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, including quantum computation, quantum simulation, and quantum networks. However, little is known about this topic in the adversarial scenario. Here we initiate a systematic study of pure-state verification in the adversarial scenario. In particular, we introduce a general method for determining the minimal number of tests required by a given verification strategy to achieve a given precision. In the case of homogeneous strategies, we can even derive an analytical formula. Furthermore, we propose a general recipe to verify multipartite pure states, stabilizer states, hypergraph states, weighted graph states, and Dicke states in the adversarial scenario, even if only local projective measurements are accessible. This paper is an extended version of the companion paper Zhu and Hayashi, Phys. Rev. Lett. 123, 260504 (2019).

I. INTRODUCTION

Quantum states encode all the information about a quantum system and play a central role in quantum information processing. For example, bipartite entangled states, especially maximally entangled states, are crucial to quantum teleportation, dense coding, and quantum cryptography [1, 2]. Multiparticle entangled states, such as graph states [3] and hypergraph states [4, 5] are especially useful in (blind) measurement-based quantum computation (MBQC) [6, 7], quantum error correction [8, 9], quantum networks [10, 11], and foundational studies [12, 13]. Another important class of multipartite states, including Dicke states [14, 15], are useful in quantum metrology [16]. Furthermore, multipartite states, such as tensor-network states, also have extensive applications in research areas beyond quantum information science, including condensed matter physics [17, 18].

To unleash the potential of multipartite quantum states in quantum information processing, it is paramount to prepare and verify these states with high precision using limited resources. To verify quantum states with traditional tomography [19], however, the resource required increases exponentially with the number of qubits. Although compressed sensing [20] and direct fidelity estimation (DFE) [21] can improve the efficiency, the exponential scaling behavior cannot be changed in general. As another alternative, self-testing [22, 23] is also quite resource consuming although it is conceptually appealing from the perspective of device independence.

Recently, a powerful approach known as quantum state verification (QSV) has attracted increasing attention [24–26]. It is particularly effective in extracting the key information—the fidelity with the target state. So far efficient or even optimal verification protocols based on local projective measurements have been constructed for bipartite pure states [27, 28], Greenberger-Horne-Zeilinger (GHZ) states [29], stabilizer states (including graph states) [30, 31], hypergraph states [32], weighted graph states [33], and Dicke states [34]. Moreover, the efficiency of this approach has been demonstrated in experiments [35].

However, the situation is much more troublesome when we turn to the adversarial scenario, in which the quantum states of interest are controlled by an untrusted party, Eve. Efficient QSV in such adversarial scenario is crucial to many applications in quantum information processing that require high security conditions, including blind MBQC [36, 37] and quantum networks [38, 39]. Unfortunately, no efficient approach is known for addressing such adversarial scenario in general. For example, to verify the simplest nontrivial hypergraph states (say of three qubits) already requires an astronomical number of measurements [40, 41]. What is worse, little is known about the resource cost of a given verification strategy to achieve a given precision [42, 43]. As a consequence, no
general guideline is known for constructing an efficient verification strategy or for comparing the efficiencies of different strategies.

In this paper we initiate a systematic study of pure-state verification in the adversarial scenario. In particular, we introduce a general method for determining the minimal number of tests required by a given verification strategy to achieve a given precision. We also introduce the concept of homogeneous strategies, which play a key role in QSV. Thanks to their high symmetry, we can derive analytical formulas for most figures of merit of practical interest. The conditions for single-copy verification are also clarified. Furthermore, we provide a general recipe to constructing efficient verification protocols for the adversarial scenario from verification protocols for the nonadversarial scenario. By virtue of this recipe, we can verify pure quantum states in the adversarial scenario with nearly 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 can be greatly simplified since it suffices to focus on the nonadversarial scenario and then apply our recipe. In addition, our study reveals that entangling measurements are less helpful and often unnecessary in improving the verification efficiency in the adversarial scenario, which is counterintuitive at first sight.

Our work is especially helpful to the verification of bipartite pure states, GHZ states, and qudit states (including graph states), hypergraph states, weighted graph states, and Dicke states, for which efficient verification protocols for the nonadversarial scenario have been constructed recently. By virtue of our recipe, all these states can be verified in the adversarial scenario with much higher efficiencies than was possible previously; moreover, only local projective measurements are required to achieve high efficiencies. For bipartite pure states, GHZ states, and qudit states, even optimal protocols can be constructed using local projective measurements; see Sec. X.

This paper is an extended version of the companion paper. The rest of this paper is organized as follows. In Sec. II we review the basic framework of QSV in the nonadversarial scenario. In Sec. III we clarify the limitation of previous approaches to QSV and motivate the current study. In Sec. IV we formulate the general ideal of QSV with homogeneous strategies. In Sec. V we introduce a general method for computing the main figures of merit in the adversarial scenario. In Sec. VI we discuss in detail QSV with homogeneous strategies. In Sec. VII we clarify the power of a single test in QSV. In Sec. VIII we determine the minimal number of tests required by a general verification strategy to achieve a given precision. In Sec. IX we propose a general recipe to constructing efficient verification protocols for the adversarial scenario from protocols devised for the nonadversarial scenario. In Sec. X we demonstrate the power of our recipe via its applications to many important bipartite and multiparticle quantum states. In Sec. XI we compare QSV with a number of other approaches for estimating or verifying quantum states. Section XII summarizes this paper. To streamline the presentation, most technical proofs are relegated to the appendix.

II. SETTING THE STAGE

In this section we first review the basic framework of QSV in the nonadversarial scenario. The main results presented here were established by Pallister, Linden, and Montanaro (PLM), but we have simplified the derivation. These results will serve as a benchmark for understanding pure-state verification in the adversarial scenario, which is the main focus of this paper. Then we discuss the connection between QSV and fidelity estimation.

A. Verification of pure states: Nonadversarial scenario

Consider a device that is supposed to produce the target state $\Psi$ in the (generally multipartite) Hilbert space $\mathcal{H}$. In practice, the device may actually produce $\sigma_1, \sigma_2, \ldots, \sigma_N$ in $N$ runs. Following Ref. [13], here we assume that the fidelity $\langle \Psi | \sigma_j | \Psi \rangle$ either equals 1 for all $j$ or satisfies $\langle \Psi | \sigma_j | \Psi \rangle \leq 1 - \epsilon$ for all $j$ (the limitation of this assumption will be analyzed in Sec. III). Now the task is to determine which is the case.

To achieve this task we can perform $N$ tests and accept the states produced if and only if (iff) all tests are passed. Each test is specified by a two-outcome measurement $\{ E_i, 1 - E_i \}$ chosen randomly from a set of accessible measurements. The test operator $E_j$ corresponds to passing the test and satisfies the condition $0 \leq E_j \leq 1$. We assume that the target state $\Psi$ can always pass the test, that is, $E_j(\Psi) = |\Psi\rangle$ for each $E_j$. A verification strategy is characterized by all the tests $E_i$ and the probabilities $\mu_i$ for performing these tests.

To determine the maximal probability of failing to reject the bad case, it is convenient to introduce the verification operator $\Omega := \sum_i \mu_i E_i$. As we shall see later, most key properties of a verification strategy are determined by the verification operator $\Omega$, irrespective of how the test operators are constructed. Therefore, $\Omega$ is also referred...
to as a strategy when there is no danger of confusion. By construction, the target state $|\Psi\rangle$ is an eigenstate of $\Omega$ with the largest eigenvalue $1$. Denote by $\beta(\Omega)$ the second largest eigenvalue of $\Omega$, then $\beta(\Omega)$ is equal to the operator norm of $\Omega - |\Psi\rangle\langle\Psi|$, that is, $\beta(\Omega) = \|\Omega - |\Psi\rangle\langle\Psi|\|$. Let $\nu(\Omega) := 1 - \beta(\Omega)$ be the spectral gap from the largest eigenvalue. When $\langle\Psi|\sigma_j|\Psi\rangle \leq 1 - \epsilon$, the maximum probability that the verification strategy fails is determined by the spectral gap $\nu(\Omega)$ of $\Omega$.

The maximization in the left-hand side runs over all quantum states $\sigma$ that satisfy the fidelity constraint $\langle\Psi|\sigma|\Psi\rangle \leq 1 - \epsilon$. Equation $\ref{eq:1}$ was originally derived by PLM $\ref{43}$ for strategies composed of projective tests, but their proof also applies to general strategies with non-projective tests; see Appendix $\ref{A}$ for a simpler proof.

After $N$ runs, $\sigma_j$ in the bad case can pass all tests with probability at most $[1 - \nu(\Omega)]^N$. This is also the maximum probability that the verification strategy fails to detect the bad case. To achieve significance level $\delta$ (confidence level $1 - \delta$), that is, $[1 - \nu(\Omega)]^N \leq \delta$, the minimum number of tests is given by

$$N_{\text{NA}}(\epsilon, \delta, \Omega) = \left[\frac{\ln \delta}{\ln(1 - \nu(\Omega)\epsilon)}\right] \leq \left[\frac{\ln \delta}{\nu(\Omega)\epsilon}\right], \quad (2)$$

where NA in the subscript means nonadversarial. This number is the main figure of merit of concern in QSV because to a large extent it determines the resource costs of implementing the verification strategy $\Omega$. Note that a single test is sufficient if

$$\nu(\Omega)\epsilon + \delta \geq 1. \quad (3)$$

According to Eq. $\ref{2}$, the efficiency of the strategy $\Omega$ is determined by the spectral gap $\nu(\Omega)$. The optimal protocol is obtained by maximizing the spectral gap $\nu(\Omega)$. If there is no restriction on the accessible measurements, then the optimal protocol is composed of the projective measurement $\{|\Psi\rangle\langle\Psi|, 1 - |\Psi\rangle\langle\Psi|\}$, in which case we have $\Omega = |\Psi\rangle\langle\Psi|$ and $\nu(\Omega) = 1$, so that

$$N_{\text{NA}}(\epsilon, \delta, \Omega) = \left[\frac{\ln \delta}{\ln(1 - \epsilon)}\right] \leq \left[\frac{\ln \delta}{\epsilon}\right]. \quad (4)$$

In addition, the requirement in Eq. $\ref{3}$ reduces to

$$\epsilon + \delta \geq 1. \quad (5)$$

This efficiency cannot be improved further even if we can perform collective measurements. In particular, the scaling behaviors of $\epsilon^{-1}\ln \delta^{-1}$ with $\epsilon$ and $\delta$ are the best we can expect.

In practice, quite often the target state $|\Psi\rangle$ is entangled, but it is not easy to perform entangling measurements. It is therefore crucial to devise efficient verification protocols based on local operations and classical communication (LOCC). Here by “efficient” we mean that the protocols can be applied in practice with reasonable resource costs, which is a much stronger requirement than what is usually understood in computer science. Ideally, the inverse spectral gap $1/\nu(\Omega)$ should be independent of the system size (the number of qubits say) or grow no faster than a low-order polynomial. In addition, the coefficients should be reasonably small. It turns out many important quantum states in quantum information processing can be verified efficiently with respect to these stringent criteria. Besides the total number $N$ of tests determined by $\epsilon$, $\delta$, and $\nu(\Omega)$, the number of potential measurement settings is also of concern if it is difficult to switch measurement settings. Nevertheless, most of our results in Secs. $\ref{X}$ are independent of the specific details (including the number of potential measurement settings) of a verification protocol once the verification operator is fixed.

Here, we compare the approach presented above with previous works Refs. $\ref{33} \ref{40}$. In mathematical statistics, we often discuss hypothesis testing in the framework of uniformly most powerful test among a certain class of tests. In this case, we fix a certain set of states $S_0$, and impose to our test the condition that the probability of erroneously rejecting states in $S_0$ is upper bounded by a certain value $\delta' \geq 0$. Under this condition, we maximize the probability of detecting a state $\sigma$ in $S^c$, where $S^c$ is the complement of $S_0$ in the state space. When a test maximizes the probability uniformly for every state $\sigma$ in $S^c$, it is called a uniformly most powerful (UMP) test. However, since the detecting probability depends on the state $\sigma$, such a test does not exist in general. In this paper, $S_0$ and $\delta'$ are chosen to be $\{|\Psi\rangle\langle\Psi|\}$ and 0, respectively. We consider the case in which the same strategy $\Omega$ is applied $N$ times. Since we support the state $|\Psi\rangle$ only when all our outcomes correspond to the pass eigenspace of $\Omega$, our test is UMP in this case.

When the set $S_0$ is chosen to be $\{|\Psi\rangle\langle\Psi|\geq 1 - \epsilon\}$, and $\delta'$ is a non-zero value, the problem is more complicated. Such a setting arises when we allow a certain amount of error. To resolve this problem, imposing a certain symmetric condition to our tests, Refs. $\ref{33} \ref{40}$ discussed several optimization problems and investigated their asymptotic behaviors when $|\Psi\rangle$ is a maximally entangled state.

### B. Connection with fidelity estimation

When all states $\sigma_j$ produced by the device are identical to $\sigma$, let $F = \langle\Psi|\sigma|\Psi\rangle$ be the fidelity between $\sigma$ and the target state $|\Psi\rangle$; then we have

$$[1 - \tau(\Omega)]F + \tau(\Omega) \leq \text{tr}(\Omega\sigma) \leq \nu(\Omega)F + \beta(\Omega), \quad (6)$$

where $\tau(\Omega)$ is the smallest eigenvalue of $\Omega$. Therefore,

$$\frac{1 - \text{tr}(\Omega\sigma)}{1 - \tau(\Omega)} \leq 1 - F \leq \frac{1 - \text{tr}(\Omega\sigma)}{\nu(\Omega)}. \quad (7)$$
So the passing probability \( \text{tr}(\Omega \sigma) \) provides upper and lower bounds for the infidelity (and fidelity). In general, Eqs. (6) and (7) still hold if \( F \) and \( \text{tr}(\Omega \sigma) \) are replaced by their averages over all \( \sigma_j \). Note that the inequalities in Eqs. (6) and (7) are saturated when \( \tau \sigma \) their averages over all \( \sigma_j \) decreases monotonically with more detail in Sec. VI. In this case we have a strategy \( \nu \), where \( \nu \) this estimation reads \( \langle \sigma \rangle = \beta(\Omega) \); such a strategy \( \Omega \) is called homogeneous and is discussed in more detail in Sec. VI. In this case we have

\[
1 - F = \frac{1 - \text{tr}(\Omega \sigma)}{\nu(\Omega)}, \quad F = \frac{\text{tr}(\Omega \sigma) - \beta(\Omega)}{\nu(\Omega)}. \tag{8}
\]

So the fidelity with the target state can be estimated from the passing probability. The standard deviation of this estimation reads

\[
\Delta F = \frac{\sqrt{p(1-p)}}{\nu \sqrt{N}} = \frac{\sqrt{(1-F)(F+\nu^{-1}-1)}}{\sqrt{N}} \leq \frac{1}{2\nu \sqrt{N}}, \tag{9}
\]

where \( p = \text{tr}(\Omega \sigma) = \nu F + \beta \geq F \) and \( N \) is the number of tests performed. Note that this standard deviation decreases monotonically with \( \nu \) and \( N \). This conclusion is related to the testing of binomial distributions discussed in Ref. [40]. When \( F \geq 1/2 \), which is the case of most interest, we also have

\[
\Delta F = \frac{\sqrt{p(1-p)}}{\nu \sqrt{N}} \leq \frac{\sqrt{F(1-F)}}{\nu \sqrt{N}} \tag{10}
\]

given that \( p \geq F \).

III. VERIFICATION OF PURE STATES: A CRITICAL REEXAMINATION

In this section we reexamine the framework of QSV proposed by PLM [13] as summarized in Sec. II A above and clarify the limitation of this framework. In addition, we show that the limitation can be eliminated when states prepared in different runs are independent. The situation is much more complicated when these states are correlated, which motivates the study of QSV in the adversarial scenario presented in the rest of this paper.

A. What is verified in QSV?

Consider a device that is supposed to produce the target state \( |\Psi\rangle \) in the Hilbert space \( \mathcal{H} \). In practice, the device may actually produce \( \sigma_1, \sigma_2, \ldots, \sigma_N \) in \( N \) runs. In the framework of PLM, it is assumed that the fidelity \( \langle \Psi | \sigma_j | \Psi \rangle \) either equals 1 for all \( j \) or satisfies \( \langle \Psi | \sigma_j | \Psi \rangle \leq 1 - \epsilon \) for all \( j \) [13]. In the independent and identically distributed (i.i.d.) case, all \( \sigma_j \) are identical, so the PLM assumption is actually not necessary (or automatically guaranteed) to derive the conclusions presented in Sec. II A. If we drop the i.i.d. assumption, then the assumption of PLM is quite unnatural and difficult to guarantee. Moreover, the conclusion on QSV drawn based on this assumption is much weaker than what the word “verify” usually conveys. Suppose the test \( E_t \) is performed with probability \( \mu_t \) and \( \Omega = \sum_j \mu_t E_t \) as in Sec. II A. After \( N \) tests are passed, we can only conclude that the probability of passing \( N \) tests is at most \( [1 - \nu(\Omega)\epsilon]^N \) if \( \langle \Psi | \sigma_j | \Psi \rangle \leq 1 - \epsilon \) for all \( j \). In other words, passing these tests only confirms that \( \langle \Psi | \sigma_j | \Psi \rangle > 1 - \epsilon \) for at least one run \( j \) with significance level \( [1 - \nu(\Omega)\epsilon]^N \).

Such a weak conclusion is usually far from enough in practice. Note that the property of each run on average is more relevant if we want to make sure that the device works as expected most of the time rather than occasionally.

B. Independent state preparation

Fortunately we can drop the PLM assumption and draw a stronger conclusion as long as all states \( \sigma_j \) are prepared independently of each other. Note that we do not need the i.i.d. assumption. The variation in \( \sigma_j \) over different runs may be caused by inevitable imperfections of the device or fluctuations in various relevant parameters for example.

Proposition 1. Suppose the \( N \) states \( \sigma_1, \sigma_2, \ldots, \sigma_N \) are independent of each other. Then the probability that they can pass all \( N \) tests associated with the strategy \( \Omega \) satisfies

\[
\prod_{j=1}^{N} \text{tr}(\Omega \sigma_j) \leq [1 - \nu(\Omega)\epsilon]^N, \tag{11}
\]

where \( \epsilon = \sum_j \epsilon_j/N \) with \( \epsilon_j = 1 - \langle \Psi | \sigma_j | \Psi \rangle \) is the average infidelity.

This proposition guarantees that the average fidelity satisfies the inequality \( \sum_j \langle \Psi | \sigma_j | \Psi \rangle/N > 1 - \epsilon \) with significance level \( \delta = [1 - \nu(\Omega)\epsilon]^N \) if \( N \) tests are passed. In addition, to verify \( |\Psi\rangle \) within infidelity \( \epsilon \) and significance level \( \delta \), which means \( [1 - \nu(\Omega)\epsilon]^N \leq \delta \), the minimum number of tests reads

\[
N_{\text{NA}}(\epsilon, \delta, \Omega) = \left\lceil \frac{\ln \delta}{\ln(1 - \nu(\Omega)\epsilon)} \right\rceil \leq \left\lceil \frac{\ln \delta^{-1}}{\nu(\Omega)\epsilon} \right\rceil \tag{12}
\]

This formula is identical to the one in Eq. (2), but it does not rely on the unnatural assumption imposed by PLM [13]. Accordingly, the meaning of “verification” is different. Here we can verify the average fidelity of the states \( \sigma_1, \sigma_2, \ldots, \sigma_N \) prepared by the device rather than the maximal fidelity. Nevertheless, our conclusion relies on the implicit assumption that the average fidelity of states produced by the device after the verification procedure is the same as the average during the verification procedure. This assumption is reasonable in the nonadversarial scenario and is often taken for granted in practice. In case this assumption does not hold, then we have to consider QSV in the adversarial scenario, which is a main focus of this paper.
Proof of Proposition\[4\]

\[
\prod_{j=1}^{N} \text{tr}(\sigma_j) \leq \prod_{j=1}^{N} [1 - \nu(\Omega)\epsilon_j] \leq [1 - \nu(\Omega)\epsilon]^{N}. \tag{13}
\]

Here the first inequality follows from Eq. (1) and is saturated iff each \(\sigma_j\) is supported in the subspace associated with the largest and second largest eigenvalues of \(\Omega\). The second inequality follows from the familiar inequality between the geometric mean and arithmetic mean and is saturated iff all \(\epsilon_j\) are equal to \(\bar{\epsilon}\); that is, all \(\sigma_j\) have the same fidelity (and infidelity) with the target state. Note that variation in \(\sigma_j\) cannot increase the passing probability once the average infidelity \(\bar{\epsilon}\) is fixed. \qed

C. Correlated state preparation

Here we show that the conclusion in Secs. IIA and IIB will fail if the states \(\sigma_1, \sigma_2, \ldots, \sigma_N\) are correlated. As a special example, suppose the device produces the ideal target state \(\langle \Psi | \Psi \rangle^\otimes N\) in \(N\) runs with probability \(0 < a < 1\) and the alternative \(\sigma^\otimes N\) with probability \(1 - a\), where \(\langle \Psi | \sigma | \Psi \rangle = 1 - \epsilon' < 1\). The reduced state of each party reads \(a(\langle \Psi | \Psi \rangle) + (1 - a)\sigma\) and its infidelity with the target state is \(\epsilon = (1 - a)\epsilon'\). Note that the device can pass \(N\) tests with probability at least \(a\) no matter how large \(N\) is. So it is impossible to verify the target state within infidelity \(\epsilon = (1 - a)\epsilon'\) and significance level \(\delta < a\) using the approach presented in Sec. IIA or that in Sec. IIB. This observation further reveals the limitation of the PLM framework of QSV. To overcome this difficulty, we need to consider a different framework of QSV as formulated in the next section.

IV. QUANTUM STATE VERIFICATION IN THE ADVERSARIAL SCENARIO

Now we turn to the adversarial scenario in which the device for generating quantum states is controlled by a potentially malicious adversary. In this case the device may produce arbitrary correlated or even entangled states. Efficient verification of quantum states in such adversarial scenario is crucial to many tasks in quantum information processing that entail high security requirements, such as blind quantum computation [12–16] and quantum networks [22–24]. However, little is known about this topic in the literature. The approach of PLM does not apply as illustrated by the example of correlated state preparation in Sec. IIC. Most other studies in the literature only focus on specific families of states, such as graph states [13, 15, 24] and hypergraph states [18, 42]. In addition, known protocols are too resource consuming to be applied in practice, especially for hypergraph states, in which case the best protocol known in the literature requires an astronomical number of tests already for three-qubit hypergraph states. The difficulty in constructing efficient verification protocols in the adversarial scenario is tied to the fact that even for a given protocol, no efficient method is available for determining the minimal resource cost necessary to reach the target precision.

In this section we introduce a general framework of pure state verification in the adversarial scenario together with the main figures of merit. The basic ideas presented here will serve as a stepping stone for the following study.

A. Formulation

To establish a reliable and efficient framework for verifying pure states in the adversarial scenario, first note that the verification and application of a quantum state cannot be completely separated in the adversarial scenario. Otherwise, the device may produce ideal target states in the verification stage and so can always pass the tests, but produce a garbage state in the application stage. To resolve this problem, suppose the device produces an arbitrary correlated or entangled state \(\rho\) on the whole system \(\mathcal{H}^\otimes (N + 1)\). Our goal is to ensure that the reduced state on one system (for application) has infidelity less than \(\epsilon\) by performing \(N\) tests on other systems. We can randomly choose \(N\) systems and apply a verification strategy \(\Omega\) to each system chosen and accept the state on the remaining system iff all \(N\) tests are passed. Since \(N\) systems are chosen randomly, we may assume that \(\rho\) is permutation invariant without loss of generality.

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

\[
p_{\rho} = \text{tr}[(\Omega^\otimes N \otimes 1)\rho]. \tag{14}\]

If \(N\) tests are passed, then the reduced state on system \(N + 1\) (assuming \(p_{\rho} > 0\)) is given by

\[
\sigma'_{N+1} = p^{-1}_{\rho} \text{tr}_{1,2,\ldots,N}[\Omega^\otimes N \otimes 1]\rho, \tag{15}\]

where \(\text{tr}_{1,2,\ldots,N}\) means the partial trace over the systems \(1, 2, \ldots, N\). The fidelity between \(\sigma'_{N+1}\) and the target state \(|\Psi\rangle\rangle\) reads

\[
F_{\rho} = \langle \Psi | \sigma'_{N+1} | \Psi \rangle = p^{-1}_{\rho} f_{\rho}, \tag{16}\]

where

\[
f_{\rho} = \text{tr}[(\Omega^\otimes N \otimes |\Psi\rangle\langle \Psi|)\rho]. \tag{17}\]

When \(\rho = \sigma^\otimes (N+1)\) is a tensor power of the state \(\sigma\) with \(0 < \epsilon' = 1 - \langle \Psi | \sigma | \Psi \rangle \leq 1\), we have \(p_{\rho} \leq [1 - \nu(\Omega)\epsilon']^{N}\), \(\sigma'_{N+1} = \sigma\), and \(F_{\rho} = 1 - \epsilon'\). These conclusions coincide with the counterpart for the nonadversarial scenario as expected. The situation is different if \(\rho\) does not have this form. Suppose \(\rho = a(|\Psi\rangle\langle \Psi|)^\otimes (N+1) + (1 - a)\sigma^\otimes (N+1)\) with \(0 < a < 1\) for example; cf. Sec. IIC. If \(N\) tests are passed, then the reduced state of party \(N + 1\) reads

\[
\sigma'_{N+1} = \frac{a|\Psi\rangle\langle \Psi| + b\sigma}{a + b}, \tag{18}\]
where \( b := (1 - a)\left|\text{tr}(\Omega \sigma)\right|^N \) satisfies
\[
b \leq (1 - a)(1 - \nu(\Omega)\epsilon)^N \tag{19}\]
and decreases exponentially with \( N \) unless \( \text{tr}(\Omega \sigma) = 0 \). Therefore, the infidelity \( 1 - \langle \Psi | \sigma' \otimes N-1 | \Psi \rangle \) approaches zero exponentially with \( N \) even if \( a \) is arbitrarily small. If the infidelity is bounded from below by \( 1 - \langle \Psi | \sigma' \otimes N-1 | \Psi \rangle \geq \epsilon \) for \( 0 < \epsilon < 1 \), then \( a \) should approach zero as \( N \) increases; accordingly, the passing probability will approach zero. This observation indicates that we can verify the target state within any given infidelity \( 0 < \epsilon < 1 \) and significance level \( 0 < \delta < 1 \) even when the states prepared are correlated, which demonstrates the advantage of the alternative approach presented above over the PLM approach. In the rest of this paper we will show that indeed it is possible to verify pure states efficiently even if the device is controlled by the adversary and can produce arbitrary correlated or even entangled states allowed by quantum mechanics.

B. Main figures of merit

To characterize the performance of the strategy \( \Omega \) adapted to the adversarial scenario, here we introduce four figures of merit. Define
\[
\zeta(N, \delta, \Omega) := \min_{\rho} \left\{ f_\rho | p_\rho \geq \delta \right\}, \quad 0 \leq \delta \leq 1, \tag{20a}
\]
\[
\eta(N, f, \Omega) := \max_{\rho} \left\{ p_\rho | f_\rho \leq f \right\}, \quad 0 \leq f \leq 1, \tag{20b}
\]
\[
F(N, \delta, \Omega) := \min_{\rho} \left\{ p_\rho^{-1} f_\rho | p_\rho \geq \delta \right\}, \quad 0 < \delta \leq 1, \tag{20c}
\]
\[
F(N, f, \Omega) := \min_{\rho} \left\{ p_\rho^{-1} f_\rho | f_\rho \geq f \right\}, \quad 0 < f \leq 1, \tag{20d}
\]
where \( N \geq 1 \) is the number of tests performed and the minimization or maximization is taken over permutation-invariant quantum states \( \rho \) on \( \mathcal{H}^\otimes (N + 1) \). 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 minimum fidelity of the reduced 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 non-decreasing in \( \delta \), while \( F(N, f, \Omega) \) and \( \eta(N, f, \Omega) \) are non-decreasing in \( f \). A simple upper bound for \( F(N, \delta, \Omega) \) can be derived by considering quantum states \( \rho \) on \( \mathcal{H}^\otimes (N + 1) \) that can be expressed as tensor powers in Eq. (20c), which yields
\[
F(N, \delta, \Omega) \leq \max \left\{ 0, 1 - \frac{1 - \delta^{1/N}}{\nu(\Omega)} \right\}. \tag{21}\]

The four figures of merit defined in Eq. (20) are tied to the two-dimensional region \( R_{N, \Omega} \) composed of all the points \( (p_\rho, f_\rho) \) for permutation-invariant density matrices \( \rho \) on \( \mathcal{H}^\otimes (N + 1) \), that is,
\[
(\{p_\rho, f_\rho\} | \rho \text{ on } \mathcal{H}^\otimes (N + 1) \text{ are permutation invariant}), \tag{22}\]
This geometric picture will be very helpful to understanding QSV 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 minimum number of tests required to reach a given precision. To this end, for \( 0 < \epsilon, \delta < 1 \), we define \( N(\epsilon, \delta, \Omega) \) as the minimum value of the positive integer \( N \) that satisfies the condition \( F(N, \delta, \Omega) \geq 1 - \epsilon \), namely
\[
N(\epsilon, \delta, \Omega) := \min \{ N \geq 1 | F(N, \delta, \Omega) \geq 1 - \epsilon \}. \tag{23}\]

Then Eq. (21) implies that
\[
N(\epsilon, \delta, \Omega) \geq \left[ \frac{\ln \delta}{\ln(1 - \nu(\Omega)\epsilon)} \right] = N_{\text{NA}}(\epsilon, \delta, \Omega) \tag{24}\]
as expected since it is much more difficult to verify a quantum state in the adversarial scenario than nonadversarial scenario. How much overhead is required in the adversarial scenario? Can we achieve the same scaling behaviors in \( \epsilon \) and \( \delta \)?

In general it is very difficult to derive an analytical formula for \( N(\epsilon, \delta, \Omega) \) if not impossible. Therefore, it is nontrivial to determine the efficiency limit of QSV in the adversarial scenario even if there is no restriction on the accessible measurements, or even if the target state belongs to a single party, which is in sharp contrast with QSV in the nonadversarial scenario. Indeed, it took a long time and a lot of efforts to settle this issue.

V. COMPUTATION OF THE MAIN FIGURES OF MERIT

In this section we develop a general method for computing the figures of merit defined in Eq. (20), which characterize the verification precision in the adversarial scenario. We also clarify the properties of these figures of merit in preparation for later study. Both algebraic derivation and geometric pictures will be helpful in our analysis.

A. Key observations

Suppose the verification operator \( \Omega \) for the target state \( |\Psi\rangle \in \mathcal{H} \) has spectral decomposition \( \Omega = \sum_{j=1}^{\beta} \lambda_j \Pi_j \), where \( \lambda_j \) are the eigenvalues of \( \Omega \) arranged in decreasing order \( 1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_\beta \geq 0 \), 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 \( \tau := \lambda_\beta \) 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 $\mathcal{H}^{(N+1)}$, which is permutation invariant (cf. Sec. IV). 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 $k = (k_1, k_2, \ldots, k_D)$ be a sequence of $D$ nonnegative integers that sum up to $N+1$, that is, $\sum_j k_j = N+1$. Let $\mathcal{F}_N$ be the set of all such sequences. For each $k \in \mathcal{F}_N$, we can define a permutation-invariant diagonal density matrix $\rho_k$ on $\mathcal{H}^{(N+1)}$ as the uniform mixture of all permutations of $\Pi_1^{\otimes k_1} \otimes \Pi_2^{\otimes k_2} \otimes \cdots \otimes \Pi_D^{\otimes k_D}$. Then any permutation-invariant diagonal density matrix $\rho$ on $\mathcal{H}^{(N+1)}$ can be expressed as $\rho = \sum_{k \in \mathcal{F}_N} c_k \rho_k$, where $c_k$ form a probability distribution on $\mathcal{F}_N$. Accordingly,

$$p_\rho = \sum_{k \in \mathcal{F}_N} c_k \eta_k(\lambda), \quad f_\rho = \sum_{k \in \mathcal{F}_N} c_k \zeta_k(\lambda),$$

$$F_\rho = \frac{p_\rho}{f_\rho} = \frac{\sum_{k \in \mathcal{F}_N} c_k \eta_k(\lambda)}{\sum_{k \in \mathcal{F}_N} c_k \zeta_k(\lambda)},$$

(25)

(26)

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

$$\eta_k(\lambda) := p_{\rho_k} = \sum_{i | k_i > 0} \frac{k_i}{N+1} \lambda_i^{k_i-1} \prod_{j \neq i} \lambda_j^{k_j},$$

$$\zeta_k(\lambda) := f_{\rho_k} = \frac{k_1}{N+1} \prod_{i | k_i > 0} \lambda_i^{k_i}. (27)$$

Here we set $\lambda_0 = 1$ even if $\lambda_1 = 0$.

The assumption $1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_D = \tau \geq 0$ implies that $\zeta_k(\lambda) \leq \eta_k(\lambda) \leq 1$; the second inequality is saturated iff $k = k_0 := (N+1, 0, \ldots, 0)$, in which case both inequalities are saturated, that is, $\zeta_k(\lambda) = \eta_k(\lambda) = 1$. As an implication, we have $f_\rho \leq p_\rho \leq 1$, and the second inequality is saturated iff $\rho = \rho_{k_0} = (|\Psi\rangle \langle \Psi|)^{\otimes (N+1)}$, in which case $f_\rho = p_\rho = 1$. This observation implies that

$$F(N, \delta = 1, \Omega) = \zeta(N, \delta = 1, \Omega) = 1,$$

$$F(N, f = 1, \Omega) = \eta(N, f = 1, \Omega) = 1.$$  

(28)  

(29)

By contrast, $\eta_k(\lambda) \geq \tau^N$, and the lower bound is saturated when $k = (0, \ldots, 0, N+1)$. 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. (22) is the convex hull of $(\eta_k(\lambda), \zeta_k(\lambda))$ for all $k \in \mathcal{F}_N$, 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 $F(N, \delta, \Omega)$, $\zeta(N, \delta, \Omega)$, and $\eta(N, f, \Omega)$ defined in Eq. (20) given that they are completely determined by the region $R_{N, \Omega}$. For example, $\zeta(N, \delta, \Omega)$ corresponds to the lower boundary of the intersection of $R_{N, \Omega}$ and the vertical line $p_\rho = \delta$ as long as $\delta \geq \tau^N$ (cf. Lemma 2 below). 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.

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 $R_{N, \Omega'} \subset R_{N, \Omega}$ and $\Omega'$ is equally efficient or more efficient than $\Omega$ in the sense that

$$F(N, \delta, \Omega') \geq F(N, \delta, \Omega), \quad N(\epsilon, \delta, \Omega') \leq N(\epsilon, \delta, \Omega).$$  

(30)

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

\section*{B. Computation of the verification precision}

Here we show that the four figures of merit $\zeta(N, \delta, \Omega)$, $\eta(N, f, \Omega)$, $F(N, \delta, \Omega)$, and $\zeta(N, f, \Omega)$ can be computed by linear programming. Lemmas 1 and 2 below are proved in Appendix A. To start with, we first determine $\eta(N, 0, \Omega)$, the maximum of $p_\rho$ under the condition $f_\rho = 0$.

Lemma 1. $\eta(N, 0, \Omega) = \delta_\epsilon$, where

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

(31)

\begin{figure}[h]
\centering
\includegraphics[width=\columnwidth]{fig1}
\caption{(color online) The region $R_{N, \Omega}$ composed of $(p_\rho, f_\rho)$ as defined in Eq. (22). This region is the convex hull of points $(\eta_k(\lambda), \zeta_k(\lambda))$ for $k \in \mathcal{F}_N$, which are highlighted as red dots. Here $\Omega$ has three distinct eigenvalues, namely, 1, 0.4, and 0.2.}
\end{figure}
Lemma 1 has implications for the figures of merit \( F(N,\delta,\Omega) \) and \( \zeta(N,\delta,\Omega) \) as well,

\[
F(N,\delta,\Omega) = \zeta(N,\delta,\Omega) = 0, \quad 0 < \delta \leq \delta_c,
\]

\[
F(N,\delta,\Omega) > 0, \quad \zeta(N,\delta,\Omega) > 0, \quad \delta_c < \delta \leq 1.
\]  (32) (33)

The equality \( \zeta(N,\delta,\Omega) = 0 \) also holds when \( \delta = 0 \).

Next, we introduce alternative definitions of the figures of merit defined in Eq. (30), which are easier to analyze and compute. Define

\[
\zeta(N,\delta,\Omega) := \begin{cases} 0, & \delta_c \leq \delta \leq 1, \\ \min_{p} \left\{ f_p : p_{\rho} = \delta \right\}, & 0 \leq \delta \leq \delta_c. \end{cases}
\]  (34a)

\[
\bar{\eta}(N, f, \Omega) := \max_{\rho} \left\{ p_{\rho} : f_{\rho} = f \right\}, \quad 0 \leq f \leq 1,
\]

\[
\bar{F}(N,\delta,\Omega) := \delta^{-1}\zeta(N,\delta,\Omega), \quad 0 < \delta \leq 1,
\]

\[
\bar{F}(N, f, \Omega) := [\bar{\eta}(N, f, \Omega)]^{-1} f, \quad 0 < f \leq 1.
\]  (34b) (34c) (34d)

Here \( \delta_c \) in Eq. (34a) can be replaced by \( \tau^N \) given that \( \min_{p} \left\{ f_p : p_{\rho} = \delta \right\} = 0 \) for \( \tau^N \leq \delta \leq \delta_c \).

**Lemma 2.** Suppose \( N \) is a positive integer and \( \Omega \) is a verification operator. Then

\[
\zeta(N,\delta,\Omega) = \zeta(N,\delta,\Omega), \quad 0 \leq \delta \leq 1,
\]

\[
\eta(N, f, \Omega) = \eta(N, f, \Omega), \quad 0 \leq f \leq 1.
\]  (35a) (35b)

\[
F(N,\delta,\Omega) = \bar{F}(N,\delta,\Omega), \quad 0 < \delta \leq 1,
\]

\[
\mathcal{F}(N, f, \Omega) = \bar{F}(N, f, \Omega), \quad 0 < f \leq 1.
\]  (35c) (35d)

For \( 0 < \delta, f \leq 1 \), Lemma 2 implies that

\[
F(N,\delta,\Omega) = \delta^{-1}\zeta(N,\delta,\Omega) = \delta^{-1}\zeta(N,\delta,\Omega),
\]

\[
\mathcal{F}(N, f, \Omega) = [\eta(N, f, \Omega)]^{-1} f = [\eta(N, f, \Omega)]^{-1} f.
\]  (36a) (36b)

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. (23) and Lemma 2, \( \zeta(N,\delta,\Omega) \) with \( \delta_c \leq \delta \leq 1 \) and \( \eta(N, f, \Omega) \) with \( 0 \leq f \leq 1 \) can be computed via linear programming,

\[
\zeta(N,\delta,\Omega) = \min_{\{c_k\}} \left\{ \sum_{k \in \mathcal{J}_N} c_k \zeta_k(\lambda) : \sum_{k \in \mathcal{J}_N} c_k \eta_k(\lambda) = \delta \right\},
\]

\[
\eta(N, f, \Omega) = \max_{\{c_k\}} \left\{ \sum_{k \in \mathcal{J}_N} c_k \eta_k(\lambda) : \sum_{k \in \mathcal{J}_N} c_k \zeta_k(\lambda) = f \right\},
\]  (37a) (37b)

where \( c_k \) form a probability distribution on \( \mathcal{J}_N \). Here the minimum in Eq. (37a) can be attained at a distribution \( \{c_k\} \) that is supported on at most two points in \( \mathcal{J}_N \); a similar conclusion holds for the maximum in Eq. (37b). 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. (37) 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 \( (\eta_k(\lambda), \zeta_k(\lambda)) \) for some \( k \in \mathcal{J}_N \); cf. Lemma 13 in Appendix 13.

**C. Properties of the main figures of merit**

Next, we summarize the main properties of the five figures of merit \( \zeta(N,\delta,\Omega) \), \( \eta(N, f, \Omega) \), \( F(N,\delta,\Omega) \), \( \mathcal{F}(N, f, \Omega) \), and \( \mathcal{N}(\epsilon,\delta,\Omega) \); the proofs are relegated to Appendix 13. These properties are tied to the fact that the region \( R_{N,\Omega} \) is a convex polygon.

**Lemma 3.** The following statements hold.

1. \( \zeta(N,\delta,\Omega) \) is convex and nondecreasing in \( \delta \) for \( 0 \leq \delta \leq 1 \) and is strictly increasing for \( \delta_c \leq \delta \leq 1 \).

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

3. \( F(N,\delta,\Omega) \) is nondecreasing in \( \delta \) for \( 0 < \delta \leq 1 \) and is strictly increasing for \( \delta_c \leq \delta \leq 1 \).

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

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

\[
\zeta(N,\delta,\Omega) = \zeta(N,\delta,\Omega), \quad \eta(N, f, \Omega) = \eta(N, f, \Omega),
\]

\[
\mathcal{F}(N, f, \Omega) = \mathcal{F}(N, f, \Omega).
\]  (38a) (38b)

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

\[
\zeta(N,\delta,\Omega) \geq \zeta(N,\delta,\Omega), \quad \eta(N, f, \Omega) \leq \eta(N, f, \Omega),
\]

\[
\mathcal{F}(N, f, \Omega) \geq \mathcal{F}(N, f, \Omega).
\]  (39a) (39b) (39c) (39d)

The first two inequalities are saturated iff \( \delta \leq \delta_c \) or \( \delta = 1 \), where \( \delta_c \) is given in Eq. (31). The last two inequalities are saturated iff \( f = 1 \).

Next, we turn to the figure of merit \( \mathcal{N}(\epsilon,\delta,\Omega) \) defined in Eq. (25). As an implication of Lemma 5, \( \mathcal{N}(\epsilon,\delta,\Omega) \) increases monotonically with \( 1/\epsilon \) and \( 1/\delta \) as expected. The following lemma provides several equivalent ways for computing \( \mathcal{N}(\epsilon,\delta,\Omega) \).

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

\[
\mathcal{N}(\epsilon,\delta,\Omega) = \min \{ N \mid \zeta(N,\delta,\Omega) \geq \zeta(1-\epsilon,\Omega) \}
\]

\[
= \min \{ N \mid \eta(N,\delta,\Omega) \leq \eta(1-\epsilon,\Omega) \}
\]

\[
= \min \{ N \mid \mathcal{F}(N,\delta(1-\epsilon),\Omega) \geq (1-\epsilon) \}. \quad (40) \quad (41) \quad (42)
\]

Finally, we present a lemma which is useful for comparing the efficiencies of two verification operators. Let \( \Omega \) be another verification operator for the same target state as \( \Omega \).
Lemma 7. Suppose \( \zeta_k(\lambda) \geq \zeta(N, \delta = \eta_k(\lambda), \tilde{\Omega}) \) for all \( k \in \mathcal{N} \).

Then
\[
\begin{align*}
\zeta(N, \delta, \Omega) & \geq \zeta(N, \delta, \tilde{\Omega}), \quad 0 \leq \delta \leq 1, \\
F(N, \delta, \Omega) & \geq F(N, \delta, \tilde{\Omega}), \quad 0 < \delta \leq 1, \\
N(\epsilon, \delta, \Omega) & \leq N(\epsilon, \delta, \tilde{\Omega}), \quad 0 < \epsilon, \delta < 1.
\end{align*}
\]

Lemma 7 is applicable in particular when the set of distinct eigenvalues of \( \Omega \) is contained in that of \( \tilde{\Omega} \), that is, \( \sigma(\Omega) \subset \sigma(\tilde{\Omega}) \), assuming \( \beta(\Omega) < 1 \); cf. Eq. (30).

VI. HOMOGENEOUS STRATEGIES

A strategy (or verification operator) \( \Omega \) for \( |\Psi\rangle \) is homogeneous if it has the form
\[
\Omega = |\Psi\rangle\langle\Psi| + \lambda(1 - |\Psi\rangle\langle\Psi|),
\]
where \( 0 \leq \lambda < 1 \). In this case, all eigenvalues of \( \Omega \) are equal to \( \lambda \) except for the largest one, so we have \( \beta = \tau = \lambda \) and \( \nu = 1 - \lambda \). 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 operator \( \tilde{\Omega} \) equal to the identity operator.

For bipartite pure states \([39, 40, 43–45]\) and stabilizer states \([43]\), the homogeneous strategy can also be realized by virtue of local projective measurements when \( \lambda \) is sufficiently large; see Sec. X.

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.

Given that the homogeneous strategy \( \Omega \) in Eq. (44) is determined by the parameter \( \lambda \), it is more informative to express the figures of merit defined in Eqs. (20) and (23) as follows,
\[
\begin{align*}
F(N, \delta, \lambda) & := F(N, \delta, \Omega), \\
F(N, f, \lambda) & := F(N, f, \Omega), \\
\zeta(N, \delta, \lambda) & := \zeta(N, \delta, \Omega), \\
\eta(N, f, \lambda) & := \eta(N, f, \Omega), \\
N(\epsilon, \delta, \lambda) & := N(\epsilon, \delta, \Omega).
\end{align*}
\]

Then Lemma 11 implies that
\[
\eta(N, 0, \lambda) = \delta_\epsilon = \begin{cases} 
\lambda^N, & \lambda > 0, \\
1/(N+1), & \lambda = 0.
\end{cases}
\]

Suppose \( \tilde{\Omega} \) is an arbitrary verification operator with eigenvalues \( 1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_D \geq 0 \). Then we have \( F(N, \delta, \lambda_j) \geq F(N, \delta, \tilde{\Omega}) \) for \( 2 \leq j \leq D \) according to Eq. (39). 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 to QSV in the adversarial scenario.

In preparation for the following discussions, we need to introduce a few more notations. Denote by \( \mathbb{Z} \) and \( \mathbb{Z}_0^+ \) the set of integers and the set of nonnegative integers, respectively. For \( k \in \mathbb{Z}_0^+ \), define
\[
\begin{align*}
\eta_k(\lambda) & := \frac{(N + 1 - k)\lambda^k + k\lambda^{k-1}}{N + 1}, \\
\zeta_k(\lambda) & := \frac{(N + 1 - k)\lambda^k}{N + 1}.
\end{align*}
\]

We take the convention that \( \lambda^0 = \eta_0(\lambda) = \zeta_0(\lambda) = 1 \) even if \( \lambda = 0 \). Note that
\[
\eta_k(\lambda) = \eta_k(\lambda), \quad \zeta_k(\lambda) = \zeta_k(\lambda)
\]
when \( k \in \{0, 1, \ldots, N + 1\} \), where \( k = (N + 1 - k, k, \lambda = (1, \lambda) \), and \( \eta_k(\lambda), \zeta_k(\lambda) \) are defined in Eq. (20). The extension of the definitions of \( \eta_k(\lambda) \) and \( \zeta_k(\lambda) \) over \( k \) to the set \( \mathbb{Z}_0^+ \) will be useful in proving several important results on homogeneous strategies.

A. Singular homogeneous strategy

When \( \lambda = 0 \), the verification operator \( \Omega = |\Psi\rangle\langle\Psi| \) is singular (has a zero eigenvalue), and Eq. (17) reduces to
\[
\begin{align*}
\eta_k(\lambda) & = \begin{cases} 
1 & k = 0, \\
(N + 1)^{-1} & k = 1, \\
0 & 1 \leq k \geq 2.
\end{cases} \\
\zeta_k(\lambda) & = \begin{cases} 
1 & k = 0, \\
0 & k \geq 1.
\end{cases}
\end{align*}
\]

By Lemma 2, we have \( F(N, \delta, \lambda = 0) = \zeta(N, \delta, \lambda = 0)/\delta \) for \( 0 < \delta \leq 1 \), where
\[
\zeta(N, \delta, \lambda = 0) = \max \left\{ 0, \frac{(N + 1)\delta - 1}{N} \right\}
\]
\[
= \begin{cases} 
0, & 0 \leq \delta \leq (N + 1)^{-1}, \\
\frac{(N + 1)\delta - 1}{N}, & (N + 1)^{-1} \leq \delta < 1.
\end{cases}
\]

Given \( 0 < \epsilon, \delta < 1 \), the minimum number of tests required to verify the pure state \( |\Psi\rangle \) within infidelity \( \epsilon \) and significance level \( \delta \) reads
\[
N(\epsilon, \delta, \lambda = 0) = \left\lceil \frac{1 - \delta}{\epsilon \delta} \right\rceil.
\]

Here the scaling with \( 1/\delta \) is not satisfactory although the strategy is optimal in the nonadversarial scenario according to Eqs. (2) and (12). Fortunately, nonsingular homogeneous strategies can achieve a better scaling behavior, as we shall see shortly.

B. Nonsingular homogeneous strategies

1. Verification precision

Here we assume \( 0 < \lambda < 1 \), so the homogeneous strategy defined in Eq. (14) is nonsingular (which means
the verification operator is positive definite). In this case, \( \eta_\kappa(\lambda) \) decreases strictly monotonically with \( k \) and \( \eta_k(\lambda) > 0 \) for \( k \in \mathbb{Z}^\geq 0 \); by contrast, \( \zeta_k(\lambda) \) decreases strictly monotonically with \( k \) and \( \zeta_k(\lambda) \geq 0 \) for \( k \in \{0, 1, \ldots, N+1\} \), while \( \zeta_k(\lambda) < 0 \) for \( k > N+1 \). Define

\[
c_k(\delta, \lambda) := \frac{\delta - \eta_{k+1}(\lambda)}{\eta_k(\lambda) - \eta_{k+1}(\lambda)},
\]

\[
\zeta(N, \delta, \lambda, k) := c_k(\delta, \lambda) \zeta_k(\lambda) + [1 - c_k(\delta, \lambda)] \zeta_{k+1}(\lambda) = \frac{\lambda \delta [1 + (N-k)\nu] - \lambda^k}{\nu(k\nu + N\lambda)},
\]

where \( \nu = 1 - \lambda \). The main properties of \( \zeta(N, \delta, \lambda, k) \) are summarized in Lemmas 18 and 19 in Appendix C. The following theorem determines the fidelity that can be achieved by a given number of tests for a given significance level; see Appendix C 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

\[
\zeta(N, \delta, \lambda) = \begin{cases} 
0, & \delta \leq \lambda^N, \\
\zeta(N, \delta, \lambda, k_\nu), & \delta > \lambda^N,
\end{cases}
\]

where \( k_\nu \) is the largest integer \( k \) that satisfies \( \eta_{k_\nu}(\lambda) \geq \delta \), that is, \((N+1-k)\lambda^k + k\lambda^{k-1} > (N+1)\delta\).

The choice of the parameter \( k_\nu \) in Theorem 1 guarantees that \( 0 < c_{k_\nu}(\delta, \lambda) \leq 1 \). Define

\[
k_+ := \lfloor \log_\lambda \delta \rfloor, \quad k_- := \lfloor \log_\lambda \delta \rfloor.
\]

If \( \lambda^N < \delta \leq 1 \), then \( 0 \leq k_+ \leq N \) and \( 0 \leq k_- \leq N-1 \). Meanwhile, we have \( \eta_{k_\nu}(\lambda) \geq \delta \) and \( \eta_{k_\nu+1}(\lambda) < \delta \) by Eq. (47), so \( k_\nu \) is equal to either \( k_+ \) or \( k_- \). In addition, when \( k \in \{0, 1, \ldots, N\} \), Theorem 1 implies that

\[
F(N, \delta = \lambda^k, \lambda) = \frac{(N-k)\lambda}{k + (N-k)\lambda},
\]

which decreases monotonically with \( k \). In particular we have \( F(N, \delta = 1, \lambda) = 1 \) as expected; cf. Eq. (25). When \( \delta = \eta_k(\lambda) \) with \( k \in \{0, 1, \ldots, N+1\} \), we have

\[
F(N, \delta = \eta_k(\lambda), \lambda) = \frac{\zeta_k(\lambda)}{\eta_k(\lambda)} = \frac{(N+1-k)\lambda}{k + (N+1-k)\lambda},
\]

which also decreases monotonically with \( k \). The dependences of \( \zeta(N, \delta, \lambda) \) and \( F(N, \delta, \lambda) \) on \( \delta \) and \( \lambda \) are illustrated in Fig. 2.

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

\[
\zeta(N, \delta, \lambda) = \max\left\{0, \max_{k \in \mathbb{Z}^\geq 0} \zeta(N, \delta, k)\right\}
\]

\[
= \max\left\{0, \zeta(N, \delta, k_+), \zeta(N, \delta, k_-)\right\}
\]

\[
= \max\left\{0, \max_{k \in \{0, 1, \ldots, N\}} \zeta(N, \delta, k)\right\}.
\]

**Corollary 2.** Suppose \( 0 \leq \lambda < 1 \). Then \( F(N, \delta, \lambda) \) is nondecreasing in \( \delta \) for \( 0 < \delta \leq 1 \) and in \( N \) for \( N \geq 1 \).

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

\[
\frac{(N-k_+)\lambda}{k_+ + (N-k_+)\lambda} \leq F(N, \delta, \lambda) \leq \frac{(N-k_-)\lambda}{k_- + (N-k_-)\lambda}.
\]

When \( \lambda = 0 \), Corollary 2 follows from Eq. (50). When \( 0 < \lambda < 1 \), Corollary 2 follows from Theorem 1 (cf. Corollary 1 above and Lemma 18 in Appendix C); alternatively, it is an implication of Lemmas 3 and 5. Corollary 3 is an immediate consequence of Corollary 2 and Eq. (50) given that \( \lambda^{k_\nu} \geq \delta \leq \lambda^{k_-} \).

### 2. Number of required tests

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

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

\[
\tilde{N}_\pm(\epsilon, \delta, \lambda) := \tilde{N}(\epsilon, \delta, \lambda, k_\pm),
\]
where \( F = 1 - \epsilon, \nu = 1 - \lambda, \text{ and } k_\pm \) are given in Eq. (59).

The main properties of \( \tilde{N}(\epsilon, \delta, \lambda, k) \) are summarized in Lemma 20 in the appendix; see also Lemma 21. In particular, \( \tilde{N}(\epsilon, \delta, \lambda, k) = \tilde{N}(\epsilon, \delta, \lambda, k-1) \) iff \( \delta \leq \lambda^k/(F + \lambda\epsilon) \), assuming that \( 0 < \epsilon, \delta, \lambda < 1 \) and \( k \) is a positive integer.

**Theorem 2.** Suppose \( 0 < \epsilon, \delta, \lambda < 1 \). Then we have

\[
N(\epsilon, \delta, \lambda) = \left[ \min_{k \geq 2} \tilde{N}(\epsilon, \delta, \lambda, k) \right] = \left[ \tilde{N}(\epsilon, \delta, \lambda, k^*) \right] \quad (65)
\]

\[
N(\epsilon, \delta, \lambda) = \left\{ \begin{array}{ll}
\tilde{N}_+(\epsilon, \delta, \lambda), & \delta \geq \frac{\lambda^{k_+}}{F + \lambda\epsilon}, \\
\tilde{N}_-(-, \delta, \lambda), & \delta \leq \frac{\lambda^{k_-}}{F + \lambda\epsilon}, 
\end{array} \right. \quad (66)
\]

where \( k^* \) is the largest integer \( k \) that satisfies the inequality \( \delta \leq \lambda^k/(F\nu + \lambda\epsilon) = \lambda^k/(F + \lambda\epsilon) \) and it is equal to either \( k_+ \) or \( k_- \).

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

\[
N(\epsilon, \delta, \lambda) \leq \left[ \tilde{N}(\epsilon, \delta, \lambda, k) \right] \quad \forall k \in \mathbb{Z}^{\geq 0}, \quad (68)
\]

where the upper bound for a given \( k \) is saturated when \( \lambda^{k+1}/(F + \lambda\epsilon) \leq \delta \leq \lambda^k/(F + \lambda\epsilon) \). Corollary 1 is an easy consequence of Theorem 2.

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

**Theorem 3.** Suppose \( 0 < \epsilon, \delta, \lambda < 1 \). Then we have

\[
k_- + \left[ \frac{k_- F}{\lambda\epsilon} \right] \leq N(\epsilon, \delta, \lambda) \leq k_+ + \left[ \frac{k_+ F}{\lambda\epsilon} \right], \quad (73)
\]

\[
N(\epsilon, \delta, \lambda) \leq \frac{\log_{\lambda\epsilon} \delta - \frac{\nu k_-}{\lambda}}{\lambda} = \left[ \frac{\ln \delta - \frac{\nu k_-}{\lambda}}{\ln \lambda} \right], \quad (74)
\]

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

The results also hold when \( \lambda = 0 \) (as long as \( 0 < \epsilon, \delta < 1 \)) according to Eq. (59). If \( \lambda^2/(F + \lambda\epsilon) \leq \delta \leq \lambda/(F + \lambda\epsilon) \), then Eq. (70) is saturated, so we have

\[
N(\epsilon, \delta, \lambda) \leq \left[ \frac{1 - \delta}{\nu \epsilon \delta} \right]. \quad (71)
\]

This result also holds when \( \lambda = 0 \) (as long as \( 0 < \epsilon, \delta < 1 \)) according to Eq. (59). If \( \lambda^2/(F + \lambda\epsilon) \leq \delta \leq \lambda/(F + \lambda\epsilon) \), then Eq. (70) is saturated, so we have

\[
N(\epsilon, \delta, \lambda) \leq \left[ \frac{1 - \delta}{\nu \epsilon \delta} \right]. \quad (71)
\]

where the lower bound is proved in Appendix C.2. Equations (71) and (72) indicate that homogeneous strategies with small \( \lambda \), say \( \lambda \leq 0.1 \), are not efficient for high-precision QSV (say \( \epsilon, \delta \leq 0.1 \)), as reflected in Fig. 1. The following theorem provides informative bounds for \( N(\epsilon, \delta, \lambda) \), which complement the analytical formulas in Theorem 2.

**Theorem 4.** Suppose \( 0 < \epsilon, \delta, \lambda < 1 \) and \( \lambda \neq 1 \). Then we have

\[
k_- + \left[ \frac{k_- F}{\lambda\epsilon} \right] \leq N(\epsilon, \delta, \lambda) \leq k_+ + \left[ \frac{k_+ F}{\lambda\epsilon} \right], \quad (73)
\]

\[
N(\epsilon, \delta, \lambda) \leq \frac{\log_{\lambda\epsilon} \delta - \frac{\nu k_-}{\lambda}}{\lambda} = \left[ \frac{\ln \delta - \frac{\nu k_-}{\lambda}}{\ln \lambda} \right], \quad (74)
\]
All three bounds in Eqs. (73) and (74) are saturated when \( \log_\lambda \delta \) is an integer.

When \( \delta \leq \lambda \leq 1/2 \), we have \( k_- \geq 1 \) and \( \nu k_-/\lambda \geq 1 \), so Eq. (74) implies that

\[
N(\epsilon, \delta, \lambda) < \frac{\ln \delta}{\lambda \epsilon \ln \lambda}.
\]

(75)

On the other hand, by virtue of Eq. (73), we can derive

\[
\lim_{\delta \rightarrow 0} \frac{N(\epsilon, \delta, \lambda)}{\ln \delta^{-1}} = \frac{F + \lambda \epsilon}{\lambda \epsilon \ln \lambda^{-1}},
\]

(76)

\[
k_- \leq \lim_{\epsilon \rightarrow 0} \epsilon N(\epsilon, \delta, \lambda) \leq \frac{k_+}{\lambda},
\]

(77)

\[
\lim_{\epsilon, \delta \rightarrow 0} \frac{\epsilon N(\epsilon, \delta, \lambda)}{\ln \delta^{-1}} = \frac{1}{\lambda \ln \lambda^{-1}}.
\]

(78)

The exact value of \( \lim_{\epsilon \rightarrow 0} \epsilon N(\epsilon, \delta, \lambda) \) can be derived by virtue of Eq. (77), with the result

\[
\lim_{\epsilon \rightarrow 0} \epsilon N(\epsilon, \delta, \lambda) = \lim_{\epsilon \rightarrow 0} \epsilon \tilde{N}(\epsilon, \delta, \lambda) = \frac{k_-}{\lambda} + \frac{\lambda k_- - \delta}{\nu \delta}.
\]

(79)

Note that the inequality \( \delta \geq \lambda k_+/(F + \lambda \epsilon) \) is always satisfied in the limit \( \epsilon \rightarrow 0 \) if \( \log_\lambda \delta \) is not an integer, while \( k_+ = k_- \) and \( \tilde{N}(\epsilon, \delta, \lambda) = \tilde{N}(\epsilon, \delta, \lambda) \) if \( \log_\lambda \delta \) is an integer.

C. Optimal homogeneous strategies

1. Optimal strategies in the high-precision limit \( \epsilon, \delta \rightarrow 0 \)

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 \( \epsilon, \delta \rightarrow 0 \).

According to Eq. (78), in the high-precision limit, the minimum number of tests can be approximated as follows,

\[
N(\epsilon, \delta, \lambda) \approx (\lambda \epsilon)^{-1} \log_\lambda \delta = (\lambda \epsilon \ln \lambda^{-1}) \ln \delta.
\]

(80)

To understand the condition of this approximation, note that \( k_+ \approx \log_\lambda \delta \) 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. (78) is close to 1, so that the two bounds are nearly tight with respect to the relative deviation. In this case, Eq. (80) is a good approximation. Furthermore, numerical calculation shows that Eq. (80) 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. (80) is not so good. Such homogeneous strategies are not efficient when \( \epsilon, \delta \leq 0.1 \) as illustrated in Fig. 1 [see also Eqs. (74) and (73)]; in addition, they are not so important due to the reasons explained in Sec. X later.

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 counterpart in the nonadversarial scenario for high-precision QSV. In the limit \( \epsilon, \delta \rightarrow 0 \), 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 \( \epsilon \) when \( \lambda = 1/e \), with \( \epsilon \) being the base of the natural logarithm. It is strictly decreasing in \( \lambda \) when \( 0 < \lambda \leq 1/e \) and strictly increasing when \( 1/e \leq \lambda < 1 \); cf. Fig. 4. Therefore, the homogeneous strategy with \( \lambda = 1/e \), that is, \( \nu = 1 - (1/e) \), is optimal in the high-precision limit \( \epsilon, \delta \rightarrow 0 \) if there is no restriction on the accessible measurements. In this case we have

\[
N(\epsilon, \delta, \lambda = e^{-1}) \approx \epsilon e^{-1} \ln \delta^{-1}.
\]

(81)

Compared with the counterpart \( \epsilon^{-1} \ln \delta^{-1} \) for the nonadversarial scenario, the overhead is only \( \epsilon \) 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 \( 1/e \) 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 \( \lambda = 1/e \) is usually 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. As a consequence, entangling measurements are less helpful and often unnecessary for constructing the optimal strategies for bipartite and multipartite systems. In the case of bipartite pure states and GHZ states for example, the optimal strategies for high-precision verification can be realized using only local projective measurements \([39, 40, 44, 45, 48]\) (cf. Sec. X).

2. Optimal strategies in the limit \( \delta \rightarrow 0 \)

Here we discuss briefly the scenario in which \( \delta \rightarrow 0 \), but \( \epsilon \) is not necessarily so small, which is relevant to entanglement detection \([44]\). According to Eq. (77), in this case, the performance of the homogeneous strategy \( \Omega \) is characterized by

\[
\mathcal{N}(\epsilon, \lambda) := \lim_{\delta \rightarrow 0} \frac{N(\epsilon, \delta, \lambda)}{\ln \delta^{-1}} = \frac{F + \lambda \epsilon}{\lambda \epsilon \ln \lambda^{-1}},
\]

(82)

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

\[
\frac{\partial \mathcal{N}(\epsilon, \lambda)}{\partial \lambda} = \frac{F + \lambda \epsilon + F \ln \lambda}{\lambda^2 \epsilon (\ln \lambda)^2}.
\]

(83)
For a given $\epsilon$, denote by $\tilde{N}_*(\epsilon)$ the minimum of $\mathcal{N}(\epsilon, \lambda)$ over $\lambda$. This minimum is attained when $\lambda = \lambda_*(\epsilon)$, where $\lambda_*(\epsilon)$ is the unique solution of the equation

$$F + \lambda \epsilon + F \ln \lambda = 0,$$

which amounts to the equality

$$F = \frac{\lambda}{\ln \lambda^{-1} + \lambda - 1}.$$  \hspace{1cm} (85)

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

$$e^{-1} F \leq \lambda_*(\epsilon) \leq e^{-1}.$$  \hspace{1cm} (86)

Next, we study the dependence of the efficiency on the parameter $\lambda$. As a benchmark, we choose the homogeneous strategy with $\lambda = 1/e$ in which case we have $\mathcal{N}(\epsilon, \lambda = 1/e) = (eF + \epsilon)/\epsilon$. Define

$$\tilde{N}(\epsilon, \lambda) := \frac{\mathcal{N}(\epsilon, \lambda)}{\mathcal{N}(\epsilon, e^{-1})} = \frac{F + \lambda \epsilon}{(eF + \epsilon) \lambda \ln \lambda^{-1}},$$

$$\tilde{N}_*(\epsilon) := \frac{\mathcal{N}_*(\epsilon)}{\mathcal{N}(\epsilon, e^{-1})} = \frac{F + \lambda_*(\epsilon) \epsilon}{(eF + \epsilon) \lambda_*(\epsilon) \ln \lambda_*(\epsilon)^{-1}}.$$  \hspace{1cm} (87, 88)

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

$$\frac{1}{\ln \lambda^{-1}} \leq \tilde{N}(\epsilon, \lambda) \leq \frac{1}{e \lambda \ln \lambda^{-1}}.$$  \hspace{1cm} (89)

The lower bound approaches zero in the limit $\lambda \to 0$. Accordingly, a homogeneous strategy $\Omega$ with a small value of $\lambda$ could be significantly more efficient than the benchmark when $\epsilon$ is large. When $\lambda > 1/e$, by contrast, $\tilde{N}(\epsilon, \lambda)$ increases monotonically with $\epsilon$, so we have

$$1 < \frac{1}{e \lambda \ln \lambda^{-1}} \leq \tilde{N}(\epsilon, \lambda) \leq \frac{1}{\ln \lambda^{-1}}.$$  \hspace{1cm} (90)

Such a homogeneous strategy is less efficient than the benchmark.

Finally, by virtue of Eqs. (85) and (88) we can derive the following equality,

$$\tilde{N}_*(\epsilon) := \frac{1}{e \lambda_*(\epsilon) - \ln \lambda_*(\epsilon) - 1}.$$  \hspace{1cm} (91)

Given that $\lambda_*(\epsilon) \leq e^{-1}$ and $\lambda_*(\epsilon)$ decreases monotonically with $\epsilon$, we can deduce that $\tilde{N}_*(\epsilon)$ decreases monotonically with $\epsilon$; it approaches 1 in the limit $\epsilon \to 0$, while it approaches 0 (quite slowly) in the limit $\epsilon \to 1$, as illustrated in Fig. 5. Although $\tilde{N}_*(\epsilon)$ could be arbitrarily small when $\epsilon$ is large, it is close to 1 when $\epsilon$ is not too large. For example, $\tilde{N}_*(\epsilon) \geq 0.965$ when $\epsilon \leq 0.5$ and $\tilde{N}_*(\epsilon) \geq 0.999$ when $\epsilon \leq 0.1$. Therefore, the homogeneous strategy $\Omega$ with $\beta(\Omega) = 1/e$ is nearly optimal for most parameter range of practical interest, as pointed out earlier.

**VII. SINGLE-COPY VERIFICATION**

In this section we analyze the possibility of QSV in the adversarial scenario using a single test. This problem is of intrinsic interest to single-copy entanglement detection \cite{44, 55}. Given a verification strategy $\Omega$, the state $|\Psi\rangle$ can be verified within infidelity $0 < \epsilon < 1$ and significance level $0 < \delta < 1$ using a single test iff

$$F(N = 1, \delta, \Omega) \geq 1 - \epsilon.$$  \hspace{1cm} (92)

Since $F(N, \delta, \Omega) = \zeta(N, \delta, \Omega)/\delta$ according to Eq. (36a), the above equation is equivalent to

$$\zeta(N = 1, \delta, \Omega) \geq \delta(1 - \epsilon).$$  \hspace{1cm} (93)

So our main task here is to determine the expression of $\zeta(N, \delta, \lambda)$ in the case $N = 1$. In the rest of this section we assume $N = 1$ except when stated otherwise. Note that $\zeta(N, \delta = 0, \Omega) = 0$ and that the range of $\delta$ of practical interest usually satisfies $0 < \delta \leq 1/2$.

**A. Single-copy verification with homogeneous strategies**

First, let us consider the homogeneous strategy $\Omega$ defined in Eq. (44).
Proposition 2. Suppose \( N = 1 \) and \( 0 \leq \lambda < 1 \); then
\[
\zeta(N, \delta, \lambda) = \max \left\{ 0, \frac{\lambda(\delta - \lambda)}{1 - \lambda}, \frac{\delta(2 - \lambda - 1)}{1 - \lambda} \right\}
\]
\[
= \begin{cases} 
0, & 0 \leq \delta \leq \lambda, \\
\frac{\lambda(\delta - \lambda)}{1 - \lambda}, & \lambda \leq \delta \leq \frac{1+\lambda}{2} \\
\frac{\delta(2 - \lambda - 1)}{1 - \lambda}, & \frac{1+\lambda}{2} \leq \delta \leq 1.
\end{cases}
\] (94)

Proposition 2 follows from Eq. (50) when \( \lambda = 0 \) and follows from Theorem 1 and Corollary 1 when \( 0 < \lambda < 1 \). As an implication, we can derive
\[
\max_{\lambda} \zeta(N, \delta, \lambda) = \max \{2 - 2\sqrt{1 - \delta - \delta}, 2\delta - 1\}
\]
\[
= \begin{cases} 
2 - 2\sqrt{1 - \delta - \delta}, & 0 \leq \delta \leq \frac{\delta}{9} \\
2\delta - 1, & \frac{\delta}{9} \leq \delta \leq 1.
\end{cases}
\] (95)

Here the maximum is attained at
\[
\lambda = \begin{cases} 
1 - \sqrt{1 - \delta}, & 0 \leq \delta \leq \frac{\delta}{9} \\
0, & \frac{\delta}{9} \leq \delta \leq 1.
\end{cases}
\] (96)

In addition, the optimal solution \( \lambda \) is unique for \( 0 < \delta < 1 \) except when \( \delta = 5/9 \), in which case there are two optimal solutions, namely, \( \lambda = 0 \) and \( \lambda = 1/3 \). This observation implies the following corollary given that the optimal strategy can always be chosen to be homogeneous if there is no restriction on the measurements.

**Corollary 5.** The target state can be verified within infidelity \( 0 < \epsilon < 1 \) and significance level \( 0 < \delta < 1 \) in the adversarial scenario using a single test iff \( \delta \) and \( \epsilon \) satisfy the condition
\[
\delta(1 - \epsilon) \leq \max \{2 - 2\sqrt{1 - \delta - \delta}, 2\delta - 1\},
\] (97)
or, equivalently, the condition
\[
\delta \geq \min \left\{ \frac{4(1 - \epsilon)}{(2 - \epsilon)^2}, \frac{1}{1 + \epsilon} \right\} = \begin{cases} 
\frac{4(1 - \epsilon)}{(2 - \epsilon)^2}, & 0 < \epsilon \leq \frac{4}{5} \\
\frac{1}{1 + \epsilon}, & \frac{4}{5} \leq \epsilon < 1.
\end{cases}
\] (98)

The parameter range of single-copy verification characterized by Corollary 5 is illustrated in Fig. 6 in contrast with the counterpart for the nonadversarial scenario in Eq. (6). Equation (108) determines the smallest significance level that can be achieved by a single test to verify the target state within infidelity \( \epsilon \). Note that the lower bound is monotonically decreasing in \( \epsilon \) for \( 0 < \epsilon < 1 \) as expected. To achieve significance level \( \delta \leq 1/2 \), the infidelity must satisfy the condition \( \epsilon \geq 2(\sqrt{2} - 1) \). When the bound in Eq. (97) or that in Eq. (98) is saturated, the target state can be verified within infidelity \( 0 < \epsilon < 1 \) and significance level \( 0 < \delta < 1 \) by a strategy \( \Omega \) iff \( \Omega \) is homogeneous and \( \beta(\Omega) \) is given by Eq. (86) with \( 0 < \delta < 1 \) or, equivalently,
\[
\beta(\Omega) = \lambda = \begin{cases} 
0, & 0 < \epsilon \leq \frac{4}{5} \\
\frac{2 - 2\epsilon}{2 - \epsilon}, & \frac{4}{5} \leq \epsilon < 1.
\end{cases}
\] (99)

When \( \delta \neq 5/9 \) (that is, \( \epsilon \neq 4/5 \)), the optimal strategy \( \Omega \) is unique as shown Eqs. (105) and (106). When \( \delta = 5/9 \) \( (\epsilon = 4/5) \), by contrast, there are two optimal strategies, both of which are homogeneous, and \( \beta(\Omega) \) can take on two possible values, namely, \( \beta(\Omega) = 0 \) and \( \beta(\Omega) = 1/3 \) (cf. Theorem 3 below).

**Corollary 6.** Given a homogeneous strategy \( \Omega \) with \( \beta(\Omega) = \lambda \), the target state can be verified within infidelity \( 0 < \epsilon < 1 \) and significance level \( 0 < \delta \leq 1/2 \) in the adversarial scenario using a single test iff
\[
\frac{\lambda(\delta - \lambda)}{1 - \lambda} \geq \delta(1 - \epsilon).
\] (100)

This requirement is equivalent to the following conditions,
\[
\delta \geq \frac{4(1 - \epsilon)}{(2 - \epsilon)^2}, \quad \lambda_- \leq \lambda \leq \lambda_+,
\] (101) (102)

where
\[
\lambda_\pm := \frac{(2 - \epsilon)\delta \pm \sqrt{(2 - \epsilon)^2\delta^2 - 4(1 - \epsilon)\delta}}{2}.
\] (103)

Equation (100) implies that \( 0 < \lambda < \delta \). So any homogeneous strategy \( \Omega \) with \( \beta(\Omega) = 0 \) or \( \beta(\Omega) \geq 1/2 \) cannot verify the target state within infidelity \( 0 < \epsilon < 1 \) and significance level \( 0 < \delta \leq 1/2 \) using a single test. This conclusion actually applies to an arbitrary strategy, not necessarily homogeneous; see Corollary 7 below. Thanks to the inequality \( 4(1 - \epsilon)\delta > 4(1 - \epsilon)\delta^2 \), \( \lambda_\pm \) defined in Eq. (103) satisfy the following equation,
\[
(1 - \epsilon)\delta < \lambda_- \leq \lambda_+ < \delta.
\] (104)
By computing the derivatives over \( \delta \) and \( \epsilon \), it is easy to verify that \( \lambda_+ (\lambda_-) \) increases (decreases) monotonically with \( \delta \) and \( \epsilon \) as expected. If \( \delta \leq 1/2 \), then we have
\[
\frac{2 - \epsilon - \sqrt{\epsilon^2 + 4\epsilon - 4}}{4} \leq \lambda_- \leq \lambda_+ \leq \frac{2 - \epsilon + \sqrt{\epsilon^2 + 4\epsilon - 4}}{4}.
\] (105)

### B. Single-copy verification with general strategies

Next, we generalize Proposition 4 to an arbitrary verification operator \( \Omega \). The following theorem shows that the efficiency of \( \Omega \) is determined by \( \beta \) and \( \tau \), where \( \beta \) and \( \tau \) denote the second largest and smallest eigenvalues of \( \Omega \), respectively. See Appendix D for a proof.

**Theorem 4.** Suppose \( N = 1 \). If \( \beta \geq 1/2 \), then
\[
\zeta(N, \delta, \Omega) = \begin{cases} 
0, & 0 \leq \delta \leq \beta, \\
\frac{\beta(\delta - \beta)}{1 - \beta}, & \beta \leq \delta \leq 1 + \beta, \\
\frac{\delta(2 - \beta)}{1 - \beta}, & 1 - \frac{\beta}{2} \leq \delta \leq 1.
\end{cases}
\] (106)

If \( \beta < 1/2 \), then
\[
\zeta(N, \delta, \Omega) = \begin{cases} 
0, & 0 \leq \delta \leq \beta, \\
\frac{\tau(\delta - \beta)}{1 + \tau - 2\beta}, & \beta \leq \delta \leq 1 + \tau, \\
\delta - \frac{1}{2}, & \frac{1}{2} - \frac{\beta}{2} \leq \delta \leq \frac{1}{2} + \beta, \\
\frac{\delta(2 - \beta)}{1 - \beta}, & 1 - \frac{\beta}{2} \leq \delta \leq 1.
\end{cases}
\] (107)

**Corollary 7.** The target state can be verified by the strategy \( \Omega \) within infidelity \( 0 < \epsilon < 1 \) and significance level \( 0 < \delta \leq 1/2 \) using a single test iff
\[
0 < \beta < \delta, \quad \frac{\tau(\delta - \beta)}{1 + \tau - 2\beta} \geq \delta(1 - \epsilon).
\] (108)

Note that the target state cannot be verified within infidelity \( 0 < \epsilon < 1 \) and significance level \( 0 < \delta \leq 1/2 \) using a single test if \( \beta = 0 \) or \( \beta \geq 1/2 \). When \( 0 < \beta < 1/2 \) and \( \delta \leq (1 + \tau) / 2 \), we have
\[
\frac{\tau(\delta - \beta)}{1 + \tau - 2\beta} \leq \min \left\{ \frac{\beta(\delta - \beta)}{1 - \beta}, \frac{\tau(\delta - \beta)}{1 - \tau} \right\}.
\] (109)

So Eq. (108) implies Eq. (109) with \( \lambda = \beta \) or \( \lambda = \tau \), which in turn implies Eq. (101) and the sequence of inequalities \( \lambda_- \leq \tau \leq \beta \leq \lambda_+ \), where \( \lambda_k \) are defined in Eq. (103). This conclusion is expected given that \( \zeta(N, \delta, \Omega) \leq \zeta(N, \delta, \beta) \) and \( \zeta(N, \delta, \Omega) \leq \zeta(N, \delta, \tau) \).

### VIII. EFFICIENCIES OF GENERAL VERIFICATION STRATEGIES

In this section we present our main results on the efficiencies of general verification strategies. 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 \( \tau \).

#### A. Singular verification strategies

The efficiency of a singular verification strategy is characterized by Lemma 8 and Theorem 5 below, which are proved in Appendix D. Note that Eqs. (112) and (113) in Theorem 5 actually apply to all verification strategies, although these bounds could be quite loose for nonsingular strategies. Define
\[
\delta^* := \frac{1 + N\beta}{N + 1} = \frac{1 + N(1 - \nu)}{N + 1}.
\] (110)

**Lemma 8.** Suppose \( \Omega \) is a singular verification operator and \( 1/(N + 1) \leq \delta \leq \delta^* \). Then
\[
F(N, \delta, \Omega) \leq 1 - \frac{1}{(N + 1)\delta}.
\] (111)

**Theorem 5.** Suppose \( 0 < \delta \leq 1 \) and \( 0 < \nu \leq 1 \). Then
\[
F(N, \delta, \Omega) \geq 1 - \frac{1 - \delta}{N\nu\delta}.
\] (112)

and the inequality is saturated when \( \delta^* \leq \delta \leq 1 \). If in addition \( \nu \geq 1/2 \), then
\[
F(N, \delta, \Omega) \geq 1 - \frac{\nu\delta}{N(1 + 1)\delta},
\] (113)

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

The bound in Eq. (112) is positive and thus nontrivial if \( \delta > 1/(N\nu + 1) \), while the one in Eq. (113) is positive if \( \delta > 1/(N + 1) \). The first bound is saturated and thus optimal when \( \delta \geq \delta^* \), while the second bound is better when \( \delta < \delta^* \). The two bounds coincide when \( \delta = \delta^* \). The bound in Eq. (113) under the condition \( \nu \geq 1/2 \) was also given in Ref. 15 under a slightly different situation. According to Lemma 8 and Theorem 5, if \( \Omega \) is singular, then
\[
F(N, \delta, \Omega) \leq \max \left\{ 0, 1 - \frac{1 - \delta}{N\nu\delta}, 1 - \frac{1}{(N + 1)\delta} \right\}.
\] (114)

If \( \nu \geq 1/2 \), by contrast, then the above inequality is reversed,
\[
F(N, \delta, \Omega) \geq \max \left\{ 0, 1 - \frac{1 - \delta}{N\nu\delta}, 1 - \frac{1}{(N + 1)\delta} \right\}.
\] (115)

If \( \Omega \) is singular and meanwhile \( \nu \geq 1/2 \), then the inequalities in Eqs. (114) and (115) are saturated.

**Corollary 8.** Suppose \( 0 < \epsilon, \delta < 1 \) and \( 0 < \nu \leq 1 \). Then
\[
N(\epsilon, \delta, \Omega) \leq \max \left\{ \frac{1 - \delta}{\nu\delta\epsilon}, \frac{1}{\delta\epsilon} - 1 \right\}.
\] (116)

If \( \Omega \) is singular, then
\[
N(\epsilon, \delta, \Omega) \geq \min \left\{ \frac{1 - \delta}{\nu\delta\epsilon}, \frac{1}{\delta\epsilon} - 1 \right\}.
\] (117)
If $\nu \geq 1/2$, then

$$N(\epsilon, \delta, \Omega) \leq \min \left\{ \left[ \frac{1 - \delta}{\nu \delta \epsilon} \right], \left[ \frac{1}{\nu \epsilon} - 1 \right] \right\}.$$  \hfill (118)

Corollary 8 is an easy consequence of Theorem 5 and Eqs. (114), (115). If $\Omega$ is singular and $\nu \geq 1/2$, then the inequalities in Eqs. (117) and (118) are saturated, so we have

$$N(\epsilon, \delta, \Omega) = \min \left\{ \left[ \frac{1 - \delta}{\nu \delta \epsilon} \right], \left[ \frac{1}{\nu \epsilon} - 1 \right] \right\},$$  \hfill (119)

which generalizes Eq. (111). The number of tests characterized by the upper bound in Eq. (119) is much smaller than what can be achieved by previous approaches that are based on the quantum de Finetti theorem [18, 42]. Nevertheless, the scaling with $1/\delta$ is still not satisfactory compared with the counterpart for the nonadversarial scenario.

### B. Nonsingular verification strategies

Next, we provide an even better bound on the number of tests when $\Omega$ is nonsingular. Lemma 9 and Theorem 6 below are proved in Appendix F.

**Lemma 9.** Suppose $0 < \delta, f \leq 1$ and $\Omega$ is a positive-definite verification operator with $0 < \tau < \beta < 1$. Then

$$F(N, \delta, \Omega) \geq \frac{N + 1 - (\ln \beta)^{-1} \ln(\tau \delta)}{N + 1 - (\ln \beta)^{-1} \ln(\tau \delta) - h \ln(\tau \delta)},$$ \hfill (120)

$$\mathcal{F}(N, f, \Omega) \geq \frac{N + 1 - (\ln \beta)^{-1} \ln f}{N + 1 - (\ln \beta)^{-1} \ln f - h \ln f}.$$ \hfill (121)

where

$$h = h(\Omega) := \max_{j \geq 2} (\lambda_j \ln \lambda_j^{-1})^{-1} = \left[ \min \{\beta \ln \beta^{-1}, \tau \ln \tau^{-1}\} \right]^{-1}.$$ \hfill (122)

Define

$$\tilde{\beta} := \begin{cases} \beta, & \beta \ln \beta^{-1} \leq \tau \ln \tau^{-1}, \\ \tau, & \beta \ln \beta^{-1} > \tau \ln \tau^{-1}. \end{cases}$$ \hfill (123)

Then we have $h = (\tilde{\beta} \ln \tilde{\beta}^{-1})^{-1}$. Note that $h > 1/|\ln \tilde{\beta}|$ and $-h \ln(\tau \delta) > (\ln \beta)^{-1} \ln(\tau \delta)$, so the denominator in Eq. (120) is positive, and so is the denominator in Eq. (121). In addition, the lower bounds in Eqs. (120) and (121) increase monotonically with $N$, which is expected in view of Lemma 9.

By virtue of Lemma 9 we can derive upper bounds for $N(\epsilon, \delta, \Omega)$ which are tight in the high-precision limit. Meanwhile, we can derive lower bounds for $N(\epsilon, \delta, \Omega)$ based on the fact that $N(\epsilon, \delta, \Omega) \geq N(\epsilon, \delta, \lambda_j)$ for $j = 2, 3, \ldots, D$, where $\lambda_j$ are the eigenvalues of $\Omega$ arranged in decreasing order $1 = \lambda_1 > \lambda_2 \geq \lambda_3 \geq \cdots \geq \lambda_D > 0$. The main results are summarized in the following theorem.

**Theorem 6.** Suppose $0 < \epsilon, \delta < 1$ and $\Omega$ is a positive-definite verification operator with $0 < \tau < \beta < 1$. Then

$$N(\epsilon, \delta, \Omega) \geq N(\epsilon, \delta, \lambda_j) \geq k_-(\lambda_j) + \frac{2^{k_-(\lambda_j) - 1}}{\lambda_j}, \quad j = 2, 3, \ldots, D,$$ \hfill (124)

$$k_-(\tilde{\beta}) + \left[ \frac{k_-(\tilde{\beta}) F}{\beta \epsilon} \right] \leq N(\epsilon, \delta, \Omega) \leq \left[ \frac{h F \ln(\tau \delta)^{-1}}{\epsilon} + \ln(\tau \delta) \right] + \frac{\ln(\tau \delta)}{\ln \beta} - 1 < \frac{h \ln(\tau \delta)^{-1}}{\epsilon},$$ \hfill (125)

$$N(\epsilon, \delta, \Omega) \leq \left[ \frac{h F \ln(\tau \delta)^{-1}}{\epsilon} + \frac{\ln(\tau \delta) \ln \beta}{\ln \beta} - 1 \right] < \frac{h \ln(\tau \delta)^{-1}}{\epsilon}.$$ \hfill (126)

The upper bounds in Eq. (125) are worse than those in Eq. (120) if $F < \tau = \tau(\Omega)$, while they are better if $F > \tau$, which is usually the case for high-precision verification. Suppose $\tau$ is bounded from below by a positive constant. Then the ratio of the lower bound over the upper bound in Eq. (125) approaches 1 in the high-precision limit $\epsilon, \delta \to 0$, so the two bounds are nearly tight, as in the case of homogeneous strategies. As a consequence, we have

$$\lim_{\epsilon, \delta \to 0} \frac{\epsilon N(\epsilon, \delta, \Omega)}{\ln \delta^{-1}} = h = \frac{1}{\beta \ln \beta^{-1}}.$$ \hfill (127)

When $\epsilon, \delta \ll 1$, accordingly, $N(\epsilon, \delta, \Omega)$ can be approximated as follows.

$$N(\epsilon, \delta, \Omega) \approx \frac{h \ln \delta^{-1}}{\epsilon} = \frac{\ln \delta}{\epsilon \beta \ln \beta}.$$ \hfill (128)
The number of tests has the same scaling behaviors with $\epsilon^{-1}$ and $\delta^{-1}$ as the counterpart for the nonadversarial scenario presented in Eqs. (2) and (12), except for an overhead characterized by $\nu h$. However, $\Omega$ is not efficient when $\tau$ is too small according to Eq. (123), as well as Eqs. (111) and (112). In addition, the scaling behavior with $\delta^{-1}$ would be worse if $\Omega$ were singular according to Eq. (113).

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 $E_1 P = P$, and redefine $f_\rho$ as $\text{tr}[(\Omega \otimes N \otimes P)\rho]$. Such an extension is useful when we want to verify whether the resultant state is correctable in a fault-tolerant way [14].

**IX. GENERAL RECIPE TO VERIFYING PURE STATES IN THE ADVERSARIAL SCENARIO**

According to Sec. [8] and [111], 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 counterpart 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. To address this problem, 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 nearly 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 operator $E$ is equal to the identity operator, that is $E = 1$, so that all the states can pass the test with certainty.

**A. The recipe**

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

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

(129)

which means the trivial test is performed with probability $p$ and $\Omega$ is performed with probability $1 - p$. Denote by $\beta_p$ and $\tau_p$, the second largest eigenvalue and smallest eigenvalue of $\Omega_p$, respectively. Then

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

(130)

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

$$\nu_p = 1 - \beta_p = (1 - p)\nu.$$

(131)

According to Secs. [11] and [111] the trivial test can only decrease the efficiency in the nonadversarial scenario. In high-precision verification for example, the number of tests required by $\Omega_p$ is about $1/(1 - p)$ times the number required by $\Omega$ according to Eqs. (2) and (12). In sharp contrast, the trivial test can increase the efficiency in the adversarial scenario by hedging the influence of small eigenvalues of $\Omega$. Therefore, $\Omega_p$ is called a *hedged verification operator* of $\Omega$.

Thanks to Eq. (125), to verify the target state $|\Psi\rangle$ within infidelity $\epsilon$ and significance level $\delta$ in the adversarial scenario, the number of tests required by the strategy $\Omega_p$ (assuming $\tau_p > 0$) is upper bounded as follows,

$$N(\epsilon, \delta, \Omega_p) < \frac{h(p, \nu, \tau)}{\epsilon} \ln(\frac{F_{\delta}}{\epsilon}),$$

(132)

where $F = 1 - \epsilon$ and

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

(133)

In comparison with the number in Eq. (2) or (12) for the nonadversarial scenario, the overhead satisfies

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

(134)

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 [11] and [114] below. When $\epsilon$ and $\delta$ approach zero, the bound in Eq. (134) becomes tight (with respect to the relative deviation) according to Eqs. (125) and (127), so we have

$$\lim_{\epsilon, \delta \to 0} \frac{N(\epsilon, \delta, \Omega_p)}{N_{\text{NA}}(\epsilon, \delta, \Omega)} = \nu h(p, \nu, \tau).$$

(135)

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

To construct an efficient hedged verification strategy, 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 $x \ln x$ is concave in the interval $0 \leq x \leq 1$ and is strictly increasing in $x$ when $0 \leq x \leq 1/e$, while it is strictly decreasing when $1/e \leq x \leq 1$; it attains the maximum $1/e$ when $x = 1/e$. Given the value of $\nu = 1 - \beta$ and $\tau$ with $\nu + \tau \leq 1$, the minimum of $h(p, \nu, \tau)$ over $p$ is denoted by $h_*(\nu, \tau)$; the unique minimizer in $p$ is denoted by $p_*(\nu, \tau)$ or $p_*$ for simplicity; cf. Fig. [7]. By definition we have

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

(136)
In addition, it is straightforward to verify that

\[ p_\ast = \min \{ p \geq 0 \mid \beta_p \geq e^{-1} \& \tau_p \ln \tau_p^{-1} \geq \beta_p \ln \beta_p^{-1} \}. \]  

(137)

Here the condition \( \beta_p \geq e^{-1} \) is required when \( \tau = \beta \) (so that \( \Omega \) is a homogeneous strategy), but is redundant when \( \tau < \beta \). Equation (137) implies that \( \beta_p \geq 1/e \); by contrast, \( \tau_p \leq 1/e \) if \( \tau \leq 1/e \).

When the strategy \( \Omega \) is homogeneous, that is, when \( \tau = \beta = 1 - \nu \), we have

\[
p_\ast(\nu, 1 - \nu) = \left\{ \begin{array}{ll} 0 & 0 < \nu \leq 1 - \frac{1}{e}, \\ \frac{1}{e} & 1 - \frac{1}{e} \leq \nu \leq 1; \end{array} \right. 
\]  

(138)

\[
h_\ast(\nu, 1 - \nu) = \left\{ \begin{array}{ll} (\beta \ln \beta^{-1})^{-1} & 0 < \nu \leq 1 - \frac{1}{e}, \\ \frac{1}{e} & 1 - \frac{1}{e} \leq \nu \leq 1. \end{array} \right. 
\]  

(139)

In this case \( \Omega_p \) is also homogeneous, so the results presented in Sec. VI can be applied directly. In general, it is not easy to derive an analytical formula for \( p_\ast \), but it is very easy to determine \( p_\ast \) numerically.

B. Properties of hedged verification strategies

To determine the overhead of QSV in the adversarial scenario, we need to clarify the properties of \( h(p, \nu, \tau) \), \( h_\ast(\nu, \tau) \), and \( p_\ast(\nu, \tau) \), which determine the performances of the hedged verification strategies \( \Omega_p \) and \( \Omega_p^\ast \). By virtue of the properties of the function \( x \ln x^{-1} \) we can derive a tight lower bound for \( h(p, \nu, \tau) \), namely,

\[ h(p, \nu, \tau) \geq \frac{1}{e}, \]  

(140)

and the bound is saturated iff \( \tau_p = \beta_p = 1/e \), that is, \( \tau = 1 - \nu \leq 1/e \) and \( p = (e\nu - e + 1)/(e\nu) \); cf. Eqs. (138) and (139).

Lemma 10. Suppose \( 0 < \nu \leq 1 \). Then \( p_\ast(\nu, 1 - \nu) \) is nondecreasing in \( \nu \), \( h_\ast(\nu, 1 - \nu) \) is nonincreasing in \( \nu \), and \( v h_\ast(\nu, 1 - \nu) \) is strictly increasing in \( \nu \). Meanwhile, \( v h_\ast(\nu, 1 - \nu) > 1 \) and \( \lim_{\nu \to 0} v h_\ast(\nu, 1 - \nu) = 1 \). If in addition \( 0 \leq p < 1 \) and \( \beta_p = 1 - \nu + p \nu > 0 \), then \( v h(p, \nu, 1 - \nu) \) is strictly increasing in \( \nu \).

Lemma 11. Suppose \( \nu \) and \( \tau \) satisfy the following conditions \( 0 < \nu \leq 1 \), \( 0 \leq \tau < 1 \), and \( \nu + \tau \leq 1 \). Then

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

If in addition \( 0 \leq p < 1 \) and \( \tau_p = (1 - \nu)p + p \nu > 0 \), then

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

Lemmas 10 and 11 are proved in Appendix C. Lemma 10 is tailored to the scenario in which \( \Omega \) is homogeneous. In Lemma 11 we assume that \( \nu \) and \( \tau \) can vary independently, which means the Hilbert space \( \mathcal{H} \) on which \( \Omega \) acts has dimension at least 3. If \( \mathcal{H} \) has dimension 2, then \( \Omega_p \) is always homogeneous and \( \tau = 1 - \nu \), so Lemma 11 is redundant given Lemma 10. Lemmas 10 and 11 summarize the main properties of \( p_\ast(\nu, \tau) \), \( h(p, \nu, \tau) \), and \( h_\ast(\nu, \tau) \) as illustrated in Fig. 7, which are very instructive to understanding QSV in the adversarial scenario. In particular Lemma 11 reveals that the overhead \( v h_\ast(\nu, \tau) \) in the number of tests becomes negligible when \( \nu \) approaches 0. To be concrete, calculation shows that \( v h_\ast(\nu, \tau) \leq 1.09, 1.19, 1.31, 1.45, 1.61 \) when \( \nu \leq 0.1, 0.2, 0.3, 0.4, 0.5 \), respectively.

When \( p_\ast(\nu, \tau) \leq p \leq p_\ast(\nu) := p_\ast(\nu, 0) \), Lemma 11 implies that

\[ h_\ast(\nu, 1 - \nu) \leq h_\ast(\nu, \tau) \leq h(p, \nu, \tau) \leq h(p_\ast(\nu, \nu, \tau)) = h_\ast(\nu), \]  

(141)

where \( h_\ast(\nu) := h_\ast(\nu, 0) \). Note that \( h(p, \nu, \tau) \) increases monotonically with \( p \) when \( p \geq p_\ast(\nu, \tau) \). Lemma 11 and Eq. (138) together yield a lower bound and an upper bound for \( p_\ast(\nu, \tau) \),

\[ p_\ast(\nu, 1 - \nu) \leq p_\ast(\nu, \tau) \leq p_\ast(1 - \tau, \tau) \leq 1/e. \]  

(142)
FIG. 8. (color online) The optimal probability \( p_\star(\nu) \) for performing the trivial test in high-precision QSV and a pretty-good approximation \( p_0(\nu) = \nu/e \) (upper plot). Variations of \( \nu h_\star(\nu) \) and its upper bound \( \nu h(p_0(\nu), \nu) \) with \( \nu \) (lower plot). The black solid curve in the lower plot represents the first upper bound for \( \nu h(p_0(\nu), \nu) \) presented in Eq. (148).

Here the third inequality is saturated iff \( \tau = 0 \); in that case, the second inequality is saturated iff \( \nu = 1 \) (cf. Lemma 12 below). Therefore, \( p_\star(\nu, \tau) \) can attain the upper bound \( 1/e \) iff \( \nu = 1 \) and \( \tau = 0 \), in which case the verification operator is homogeneous and singular. As a corollary, we have \( 1/\left[1 - p_\star(\nu, \tau)\right] \leq e/(e - 1) < 1.6 \), so the number of tests required by \( \Omega_{p_\star} \) 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 11 and Eq. (159) yield a lower bound for \( h_\star(\nu, \tau) \),

\[
h_\star(\nu, \tau) \geq \left\{ \begin{array}{ll}
(\beta \ln \beta^{-1})^{-1}, & 0 < \nu \leq 1 - \frac{1}{e}, \\
1 - \frac{1}{e} & \frac{1}{e} \leq \nu \leq 1,
\end{array} \right.
\]

where \( \beta = 1 - \nu \).

When \( 0 < \tau < \beta \) and \( \tau \ln \tau^{-1} \geq \beta \ln \beta^{-1} \), Eq. (137) implies that

\[
p_\star(\nu, \tau) = 0, \quad h_\star(\nu, \tau) = (\beta \ln \beta^{-1})^{-1}.
\]

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

\[
\beta_p \ln \beta_p = \tau_p \ln \tau_p, \quad 0 < p < 1.
\]

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.

In view of Lemma 11, a singular verification operator \( \Omega \) with \( \tau = 0 \) is of special interest because the overhead \( \nu h_\star(\nu, \tau) \) for a given \( \nu \) is maximized when \( \tau = 0 \). In this case, \( \tau_p = p \) and the optimal probability in Eq. (137) reduces to

\[
p_\star = \min \{ p > 0 | \beta_p \geq e^{-1} \ \& \ p \ln p = \beta_p \ln \beta_p \}.
\]

The requirement \( \beta_p \geq e^{-1} \) is redundant when \( \beta > 0 \), in which case \( p_\star \) is also the unique solution of the equation \( p \ln p = \beta_p \ln \beta_p \) for \( 0 < p < 1 \). In general, we have \( h_\star(\nu) = (p_\star \ln p_\star^{-1})^{-1} \). Furthermore, \( p_\star(\nu) = p_\star(\nu, 0) \) can be approximated by

\[
p_0 = p_0(\nu) = \frac{\nu}{e} = \frac{1 - \beta}{e},
\]

which is exact when \( \nu = 1 \), as illustrated in Fig. 8. Let \( h(p, \nu) := h(p, \nu, 0) \); then \( h(p_0(\nu), \nu) = h(e^{-1}\nu, \nu) = h(e^{-1}\nu, \nu, 0) \).

**Lemma 12.** Suppose \( 0 < \nu \leq 1 \). Then \( p_\star(\nu), \nu h_\star(\nu) \), and \( \nu h(e^{-1}\nu, \nu) \) are strictly increasing in \( \nu \), while \( h_\star(\nu) \) and \( \nu h(e^{-1}\nu, \nu) \) are strictly decreasing in \( \nu \). In addition,

\[
\nu h_\star(\nu) \leq \nu h(e^{-1}\nu, \nu) \leq (1 - \nu + e^{-1}\nu^2)^{-1} \\
\leq 1 + (e - 1)\nu \leq e.
\]

**Lemma 12** is proved in Appendix C. Calculation shows that the difference between \( \nu h(e^{-1}\nu, \nu) \) and \( \nu h_\star(\nu) \) is less than 2% (cf. Fig. 8); therefore, \( p_0 = \nu/e \) is indeed a good approximation of \( p_\star(\nu) \). When \( p_\star(\nu, \tau) \leq p \leq p_\star(\nu) \), Lemma 12 and Eq. (141) imply that

\[
\nu h_\star(\nu, \tau) \leq \nu h(p, \nu, \tau) \leq \nu h_\star(\nu) \leq \nu h(e^{-1}\nu, \nu) \leq (1 - \nu + e^{-1}\nu^2)^{-1} \leq 1 + e\nu - \nu \leq e.
\]

In addition, we have \( h(e^{-1}\nu, \nu, \tau) \leq h(e^{-1}\nu, \nu) \) according to Lemma 11. So Lemma 12 has implications for all verification operators, not necessarily singular.

### C. Overhead of QSV in the adversarial scenario

The overhead of QSV in the adversarial scenario compared with the nonadversarial scenario is of fundamental interest. The following theorem is a key to clarifying this issue. It follows from Lemma 11 as well as Eqs. (132) and (149).
Theorem 7. Suppose $\Omega$ is a verification operator for $|\Psi\rangle$, $\nu = \nu(\Omega)$, and $\tau = \tau(\Omega)$. If $p = \nu/e$, then
\[
N(\epsilon, \delta, \Omega_p) < \frac{h(e^{-1}\nu, \nu, \tau) \ln(F\delta)^{-1}}{\epsilon} \leq \frac{h(e^{-1}\nu, \nu) \ln(F\delta)^{-1}}{\epsilon} \leq \frac{\ln(F\delta)^{-1}}{(1 - \nu + e^{-1}\nu^2)\nu\epsilon} \leq \frac{(1 + \nu - \nu)\ln(F\delta)^{-1}}{\nu\epsilon},
\]
where $F = 1 - \epsilon$. If $p_\ast(\nu, \tau) \leq p \leq p_\ast(\nu)$, then
\[
N(\epsilon, \delta, \Omega_p) < \frac{h(p, \nu, \tau) \ln(F\delta)^{-1}}{\epsilon} \leq \frac{h_\ast(\nu) \ln(F\delta)^{-1}}{\epsilon} \leq \frac{h(e^{-1}\nu, \nu) \ln(F\delta)^{-1}}{\epsilon} \leq \frac{\ln(F\delta)^{-1}}{(1 - \nu + e^{-1}\nu^2)\nu\epsilon}.
\]
In conjunction with Eq. [12] [see also Eqs. [135] and [149]], Theorem 7 sets a general upper bound on the overhead of QSV in the adversarial scenario. If $p = \nu/e$ or $p_\ast(\nu, \tau) \leq p \leq p_\ast(\nu)$ for example, then
\[
\frac{N(\epsilon, \delta, \Omega_p)}{N_{\text{NA}}(\epsilon, \delta, \Omega)} < \nu h(e^{-1}\nu, \nu) \ln(1 - \nu\epsilon)^{-1} \ln(F\delta)^{-1} \leq \frac{\ln(1 - \nu\epsilon)^{-1} \ln(F\delta)}{(1 - \nu + e^{-1}\nu^2)\nu\epsilon \ln \delta} \leq \frac{(1 + \nu - \nu)\ln(1 - \nu\epsilon)^{-1} \ln(F\delta)}{\nu\epsilon \ln \delta}.
\]
\[\text{FIG. 9. (color online) Upper bound on the ratio of } N(\epsilon, \delta, \Omega_p) \text{ over } N_{\text{NA}}(\epsilon, \delta, \Omega) \text{ according to the first bound in Eq. [152] with } \delta = \epsilon, \text{ where } p = \nu/e \text{ or } p_\ast(\nu, \tau) \leq p \leq p_\ast(\nu). \text{ This ratio characterizes the overhead of QSV in the adversarial scenario.}\]

By virtue of Lemmas [11] and [11], it is easy to verify that all three bounds in Eq. [152] decrease monotonically with $1/\epsilon$, $1/\delta$, and $1/\nu$, as illustrated in Figs. [13] and [14]. Theorem 5 has profound implications for QSV in the adversarial scenario. With the help of the trivial test, the number of required tests can achieve the same scaling behaviors with $\epsilon^{-1}$ and $\delta^{-1}$ as the counterpart for the nonadversarial scenario presented in Eq. [13] and Eq. [14]. The overhead is at most four times when $\epsilon, \delta \leq 1/4$ and $\nu, \epsilon, \delta \leq 1/10$; furthermore, the overhead becomes negligible when $\nu, \epsilon, \delta$ approach zero. It should be emphasized that our recipe for addressing the adversarial scenario is independent of the specific construction of the verification protocol once the verification operator is fixed. This fact means that our general results can be applied in various contexts with different constraints on measurements. Moreover, the protocol for the adversarial scenario requires the same measurement settings (except for the trivial test) as employed for the nonadversarial scenario, which is the best we can hope for. Therefore, pure states can be verified in the adversarial scenario with nearly the same efficiency as in the nonadversarial scenario with respect to not only the total number of tests, but also the number of measurement settings.

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 11, the difference between $h_\ast(\nu, \tau_1)$ and $h_\ast(\nu, \tau_2)$ for a given $\nu$ is maximized when $\tau_1 = 0$ [in which case $h_\ast(\nu, \tau_1) = h_\ast(\nu)$, cf. Eq. [148]] and $\tau_2 = 1 - \nu$ [cf. Eq. [149]]. Calculation shows that the difference between $h_\ast(\nu)$ and $h_\ast(\nu, 1 - \nu)$ is less than 12%, and it is even smaller when $\nu$ is close to zero or close to 1, as illustrated in Fig. 7. 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, both the choices $p = p_\ast(\nu)$ and $p = p_0(\nu) = \nu/e$ are nearly optimal. These observations are very helpful to constructing efficient verification protocols for the adversarial scenario 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 $p_\ast(\nu, \tau)$, $p_\ast(\nu)$, or $p_0(\nu) = \nu/e$. Without this insight, it would be much more difficult to devise efficient verification protocols.

X. APPLICATIONS

Our recipe presented in Sec. 1X can be applied to verifying any pure state in the adversarial scenario as long as we can construct a verification strategy for the nonadversarial scenario. In this section we discuss the applications of this recipe to verifying many important quantum states, some of which have already been published or appeared on arXiv [41, 42, 44, 45, 46]. The main results are summarized in Table 1. All verification strategies considered here are based on (adaptive) local projective measurements together with classical communication, which
are most convenient for practical applications, although our general recipe for the adversarial scenario is independent of how the verification strategy is constructed. The results presented here are also very useful to verifying quantum gates [56, 57].

A. Minimum measurement settings for verifying multipartite pure states

Before considering specific quantum states, it is instructive to clarify the limitation of local measurements in general. As a first step towards this goal, we determine the minimum 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 a tensor product of two pure states [2]. The following proposition sets a fundamental lower bound for the number of measurement settings required by each party; see Appendix H for a proof.

Proposition 3. To verify a multipartite pure state with adaptive local projective measurements, each party needs at least two measurement settings, unless the party is not entangled with other parties.

Here we do not assume that the test operators are projectors. In general many different test operators can be constructed from a given measurement setting using different data-processing methods. If a party is not entangled with other parties, then its reduced state is a pure state and the party needs to perform only one projective measurement with the pure state as a basis state.

As an implication of Proposition 3, each party needs at least two measurement settings when the state is GME. It turns out two measurement settings for each party are also sufficient for verifying many important quantum states, such as bipartite maximally entangled states [44], hypergraph states [43], and Dicke states [51]. Nevertheless, more measurement settings can often improve the efficiency with respect to the total number of tests.

B. Maximally entangled states and GHZ states

First, consider bipartite maximally entangled states in dimension $d \times d$, which have the form

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle$$

up to some local unitary transformations. According to Refs. [23, 44], the maximum spectral gap of any verification strategy $\Omega$ based on LOCC or separable measurements is

$$\nu(\Omega) = \frac{d}{d+1}.$$  \hspace{1cm} (154)

Thanks to Eq. (12), the minimum number of tests required to verify $|\Phi\rangle$ within infidelity $\epsilon$ and significance level $\delta$ in the nonadversarial scenario reads

$$N_{\text{NA}} = \left\lceil \frac{\ln \delta}{\ln [1 - d(d+1)^{-1} \epsilon]} \right\rceil \leq \left\lceil \frac{d+1}{d} \ln \delta^{-1} \right\rceil. \hspace{1cm} (155)$$

Here the upper bound is nearly tight when $\epsilon$ is small, so we will neglect such small difference in favor of a simpler expression in the following discussions. In addition, the verification operator $\Omega$ is necessarily homogeneous when $\nu(\Omega)$ attains the upper bound $d/(d+1)$. So the strategy can be employed for fidelity estimation by Eq. (8). According to Eq. (9), the standard deviation of this estimation reads

$$\Delta F = \frac{\sqrt{\rho(1-p)}}{\nu(\Omega) \sqrt{N}} = \frac{(1-F)(F+d-1)}{\sqrt{N}}, \hspace{1cm} (156)$$

where $p = \text{tr}(\sigma \sigma)$ with $\sigma = \nu(\Omega) F + \beta(\Omega)$.

By adding the trivial test with a suitable probability, any homogeneous strategy $\Omega$ with $\nu(\Omega) \leq d/(d+1)$ (that is, $\beta(\Omega) \geq 1/(d+1)$) can be constructed using LOCC. In particular, we can construct a homogeneous strategy $\Omega$ with $\beta(\Omega) = 1/e$, which is optimal for high-precision verification in the adversarial scenario according to Sec. VI.

Then the number of required tests satisfies

$$N \leq \left\lceil \frac{e \epsilon^{-1} \ln \delta^{-1}}{2} \right\rceil \hspace{1cm} (157)$$

by Theorem 3. When $\delta \leq 1/e$, the above bound can be strengthened by Eq. (58), which yields $N < e \epsilon^{-1} \ln \delta^{-1}$. This bound is nearly tight in the high-precision limit.

Equations (154)–(157) above also apply to the $n$-qudit GHZ state for $n \geq 3$ as shown in Ref. 48.

C. Bipartite pure states

Next, consider a general bipartite pure state of the form $|\Psi\rangle = \sum_{j=0}^{d-1} s_j |jj\rangle$, where the Schmidt coefficients $s_j$ are arranged in decreasing order and satisfy the condition $\sum_{j=0}^{d-1} s_j^2 = 1$. When $d = 2$, by virtue of adaptive measurements with two-way communication, one can construct a verification operator $\Omega$ with spectral gap $(1 + s_0 s_1)^{-1}$, which attains the maximum over separable measurements [40]. For a general bipartite pure state, the spectral gap achievable so far is [43, 47]

$$\nu(\Omega) = \frac{2}{2 + s_0^2 + s_1^2} \geq \frac{2}{3}. \hspace{1cm} (158)$$

With this strategy, the number of tests required for the nonadversarial scenario reads

$$N_{\text{NA}} = \left\lceil \frac{2 + s_0^2 + s_1^2}{2 \epsilon} \ln \delta^{-1} \right\rceil \leq \left\lceil \frac{3}{2 \epsilon} \ln \delta^{-1} \right\rceil. \hspace{1cm} (159)$$

Moreover, this strategy can be turned into a homogeneous strategy with the same spectral gap [43], which is
TABLE I. Verification of bipartite and multipartite quantum states using local projective measurements. The second column shows spectral gaps of efficient verification strategies (not necessarily optimal) for the nonadversarial scenario. The third column indicates whether homogeneous strategies with given spectral gaps can be constructed. The last two columns show the numbers of tests required to verify these states within infidelity $\epsilon$ and significance level $\delta$ in the nonadversarial scenario ($N_{\text{NA}}$) and adversarial scenario ($N$), respectively. Strategies for the adversarial scenario can be constructed using the recipe presented in Sec. IX. Here $d$ is the local dimension, $n$ is the number of parties, and $\chi(G)$ is the chromatic number of the hypergraph or weighted graph $G$. For bipartite pure states and stabilizer states, the table only shows the results in the worst case.

| Quantum states | $\nu(\Omega)$ | homogeneous | $N_{\text{NA}}$ | $N$ |
|---------------|-------------|-------------|----------------|-----|
| Maximally entangled states | $d/d_{\text{max}}$ | yes | $[d_{\text{max}} + 1/\delta - 1] \ln^{-1} 1$ | $[\epsilon^{-1} / \delta]$ |
| Bipartite pure states | $\frac{1}{2}$ | yes | $[\epsilon^{-1} / \delta]$ | $[\epsilon^{-1} / \delta]$ |
| GHZ states | $\frac{1}{2}$ | yes | $[d_{\text{max}} + 1/\delta - 1] \ln^{-1} 1$ | $[\epsilon^{-1} / \delta]$ |
| Qubit stabilizer states | $\frac{1}{2}$ | yes | $[2\epsilon^{-1} \ln^{-1} 1]$ | $[2(\ln 2)^{-1} \ln^{-1} \delta]$ |
| Qudit stabilizer states ($d$ odd prime) | $\frac{1}{2}$ | yes | $[d_{\text{max}} + 1/\delta - 1] \ln^{-1} 1$ | $[\epsilon^{-1} / \delta]$ |
| Hypergraph state $|G\rangle$ | $\chi(G)^{-1}$ | no | $[\chi(G) \ln^{-1} 1]$ | $[\chi(G) + 1] \ln^{-1} \delta^{-1}$ |
| Weighted graph state $|G\rangle$ | $\chi(G)^{-1}$ | no | $[\chi(G) \ln^{-1} 1]$ | $[\chi(G) + 1] \ln^{-1} \delta^{-1}$ |
| Dicke states ($n = 3$) | $\frac{1}{2}$ | no | $[3\epsilon^{-1} \ln^{-1} 1]$ | $[4.1 \epsilon^{-1} \ln^{-1} \delta^{-1}]$ |
| Dicke states ($n \geq 4$) | $(n - 1)^{-1}$ | no | $[(n - 1) \epsilon^{-1} \ln^{-1} 1]$ | $[(n + 1) \epsilon^{-1} \ln^{-1} \delta^{-1}]$ |

useful for fidelity estimation by Eqs. [8] and [9]. The standard deviation of this estimation satisfies

$$\Delta F = \frac{\sqrt{p(1-p)}}{\nu(\Omega) \sqrt{N}} \leq \frac{\sqrt{(1-F)(F + 2 - 1)}}{\sqrt{N}},$$

(160)

where $p = \text{tr}(\sigma) = \nu(\Omega) F + \beta(\Omega)$ and the inequality follows from the inequality $\nu(\Omega) \geq 2/3$, given that the standard deviation decreases monotonically with $\nu(\Omega)$.

By adding the trivial test with a suitable probability, any homogeneous strategy $\Omega$ with $\nu(\Omega) \leq 2/(2 + s_0^2 + s_1^2)$ can be constructed using LOCC [43]. In particular, we can construct a homogeneous strategy $\Omega$ with $\beta(\Omega) = 1/\epsilon$ (that is, $\nu(\Omega) = 1 - (1/\epsilon)$), which is optimal for high-precision verification in the adversarial scenario, so Eq. (157) also applies to general bipartite pure states. Despite the simplicity of bipartite pure states, we are not aware of any other protocol for verifying them in the adversarial scenario that does not rely on our result. Note that self-testing can only verify a pure state up to some local isometry [37, 38, 39], which is different from what we consider here.

D. Stabilizer states

For stabilizer states, which are equivalent to graph states under local Clifford transformations [53, 60], several verification protocols are known in the literature [13–15, 24, 43]. If the total number of tests is the main figure of merit, then the protocol introduced by PLM [43] is an ideal choice. Recall that each $n$-qubit stabilizer state $|G\rangle$ is uniquely determined by $n$ commuting stabilizer generators in the Pauli group, which generate the stabilizer group of order $2^n$. The PLM protocol is composed of $2^n - 1$ projective tests associated with $2^n - 1$ nontrivial stabilizer operators of $|G\rangle$. The corresponding verification operator reads [43]

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

(161)

which is homogeneous with

$$\beta(\Omega_{\text{PLM}}) = \frac{2^{n-1} - 1}{2^n - 1} \leq \frac{1}{2}, \quad \nu(\Omega_{\text{PLM}}) = \frac{2^{n-1} - 1}{2^n - 1} \geq \frac{1}{2},$$

(162)

To verify $|G\rangle$ within infidelity $\epsilon$ and significance level $\delta$, the number of tests required by this protocol is

$$[2^{1-n}(2^n - 1) \epsilon^{-1} \ln^{-1} 1] \leq [2 \epsilon^{-1} \ln^{-1} \delta^{-1}],$$

(163)

which is almost independent of the number $n$ of qubits especially when $n$ is large. Since the strategy in Eq. (161) is homogeneous, it can also be applied for fidelity estimation by virtue of Eqs. [8] and [9]. The standard deviation of this estimation satisfies

$$\Delta F = \frac{\sqrt{p(1-p)}}{\nu \sqrt{N}} \leq \frac{\sqrt{1-F^2}}{\sqrt{N}},$$

(164)

where $p = \text{tr}(\Omega\sigma) = \nu F + \beta$, $\nu = \nu(\Omega_{\text{PLM}}) \geq 1/2$ and

$$\beta = \beta(\Omega_{\text{PLM}}) \leq 1/2.$$

When adapted to the adversarial scenario, the strategy in Eq. (161) is nearly optimal thanks to Theorem [8] and Eq. (157); the number of required tests satisfies

$$N \leq \left[ \frac{\ln \delta}{(\beta \ln \beta) \epsilon} \right] \leq \left[ \frac{2 \ln \delta^{-1}}{(\ln 2) \epsilon} \right] \leq \left[ \frac{2.89 \ln \delta^{-1}}{\epsilon} \right] .$$

(165)

Here the latter two upper bounds are independent of the number of qubits and the specific stabilizer state (or graph state). Moreover, the scaling behaviors in $\epsilon$ and $\delta$
are both optimal. Such a high efficiency in the adversarial scenario is achieved for the first time. Previously, the best protocol for the adversarial scenario (without using our result) required \( [n^3/(d\epsilon)] \) tests \( (n^3/(d\epsilon)) \) tests in the worst case) when \( |G\rangle \) is a graph state whose underlying graph \( G \) is \( m \)-colorable [13, 49].

E. Qudit stabilizer states

Here we introduce an efficient protocol for verifying qudit stabilizer states (including qudit graph states), assuming that the local dimension \( d \) is a prime. Our protocol reduces to the PLM protocol [43] for qudit stabilizer states \( (d = 2) \). Let \( |G\rangle \) be a stabilizer state of \( n \)-qudits. The stabilizer group \( S \) of \( |G\rangle \) is composed of all qudit Pauli operators that stabilize \( |G\rangle \) and is isomorphic to the group \( \mathbb{Z}_d^2 \), where \( \mathbb{Z}_d \) is the field of integers modulo \( d \). Note that \( \mathbb{Z}_d^2 \) is also an \( n \) dimensional vector space over \( \mathbb{Z}_d \). The stabilizer group can be generated by \( n \) commuting Pauli operators, say, \( K_1, K_2, \ldots, K_n \), which satisfy \( K_r^2 = 1 \) for \( r = 1, 2, \ldots, n \). Each stabilizer operator in \( S \) has the form \( \prod_{r=1}^n K_r^{k_r} \) with \( k := (k_1, k_2, \ldots, k_n) \in \mathbb{Z}_d^n \). If \( k = (0, 0, \ldots, 0) \), then this stabilizer operator is equal to the identity operator; otherwise, it has \( d \) distinct eigenvalues \( \omega^j \) for \( j = 0, 1, \ldots, d - 1 \), where \( \omega = e^{2\pi i/d} \) is a primitive \( d \)th root of unity. For each nonzero element \( k \) in \( \mathbb{Z}_d^n \) we can construct a test for \( |G\rangle \) by measuring the stabilizer operator \( \prod_{r=1}^n K_r^{k_r} \); each party performs a Pauli measurement determined by the decomposition of \( \prod_{r=1}^n K_r^{k_r} \) in terms of local Pauli operators. The test is passed if the outcome corresponds to the eigenspace of \( \prod_{r=1}^n K_r^{k_r} \) with eigenvalue 1. The corresponding test projector reads

\[
P_k = \frac{1}{d} \sum_{j=0}^{d-1} \left( \prod_{r=1}^n K_r^{k_r} \right)^j.
\]

Note that \( jk \) for \( j \in \mathbb{Z}_d \) will lead to the same measurement and test operator. Moreover, \( P_k = P_k' \) if \( k' = jk \) for some \( j \in \mathbb{Z}_d \) with \( j \neq 0 \) (this conclusion may fail if \( d \) is not a prime, and that is why we assume that \( d \) is a prime). So each test corresponds to a line in \( \mathbb{Z}_d^n \) that passes through the origin, and vice versa. In total \((d^n - 1)/(d - 1)\) distinct tests can be constructed in this way.

A verification protocol for \( |G\rangle \) can be constructed by performing all distinct tests \( P_k \) randomly each with probability \((d-1)/(d^n-1)\). The resulting verification operator reads

\[
\Omega = \frac{1}{d^n - 1} \sum_{k \in \mathbb{Z}_d^n, k \neq (0,0,\ldots,0)} P_k
= |G\rangle \langle G| + \frac{d^n - 1}{d^n - 1} (1 - |G\rangle \langle G|),
\]

which is homogeneous with

\[
\beta(\Omega) = \frac{d^n - 1}{d^n - 1} \leq \frac{1}{d}, \quad \nu(\Omega) = \frac{d^n - d^n - 1}{d^n - 1} \geq \frac{d - 1}{d}.
\]

The number of tests required by this protocol is

\[
\left\lfloor \frac{d^n - 1}{d^n - d^n - 1} \ln \delta^{-1} \right\rfloor \leq \left\lfloor \frac{d - 1}{d - 1} \ln \delta^{-1} \right\rfloor,
\]

which decreases monotonically with the local dimension \( d \). Surprisingly, qudit stabilizer states with \( d > 2 \) (assuming \( d \) is a prime) can be verified more efficiently than qubit stabilizer states.

Similar to the qubit case, the above protocol can be applied for fidelity estimation. According to Eq. (166), the standard deviation of this estimation satisfies

\[
\Delta F = \frac{\sqrt{p(1-p)}}{\nu \sqrt{N}} \leq \sqrt{(1 - F)'[F + (d - 1)^{-1}]} \frac{1}{\sqrt{N}}
\]

given that \( \nu \geq (d - 1)/d \), where \( p = \text{tr}(\Omega \sigma) = \nu F + \beta \).

By adding the trivial test with a suitable probability we can construct any homogeneous verification operator \( \Omega \) for \( |G\rangle \) with \( \delta \geq \beta(\Omega) < 1 \) using LOCC. When \( d \) is an odd prime, we can construct a homogeneous verification operator \( \Omega \) with \( \beta(\Omega) = 1/e \), which is optimal for the adversarial scenario in the high-precision limit. Then the number of required tests satisfies \( N \leq \left\lfloor e^{-1} \ln \delta^{-1} \right\rfloor \) as in Eq. (167).

The verification protocol presented above is also highly efficient for certifying GME. Suppose \( |G\rangle \) is a qudit graph state associated with a connected graph, where the local dimension \( d \) is a prime. Then \( |G\rangle \) is GME; in addition, \( \rho \) is GME if its fidelity with \( |G\rangle \) is larger than \( 1/d \). In general, to certify the GME of the graph state \( |G\rangle \) with significance level \( \delta \), we need to guarantee \( \langle G|\rho|G\rangle > 1/d \) with significance level \( \delta \). Given a verification strategy \( \Omega \), then it suffices to perform

\[
N = \left\lfloor \frac{\ln \delta}{\ln[1 - (d - 1)^{1/d}]} \right\rfloor
\]

tests according to Eq. (12) with \( \epsilon = (d - 1)/d \). For the strategy in Eq. (167), we have \( \nu(\Omega) \geq (d - 1)/d \), so the minimum number of tests satisfy

\[
N \leq \left\lfloor \frac{\ln \delta}{\ln[1 - (d - 1)^2/d^2]} \right\rfloor = \left\lfloor \ln \delta / \ln[(2d - 1)/d^2] \right\rfloor.
\]

Surprisingly, only one test is required to certify the GME of \( |G\rangle \) when \( \delta \geq (2d - 1)/d^2 \), that is, \( d \geq (1 + \sqrt{1 - \delta})/\delta \).

In the adversarial scenario, we can construct a homogeneous strategy \( \Omega \) with \( \beta(\Omega) = 2/(d + 1) \) using local projective measurements according to the above analysis. Thanks to Corollary 14 with \( \epsilon = (d - 1)/d \), then the GME of \( |G\rangle \) can be certified using only one test as long as the significance level satisfies \( \delta \geq 4d/(d + 1)^2 \), that is, \( d \geq (2 + 2\sqrt{1 - \delta - \delta})/\delta \) (cf. Theorem 3 in Ref. [14]). According to Corollary 15, the lower bound for \( \delta \) cannot
be decreased if \( d \geq 5 \) and if we can perform only one test. Therefore, the GME of a connected graph state can be certified with any given significance level using only one test as long as the local dimension \( d \) is large enough, assuming \( d \) is a prime. Previously, a similar result was known only for GHZ states [48].

F. Hypergraph states

A hypergraph \( G = (V, E) \) is characterized by a set \( V \) of vertices and a set \( E \) of hyperedges \([5, 6]\). For each hypergraph \( G \), one can construct a hypergraph state by preparing the state \(|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \) for each vertex of \( G \) and then applying the generalized controlled-\( Z \) operation on the vertices of each hyperedge \( e \in E \) \([7, 8, 49]\). As a generalization of graph states, hypergraph states are very useful to quantum computation and foundational studies.

Recently, the authors proposed an efficient protocol—the cover protocol—for verifying general hypergraph states, which requires only Pauli \( X \) and \( Z \) measurements for each party \([49]\). As a special case, a coloring protocol can be constructed for each coloring of the hypergraph \( G \). Suppose \( G \) has chromatic number \( \chi(G) \); then the optimal coloring protocol requires only \( \chi(G) \) distinct measurement settings and can achieve a spectral gap of

\[
\nu(\Omega) = \chi(G)^{-1} \geq |\Delta(G) + 1|^{-1} \geq n^{-1},
\]

(173)

where \( \Delta(G) \) is the degree of \( G \) and \( n \) is the number of qubits. Accordingly, the number of required tests reads

\[
N_{\text{NA}} = \left[ \chi(G) e^{-1} \ln \delta^{-1} \right] \leq \left[ ne^{-1} \ln \delta^{-1} \right].
\]

(174)

This performance is nearly optimal if the chromatic number \( \chi(G) \) is small. For example, Union Jack states \([17]\) can be verified with a very high efficiency since the chromatic number of the underlying Union Jack lattice is only 3. These states are particularly interesting because they can realize universal quantum computation under Pauli measurements \([17]\).

By virtue of the general recipe presented in Sec. IX, we can construct a hedged coloring protocol as characterized by the verification operator \( \Omega_p \) with \( p = \nu/e \) \([49]\). In the adversarial scenario, the number of tests required by \( \Omega_p \) satisfies

\[
N \leq \left[ \frac{\chi(G) + e - 1}{1 - \epsilon} \ln (F\delta)^{-1} \right] \leq \left( n + e - 1 \right) \ln (F\delta)^{-1} \frac{1}{\epsilon},
\]

(175)

where \( F = 1 - \epsilon \). The bound is comparable to the counterpart for the nonadversarial scenario especially when \( n \) is large. The hedged coloring protocol is dramatically more efficient than previous protocols for verifying hypergraph states as proposed in Refs. 18, 42. For example, the protocol of Ref. 42 (which improves over Ref. 18) requires more than \((2 \ln 2) n^3 e^{-15}\) tests when \( \delta = \epsilon \) and \( 4ne \leq 1 \) (the number of required tests was derived only for a restricted parameter range) \([49]\). This number is astronomical even when \( n = 3 \) and \( \epsilon = \delta = 0.05 \). In addition, the protocol of Ref. 42 requires adaptive stabilizer tests with \( n \) measurement settings. By contrast, the hedged coloring protocol requires at most \( \Delta(G) + 1 \) settings without adaption [the number of settings can be reduced to \( \chi(G) \) if an optimal coloring can be found; here we do not count the setting corresponding to the trivial test]. The hedged coloring protocol is instrumental to realizing verifiable blind MBQC and quantum supremacy. Its high efficiency demonstrates the power of our general recipe to constructing efficient verification protocols for the adversarial scenario.

Incidentally, the above results also apply to qudit hypergraph states, including qudit graph states in particular \([49]\). For graph states, the hedged coloring protocol is less efficient than the PLM protocol \([43]\) adapted for the adversarial scenario as discussed in Sec. XE and its generalization in Sec. XE but requires much fewer measurement settings.

G. Weighted graph states

Next, consider weighted graph states \([61]\). Recently, Hayashi and Takeuchi introduced several efficient protocols for verifying the weighted graph state \(| G \rangle \) associated with any weighted graph \( G \) \([60]\). One of their protocols is based on a coloring of \( G \) and adaptive local projective measurements. It can achieve the same spectral gap as in Eq. (173), that is, \( \nu(\Omega) = \chi(G)^{-1} \geq n^{-1} \), where \( \chi(G) \) now refers to the chromatic number of the weighted graph \( G \). As in the case of hypergraph states, we can construct a hedged coloring protocol characterized by the verification operator \( \Omega_p \) with \( p = \nu/e \). Then the number of tests required by \( \Omega_p \) to verify \(| G \rangle \) in the adversarial scenario satisfies

\[
N \leq \frac{\chi(G) + e - 1}{\epsilon} \frac{\ln (F\delta)^{-1}}{\epsilon} \leq \frac{(n + e - 1) \ln (F\delta)^{-1}}{\epsilon},
\]

(176)

as in Eq. (175). So weighted graph states can be verified with the same efficiency as hypergraph states.

It should be pointed out that the original protocol in Ref. 54 is based on an earlier version of this paper for dealing with the adversarial scenario \([arXiv:1806.05565]\), so the scaling behavior of \( N \) with the significance level is suboptimal. The latest results developed in our study as presented in Sec. IX are required to achieve the optimal scaling behavior shown in Eq. (170). We are not aware of any other protocol for verifying weighted graph states in the adversarial scenario.

H. Dicke states

Dicke states are another important class of multiparticle quantum states which are useful for quantum metrology.
The $n$-qubit Dicke state with $k$ excitations reads

$$|D^k_{n,n}⟩ = \binom{n}{k}^{-1/2} \sum_{x \in B_{n,k}} |x⟩,$$  \hspace{1cm} (177)

where $B_{n,k}$ denotes the set of strings in $\{0,1\}^n$ with Hamming weight $k$. To avoid trivial cases, here we assume that $n \geq 3$ and $1 \leq k \leq n - 1$. The Dicke state reduces to a $W$ state when $k = 1$. Recently, Liu et al. \[51\] proposed an efficient protocol for verifying the Dicke state, which can achieve a spectral gap of

$$\nu(Ω) = \begin{cases} \frac{1}{3}, & n = 3, \\ \frac{1}{n - 1}, & n \geq 4. \end{cases}$$  \hspace{1cm} (178)

To verify the Dicke state within infidelity $\epsilon$ and significance level $\delta$, the number of required tests reads

$$N_{NA} = \begin{cases} 3\epsilon^{-1}\ln \delta^{-1}, & n = 3, \\ (n - 1)\epsilon^{-1}\ln \delta^{-1}, & n \geq 4. \end{cases}$$  \hspace{1cm} (179)

In the adversarial scenario, we can construct a hedged verification strategy $Ω_p$ with $p = \nu/\epsilon$ according to the recipe in Sec. \[IX\]. Thanks to Theorem 7, the number of tests required by $Ω_p$ satisfies

$$N \leq \begin{cases} 4.1\epsilon^{-1}\ln \delta^{-1}, & n = 3, \\ (n + e - 2)\epsilon^{-1}\ln \delta^{-1}, & n \geq 4. \end{cases}$$  \hspace{1cm} (180)

This number is comparable to the counterpart for the nonadversarial scenario. To the best of our knowledge, no protocol is known previously for verifying general Dicke states in the adversarial scenario, although there are several works on self-testing Dicke states \[62, 63\].

To summarize the above discussions, by virtue of our recipe presented in Sec. \[IX\] optimal verification protocols for the adversarial scenario can be constructed using local projective measurements for all bipartite pure states, GHZ states, and qudit stabilizer states whose local dimension is an odd prime. Nearly optimal protocols can be constructed for qubit stabilizer states and those hypergraph states with small chromatic numbers, including Union Jack states. For general hypergraph states, weighted graph states, and Dicke states, the number of required tests is only about $n\epsilon^{-1}\ln \delta^{-1}$ as shown in Table \[I\] which is dramatically smaller than what is required by previous verification protocols (whenever such protocols are available).

XI. COMPARISON WITH OTHER APPROACHES

Before concluding this paper, it is instructive to compare QSV with other approaches for estimating or verifying quantum states, such as (traditional) quantum state tomography \[34\], compressed sensing \[35\], direct fidelity estimation (DFE) \[36\], and self-testing \[37, 38\]. In this way we hope to put QSV in a wide context, but we do not intend to be exhaustive. Here we are mainly interested in the efficiencies of these approaches with respect to the total number of tests, measurements, or copies of the state required to reach a given precision. Before such a comparison, it should be pointed out that different approaches rely on different assumptions and address different problems. So it is impossible to make a completely fair comparison.

In quantum state tomography, compressed sensing, and DFE, we usually assume that the states prepared in different runs are independent and identical and that the measurement devices are trustworthy. In addition, many protocols only require local projective measurements or even Pauli measurements, which are usually much easier to implement than other more complicated operations. In QSV, the measurement devices are still trustworthy, but the states for different runs may be different as long as they are independent (cf. Sec. \[III\]). In the adversarial scenario, arbitrary correlated or entangled state preparation is allowed. In self-testing, even the measurement devices are not trusted \[32, 35\]. The different strengths of assumptions underlying these approaches are illustrated in Fig. \[10\].

In addition, different approaches address different questions. Quantum state tomography aims to address the following question: What is the state? To answer this question amounts to reconstructing the density matrix, so the number of parameters to be determined increases exponentially with the number of qubits (here we assume that each subsystem is a qubit for simplicity; the general situation is similar). That is why the resource overhead of tomography increases exponentially with the number of qubits. Compressed sensing addresses a similar question, and so cannot avoid the exponential scal-
ing of resource costs. Nevertheless, it can reduce the resource overhead significantly by exploiting the structure of quantum states of low ranks.

DFE, QSV, and self-testing address a different type of questions: Is the state identical to the target state, or how close is it? Here the target state is usually a pure state, and the closeness is usually quantified by fidelity or infidelity. Quite often answering these questions is sufficient for many applications in quantum information processing, so it is of fundamental interest to extract such key information efficiently without full tomography. DFE aims to determine the fidelity (infidelity) between the state prepared and the target state. QSV tries to decide whether the fidelity (infidelity) is larger (smaller) than a given threshold, which is usually easier than fidelity estimation. Self-testing can only provide a lower bound for the fidelity up to some local isometry because the measurement devices are not trustworthy, and the conclusion is solely based on the observed probabilities.

Suppose we can optimize measurement settings and data-processing procedures, then the efficiency of an approach is mainly determined by the strength of the underlying assumptions and the amount of information it extracts. However, in general it is very difficult to determine the efficiency limit of a given approach because it is very difficult to perform such optimization. In addition, it is highly nontrivial to determine the impacts of various assumptions.

Although DFE is much more efficient than quantum state tomography, the resource cost still increases exponentially with the number of qubits, except for some special families of states, such as stabilizer states. The DFE protocol originally proposed in Ref. only requires Pauli measurements; it is not clear whether we can avoid the exponential scaling behavior if more general local measurements are taken into account. In the case of self-testing, there are already numerous research works (see the review paper Ref.); however, little is known about the resource cost to reach a given precision, especially in the multipartite setting. A few known protocols for self-testing multipartite states are highly resource consuming and hardly practical for systems of more than ten qubits. For example, the resource required to self-test Dicke states increases exponentially with the number of qubits. It is still not clear whether this inefficiency is fundamentally inevitable or is due to our lack of imagination.

In QSV in the nonadversarial scenario, we have shown in Sec. that the variation in states prepared in different runs does not incur any resource overhead as long as these states are independent of each other. In other words, as far as the efficiency is concerned, we can assume that these states are identical and independent as assumed in quantum state tomography, compressed sensing, and DFE. Moreover, thanks to our recipe presented in Sec. pure states can be verified in the adversarial scenario with nearly the same efficiency as in the nonadversarial scenario. In many cases, we can even construct optimal protocols, which are quite rare for other approaches. Therefore, we can expect that QSV even in the adversarial scenario is more efficient than DFE and self-testing, as illustrated in Fig. This is indeed the case for all states for which verification protocols have been found, such as bipartite pure states, GHZ states, stabilizer states (including graph states), hypergraph states, weighted graph states, and Dicke states. For example, Dicke states, hypergraph states, and weighted graph states can be verified efficiently in the adversarial scenario, although no efficient DFE or self-testing protocols are available. In the case of general hypergraph states and weighted graph states, actually, no self-testing protocols are known at all.

As pointed out earlier, it would be unfair to compare QSV with self-testing directly, but so far the former is the only practical choice for intermediate and large quantum systems especially in the adversarial scenario. Although self-testing has been studied more intensively in the literature, it is still very difficult to construct efficient self-testing protocols for multipartite states because the measurement devices are not trustworthy. Insight from QSV may be helpful to studying self-testing, and vice versa. The relations between QSV and self-testing are worth further exploration in the future. In particular, it would be desirable to combine the merits of the two approaches. We hope that our work can stimulate further progresses along this direction.

XII. SUMMARY

We presented a comprehensive study of pure-state verification in the adversarial scenario. Notably, we introduced a general method for computing the main figures of merit pertinent to QSV in the adversarial scenario, such as the fidelity and the number of required tests. In addition, we introduced homogeneous strategies and derived analytical formulas for the main figures of merit of practical interest. The conditions for single-copy verification are also clarified, which are instructive to understanding single-copy entanglement detection. Moreover, we proposed a simple, but powerful recipe to constructing efficient verification protocols for the adversarial scenario from the counterpart for the nonadversarial scenario. Thanks to this recipe, any pure state can be verified in the adversarial scenario with nearly the same efficiency as in the nonadversarial scenario. Therefore, to verify a pure quantum state efficiently in the adversarial scenario, it remains to find an efficient protocol for the nonadversarial scenario, which is usually much easier.

Our recipe can readily be applied to the verification of many important quantum states in quantum information processing, including bipartite pure states, GHZ states, stabilizer states, hypergraph states, weighted graph states, and Dicke states. Recently, efficient protocols based on local projective measurements have been
constructed for verifying these states in the nonadversarial scenario. By virtue of our recipe, all these states can be verified efficiently in the adversarial scenario using local projective measurements. These results are instrumental to many applications in quantum information processing that demand high security requirements, such as blind MBQC and quantum networks. The potential of our study is to be unleashed further in the future.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (Grant No. 11875110). MH is 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 1-6, Lemmas 1-12, and Proposition 3. We also present a simpler proof of Eq. (1), which was originally proved in Ref. [43].

Appendix A: Proof of Eq. (1)

Here we present a simpler proof of Eq. (1), which was originally proved in Ref. [43].



Proof. Let \( \rho \) be an arbitrary permutation-invariant diagonal density matrix on \( \mathcal{H}^{\otimes(N+1)} \) with decomposition \( \rho = \sum_{k} c_k \rho_k \), where \( c_k \) form a probability distribution on \( \mathcal{S}_N \). Recall that \( \mathcal{S}_N \) is the set of all sequences \( k = (k_1, k_2, \ldots, k_D) \) of \( D \) nonnegative integers that sum up to \( N+1 \), that is, \( \sum_j k_j = N+1 \). If \( f_\rho = 0 \), then \( \zeta_k(\lambda) = 0 \) whenever \( c_k > 0 \). Therefore,

\[
\eta(N, 0, 0) = \max_{k \in \mathcal{S}_N} \{ \eta_k(\lambda) | \zeta_k(\lambda) = 0 \}. \tag{B1}
\]

To compute \( \eta(N, 0, \Omega) \), we need to determine those \( k \in \mathcal{S}_N \) at which \( \zeta_k(\lambda) = 0 \). By Eq. (27), 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, we have \( \eta_k(\lambda) \leq \beta^N \), and the inequality is saturated when \( k = (0, N+1, 0, \ldots, 0) \). In the second case, we have

\[
\eta_k(\lambda) = \frac{k_i^{k_i - 1}}{N+1} \prod_{j \neq i, k_j > 0} \lambda_j^{k_j} \leq \frac{1}{N+1}. \tag{B2}
\]

and the inequality is saturated when \( k = (N, 0, \ldots, 0) \). If \( \tau > 0 \), then only the first case can occur, so we have \( \eta(N, 0, 0) = \beta^N \). If \( \tau = 0 \), then both cases can occur, so \( \eta(N, 0, 0) = \max\{ \beta^N, 1/(N+1) \} \). In conclusion, we have \( \eta(N, 0, 0) = \delta_c \), which confirms Lemma \( \text{[43]} \)

Next, consider the proofs of Lemmas 2 and 3. From the definitions in Eqs. \( \text{(20)} \) and \( \text{(41)} \) together with the results in Eqs. \( \text{(21)} \) and \( \text{(41)} \) we can deduce the following relations.

\[
\zeta(N, \delta, \Omega) = \min_{\delta' \geq \delta} \tilde{\zeta}(N, \delta', \Omega) \leq \zeta(N, \delta, \Omega), \tag{B3a}
\]

\[
\eta(N, f, \Omega) \leq \max_{f' \leq f} \tilde{\eta}(N, f', \Omega) \leq \tilde{\eta}(N, f, \Omega), \tag{B3b}
\]

\[
F(N, \delta, \Omega) = \min_{\delta' \geq \delta} \tilde{F}(N, \delta', \Omega) \leq \tilde{F}(N, \delta, \Omega), \tag{B3c}
\]

\[
\mathcal{E}(N, f, \Omega) = \min_{f' \geq f} \tilde{\mathcal{E}}(N, f', \Omega) \leq \tilde{\mathcal{E}}(N, f, \Omega). \tag{B3d}
\]

Therefore, Lemmas 2 and 3 are immediate consequences of Lemma \( \text{[43]} \) below.

Lemma 13. The following statements hold.

1. \( \tilde{\zeta}(N, \delta, \Omega) \) is convex and nondecreasing in \( \delta \) for \( 0 \leq \delta \leq 1 \) and is strictly increasing for \( \delta_c \leq \delta \leq 1 \).

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 nondecreasing in \( \delta \) for \( 0 < \delta \leq 1 \) and is strictly increasing for \( \delta_c \leq \delta \leq 1 \).
4. $\tilde{F}(N, f, \Omega)$ is strictly increasing in $f$ for $0 < f \leq 1$.

Here $\delta_c$ is defined in Eq. [34]. The convexity of $\zeta(N, \delta, \Omega)$ means

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

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

$$\tilde{\eta}(N, f, \Omega) \geq (1 - s)\tilde{\eta}(N, f_1, \Omega) + s\tilde{\eta}(N, f_2, \Omega) \tag{B5}$$

for $f = (1 - s)f_1 + sf_2$ and $0 \leq s, f_1, f_2 \leq 1$.

**Proof of Lemma 13** The convexity of $\zeta(N, \delta, \Omega)$ in $\delta$ can be proved by virtue of the definition in Eq. [34]. Suppose $0 \leq \delta_1 < \delta_2 \leq 1$ and $0 < s < 1$; let $\delta = (1 - s)\delta_1 + s\delta_2$. If $\delta_1 > \delta_2$, then there exist two quantum states $\rho_1$ and $\rho_2$ that satisfy

$$p_{\rho_1} = \delta_1, \quad f_{\rho_1} = \zeta(N, \delta_1, \Omega),$$

$$p_{\rho_2} = \delta_2, \quad f_{\rho_2} = \zeta(N, \delta_2, \Omega). \tag{B6}$$

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

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

so that

$$\zeta(N, \delta, \Omega) \leq p_\rho = (1 - s)\zeta(N, \delta_1, \Omega) + s\zeta(N, \delta_2, \Omega), \tag{B8}$$

which confirms Eq. [34].

If $\delta_1 \leq \delta_2$ and $\delta \leq \delta_2$, then $\zeta(N, \delta, \Omega) = \zeta(N, \delta_1, \Omega) = 0$, while $\zeta(N, \delta_2, \Omega) \geq 0$, so Eq. [B4] holds.

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

$$\zeta(N, \delta, \Omega) \leq p_\rho = s'\zeta(N, \delta_2, \Omega) + s\zeta(N, \delta_2, \Omega)$$

$$= (1 - s)\zeta(N, \delta_1, \Omega) + s\zeta(N, \delta_2, \Omega), \tag{B9}$$

which confirms Eq. [34] again. Therefore, $\zeta(N, \delta, \Omega)$ is convex in $\delta$ for $0 \leq \delta \leq 1$.

To prove the monotonicity of $\zeta(N, \delta, \Omega)$ with $\delta$, let $\delta_1, \delta_2$ be real numbers that satisfy $\delta_1 \leq \delta_2 \leq 1$. Then there exists a quantum state $\rho_2$ such that $p_{\rho_2} = \delta_2$ and $f_{\rho_2} = \zeta(N, \delta_2, \Omega) > 0$. Let $s$ be the solution to the equation $\delta_1 = (1 - s)\delta_2 + s\delta_2$; then $0 \leq s \leq 1$. Let $\rho = (1 - s)\rho_\delta + s\rho_\delta$; then $p_\rho = \delta$, so that

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

It follows that $\zeta(N, \delta, \Omega)$ is strictly increasing in $\delta$ when $\delta_1 \leq \delta \leq 1$. As a corollary, $\zeta(N, \delta, \Omega)$ is nondecreasing in $\delta$ for $0 \leq \delta \leq 1$ given that $\zeta(N, \delta, \Omega) = 0$ for $0 \leq \delta \leq \delta_c$.

Next, consider statement 2 in Lemma 13. The convexity of $\tilde{\eta}(N, f, \Omega)$ follows from a similar reasoning that leads to Eq. [B8].

To prove the monotonicity of $\tilde{\eta}(N, f, \Omega)$ over $f$, choose $0 \leq f_1 < f_2 \leq 1$. Then there exists a quantum state $\rho_1$ such that $f_{\rho_1} = f_1$ and $p_{\rho_1} = \tilde{\eta}(N, f_1, \Omega) < 1$. Choose $\varphi = (|\Psi\rangle \langle \Psi|)^{\otimes (N+1)}$; then $f_\varphi = p_\varphi = 1$. Let $s$ be the solution to the equation $f_2 = (1 - s)f_1 + s$; note that $0 < s \leq 1$ because of the assumption $f_1 < f_2 \leq 1$. Let $p_{\rho_2} = (1 - s)p_\varphi + sp_\varphi$; then $f_{\rho_2} = f_2$, so that

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

Here the second inequality follows from the facts that $0 < s \leq 1$ and that $\tilde{\eta}(N, f_1, \Omega) < 1$.

Next, consider statement 3 in Lemma 13. Suppose $\delta_1, \delta_2$ are real numbers that satisfy $\delta_1 \leq \delta_2 \leq 1$. Then $\tilde{F}(N, \delta_2, \Omega) \geq F(N, \delta_2, \Omega) > 0$ and there is a quantum state $\rho_2$ such that $p_{\rho_2} = \delta_2$ and $f_{\rho_2} = \delta_2 \tilde{F}(N, \delta_2, \Omega)$. By assumption, $\delta_1$ can be expressed as a convex sum of $\delta_2$ and $\delta_c$, that is, $\delta_1 = s\delta_2 + (1 - s)\delta_c$ with $0 \leq s \leq 1$. Let $p_\rho = sp_2 + (1 - s)p_c$, then

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

so that

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

Therefore, $\tilde{F}(N, \delta, \Omega)$ is strictly increasing in $\delta$ whenever $\delta_c \leq \delta \leq 1$. As a corollary, $\tilde{F}(N, \delta, \Omega)$ is nondecreasing in $\delta$ for $0 < \delta \leq 1$ given that $\tilde{F}(N, \delta, \Omega) = 0$ for $0 \leq \delta \leq \delta_c$.

Finally, consider statement 4 in Lemma 13. Suppose $f_1$ and $f_2$ are real numbers that satisfy $0 < f_1 < f_2 \leq 1$ and let $s = f_1/f_2$. Then $0 < s \leq 1$ and there exists a quantum state $\rho_2$ such that $f_{\rho_2} = f_2$ and $p_{\rho_2} = f_2/\tilde{F}(N, f_2, \Omega)$. Let $p_\rho = sp_2 + (1 - s)p_c$, where $\rho_c$ is a quantum state that satisfies $p_{\rho_c} = \delta_c$ and $f_{\rho_c} = 0$. Then we have

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

so that

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

Therefore, $\tilde{F}(N, f, \Omega)$ increases strictly monotonically with $f$ for $0 < f \leq 1$. 

2. Proofs of Lemmas 4 to 7

**Proof of Lemma 4** To prove Eq. [35a] in the lemma, let $f_1 = \zeta(N, \delta, \Omega)$ and $\delta_1 = \eta(N, f_1, \Omega)$. If $\delta$ satisfies the condition $0 < \delta \leq \delta_c$, then $f_1 = 0$ and $\delta_1 = \delta_c$ according to Lemma 4 which confirms Eq. [35a].
Now suppose $\delta_c < \delta \leq 1$; then $\max\{\delta, \delta_c\} = \delta$. In addition, there exists a quantum state $\rho$ on $\mathcal{H}^{(N+1)}$ such that $p_p = \delta$ and $f_p = f_1$, 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 $p_{\rho'} = 1 - \delta$, which implies that $\zeta(N, \delta_1, \Omega) \leq f_1 = \zeta(N, \delta_2, \Omega)$. Since $\zeta(N, \delta, \Omega)$ is strictly increasing in \(\delta\) for $\delta_c \leq \delta \leq 1$ according to Lemma 3, we conclude that $\delta_1 \leq \delta$. This observation implies that $\delta_1 = \delta$ and confirms Eq. (38a) given the opposite inequality derived above.

Next, consider Eq. (38b). Let $\delta_1 = \eta(N, f, \Omega)$ and $f_1 = \zeta(N, \delta_1, \Omega)$. Then $\delta_1 \geq \delta_c$ and there exists a quantum state $\rho$ on $\mathcal{H}^{(N+1)}$ such that $p_\rho = f_1$ and $p_\rho = 1 - \delta$, which implies that $f_1 = \zeta(N, \delta_1, \Omega) \leq f$. Meanwhile, there exists a state $\rho'$ such that $p_{\rho'} = 1 - \delta$ and $f_{\rho'} = f_1$, 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 $0 \leq f \leq 1$ according to Lemma 3, we conclude that $f_1 \geq f$. This observation implies that $f_1 = f$ and confirms Eq. (38b) given the opposite inequality derived above.

Proof of Lemma 3. 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 $\eta_k$ for some $k \in \mathcal{F}_N$ at which $\zeta(N, \delta = \eta_k, \Omega) = \zeta_k$ (cf. Lemma 4 below). Here $\eta_k$ and $\zeta_k$ are short-hand for $\eta_{\lambda_k}(\lambda)$ and $\zeta_{\lambda_k}(\lambda)$, respectively, which are defined in Eq. (27). To prove Eq. (39a), it suffices to prove the inequality $\zeta_k \geq \zeta(N - 1, \eta_k, \Omega)$ for each turning point.

If $k_1 = 0$, then $\zeta_k = 0$, which implies that $\eta_k \geq \delta_c$ according to Lemma 1 so that $\zeta(N - 1, \eta_k, \Omega) = 0 \leq \zeta_k$. If $k_1 \geq 1$, let $k' = (k_1 - 1, k_2, \ldots, k_D)$. Then

$$\eta_{k', N-1} \geq \eta_k, \quad \zeta_{k', N-1} \leq \zeta_k,$$  

(B16)

where $\eta_{k', N-1}$ and $\zeta_{k', N-1}$ are given in Eq. (27) with $N$ replaced by $N-1$ and $k$ replaced by $k'$. In conjunction with Lemma 3, we conclude that

$$\zeta(N - 1, \eta_k, \Omega) \leq \zeta(N - 1, \eta_{k', N-1}, \Omega) \leq \zeta_{k', N-1} \leq \zeta_k,$$  

(B17)

which implies Eq. (39a) as desired.

If $\delta \leq \delta_c$, 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. (39a) is saturated in both cases.

If the upper bound in Eq. (B17) is saturated, then $\zeta_{k', N-1} = \zeta_k$, which implies that $\eta_k = 0$ (which means $\eta_k \leq \delta_c$) or $\eta_k = 1$ (which means $\eta_k = 1$). So the upper bound in Eq. (B17) cannot be saturated whenever the turning point satisfies $\delta_c < \eta_k < 1$. In conjunction with Eqs. (32) and (33), this observation implies that the inequality in Eq. (39a) is saturated iff $\delta \leq \delta_c$ or $\delta = 1$. According to Lemma 2, Eq. (39b) and Eq. (39a) are equivalent, so the same conclusion also applies to Eq. (39a).

Equation (39c) and the equality condition can be derived using a similar reasoning as presented above. Equations (39a) and (39c) are equivalent according to Lemma 2.

Alternatively, Eq. (39c) can be derived from Lemmas 1 and Eq. (39a). To be specific, if $f = 0$, then $\eta(N, f, \Omega) < \eta(N - 1, f, \Omega)$ according to Lemma 1, so Eq. (39a) holds with strict inequality. If $f > 0$, then

$$\eta(N, f, \Omega) > \eta(N - 1, f, \Omega), \quad (B18)$$

$$\eta(N - 1, f, \Omega) > \eta(N - 1, 0, \Omega) > \delta_c,$$  

(B19)

according to Lemmas 1 and 3, where $\delta_c$ is given in Eq. (31). In addition, Eq. (39a) and Lemma 1 imply that

$$\zeta(N - 1, f, \Omega), \Omega) \geq \zeta(N - 1, N - 1, f, \Omega), \Omega)$$

$$= f = \zeta(N, \eta(N, f, \Omega), \Omega).$$  

(B20)

In conjunction with Lemma 3, this equation implies that

$$\eta(N, f, \Omega) \leq \eta(N - 1, f, \Omega), \quad (B21)$$

and confirms Eq. (39c). If the inequality in Eq. (39c) is saturated, then the inequality in Eq. (39a) is saturated, so that $\eta(N - 1, f, \Omega) \leq \delta_c$ or $\eta(N - 1, f, \Omega) = 1$. The first case cannot happen, while the second case holds iff $f = 1$. Therefore, the inequality in Eq. (39c) is saturated iff $f = 1$.

Proof of Lemma 4. Lemma 4 follows from the definition of $N(\epsilon, \delta, \Omega)$ in Eq. (23) and the fact that the following four inequalities are equivalent,

$$F(N, \delta, \Omega) \geq 1 - \epsilon,$$  

(B22)

$$\zeta(N, \delta, \Omega) \geq \delta(1 - \epsilon),$$  

(B23)

$$\eta(N, \delta(1 - \epsilon), \Omega) \leq \delta,$$  

(B24)

$$F(N, \delta(1 - \epsilon), \Omega) \geq (1 - \epsilon).$$  

(B25)

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 $\delta > \delta_c$ if either inequality is satisfied.

Proof of Lemma 5. Equation (43b) is an immediate consequence of Eqs. (36a) and (45a); Eq. (43c) is an immediate consequence of Eqs. (29) and (43b). So to prove Lemma 5, it suffices to prove Eq. (45a).

By the definition in Eq. (20a) and Eq. (25) we have

$$\zeta(N, \delta, \Omega) = \min_{\{c_k\}} \left\{ \sum_{k \in \mathcal{F}_N} c_k \zeta_k(\lambda) \mid \sum_{k \in \mathcal{F}_N} c_k \eta_k(\lambda) \geq \delta \right\}$$

$$\geq \min_{\{c_k\}} \left\{ \sum_{k \in \mathcal{F}_N} c_k \zeta_k(N, \delta = \eta_k(\lambda), \tilde{\Omega}) \mid \sum_{k \in \mathcal{F}_N} c_k \eta_k(\lambda) \geq \delta \right\}$$

$$\geq \min_{\{c_k\}} \left\{ \zeta(N, \sum_{k \in \mathcal{F}_N} c_k \eta_k(\lambda), \tilde{\Omega}) \mid \sum_{k \in \mathcal{F}_N} c_k \eta_k(\lambda) \geq \delta \right\}$$

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

(B26)
which confirms Eq. (43a). Here \( \{c_k\} \) is a probability distribution on \( \mathcal{S}_N \); the first inequality in Eq. (120) follows from the assumption \( \zeta_k(\lambda) \geq \zeta(N, \delta = \eta_k(\lambda)) \) for all \( k \in \mathcal{S}_N \), and the second inequality follows from the convexity of \( \zeta(N, \delta', \Omega) \) in \( \delta' \) (cf. Lemma 3); the last equality follows from the monotonicity of \( \zeta(N, \delta', \Omega) \) in \( \delta' \). □

By Eq. (47) 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 \( \eta_k(\lambda) \) for certain \( k \in \mathcal{S}_N \). In conjunction with the monotonicity and convexity (concavity) of \( \zeta(N, \delta, \Omega) \) stated in Lemma 3 (see also Lemma 4), we can deduce the following conclusion. Here \( \delta_c \) is defined in Eq. (41).

**Lemma 14.** \( \zeta(N, \delta, \Omega) \) for \( \delta_c \leq \delta \leq 1 \) and \( \eta(N, f, \Omega) \) for \( 0 \leq f \leq 1 \) can be expressed as follows,

\[
\zeta(N, \delta, \Omega) = \frac{a_{j+1} - \delta}{a_{j+1} - a_j} b_j + \frac{\delta - a_j}{a_{j+1} - a_j} b_{j+1}, \quad (B27)
\]

\[
\eta(N, f, \Omega) = \frac{b_{l+1} - f}{b_{l+1} - b_l} a_l + \frac{f - b_l}{b_{l+1} - b_l} a_{l+1}, \quad (B28)
\]

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 \( a_j = \eta_{k(j)}(\lambda) \) and \( b_j = \zeta_{k(j)}(\lambda) \) with \( k(j) \in \mathcal{S}_N \) for \( j = 0, 1, \ldots, m \), which satisfy the following conditions

\[
\delta_c = a_0 < a_1 < \ldots < a_{m-1} < a_m = 1, \quad (B29)
\]

\[
0 = b_0 < b_1 < \ldots < b_{m-1} < b_m = 1, \quad (B30)
\]

\[
0 = \frac{b_0}{a_0} < \frac{b_1}{a_1} < \ldots < \frac{b_{m-1}}{a_{m-1}} < \frac{b_m}{a_m} = 1. \quad (B31)
\]

Note that we can choose strict inequalities \( \delta > a_j \) and \( f > b_l \) in Lemma 4 if \( \delta > \delta_c \) and \( f > 0 \). If \( \Omega \) is a nonsingular homogeneous strategy defined in Eq. (44) for example, then we have \( \delta_c = \lambda^N, m = N + 1, \ a_j = \eta_{N+1-j}(\lambda), \) and \( b_j = \zeta_{N+1-j}(\lambda) \); cf. Theorem 4 in the main text.

**Lemma 15** is very helpful to understand the properties of \( \zeta(N, \delta, \Omega) \) and \( \eta(N, f, \Omega) \), although, in general, it is not easy to determine the values of \( m, k^{(j)}, a_j, \) 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 \( (\tau^N, 0) \), as illustrated in Fig. 1. This conclusion is tied to Lemma 23 presented in Appendix B.

**Appendix C: Homogeneous strategies**

1. **Auxiliary 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 \( j, k \in \mathbb{Z}_{\geq 0} \) and \( 0 < \lambda < 1 \), define

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

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

where \( \eta_k(\lambda) \) and \( \zeta_k(\lambda) \) are defined in Eq. (17), assuming that \( N \) is a positive integer. To simplify the notations, we shall use \( \eta_k, \zeta_k, g_{kj}, g_{kj} \) as shorthands for \( \eta_k(\lambda), \zeta_k(\lambda), g_{kj}(\lambda), g_{kj}(\lambda) \) if there is no danger of confusion. Geometrically, \( g_{jk} \) and \( g_{kj} \) denote the slope of the line passing through the two points \( (\eta_j, \zeta_j) \) and \( (\eta_k, \zeta_k) \).

**Lemma 15.** 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 16.** Let \( 0 \leq \lambda < 1 \) and \( k \in \{1, 2, \ldots, N + 1\} \). Then

\[
\frac{1}{1 - \lambda^N} \leq \frac{1 - \zeta_k(\lambda)}{1 - \eta_k(\lambda)} \leq \frac{1 + N(1 - \lambda)}{N(1 - \lambda)} = \frac{1 + N\nu}{N\nu}. \quad (C3)
\]

The first inequality is saturated iff \( k = N + 1 \), or \( k \geq 2 \) and \( \lambda = 0 \); the second inequality is saturated iff \( k = 1 \).

When \( 0 \leq \lambda < 1 \) (and \( N \) is a positive integer), Lemma 10 implies that

\[
\frac{1}{1 - \lambda^N} < \frac{1 + N\nu}{N\nu}, \quad \lambda^N < \frac{1}{N\nu + 1}. \quad (C4)
\]

The two inequalities actually hold for a wider parameter range according to Lemma 17 below.

**Lemma 17.** Suppose \( 0 < \lambda \leq 1, \nu = 1 - \lambda \), and \( a \) is a real number. Then

\[
\lambda^{-a} - a
\]

\[
\lambda^{-a} - a - 1 \geq 0 \quad \text{if} \ a \geq 0 \ or \ a \leq -1, \quad (C5)
\]

\[
\lambda^{-a} - a - 1 \leq 0 \quad \text{if} \ -1 \leq a < 0. \quad (C6)
\]

If \( a \neq -1, 0 \), then the inequality in Eq. (C5) is saturated iff \( \lambda = 1 \); the same holds for the inequality in Eq. (C6).

**Lemma 18.** Let \( 0 < \lambda < 1, 0 \leq \delta \leq 1 \), and \( k \in \mathbb{Z}_{\geq 0} \). Then \( \zeta(N, \delta, \lambda, \lambda) \) increases strictly monotonically with \( \delta \) when \( k \leq N + 1 \). Also, \( \zeta(N, \delta, \lambda, k) \) increases strictly monotonically with \( N \) except when \( \delta = 1 \) and \( k = 0 \).

Here \( \zeta(N, \delta, \lambda, k) \) is defined in Eq. (43) in the main text. Note that \( \zeta(N, \delta, \lambda, k) = 1 \) is independent of \( N \) and \( \lambda \) when \( \delta = 1 \) and \( k = 0 \).

**Lemma 19.** Suppose \( 0 < \lambda < 1 \) and \( 0 < \delta \leq 1 \). Then

\[
\max_{k \in \mathbb{Z}_{\geq 0}} \zeta(N, \delta, \lambda, k) = \zeta(N, \delta, \lambda, k_+), \quad (C7)
\]

\[
\max\left\{0, \zeta(N, \delta, \lambda, k_+)\right\} = \max\left\{0, \max_{k \in \{0, 1, \ldots, N\}} \zeta(N, \delta, \lambda, k)\right\} = \max\left\{0, \zeta(N, \delta, \lambda, k_+), \zeta(N, \delta, \lambda, k_-)\right\}, \quad (C8)
\]

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,

\[
\zeta(N, \delta, \lambda, k_+) \leq 0, \quad 0 \leq \delta \leq \lambda^N, \quad (C9)
\]

\[
\zeta(N, \delta, \lambda, k_+) > 0, \quad \lambda^N < \delta \leq 1. \quad (C10)
\]
Lemma 20. Suppose $0 < \epsilon, \delta, \lambda < 1$ and $k \in \mathbb{Z}^{\geq 0}$. Then

$$
\tilde{N}(\epsilon, \delta, \lambda, k) > 0 \text{ and it decreases strictly monotonically with } \epsilon \text{ and } \delta. \text{ If } \delta \leq \lambda^k/(F + \lambda \epsilon), \text{ then } \tilde{N}(\epsilon, \delta, \lambda, k) > k - 1. \text{ Given } k \geq 1, \text{ then } \tilde{N}(\epsilon, \delta, \lambda, k) \leq \tilde{N}(\epsilon, \delta, \lambda, k - 1) \text{ iff } \delta \leq \lambda^k/(F + \lambda \epsilon). \text{ In addition,}
$$

$$
\min_{k \in \mathbb{Z}^{\geq 0}} \tilde{N}(\epsilon, \delta, \lambda, k) = \min \{\tilde{N}_+(\epsilon, \delta, \lambda), \tilde{N}_-(\epsilon, \delta, \lambda)\} \leq k^* \quad (C11)
$$

where $k^*$ is the largest integer $k$ that satisfies the inequality $\delta \leq \lambda^k/(F + \lambda \epsilon)$ and $\tilde{N}_+(\epsilon, \delta, \lambda) = \tilde{N}(\epsilon, \delta, \lambda, k) \pm$ with $k_+ = \lceil \log_\lambda \delta \rceil$ and $k_- = \lfloor \log_\lambda \delta \rfloor$.

Here $\tilde{N}(\epsilon, \delta, \lambda, k)$ is defined in Eq. (C8).

Lemma 21. Suppose $0 < \epsilon, \delta, \lambda < 1$. Then

$$
\tilde{N}_-(\epsilon, \delta, \lambda) \leq \frac{F \nu + \lambda \delta - \log_\lambda \delta - k_-}{\lambda \epsilon} = \frac{\log_\lambda \delta - \nu k_-}{\lambda \epsilon} \quad (C14)
$$

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

Proof of Lemma 17. According to Eqs. (C1) and (C2) as well as the definitions of $\eta_k(\lambda)$ and $\zeta_k(\lambda)$ in Eq. (C17), we have

$$
\eta_k(\lambda) - \eta_{k+1}(\lambda) = \frac{\lambda}{N \lambda + k \nu} > 0, \quad (C16)
$$

where $\nu = 1 - \lambda$. So $g_k(\lambda)$ decreases strictly monotonically with $k$ for $k \in \mathbb{Z}^{\geq 0}$.

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

$$
g_k(\lambda) = \sum_{m=k}^{j-1} \eta_m(\lambda) - \eta_{m+1}(\lambda) g_m(\lambda). \quad (C17)
$$

Here the weight for each $g_m(\lambda)$ is strictly positive given that $\eta_m(\lambda)$ decreases strictly monotonically with $m$ for $m \in \mathbb{Z}^{\geq 0}$. So $g_j(\lambda) < g_{j-1}(\lambda) \leq g_k(\lambda)$ when $k + 1 < j$. In addition, $g_{k(j+1)}(\lambda)$ is a convex sum of $g_k(\lambda)$ and $g_j(\lambda)$, that is,

$$
g_{k(j+1)}(\lambda) = \frac{(\eta_k - \eta_j)g_k + (\eta_j - \eta_{j+1})g_j}{\eta_k - \eta_{j+1}} \quad (C18)
$$

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

Proof of Lemma 17. When $0 < \lambda < 1$, Lemma 16 is an immediate consequence of Lemma 15 given that

$$
\eta_0(\lambda) = \zeta_0(\lambda) = 1, \quad \eta_{N+1}(\lambda) = \lambda^N, \quad \zeta_{N+1}(\lambda) = 0 \quad (C19)
$$

$$
\eta(\lambda) = \frac{1 + N \lambda}{N + 1}, \quad \zeta(\lambda) = \frac{N \lambda}{N + 1} \quad (C20)
$$

so that

$$
g_{0k}(\lambda) = \frac{1 - \zeta_k(\lambda)}{1 - \eta_k(\lambda)} = \begin{cases} 
1 + \frac{N(1-\lambda)}{N(1-\lambda)} & k = 1,
1 & k = N + 1.
\end{cases} \quad (C21)
$$

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 16 can be verified explicitly.

Proof of Lemma 17. Note that $\lambda^{-a} - \nu = 1$ when $\lambda = 1$, or $a = 0$, or $a = -1$. The derivative of $\lambda^{-a} - \nu = 1$ over $\lambda$ reads $a(1 - \lambda^{-a-1})$, and it satisfies

$$
a(1 - \lambda^{-a-1}) \leq 0 \quad \text{if } a \geq 0 \text{ or } a \leq -1, \quad (C22)
a(1 - \lambda^{-a-1}) \geq 0 \quad \text{if } -1 \leq a \leq 0, \quad (C23)
$$

which imply the inequalities in Eqs. (C15) and (C16) given that $\lambda^{-a} - \nu = 1$ when $\lambda = 1$. If $a \neq -1$, then the inequality in Eq. (C22) is saturated iff $a = 1$, and the same holds for the inequality in Eq. (C23). Therefore, both Eq. (C15) and Eq. (C16) are saturated iff $a = 1$, which completes the proof of Lemma 17.

Proof of Lemma 18. The monotonicity of $\zeta(N, \delta, \lambda, k)$ with $\delta$ follows from the facts that $\zeta(N, \delta, \lambda, k)$ is linear in $\delta$ and that $1 + (N - k)\nu > 0$ when $k \leq N + 1$.

According to the following equation

$$
\zeta(N + 1 + \delta, \lambda, k) - \zeta(N, \delta, \lambda, k) = \frac{\lambda^{k+1} + \delta(k \nu - \lambda)}{\nu(N \lambda + k \nu)((N + 1) \lambda + k \nu)}, \quad (C24)
$$

to prove the monotonicity of $\zeta(N, \delta, \lambda, k)$ with $N$, it suffices to prove the inequality

$$
\lambda^{k+1} + \delta(k \nu - \lambda) \leq 0, \quad (C25)
$$

which is saturated iff $\delta = 1$ and $k = 0$. To this end, it suffices to consider the two special cases $\delta = 0$ and $\delta = 1$ since the left-hand side in Eq. (C24) is linear in $\delta$. In the first case, the inequality is strict. In the second case, according to Lemma 17 with $a = -(k + 1)$, we have

$$
\lambda^{k+1} + k \nu - \lambda \geq -(k + 1)\nu + 1 + k \nu - \lambda = 0, \quad (C26)
$$

and the inequality is saturated iff $k = 0$. This observation confirms the inequality in Eq. (C24) and the saturation condition, which in turn confirms Lemma 18.
Proof of Lemma [13] When \( k - 1 \in \mathbb{Z}^{\geq 0} \), by the definition of \( \zeta(N, \delta, \lambda, k) \) in Eq. (C3), we can derive
\[
\zeta(N, \delta, \lambda, k) - \zeta(N, \delta, \lambda, k - 1) = \frac{\lambda^k [k + (N + 1 - k) \lambda] - (N + 1) \lambda^k}{(k\nu + N\lambda) \nu + N\lambda}. \tag{C27}
\]
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 \( \eta_k \geq \delta \), that is, \( k = k_* \), which confirms Eq. (C7).

Before proving Eq. (C8), we first prove Eqs. (C9) and (C10). According to Eq. (C6) 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. (C9). Conversely, if \( \lambda^N < \delta \leq \lambda \), then \( k_* \leq N \), which implies that \( \zeta_k(\lambda) > 0 \) and \( \zeta_{k+1}(\lambda) \leq 0 \). So \( \zeta(N, \delta, \lambda, k_*) > 0 \), which confirms Eq. (C10).

Alternatively, to prove Eq. (C9), 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. (C3), we have
\[
\zeta(N, \delta = 0, \lambda, k) = -\frac{\lambda^{k+1}}{\nu(k\nu + N\lambda)} < 0, \tag{C28}
\]
\[
\zeta(N, \delta = \lambda^N, \lambda, k) = \frac{{\lambda}\lambda^N [1 + (N - k) \nu] - \lambda^k}}{\nu(k\nu + N\lambda)} \leq 0, \tag{C29}
\]
which imply Eq. (C9). Here \( \nu = 1 - \lambda \) and the inequality in Eq. (C29) follows from Lemma [17] with \( a = N - k \).

Finally, we can prove Eq. (C8). If \( 0 < \delta \leq \lambda^N \), then Eq. (C8) follows from Eq. (C7) and the fact that \( \zeta(N, \delta, \lambda, k_*) \leq 0 \). If instead \( \lambda^N < \delta \leq 1 \), then we have \( 0 \leq k_* \leq N \) and \( 0 \leq k_* < N - 1 \); in addition, \( \eta_k(\lambda) \geq \delta \) and \( \eta_{k+1}(\lambda) < \delta \). Therefore, \( k_* \in \{0, 1, \ldots, N\} \) and \( k_* \) is equal to either \( k_* \) or \( k_- \), which implies Eq. (C8) given Eq. (C7).

Proof of Lemma [20] To prove Lemma [20] we first investigate the monotonicity of \( \tilde{N}(\epsilon, \delta, \lambda, k) \) defined in Eq. (C3) for \( 0 < \epsilon, \delta \leq 1 \), \( 0 < \lambda < 1 \), and \( k \in \mathbb{Z}^{\geq 0} \). The partial derivative of \( \tilde{N}(\epsilon, \delta, \lambda, k) \) over \( \epsilon \) reads
\[
\frac{\partial \tilde{N}(\epsilon, \delta, \lambda, k)}{\partial \epsilon} = -\frac{\lambda^{k+1} + \delta(k\nu - \lambda)}{\nu \lambda \nu \delta^2} \leq 0, \tag{C30}
\]
where the inequality is saturated iff \( k = 0 \) and \( \delta = 1 \); cf. Eq. (C25). Therefore, \( \tilde{N}(\epsilon, \delta, \lambda, k) \) is strictly decreasing in \( \epsilon \) for \( 0 < \epsilon \leq 1 \) except when \( k = 0 \) and \( \delta = 1 \), in which case \( \tilde{N}(\epsilon, \delta, \lambda, k) = 0 \).

Next, the partial derivative of \( \tilde{N}(\epsilon, \delta, \lambda, k) \) over \( \delta \) reads
\[
\frac{\partial \tilde{N}(\epsilon, \delta, \lambda, k)}{\partial \delta} = -\frac{\lambda^k}{\nu \delta^2} \epsilon < 0. \tag{C31}
\]
So \( \tilde{N}(\epsilon, \delta, \lambda, k) \) is strictly decreasing in \( \delta \) for \( 0 < \delta \leq 1 \). According to the above analysis,
\[
\tilde{N}(\epsilon, \delta, \lambda, k) \geq \tilde{N}(\epsilon = 1, \delta = 1, \lambda, k) = \frac{\lambda^k + k\nu - 1}{\nu} \geq 0. \tag{C32}
\]
Here the first inequality is saturated iff \( \epsilon = \delta = 1 \), or \( \delta = 1 \) and \( k = 0 \); the second inequality is saturated \( k = 0 \) (cf. Lemma [17]). Therefore, \( \tilde{N}(\epsilon, \delta, \lambda, k) > 0 \), except when \( \delta = 1 \) and \( k = 0 \), or \( \epsilon = \delta = k = 1 \). Given the assumption \( 0 < \epsilon, \delta < 1 \), then \( \tilde{N}(\epsilon, \delta, \lambda, k) > 0 \) and \( \tilde{N}(\epsilon, \delta, \lambda, k) \) decreases strictly monotonically with \( \epsilon \) and \( \delta \).

Next, suppose \( 0 < \epsilon, \delta < 1 \). If \( \delta \leq \lambda^k/(F + \lambda\epsilon) \) and \( k = 0 \), then \( \tilde{N}(\epsilon, \delta, \lambda, k) > k - 1 \) according to the first statement in Lemma [20]. If instead \( \delta = \lambda^k/(F + \lambda\epsilon) \) and \( k \geq 1 \), then
\[
\tilde{N}(\epsilon, \delta, \lambda, k) = k - 1 + \frac{kF}{\lambda \epsilon} > k - 1. \tag{C33}
\]
So \( \tilde{N}(\epsilon, \delta, \lambda, k) > k - 1 \) whenever \( \delta \leq \lambda^k/(F + \lambda\epsilon) \) given that \( \tilde{N}(\epsilon, \delta, \lambda, k) \) is monotonically decreasing in \( \delta \).

Next, if \( k \geq 1 \), then
\[
\tilde{N}(\epsilon, \delta, \lambda, k) - \tilde{N}(\epsilon, \delta, \lambda, k - 1) = \frac{\nu \delta (F \nu + \lambda) + \lambda^{k+1} - \lambda^k}{\lambda \nu \delta \epsilon} = \frac{\delta(F + \lambda\epsilon) - \lambda^k}{\lambda \nu \delta \epsilon}, \tag{C34}
\]
so \( \tilde{N}(\epsilon, \delta, \lambda, k) < k - 1 \) iff \( \delta \leq \lambda^k/(F + \lambda\epsilon) \). Consequently, the minimum of \( \tilde{N}(\epsilon, \delta, \lambda, k) \) over \( k \in \mathbb{Z}^{\geq 0} \) is attained when \( k \) is the largest integer that satisfies the inequality \( \delta \leq \lambda^k/(F + \lambda\epsilon) \), that is, \( k = k^* \), which confirms Eq. (C11).

In addition, we have
\[
\frac{\lambda^{k+1}}{F + \lambda \epsilon} < \lambda^k \leq \delta \leq \lambda^{k^*} < \frac{\lambda^{k^*}}{F + \lambda \epsilon}, \tag{C35}
\]
given that \( \lambda < F + \lambda \epsilon < 1 \). So \( k^* \) in Eq. (C11) is equal to either \( k^- \) or \( k^- \), which implies Eq. (C12). Finally, Eq. (C13) is an easy consequence of Eq. (C34).

Proof of Lemma [23] The equality in Eq. (C14) can be verified by straightforward calculation given the equality \( F \nu + \lambda = 1 - \nu \epsilon \). According to the definitions in Eqs. (C3) and (C4), we have
\[
\tilde{N}^{-}(\epsilon, \delta, \lambda, \nu) = \frac{k - \epsilon^2 \delta F + \lambda^{k+1} + \lambda \delta (k \nu - 1)}{\lambda \nu \delta \epsilon} = \frac{F \nu + \lambda - k^-}{\lambda \epsilon} + \frac{\lambda^{k+1} - \lambda \delta}{\lambda \nu \delta \epsilon} = \frac{F \nu + \lambda - k^- + \lambda^{k^*} - \lambda \nu \delta \epsilon}{\lambda \nu \delta \epsilon}. \tag{C36}
\]
So the inequality in Eq. (C11) is equivalent to the following inequality
\[
\lambda^{k^*} - \lambda - \nu \delta \epsilon \leq 0, \tag{C37}
\]
where $b = \log_\lambda \delta - k_- = \log_\lambda \delta - |\log_\lambda \delta|$, which satisfies $0 \leq b < 1$. Equation (C57) holds because the function $\lambda^{1-b} - \lambda^{-b}$ is strictly convex in $b$ (given the assumption $0 < \lambda < 1$) and it is equal to 0 when $b = 0$ and $b = 1$ (the function is well defined when $b = 1$ although this value cannot be attained here). In addition, the inequality in Eq. (C57) is saturated iff $b = 0$, which means $\log_\lambda \delta$ is an integer. Alternatively, these conclusions follow from Lemma 17 with $a = b - 1$. Therefore, the inequality in Eq. (C14) is saturated if $\log_\lambda \delta$ is an integer. □

2. Proofs of Theorems [13] and Eq. (72)

**Proof of Theorem 1.** According to Lemma 2, we have $F(N, \delta, \lambda) = \zeta(N, \delta, \lambda)/\delta$. If $\delta \leq \delta_\epsilon = \lambda^N$, then we have $\zeta(N, \delta, \lambda) = 0$ by Eq. (C22). If $\delta > \lambda^N$, then

$$\zeta(N, \delta, \lambda) = \min_{0 \leq k < j \leq \lceil N \rceil} (c_j \zeta_j + c_k \zeta_k), \quad (C38)$$

where $\zeta_j, \zeta_k$ are short hands 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

$$c_j + c_k = 1, \quad c_j \eta_j + c_k \eta_k = \delta, \quad (C39)$$

which yield

$$c_j = \frac{\eta_k - \delta}{\eta_k - \eta_j}, \quad c_k = \frac{\delta - \eta_j}{\eta_k - \eta_j}, \quad (C40)$$

Therefore,

$$c_j \zeta_j + c_k \zeta_k = \frac{\eta_k - \delta}{\eta_k - \eta_j} \zeta_j + \frac{\delta - \eta_j}{\eta_k - \eta_j} \zeta_k = \zeta_j + g_{kj}(\delta - \eta_j) = \zeta_j + g_{kj}(\delta - \eta_k), \quad (C41)$$

where $g_{kj} = g_{kj}(\lambda)$ is defined in Eq. (C11).

If $j > k + 1$, then $\eta_{j-1} < \delta$ or $\eta_{j+1} \geq \delta$, so the value of $c_j \zeta_j + c_k \zeta_k$ does not increase if we replace $j$ with $j - 1$ or $k$ with $k + 1$ according to Lemma 16. Therefore, the minimum in Eq. (C38) can be attained when $j = k + 1$ and $\eta_{k+1} < \delta \leq \eta_k$, in which case $k = k_\ast$ is the largest integer that satisfies the condition $\eta_k \geq \delta$. In addition we have $c_k = c_k(\delta, \lambda)$ and $c_j = 1 - c_k(\delta, \lambda)$, so that

$$\zeta(N, \delta, \lambda) = c_j \zeta_j + c_k \zeta_k = \zeta(N, \delta, \lambda, k_\ast), \quad (C42)$$

which confirms Eq. (C54). □

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

$$\zeta(N, \delta, \lambda) \geq F\delta, \quad (C43)$$

where $F\delta > 0$. According to Corollary 11 in the main text, Eq. (C43) is equivalent to

$$\max_{k \in \mathbb{Z}^+} \zeta(N, \delta, \lambda, k) \geq F\delta. \quad (C44)$$

Note that the maximum in the left-hand side can be attained at a finite value of $k$. From the definition of $\zeta(N, \delta, \lambda, k)$ in Eq. (C53) we can deduce that the inequality $\zeta(N, \delta, \lambda, k) \geq F\delta$ is satisfied iff

$$N \geq \tilde{N}(\epsilon, \delta, \lambda, k) = \frac{k\nu^2 \delta F + \lambda^{k+1} + \lambda \delta(k\nu - 1)}{\lambda \nu \delta \epsilon}. \quad (C45)$$

So Eq. (C43) is satisfied iff

$$N \geq \min_{k \in \mathbb{Z}^+} \tilde{N}(\epsilon, \delta, \lambda, k), \quad (C46)$$

which implies Theorem 2 given Lemma 20. □

**Proof of Eq. (72).** The equality in Eq. (72) follows from Theorem 2 and Corollary 3. Let $\lambda = \lambda(\epsilon, \delta, \lambda, 1)$ be the unique solution of $\partial \tilde{N}(\epsilon, \delta, \lambda, 1) / \partial \lambda = 0$.

Therefore,

$$N(\epsilon, \delta, \lambda) \geq \tilde{N}(\epsilon, \delta, \lambda, 1) \geq \tilde{N}(\epsilon, \delta, \lambda_\ast, 1) = \frac{\sqrt{(1 - \delta)F}}{1 - \delta + \sqrt{\delta F}}. \quad (C49)$$

which confirms the lower bound in Eq. (72). □

**Proof of Theorem 3.** Let $N = k_\ast + \lceil \delta / \lambda \rceil$. According to Corollary 3 we have

$$F(N, \delta, \lambda) \geq \frac{(N - k_\ast)\lambda}{k_\ast + (N - k_\ast)\lambda} = \frac{k_\ast F}{k_\ast + k_\ast F} = F = 1 - \epsilon, \quad (C51)$$

which implies that $N(\epsilon, \delta, \lambda) \leq N$ and confirms the upper bound in Eq. (73). Next, let $N = k_\ast + \lceil \delta / \lambda \rceil$. If $k_- = 0$, then we have $N = 0 < N(\epsilon, \delta, \lambda)$. If $k_- \geq 1$, then $N - 1 \geq k_- \geq 1$. By virtue of Corollary 3 we can deduce that

$$F(N - 1, \delta, \lambda) \leq \frac{(N - 1 - k_-)\lambda}{k_- + (N - 1 - k_-)\lambda} = \frac{(\lceil \delta F \rceil - 1)\lambda}{k_- + (\lceil \delta F \rceil - 1)\lambda} < \frac{\delta \epsilon}{k_- + \delta \epsilon} = 1 - \epsilon, \quad (C52)$$

which follows from Eq. (72). □
which implies that $N(\varepsilon, \delta, \lambda) \geq N$ and confirms the lower bound in Eq. (74).

If $\log_3 \delta$ is an integer, then $k_+ = k_-$, so the lower bound and upper bound in Eq. (74) coincide, which means both of them are saturated. Alternatively, this fact can be verified by virtue of Theorem 2.

Finally, let us prove Eq. (74). Theorem 2 in the main text and Lemma 24 imply that

$$N(\varepsilon, \delta, \lambda) = \lfloor \log_3 \delta \epsilon - \frac{\nu k_-}{\lambda} \rfloor,$$

which confirms Eq. (74). If $\log_3 \delta$ is an integer, then both inequalities are saturated, so the bound in Eq. (74) is saturated.

Appendix D: Proof of Theorem 4

Proof. If the strategy $\Omega$ is homogeneous, then we have $\zeta(N, \delta, \Omega) = \zeta(N, \delta, \beta)$, and Theorem 4 follows from Proposition 2. In general, Theorem 4 can be proved based on Eq. (77) and the observation that $\eta_k(\lambda) - \zeta_k(\lambda) = 1/2$ for all $k \in S_\lambda$ with $k_1 = 1$ given the assumption $N = 1$. Here $S_\lambda$ is defined in the paragraph before Eq. (25) in the main text. Geometrically, this fact means that all points $(\eta_k(\lambda), \zeta_k(\lambda))$ for $k \in S_\lambda$ with $k_1 = 1$ lie on a line segment.

To be specific, recall that $\zeta(N, \delta, \Omega) \leq \zeta(N, \delta, \beta)$. When $\beta \geq 1/2$, Eq. (104) holds because the opposite inequality $\zeta(N, \delta, \Omega) \geq \zeta(N, \delta, \beta)$ also holds. In view of Lemma 1 to verify this claim, it suffices to prove that

$$\zeta_k(\lambda) \geq \zeta(N, \delta = \eta_k(\lambda), \beta) \quad \forall k \in S_\Omega.$$

The assumption $k \in S_\Omega$ means $k_j \geq 0$ and $\sum_j k_j = 2$. When $k_1 = 2$, we have $\zeta_k(\lambda) = \eta_k(\lambda) = 1$, so Eq. (D1) holds. When $k_1 = 0$, we have $\zeta_k(\lambda) = 0$, while $\eta_k(\lambda) \leq \beta$ according to Lemma 1, so that $\zeta(N, \delta = \eta_k(\lambda), \beta) = 0$ (cf. Theorem 1 and Eq. (111) also holds. When $k_1 = 1$, according to Eq. (27), we have

$$\eta_k(\lambda) = \frac{1 + \lambda_j}{2}, \quad \zeta_k(\lambda) = \frac{\lambda_j}{2},$$

for some $2 \leq j \leq D$. If $(1 + \lambda_j)/2 \leq \beta$, then we have $\zeta(N, \delta = \eta_k(\lambda), \beta) = 0$ according to Eq. (D1), so Eq. (D1) holds. If $(1 + \lambda_j)/2 \geq \beta$ (note that $\lambda_j \leq \beta$), then

$$\zeta_k(\lambda) - \zeta(N, \delta = \eta_k(\lambda), \beta) = \frac{\lambda_j}{2} - \frac{\beta(1 + \lambda_j - 2\beta)}{2(1 - \beta)} \geq 0.$$

Therefore, Eq. (121) holds for all $k \in S_\Omega$, which implies that $\zeta(N, \delta, \Omega) \geq \zeta(N, \delta, \beta)$. In conjunction with the opposite inequality, we can deduce the desired equality $\zeta(N, \delta, \Omega) = \zeta(N, \delta, \beta)$, which confirms Eq. (106).

Next, consider the case $\beta < 1/2$. If $\tau = \beta$, then Eq. (107) follows from Proposition 2. If $\tau < \beta$, let $\hat{\Omega}$ be a verification operator with three distinct eigenvalues, $1, \beta, \tau$ (the eigenvalue $1$ is nondegenerate); then we have $\zeta(N, \delta, \hat{\Omega}) \leq \zeta(N, \delta, \hat{\Omega})$. In addition, it is straightforward to verify Eq. (107) if $\delta$ is replaced by $\Omega$. To prove Eq. (107), it suffices to prove that $\zeta(N, \delta, \Omega) \geq \zeta(N, \delta, \hat{\Omega})$. Thanks to Lemma 7, this condition can be simplified to

$$\zeta_k(\lambda) \geq \zeta(N, \delta = \eta_k(\lambda), \hat{\Omega}) \quad \forall k \in S_\Omega.$$

When $k_1 = 2$, we have $\zeta_k(\lambda) = \eta_k(\lambda) = 1$, so Eq. (D4) holds. When $k_1 = 0$, we have $\zeta_k(\lambda) = 0$ and $\eta_k(\lambda) \leq \beta$ according to Eq. (27), so

$$\zeta(N, \delta = \eta_k(\lambda), \hat{\Omega}) \leq \zeta(N, \delta = \eta_k(\lambda), \beta) = 0,$$

and Eq. (D4) also holds. When $k_1 = 1$, Eq. (D2) and the inequality $\tau \leq \lambda_j \leq \beta$ imply that

$$\zeta(N, \delta = \eta_k(\lambda), \hat{\Omega}) = \frac{\lambda_j}{2} = \zeta_k(\lambda);$$

recall that Eq. (107) holds if $\delta$ is replaced by $\hat{\Omega}$. This observation confirms Eq. (123) and implies the inequality $\zeta(N, \delta, \Omega) \geq \zeta(N, \delta, \hat{\Omega})$. In conjunction with the opposite inequality, we conclude that $\zeta(N, \delta, \Omega) = \zeta(N, \delta, \hat{\Omega})$, which implies Eq. (107).

Appendix E: Proofs of Lemma 8 and Theorem 5

1. Main body of the proofs

Proof of Lemma 8 By the definition of $F(N, \delta, \Omega)$ in Eq. (26), to prove the inequality in Eq. (114) in the lemma, it suffices to find a permutation-invariant quantum state $\rho$ on $H^{(N+1)}$ such that $p_{\rho} = \delta$ and

$$f_\rho = p_\rho - \frac{1}{N + 1} \quad \text{(E1)}$$

for each $\delta$ in the interval $1/(N+1) \leq \delta \leq \delta^*$. 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 $\rho = \rho_k$ with $k = (N,0,\ldots,0,1)$, in which case $p_\rho = 1/(N+1)$ and $f_\rho = 0$ by Eq. (27), so Eq. (115) holds as desired; note that $\Omega$ is singular by assumption, which means $\tau = \lambda_D = 0$.

In the case $\delta = \delta^*$, we can choose the state $\rho = \rho_k$ with $k_j = (N,1,0,\ldots,0)$. Then Eq. (27) [cf. Eq. (17)] yields

$$p_\rho = \eta_{k_1}(\lambda) = \frac{1 + N\beta}{N + 1} = \frac{1 + N(1 - \nu)}{N + 1} = \delta^*,$$

$$f_\rho = \zeta_{k_1}(\lambda) = \frac{N\beta}{N + 1} = \frac{N(1 - \nu)}{N + 1}. \quad \text{(E2)}$$

Therefore,

$$p_\rho - f_\rho = \eta_{k_1}(\lambda) - \zeta_{k_1}(\lambda) = \frac{1}{N + 1}. \quad \text{(E3)}$$
and Eq. (E1) holds again. This observation completes the proof of Lemma 23.

**Proof of Theorem 5.** To prove the inequality in Eq. (112) in the theorem, let \( r = \sum_{k \in \mathcal{J}_N} c_k p_k \) as in Eq. (29), where \( c_k \) form a probability distribution on \( \mathcal{J}_N \). If \( r > 1 \), then \( c_k = \delta_{2,k_0} \) with \( k_0 := (N+1, \ldots, 0) \), in which case we have \( F_r = f_r = 1 \) and \( F(N, \delta = 1, \Omega) = 1 \), so Eq. (112) holds. If \( 0 < r < 1 \), then \( c_k > 0 \) and \( \delta < 1 \). Since both \( s \) and \( \rho \) have equality in Eq. (E6) can be saturated when \( \delta \) is in \( \mathcal{J}_N \). If \( \rho = 1 \), then \( c_k = \delta_{2,k_0} \) with \( k_0 := (N+1, \ldots, 0) \), in which case we have \( F_\rho = f_\rho = 1 \) and \( F(N, \delta = 1, \Omega) = 1 \), so Eq. (E6) is also saturated. When \( \delta \) satisfies \( 1/(N+1) \leq \delta \leq \delta^* \), then this bound is saturated according to Lemma 8.

### 2. Auxiliary lemmas

Here we assume that \( \lambda_j \) are the eigenvalues of a verification operator \( \Omega \) that are arranged in decreasing order of \( \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_D > 0 \). In addition, \( \beta = \lambda_2 \) and \( \tau = \lambda_D \) are the second largest and the smallest eigenvalues; meanwhile, \( \nu = 1 - \beta \).

**Lemma 22.** \( \eta_k(\lambda) - \zeta_k(\lambda) \leq 1/(N+1) \) for all \( k \in \mathcal{J}_N \) if \( \beta \leq 1/2 \).

**Proof.** If \( k = k_0 \), then \( \eta_k(\lambda) = \zeta_k(\lambda) = 1 \), so we have \( \eta_k(\lambda) - \zeta_k(\lambda) = 0 \leq 1/(N+1) \). If \( k \neq k_0 \), then Eq. (27) implies that

\[
\eta_k(\lambda) - \zeta_k(\lambda) = \sum_{i \geq 2|k_i| \geq 1} \frac{k_i}{(N+1)} \lambda_i^{k_i-1} \prod_{j \neq i} \lambda_j^{k_j} \leq \frac{N+1-k_1}{N+1} \beta^{N-k_1} \leq \frac{N+1}{N+1} \leq 1.
\]

The first inequality follows from the facts that \( \lambda_j \leq \beta \) for \( j \geq 2 \) and that \( 0 \leq N - k_1 \leq N \); the second inequality follows from the assumption \( \beta \leq 1/2 \).

Define

\[
\xi_k(\lambda) := \frac{1 - \eta_k(\lambda)}{1 - \zeta_k(\lambda)}, \quad k \in \mathcal{J}_N^*, \quad (E13)
\]

where \( \mathcal{J}_N^* := \mathcal{J}_N \setminus \{k_0\} \) is the subset of \( \mathcal{J}_N \) without the vector \( k_0 := (N+1, \ldots, 0) \).

**Lemma 23.** For each \( k \in \mathcal{J}_N^* \), we have

\[
\frac{N\nu}{N+1} \leq \xi_k(\lambda) \leq 1 - \tau^N, \quad (E14)
\]

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. (E14) can be expressed as

\[
\frac{N\nu}{N+1} = \frac{1 - \eta_k(\lambda)}{1 - \zeta_k(\lambda)}, \quad (E15)
\]
where \( k_1 := (N,1,0,\ldots,0) \). According to Eq. (34), we have
\[
\frac{N\nu}{N\nu + 1} < 1 - \beta^N \leq 1 - \tau^N.
\] (E16)

Lemma 23 implies that the region \( R_{N,\Omega} \) is contained in the triangle determined by the following three lines
\[
f = 0, \\
1 - p = (1 - \tau^N)(1 - f), \\
1 - p = \frac{N\nu}{N\nu + 1}(1 - f).
\] (E17)
The three vertices of the triangle are \((1,1), (\tau^N,0), \) and \((1/(N\nu+1),0)\); the first two vertices are the extremal points of \( R_{N,\Omega} \).

**Proof of Lemma 24.** The assumption \( k \in \mathcal{K}_N^* \) implies that \( \sum_j k_j = N + 1 \) and \( k_1 \leq N \). Thanks to Lemma 23 below, we have
\[
\xi_k(\lambda) \geq \xi_k(1,\beta,\ldots,\beta) = \xi(k_i,N-k_i+1)(1,\beta)
\]
\[
= \frac{1 - \eta_{N-k_i+1}(\beta)}{1 - \xi_{N-k_i+1}(\beta)} \geq \frac{N\nu}{N\nu + 1},
\] (E18)
where the second inequality follows from Lemma 16 in Appendix C. Note that the definition of \( \xi_k(\lambda) \) as well as that of \( \eta_k(\lambda) \) and \( \xi_k(\lambda) \) can be extended as long as \( k \) and \( \lambda \) have the same number of components.

By the same token, we have
\[
\xi_k(\lambda) \leq \xi_k(1,\tau,\ldots,\tau) = \xi(k_i,N-k_i+1)(1,\tau)
\]
\[
= \frac{1 - \eta_{N-k_i+1}(\tau)}{1 - \xi_{N-k_i+1}(\tau)} \leq 1 - \tau^N,
\] (E19)
where the two inequalities follow from Lemma 24 and Lemma 16 respectively.

Here it is instructive to take a look at the special scenario in which \( \xi_k(\lambda) = 0 \) (cf. the proof of Lemma 1 in Appendix B), which means \( k_i = 0 \), or \( \lambda_i = 0 \) and \( k_i \geq 1 \) for some \( 2 \leq i \leq D \). In the first case, we have \( \tau^N \leq \eta_k(\lambda) \leq \beta^N \) by Eq. (24), so that
\[
\xi_k(\lambda) = 1 - \eta_k(\lambda) \leq 1 - \tau^N,
\] (E20)
\[
\xi_k(\lambda) \geq 1 - \beta^N \geq \frac{N\nu}{N\nu + 1},
\] (E21)
where the last inequality follows from Eq. (34). In the second case, we have \( \tau = 0 \) and
\[
\eta_k(\lambda) = \frac{k_i\lambda_i^{-1}}{N + 1} \prod_{j \neq i, k_j > 0} \lambda_j^{k_j} \leq \frac{1}{N + 1},
\] (E22)
which implies that
\[
\xi_k(\lambda) = 1 - \eta_k(\lambda) \leq 1 - \tau^N,
\] (E23)
\[
\xi_k(\lambda) \geq \frac{N}{N + 1} \geq \frac{N\nu}{N\nu + 1}.
\] (E24)
These results are compatible with Lemma 23 as expected.

**Lemma 24.** Suppose \( k = (k_1,k_2,\ldots,k_m) \) is a sequence of \( m \geq 2 \) nonnegative integers that satisfies \( k_1 \leq N \) and \( \sum_j k_j = N + 1 \), where \( N \) is a positive integer. Let \( u, v \) be two \( m \)-component vectors that satisfy \( 0 \leq u \leq v \leq 1 \) and \( u_1 = v_1 = 1 \). Then we have \( \zeta_k(u) \geq \zeta_k(v) \).

The inequality \( 0 \leq u \leq v \leq 1 \) in the above lemma means \( 0 \leq u_j \leq v_j \leq 1 \) for each \( j = 1,2,\ldots,m \).

**Proof.** The assumption \( 0 \leq u \leq v \leq 1 \) and Eq. (27), imply that \( \zeta_k(u) \leq \zeta_k(v) \leq k_1/(N + 1) < 1 \), so \( \zeta_k(u) \) is continuous in \( u \) for \( 0 \leq u \leq 1 \) by the definition in Eq. (E13). Therefore, it suffices to prove the lemma when \( 0 < u \leq v \leq 1 \), in which case \( \eta_k(u) \) and \( \zeta_k(u) \) can be expressed as follows,
\[
\eta_k(u) = \theta \sum_j \frac{k_i}{u_j}, \quad \zeta_k(u) = \theta k_1,
\] (E25)
where \( \theta := (\prod_i u_i^\nu)/(N + 1) \).

For \( j \geq 2 \), calculation shows that
\[
\frac{\partial \zeta_k(u)}{\partial u_j} = \theta \left\{ \frac{k_j}{u_j} \sum_i \frac{k_i}{u_i} - \frac{k_j}{u_j^2} \right\},
\]
\[
\frac{\partial \zeta_k(u)}{\partial u_j} = \theta k_j u_j.
\] (E26)
These derivatives have well-defined limits even when some components \( u_i \) approach zero; this fact would be clearer if we insert the expression of \( \theta \). In addition,
\[
\frac{\partial \zeta_k(u)}{\partial u_j} = -\theta k_j u_j \sum_{i \geq 1,i \neq j} \frac{k_i}{u_i} - \theta k_j + \theta^2 k_j k_1 u_j
\]
\[
= -\theta k_j \left[ u_j \sum_{i \geq 1,i \neq j} \frac{k_i}{u_i} + (k_j - 1) + k_1 \right] \left( 1 - \theta k_1 u_j^2 \right) \leq 0,
\] (E27)
note that \( 1 - \theta k_1 \geq 1/(N + 1) > 0 \). The inequality in Eq. (E27) is strict except when \( k_j = 0 \), in which case \( \zeta_k(u) \) is independent of \( u_j \), and so are \( \eta_k(u) \) and \( \zeta_k(u) \) [cf. Eq. (27) in the main text]. Therefore, \( \zeta_k(u) \) is non-increasing in \( u_j \) for \( j \geq 2 \), which means \( \zeta_k(u) \geq \zeta_k(v) \) whenever \( 0 < u \leq v \leq 1 \) and \( u_1 = v_1 = 1 \). The condition \( 0 \leq u \leq v \leq 1 \) can be relaxed to \( 0 \leq u \leq v \leq 1 \) by continuity.

**Appendix F: Proofs of Lemma 9 and Theorem 6**

1. Auxiliary lemmas

Before proving Lemma 9 and Theorem 6 we need to introduce a few auxiliary notions and results.

Denote by \( \mathcal{K}_N \) the convex hull of \( \mathcal{K}_N \), then \( \mathcal{K}_N \) is composed of real vectors \( k = (k_1,k_2,\ldots,k_D) \) that satisfy \( \sum_{j=1}^D k_j = N + 1 \) and \( k_j \geq 0 \) for \( j = 1,2,\ldots,D \). When \( \Omega \) is positive definite, that is, \( \tau(\Omega) > 0 \), we can extend the definition of \( \eta_k(\lambda) \) and \( \xi_k(\lambda) \) over \( k \) to \( \mathcal{K}_N \) [cf. Eq. (27)].
Since all eigenvalues $\lambda_j$ of $\Omega$ for $j = 1, 2, \ldots, D$ are positive, we have $\eta_k(\lambda) > 0$ for all $k \in \mathcal{N}$. The following analogs of $\zeta(N, \delta, \Omega)$ and $\eta(N, f, \Omega)$ [cf. Eq. (F3)] will play key roles in proving Lemma 25 and Theorem 26. Define

$$
\zeta(N, \delta, \Omega) := \min_{k \in \mathcal{N}} \left\{ \eta_k(\lambda) | \eta_k(\lambda) = \delta \right\}, \quad \beta^N \leq \delta \leq 1,
$$

$$
0 \leq \delta \leq \beta^N;
$$

$$
\eta(N, f, \Omega) := \max_{k \in \mathcal{N}} \left\{ \eta_k(\lambda) | \zeta_k(\lambda) = f \right\}, \quad 0 \leq f \leq 1,
$$

where $\beta$ is the second largest eigenvalue of $\Omega$. Incidentally, $\eta(N, f = 0, \Omega) = \delta_e = \beta^N$ since $\tau > 0$; see Lemma 24.

**Lemma 25.** Suppose $0 \leq \delta, f \leq 1$ and $\Omega$ is a positive-definite verification operator; then

$$
\zeta(N, \delta, \Omega) \leq \zeta(N, \delta, \Omega),
$$

$$
\eta(N, f, \Omega) \leq \eta(N, f, \Omega).
$$

**Proof.** When $\delta$ satisfies $0 \leq \delta \leq \beta^N$, by definition we have $\zeta(N, \delta, \Omega) = 0 \leq \zeta(N, \delta, \Omega)$, so Eq. (E23) holds.

When $\delta > \beta^N$, by Lemma 24 in Appendix B we can find vectors $q_0, q_1 \in \mathcal{N}$ such that $\beta^N \leq \eta_0 < \eta_1 \leq 1$, $\eta_0 < \delta \leq \eta_1$, $0 \leq \zeta_0 < \zeta_1 \leq 1$, and $0 \leq F_0 < F_1 \leq 1$, where $\eta_j = \eta_j(\lambda)$, $\zeta_j = \zeta_j(\lambda)$, and $F_j = \zeta_j/\eta_j$ for $j = 0, 1$. In addition, $\zeta(N, \delta, \Omega) = c_0\zeta_0 + c_1\zeta_1$, where $c_0$ 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,

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

If $\delta = \eta_1$, then $\zeta(N, \delta, \Omega) = \zeta_1$ and Eq. (F3) holds because $\mathcal{N} \subset \mathcal{N}$. So it remains to consider the scenario $\eta_0 < \delta < \eta_1$, in which case we have $0 < c_0, c_1 < 1$. Geometrically, the point $(\delta, \zeta(N, \delta, \Omega))$ lies on the line segment that connects the two end points $(\eta_0, \zeta_0)$ and $(\eta_1, \zeta_1)$, which has slope $(\zeta_1 - \zeta_0)/(\eta_1 - \eta_0)$.

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

$$
k(t) = q_0(1-t) + q_1 t = q_0 + (q_1 - q_0) t, \quad \eta(t) = \eta_{k(t)}(\lambda), \quad \zeta(t) = \zeta_{k(t)}(\lambda),
$$

Note that $k(t) \in \mathcal{N}$ for $0 \leq t \leq 1$; in addition, $\eta(0) = \eta_0$ and $\zeta(0) = \zeta_0$, while $\eta(1) = \eta_1$ and $\zeta(1) = \zeta_1$. So Eq. (F7) defines a parametric curve $(\eta(t), \zeta(t))$ that connects $(\eta_0, \zeta_0)$ and $(\eta_1, \zeta_1)$. The explicit expressions of $\eta(t)$ and $\zeta(t)$ can be derived by virtue of Eq. (F7), with the result

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

where

$$
\theta(t) = \frac{1}{N + 1} \prod_j \lambda_j^{k_j(t)}.
$$

Let

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

then $F(0) = F_0$ and $F(1) = F_1$.

Let $t_0$ be the smallest value of $t$ such that $\eta(t) = \delta$; then $\zeta(N, \delta, \Omega) \leq \zeta(t_0)$. So Eq. (F23) would follow if we can prove that $\zeta(t_0) \leq \zeta(N, \delta, \Omega)$.

To achieve our goal, we shall prove that the parametric curve $(\eta(t), \zeta(t))$ for $0 \leq t \leq t_0$ lies below the line segment passing through 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

$$
\frac{d^2 \zeta(t)}{dt^2} = \frac{\zeta''(t)}{\eta''(t)} = \frac{\ln \lambda_j}{\eta(t)} \left[ k_j(t) \ln \frac{\theta_1}{\theta_0} + (\eta_1 - \eta_0) \right],
$$

Here the derivatives with respect to $t$ can be computed explicitly by virtue of Eq. (F8), with the result

$$
\eta'(t) = \frac{d\eta(t)}{dt} = \eta(t) \sum_j (q_1 - q_0) \ln \lambda_j + \theta(t) \sum_j \frac{q_1 - q_0}{\lambda_j} = \theta(t) \left[ \frac{\eta(t)}{\theta(t)} \ln \frac{\theta_1}{\theta_0} + \left( \frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0} \right) \right],
$$

$$
\zeta'(t) = \frac{d\zeta(t)}{dt} = \zeta(t) \sum_j (q_1 - q_0) \ln \lambda_j + \theta(t)(q_11 - q_01) = \theta(t) \left[ k_1(t) \ln \frac{\theta_1}{\theta_0} + (q_11 - q_01) \right],
$$

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

$$
\zeta''(t) = \frac{d^2 \zeta(t)}{dt^2} = \theta(t) \left[ \ln \frac{\theta_1}{\theta_0} \right] \left[ k_1(t) \ln \frac{\theta_1}{\theta_0} + 2(q_11 - q_01) \right].
where
\[ \theta_0 = \theta(t = 0) = \frac{1}{N + 1} \prod_j \lambda_j^{q_{0j}}, \quad \theta_1 = \theta(t = 1) = \frac{1}{N + 1} \prod_j \lambda_j^{q_{1j}}. \] (F16)

Note that
\[ \theta'(t) = \frac{d\theta(t)}{dt} = \theta(t) \sum_j (q_{1j} - q_{0j}) \ln \lambda_j = \theta(t) \ln \frac{\theta_1}{\theta_0}. \] (F17)

Therefore,
\[ \zeta''(t)\eta'(t) - \eta''(t)\zeta'(t) = \theta(t)^2 \left( \ln \frac{\theta_1}{\theta_0} \right)^2 \left[ (q_{11} - q_{01}) \frac{\eta_1(t)}{\theta(t)} \frac{\eta(t)}{\theta(t)} \right] - \left( \frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0} \right) k_1(t) \]
\[ = \theta(t)^2 \left( \ln \frac{\theta_1}{\theta_0} \right)^2 \left[ \left( q_{11} - q_{01} \right) \frac{\eta_0}{\theta_0} \left( \frac{\eta_1}{\theta_1} + \frac{\eta_0}{\theta_0} \right) \right] - \left( \frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0} \right) [q_{01} + (q_{11} - q_{01})t] \]
\[ = \theta(t)^2 \left( \ln \frac{\theta_1}{\theta_0} \right)^2 \left( \eta_0 q_{01} + \eta_1 q_{11} - \frac{\eta_0}{\theta_0} \right) \theta(t)^2 \left( \ln \frac{\theta_1}{\theta_0} \right)^2 \eta_0 q_{01} \left( \frac{\theta_1 q_{11}}{\theta_1 - \frac{\theta_0 q_{01}}{\theta_0}} \right) \]
\[ = \theta(t)^2 \left( \ln \frac{\theta_1}{\theta_0} \right)^2 \eta_0 q_{01} (F_1 - F_0) \geq 0. \] (F18)

Here the inequality is strict except when \( \theta_1 = \theta_0 \), in which case \( \theta(t) \) is independent of \( t \), while both \( \eta(t) \) and \( \zeta(t) \) are linear in \( t \). So the derivative \( \frac{d^2 \zeta(t)}{d\eta(t)^2} \) has the same sign as \( \eta'(t) \) unless it is identically zero.

Note that \( \eta(t)/\theta(t) \) is a linear function of \( t \). So \( \eta'(t)/\theta(t) \) is linear and thus monotonic in \( t \) according to Eq. (F12), actually, \( \eta(t)/\theta(t) \) is strictly monotonic in \( t \) unless it is a constant. When \( t = 0 \), we have
\[ \eta'(0) = \eta_0 \left[ \ln \frac{\theta_1}{\theta_0} + \frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0} \right] \]
\[ > \eta_0 \left[ \ln \frac{\theta_1}{\theta_0} + \frac{\theta_0}{\theta_1} - 1 \right] \geq 0 \] (F19)
given that \( \eta_1 > \eta_0 > 0 \). Since \( \theta(t) > 0 \), it follows that \( \eta'(t) \) has at most one zero point in the interval \( 0 \leq t \leq 1 \).

If \( \eta'(t) > 0 \) in this interval, then \( \frac{d^2 \zeta(t)}{d\eta(t)^2} \leq 0 \) and \( \zeta(t) \) is a convex function of \( \eta(t) \) for \( 0 \leq t \leq 1 \), so 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 the inequality \( \zeta(t_5) \leq \zeta(N, \delta, \Omega) \) and Eq. (F3). Here \( t_5 \) is the smallest value of \( t \) such that \( \zeta(t) = \delta \). Otherwise, \( \eta'(t) \) has a unique zero point \( 0 < t_2 < 1 \). If \( t_2 = 1 \), then the same conclusion holds. If \( t_2 < 1 \), then \( \eta'(t) > 0 \) for \( 0 \leq t < t_2 \) and \( \eta'(t) < 0 \) for \( t_2 < t \leq 1 \), 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 \( 0 \leq t \leq t_3 \) and that \( \zeta(t) < \eta(t) \). To prove Eq. (F3), it suffices to prove the inequality \( \zeta(t_3) \leq \zeta_1 \), that is, \( F(t_3) \leq F_1 \), given that \( \eta(t_3) = \eta_1 \).

To proceed, we compute the derivative of \( F(t) \) over \( t \), with the result
\[ \frac{dF(t)}{dt} = \frac{\theta(t)^2}{\eta(t)^2} \eta_0 \eta_1 (F_1 - F_0) > 0. \] (F20)

This derivative can be derived either from Eq. (F10) or from Eqs. (F12) and (F13) given that \( F(t) = \zeta(t)/\eta(t) \).

So \( F(t) \) increases monotonically with \( t \) for \( 0 \leq t \leq 1 \), which implies that \( F(t_3) \leq F(1) = F_1 \) and that \( \zeta(t_3) \leq \zeta(1) = \zeta_1 \). Therefore, the parametric curve \( (\eta(t), \zeta(t)) \) for \( 0 \leq t \leq t_3 \) lies below the line segment that connects the two points \((\eta_0, \zeta_0)\) and \((\eta_1, \zeta_1)\), which implies that \( \zeta(t_3) \leq \zeta(N, \delta, \Omega) \) and confirms Eq. (F3).

Equation (F4) can be proved using a similar reasoning used for proving Eq. (F6). When \( f = 0 \), we have
\[ \bar{\eta}(N, f, \Omega) = \max_{k \in \mathcal{N}} \{ \eta_k(\lambda) | \zeta_k(\lambda) = 0 \} \]
\[ \geq \max_{k \in \mathcal{N}} \{ \eta_k(\lambda) | \zeta_k(\lambda) = 0 \} = \eta(N, f, \Omega), \] (F21)
which confirms Eq. (F11); here the inequality follows from the fact that \( \mathcal{N} \) is contained in \( \mathcal{N} \). When \( f > 0 \), we can choose \( q_0, q_1 \in \mathcal{N} \) and define \( \eta_0, \zeta_0, \eta_1, \zeta_1, \eta(t), \zeta(t) \) in a similar way to the proof of Eq. (F15), but with the requirement \( \eta_0 \leq \delta \leq \eta_1 \) replaced by \( \zeta_0 \leq f < \zeta_1 \). Since the case \( f = \zeta_1 \) is trivial, we can assume \( \zeta_0 \leq f < \zeta_1 \). Then Eqs. (E6) and (E20) still apply. According to Eq. (F18) and the following equation
\[ \frac{d^2 \eta(t)}{d\zeta(t)^2} = -\frac{\zeta''(t)\eta'(t) - \eta''(t)\zeta'(t)}{\zeta'(t)^3} \] (F22)
the derivative \( \frac{d^2 \eta(t)}{d\zeta(t)^2} \) has the opposite sign to \( \zeta'(t) \) unless it is identically zero.
When \( t = 0 \), we have
\[
\zeta'(0) = \theta_0 \left[ q_{01} \ln \frac{\theta_1}{\theta_0} + (q_{11} - q_{01}) \right]
\geq \theta_0 \left[ q_{01} \left( 1 - \frac{\theta_0}{\theta_1} \right) + (q_{11} - q_{01}) \right]
= \theta_0 \frac{q_{11} \theta_1 - q_{01} \theta_0}{\theta_1} = \theta_0 \frac{\zeta_1 - \zeta_0}{\theta_1} > 0. \tag{F23}
\]

In addition, \( \theta(t) > 0 \), and \( \zeta'(t)/\theta(t) \) is a linear and thus monotonic function of \( t \) according to Eq. (F23). Therefore, \( \zeta'(t) \) has at most one zero point in the interval \( 0 \leq t \leq 1 \) as is the case for \( \eta'(t) \). Now Eq. (F23) can be proved using a similar reasoning as presented after Eq. (F19), though “convex” is replaced by “concave”.

**Lemma 26.** Suppose \( 1 > x_1 \geq x_2 \geq \cdots , x_m > 0 \) and \( c < 0 \). Then
\[
\max_{a_1, a_2, \ldots, a_m \geq 0} \left\{ \sum_j a_j \ln x_j \right\} = \frac{c}{y \ln y}, \tag{F24}
\]

where \( y = x_1 \) if \( x_1 \ln x_1 \leq x_m \ln x_m \) and \( y = x_m \) otherwise.

**Proof.** The maximization in Eq. (F24) is a linear programming in which the feasible region is defined by the inequalities \( a_1, a_2, \ldots, a_m \geq 0 \) and the equality \( \sum_j a_j \ln x_j = c \). If \( c = 0 \), then \( a_1 = a_2 = \cdots = a_m = 0 \), so Eq. (F24) holds.

If \( c < 0 \), then the maximum in Eq. (F24) can be attained at one of the extremal points of the feasible region, which have the form
\[
a_j = \frac{c}{\ln x_j}, \quad a_i = 0 \quad \forall i \neq j, \quad j = 1, 2, \ldots, m. \tag{F25}
\]

Therefore,
\[
\max_{a_1, a_2, \ldots, a_m \geq 0} \left\{ \sum_j a_j \ln x_j \right\} = \max_j \frac{c}{x_j \ln x_j} = \max_j \frac{c}{x_j \ln x_j} = \frac{c}{y \ln y}. \tag{F26}
\]

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

**2. Main body of the proofs**

Now we are ready to prove Lemma 9.

**Proof of Lemma 9.** We shall first prove Eq. (121). According to Lemma 26,
\[
\mathcal{F}(N, f, \Omega) = \frac{f}{\eta(N, f, \Omega)} \geq \frac{f}{\eta(N, f, \Omega)} \tag{F27}
\]
which implies that \( N + 1 - k_1 \leq f \ln f / \ln \beta = \log_\beta f \), that is, \( k_1 \geq N + 1 - (\ln f / \ln \beta) \). In addition, the above equation implies that \( 0 \geq \sum_{j=2}^D k_j \ln \lambda_j \geq \ln f \), which in turn implies that \( \sum_{j=2}^D (k_j / \lambda_j) \leq f / (\ln \beta \ln \tilde{\beta}) \) in view of Lemma 26. Therefore,
\[
\mathcal{F}(N, f, \Omega) \geq \frac{\min_{k_1 \in \mathcal{S}} k_1}{N + 1 - (\ln \beta)^{-1} \ln f} \tag{F28}
\]
which confirms Eq. (120).

Next, let us prove Eq. (120). If \( \delta < \beta^N \), then we have \( \tau \delta \leq \beta^{N+1} \) and \( N + 1 - (\ln \beta)^{-1} \ln \tau \delta \leq 0 \), so the bound in Eq. (120) is either zero or negative and is thus trivial. If \( \delta \geq \beta^N \), then Lemma 26 implies that
\[
\mathcal{F}(N, f, \Omega) = \frac{\zeta(N, \delta, \Omega)}{\delta} \geq \frac{\zeta(N, \delta, \Omega)}{\delta} \tag{F29}
\]

The condition \( \eta_\delta(\lambda) = \delta \) entails the following inequality,
\[
\tau \delta = \tau \eta_\delta(\lambda) = \frac{\tau}{N + 1} \left( \prod_j \lambda_j \right) \left( \sum_j k_j / \lambda_j \right) \leq \frac{D}{2} \lambda_j \leq \beta^{N+1-k_1}. \tag{F30}
\]

Now, Eq. (120) can be proved using a similar reasoning that leads to Eq. (129), but with \( f \) replaced by \( \tau \delta \).

**Proof of Theorem 7.** Equation (121) follows from Eq. (30) and Theorem 8 in the main text. The lower bound in Eq. (120) follows from Eq. (124) given that \( \beta = \beta_2 = \beta \) or \( \beta = \tau = \lambda D \).

To prove the upper bounds in Eq. (120), let \( f = F \delta \) with \( F = 1 - \epsilon \) and
\[
N = \left[ \frac{h \ln f}{\epsilon} + \frac{\ln f}{\ln \beta} - 1 \right]; \tag{F31}
\]
where \( h \) is the capacity of the symbol. The upper bound in Eq. (120) can be proved using a similar reasoning that leads to Eq. (129), but with \( \tau \delta \) replaced by \( \tau \delta \).
then $N \geq 1$ since
\[
\frac{hF \ln f^{-1} - \ln f}{\epsilon} + \frac{F \ln F}{\epsilon \ln \beta} + \frac{\ln F}{\epsilon \ln \beta} > 1.
\]

Here the second inequality is equivalent to
\[
F \ln F + \epsilon \ln \beta F - \epsilon \beta \ln \beta < 0.
\]

To prove this inequality, note that for a given $0 < \beta < 1$, the left-hand side is maximized when $\beta = F/e$. So
\[
F \ln F + \epsilon \beta \ln F - \epsilon \beta \ln \beta \leq \frac{F(1 - F + \epsilon \ln F)}{e} < 0.
\]

In addition, Lemma 9 implies that
\[
F(N, f, \Omega) \geq \frac{N + 1 - (\ln \beta)^{-1} \ln f}{N + 1 - (\ln \beta)^{-1} \ln f - h \ln f} \geq \frac{hF \epsilon^{-1} \ln f^{-1}}{hF \epsilon^{-1} \ln f^{-1} - h \ln f} = 1 - \epsilon.
\]

In conjunction with Lemma 6 this equation implies that $N(\epsilon, \delta, \Omega) < N$, which confirms the first upper bound in Eq. (125). Furthermore, we have $h > 1/\ln \beta$ since $0 < \beta < 1$ and $|\beta \ln \beta| < |\ln \beta|$. Therefore,
\[
N = \left[ \frac{h(1 - \epsilon) \ln f^{-1}}{\epsilon} + \frac{\ln f}{\ln \beta} - 1 \right] \leq \frac{h \ln f^{-1}}{\epsilon} - h \ln f^{-1} + \frac{\ln f}{\ln \beta} \leq \frac{h \ln f^{-1}}{\epsilon} = \frac{h \ln(F \delta)^{-1}}{\epsilon},
\]

which confirms the second upper bound in Eq. (125).

Equation (126) can be proved using a similar reasoning used to prove the upper bounds in Eq. (125), but with $F \delta$ replaced by $\tau \delta$ and $F(N, f, \Omega)$ replaced by $F(N, \delta, \Omega)$.

Appendix G: Proofs of Lemmas 10-12

**Proof of Lemma 14** By Eqs. (135) and (139) in the main text, it is clear that $p_\nu(\nu', \tau)$ is nondecreasing in $\nu$, and $h_\nu(\nu, 1 - \nu)$ is nonincreasing in $\nu$. If $1 - e^{-1} \leq \nu \leq 1$, then
\[
\nu h_\nu(\nu, 1 - \nu) = \nu \geq e(1 - e^{-1}) = e - 1 > 1,
\]

and $\nu h_\nu(\nu, 1 - \nu)$ is strictly increasing in $\nu$. On the other hand, if $0 < \nu \leq 1 - e^{-1}$, then
\[
\nu h_\nu(\nu, 1 - \nu) \leq \nu(1 - \nu) \ln(1 - \nu)^{-1} = 1,
\]

so that
\[
\lim_{\nu \to 0} \nu h_\nu(\nu, 1 - \nu) = \lim_{\nu \to 0} \nu(1 - \nu) \ln(1 - \nu)^{-1} = 1.
\]

By computing the derivative of $\nu h_\nu(\nu, 1 - \nu)$ over $\nu$ [cf. Eq. (G5) below with $p = 0$], it is straightforward to verify that $\nu h_\nu(\nu, 1 - \nu)$ is strictly increasing in $\nu$ for $0 < \nu \leq 1 - e^{-1}$. In conjunction with Eq. (G1), we conclude that $\nu h_\nu(\nu, 1 - \nu) > 1$ and it is strictly increasing in $\nu$ for $0 < \nu \leq 1$.

In addition,
\[
\nu h(p, \nu, 1 - \nu) = \nu(\beta_p \ln \beta_p^{-1})^{-1},
\]

where $\beta_p = 1 - \nu + \nu \nu$ satisfies $0 < \beta_p < 1$. The derivative of $\nu h(p, \nu, 1 - \nu)$ over $\nu$ reads
\[
\frac{d}{d\nu} \left( \frac{\nu}{\beta_p \ln \beta_p^{-1}} \right) = -\frac{(1 - p)\nu + \ln(1 - \nu + \nu \nu)}{[(1 - \nu + \nu \nu)]^2} > 0,
\]

where the last inequality follows from the simple fact that $\ln(1 + x) < x$ when $x > -1$ and $x \neq 0$. Therefore, $\nu h(p, \nu, 1 - \nu)$ increases strictly monotonically with $\nu$. Incidentally, the derivative in Eq. (G5) approaches $1/2$ in the limit $\nu \to 0$.

**Proof of Lemma 17** We shall prove the seven statements of Lemma 11 in the order $1, 6, 2, 3, 4, 7, 5$.

Recall that $p_\nu(\nu, \tau)$ is the smallest value of $p \geq 0$ that satisfies $\beta_p \geq 1/e$ and $\tau_p \ln \tau_p^{-1} \geq \beta_p \ln \beta_p^{-1}$; see Eq. (137). Let $q = p_\nu(\nu, \tau)$, then $0 \leq q < 1$. Suppose $0 < \nu' < \nu$ and let $\beta' = 1 - \nu' \nu$. Then we have $1 > \beta' > \beta \geq 0$ and $1 > \beta_q > \beta_q \geq 1/e$, so that
\[
\beta_p \ln \beta_p^{-1} < \beta_q \ln \beta_q^{-1} \leq \gamma_q \ln \gamma_q^{-1},
\]

which implies that $p_\nu(\nu', \tau) \leq q = p_\nu(\nu, \tau)$, that is, $p_\nu(\nu, \tau)$ is nondecreasing in $\nu$. If $q > 0$, actually we can deduce a stronger conclusion, namely, $p_\nu(\nu', \tau) < p_\nu(\nu, \tau)$.

In addition, the inequalities $\gamma_p \leq \beta_p \leq \beta_q$ imply that
\[
\beta_p \ln \beta_p^{-1} \geq \min\{\beta_p \ln \beta_q^{-1}, \gamma_p \ln \gamma_q^{-1}\}
\]

and that
\[
h(p, \nu', \tau) = \left[ \min\{\beta_p \ln \beta_p^{-1}, \gamma_p \ln \gamma_q^{-1}\} \right]^{-1} \geq \left[ \min\{\beta_p \ln \beta_q^{-1}, \gamma_q \ln \gamma_q^{-1}\} \right]^{-1} = h(p, \nu, \tau).
\]

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

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

Next, suppose $\tau \leq \tau' \leq \beta$. Then we have $\gamma_q \leq \gamma_q \leq \beta_q$, $\bq \geq 1/e$, and
\[
\gamma_q \ln \gamma_q^{-1} \geq \min\{\beta_q \ln \beta_q^{-1}, \gamma_q \ln \gamma_q^{-1}\} = \beta_q \ln \beta_q^{-1},
\]

which implies that $p_\nu(\nu, \tau') \leq q = p_\nu(\nu, \tau)$. Therefore, $p_\nu(\nu, \tau)$ is nonincreasing in $\tau$, which confirms statement 1.
of Lemma 11 given that $p_*(\nu, \tau)$ is nondecreasing in $\nu$ as shown above.

In addition, the inequalities $\tau_p \leq \tau_p' \leq \beta_p$ imply that

$$\tau_p' \ln \tau_p'^{-1} \geq \min \{ \beta_p \ln \beta_p^{-1}, \tau_p \ln \tau_p^{-1} \}$$  \hspace{1cm} (G11)

and that

$$h(p, \nu, \tau') = \left[ \min \{ \beta_p \ln \beta_p^{-1}, \tau_p' \ln \tau_p'^{-1} \} \right]^{-1} \leq \left[ \min \{ \beta_p \ln \beta_p^{-1}, \tau_p \ln \tau_p^{-1} \} \right]^{-1} = h(p, \nu, \tau). \hspace{1cm} (G12)$$

So $h(p, \nu, \tau)$ is nonincreasing in $\tau$, which confirms statement 6 of Lemma 11 in view of the above conclusion. When $p = p_*(\nu, \tau)$, Eq. (G12) implies that

$$h_*(\nu, \tau) = h(p, \nu, \tau) \geq h(p, \nu, \tau') = h_*(\nu, \tau'). \hspace{1cm} (G13)$$

So $h_*(\nu, \tau)$ is also nonincreasing in $\tau$, which confirms statement 2 of Lemma 11.

Next, consider statements 3 and 4 in Lemma 11. By Lemma 10 and statement 2 in Lemma 11 proved above, we have $\nu h_*(\nu, \tau) \geq \nu h_*(\nu, 1-\nu) > 1$, which confirms statement 3 in Lemma 11. In addition, the following equations

$$\lim_{\nu \to 0} \nu h_*(\nu, \tau') \geq \lim_{\nu \to 0} \nu h_*(\nu, 1-\nu) = 1, \hspace{1cm} (G14)$$

$$\lim_{\nu \to 1} \nu h_*(\nu, \tau) \leq \lim_{\nu \to 1} \nu h(\nu, \nu, \tau) = 1, \hspace{1cm} (G15)$$

imply the equality $\lim_{\nu \to 0} \nu h_*(\nu, \tau') = 1$ and confirm statement 4 in Lemma 11.

Finally, we can prove statements 7 and 5 in Lemma 11. By definition we have

$$\nu h_*(\nu, \nu, \tau) = \max \left\{ \nu \left( \beta_p \ln \beta_p^{-1} \right)^{-1}, \nu \left( \tau_p \ln \tau_p^{-1} \right)^{-1} \right\}, \hspace{1cm} (G16)$$

where $\beta_p = 1 - \nu + \nu \nu$. It is clear that $\nu \left( \tau_p \ln \tau_p^{-1} \right)^{-1}$ increases strictly monotonically with $\nu$. The same conclusion holds for $\nu \left( \beta_p \ln \beta_p^{-1} \right)^{-1}$ according to the derivative in Eq. (G25). Therefore, $\nu h_*(\nu, \nu, \tau)$ increases strictly monotonically with $\nu$, which confirms statement 7 in Lemma 11.

Suppose $0 < \nu' < \nu \leq 1$. Then

$$\nu' h_*(\nu', \nu, \tau) \leq \nu' h(q, \nu', \tau) \leq \nu h(q, \nu, \tau) = \nu h_*(\nu, \nu, \tau), \hspace{1cm} (G17)$$

where $q = p_*(\nu, \tau)$. So $h_*(\nu, \nu, \tau)$ increases strictly monotonically with $\nu$, which confirms statement 5 in Lemma 11.

Proof of Lemma 12. Recalling that $p_*(\nu)$ is the smallest value of $p > \nu$ that satisfies the condition $\beta_p \geq 1/e$ and $\ln p = \beta_p \ln \beta_p$; see Eq. (112). Let $q = p_*(\nu)$; then $0 < q \leq \nu > 1/e$. Suppose $0 < \nu' < \nu$ and let $\beta' = 1 - \nu'$. Then $1 > \beta' > \beta' > 0$ and $1 > \beta' > \beta > 1/e$, so that

$$\beta' \ln \beta'^{-1} < q \ln q^{-1} = q \ln q^{-1} \hspace{1cm} (G18)$$

which implies that $p_*(\nu') < q = p_*(\nu)$ and that $p_*(\nu)$ is strictly increasing in $\nu$. Consequently, $h_*(\nu)$ is strictly decreasing in $\nu$ given that $h_*(\nu) = \left[ p_*(\nu) \ln p_*(\nu)^{-1} \right]^{-1}$ and $0 < p_*(\nu) \leq 1/e$. By contrast, $\nu h_*(\nu)$ is strictly increasing in $\nu$ according to Lemma 11.

Next, let us consider the monotonicity of $h(e^{-\nu} \nu, \nu)$ and $\nu h(e^{-\nu} \nu, \nu)$. By definition we have

$$h(e^{-\nu} \nu, \nu) = \left[ \min \left\{ \beta_{p_0} \ln \beta_{p_0}^{-1}, \nu \ln \frac{e}{\nu} \right\} \right]^{-1}, \hspace{1cm} (G19)$$

$$\nu h(e^{-\nu} \nu, \nu) = \max \left\{ \nu \left( \beta_{p_0} \ln \beta_{p_0}^{-1} \right)^{-1}, e \left( \ln \frac{e}{\nu} \right)^{-1} \right\}, \hspace{1cm} (G20)$$

where $p_0 = \nu/e$ and $\beta_{p_0} = 1 - \nu + (\nu^2)/e$. As $\nu$ increases to 1, $\beta_{p_0}$ decreases strictly monotonically to 1/e, while $\nu/e$ increases strictly monotonically to 1/e. So $h(e^{-\nu} \nu, \nu)$ decreases strictly monotonically with $\nu$.

In addition, $e \left( \ln \frac{e}{\nu} \right)^{-1}$ is strictly increasing in $\nu$ for $0 < \nu \leq 1$. Meanwhile we have

$$\frac{d[\nu \left( \beta_{p_0} \ln \beta_{p_0}^{-1} \right)^{-1}]}{d\nu} = \frac{e \beta_{p_0} - (e - \nu^2) \ln(e \beta_{p_0})}{e^2 \beta_{p_0}^2 (\ln \beta_{p_0})^2}, \hspace{1cm} (G21)$$

where the denominator is positive. The numerator is also positive according to the following equation.

$$e \beta_{p_0} - (e - \nu^2) \ln(e \beta_{p_0}) = e - e\nu + \nu^2 - (e - \nu^2) \ln(e - e\nu + \nu^2) \geq e - e\nu + \nu^2 - (e - \nu^2)(1 - \nu) = (2 - \nu)\nu^2 > 0. \hspace{1cm} (G22)$$

Here the first inequality follows from the inequality below

$$\ln(e - e\nu + \nu^2) \leq 1 - \nu, \hspace{1cm} (G23)$$

which can be proved by inspecting the derivative. Therefore, both $\nu \left( \beta_{p_0} \ln \beta_{p_0}^{-1} \right)^{-1}$ and $e \left( \ln \frac{e}{\nu} \right)^{-1}$ are strictly increasing in $\nu$, which implies that $\nu h(e^{-\nu} \nu, \nu)$ is strictly increasing in $\nu$.

Finally, we are ready to prove Eq. (118). The first inequality there follows from the definition of $h_*(\nu)$. To prove the rest inequalities, note that

$$\ln \beta_{p_0}^{-1} = -\ln(1 - \nu + e^{-\nu} \nu^2) \geq \nu, \hspace{1cm} (G24)$$

$$\beta_{p_0} \ln \beta_{p_0}^{-1} \geq (1 - \nu + e^{-\nu} \nu^2) \nu \hspace{1cm} (G25)$$

by Eq. (G23), where $p_0 = \nu/e$. In addition, it is straightforward to verify the following inequality.

$$p_0 \ln(p_0)^{-1} = \frac{\nu}{e} \ln \frac{e}{\nu} \geq (1 - \nu + e^{-\nu} \nu^2) \nu. \hspace{1cm} (G26)$$

Therefore,

$$\nu h(e^{-\nu} \nu, \nu) \leq (1 - \nu + e^{-\nu} \nu^2)^{-1} \leq 1 + (e - 1)\nu \leq e, \hspace{1cm} (G27)$$

which confirms Eq. (118) in Lemma 12. Here the second inequality follows from the inequality below

$$\nu \left(1 - \nu + e^{-\nu} \nu^2 \right) \leq 1 + e^{-\nu} (1 - \nu)(e^2 - 2e + \nu - e\nu) \geq 1, \hspace{1cm} (G28)$$

given that $0 < \nu \leq 1$. \qed
Appendix H: Proof of Proposition 3

Proof. First consider the bipartite case, let $|\Psi\rangle$ be any bipartite entangled state shared between Alice and Bob. Suppose on the contrary that $|\Psi\rangle$ can be verified by a strategy $\Omega$ for which Alice performs only one projective measurement. Without loss of generality, we may assume that this is a complete projective measurement associated with an orthonormal basis, say $\{|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_d\rangle\}$, where $d$ is the dimension of the Hilbert space of Alice. Let $P_k = |\varphi_k\rangle\langle\varphi_k|$ be the corresponding rank-1 projectors. Then any test operator necessarily has the form $E = \sum_{k=1}^{d} P_k \otimes Q_k$, where $Q_k$ are positive operators on the Hilbert space of Bob that satisfy $0 \leq Q_k \leq 1$. To ensure that the target state can always pass the test, $E$ must satisfy the condition $\langle\Psi|E|\Psi\rangle = 1$.

Let $|\tilde{\psi}_k\rangle = \langle\varphi_k|\Psi\rangle$ be the unnormalized reduced state of Bob when Alice obtains outcome $k$ and $p_k = \langle\tilde{\psi}_k|\tilde{\psi}_k\rangle$ the corresponding probability. Let $|\psi_k\rangle = |\tilde{\psi}_k\rangle/\sqrt{p_k}$ when $p_k > 0$. Then

$$\langle\Psi|E|\Psi\rangle = \sum_k \langle\tilde{\psi}_k|Q_k|\tilde{\psi}_k\rangle \leq \sum_k \langle\tilde{\psi}_k|\tilde{\psi}_k\rangle = \sum_k p_k = 1. \tag{H1}$$

By assumption, this inequality is saturated, which implies that $\langle\psi_k|Q_k|\psi_k\rangle = 1$ whenever $p_k > 0$, in which case $|\psi_k\rangle$ is an eigenstate of $Q_k$ with eigenvalue 1. So all kets $|\varphi_k\rangle \otimes |\psi_k\rangle$ with $p_k > 0$ belong to the pass eigenspace (corresponding to the eigenvalue 1) of each test operator $E$ and thus the pass eigenspace of $\Omega$. Note that the number of outcomes with $p_k > 0$ is at least equal to the Schmidt rank of $|\Psi\rangle$. So the dimension of the pass eigenspace of $\Omega$ is not smaller than the Schmidt rank of $|\Psi\rangle$; in particular, it is not smaller than 2 given that $|\Psi\rangle$ is entangled. Therefore, $|\Psi\rangle$ cannot be verified if Alice performs only one projective measurement; the same conclusion holds if Bob performs only one projective measurement.

In general, the proposition follows from the fact that a multipartite state can also be considered as a bipartite state between one party and the other parties. \qed

[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] M. Hein, J. Eisert, and H. J. Briegel, “Multipart entanglement in graph states,” Phys. Rev. A 69, 062311 (2004).
[4] C. Kruszynska and B. Kraus, “Local entanglability and multipartite entanglement,” Phys. Rev. A 79, 052304 (2009).
[5] R. Qu, J. Wang, Z.-s. Li, and Y.-r. Bao, “Encoding hypergraphs into quantum states,” Phys. Rev. A 87, 022311 (2013).
[6] M. Rossi, M. Huber, D. Bruß, and C. Macchiavello, “Quantum hypergraph states,” New J. Phys. 15, 110322 (2013).
[7] F. E. S. Steinhoff, C. Ritz, N. I. Miklin, and O. Gühne, “Qudit hypergraph states,” Phys. Rev. A 95, 052340 (2017).
[8] 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).
[9] R. Raussendorf and H. J. Briegel, “A one-way quantum computer,” Phys. Rev. Lett. 86, 5188–5191 (2001).
[10] R. Raussendorf, D. E. Browne, and H. J. Briegel, “Measurement-based quantum computation on cluster states,” Phys. Rev. A 68, 022312 (2003).
[11] A. Broadbent, J. Fitzsimons, and E. Kashefi, “Universal blind quantum computation,” in Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (IEEE Computer Society, Washington, DC, USA, 2009) pp. 517–526.
[12] T. Morimae and K. Fujii, “Blind quantum computation protocol in which Alice only makes measurements,” Phys. Rev. A 87, 050301(R) (2013).
[13] M. Hayashi and T. Morimae, “Verifiable measurement-only blind quantum computing with stabilizer testing,” Phys. Rev. Lett. 115, 220502 (2015).
[14] K. Fujii and M. Hayashi, “Verifiable fault tolerance in measurement-based quantum computation,” Phys. Rev. A 96, 030301(R) (2017).
[15] M. Hayashi and M. Hajdušek, “Self-guaranteed measurement-based quantum computation,” Phys. Rev. A 97, 052308 (2018).
[16] Y. Takeuchi, T. Morimae, and M. Hayashi, “Quantum computational universality of hypergraph states with Pauli-X and Z basis measurements,” Sci. Rep. 9, 13585 (2019).
[17] J. Miller and A. Miyake, “Hierarchy of universal entanglement in 2D measurement-based quantum computation,” npj Quantum Inf. 2, 16036 (2016).
[18] T. Morimae, Y. Takeuchi, and M. Hayashi, “Verification of hypergraph states,” Phys. Rev. A 96, 062321 (2017).
[19] M. Gachechiladze, O. Gühne, and A. Miyake, “Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states,” Phys. Rev. A 99, 052304 (2019).
[20] 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.
[21] D. Schlingemann and R. F. Werner, “Quantum error-correcting codes associated with graphs,” Phys. Rev. A 65, 012308 (2001).
[22] 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).
