k_1(t)\Big]\\
&=\theta(t)^2\Big(\ln\frac{\theta_1}{\theta_0}\Big)^2\Big[(q_{11}-q_{01})\sum_j\frac{q_{0j}+(q_{1j}-q_{0j})t}{\lambda_j}-\Big(\frac{\eta_1}{\theta_1}-\frac{\eta_0}{\theta_0}\Big)[q_{01}+(q_{11}-q_{01})t]\Big]\\
&=\theta(t)^2\Big(\ln\frac{\theta_1}{\theta_0}\Big)^2\Big(\frac{\eta_0q_{11}}{\theta_0}-\frac{\eta_1q_{01}}{\theta_1}\Big)=\theta(t)^2\Big(\ln\frac{\theta_1}{\theta_0}\Big)^2\frac{\eta_0\eta_1}{\theta_0\theta_1}\Big(\frac{\theta_1q_{11}}{\eta_1}-\frac{\theta_0q_{01}}{\theta_0}\Big)\\
&=\theta(t)^2\Big(\ln\frac{\theta_1}{\theta_0}\Big)^2\frac{\eta_0\eta_1}{\theta_0\theta_1}(F_1-F_0)>0.\end{aligned} \tag{E16}$$

So the sign of $\frac{d\zeta(t)^2}{d\eta(t)^2}$ is identical with that of $\eta'(t)$.

Note that $\eta(t)/\theta(t)$ is a linear function of $t$ and $\eta(t)/\theta(t)>0$ for $0\le t\le 1$. So $\eta'(t)/\eta(t)$ is monotonic in $t$ for $0\le t\le 1$ according to Eq. (E10); actually, $\eta'(t)/\eta(t)$ is strictly monotonic in $t$ unless $\eta'(t)/\eta(t)$ is a positive constant. When $t=0$, we have

$$\begin{aligned}\eta'(0)&=\eta_0\Big[\ln\frac{\theta_1}{\theta_0}+\Big(\frac{\eta_1\theta_0}{\theta_1\eta_0}-1\Big)\Big]\\
&>\eta_0\Big[\ln\frac{\theta_1}{\theta_0}+\Big(\frac{\theta_0}{\theta_1}-1\Big)\Big]\ge 0.\end{aligned} \tag{E17}$$

It follows that $\eta'(t)$ has at most one zero point in the interval $0\le t\le 1$. If $\eta'(t)>0$ in this interval, then $\frac{d\zeta(t)^2}{d\eta(t)^2}\ge 0$, so $\zeta(t)$ is a convex function of $\eta(t)$ for $0\le t\le 1$, and the parametric curve $(\eta(t),\zeta(t))$ lies below the line segment that connects the two points $(\eta_0,\zeta_0)$ and $(\eta_1,\zeta_1)$, which implies Eq. (E3). Otherwise, $\eta'(t)$ has a unique zero point $0<t_2\le 1$. If $t_2=1$, the same conclusion holds. If $t_2<1$, then $\eta'(t)>0$ for $0\le t<t_2$ and $\eta'(t)<0$ for $t_2<t\le 1$, which implies that $\eta(t_2)>\eta_1$. So there exists a unique real number $t_3$ that satisfies the conditions $0<t_3<t_2$ and $\eta(t_3)=\eta_1$. Note that $\zeta(t)$ is convex in $\eta(t)$ for $0\le t\le t_3$ and that $t_\delta<t_3$. To prove Eq. (E3), it suffices to prove the inequality $\zeta(t_3)\le\zeta_1$, that is, $F(t_3)\le F_1$.

To proceed, we compute the derivative of $F(t)$, with the result

$$\frac{dF(t)}{dt}=\frac{\theta(t)^2}{\eta(t)^2}\frac{\eta_0\eta_1}{\theta_0\theta_1}(F_1-F_0)>0. \tag{E18}$$

This derivative can be derived either from Eq. (E8) or from Eqs. (E10) and (E11). So $F(t)$ increases monotonically with $t$, which implies that $F(t_3)\le F(1)=F_1$. This observation implies that the parametric curve $(\eta(t),\zeta(t))$ for $0\le t\le t_3$ lies below the line segment that connects the two points $(\eta_0,\zeta_0)$ and $(\eta_1,\zeta_1)$, which confirms Eq. (E3).

Equation (E4) can be proved using a similar reasoning used for proving Eq. (E3). In view of Eq. (E16) and the following equation

$$\frac{d\eta(t)^2}{d\zeta(t)^2}=-\frac{\zeta''(t)\eta'(t)-\eta''(t)\zeta'(t)}{\zeta'(t)^3}, \tag{E19}$$

the sign of $\frac{d\eta(t)^2}{d\zeta(t)^2}$ is opposite to that of $\zeta'(t)$. When $t=0$, we have

$$\zeta'(0)=\theta_0\Big[q_{01}\ln\frac{\theta_1}{\theta_0}+(q_{11}-q_{01})\Big]. \tag{E20}$$

If $q_{01}=0$, then $\zeta'(0)=\theta_0q_{11}>0$. If $q_{01}>0$, then $\zeta_0=\theta_0q_{01}>0$ and

$$\begin{aligned}\zeta'(0)&=\theta_0q_{01}\Big(\ln\frac{\theta_1}{\theta_0}+\frac{q_{11}}{q_{01}}-1\Big)=\zeta_0\Big(\ln\frac{\theta_1}{\theta_0}+\frac{\zeta_1\theta_0}{\zeta_0\theta_1}-1\Big)\\
&>\zeta_0\Big(\ln\frac{\theta_1}{\theta_0}+\frac{\theta_0}{\theta_1}-1\Big)\ge 0.\end{aligned} \tag{E21}$$

So the inequality $\zeta'(0)>0$ holds in both cases. In addition, $\theta(t)>0$ and $\zeta'(t)/\theta(t)$ is a linear and thus monotonic function of $t$ for $0\le t\le 1$ according to Eq. (E11). Therefore, $\zeta'(t)$ has at most one zero point in the interval $0\le t\le 1$ as is the case for $\eta'(t)$. Now Eq. (E4) can be proved based on a similar reasoning presented after Eq. (E17), though "convex" is replaced by "concave". □

*Lemma* 22. Suppose $1 > x_1 \ge x_2 \ge \cdots, x_m > 0$ and $c$ is a negative constant. Then

$$\max_{a_1,a_2,\ldots,a_m\ge 0}\biggl\{\sum_j \frac{a_j}{x_j}\biggm|\sum_j a_j\ln x_j = c\biggr\} = \frac{c}{y\ln y}, \tag{E22}$$

where $y = x_1$ if $x_1\ln x_1^{-1} \le x_m \ln x_m^{-1}$ and $y = x_m$ otherwise.

*Proof.* The maximization in Eq. (E22) is a linear programming, so the maximum can be attained at one of the extremal points of the feasible region defined by the inequality $a_1, a_2, \ldots, a_m \ge 0$ and the equality $\sum_j a_j \ln x_j = c$. All the extremal points have the form

$$a_j = \frac{c}{\ln x_j}, \quad x_i = 0 \quad i \neq j, \quad j = 1,2,\ldots,m. \tag{E23}$$

Therefore,

$$\begin{aligned}&\max_{a_1,a_2,\ldots,a_m\ge 0}\biggl\{\sum_j \frac{a_j}{x_j}\biggm|\sum_j a_j\ln x_j = c\biggr\} = \max_j \frac{c}{x_j\ln x_j}\\ &= \max\biggl\{\frac{c}{x_1\ln x_1}, \frac{c}{x_m \ln x_m}\biggr\} = \frac{c}{y\ln y}.\end{aligned} \tag{E24}$$

Here the second equality follows from the assumption $1 > x_1 \ge x_2 \ge \cdots, x_m > 0$ and the fact that the function $c/(x\ln x)$ is convex in $x$, given that $c$ is negative. □

Now we are ready to prove Lemma 8.

*Proof of Lemma 8.* According to Lemma 21,

$$\begin{aligned}\mathcal{F}(N,f,\Omega) &= \frac{f}{\eta(N,f,\Omega)} \ge \frac{f}{\bar\eta(N,f,\Omega)}\\ &= \min_{\mathbf{k}\in\mathscr{S}|\zeta_{\mathbf{k}}(\boldsymbol{\lambda})=f} \frac{k_1}{\sum_j (k_j/\lambda_j)}\\ &= \min_{\mathbf{k}\in\mathscr{S}|\zeta_{\mathbf{k}}(\boldsymbol{\lambda})=f} \frac{k_1}{k_1 + \sum_{j=2}^D (k_j/\lambda_j)}.\end{aligned} \tag{E25}$$

The condition $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = f$ entails the following inequality,

$$f = \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = \frac{k_1}{N+1}\prod_j \lambda_j^{k_j} \le \prod_{j=2}^D \lambda_j^{k_j} \le \beta^{N+1-k_1}, \tag{E26}$$

which implies that $N + 1 - k_1 \le \ln f/\ln\beta = \log_\beta f$, that is, $k_1 \ge N + 1 - (\ln f/\ln\beta)$. In addition, the above equation implies that $0 > \sum_{j=2}^D k_j \ln\lambda_j \ge \ln f$, which in turn implies that $\sum_{j=2}^D (k_j/\lambda_j) \le \ln f/(\tilde\beta\ln\tilde\beta)$ in view of Lemma 22. Therefore,

$$\begin{aligned}\mathcal{F}(N,f,\Omega) &\ge \frac{N+1-(\ln\beta)^{-1}(\ln f)}{N+1-(\ln\beta)^{-1}(\ln f)+\sum_{j=2}^D(k_j/\lambda_j)}\\ &\ge \frac{N+1-(\ln\beta)^{-1}(\ln f)}{N+1-(\ln\beta)^{-1}(\ln f)+(\tilde\beta\ln\tilde\beta)^{-1}\ln f}.\end{aligned} \tag{E27}$$

□

*Proof of Theorem 5.* Equation (94) follows from Eq. (17) and Theorem 3 in the main text. The lower bound in Eq. (95) follows from Eq. (94) given that $\tilde\beta = \beta = \lambda_2$ or $\tilde\beta = \tau = \lambda_D$.

To prove the upper bound in Eq. (95), let $f = F\delta$ and

$$N = \biggl\lceil \frac{1-\epsilon}{\epsilon}\frac{\ln(F\delta)}{\tilde\beta\ln\tilde\beta} + \frac{\ln(F\delta)}{\ln\beta} - 1\biggr\rceil; \tag{E28}$$

then Lemma 8 implies that

$$\begin{aligned}\mathcal{F}(N,f,\Omega) &\ge \frac{N+1-(\ln\beta)^{-1}(\ln f)}{N+1-(\ln\beta)^{-1}(\ln f)+(\tilde\beta\ln\tilde\beta)^{-1}\ln f}\\ &\ge \frac{\frac{1-\epsilon}{\epsilon}\frac{\ln f}{\tilde\beta\ln\tilde\beta}}{\frac{1-\epsilon}{\epsilon}\frac{\ln f}{\tilde\beta\ln\tilde\beta}+(\tilde\beta\ln\tilde\beta)^{-1}\ln f} = 1-\epsilon.\end{aligned} \tag{E29}$$

In conjunction with Lemma 6 this equation implies that $N(\epsilon,\delta,\Omega) \le N$, which confirms the first upper bound in Eq. (95).

By definition, $|\tilde\beta\ln\tilde\beta| \le |\beta\ln\beta| < |\ln\beta|$. Therefore,

$$N \le \biggl\lceil \frac{\ln(F\delta)}{\epsilon\tilde\beta\ln\tilde\beta} - 1\biggr\rceil < \frac{\ln(F\delta)}{\epsilon\tilde\beta\ln\tilde\beta}, \tag{E30}$$

which confirms the second upper bound in Eq. (95). □

## Appendix F: Proofs of Lemmas 9-11

*Proof of Lemma 9.* By Eqs. (105) and (106) in the main text, it is clear that $p_*(\nu, 1-\nu)$ is nondecreasing in $\nu$, and $h_*(\nu, 1-\nu)$ is nonincreasing in $\nu$. If $1-\mathrm{e}^{-1} \le \nu \le 1$, then

$$\nu h_*(\nu,1-\nu) = \mathrm{e}\nu \ge \mathrm{e}(1-\mathrm{e}^{-1}) = \mathrm{e}-1 > 1, \tag{F1}$$

and $\nu h_*(\nu, 1-\nu)$ is strictly increasing in $\nu$. On the other hand, i f $0 < \nu \le 1-\mathrm{e}^{-1}$, then

$$\nu h_*(\nu,1-\nu) = \nu\bigl[(1-\nu)\ln(1-\nu)^{-1}\bigr]^{-1} > 1. \tag{F2}$$

By computing the derivative of $\nu h_*(\nu, 1-\nu)$ over $\nu$ [cf. Eq. (F5) with $p = 0$] it is straightforward to verify that $\nu h_*(\nu, 1-\nu)$ is strictly increasing in $\nu$. In conjunction with Eq. (F1), we conclude that $\nu h_*(\nu, 1-\nu) > 1$ and it is strictly increasing in $\nu$ for $0 < \nu \le 1$. In addition,

$$\lim_{\nu\to 0}\nu h_*(\nu,1-\nu) = \lim_{\nu\to 0}\nu\bigl[(1-\nu)\ln(1-\nu)^{-1}\bigr]^{-1} = 1. \tag{F3}$$

By definition

$$\nu h(p,\nu,1-\nu) = \nu\bigl(\beta_p\ln\beta_p^{-1}\bigr)^{-1}, \tag{F4}$$

where $\beta_p = 1-\nu+p\nu$. The derivative of $\nu h(p,\nu,1-\nu)$ over $\nu$ reads

$$\frac{d}{d\nu}\biggl(\frac{\nu}{\beta_p\ln\beta_p^{-1}}\biggr) = -\frac{(1-p)\nu+\ln(1-\nu+p\nu)}{[(1-\nu+p\nu)\ln(1-\nu+p\nu)]^2} > 0, \tag{F5}$$

where the last inequality follows from the simple fact that $\ln(1+x) < x$ when $x > -1$ and $x \neq 0$. Incidentally, the derivative in Eq. (F5) approaches $1/2$ in the limit $\nu \to 0$. Therefore, $\nu h(p,\nu,1-\nu)$ increases strictly monotonically with $\nu$. □

*Proof of Lemma 10.* We shall prove the seven statements of Lemma 10 in the order 1, 6, 2; 3, 4; 7, 5.

Recall that $p_*(\nu,\tau)$ is the smallest value of $p \geq 0$ that satisfies $\tau_p \ln \tau_p^{-1} \geq \beta_p \ln \beta_p^{-1}$. Let $q = p_*(\nu,\tau)$; then $0 \leq q < 1$. Suppose $0 < \nu' \leq \nu$; let $\beta' = 1 - \nu'$. Then we have $1 > \beta' \geq \beta \geq 0$ and $1 > \beta_q' \geq \beta_q \geq 1/\mathrm{e}$, so that

$$\beta_q' \ln {\beta_q'}^{-1} \leq \beta_q \ln \beta_q^{-1} \leq \tau_q \ln \tau_q^{-1}, \tag{F6}$$

which implies that $p_*(\nu',\tau) \leq q = p_*(\nu,\tau)$, that is, $p_*(\nu,\tau)$ is nondecreasing in $\nu$.

In addition, $\tau_p \leq \beta_p \leq \beta_p'$, which implies that

$$\beta_p \ln {\beta_p}^{-1} \geq \min\bigl\{\beta_p' \ln {\beta_p'}^{-1}, \tau_p \ln \tau_p^{-1}\bigr\} \tag{F7}$$

and that

$$\begin{aligned} h(p,\nu',\tau) &= \bigl[\min\bigl\{\beta_p' \ln {\beta_p'}^{-1}, \tau_p \ln \tau_p^{-1}\bigr\}\bigr]^{-1} \\ &\geq \bigl[\min\bigl\{\beta_p \ln \beta_p^{-1}, \tau_p \ln \tau_p^{-1}\bigr\}\bigr]^{-1} = h(p,\nu,\tau). \end{aligned} \tag{F8}$$

So $h(p,\nu,\tau)$ is nonincreasing in $\nu$. When $p = p_*(\nu',\tau)$, the above equation implies that

$$h_*(\nu',\tau) = h(p,\nu',\tau) \geq h(p,\nu,\tau) \geq h_*(\nu,\tau). \tag{F9}$$

So $h_*(\nu,\tau)$ is also nonincreasing in $\nu$.

Next, suppose $\tau \leq \tau' \leq \beta$. Then $\tau_q \leq \tau_q' \leq \beta_q$ and

$$\tau_q' \ln {\tau_q'}^{-1} \geq \min\{\beta_q \ln \beta_q^{-1}, \tau_q, \ln \tau_q^{-1}\} = \beta_q \ln \beta_q^{-1}, \tag{F10}$$

which implies that $p_*(\nu,\tau') \leq q = p_*(\nu,\tau)$, that is, $p_*(\nu,\tau)$ is nonincreasing in $\tau$. This observation confirms statement 1 of Lemma 10 given that $p_*(\nu,\tau)$ is nondecreasing in $\nu$ according to the above analysis.

In addition, $\tau_p \leq \tau_p' \leq \beta_p$, which implies that

$$\tau_p' \ln {\tau_p'}^{-1} \geq \min\bigl\{\beta_p \ln {\beta_p}^{-1}, \tau_p \ln {\tau_p}^{-1}\bigr\} \tag{F11}$$

and that

$$\begin{aligned} h(p,\nu,\tau') &= \bigl[\min\bigl\{\beta_p \ln {\beta_p}^{-1}, \tau_p' \ln {\tau_p'}^{-1}\bigr\}\bigr]^{-1} \\ &\leq \bigl[\min\bigl\{\beta_p \ln \beta_p^{-1}, \tau_p \ln \tau_p^{-1}\bigr\}\bigr]^{-1} = h(p,\nu,\tau). \end{aligned} \tag{F12}$$

So $h(p,\nu,\tau)$ is nonincreasing in $\tau$, which confirms statement 6 of Lemma 10 in view of the above conclusion. When $p = p_*(\nu,\tau)$, Eq. (F12) implies

$$h_*(\nu,\tau) = h(p,\nu,\tau) \geq h(p,\nu,\tau') \geq h_*(\nu,\tau'). \tag{F13}$$

So $h_*(\nu,\tau)$ is also nonincreasing in $\tau$, which confirms statement 2 of Lemma 10.

Next, consider statements 3 and 4 in Lemma 10. By Lemma 9 and statement 2 in Lemma 10 proved above, we have $\nu h_*(\nu,\tau) \geq \nu h_*(\nu, 1-\nu) > 1$, which confirms statement 3 in Lemma 10. In addition,

$$\lim_{\nu\to 0} \nu h_*(\nu,\tau) \geq \lim_{\nu\to 0} \nu h_*(\nu,1-\nu) = 1. \tag{F14}$$

On the other hand,

$$\lim_{\nu\to 0} \nu h_*(\nu,\tau) \leq \lim_{\nu\to 0} \nu h(\nu,\nu,\tau) = 1, \tag{F15}$$

which implies that $\lim_{\nu\to 0} \nu h_*(\nu,\tau) = 1$ and confirms statement 4 in Lemma 10 given the opposite inequality derived above.

Finally, we can prove statements 7 and 5 in Lemma 10. By definition

$$\nu h(p,\nu,\tau) = \max\Bigl\{\nu\bigl(\beta_p \ln \beta_p^{-1}\bigr)^{-1}, \nu\bigl(\tau_p \ln \tau_p^{-1}\bigr)^{-1}\Bigr\}, \tag{F16}$$

where $\beta_p = 1 - \nu + p\nu$. It is clear that $\nu\bigl(\tau_p \ln \tau_p^{-1}\bigr)^{-1}$ increases strictly monotonically with $\nu$. The same conclusion holds for $\nu\bigl(\beta_p \ln \beta_p^{-1}\bigr)^{-1}$ according to the derivative in Eq. (F5). Therefore, $\nu h(p,\nu,\tau)$ increases strictly monotonically with $\nu$, which confirms statement 7 in Lemma 10.

Suppose $0 < \nu' < \nu \leq 1$. Let $p = p_*(\nu,\tau)$; note that $p > 0$ if $\tau = 0$, so that $\tau_p > 0$. Therefore,

$$\nu' h_*(\nu',\tau) \leq \nu' h(p,\nu',\tau) < \nu h(p,\nu,\tau) = \nu h_*(\nu,\tau). \tag{F17}$$

So $\nu h_*(\nu,\tau)$ increases strictly monotonically with $\nu$, which confirms statement 5 in Lemma 10. □

*Proof of Lemma 11.* By definition we have $p_0 = \nu/\mathrm{e}$ and $\beta_{p_0} = 1 - \nu + (\nu^2/\mathrm{e})$. From the assumption $0 < \nu \leq 1$ we can deduce that

$$\ln \beta_{p_0}^{-1} = -\ln\Bigl(1 - \nu + \frac{\nu^2}{\mathrm{e}}\Bigr) \geq \nu. \tag{F18}$$

Here the inequality can be proved by inspecting the derivative of the function $-\ln\Bigl(1-\nu+\frac{\nu^2}{\mathrm{e}}\Bigr)-\nu$. It follows that

$$\beta_{p_0} \ln \beta_{p_0}^{-1} \geq \Bigl(1 - \nu + \frac{\nu^2}{\mathrm{e}}\Bigr)\nu. \tag{F19}$$

In addition,

$$p_0 \ln(p_0^{-1}) = \frac{\nu}{\mathrm{e}} \ln \frac{\mathrm{e}}{\nu} \geq \Bigl(1 - \nu + \frac{\nu^2}{\mathrm{e}}\Bigr)\nu. \tag{F20}$$

Therefore,

$$\nu h(p_0,\nu,\tau) \leq \Bigl(1 - \nu + \frac{\nu^2}{\mathrm{e}}\Bigr)^{-1} \leq 1 + (\mathrm{e}-1)\nu \leq \mathrm{e}, \tag{F21}$$

which confirms Eq. (115) and implies Eq. (114) in Lemma 11. Here the second inequality follows from the inequality below

$$\begin{aligned} &\Bigl(1 - \nu + \frac{\nu^2}{\mathrm{e}}\Bigr)[1 + (\mathrm{e}-1)\nu] \\ &\quad = 1 + \nu\Bigl[\Bigl(1 - \frac{1}{\mathrm{e}}\Bigr)\nu^2 - \Bigl(\mathrm{e} - 1 - \frac{1}{\mathrm{e}}\Bigr)\nu + \mathrm{e} - 2\Bigr] \geq 1, \end{aligned} \tag{F22}$$

note that the term in the square brackets is nonnegative for $0 \leq \nu \leq 1$. □

## Appendix G: Proof of Theorem 8

In this section we present an independent proof of Theorem 8, which was originally proved in Ref. [47]. This theorem is an immediate consequence of Lemmas 24 and 25 presented below. Before stating and proving these auxiliary results, we need to introduce a few additional concepts. Let $|\Psi\rangle\langle\Psi|$ be an $n$-partite pure state of the parties $V = \{1, 2, \ldots, n\}$. For each nonempty proper subset $A$ of $V$, denote by $\varrho_A$ the reduced state of $|\Psi\rangle\langle\Psi|$ over the parties in $A$, that is, $\varrho_A = \mathrm{tr}_{(V\setminus A)}(|\Psi\rangle\langle\Psi|)$. Define

$$\kappa(|\Psi\rangle) := \max_A \|\varrho_A\|, \tag{G1}$$

where $\|\varrho_A\|$ denotes the operator norm (the largest eigenvalue) of $\varrho_A$ and the maximum is taken over all nonempty proper subsets $A$ of $V$. Note that $\kappa(|\Psi\rangle)$ is invariant under local unitary transformations. Given a hypergraph $G$, define $\kappa(G) := \kappa(|G\rangle)$.

Lemmas 23 and 24 below were known before [2], but we provide self-contained proofs for completeness.

*Lemma* 23. The state $|\Psi\rangle$ is GME iff $\kappa(|\Psi\rangle) < 1$.

*Proof.* To prove the lemma, it is equivalent to prove the statement that the state $|\Psi\rangle$ is biseparable iff $\kappa(|\Psi\rangle) = 1$. If $\kappa(|\Psi\rangle) = 1$, then $|\Psi\rangle$ has a nontrivial reduced state that is pure, which implies that $|\Psi\rangle$ is biseparable. Conversely, if $|\Psi\rangle$ is biseparable, then it has a nontrivial reduced state that is pure, which implies that $\kappa(|\Psi\rangle) = 1$. □

*Lemma* 24. Suppose $|\Psi\rangle$ is GME and a state $\rho$ satisfies $\langle\Psi|\rho|\Psi\rangle > \kappa(|\Psi\rangle)$. Then $\rho$ is GME.

*Proof.* Suppose $|\Phi\rangle$ is an arbitrary pure state that is biseparable over the partition $A$ and $V \setminus A$, that is, $|\Phi\rangle$ has the form $|\Phi\rangle = |\Phi_A\rangle \otimes |\Phi_{V\setminus A}\rangle$. Then

$$|\langle\Psi|\Phi\rangle|^2 \leq \langle\Phi_A|\varrho_A|\Phi_A\rangle \leq \|\varrho_A\| \leq \kappa(|\Psi\rangle), \tag{G2}$$

where $\varrho_A$ is the reduced state of $|\Psi\rangle\langle\Psi|$ over the parties in $A$. If $\rho$ is not GME, then it is a convex combination of biseparable states, so that $\langle\Psi|\rho|\Psi\rangle \leq \kappa(|\Psi\rangle)$. Therefore, $\rho$ is GME whenever $\langle\Psi|\rho|\Psi\rangle > \kappa(|\Psi\rangle)$. □

*Lemma* 25. Suppose $G$ is a connected order-$k$ hypergraph with $n \geq k \geq 2$. Then $\kappa(G) \leq 1 - 2^{1-k}$.

*Proof.* This lemma is an easy consequence of Lemma 26 below. When $|G\rangle$ is a connected graph state, Lemma 25 is known much earlier [2, 48, 49], in which case the bound $\kappa(G) \leq 1-2^{1-k}$ with $k = 2$ is always saturated. This conclusion follows from the fact that any nontrivial reduced density matrix of the graph state $|G\rangle\langle G|$ is proportional to a projector of rank at least 2. □

Besides the application in proving Theorem 8, Lemma 25 shows that any order-$k$ hypergraph state $|G\rangle$ with $k \geq 2$ and $\kappa(G) = 1 - 2^{1-k}$ is not equivalent to any order-$k'$ hypergraph state with $k' < k$ under local unitary transformations.

The bound $\kappa(G) \leq 1 - 2^{1-k}$ is saturated if $G$ contains an order-$k$ leaf. Here a leaf of $G$ is a vertex that belongs to only one hyperedge with order at least 2. The order of the leaf is the order of this unique hyperedge. In this case $\|\varrho_A\| = 1 - 2^{1-k}$ when $A$ is composed of the leaf. To verify this claim, it suffices to consider the scenario in which $n = k$ and $G$ contains a single hyperedge (which necessarily has order $k$). Now it is straightforward to verify that each single-qubit reduced state of $|G\rangle$ has two eigenvalues equal to $1 - 2^{1-k}$ and $2^{1-k}$, respectively, so the bound $\kappa(G) \leq 1-2^{1-k}$ is indeed saturated. In particular, the above observation implies that $\kappa(G) = 1 - 2^{1-k}$ when $|G\rangle$ is a 1D order-$k$ cluster state. Straightforward calculations also show that the bound $\kappa(G) \leq 1 - 2^{1-k}$ is saturated for 2D order-3 cluster states and Union Jack states for which $\kappa(G) = 3/4$.

*Lemma* 26. Suppose $G = (V, E)$ is a hypergraph and $A$ is any nonempty proper subset of $V$ that is adjacent to $V \setminus A$. Let $\varrho_A$ be the reduced state of $|G\rangle$ over the parties in $A$. Then $\|\varrho_A\| \leq 1 - 2^{1-k}$, where $k$ is the maximal order of hyperedges that connect $A$ and $V \setminus A$.

Here two disjoint nonempty subsets $A$ and $B$ of the vertex set $V$ of $G$ are adjacent if $E$ contains a hyperedge that connects a vertex in $A$ and a vertex in $B$.

*Proof.* We shall prove Lemma 26 by induction. Note that $n \geq k \geq 2$ by assumption, where $n = |V|$. It is straightforward to verify that the lemma holds when $n = k = 2$. Suppose the lemma holds for $2 \leq k \leq n \leq n_0$ with $n_0 \geq 2$. We shall prove that the lemma also holds for $2 \leq k \leq n = n_0 + 1$.

It is instructive to note that $\|\varrho_A\|$ does not change if we add or delete hyperedges among vertices in $A$ or hyperedges among vertices in $V \setminus A$. So we may assume that $G$ has neither hyperedges among vertices in $A$ nor hyperedges among vertices in $V \setminus A$; in other words, every hyperedge of $G$ contains at least one vertex in $A$ and one vertex in $V \setminus A$. Then $k$ is equal to the order of $G$. In addition, we may assume that $G$ has no isolated vertices. Note that the order of $G$ does not change if any isolated vertex, say $j$, is deleted; meanwhile, $\varrho_A$ does not change after this deletion if $j \in V \setminus A$, while $\|\varrho_A\| = \|\varrho_{A\setminus\{j\}}\|$ if $j \in A$. Furthermore, we may assume $|A| \leq n - 2$ without loss of generality given that $\|\varrho_A\| = \|\varrho_{V\setminus A}\|$. By relabeling the parties if necessary, we may assume that $n \notin A$, that is, $n \in V \setminus A$.

According to Proposition 7.16 of Ref. [51],

$$\varrho_{V\setminus\{n\}} = \frac{1}{2}(|G_0\rangle\langle G_0| + |G_1\rangle\langle G_1|), \tag{G3}$$

where $G_0, G_1$ are subhypergraphs of $G$ defined as follows

$$\begin{aligned} G_0 &= (V \setminus \{n\}, \{e \in E \,|\, n \notin e\}), \\ G_1 &= (V \setminus \{n\}, \{e \in E \,|\, n \notin e\} \Delta \{e \setminus \{n\} \,|\, n \in e \in E\}). \end{aligned} \tag{G4}$$

Here $A\Delta B$ denotes the symmetric difference of $A$ and $B$, that is, $(A \cup B) \setminus (A \cap B)$. Literally, $G_0$ is the subhypergraph of $G$ obtained by deleting the vertex $n$ and all the hyperedges containing $n$; $G_1$ is the subhypergraph of $G$ obtained by deleting the vertex $n$, shrinking all the hyperedges containing $n$, and then deleting repeated hyperedges.

Let $B = V\setminus\{n\}\setminus A$; note that $B$ is nonempty due to the assumption $|A| \leq n-2$. In addition, $A \cup B = V \setminus \{n\}$ is the vertex set of both $G_0$ and $G_1$. Let $\varrho_0 = \operatorname{tr}_B(|G_0\rangle\langle G_0|)$ and $\varrho_1 = \operatorname{tr}_B(|G_1\rangle\langle G_1|)$. Then $\varrho_A = (\varrho_0 + \varrho_1)/2$ and

$$\|\varrho_A\| \leq \frac{1}{2}(\|\varrho_0\| + \|\varrho_1\|). \tag{G5}$$

If $A$ is adjacent to $B$ with respect to both $G_0$ and $G_1$, then the induction hypothesis implies that

$$\|\varrho_0\| \leq 1-2^{1-k_0} \leq 1-2^{1-k}, \quad \|\varrho_1\| \leq 1-2^{1-k_1} \leq 1-2^{1-k}, \tag{G6}$$

which in turn implies that $\|\varrho_A\| \leq 1-2^{1-k}$. Here $k_0$ and $k_1$ denote the orders of $G_0$ and $G_1$, respectively, which satisfy $k_0, k_1 \leq k$.

If $A$ is not adjacent to $B$ with respect to $G_0$, then $G_0$ has no hyperedges, which implies that all hyperedges of $G$ contain the vertex $n$. Recall that by assumption $G$ has neither hyperedges among vertices in $A$ nor hyperedges among vertices in $V \setminus A$. Consequently, $G_1$ has order at most $k-1$. If, in addition, $A$ is adjacent to $B$ with respect to $G_1$, then $\|\varrho_1\| \leq 1 - 2^{2-k}$, which implies that

$$\|\varrho_A\| \leq \frac{1}{2}(\|\varrho_0\| + \|\varrho_1\|) \leq \frac{1}{2}(1+1-2^{2-k}) = 1-2^{1-k}. \tag{G7}$$

Otherwise, if $A$ is not adjacent to $B$ with respect to $G_1$, then no hyperedge of $G$ contains any vertex in $B$; in other words, all vertices of $B$ are isolated with respect to $G$, which contradicts our assumption.

It remains to consider the case in which $A$ is adjacent to $B$ with respect to $G_0$, but not adjacent to $B$ with respect to $G_1$. In view of Eq. (G4), we conclude that $G_0$ has order at most $k-1$ since, otherwise, any order-$k$ hyperedge of $G_0$ (which necessarily connects $A$ and $B$) would also be a hyperedge of $G_1$. Therefore,

$$\|\varrho_A\| \leq \frac{1}{2}(\|\varrho_0\| + \|\varrho_1\|) \leq \frac{1}{2}(1-2^{2-k}+1) = 1-2^{1-k}. \tag{G8}$$

This observation completes the proof of Lemma 26. □

## Appendix H: Verification of GHZ states

In this section we provide more details on the verification of GHZ states using the (hedged) cover or coloring protocol and discuss the distinctions of our approach from previous works.

Let $G = (V, E)$ be the star graph in which vertex 1 is adjacent to the rest $n-1$ vertices, which are themselves not adjacent pairwise. In other words, the edge set $E$ is composed of $\{1, j\}$ for $j = 2, 3, \ldots, n$. The corresponding graph state has the form

$$|G\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \otimes |+\rangle^{\otimes(n-1)} + |1\rangle \otimes |-\rangle^{\otimes(n-1)}\big), \tag{H1}$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The graph state $|G\rangle$ is stabilized by the following $n$ stabilizer generators,

$$K_1 = X_1 \prod_{i=2}^{n} Z_i, \quad K_j = Z_1 X_j, \quad \forall j = 2, \ldots, n. \tag{H2}$$

It is equivalent to the more familiar form of the GHZ state under local unitary transformations. More precisely, we have

$$\left(\prod_{j=2}^{n} H_j\right)|G\rangle = |\mathrm{GHZ}\rangle := \frac{1}{\sqrt{2}}(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}), \tag{H3}$$

where $H_j$ is the Hadamard gate $H$ acting on the $j$th qubit, recall that $H := \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$.

It is straightforward to verify that $\chi(G) = \varpi(G) = 2$ and $\gamma(G) = 1/2$. An optimal independence cover of $G$ can be constructed from the coloring composed of the two sets $\{1\}$ and $\{2, 3, \ldots, n\}$ with equal weight of $1/2$. Based on this observation, we can construct a verification protocol with only two distinct tests. Each test is based on Pauli measurements on individual qubits. The measurement outcome on the $j$th qubit will be denoted by $\tilde{o}_j$, which can take on two possible values, that is, $\tilde{o}_j = \pm 1$. In the first test, we measure $X$ on the first qubit and measure $Z$ on the rest qubits. The test is passed if the measurement outcomes have even parity, that is, $\prod_{j=1}^{n} \tilde{o}_j = 1$. In the second test, we measure $Z$ on the first qubit and measure $X$ on the rest qubits. The test is passed if all outcomes coincide, that is, $\tilde{o}_1 = \tilde{o}_2 = \cdots = \tilde{o}_n$. The projectors onto the pass eigenspaces are respectively given by

$$P_1 = \frac{1+K_1}{2}, \quad P_2 = \prod_{j=2}^{n} \frac{1+K_j}{2}, \tag{H4}$$

which satisfy $P_1 P_2 = |G\rangle\langle G|$. The verification operator $\Omega$ has the form

$$\Omega = \frac{1}{2}(P_1 + P_2) = \frac{1}{2}\left(\frac{1+K_1}{2} + \prod_{j=2}^{n} \frac{1+K_j}{2}\right). \tag{H5}$$

It is straightforward to confirm that $\nu(\Omega) = 1/2$, in agreement with Theorem 7 in the main text. To verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$, it suffices to perform

$$N = \left\lceil \frac{\ln \delta}{\ln[1-(\epsilon/2)]} \right\rceil \leq \left\lceil \frac{2}{\epsilon} \ln \delta^{-1} \right\rceil \tag{H6}$$

tests. To certify GME of the GHZ state with significance level $\delta$, the number of required tests is given by Eq. (H6) with $\epsilon = 1/2$, that is, $\lceil \ln\delta/\ln(3/4)\rceil$; cf. Eq. (157) in the main text.

In the adversarial scenario, Eq. (H6) is replaced by

$$N = \min\left\{ \left\lceil \frac{2(1-\delta)}{\delta\epsilon} \right\rceil, \left\lceil \frac{1}{\delta\epsilon} - 1 \right\rceil \right\} \tag{H7}$$

according to the lower bound in Eq. (149), which is saturated in this case because $\nu(\Omega) = 1/2$. The performance can be improved by virtue of the hedged cover protocol proposed in Sec. V C. According to Eq. (155), the number of tests can be reduced to

$$N = \left\lfloor \frac{h_*(1/2)\ln(F\delta)^{-1}}{\epsilon} \right\rfloor \leq \left\lfloor \frac{3.22\ln(F\delta)^{-1}}{\epsilon} \right\rfloor, \tag{H8}$$

where $F = 1-\epsilon$. To certify GME of the GHZ state with significance level $\delta$ in the adversarial scenario, the number of tests is given by Eq. (H8) with $\epsilon = 1/2$, that is, $\lfloor 6.44\ln(2/\delta)\rfloor$; cf. Eq. (161) in the main text.

In view of Eq. (H3), the cover protocol for verifying $|G\rangle$ can be adapted for $|\text{GHZ}\rangle$ immediately by a simple change of measurement bases. To be specific, in the first test, we measure $X$ on all qubits, and the test is passed if the measurement outcomes have even parity. In the second test, we measure $Z$ on all qubits, and the test is passed if all outcomes coincide. The projectors onto the pass eigenspaces are respectively given by

$$P_1 = \frac{1+X^{\otimes n}}{2}, \quad P_2 = (|0\rangle\langle 0|)^{\otimes n} + (|1\rangle\langle 1|)^{\otimes n}. \tag{H9}$$

The total number of tests required is still determined by Eq. (H6). Similarly, Eqs. (H7) and (H8) are also applicable to the verification of $|\text{GHZ}\rangle$.

In the case of GHZ states, the measurements employed above for state verification have been applied to entanglement detection [48, 49]. However, the number of required tests was not discussed as in the current work. Our approach is appealing because it follows from a universal recipe, which applies to all hypergraph states and has a simple graph theoretic interpretation. Furthermore, our protocols can be applied to the adversarial scenario, while retaining almost the same efficiency.

## Appendix I: Comparison with existing works

In this section we discuss the connections and distinctions between our work and entanglement detection. We then compare our approach to state verification with a number of existing works, including direct fidelity estimation (DFE) [31] and Refs. [23, 39, 42, 52].

### 1. State verification and entanglement detection

In the main text, we introduced a simple and efficient protocol for verifying general hypergraph states. Our protocol can also be applied to detecting GME, though it is not necessarily optimized for this purpose. In the literature, there are many works on the detection of entanglement, including GME in particular [2]. The main distinction between state verification and entanglement detection lies in the motivations, which are reflected in the following two questions.

1. Is the quantum state prepared good enough for a given task, such as quantum computation, quantum communication, or quantum metrology?

2. Is the quantum state prepared GME?

The main motivation of the current work is to provide an efficient tool for answering the first question, while most works on entanglement detection focus on the second question directly. Question 2 is definitely interesting in itself since GME is a key resource in quantum information processing and a focus of foundational studies. In addition, demonstrating GME in experiments is usually highly nontrivial and may serve as a signature of the advance in quantum information science. On the other hand, although there are intimate connections between the two questions, the answer to question 2 is in general far from enough for answering question 1, which usually entails high fidelity with the target state. Instead of demonstrating certain quantum signature, eventually, we need to answer more specific and practical questions directly. Crucial to achieving this task is efficient state verification, which is the focus of this work.

In addition, most works on entanglement detection are based on the expectation values of certain witness operators and usually do not discuss the number of tests required to make a conclusion. With the cover protocol, by contrast, we can not only provide more precise information about the quantum state prepared, but also determine the explicit number of tests required. In addition, our approach can be applied to the adversarial scenario, which is appealing to many applications.

### 2. Comparison with direct fidelity estimation

In this section we compare our cover protocol with DFE introduced by Flammia and Liu [31]. Compared with the cover protocol, DFE can be applied to any pure state and thus has wider applications. The number of measurements required by DFE is smaller than tomography by a factor of $D = 2^n$, where $n$ is the number of qubits. Moreover, this number does not increase with the number of qubits in the case of stabilizer states. From this perspective, DFE is very efficient and very useful. However, DFE has several drawbacks as mentioned below which limit its applications to hypergraph states and many other states of quantum systems of more than 15 qubits.

1. To apply DFE it is necessary to sample from the squared characteristic function defined on the dis-

crete phase space of $2^{2n}$ points. In general, it is not easy to compute and store this function for large quantum systems; also, it is not easy to implement the sampling even if the characteristic function is determined.

2. The number of potential measurement settings increases exponentially with the number of qubits even for stabilizer states. The number of actual measurement settings $\lceil 1/(\epsilon^2\delta)\rceil$ depends on the target infidelity $\epsilon$ and significance level $\delta$. Specific measurement settings cannot be determined before implementing the protocol. Also, the total number of measurements cannot be determined in advance.

3. The average total number of measurements reads

$$\begin{aligned} N_{\mathrm{DFE}} &\approx 1+\frac{1}{\epsilon^2\delta}+\frac{2g}{D\epsilon^2}\ln(2/\delta) \\ &= 1+\frac{1}{\epsilon^2\delta}+\frac{2\tilde{g}}{\epsilon^2}\ln(2/\delta), \end{aligned} \tag{I1}$$

where $D=2^n$, $\tilde{g}=g/2^n$, and $g$ is the number of points at which the characteristic function is nonzero [31]. It is known that $g\geq D$ and the lower bound is saturated iff the target state is a stabilizer state. For a generic state $g\approx D^2$, so the number of measurements increases exponentially with $n$. As we shall see shortly, the exponential growth is also inevitable for many hypergraph states.

The number $N_{\mathrm{DFE}}$ in Eq. (I1) can be reduced for a well-conditioned state $\rho$, which means either $|\operatorname{tr}(\rho W_{x,z})|=0$ or $|\operatorname{tr}(\rho W_{x,z})|\geq c$ for all Pauli operators $W_{x,z}$ [cf. Eq. (I4) below], where $c$ is a positive constant whose inverse is upper bounded by a polynomial of $n$. In this case, $N_{\mathrm{DFE}}$ can be reduced to $O\bigl(\ln(1/\delta)/(c^2\epsilon^2)\bigr)$, though the quadratic scaling behavior with $1/\epsilon$ does not change. However, many hypergraph states are not well-conditioned. In addition, no simple way is known for determining whether a generic hypergraph state is well-conditioned or not when the number of qubits is large.

To analyze the supports of the characteristic functions of hypergraph states, it is instructive to point out that any hypergraph state is a real equally weighted state and vice versa [17, 18]. In other words, any $n$-qubit hypergraph state can be written as

$$|\Psi_f\rangle = 2^{-n/2}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle, \tag{I2}$$

where $f$ is a Boolean function from $\{0,1\}^n$ to $\{0,1\}$. For example, the Boolean function corresponding to the hypergraph state $|G\rangle=\bigl(\prod_{e\in E}CZ_e\bigr)|+\rangle^{\otimes n}$ is given by

$$f(x)=\sum_{e\in E}\prod_{j\in e}x_j, \tag{I3}$$

where the addition is modulo 2. Up to a phase factor, any $n$-qubit Pauli operator can be written as

$$W_{x,z}:=\left(\prod_{j=1}^n X_j^{x_j}\right)\left(\prod_{j=1}^n Z_j^{z_j}\right),\quad x,z\in\{0,1\}^n, \tag{I4}$$

where $X_j$ and $Z_j$ are the Pauli $X$ and $Z$ operators for the $j$th qubit. Here we are mainly interested in the absolute value of the characteristic function, so the phase factor does not matter. Calculation shows that

$$\langle\Psi_f|W_{x,z}|\Psi_f\rangle=\frac{1}{2^n}\sum_{u=0}^{2^n-1}(-1)^{f(u)+f(u+x)}(-1)^{z\cdot u}, \tag{I5}$$

where the addition $u+x$ is modulo 2 and so is the product $z\cdot u:=\sum_{j=1}^n z_ju_j$. The cardinality of the support of the characteristic function reads

$$g(f)=\bigl|\bigl\{(x,z)\in\{0,1\}^{2n}\,|\,\langle\Psi_f|W_{x,z}|\Psi_f\rangle\neq 0\bigr\}\bigr|. \tag{I6}$$

In the rest of this section, we provide several concrete examples of hypergraph states for which $\tilde{g}=g/2^n$ increases exponentially with the number $n$ of qubits, which means $N_{\mathrm{DFE}}$ increases exponentially with $n$. First, consider the special hypergraph with only one hyperedge, which contains all $n$ vertices. The corresponding Boolean function $f_n$ reads

$$f_n(u):=\prod_{j=1}^n u_j=\begin{cases}1 & u=11\cdots 1,\\ 0 & \text{otherwise.}\end{cases} \tag{I7}$$

In this case, we have

$$2^n\bigl|\langle\Psi_{f_n}|W_{x,z}|\Psi_{f_n}\rangle\bigr|=\begin{cases}2^n & x=z=0,\\ 2^n-4 & z=0, x\neq 0,\\ 4 & x\neq 0, z\neq 0, x\cdot z=0,\\ 0 & x\cdot z=1,\ \text{or } x=0, z\neq 0,\end{cases} \tag{I8}$$

which implies that

$$g(f_n)=2^{2n-1}-2^{n-1}+1,\quad \tilde{g}\approx 2^{n-1}-2^{-1}. \tag{I9}$$

So the number of measurements in Eq. (I1) reduces to

$$N_{\mathrm{DFE}}\approx 1+\frac{1}{\epsilon^2\delta}+\frac{2^n-1}{\epsilon^2}\ln(2/\delta), \tag{I10}$$

which increases exponentially with the number of qubits. By contrast, the number of tests required by our cover protocol is at most

$$\left\lceil \frac{n}{\epsilon} \ln(1/\delta) \right\rceil \tag{I11}$$

according to Eq. (145) in the main text, which is exponentially smaller than $N_{\rm DFE}$.

As another example, consider the tensor power $|\Psi_{f_3}\rangle^{\otimes n/3}$, which corresponds to the hypergraph state with $n/3$ disjoint hyperedges of order 3, assuming that $n$ is divisible by 3. In this case,

$$g = g(f_3)^{n/3} = 29^{n/3} > 3^n, \quad \tilde{g} = \frac{29^{n/3}}{2^n} \geq \left(\frac{3}{2}\right)^n. \tag{I12}$$

So the number of measurements in Eq. (I1) reduces to

$$\begin{aligned} N_{\rm DFE} &\approx 1 + \frac{1}{\epsilon^2\delta} + \frac{2 \times 29^{n/3}}{2^n \epsilon^2} \ln(2/\delta) \\ &\geq 1 + \frac{1}{\epsilon^2\delta} + \frac{2\left(\frac{3}{2}\right)^n}{\epsilon^2} \ln(2/\delta), \end{aligned} \tag{I13}$$

which also increases exponentially with the number of qubits. By contrast, the number of tests required by the cover protocol is

$$\left\lceil \frac{3}{\epsilon} \ln(1/\delta) \right\rceil, \tag{I14}$$

which is again exponentially smaller than $N_{\rm DFE}$.

Furthermore, numerical calculations show that $\tilde{g}$ increases exponentially with $n$ for order-3 cluster states and Union Jack states on a chain or on a two-dimensional lattice (cf. Fig. 10), so $N_{\rm DFE}$ also increases exponentially with $n$ for these states. The number of tests required by the cover protocol is still $\lceil(3/\epsilon)\ln(1/\delta)\rceil$.

### 3. Comparison with Ref. [23]

Recently, Morimae, Takeuchi, and Hayashi (MTH) [23] introduced a method for verifying hypergraph states in the adversarial scenario. They only considered the case in which all hyperedges have orders at most three. Although their method may potentially be extended to more general settings, a direct extension of their approach entails exponential increase in the resource overhead with the order of the hypergraph. Even for order-3 hypergraph states, the resource overhead increases exponentially with the number of hyperedges (and thus the degree of the hypergraph). Another drawback of the MTH protocol is that even the target hypergraph state $|G\rangle$ cannot pass the test with certainty. Consequently, the number of tests required increases quadratically with the inverse infidelity.

More specifically, suppose $|G\rangle$ is an $n$-qubit hypergraph state to be verified. Let $K_j$ be the stabilizer operator corresponding to vertex $j$ as defined in Eq. (131) in the main text; let $r_j$ be the number of order-3 hyperedges that contain the vertex $j$. The MTH verification protocol is composed of $n$ stabilizer tests. For each stabilizer $K_j$, MTH devised a test, which requires $4^{r_j}$ potential measurement settings. The total number of potential measurement settings is given by

$$\sum_{j=1}^{n} 4^{r_j}, \tag{I15}$$

which increases exponentially with the number of order-3 hyperedges. MTH also set a criterion such that the probability of a state $\rho$ to satisfy the criterion is given by

$$p = \frac{1}{2} + \frac{\operatorname{tr}(\rho K_j)}{2^{r_j+1}} = \frac{1}{2} + \frac{1-a_j}{2^{r_j+1}}, \tag{I16}$$

where $a_j := 1 - \operatorname{tr}(\rho K_j)$. Although the target state $|G\rangle$ can attain the maximum probability $(1/2) + (1/2^{r_j+1})$, it generally cannot satisfy the criterion with certainty. Suppose the test is performed $N_j$ times, and the criterion is satisfied $t_j$ times. Then the stabilizer test is passed if the frequency $f_j = t_j/N_j$ satisfies

$$f_j \geq \frac{1}{2} + \frac{1-\theta}{2^{r_j+1}}, \tag{I17}$$

where $\theta$ is a small positive constant. The state $\rho$ is accepted if it can pass all the stabilizer tests. The choice of $\theta$ needs to guarantee that the target state $|G\rangle$ can pass all the tests with high probability; meanwhile, any state that has low fidelity with $|G\rangle$ should fail some test with high probability. When $a_j \geq \theta$, the probability that $\rho$ can pass the stabilizer test associated with $K_j$ can be upper bounded as follows,

$$\begin{aligned} &\Pr\left(f_j \geq \frac{1}{2} + \frac{1-\theta}{2^{r_j+1}}\right) = \Pr\left(f_j \geq p + \frac{a_j-\theta}{2^{r_j+1}}\right) \\ &\leq \exp\left(-2\frac{(a_j-\theta)^2}{4^{r_j+1}} N_j\right), \end{aligned} \tag{I18}$$

where the last step follows from the Hoeffding inequality. Similarly, the probability that the target state $|G\rangle$ passes the test can be lower bounded by virtue of the Hoeffding inequality.

MTH did not give an explicit number of tests needed to verify a hypergraph state within infidelity $\epsilon$ and significance level $\delta$. They considered a related, but different verification problem with a different criterion, which requires about $nk+1+m$ tests, where $k = 2^{2r+3}n^7$, $m \geq 2n^7k^2\ln 2$, and $r = \max_j r_j$. In other words, the number of required tests satisfies

$$\begin{aligned} nk+1+m &\geq nk+1+2n^7k^2\ln 2 \cong 2n^7k^2\ln 2 \\ &= 2^{4r+7}n^{21}\ln 2. \end{aligned} \tag{I19}$$

While this number is still polynomial in $n$ if $r$ does not increase with $n$, it grows rapidly with $n$. Actually, this number is already astronomical when $n = 5$ and $r = 2$

(note that $r=8$ for generic Union Jack states on 2D lattices), while any useful MBQC would require more than five qubits. So the MTH protocol is hardly practical. In contrast, the number of tests required by our cover protocol is only

$$N \leq \left\lceil \frac{\Delta(G)+1}{\delta\epsilon} \right\rceil \leq \left\lceil \frac{2r+1}{\delta\epsilon} \right\rceil \tag{I20}$$

according to Eq. (150), which is independent of $n$ and outperforms the MTH protocol dramatically. According to Eq. (153), the hedged cover protocol can further reduce the number of tests to

$$N \leq \frac{[\Delta(G)+\mathrm{e}]\ln[(F\delta)^{-1}]}{\epsilon} \leq \frac{(2r+\mathrm{e})\ln[(F\delta)^{-1}]}{\epsilon}. \tag{I21}$$

It is natural to ask whether the number of tests can be reduced significantly if the MTH protocol is adapted to the nonadversarial scenario considered in the main text. Here we try to give a rough estimate.

To verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$, suppose $1-\langle G|\rho|G\rangle \geq \epsilon$, we need to estimate the maximal probability that $\rho$ can pass all the stabilizer tests and make sure that this probability is smaller than $\delta$, that is,

$$\prod_j \Pr\left(f_j \geq \frac{1}{2}+\frac{1-\theta}{2^{r_j+1}}\right) = \Pr\left(f_j \geq p+\frac{a_j-\theta}{2^{r_j+1}}\right) \leq \delta. \tag{I22}$$

According to Eq. (I18), it suffices to guarantee that

$$\prod_{j|a_j\geq\theta} \exp\left(-2\frac{(a_j-\theta)^2}{4^{r_j+1}}N_j\right) \leq \delta. \tag{I23}$$

Note that the infidelity of $\rho$ with $|G\rangle$ satisfies

$$\begin{aligned}1-\langle G|\rho|G\rangle &= 1-\operatorname{tr}\left(\rho\prod_j \frac{K_j+1}{2}\right)\\ &\leq \sum_j\left[1-\operatorname{tr}\left(\rho\frac{K_j+1}{2}\right)\right] = \frac{1}{2}\sum_j a_j.\end{aligned} \tag{I24}$$

If the infidelity is at least $\epsilon$, then $(\sum_j a_j)/2 \geq \epsilon$. We need to determine the minimum of $\sum_j N_j$ under the requirement that Eq. (I23) holds whenever $(\sum_j a_j)/2 \geq \epsilon$. Choose

$$a_j = \frac{2\epsilon\times 2^{r_j}}{\sum_k 2^{r_k}}, \tag{I25}$$

then Eq. (I23) implies that

$$\exp\left(-\frac{2\epsilon^2\sum_j N_j}{\left(\sum_j 2^{r_j}\right)^2}\right) \leq \delta, \tag{I26}$$

which in turn implies that

$$N_{\mathrm{MTH}} = \sum_j N_j \geq \frac{\left(\sum_j 2^{r_j}\right)^2 \ln\delta^{-1}}{2\epsilon^2}. \tag{I27}$$

If all $r_j$ are equal to $r$, then the MTH protocol requires $4^r n$ potential measurement settings and at least

$$N_{\mathrm{MTH}} \geq \frac{4^r n^2 \ln\delta^{-1}}{2\epsilon^2} \tag{I28}$$

tests. The bounds in the above two equations have much better scaling behavior with $n$ compared with the bound in Eq. (I19). However, these bounds are already very large for a small value of $n$ for Union Jack states and many other states for which $r$ is not so small. In general, it is too prohibitive to implement the MTH protocol except for hypergraph states of no more than ten qubits.

A few comments are in order. First, we do not know how tight are the bounds in Eqs. (I27) and (I28). Nevertheless, these bounds are sufficient for comparing the MTH protocol with our protocol, and it is not so important to derive a tighter bound with more involved analysis. Second, Eq. (I27) is based on Eqs. (I18) and (I24). Note that the bound in (I24) is tight. The Hoeffding inequality in Eq. (I18) may potentially be improved, thereby reducing $N_{\mathrm{MTH}}$. However, this possibility was not considered by MTH. We are not aware of any simple method for improving the Hoeffding inequality either and do not expect a significant improvement even with more sophisticated analysis. In this regard, our protocol is not only much more efficient, but also much easier to implement and to analyze its performance.

In the rest of this section, we consider the performance of the MTH protocol adapted to the nonadversarial scenario for several concrete order-3 hypergraph states. As a start, consider the complete order-3 hypergraph state whose underlying hypergraph contains all possible order-3 hyperedges. In this case, the total number of hyperedges is $\binom{n}{3}=n(n-1)(n-2)/6$ and $r_j=r=\binom{n-1}{2}=(n-1)(n-2)/2$ for $j=1,2,\ldots,n$. Therefore,

$$N_{\mathrm{MTH}} \geq \frac{2^{(n-1)(n-2)}n^2\ln\delta^{-1}}{2\epsilon^2}. \tag{I29}$$

Here both the number of potential measurement settings and the number of tests required by the MTH protocol increase exponentially with the number of qubits. By contrast, our cover protocol requires at most $n$ potential measurement settings and $\lceil (n/\epsilon)\ln(1/\delta)\rceil$ tests according to Eq. (145).

The rest examples considered below are 3-colorable, so our protocol requires three measurement settings and $\lceil(3/\epsilon)\ln(1/\delta)\rceil$ tests to verify each hypergraph state within infidelity $\epsilon$ and significance level $\delta$. First, consider the tensor power $|\Psi_{f_3}\rangle^{\otimes n/3}$ introduced in Appendix I 2, assuming $n$ is divisible by 3. In this case $r_j=r=1$ for all $j=1,2,\ldots,n$. Therefore, Eq. (I28) reduces to

$$N_{\mathrm{MTH}} \geq \frac{2n^2\ln\delta^{-1}}{\epsilon^2}. \tag{I30}$$

Next, consider order-3 cluster states. In the 1D case, the vertices of the underlying hypergraph are arranged in a chain and labeled by natural numbers; all hyperedges have the form $\{j, j+1, j+2\}$ with $j \geq 1$ and $j \leq n-2$, assuming $n \geq 3$. If we use $0, 1, 2$ to denote three colors, then the hypergraph can be colored by assigning vertex $j$ with the color ($j \mod 3$). Similar analysis applies to 2D and higher-dimensional lattices. For simplicity, here we focus on the 1D case, so that

$$r_j = \begin{cases} 1 & n = 3 \text{ or } j = 1 \text{ or } j = n, \\ 2 & n \geq 4, j = 2 \text{ or } j = n-1, \\ 3 & j \neq 1, 2, n-1, n. \end{cases} \tag{I31}$$

Therefore,

$$\sum_j 2^{r_j} = \begin{cases} 6 & n = 3, \\ 8n - 20 & n \geq 4, \end{cases} \tag{I32}$$

which implies that

$$N_{\mathrm{MTH}} \geq \begin{cases} \frac{18 \ln \delta^{-1}}{\epsilon^2} & n = 3, \\ \frac{8(2n-5)^2 \ln \delta^{-1}}{\epsilon^2} & n \geq 4. \end{cases} \tag{I33}$$

Now consider the Union Jack state on the Union Jack chain; cf. Fig. 9 in the main text. In this case, we have $r_j = 2$ when $j$ corresponds to one of the four corners and $r_j = 4$ otherwise. Therefore,

$$\sum_j 2^{r_j} = 16n - 48, \quad N_{\mathrm{MTH}} \geq \frac{128(n-3)^2 \ln \delta^{-1}}{\epsilon^2}. \tag{I34}$$

Finally, consider the Union Jack state on the Union Jack lattice with $\tilde{n} \times \tilde{n}$ cells and $n = \tilde{n}^2 + (\tilde{n}+1)^2$ qubits. Calculation shows that

$$\begin{aligned} \sum_j 2^{r_j} &= 2^8(\tilde{n}-1)^2 + 2^4[\tilde{n}^2 + 4(\tilde{n}-1)] + 2^2 \times 4 \\ &= 16(17\tilde{n}^2 - 28\tilde{n} + 13), \end{aligned} \tag{I35}$$

so that

$$N_{\mathrm{MTH}} \geq \frac{128(17\tilde{n}^2 - 28\tilde{n} + 13)^2 \ln \delta^{-1}}{\epsilon^2}. \tag{I36}$$

### 4. Comparison with Ref. [39]

Here, in the adversarial setting, we compare our method with the method proposed by Hayashi and Hajdušek (HH) [39], who considered the verification of graph states, but not hypergraph states. In addition, HH mainly focused on the case in which the graph is 3-colorable. They mentioned the general case briefly, but did not analyze the performance of their protocol in detail. Since the main focus of Ref. [39] is self-testing, HH do not trust their measurement devices. However, after the verification of their measurement devices, they verify their graph state under the assumption that their measurement devices are trusty.

Let $|G\rangle$ be a graph state associated with the graph $G$. When $G$ is $m$-colorable, HH (Appendix F of Ref. [39]) proposed the following verification protocol, which consists of $m$ stabilizer tests. Given a coloring $\mathscr{A} = \{A_1, A_2, \ldots, A_m\}$ of $G$ with $m$ colors, the verifier asks the adversary to prepare $N+1$ systems with $N = mN'$. After a random permutation of the $N+1$ systems, $N$ systems are chosen and divided into $m$ groups each with $N'$ systems. Then all systems in the $l$th group for $l = 1, 2, \ldots, m$ are subjected to the stabilizer test with $P_l$ [cf. Eq. (135) in the main text] as the projector onto the pass eigenspace. Let $\sigma$ be the reduced state of the remaining system after all these tests are passed. If the $l$th test $P_l$ is passed with significance level $\delta'$, then one can guarantee that $\mathrm{tr}[\sigma(1 - P_l)] \leq \frac{1}{\delta'(N'+1)}$. If all the tests $P_1, \ldots, P_m$ are passed, with significance level $\delta := m\delta'$, then one can guarantee that

$$\begin{aligned} \epsilon = \mathrm{tr}[\sigma(1 - |G\rangle\langle G|)] &\leq \sum_{l=1}^m \mathrm{tr}[\sigma(1 - P_l)] \\ &\leq \sum_{l=1}^m \frac{1}{\delta'(N'+1)} = \frac{m^2}{\delta(N/m+1)} \cong \frac{m^3}{\delta N}. \end{aligned} \tag{I37}$$

To verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$ in the adversarial scenario, the HH protocol requires about $\lceil m^3/(\delta\epsilon) \rceil$ tests.

Now, we explain how our method outperforms the HH method. If we employ the cover protocol and randomly choose the $l$th measurement setting with probability $1/m$, then $\nu(\Omega) = 1/m$ according to Theorem 7. If the tests are passed with significance level $\delta$, then Theorem 4 guarantees that

$$\epsilon = \mathrm{tr}[\sigma(1 - |G\rangle\langle G|)] \leq \frac{m(1-\delta)}{N\delta}. \tag{I38}$$

To verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$ in the adversarial scenario, the cover protocol requires only $\lceil m(1-\delta)/(\delta\epsilon) \rceil$ tests, which significantly outperforms the HH protocol. According to Eq. (152), the hedged cover protocol can further reduce the number to

$$N = \left\lfloor \frac{h_*(1/m) \ln(F\delta)^{-1}}{\epsilon} \right\rfloor \leq \frac{(m + \mathrm{e} - 1) \ln[(F\delta)^{-1}]}{\epsilon}, \tag{I39}$$

where $F = 1 - \epsilon$.

### 5. Comparison with Ref. [42]

Very recently, Takeuchi and Morimae (TM) [42] introduced a protocol for verifying general hypergraph states whose orders are upper bounded by a constant. Recall that the order of a hypergraph $G = (V, E)$ is the maximum cardinality of hyperedges in the edge set $E$.

Let $G = (V, E)$ be a hypergraph such that $2 \leq |e| \leq c$ for all $e \in E$, where $c$ is a positive constant. Let

$k \geq (4n)^7$ and $m \geq 2n^3 k^{18/7} \ln 2$ be positive integers. According to Theorem 5 in Ref. [42], to verify the hypergraph state $|G\rangle$ within infidelity $\epsilon = k^{-1/7}$ and significance level $\delta = k^{-1/7}$, the number of tests required by the TM protocol is given by

$$N_{\mathrm{TM}} = m + nk \geq 2n^3 k^{18/7} \ln 2 + nk > 2n^3 k^{18/7} \ln 2. \tag{I40}$$

For example, when $k = (4n)^7$, $\epsilon = \delta = k^{-1/7} = 1/(4n)$, the number of tests satisfies

$$\begin{aligned} N_{\mathrm{TM}} &\geq 2n^3 (4n)^{18} \ln 2 + n(4n)^7 = 2^{37} n^{21} \ln 2 + 2^{14} n^8 \\ &> 2^{37} n^{21} \ln 2 > 9.5 \times 10^{10} n^{21}. \end{aligned} \tag{I41}$$

Although this number is still polynomial in $n$, it is already astronomical in the simplest nontrivial scenario with $n = 3$. So it is too prohibitive to apply the TM protocol in any scenario of practical interest. By contrast, the number of tests required by our coloring protocol satisfies

$$N \leq (16n^2 - 4n)\chi(G) < 16n^2 \chi(G) \leq 16n^3 \tag{I42}$$

according to Eq. (150) in the main text, which is dramatically smaller than $N_{\mathrm{TM}}$. The hedged coloring protocol can further reduce the number of tests according to Eq. (153).

Our protocols are not only much more efficient than the TM protocol, but also much simpler to apply. In particular, the TM protocol relies on adaptive stabilizer tests, while our protocols do not rely on any adaption. In addition, the data processing in the TM protocol is a bit involved, while it is very simple in our protocols. Furthermore, TM did not derive the explicit number of required tests except for restricted choices of the infidelity $\epsilon$ and significance level $\delta$, which makes it difficult to apply their result in many scenarios of practical interest. By contrast, we derive the explicit number of required tests for all valid choices of $\epsilon$ and $\delta$.

### 6. Comparison with Ref. [52]

Recently, Takeuchi, Mantri, Morimae, Mizutani, and Fitzsimons [52] introduced a protocol for verifying graph states with a very small significance level. Given a graph state $|G\rangle$ of $n$ qubits, suppose one can perform $N_{\mathrm{TMMMF}} = 2n\lceil (5n^4 \ln n)/32 \rceil$ tests, then the protocol given in Ref. [52] guarantees that the resultant state $\sigma$ satisfies

$$\langle G|\sigma|G\rangle \geq 1 - \frac{2\sqrt{c}+1}{n} \tag{I43}$$

if these tests are passed with significance level $n^{1-5c/64}$. Here, $c$ is a constant that satisfies $\frac{64}{5} < c < \frac{(n-1)^2}{4}$.

Next, we analyze the performance of our approach based on a homogeneous strategy $\Omega$; see Sec. III C. According to Theorem 3, to verify $|G\rangle$ within the same infidelity $\epsilon = (2\sqrt{c}+1)/n$ and significance level $\delta = n^{1-5c/64}$, the number of required tests is only

$$N\Big(\frac{2\sqrt{c}+1}{n}, n^{1-5c/64}, \Omega\Big) \leq \left\lceil \frac{(1-\frac{5c}{64})n \ln n}{(2\sqrt{c}+1)(\lambda \ln \lambda)} \right\rceil, \tag{I44}$$

where $\lambda = \beta(\Omega)$ is the second largest eigenvalue of $\Omega$. In conjunction with the homogeneous strategy $\Omega_{\mathrm{PLM}}$ proposed in Ref. [40, (S89)] (cf. Eq. (146) in the main text), we have

$$\begin{aligned} &N\Big(\frac{2\sqrt{c}+1}{n}, n^{1-5c/64}, \Omega_{\mathrm{PLM}}\Big) \leq \left\lceil \frac{3(\frac{5c}{64}-1)n \ln n}{(2\sqrt{c}+1)} \right\rceil \\ &= O(n \ln n), \end{aligned} \tag{I45}$$

given that $1/3 \leq \lambda = \beta(\Omega_{\mathrm{PLM}}) \leq 1/2$, which implies that $1/(\lambda \log \lambda^{-1}) \leq 3$. This number is much smaller than $N_{\mathrm{TMMMF}}$.

Alternatively, we can apply the hedged cover or coloring protocol proposed in Sec. V C, which requires much fewer measurement settings. According to Eq. (155), suppose the graph $G$ is $m$ colorable, then the number of required tests is given by

$$\begin{aligned} N &= \left\lfloor \frac{h_*(1/m) \ln(F\delta)^{-1}}{\epsilon} \right\rfloor \leq \frac{(m + \mathrm{e} - 1) \ln[(F\delta)^{-1}]}{\epsilon}, \\ &\approx \frac{(m + \mathrm{e} - 1)(\frac{5c}{64} - 1)n \ln n}{(2\sqrt{c}+1)} = O(n^2 \ln n), \end{aligned} \tag{I46}$$

where $F = 1 - \epsilon$ and the approximation holds as long as $\epsilon, \delta \ll 1$. For most graph states of practical interest, $m$ is upper bounded by a small constant, so $N = O(n \ln n)$. Again, the number of tests is much smaller than $N_{\mathrm{TMMMF}}$. Therefore, our approach is much more efficient that the approach of Ref. [52].

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," Rev. Mod. Phys. **81**, 865 (2009).

[2] O. Gühne and G. Tóth, "Entanglement detection," Phys. Rep. **474**, 1 (2009).

[3] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," Phys. Rev. Lett. **86**, 5188–5191 (2001).

[4] R. Raussendorf, D. E. Browne, and H. J. Briegel, "Measurement-based quantum computation on cluster states," Phys. Rev. A **68**, 022312 (2003).

[5] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*, FOCS'09 (2009) pp. 517–526.

[6] T. Morimae and K. Fujii, "Blind quantum computation protocol in which Alice only makes measurements," Phys. Rev. A **87**, 050301 (2013).

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

[8] D. Gottesman, *Stabilizer Codes and Quantum Error Correction*, Ph.D. thesis, California Institute of Technology (1997), available at http://arxiv.org/abs/quant-ph/9705052.

[9] D. Schlingemann and R. F. Werner, "Quantum error-correcting codes associated with graphs," Phys. Rev. A **65**, 012308 (2001).

[10] S. Perseguers, G. J. Lapeyre Jr, D. Cavalcanti, M. Lewenstein, and A. Acín, "Distribution of entanglement in large-scale quantum networks," Rep. Prog. Phys. **76**, 096001 (2013).

[11] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. G. Rarity, and M. S. Tame, "Experimental verification of multipartite entanglement in quantum networks," Nature Commun. **7**, 13251 (2016).

[12] D. Markham and A. Krause, "A simple protocol for certifying graph states and applications in quantum networks," (2018), arXiv:1801.05057.

[13] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, "Bell's theorem without inequalities," American J. Phys. **58**, 1131–1143 (1990).

[14] V. Scarani, A. Acín, E. Schenck, and M. Aspelmeyer, "Nonlocality of cluster states of qubits," Phys. Rev. A **71**, 042325 (2005).

[15] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, "Bell inequalities for graph states," Phys. Rev. Lett. **95**, 120405 (2005).

[16] C. Kruszynska and B. Kraus, "Local entanglability and multipartite entanglement," Phys. Rev. A **79**, 052304 (2009).

[17] R. Qu, J. Wang, Z.-s. Li, and Y.-r. Bao, "Encoding hypergraphs into quantum states," Phys. Rev. A **87**, 022311 (2013).

[18] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, "Quantum hypergraph states," New J. Phys. **15**, 113022 (2013).

[19] F. E. S. Steinhoff, C. Ritz, N. I. Miklin, and O. Gühne, "Qudit hypergraph states," Phys. Rev. A **95**, 052340 (2017).

[20] F.-L. Xiong, Y.-Z. Zhen, W.-F. Cao, K. Chen, and Z.-B. Chen, "Qudit hypergraph states and their properties," Phys. Rev. A **97**, 012323 (2018).

[21] J. Miller and A. Miyake, "Hierarchy of universal entanglement in 2D measurement-based quantum computation," npj Quantum Inf. **2**, 16036 (2016).

[22] J. Miller and A. Miyake, "Latent computational complexity of symmetry-protected topological order with fractional symmetry," Phys. Rev. Lett. **120**, 170503 (2018).

[23] T. Morimae, Y. Takeuchi, and M. Hayashi, "Verification of hypergraph states," Phys. Rev. A **96**, 062321 (2017).

[24] M. Gachechiladze, C. Budroni, and O. Gühne, "Extreme violation of local realism in quantum hypergraph states," Phys. Rev. Lett. **116**, 070401 (2016).

[25] M. Gachechiladze, O. Gühne, and A. Miyake, "Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states," (2018), arXiv:1805.12093.

[26] Y. Takeuchi, T. Morimae, and M. Hayashi, "Quantum computational universality of hypergraph states with Pauli-X and Z basis measurements," (2018), arXiv:1809.07552.

[27] M. J. Bremner, A. Montanaro, and D. J. Shepherd, "Average-case complexity versus approximate simulation of commuting quantum computations," Phys. Rev. Lett. **117**, 080501 (2016).

[28] F. Verstraete, V. Murg, and J. I. Cirac, "Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems," Adv. Phys. **57**, 143–224 (2008).

[29] R. Orús, "A practical introduction to tensor networks: Matrix product states and projected entangled pair states," Ann. Phys. **349**, 117–158 (2014).

[30] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, "Quantum state tomography via compressed sensing," Phys. Rev. Lett. **105**, 150401 (2010).

[31] S. T. Flammia and Y.-K. Liu, "Direct fidelity estimation from few Pauli measurements," Phys. Rev. Lett. **106**, 230501 (2011).

[32] 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).

[33] M. Hayashi, "Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing," New J. Phys. **11**, 043028 (2009).

[34] H. Zhu and M. Hayashi, "Optimal verification and fidelity estimation of maximally entangled states," (2019), arXiv:1901.09772.

[35] Z. Li, Y.-G. Han, and H. Zhu, "Efficient verification of bipartite pure states," (2019), arXiv:1901.09783.

[36] K. Wang and M. Hayashi, "Optimal Verification of Two-Qubit Pure States," (2019), arXiv:1901.09467.

[37] X.-D. Yu, J. Shang, and O. Gühne, "Optimal verification of general bipartite pure states," (2019), arXiv:1901.09856.

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

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

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

[41] M. Hayashi and Y. Takeuchi, "Verifying commuting quantum computations via fidelity estimation of weighted graph states," (2019), arXiv:1902.03369.

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

[43] B. Yoshida, "Topological phases with generalized global symmetries," Phys. Rev. B **93**, 155131 (2016).

[44] D. Schlingemann, "Stabilizer codes can be realized as graph codes," Quantum Info. Comput. **2**, 307–323 (2002).

[45] M. Grassl, A. Klappenecker, and M. Rötteler, "Graphs, quadratic forms, and quantum codes," in *Proceedings of the 2002 IEEE International Symposium on Information Theory* (Lausanne, Switzerland, 2002) available at arXiv:quant-ph/0703112.

[46] K. Chen and H.-K. Lo, "Multi-partite quantum cryptographic protocols with noisy GHZ states," Quantum Info. Comput. **7**, 689–715 (2007).

[47] M. Ghio, D. Malpetti, M. Rossi, D. Bruß, and C. Macchiavello, "Multipartite entanglement detection for hypergraph states," J. Phys. A: Math. Theor. **51**, 045302 (2018).

[48] G. Tóth and O. Gühne, "Detecting genuine multipartite entanglement with two local measurements," Phys. Rev. Lett. **94**, 060501 (2005).

[49] G. Tóth and O. Gühne, "Entanglement detection in the stabilizer formalism," Phys. Rev. A **72**, 022340 (2005).

[50] A. Dimić and B. Dakić, "Single-copy entanglement detection," npj Quantum Inf. **4**, 11 (2018).

[51] D. W. Lyons, D. J. Upchurch, S. N. Walck, and C. D. Yetter, "Local unitary symmetries of hypergraph states," J. Phys. A: Math. Theor. **48**, 095301 (2015).

[52] Y. Takeuchi, A. Mantri, T. Morimae, A. Mizutani, and J. F. Fitzsimons, "Resource-efficient verification of quantum computing using Serfling's bound," (2018), arXiv:1806.09138.