General framework for verifying pure quantum states in the adversarial scenario

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

[1] *Department of Physics and Center for Field Theory and Particle Physics, Fudan University, Shanghai 200433, China*
[2] *State Key Laboratory of Surface Physics, Fudan University, Shanghai 200433, China*
[3] *Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China*
[4] *Collaborative Innovation Center of Advanced Microstructures, Nanjing 210093, China*
[5] *Graduate School of Mathematics, Nagoya University, Nagoya, 464-8602, Japan*
[6] *Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, 518055, China*
[7] *Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518000, China*
[8] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542, Singapore*

(Received 27 June 2019; published 27 December 2019)

Bipartite and multipartite entangled states are of central interest in quantum information processing and foundational studies. Efficient verification of these states, especially in the adversarial scenario, is a key to various applications, 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 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 verifying pure quantum states in the adversarial scenario by virtue of protocols for the nonadversarial scenario. Thanks to this recipe, the resource cost for verifying an arbitrary pure state in the adversarial scenario is comparable to the counterpart for the nonadversarial scenario, and the overhead is at most three times for high-precision verification. Our recipe can readily be applied to efficiently verify bipartite 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).

DOI: 10.1103/PhysRevA.100.062335

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]. Multipartite entangled states, such as graph states [3] and hypergraph states [4–8], are especially useful in (blind) measurement-based quantum computation (MBQC) [9–19], quantum error correction [20,21], quantum networks [22–24], and foundational studies [25–28]. Another important class of multipartite states, including Dicke states [29,30], are useful in quantum metrology [31]. Furthermore, multipartite states, such as tensor-network states, also have extensive applications in research areas beyond quantum information science, including condensed matter physics [32,33].

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 [34], however, the resource required increases exponentially with the number of qubits. Although compressed sensing [35] and direct fidelity estimation (DFE) [36] can improve the efficiency, the exponential scaling behavior cannot be changed in general. As another alternative, self-testing [15,37,38] 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 [39–43]. 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 [39,40,43–47], Greenberger-Horne-Zeilinger (GHZ) states [48], stabilizer states (including graph states) [13–15,24,43,49], hypergraph states [49], weighted graph states [50], and Dicke states [51]. Moreover, the efficiency of this approach has been demonstrated in experiments [52].

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 [12–16] and quantum networks [22–24]. 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 [18,42]. What is worse,

*zhuhuangjun@fudan.edu.cn

little is known about the resource cost of a given verification strategy to achieve a given precision [42,53]. 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 [39,40,43–47], GHZ states [48], stabilizer states (including graph states) [43,49], hypergraph states [49], weighted graph states [50], and Dicke states [51], 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 stabilizer states, even optimal protocols can be constructed using local projective measurements [45,48]; see Sec. X.

This paper is an extended version of the companion paper [54].[1] 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 in the adversarial scenario and introduce the main figures of merit. 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 multipartite 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 Appendices. In these Appendices, 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].

[1]This work was originally motivated by the verification of qubit and qudit hypergraph states and is contained as a part of the preprint arXiv:1806.05565 (cf. Ref. [49]). However, the general framework of QSV in the adversarial scenario we developed applies to all pure states, not only to hypergraph states. To discuss this topic comprehensively, we finally decided to present these results independently.

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) [43], 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 $|\Psi\rangle$ 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. [43], we assume the fidelity $\langle\Psi|\sigma_j|\Psi\rangle$ either equals 1 for all j or satisfies $\langle\Psi|\sigma_j|\Psi\rangle \leqslant 1-\epsilon$ 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 $\{E_l, 1-E_l\}$ chosen randomly from a set of accessible measurements. The test operator E_l corresponds to passing the test and satisfies the condition $0 \leqslant E_l \leqslant 1$. We assume that the target state $|\Psi\rangle$ can always pass the test, that is, $E_l|\Psi\rangle = |\Psi\rangle$ for each E_l. A verification strategy is characterized by all the tests E_l and the probabilities μ_l for performing these tests.

To determine the maximal probability of failing to reject the bad case, it is convenient to introduce the verification operator $\Omega := \sum_l \mu_l E_l$. As we shall see later, most key properties of a verification strategy are determined by the verification operator Ω, irrespective of how the test operators are constructed. Therefore, Ω 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 Ω with the largest eigenvalue 1. Denote by $\beta(\Omega)$ the second largest eigenvalue of Ω, 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 $\langle\Psi|\sigma_j|\Psi\rangle \leqslant 1-\epsilon$, the maximum probability that σ_j can pass a test on

average is given by

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

where the maximization in the left-hand side runs over all quantum states σ that satisfy the fidelity constraint $\langle\Psi|\sigma|\Psi\rangle \leqslant 1-\epsilon$. Equation (1) was originally derived by PLM [43] for strategies composed of projective tests, but their proof also applies to general strategies with nonprojective tests; see Appendix A for a simpler proof.

After N runs, σ_j in the bad case can pass all tests with probability at most $[1-\nu(\Omega)\epsilon]^N$. This is also the maximum probability that the verification strategy fails to detect the bad case. To achieve significance level δ (confidence level $1-\delta$), that is, $[1-\nu(\Omega)\epsilon]^N \leqslant \delta$, the minimum number of tests is given by [43]

$$N_{\mathrm{NA}}(\epsilon,\delta,\Omega) = \left\lceil \frac{\ln\delta}{\ln[1-\nu(\Omega)\epsilon]} \right\rceil \leqslant \left\lceil \frac{\ln\delta^{-1}}{\nu(\Omega)\epsilon} \right\rceil, \quad (2)$$

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 Ω. Note that a single test is sufficient if

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

According to Eq. (2), the efficiency of the strategy Ω 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

$$N_{\mathrm{NA}}(\epsilon,\delta,\Omega) = \left\lceil \frac{\ln\delta}{\ln(1-\epsilon)} \right\rceil \leqslant \left\lceil \frac{\ln\delta^{-1}}{\epsilon} \right\rceil. \quad (4)$$

In addition, the requirement in Eq. (3) reduces to

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

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 ϵ and δ 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. Aside from the total number N of tests determined by ϵ, δ, 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. II–IX 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 [39,40]. 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 $\mathcal{S}_0$, and impose to our test the condition that the probability of erroneously rejecting states in $\mathcal{S}_0$ is upper bounded by a certain value $\delta' \geqslant 0$. Under this condition, we maximize the probability of detecting a state σ in $\mathcal{S}^{\mathrm{c}}$, where $\mathcal{S}^{\mathrm{c}}$ is the complement of $\mathcal{S}_0$ in the state space. When a test maximizes the probability uniformly for every state σ in $\mathcal{S}^{\mathrm{c}}$, it is called a uniformly most powerful (UMP) test. However, since the detecting probability depends on the state σ, such a test does not exist in general. In this paper, $\mathcal{S}_0$ and δ' are chosen to be $\{|\Psi\rangle\langle\Psi|\}$ and 0, respectively. We consider the case in which the same strategy Ω is applied N times. Since we support the state $|\Psi\rangle$ only when all our outcomes correspond to the pass eigenspace of Ω, our test is UMP in this case.

When the set $\mathcal{S}_0$ is chosen as $\{\sigma \mid \langle\Psi|\sigma|\Psi\rangle \geqslant 1-\epsilon'\}$, and δ' is a nonzero 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. [39,40] 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 σ_j produced by the device are identical to σ, let $F = \langle\Psi|\sigma|\Psi\rangle$ be the fidelity between σ and the target state $|\Psi\rangle$; then we have

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

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

$$\frac{1-\mathrm{tr}(\Omega\sigma)}{1-\tau(\Omega)} \leqslant 1-F \leqslant \frac{1-\mathrm{tr}(\Omega\sigma)}{\nu(\Omega)}. \quad (7)$$

So the passing probability $\mathrm{tr}(\Omega\sigma)$ provides upper and lower bounds for the infidelity (and fidelity). In general, Eqs. (6) and (7) still hold if F and $\mathrm{tr}(\Omega\sigma)$ are replaced by their averages over all σ_j. Note that the inequalities in Eqs. (6) and (7) are saturated when $\tau(\Omega)=\beta(\Omega)$; such a strategy Ω is called *homogeneous* and is discussed in more detail in Sec. VI. In this case, we have

$$1-F = \frac{1-\mathrm{tr}(\Omega\sigma)}{\nu(\Omega)}, \quad F = \frac{\mathrm{tr}(\Omega\sigma)-\beta(\Omega)}{\nu(\Omega)}. \quad (8)$$

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

$$\Delta F = \frac{\sqrt{p(1-p)}}{\nu\sqrt{N}} = \frac{\sqrt{(1-F)(F+\nu^{-1}-1)}}{\sqrt{N}} \leqslant \frac{1}{2\nu\sqrt{N}}, \quad (9)$$

where $p = \mathrm{tr}(\Omega\sigma) = \nu F + \beta \geqslant F$ and N is the number of tests performed. Note that this standard deviation decreases monotonically with ν and N. This conclusion is related to the

testing of binomial distributions discussed in Ref. [40]. When $F \geqslant 1/2$, which is the case of most interest, we also have

$$\Delta F = \frac{\sqrt{p(1-p)}}{\nu\sqrt{N}} \leqslant \frac{\sqrt{F(1-F)}}{\nu\sqrt{N}} \tag{10}$$

given that $p \geqslant F$.

III. VERIFICATION OF PURE STATES: A CRITICAL REEXAMINATION

In this section we reexamine the framework of QSV proposed by PLM [43] 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 $\langle\Psi|\sigma_j|\Psi\rangle \leqslant 1-\epsilon$ for all j [43]. In the independent and identically distributed (i.i.d.) case, all σ_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_l is performed with probability μ_l and $\Omega = \sum_l \mu_l E_l$ 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 $\langle\Psi|\sigma_j|\Psi\rangle \leqslant 1-\epsilon$ 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 σ_j are prepared independently of each other. Note that we do not need the i.i.d. assumption. The variation in σ_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 Ω satisfies

$$\prod_{j=1}^{N} \mathrm{tr}(\Omega\sigma_j) \leqslant [1-\nu(\Omega)\bar{\epsilon}]^N, \tag{11}$$

where $\bar{\epsilon} = \sum_j \epsilon_j/N$ 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 ϵ and significance level δ, which means $[1-\nu(\Omega)\epsilon]^N \leqslant \delta$, the minimum number of tests reads as

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

This formula is identical to the one in Eq. (2), but it does not rely on the unnatural assumption imposed by PLM [43]. 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 1.

$$\prod_{j=1}^{N} \mathrm{tr}(\Omega\sigma_j) \leqslant \prod_{j=1}^{N} [1-\nu(\Omega)\epsilon_j] \leqslant [1-\nu(\Omega)\bar{\epsilon}]^N. \tag{13}$$

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

C. Correlated state preparation

Here, we show that the conclusion in Secs. II A and III B 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 $(|\Psi\rangle\langle\Psi|)^{\otimes N}$ in N runs with probability $0 < a < 1$ and the alternative quantum state $\sigma^{\otimes N}$ with probability $1-a$, where $\langle\Psi|\sigma|\Psi\rangle = 1-\epsilon' < 1$. The reduced state of each party reads as $a(|\Psi\rangle\langle\Psi|) + (1-a)\sigma$ 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. II A or that in Sec. III B. 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. III C. 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 ρ 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 ϵ by performing N tests on other systems. We can randomly choose N systems and apply a verification strategy Ω 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 ρ is permutation invariant without loss of generality.

Suppose the strategy Ω is applied to the first N systems, then the probability that ρ can pass N tests reads as

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

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

$$\sigma'_{N+1} = p_\rho^{-1}\, \mathrm{tr}_{1,2,\ldots,N}[(\Omega^{\otimes N} \otimes 1)\rho], \tag{15}$$

where $\mathrm{tr}_{1,2,\ldots,N}$ means the partial trace over the systems $1, 2, \ldots, N$. The fidelity between σ'_{N+1} and the target state $|\Psi\rangle$ reads as

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

where

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

When $\rho = \sigma^{\otimes(N+1)}$ is a tensor power of the state σ with $0 < \epsilon' = 1 - \langle\Psi|\sigma|\Psi\rangle < 1$, we have $p_\rho \leqslant [1 - \nu(\Omega)\epsilon']^N$, $\sigma'_{N+1} = \sigma$, and $F_\rho = 1 - \epsilon'$. These conclusions coincide with the counterpart for the nonadversarial scenario as expected. The situation is different if ρ 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. III C). If N tests are passed, then the reduced state of party $N+1$ reads as

$$\sigma'_{N+1} = \frac{a|\Psi\rangle\langle\Psi| + b\sigma}{a+b}, \tag{18}$$

where $b := (1-a)[\mathrm{tr}(\Omega\sigma)]^N$ satisfies

$$b \leqslant (1-a)[1 - \nu(\Omega)\epsilon']^N \tag{19}$$

and decreases exponentially with N unless $\mathrm{tr}(\Omega\sigma) = 0$. Therefore, the infidelity $1 - \langle\Psi|\sigma'_{N+1}|\Psi\rangle$ approaches zero exponentially with N even if a is arbitrarily small. If the infidelity is bounded from below $1 - \langle\Psi|\sigma'_{N+1}|\Psi\rangle \geqslant \epsilon$ 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 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 Ω adapted to the adversarial scenario, here we introduce four figures of merit. Define

$$\zeta(N, \delta, \Omega) := \min_\rho\{f_\rho \,|\, p_\rho \geqslant \delta\}, \quad 0 \leqslant \delta \leqslant 1, \tag{20a}$$

$$\eta(N, f, \Omega) := \max_\rho\{p_\rho \,|\, f_\rho \leqslant f\}, \quad 0 \leqslant f \leqslant 1, \tag{20b}$$

$$F(N, \delta, \Omega) := \min_\rho \left\{p_\rho^{-1} f_\rho \middle| p_\rho \geqslant \delta\right\}, \quad 0 < \delta \leqslant 1, \tag{20c}$$

$$\mathcal{F}(N, f, \Omega) := \min_\rho \left\{p_\rho^{-1} f_\rho \middle| f_\rho \geqslant f\right\}, \quad 0 < f \leqslant 1, \tag{20d}$$

where $N \geqslant 1$ is the number of tests performed and the minimization or maximization is taken over permutation-invariant quantum states ρ 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 ρ can pass N tests with significance level at least δ. By definition, $F(N, \delta, \Omega)$ and $\zeta(N, \delta, \Omega)$ are nondecreasing in δ, while $\mathcal{F}(N, f, \Omega)$ and $\eta(N, f, \Omega)$ are nondecreasing in f. A simple upper bound for $F(N, \delta, \Omega)$ can be derived by considering quantum states ρ on $\mathcal{H}^{\otimes(N+1)}$ that can be expressed as tensor powers in Eq. (20c),

which yields

$$F(N,\delta,\Omega)\leqslant \max\left\{0,1-\frac{1-\delta^{1/N}}{\nu(\Omega)}\right\}. \tag{21}$$

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_ρ, f_ρ) for permutation-invariant density matrices ρ 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_ρ, f_ρ are both linear in ρ. 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 $F(N,\delta,\Omega)\geqslant 1-\epsilon$, namely,

$$N(\epsilon,\delta,\Omega):=\min\{N\geqslant 1\,|\,F(N,\delta,\Omega)\geqslant 1-\epsilon\}. \tag{23}$$

Then Eq. (21) implies that

$$N(\epsilon,\delta,\Omega)\geqslant \left\lceil \frac{\ln\delta}{\ln[1-\nu(\Omega)\epsilon]}\right\rceil = N_{\mathrm{NA}}(\epsilon,\delta,\Omega) \tag{24}$$

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 ϵ and δ?

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 Ω for the target state $|\Psi\rangle\in\mathcal{H}$ has spectral decomposition $\Omega=\sum_{j=1}^{D}\lambda_j\Pi_j$, where λ_j are the eigenvalues of Ω arranged in decreasing order $1=\lambda_1>\lambda_2\geqslant\cdots\geqslant\lambda_D\geqslant 0$, and Π_j are mutually orthogonal rank-1 projectors with $\Pi_1=|\Psi\rangle\langle\Psi|$. Here, the second largest eigenvalue $\beta:=\lambda_2$ and the smallest eigenvalue $\tau:=\lambda_D$ deserve special attention because they determine the performance of Ω to a large extent, as we shall see later. Suppose the adversary produces the state ρ on the whole system $\mathcal{H}^{\otimes(N+1)}$, which is permutation invariant (cf. Sec. IV). Without loss of generality, we may assume that ρ is diagonal in the product basis constructed from the eigenbasis of Ω (as determined by the projectors Π_j) since p_ρ, f_ρ, and F_ρ only depend on the diagonal elements of ρ.

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

$$p_\rho=\sum_{\mathbf{k}\in\mathscr{S}_N}c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda}),\quad f_\rho=\sum_{\mathbf{k}\in\mathscr{S}_N}c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda}), \tag{25}$$

$$F_\rho=\frac{f_\rho}{p_\rho}=\frac{\sum_{\mathbf{k}\in\mathscr{S}_N}c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda})}{\sum_{\mathbf{k}\in\mathscr{S}_N}c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda})}, \tag{26}$$

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

$$\begin{aligned}\eta_{\mathbf{k}}(\boldsymbol{\lambda}):=p_{\rho_{\mathbf{k}}}&=\sum_{i|k_i>0}\frac{k_i}{(N+1)}\lambda_i^{k_i-1}\prod_{j\neq i|k_j>0}\lambda_j^{k_j},\\ \zeta_{\mathbf{k}}(\boldsymbol{\lambda}):=f_{\rho_{\mathbf{k}}}&=\frac{k_1}{N+1}\prod_{i|k_i>0}\lambda_i^{k_i}.\end{aligned} \tag{27}$$

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

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

$$F(N,\delta=1,\Omega)=\zeta(N,\delta=1,\Omega)=1, \tag{28}$$

$$\mathcal{F}(N,f=1,\Omega)=\eta(N,f=1,\Omega)=1. \tag{29}$$

By contrast, $\eta_{\mathbf{k}}(\boldsymbol{\lambda})\geqslant\tau^N$, and the lower bound is saturated when $\mathbf{k}=(0,\ldots,0,N+1)$. Accordingly, $p_\rho\geqslant\tau^N$, 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 $(\eta_{\mathbf{k}}(\boldsymbol{\lambda}),\zeta_{\mathbf{k}}(\boldsymbol{\lambda}))$ for all $\mathbf{k}\in\mathscr{S}_N$, which is a polygon, as illustrated in Fig. 1. It should be emphasized that $R_{N,\Omega}$ only depends on the distinct eigenvalues of Ω, but not on their degeneracies (although λ_1 is not degenerate by assumption). The same conclusion also applies to the figures of merit $F(N,\delta,\Omega)$, $\mathcal{F}(N,f,\Omega)$, $\zeta(N,\delta,\Omega)$, and $\eta(N,f,\Omega)$ defined in Eq. (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 $\delta\geqslant\tau^N$ (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 Ω. If Ω' is another verification operator for $|\Psi\rangle$ with $\beta(\Omega')<1$ and

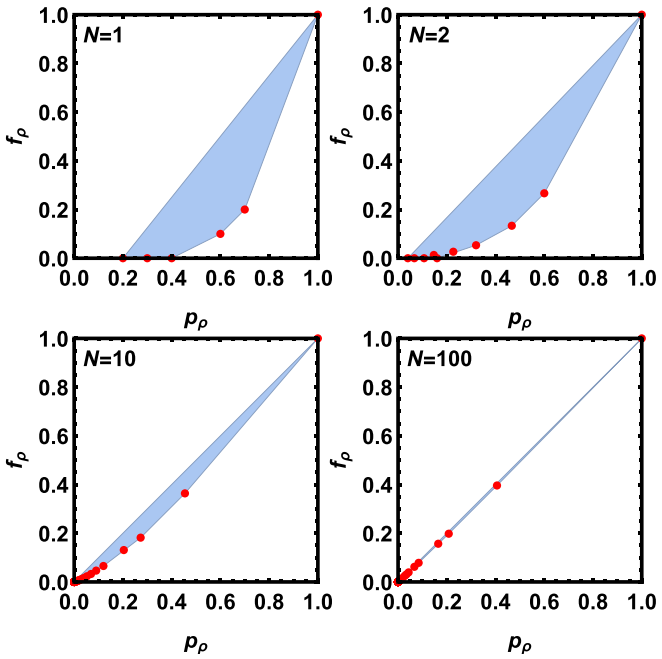

FIG. 1. The region $R_{N,\Omega}$ composed of (p_ρ, f_ρ) as defined in Eq. (22). This region is the convex hull of points $(\eta_{\mathbf{k}}(\boldsymbol{\lambda}), \zeta_{\mathbf{k}}(\boldsymbol{\lambda}))$ for $\mathbf{k} \in \mathscr{S}_N$, which are highlighted as red dots. Here, Ω has three distinct eigenvalues, namely, 1, 0.4, and 0.2.

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

$$F(N,\delta,\Omega') \geqslant F(N,\delta,\Omega), \quad N(\epsilon,\delta,\Omega') \leqslant N(\epsilon,\delta,\Omega). \tag{30}$$

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

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 $\mathcal{F}(N,f,\Omega)$ can be computed by linear programming. Lemmas 1 and 2 below are proved in Appendix B. To start with, we first determine $\eta(N,0,\Omega)$, the maximum of p_ρ under the condition $f_\rho = 0$.

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

$$\delta_{\mathrm{c}} := \begin{cases} \beta^N, & \tau > 0, \\ \max\{\beta^N, 1/(N+1)\}, & \tau = 0. \end{cases} \tag{31}$$

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

$$F(N,\delta,\Omega) = \zeta(N,\delta,\Omega) = 0, \quad 0 < \delta \leqslant \delta_{\mathrm{c}} \tag{32}$$

$$F(N,\delta,\Omega) > 0, \quad \zeta(N,\delta,\Omega) > 0, \quad \delta_{\mathrm{c}} < \delta \leqslant 1. \tag{33}$$

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

Next, we introduce simple alternative definitions of the figures of merit defined in Eq. (20). Define

$$\tilde{\zeta}(N,\delta,\Omega) := \begin{cases} \min_\rho\{f_\rho \,|\, p_\rho = \delta\}, & \delta_{\mathrm{c}} \leqslant \delta \leqslant 1, \\ 0, & 0 \leqslant \delta \leqslant \delta_{\mathrm{c}}, \end{cases} \tag{34a}$$

$$\tilde{\eta}(N,f,\Omega) := \max_\rho\{p_\rho | f_\rho = f\}, \quad 0 \leqslant f \leqslant 1, \tag{34b}$$

$$\tilde{F}(N,\delta,\Omega) := \delta^{-1}\tilde{\zeta}(N,\delta,\Omega), \quad 0 < \delta \leqslant 1, \tag{34c}$$

$$\tilde{\mathcal{F}}(N,f,\Omega) := [\tilde{\eta}(N,f,\Omega)]^{-1} f, \quad 0 < f \leqslant 1. \tag{34d}$$

Here, δ_{c} in Eq. (34a) can be replaced by τ^N given that $\min_\rho\{f_\rho \,|\, p_\rho = \delta\} = 0$ for $\tau^N \leqslant \delta \leqslant \delta_{\mathrm{c}}$.

Lemma 2. Suppose N is a positive integer and Ω is a verification operator. Then

$$\zeta(N,\delta,\Omega) = \tilde{\zeta}(N,\delta,\Omega), \quad 0 \leqslant \delta \leqslant 1, \tag{35a}$$

$$\eta(N,f,\Omega) = \tilde{\eta}(N,f,\Omega), \quad 0 \leqslant f \leqslant 1, \tag{35b}$$

$$F(N,\delta,\Omega) = \tilde{F}(N,\delta,\Omega), \quad 0 < \delta \leqslant 1, \tag{35c}$$

$$\mathcal{F}(N,f,\Omega) = \tilde{\mathcal{F}}(N,f,\Omega), \quad 0 < f \leqslant 1. \tag{35d}$$

For $0 < \delta, f \leqslant 1$, Lemma 2 implies that

$$F(N,\delta,\Omega) = \delta^{-1}\tilde{\zeta}(N,\delta,\Omega) = \delta^{-1}\zeta(N,\delta,\Omega), \tag{36a}$$

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

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. (25) and Lemma 2, $\zeta(N,\delta,\Omega)$ with $\delta_{\mathrm{c}} \leqslant \delta \leqslant 1$ and $\eta(N,f,\Omega)$ with $0 \leqslant f \leqslant 1$ can be computed via linear programming,

$$\zeta(N,\delta,\Omega) = \min_{\{c_{\mathbf{k}}\}} \left\{ \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \middle| \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \delta \right\}, \tag{37a}$$

$$\eta(N,f,\Omega) = \max_{\{c_{\mathbf{k}}\}} \left\{ \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda}) \middle| \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = f \right\}, \tag{37b}$$

where $c_{\mathbf{k}}$ form a probability distribution on $\mathscr{S}_N$. Here, the minimum in Eq. (37a) can be attained at a distribution $\{c_{\mathbf{k}}\}$ that is supported on at most two points in $\mathscr{S}_N$; 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 $(\eta_{\mathbf{k}}(\boldsymbol{\lambda}), \zeta_{\mathbf{k}}(\boldsymbol{\lambda}))$ for some $\mathbf{k} \in \mathscr{S}_N$ (cf. Lemma 14 in Appendix B).

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 $N(\epsilon,\delta,\Omega)$; the proofs are relegated to Appendix B. 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 δ for $0 \leqslant \delta \leqslant 1$ and is strictly increasing for $\delta_{\mathrm{c}} \leqslant \delta \leqslant 1$.

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

(3) $F(N,\delta,\Omega)$ is nondecreasing in δ for $0 < \delta \leqslant 1$ and is strictly increasing for $\delta_{\mathrm{c}} \leqslant \delta \leqslant 1$.

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

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

$$\eta(N, \zeta(N, \delta, \Omega), \Omega) = \max\{\delta, \delta_c\}, \tag{38a}$$

$$\zeta(N, \eta(N, f, \Omega), \Omega) = f. \tag{38b}$$

Lemma 5. Suppose $N \geqslant 2$ and $0 < \delta, f \leqslant 1$. Then

$$\zeta(N, \delta, \Omega) \geqslant \zeta(N-1, \delta, \Omega), \tag{39a}$$

$$F(N, \delta, \Omega) \geqslant F(N-1, \delta, \Omega), \tag{39b}$$

$$\eta(N, f, \Omega) \leqslant \eta(N-1, f, \Omega), \tag{39c}$$

$$\mathcal{F}(N, f, \Omega) \geqslant \mathcal{F}(N-1, f, \Omega). \tag{39d}$$

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

Next, we turn to the figure of merit $N(\epsilon, \delta, \Omega)$ defined in Eq. (23). As an implication of Lemma 3, $N(\epsilon, \delta, \Omega)$ increases monotonically with $1/\epsilon$ and $1/\delta$ as expected. The following lemma provides several equivalent ways for computing $N(\epsilon, \delta, \Omega)$.

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

$$N(\epsilon, \delta, \Omega) = \min\{N \,|\, \zeta(N, \delta, \Omega) \geqslant \delta(1-\epsilon)\} \tag{40}$$

$$= \min\{N \,|\, \eta(N, \delta(1-\epsilon), \Omega) \leqslant \delta\} \tag{41}$$

$$= \min\{N \,|\, \mathcal{F}(N, \delta(1-\epsilon), \Omega) \geqslant (1-\epsilon)\}. \tag{42}$$

Finally, we present a lemma which is useful for comparing the efficiencies of two verification operators. Let $\tilde{\Omega}$ be another verification operator for the same target state as Ω.

Lemma 7. Suppose $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \geqslant \zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \tilde{\Omega})$ for all $\mathbf{k} \in \mathscr{S}_N$. Then

$$\zeta(N, \delta, \Omega) \geqslant \zeta(N, \delta, \tilde{\Omega}), \quad 0 \leqslant \delta \leqslant 1, \tag{43a}$$

$$F(N, \delta, \Omega) \geqslant F(N, \delta, \tilde{\Omega}), \quad 0 < \delta \leqslant 1, \tag{43b}$$

$$N(\epsilon, \delta, \Omega) \leqslant N(\epsilon, \delta, \tilde{\Omega}), \quad 0 < \epsilon, \delta < 1. \tag{43c}$$

Lemma 7 is applicable in particular when the set of distinct eigenvalues of Ω is contained in the counterpart 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) Ω for $|\Psi\rangle$ is *homogeneous* if it has the form

$$\Omega = |\Psi\rangle\langle\Psi| + \lambda(1 - |\Psi\rangle\langle\Psi|), \tag{44}$$

where $0 \leqslant \lambda < 1$. In this case, all eigenvalues of Ω are equal to λ except for the largest one, so we have $\beta = \tau = \lambda$ and $\nu = 1 - \lambda$. Incidentally, the homogeneous strategy Ω can always be realized by performing the test $P = |\Psi\rangle\langle\Psi|$ with probability $1 - \lambda$ and the trivial test with probability λ. By "trivial test" we mean the test operator is 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 λ is sufficiently large (see Sec. X).

In the nonadversarial scenario, a smaller λ achieves a better performance among homogeneous strategies. Here, we clarify what λ is optimal in the adversarial scenario, which turns out to be very different from the nonadversarial scenario.

Given that the homogeneous strategy Ω in Eq. (44) is determined by the parameter λ, it is more informative to express the figures of merit defined in Eqs. (20) and (23) as follows:

$$F(N, \delta, \lambda) := F(N, \delta, \Omega), \tag{45a}$$

$$\mathcal{F}(N, f, \lambda) := \mathcal{F}(N, f, \Omega), \tag{45b}$$

$$\zeta(N, \delta, \lambda) := \zeta(N, \delta, \Omega), \tag{45c}$$

$$\eta(N, f, \lambda) := \eta(N, f, \Omega), \tag{45d}$$

$$N(\epsilon, \delta, \lambda) := N(\epsilon, \delta, \Omega). \tag{45e}$$

Then Lemma 1 implies that

$$\eta(N, 0, \lambda) = \delta_c = \begin{cases} \lambda^N, & \lambda > 0, \\ 1/(N+1), & \lambda = 0. \end{cases} \tag{46}$$

Suppose $\tilde{\Omega}$ is an arbitrary verification operator with eigenvalues $1 = \tilde{\lambda}_1 > \tilde{\lambda}_2 \geqslant \cdots \geqslant \tilde{\lambda}_D \geqslant 0$. Then we have the inequality $F(N, \delta, \tilde{\lambda}_j) \geqslant F(N, \delta, \tilde{\Omega})$ for $2 \leqslant j \leqslant D$ according to Eq. (30). 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 $\mathbb{Z}^{\geqslant 0}$ the set of integers and the set of non-negative integers, respectively. For $k \in \mathbb{Z}^{\geqslant 0}$, define

$$\eta_k(\lambda) := \frac{(N+1-k)\lambda^k + k\lambda^{k-1}}{N+1}, \qquad \zeta_k(\lambda) := \frac{(N+1-k)\lambda^k}{N+1}. \tag{47}$$

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

$$\eta_k(\lambda) = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \quad \zeta_k(\lambda) = \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \tag{48}$$

when $k \in \{0, 1, \ldots, N+1\}$, where $\mathbf{k} = (N+1-k, k)$, $\boldsymbol{\lambda} = (1, \lambda)$, and $\eta_{\mathbf{k}}(\boldsymbol{\lambda})$, $\zeta_{\mathbf{k}}(\boldsymbol{\lambda})$ are defined in Eq. (27). The extension of the definitions of $\eta_k(\lambda)$ and $\zeta_k(\lambda)$ over k to the set $\mathbb{Z}^{\geqslant 0}$ 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. (47) reduces to

$$\eta_k(\lambda) = \begin{cases} 1, & k = 0, \\ (N+1)^{-1}, & k = 1, \\ 0, & k \geqslant 2, \end{cases} \quad \zeta_k(\lambda) = \begin{cases} 1, & k = 0, \\ 0, & k \geqslant 1. \end{cases} \tag{49}$$

By Lemma 2, we have $F(N, \delta, \lambda = 0) = \zeta(N, \delta, \lambda = 0)/\delta$ for $0 < \delta \leqslant 1$, where

$$\zeta(N, \delta, \lambda = 0) = \max\left\{0, \frac{(N+1)\delta - 1}{N}\right\} = \begin{cases} 0, & 0 \leqslant \delta \leqslant (N+1)^{-1}, \\ \frac{(N+1)\delta - 1}{N}, & (N+1)^{-1} \leqslant \delta \leqslant 1. \end{cases} \tag{50}$$

Given $0 < \epsilon, \delta < 1$, the minimum number of tests required to verify the pure state $|\Psi\rangle$ within infidelity ϵ and significance level δ reads as

$$N(\epsilon, \delta, \lambda = 0) = \left\lceil \frac{1-\delta}{\epsilon\delta} \right\rceil. \tag{51}$$

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. (44) is nonsingular (which means the verification operator is positive definite). In this case, $\eta_k(\lambda)$ decreases strictly monotonically with k and $\eta_k(\lambda) > 0$ for $k \in \mathbb{Z}^{\geqslant 0}$; by contrast, $\zeta_k(\lambda)$ decreases strictly monotonically with k and $\zeta_k(\lambda) \geqslant 0$ for $k \in \{0, 1, \ldots, N+1\}$, while $\zeta_k(\lambda) < 0$ for all $k > N+1$. Define

$$c_k(\delta, \lambda) := \frac{\delta - \eta_{k+1}(\lambda)}{\eta_k(\lambda) - \eta_{k+1}(\lambda)}, \tag{52}$$

$$\begin{aligned}\zeta(N, \delta, \lambda, k) &:= c_k(\delta, \lambda)\zeta_k(\lambda) + [1 - c_k(\delta, \lambda)]\zeta_{k+1}(\lambda) \\ &= \frac{\lambda\{\delta[1 + (N-k)\nu] - \lambda^k\}}{\nu(k\nu + N\lambda)},\end{aligned} \tag{53}$$

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 2 for a proof).

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

$$\zeta(N, \delta, \lambda) = \begin{cases} 0, & \delta \leqslant \lambda^N, \\ \zeta(N, \delta, \lambda, k_*), & \delta > \lambda^N, \end{cases} \tag{54}$$

where k_* is the largest integer k that satisfies $\eta_k(\lambda) \geqslant \delta$, that is, $(N+1-k)\lambda^k + k\lambda^{k-1} \geqslant (N+1)\delta$.

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

$$k_+ := \lceil \log_\lambda \delta \rceil, \quad k_- := \lfloor \log_\lambda \delta \rfloor. \tag{55}$$

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

$$F(N, \delta = \lambda^k, \lambda) = \frac{(N-k)\lambda}{k + (N-k)\lambda}, \tag{56}$$

which decreases monotonically with k. In particular, we have $F(N, \delta = 1, \lambda) = 1$ as expected [cf. Eq. (28)]. Furthermore, when $\delta = \eta_k(\lambda)$ with $k \in \{0, 1, \ldots, N+1\}$, we have

$$F(N, \delta = \eta_k(\lambda), \lambda) = \frac{\zeta_k(\lambda)}{\eta_k(\lambda)} = \frac{(N+1-k)\lambda}{k + (N+1-k)\lambda}, \tag{57}$$

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

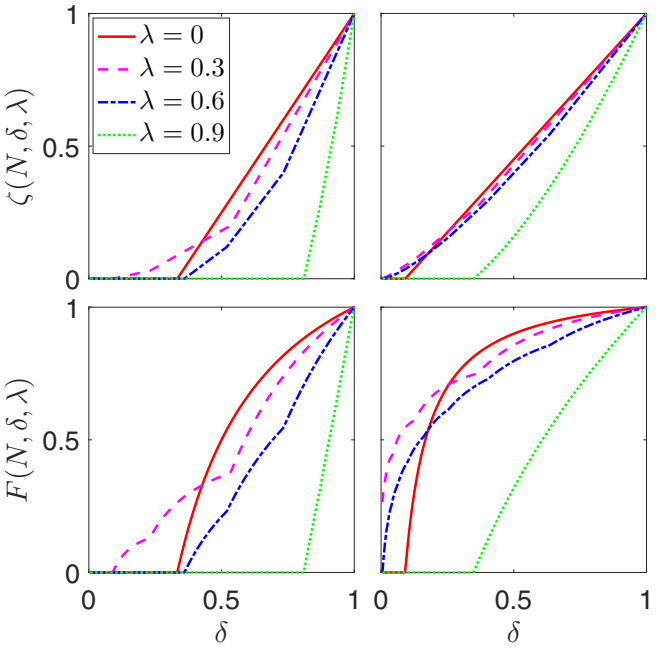

FIG. 2. Variations of $\zeta(N, \delta, \lambda)$ and $F(N, \delta, \lambda)$ with δ and λ for $N = 2$ (left plots) and $N = 10$ (right plots).

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

$$\zeta(N, \delta, \lambda) = \max\left\{0, \max_{k \in \mathbb{Z}^{\geqslant 0}} \zeta(N, \delta, \lambda, k)\right\} \tag{58}$$

$$= \max\{0, \zeta(N, \delta, \lambda, k_+), \zeta(N, \delta, \lambda, k_-)\} \tag{59}$$

$$= \max\left\{0, \max_{k \in \{0,1,\ldots,N\}} \zeta(N, \delta, \lambda, k)\right\}. \tag{60}$$

Corollary 1 follows from Theorem 1 above and Lemma 19 in Appendix C. Equation (58) provides a family of lower bounds for $\zeta(N, \delta, \lambda)$, namely,

$$\zeta(N, \delta, \lambda) \geqslant \zeta(N, \delta, \lambda, k) \quad \forall\, k \in \mathbb{Z}^{\geqslant 0}. \tag{61}$$

Corollary 2. Suppose $0 \leqslant \lambda < 1$. Then $F(N, \delta, \lambda)$ is nondecreasing in δ for $0 < \delta \leqslant 1$ and in N for $N \geqslant 1$.

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

$$\frac{(N-k_+)\lambda}{k_+ + (N-k_+)\lambda} \leqslant F(N, \delta, \lambda) \leqslant \frac{(N-k_-)\lambda}{k_- + (N-k_-)\lambda}. \tag{62}$$

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 the Appendix); alternatively, it is an implication of Lemmas 3 and 5. Corollary 3 is an immediate consequence of Corollary 2 and Eq. (56) given that $\lambda^{k_+} \leqslant \delta \leqslant \lambda^{k_-}$.

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 ϵ and significance level δ in the adversarial scenario. Theorems 2 and 3 below are proved in Appendix C 2. The results

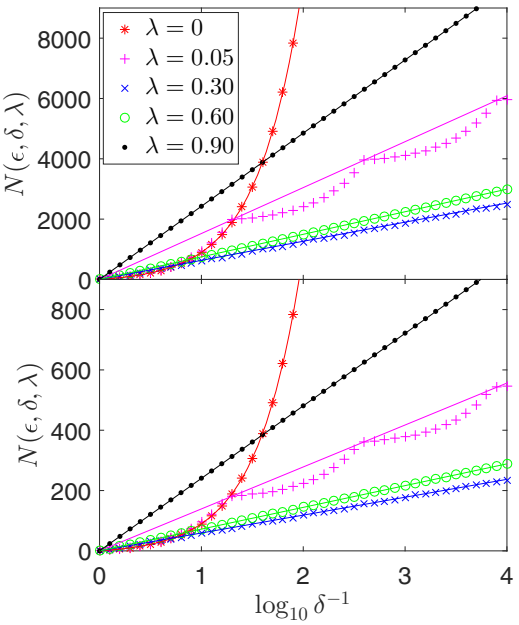

FIG. 3. Minimum numbers of tests required to verify a pure state with five different homogeneous strategies. Here, $\epsilon = 0.01$ in the upper plot and $\epsilon = 0.1$ in the lower plot. In each plot, the red curve represents the approximate formula $(1-\delta)/(\epsilon\delta)$ when $\lambda = 0$ [cf. Eq. (51)]. The four lines represent the approximate formula $(F+\lambda\epsilon)\log_{10}\delta/(\lambda\epsilon\log_{10}\lambda)$ [cf. Eq. (76)].

are illustrated in Figs. 3 and 4. Define

$$\tilde{N}(\epsilon,\delta,\lambda,k) := \frac{k\nu^2\delta F + \lambda^{k+1} + \lambda\delta(k\nu-1)}{\lambda\nu\delta\epsilon}, \tag{63}$$

$$\tilde{N}_\pm(\epsilon,\delta,\lambda) := \tilde{N}(\epsilon,\delta,\lambda,k_\pm), \tag{64}$$

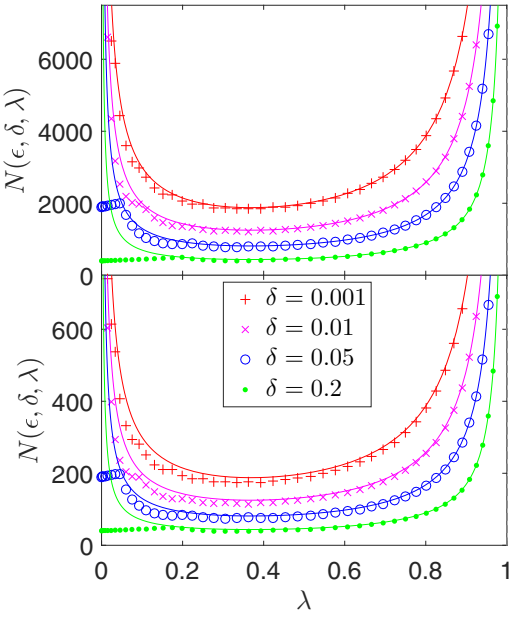

FIG. 4. Variation of $N(\epsilon,\delta,\lambda)$ with λ and δ. Here, $\epsilon = 0.01$ in the upper plot and $\epsilon = 0.1$ in the lower plot. The four curves in each plot represent the approximate formula $\ln\delta/(\lambda\epsilon\ln\lambda)$ [cf. Eqs. (78) and (80)].

where $F = 1-\epsilon$, $\nu = 1-\lambda$, and $k_\pm$ are given in Eq. (55). The main properties of $\tilde{N}(\epsilon,\delta,\lambda,k)$ are summarized in Lemma 20. In particular, $\tilde{N}(\epsilon,\delta,\lambda,k) \leqslant \tilde{N}(\epsilon,\delta,\lambda,k-1)$ iff $\delta \leqslant \lambda^k/(F+\lambda\epsilon)$, assuming that $0<\epsilon,\delta,\lambda<1$ and k is a positive integer.

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

$$N(\epsilon,\delta,\lambda) = \left\lceil \min_{k\in\mathbb{Z}^{\geqslant 0}} \tilde{N}(\epsilon,\delta,\lambda,k) \right\rceil = \lceil \tilde{N}(\epsilon,\delta,\lambda,k^*)\rceil \tag{65}$$

$$= \lceil \min\{\tilde{N}_+(\epsilon,\delta,\lambda), \tilde{N}_-(\epsilon,\delta,\lambda)\}\rceil \tag{66}$$

$$= \begin{cases} \lceil \tilde{N}_-(\epsilon,\delta,\lambda)\rceil, & \delta \geqslant \frac{\lambda^{k_+}}{F+\lambda\epsilon}, \\ \lceil \tilde{N}_+(\epsilon,\delta,\lambda)\rceil, & \delta \leqslant \frac{\lambda^{k_+}}{F+\lambda\epsilon}, \end{cases} \tag{67}$$

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

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

$$N(\epsilon,\delta,\lambda) \leqslant \lceil \tilde{N}(\epsilon,\delta,\lambda,k)\rceil \quad \forall\, k\in\mathbb{Z}^{\geqslant 0}, \tag{68}$$

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

Corollary 4 is an easy consequence of Theorem 2. The two cases $k = 0, 1$ are of special interest:

$$N(\epsilon,\delta,\lambda) \leqslant \lceil \tilde{N}(\epsilon,\delta,\lambda,0)\rceil = \left\lceil \frac{1-\delta}{\nu\epsilon\delta} \right\rceil, \tag{69}$$

$$N(\epsilon,\delta,\lambda) \leqslant \lceil \tilde{N}(\epsilon,\delta,\lambda,1)\rceil = \left\lceil \frac{\nu^2\delta F + \lambda^2 - \lambda^2\delta}{\lambda\nu\delta\epsilon} \right\rceil. \tag{70}$$

If $\lambda/(F+\lambda\epsilon) \leqslant \delta < 1$, then Eq. (69) is saturated, so we have

$$N(\epsilon,\delta,\lambda) = \left\lceil \frac{1-\delta}{\nu\epsilon\delta} \right\rceil. \tag{71}$$

This result also holds when $\lambda = 0$ (as long as $0<\epsilon,\delta<1$) according to Eq. (51). If $\lambda^2/(F+\lambda\epsilon) \leqslant \delta \leqslant \lambda/(F+\lambda\epsilon)$, then Eq. (70) is saturated, so we have

$$N(\epsilon,\delta,\lambda) = \left\lceil \frac{\nu^2\delta F + \lambda^2 - \lambda^2\delta}{\lambda\nu\delta\epsilon} \right\rceil \geqslant \frac{2\sqrt{(1-\delta)F}}{\epsilon\sqrt{\delta}}, \tag{72}$$

where the lower bound is proved in Appendix C 2. Equations (71) and (72) indicate that homogeneous strategies with small λ, say $\lambda \leqslant 0.1$, are not efficient for high-precision QSV (say $\epsilon,\delta \leqslant 0.1$), as reflected in Fig. 4.

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

$$k_- + \left\lceil \frac{k_- F}{\lambda\epsilon} \right\rceil \leqslant N(\epsilon,\delta,\lambda) \leqslant k_+ + \left\lceil \frac{k_+ F}{\lambda\epsilon} \right\rceil, \tag{73}$$

$$N(\epsilon,\delta,\lambda) \leqslant \left\lceil \frac{\log_\lambda\delta}{\lambda\epsilon} - \frac{\nu k_-}{\lambda} \right\rceil = \left\lceil \frac{\ln\delta}{\lambda\epsilon\ln\lambda} - \frac{\nu k_-}{\lambda} \right\rceil. \tag{74}$$

All three bounds in Eqs. (73) and (74) are saturated when $\log_\lambda\delta$ is an integer.

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

$$N(\epsilon,\delta,\lambda) < \frac{\ln\delta}{\lambda\epsilon\ln\lambda}. \tag{75}$$

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

$$\lim_{\delta\to 0}\frac{N(\epsilon,\delta,\lambda)}{\ln\delta^{-1}}=\frac{F+\lambda\epsilon}{\lambda\epsilon\ln\lambda^{-1}}, \tag{76}$$

$$\frac{k_-}{\lambda}\leqslant\lim_{\epsilon\to 0}\epsilon N(\epsilon,\delta,\lambda)\leqslant\frac{k_+}{\lambda}, \tag{77}$$

$$\lim_{\epsilon,\delta\to 0}\frac{\epsilon N(\epsilon,\delta,\lambda)}{\ln\delta^{-1}}=\frac{1}{\lambda\ln\lambda^{-1}}. \tag{78}$$

The exact value of $\lim_{\epsilon\to 0}\epsilon N(\epsilon,\delta,\lambda)$ can be derived by virtue of Eq. (67), with the result

$$\lim_{\epsilon\to 0}\epsilon N(\epsilon,\delta,\lambda)=\lim_{\epsilon\to 0}\epsilon\tilde{N}_-(\epsilon,\delta,\lambda)=\frac{k_-}{\lambda}+\frac{\lambda^{k_-}-\delta}{\nu\delta}. \tag{79}$$

Note that the inequality $\delta\geqslant\lambda^{k_+}/(F+\lambda\epsilon)$ is always satisfied in the limit $\epsilon\to 0$ 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 $\epsilon,\delta\to 0$

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 λ that minimizes $N(\epsilon,\delta,\lambda)$ depends on the target precision, as characterized by ϵ and δ. We cannot find a homogeneous strategy that is optimal for all ϵ and δ, unlike the nonadversarial scenario. Here, we are mostly interested in the high-precision limit, which means $\epsilon,\delta\to 0$.

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

$$N(\epsilon,\delta,\lambda)\approx(\lambda\epsilon)^{-1}\log_\lambda\delta=(\lambda\epsilon\ln\lambda)^{-1}\ln\delta. \tag{80}$$

To understand the condition of this approximation, note that $k_\pm\approx\log_\lambda\delta$ if $\delta\ll\lambda$, which is usually the case in high-precision verification. If in addition $\epsilon\ll 1$, then the ratio of the lower bound over the upper bound in Eq. (73) 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 ranges of interest, as illustrated in Figs. 3 and 4. When λ is very small, the approximation in Eq. (80) is not so good. Such homogeneous strategies are not efficient when $\epsilon,\delta\leqslant 0.1$ as illustrated in Fig. 4 [see also Eqs. (71) and (72)]; in addition, they are not so important due to the reasons explained in Sec. IX later.

Thanks to Theorems 2 and 3, the number of tests required by any nonsingular homogeneous strategy can achieve the same scaling behaviors with ϵ and δ as the counterpart in the nonadversarial scenario for high-precision QSV. In the limit $\epsilon,\delta\to 0$, the efficiency is characterized by the function $(\lambda\ln\lambda^{-1})^{-1}$. Analysis shows that the function $(\lambda\ln\lambda^{-1})^{-1}$ is convex for $0<\lambda<1$ and attains the minimum e when $\lambda=1/\mathrm{e}$, with e being the base of the natural logarithm. It is strictly decreasing in λ when $0<\lambda\leqslant 1/\mathrm{e}$ and strictly increasing when $1/\mathrm{e}\leqslant\lambda<1$ (cf. Fig. 4). Therefore, the homogeneous strategy with $\lambda=1/\mathrm{e}$, that is, $\nu=1-(1/\mathrm{e})$, is optimal in the high-precision limit $\epsilon,\delta\to 0$ if there is no restriction on the accessible measurements. In this case we have

$$N(\epsilon,\delta,\lambda=\mathrm{e}^{-1})\approx\mathrm{e}\epsilon^{-1}\ln\delta^{-1}. \tag{81}$$

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

Although we cannot find a value of λ that is optimal for all ϵ and δ, the optimal value usually lies in a neighborhood, say $[0.32, 0.38]$, of $1/\mathrm{e}$ for the values of ϵ and δ that are of practical interest, say $\epsilon,\delta\leqslant 0.1$. In addition, $N(\epsilon,\delta,\lambda)$ varies quite slowly with λ in this neighborhood, as illustrated in Fig. 4. So, the choice $\lambda=1/\mathrm{e}$ 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 $\delta\to 0$

Here, we discuss briefly the scenario in which $\delta\to 0$, but ϵ is not necessarily so small, which is relevant to entanglement detection [44]. According to Eq. (76), in this case, the performance of the homogeneous strategy Ω is characterized by

$$\mathcal{N}(\epsilon,\lambda):=\lim_{\delta\to 0}\frac{N(\epsilon,\delta,\lambda)}{\ln\delta^{-1}}=\frac{F+\lambda\epsilon}{\lambda\epsilon\ln\lambda^{-1}}, \tag{82}$$

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

$$\frac{\partial\mathcal{N}(\epsilon,\lambda)}{\partial\lambda}=\frac{F+\lambda\epsilon+F\ln\lambda}{\lambda^2\epsilon(\ln\lambda)^2}. \tag{83}$$

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

$$F+\lambda\epsilon+F\ln\lambda=0, \tag{84}$$

which amounts to the equality

$$F=\frac{\lambda}{\ln\lambda^{-1}+\lambda-1}. \tag{85}$$

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

$$\mathrm{e}^{-1}F\leqslant\lambda_*(\epsilon)\leqslant\mathrm{e}^{-1}. \tag{86}$$

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

$$\bar{\mathcal{N}}(\epsilon,\lambda):=\frac{\mathcal{N}(\epsilon,\lambda)}{\mathcal{N}(\epsilon,\mathrm{e}^{-1})}=\frac{F+\lambda\epsilon}{(\mathrm{e}F+\epsilon)\lambda\ln\lambda^{-1}}, \tag{87}$$

$$\bar{\mathcal{N}}_*(\epsilon):=\frac{\mathcal{N}_*(\epsilon)}{\mathcal{N}(\epsilon,\mathrm{e}^{-1})}=\frac{F+\lambda_*(\epsilon)\epsilon}{(\mathrm{e}F+\epsilon)\lambda_*(\epsilon)\ln\lambda_*(\epsilon)^{-1}}. \tag{88}$$

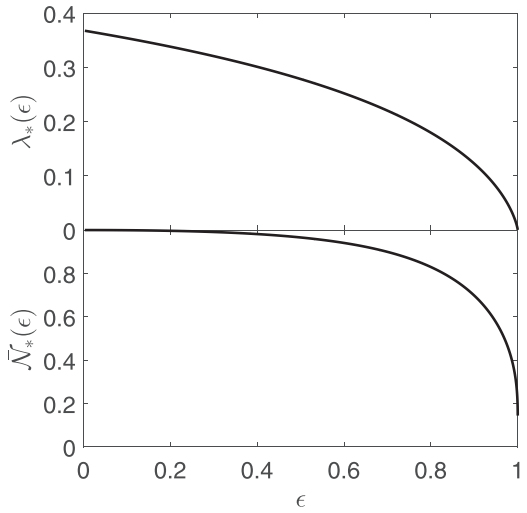

FIG. 5. Optimal homogeneous strategy in the limit $\delta \to 0$. Here $\lambda_*(\epsilon)$ denotes the value of λ that minimizes $\mathcal{N}(\epsilon, \lambda)$ defined in Eq. (82), which determines the number of required tests. $\bar{\mathcal{N}}_*(\epsilon)$ denotes the number of required tests normalized with respect to the benchmark, as defined in Eq. (88).

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

$$\frac{1}{\ln \lambda^{-1}} \leqslant \bar{\mathcal{N}}(\epsilon, \lambda) \leqslant \frac{1}{\mathrm{e}\lambda \ln \lambda^{-1}}. \tag{89}$$

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

$$1 < \frac{1}{\mathrm{e}\lambda \ln \lambda^{-1}} \leqslant \bar{\mathcal{N}}(\epsilon, \lambda) \leqslant \frac{1}{\ln \lambda^{-1}}. \tag{90}$$

Such a homogeneous strategy is less efficient than the benchmark.

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

$$\bar{\mathcal{N}}_*(\epsilon) := \frac{1}{\mathrm{e}\lambda_*(\epsilon) - \ln \lambda_*(\epsilon) - 1}. \tag{91}$$

Given that $\lambda_*(\epsilon) \leqslant \mathrm{e}^{-1}$ and $\lambda_*(\epsilon)$ decreases monotonically with ϵ, we can deduce that $\bar{\mathcal{N}}_*(\epsilon)$ decreases monotonically with ϵ; 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 $\bar{\mathcal{N}}_*(\epsilon)$ could be arbitrarily small when ϵ is large, it is close to 1 when ϵ is not too large. For example, $\bar{\mathcal{N}}_*(\epsilon) \geqslant 0.965$ when $\epsilon \leqslant 0.5$ and $\bar{\mathcal{N}}_*(\epsilon) \geqslant 0.999$ when $\epsilon \leqslant 0.1$. Therefore, the homogeneous strategy Ω with $\beta(\Omega) = 1/\mathrm{e}$ is nearly optimal for most parameter ranges 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 [44,55]. Given a verification strategy Ω, the state $|\Psi\rangle$ can be verified within infidelity $0 < \epsilon < 1$ and significance level $0 < \delta < 1$ using a single test iff

$$F(N = 1, \delta, \Omega) \geqslant 1 - \epsilon. \tag{92}$$

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

$$\zeta(N = 1, \delta, \Omega) \geqslant \delta(1 - \epsilon). \tag{93}$$

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 δ of practical interest usually satisfies $0 < \delta \leqslant 1/2$.

A. Single-copy verification with homogeneous strategies

First, let us consider the homogeneous strategy Ω defined in Eq. (44).

Proposition 2. Suppose $N = 1$ and $0 \leqslant \lambda < 1$; then

$$\zeta(N, \delta, \lambda) = \max\left\{0, \frac{\lambda(\delta - \lambda)}{1 - \lambda}, \frac{\delta(2 - \lambda) - 1}{1 - \lambda}\right\} = \begin{cases} 0, & 0 \leqslant \delta \leqslant \lambda, \\ \frac{\lambda(\delta-\lambda)}{1-\lambda}, & \lambda \leqslant \delta \leqslant \frac{1+\lambda}{2}, \\ \frac{\delta(2-\lambda)-1}{1-\lambda}, & \frac{1+\lambda}{2} \leqslant \delta \leqslant 1. \end{cases} \tag{94}$$

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

$$\max_{\lambda} \zeta(N, \delta, \lambda) = \max\{2 - 2\sqrt{1 - \delta} - \delta,\ 2\delta - 1\} = \begin{cases} 2 - 2\sqrt{1-\delta} - \delta, & 0 \leqslant \delta \leqslant \frac{5}{9}, \\ 2\delta - 1, & \frac{5}{9} \leqslant \delta \leqslant 1. \end{cases} \tag{95}$$

Here, the maximum is attained at

$$\lambda = \begin{cases} 1 - \sqrt{1-\delta}, & 0 \leqslant \delta \leqslant \frac{5}{9}, \\ 0, & \frac{5}{9} \leqslant \delta \leqslant 1. \end{cases} \tag{96}$$

In addition, the optimal solution λ is unique for $0 < \delta < 1$ except when $\delta = \frac{5}{9}$, in which case there are two optimal solutions, namely, $\lambda = 0$ and $\lambda = \frac{1}{3}$. 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 δ and ϵ satisfy the condition

$$\delta(1 - \epsilon) \leqslant \max\{2 - 2\sqrt{1 - \delta} - \delta,\ 2\delta - 1\} \tag{97}$$

or, equivalently, the condition

$$\delta \geqslant \min\left\{\frac{4(1-\epsilon)}{(2-\epsilon)^2}, \frac{1}{1+\epsilon}\right\} = \begin{cases} \frac{1}{1+\epsilon}, & 0 < \epsilon \leqslant \frac{4}{5}, \\ \frac{4(1-\epsilon)}{(2-\epsilon)^2}, & \frac{4}{5} \leqslant \epsilon < 1. \end{cases} \tag{98}$$

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. (5). Equation (98) determines the smallest significance level that can be achieved by a single test to verify the target state

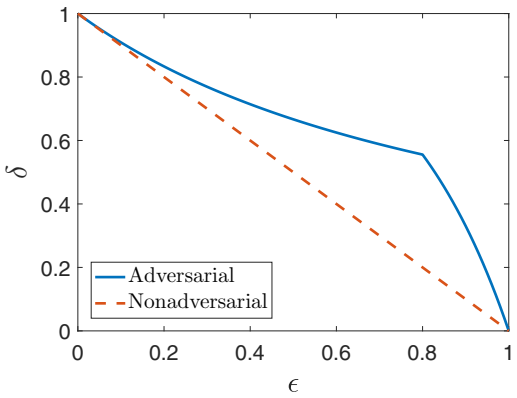

FIG. 6. Single-copy verification in the adversarial scenario and nonadversarial scenario. The target state can be verified within infidelity ϵ and significance level δ in the adversarial (nonadversarial) scenario using a single test if the value of δ lies above the blue solid curve (red dashed line) [cf. Eqs. (98) and (5)].

within infidelity ϵ. Note that the lower bound is monotonically decreasing in ϵ for $0 < \epsilon < 1$ as expected. To achieve significance level $\delta \leqslant 1/2$, the infidelity must satisfy the condition $\epsilon \geqslant 2(\sqrt{2}-1)$. 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 Ω iff Ω is homogeneous and $\beta(\Omega)$ is given by Eq. (96) with $0 < \delta < 1$ or, equivalently,

$$\beta(\Omega) = \lambda = \begin{cases} 0, & 0 < \epsilon \leqslant \frac{4}{5}, \\ \frac{2-2\epsilon}{2-\epsilon}, & \frac{4}{5} \leqslant \epsilon < 1. \end{cases} \tag{99}$$

When $\delta \neq 5/9$ (that is, $\epsilon \neq 4/5$), the optimal strategy Ω is unique as shown Eqs. (96) and (99). 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 4 below).

Corollary 6. Given a homogeneous verification strategy Ω with $\beta(\Omega) = \lambda$, the target state can be verified within infidelity $0 < \epsilon < 1$ and significance level $0 < \delta \leqslant 1/2$ in the adversarial scenario using a single test iff

$$\frac{\lambda(\delta-\lambda)}{1-\lambda} \geqslant \delta(1-\epsilon). \tag{100}$$

This requirement is equivalent to the following conditions:

$$\delta \geqslant \frac{4(1-\epsilon)}{(2-\epsilon)^2}, \tag{101}$$

$$\lambda_- \leqslant \lambda \leqslant \lambda_+, \tag{102}$$

where

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

Equation (100) implies that $0 < \lambda < \delta$. So, any homogeneous verification strategy Ω with $\beta(\Omega) = 0$ or $\beta(\Omega) \geqslant 1/2$ cannot verify the target state within infidelity $0 < \epsilon < 1$ and significance level $0 < \delta \leqslant 1/2$ 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 equation

$$(1-\epsilon)\delta < \lambda_- \leqslant \lambda_+ < \delta. \tag{104}$$

By computing the derivatives over δ and ϵ, it is easy to verify that λ_+ (λ_-) increases (decreases) monotonically with δ and ϵ as expected. If $\delta \leqslant 1/2$, then we have

$$\frac{2-\epsilon-\sqrt{\epsilon^2+4\epsilon-4}}{4} \leqslant \lambda_- \leqslant \lambda_+ \leqslant \frac{2-\epsilon+\sqrt{\epsilon^2+4\epsilon-4}}{4}. \tag{105}$$

B. Single-copy verification with general strategies

Next, we generalize Proposition 2 to an arbitrary verification operator Ω. The following theorem shows that the efficiency of Ω is determined by β and τ, where β and τ denote the second largest and smallest eigenvalues of Ω, respectively. See Appendix D for a proof.

Theorem 4. Suppose $N = 1$. If $\beta \geqslant 1/2$, then

$$\zeta(N,\delta,\Omega) = \begin{cases} 0, & 0 \leqslant \delta \leqslant \beta, \\ \frac{\beta(\delta-\beta)}{1-\beta}, & \beta \leqslant \delta \leqslant \frac{1+\beta}{2}, \\ \frac{\delta(2-\beta)-1}{1-\beta}, & \frac{1+\beta}{2} \leqslant \delta \leqslant 1. \end{cases} \tag{106}$$

If $\beta < 1/2$, then

$$\zeta(N,\delta,\Omega) = \begin{cases} 0, & 0 \leqslant \delta \leqslant \beta, \\ \frac{\tau(\delta-\beta)}{1+\tau-2\beta}, & \beta \leqslant \delta \leqslant \frac{1+\tau}{2}, \\ \delta - \frac{1}{2}, & \frac{1+\tau}{2} \leqslant \delta \leqslant \frac{1+\beta}{2}, \\ \frac{\delta(2-\beta)-1}{1-\beta}, & \frac{1+\beta}{2} \leqslant \delta \leqslant 1. \end{cases} \tag{107}$$

Corollary 7. The target state can be verified by the verification strategy Ω within infidelity $0 < \epsilon < 1$ and significance level $0 < \delta \leqslant 1/2$ using a single test iff

$$0 < \beta < \delta, \quad \frac{\tau(\delta-\beta)}{1+\tau-2\beta} \geqslant \delta(1-\epsilon). \tag{108}$$

Note that the target state cannot be verified within infidelity $0 < \epsilon < 1$ and significance level $0 < \delta \leqslant 1/2$ using a single test if $\beta = 0$ or $\beta \geqslant 1/2$. In contrast, when $0 < \beta < 1/2$ and $\beta \leqslant \delta \leqslant (1+\tau)/2$, we have

$$\frac{\tau(\delta-\beta)}{1+\tau-2\beta} \leqslant \min\left\{\frac{\beta(\delta-\beta)}{1-\beta}, \frac{\tau(\delta-\tau)}{1-\tau}\right\}. \tag{109}$$

So, Eq. (108) implies Eq. (100) with $\lambda = \beta$ or $\lambda = \tau$, which in turn implies Eq. (101) and the sequence of inequalities $\lambda_- \leqslant \tau \leqslant \beta \leqslant \lambda_+$, where $\lambda_\pm$ are defined in Eq. (103). This conclusion is expected given that $\zeta(N,\delta,\Omega) \leqslant \zeta(N,\delta,\beta)$ and $\zeta(N,\delta,\Omega) \leqslant \zeta(N,\delta,\tau)$.

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 Ω of a pure state $|\Psi\rangle$ is mainly determined by its second largest eigenvalue β (or, equivalently, $\nu = 1-\beta$) and the smallest eigenvalue τ.

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 E. 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

$$\delta^* := \frac{1+N\beta}{N+1} = \frac{1+N(1-\nu)}{N+1}. \tag{110}$$

Lemma 8. Suppose Ω is a singular verification operator and $1/(N+1) \leqslant \delta \leqslant \delta^*$. Then

$$F(N,\delta,\Omega) \leqslant 1 - \frac{1}{(N+1)\delta}. \tag{111}$$

Theorem 5. Suppose $0 < \delta \leqslant 1$ and $0 < \nu \leqslant 1$. Then

$$F(N,\delta,\Omega) \geqslant 1 - \frac{1-\delta}{N\nu\delta}, \tag{112}$$

and the inequality is saturated when $\delta^* \leqslant \delta \leqslant 1$. If in addition $\nu \geqslant 1/2$, then

$$F(N,\delta,\Omega) \geqslant 1 - \frac{1}{(N+1)\delta}, \tag{113}$$

and the inequality is saturated when Ω is singular and δ satisfies $1/(N+1) \leqslant \delta \leqslant \delta^*$.

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 $\delta \geqslant \delta^*$, while the second bound is better when $\delta < \delta^*$. The two bounds coincide when $\delta = \delta^*$. The bound in Eq. (113) under the condition $\nu \geqslant 1/2$ was also given in Ref. [13] under a slightly different situation. According to Lemma 8 and Theorem 5, if Ω is singular, then

$$F(N,\delta,\Omega) \leqslant \max\left\{0, 1 - \frac{1-\delta}{N\nu\delta}, 1 - \frac{1}{(N+1)\delta}\right\}. \tag{114}$$

If $\nu \geqslant 1/2$, by contrast, then the above inequality is reversed:

$$F(N,\delta,\Omega) \geqslant \max\left\{0, 1 - \frac{1-\delta}{N\nu\delta}, 1 - \frac{1}{(N+1)\delta}\right\}. \tag{115}$$

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

Corollary 8. Suppose $0 < \epsilon, \delta < 1$ and $0 < \nu \leqslant 1$. Then

$$N(\epsilon,\delta,\Omega) \leqslant \left\lceil \frac{1-\delta}{\nu\delta\epsilon} \right\rceil. \tag{116}$$

If Ω is singular, then

$$N(\epsilon,\delta,\Omega) \geqslant \min\left\{\left\lceil \frac{1-\delta}{\nu\delta\epsilon} \right\rceil, \left\lceil \frac{1}{\delta\epsilon} - 1 \right\rceil\right\}. \tag{117}$$

If $\nu \geqslant 1/2$, then

$$N(\epsilon,\delta,\Omega) \leqslant \min\left\{\left\lceil \frac{1-\delta}{\nu\delta\epsilon} \right\rceil, \left\lceil \frac{1}{\delta\epsilon} - 1 \right\rceil\right\}. \tag{118}$$

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

$$N(\epsilon,\delta,\Omega) = \min\left\{\left\lceil \frac{1-\delta}{\nu\delta\epsilon} \right\rceil, \left\lceil \frac{1}{\delta\epsilon} - 1 \right\rceil\right\}, \tag{119}$$

which generalizes Eq. (51). The number of tests characterized by the upper bound in Eq. (116) 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 Ω is nonsingular. Lemma 9 and Theorem 6 below are proved in Appendix F.

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

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

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

where

$$\begin{aligned} h = h(\Omega) &:= \max_{j\geqslant 2}\left(\lambda_j \ln\lambda_j^{-1}\right)^{-1} \\ &= [\min\{\beta\ \ln\beta^{-1}, \tau\ \ln\tau^{-1}\}]^{-1}. \end{aligned} \tag{122}$$

Define

$$\tilde{\beta} := \begin{cases} \beta, & \beta\ \ln\beta^{-1} \leqslant \tau\ln\tau^{-1}, \\ \tau, & \beta\ \ln\beta^{-1} > \tau\ln\tau^{-1}. \end{cases} \tag{123}$$

Then we have $h = (\tilde{\beta}\ \ln\tilde{\beta}^{-1})^{-1}$. Note that $h > 1/|\ln\beta|$ 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 5.

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 $N(\epsilon,\delta,\Omega) \geqslant N(\epsilon,\delta,\lambda_j)$ for $j = 2,3,\ldots,D$, where λ_j are the eigenvalues of Ω arranged in decreasing order $1 = \lambda_1 > \lambda_2 \geqslant \lambda_3 \geqslant \cdots \geqslant \lambda_D > 0$. The main results are summarized in the following theorem.

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

$$N(\epsilon,\delta,\Omega) \geqslant N(\epsilon,\delta,\lambda_j) \geqslant k_-(\lambda_j) + \left\lceil \frac{k_-(\lambda_j)F}{\lambda_j\epsilon} \right\rceil, \quad j = 2,3,\ldots,D, \tag{124}$$

$$k_-(\tilde{\beta}) + \left\lceil \frac{k_-(\tilde{\beta})F}{\tilde{\beta}\epsilon} \right\rceil \leqslant N(\epsilon,\delta,\Omega) \leqslant \left\lceil \frac{hF\ \ln(F\delta)^{-1}}{\epsilon} + \frac{\ln(F\delta)}{\ln\beta} - 1 \right\rceil < \frac{h\ \ln(F\delta)^{-1}}{\epsilon}, \tag{125}$$

$$N(\epsilon, \delta, \Omega) \leqslant \left\lceil \frac{hF\ \ln(\tau\delta)^{-1}}{\epsilon} + \frac{\ln(\tau\delta)}{\ln\beta} - 1 \right\rceil < \frac{h\ \ln(\tau\delta)^{-1}}{\epsilon}, \tag{126}$$

where we have $F = 1 - \epsilon$, $k_-(\lambda_j) = \lfloor (\ln\delta)/\ln\lambda_j \rfloor$, and $k_-(\tilde{\beta}) = \lfloor (\ln\delta)/\ln\tilde{\beta} \rfloor$.

The upper bounds in Eq. (125) are worse than those in Eq. (126) if $F < \tau = \tau(\Omega)$, while they are better if $F > \tau$, which is usually the case for high-precision verification. Suppose τ 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

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

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

$$N(\epsilon, \delta, \Omega) \approx \frac{h\ \ln\delta^{-1}}{\epsilon} = \frac{\ln\delta}{\epsilon\tilde{\beta}\ \ln\tilde{\beta}}. \tag{128}$$

The number of tests has the same scaling behaviors with ϵ^{-1} and δ^{-1} as the counterpart for the nonadversarial scenario presented in Eqs. (2) and (12), except for an overhead characterized by νh. However, Ω is not efficient when τ is too small according to Eq. (124) as well as Eqs. (71) and (72). In addition, the scaling behavior with δ^{-1} would be worse if Ω were singular according to Eq. (117).

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 $E_l P = P$, and redefine f_ρ as $\mathrm{tr}[(\Omega^{\otimes N} \otimes P)\rho]$. 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. VIII, the number $N(\epsilon, \delta, \Omega)$ of tests required to verify a pure state in the adversarial scenario has the same scaling behavior with ϵ^{-1} and δ^{-1} as the counterpart for the nonadversarial scenario as long as the verification operator Ω is nonsingular, and its smallest eigenvalue τ is bounded from below by a positive constant. However, the scaling behavior of $N(\epsilon, \delta, \Omega)$ with δ is suboptimal when Ω is singular, that is, $\tau = 0$. Similarly, the efficiency is limited when τ 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 Ω is a verification operator for the pure state $|\Psi\rangle$. Based on Ω, we can construct a new verification operator as follows:

$$\Omega_p = (1 - p)\Omega + p, \quad 0 \leqslant p < 1, \tag{129}$$

which means the trivial test is performed with probability p and Ω is performed with probability $1 - p$. Denote by β_p and τ_p the second largest eigenvalue and smallest eigenvalue of Ω_p, respectively. Then

$$\beta_p = (1 - p)\beta + p = 1 - \nu + p\nu, \quad \tau_p = (1 - p)\tau + p, \tag{130}$$

where β and τ are the second largest eigenvalue and smallest eigenvalue of Ω, which satisfy the inequality $\tau \leqslant \beta$. Here we view β_p as a function of $\nu = 1 - \beta$ and p. The spectral gap of Ω_p reads as

$$\nu_p = 1 - \beta_p = (1 - p)\nu. \tag{131}$$

According to Secs. II and III, the trivial test can only decrease the efficiency in the nonadversarial scenario. In high-precision verification, for example, the number of tests required by Ω_p is about $1/(1 - p)$ times the number required by Ω 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 Ω. Therefore, Ω_p is called a *hedged verification operator* of Ω.

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

$$N(\epsilon, \delta, \Omega_p) < \frac{h(p, \nu, \tau)\ln(F\delta)^{-1}}{\epsilon}, \tag{132}$$

where $F = 1 - \epsilon$ and

$$h(p, \nu, \tau) = h(\Omega_p) = \left[\min\left\{\beta_p \ln\beta_p^{-1}, \tau_p \ln\tau_p^{-1}\right\}\right]^{-1}. \tag{133}$$

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

$$\frac{N(\epsilon, \delta, \Omega_p)}{N_{\mathrm{NA}}(\epsilon, \delta, \Omega)} < \nu h(p, \nu, \tau)\frac{[\ln(1 - \nu\epsilon)^{-1}]\ln(F\delta)}{\nu\epsilon\ \ln\delta}. \tag{134}$$

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 10 and 11 below. When ϵ and δ approach zero, the bound in Eq. (132) becomes tight (with respect to the relative deviation) according to Eqs. (125) and (127), so we have

$$\lim_{\epsilon,\delta\to 0} \frac{N(\epsilon, \delta, \Omega_p)}{N_{\mathrm{NA}}(\epsilon, \delta, \Omega)} = \nu h(p, \nu, \tau). \tag{135}$$

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.

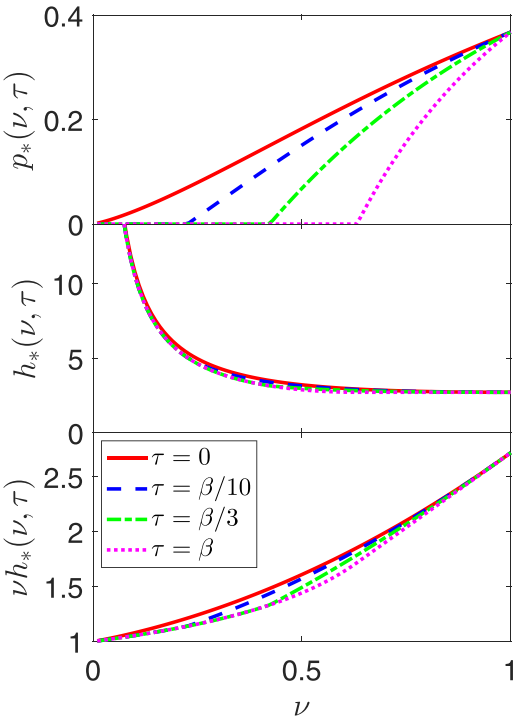

FIG. 7. The optimal probability $p_*(\nu,\tau)$ for performing the trivial test (upper plot), the prefactor $h_*(\nu,\tau)$ (middle plot), and the overhead $\nu h_*(\nu,\tau)$ (lower plot) for high-precision QSV in the adversarial scenario. In the legend, $\beta=1-\nu$.

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 $x\ln x^{-1}$ is concave in the interval $0\leqslant x\leqslant 1$ and is strictly increasing in x when $0\leqslant x\leqslant 1/\mathrm{e}$, while it is strictly decreasing when $1/\mathrm{e}\leqslant x\leqslant 1$; it attains the maximum $1/\mathrm{e}$ when $x=1/\mathrm{e}$. Given the value of $\nu=1-\beta$ and τ with $\nu+\tau\leqslant 1$, 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

$$h_*(\nu,\tau):=\min_{0\leqslant p<1} h(p,\nu,\tau)=h(p_*,\nu,\tau). \tag{136}$$

In addition, it is straightforward to verify that

$$p_*=\min\left\{p\geqslant 0|\beta_p\geqslant \mathrm{e}^{-1}\text{ and }\tau_p\ln\tau_p^{-1}\geqslant\beta_p\ln\beta_p^{-1}\right\}. \tag{137}$$

Here, the condition $\beta_p\geqslant\mathrm{e}^{-1}$ is required when $\tau=\beta$ (so that Ω is a homogeneous strategy), but is redundant when $\tau<\beta$. Equation (137) implies that $\beta_{p_*}\geqslant 1/\mathrm{e}$; by contrast, $\tau_{p_*}\leqslant 1/\mathrm{e}$ if $\tau\leqslant 1/\mathrm{e}$.

When the verification strategy Ω is homogeneous, that is, when $\tau=\beta=1-\nu$, we have

$$p_*(\nu,1-\nu)=\begin{cases}0, & 0<\nu\leqslant 1-\frac{1}{\mathrm{e}},\\ \frac{\mathrm{e}\nu-\mathrm{e}+1}{\mathrm{e}\nu}, & 1-\frac{1}{\mathrm{e}}\leqslant\nu\leqslant 1;\end{cases} \tag{138}$$

$$h_*(\nu,1-\nu)=\begin{cases}(\beta\ln\beta^{-1})^{-1}, & 0<\nu\leqslant 1-\frac{1}{\mathrm{e}},\\ \mathrm{e}, & 1-\frac{1}{\mathrm{e}}\leqslant\nu\leqslant 1.\end{cases} \tag{139}$$

In this case Ω_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_*, but it is very easy to determine p_* numerically.

B. Properties of hedged verification strategies

To determine the overhead of QSV in the adversarial scenario, we need to clarify the properties of $h(p,\nu,\tau)$, $h_*(\nu,\tau)$, and $p_*(\nu,\tau)$, which determine the performances of the hedged verification strategies Ω_p and Ω_{p_*}. 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,

$$h(p,\nu,\tau)\geqslant\mathrm{e}, \tag{140}$$

and the bound is saturated iff $\tau_p=\beta_p=1/\mathrm{e}$, that is, $\tau=1-\nu\leqslant 1/\mathrm{e}$ and $p=(\mathrm{e}\nu-\mathrm{e}+1)/(\mathrm{e}\nu)$ [cf. Eqs. (138) and (139)].

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

Lemma 11. Suppose ν and τ satisfy the following conditions $0<\nu\leqslant 1$, $0\leqslant\tau<1$, and $\nu+\tau\leqslant 1$. Then

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

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

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

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

When $p_*(\nu,\tau)\leqslant p\leqslant p_*(\nu):=p_*(\nu,0)$, Lemma 11 implies that

$$h_*(\nu,1-\nu)\leqslant h_*(\nu,\tau)\leqslant h(p,\nu,\tau)\leqslant h(p_*(\nu),\nu,\tau)=h_*(\nu), \tag{141}$$

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

$$p_*(\nu,1-\nu)\leqslant p_*(\nu,\tau)\leqslant p_*(1-\tau,\tau)\leqslant 1/\mathrm{e}. \tag{142}$$

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, $p_*(\nu,\tau)$ can attain the upper bound $1/\mathrm{e}$ iff $\nu=1$ and $\tau=0$, in which case the verification operator is homogeneous and singular. As a corollary, we have the

result $1/[1-p_*(\nu,\tau)] \leqslant \mathrm{e}/(\mathrm{e}-1) < 1.6$, so the number of tests required by Ω_{p_*} is at most 60% more than the number required by Ω for high-precision verification in the nonadversarial scenario although here we are mainly interested in the adversarial scenario. By contrast, Lemma 11 and Eq. (139) yield a lower bound for $h_*(\nu,\tau)$,

$$h_*(\nu,\tau) \geqslant \begin{cases} (\beta \ln \beta^{-1})^{-1}, & 0 < \nu \leqslant 1-\frac{1}{\mathrm{e}}, \\ \mathrm{e}, & 1-\frac{1}{\mathrm{e}} \leqslant \nu \leqslant 1, \end{cases} \tag{143}$$

where $\beta = 1-\nu$.

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

$$p_*(\nu,\tau) = 0, \quad h_*(\nu,\tau) = (\beta \ln \beta^{-1})^{-1}. \tag{144}$$

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

$$\beta_p \ln \beta_p = \tau_p \ln \tau_p, \quad 0 < p < 1. \tag{145}$$

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 τ is too small.

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

$$p_* = \min\{p > 0 | \beta_p \geqslant \mathrm{e}^{-1} \text{ and } p \ln p = \beta_p \ln \beta_p\}. \tag{146}$$

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

$$p_0 = p_0(\nu) = \frac{\nu}{\mathrm{e}} = \frac{1-\beta}{\mathrm{e}}, \tag{147}$$

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

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

$$\begin{aligned} \nu h_*(\nu) &\leqslant \nu h(\mathrm{e}^{-1}\nu,\nu) \leqslant (1-\nu+\mathrm{e}^{-1}\nu^2)^{-1} \\ &\leqslant 1+(\mathrm{e}-1)\nu \leqslant \mathrm{e}. \end{aligned} \tag{148}$$

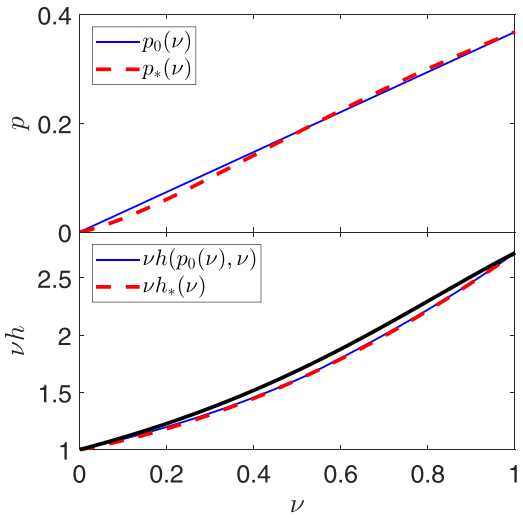

FIG. 8. The optimal probability $p_*(\nu)$ for performing the trivial test in high-precision QSV and a pretty-good approximation $p_0(\nu) = \nu/\mathrm{e}$ (upper plot). Variations of $\nu h_*(\nu)$ and its upper bound $\nu h(p_0(\nu),\nu)$ with ν (lower plot). The black solid curve in the lower plot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

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

$$\begin{aligned} \nu h_*(\nu,\tau) &\leqslant \nu h(p,\nu,\tau) \leqslant \nu h_*(\nu) \leqslant \nu h(\mathrm{e}^{-1}\nu,\nu) \\ &\leqslant (1-\nu+\mathrm{e}^{-1}\nu^2)^{-1} \leqslant 1+\mathrm{e}\nu-\nu \leqslant \mathrm{e}. \end{aligned} \tag{149}$$

In addition, we have $h(\mathrm{e}^{-1}\nu,\nu,\tau) \leqslant h(\mathrm{e}^{-1}\nu,\nu)$ 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 Ω is a verification operator for $|\Psi\rangle$, $\nu = \nu(\Omega)$, and $\tau = \tau(\Omega)$. If $p = \nu/\mathrm{e}$, then

$$N(\epsilon,\delta,\Omega_p) < \frac{h(\mathrm{e}^{-1}\nu,\nu,\tau)\ln(F\delta)^{-1}}{\epsilon} \leqslant \frac{h(\mathrm{e}^{-1}\nu,\nu)\ln(F\delta)^{-1}}{\epsilon} \leqslant \frac{\ln(F\delta)^{-1}}{(1-\nu+\mathrm{e}^{-1}\nu^2)\nu\epsilon} \leqslant \frac{(1+\mathrm{e}\nu-\nu)\ln(F\delta)^{-1}}{\nu\epsilon}, \tag{150}$$

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

$$N(\epsilon,\delta,\Omega_p) < \frac{h(p,\nu,\tau)\ln(F\delta)^{-1}}{\epsilon} \leqslant \frac{h_*(\nu)\ln(F\delta)^{-1}}{\epsilon} \leqslant \frac{h(\mathrm{e}^{-1}\nu,\nu)\ln(F\delta)^{-1}}{\epsilon} \leqslant \frac{\ln(F\delta)^{-1}}{(1-\nu+\mathrm{e}^{-1}\nu^2)\nu\epsilon}. \tag{151}$$

In conjunction with Eq. (12) [see also Eqs. (134) and (149)], Theorem 7 sets a general upper bound on the overhead of QSV in the adversarial scenario. If $p = \nu/\mathrm{e}$ or $p_*(\nu,\tau) \leqslant p \leqslant p_*(\nu)$, for example, then

$$\frac{N(\epsilon,\delta,\Omega_p)}{N_{\mathrm{NA}}(\epsilon,\delta,\Omega)} < \nu h(\mathrm{e}^{-1}\nu,\nu)\frac{[\ln(1-\nu\epsilon)^{-1}]\ln(F\delta)}{\nu\epsilon\ln\delta} \leqslant \frac{[\ln(1-\nu\epsilon)^{-1}]\ln(F\delta)}{(1-\nu+\mathrm{e}^{-1}\nu^2)\nu\epsilon\ln\delta} \leqslant \frac{(1+\mathrm{e}\nu-\nu)[\ln(1-\nu\epsilon)^{-1}]\ln(F\delta)}{\nu\epsilon\ln\delta}. \tag{152}$$

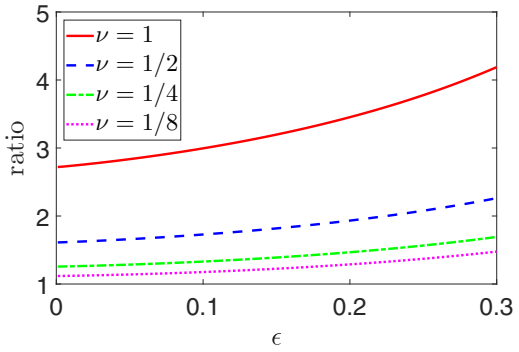

FIG. 9. Upper bound on the ratio of $N(\epsilon, \delta, \Omega_p)$ over $N_{\mathrm{NA}}(\epsilon, \delta, \Omega)$ according to the first bound in Eq. (152) with $\delta = \epsilon$, where $p = \nu/\mathrm{e}$ or $p_*(\nu, \tau) \leqslant p \leqslant p_*(\nu)$. This ratio characterizes the overhead of QSV in the adversarial scenario.

By virtue of Lemmas 10 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. 7–9. Theorem 7 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 ϵ^{-1} and δ^{-1} as the counterpart for the nonadversarial scenario presented in Eqs. (2) and (12). The overhead is at most four times when $\epsilon, \delta \leqslant 1/4$ and three times when $\epsilon, \delta \leqslant 1/10$; furthermore, the overhead becomes negligible when ν, ϵ, δ 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 Ω is very sensitive to the smallest eigenvalue τ, surprisingly, the performance of Ω_{p_*} is not sensitive to τ at all. According to Lemma 11, the difference between $h_*(\nu, \tau_1)$ and $h_*(\nu, \tau_2)$ for a given ν is maximized when $\tau_1 = 0$ [in which case $h_*(\nu, \tau_1) = h_*(\nu)$, cf. Eq. (148)] and $\tau_2 = 1 - \nu$ [cf. Eq. (139)]. Calculation shows that the difference between $h_*(\nu)$ and $h_*(\nu, 1-\nu)$ is less than 12%, and it is even smaller when ν is close to zero or close to 1, as illustrated in Fig. 7. Therefore, the influence of τ on the performance of Ω_{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 τ, while achieving nearly optimal performance. Actually, both the choices $p = p_*(\nu)$ and $p = p_0(\nu) = \nu/\mathrm{e}$ are nearly optimal. These observations are very helpful to constructing efficient verification protocols for the adversarial scenario because we can focus on ν without worrying about the impact of τ or even knowing the value of τ. Suppose Ω is a verification operator with the largest possible ν (under given conditions), then Ω_p is guaranteed to be nearly optimal, where p can be chosen to be $p_*(\nu, \tau)$, $p_*(\nu)$, or $p_0(\nu) = \nu/\mathrm{e}$. Without this insight, it would be much more difficult to devise efficient verification protocols.

X. APPLICATIONS

Our recipe presented in Sec. IX 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 [44,45,48–50]. The main results are summarized in Table I. 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

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 ϵ and significance level δ in the nonadversarial scenario (N_{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_{NA}	N
Maximally entangled states	$\frac{d}{d+1}$	yes	$\lceil \frac{d+1}{d}\epsilon^{-1} \ln \delta^{-1} \rceil$	$\lceil \mathrm{e}\epsilon^{-1} \ln \delta^{-1} \rceil$
Bipartite pure states	$\frac{2}{3}$	yes	$\lceil \frac{3}{2}\epsilon^{-1} \ln \delta^{-1} \rceil$	$\lceil \mathrm{e}\epsilon^{-1} \ln \delta^{-1} \rceil$
GHZ states	$\frac{d}{d+1}$	yes	$\lceil \frac{d+1}{d}\epsilon^{-1} \ln \delta^{-1} \rceil$	$\lceil \mathrm{e}\epsilon^{-1} \ln \delta^{-1} \rceil$
Qubit stabilizer states	$\frac{1}{2}$	yes	$\lceil 2\epsilon^{-1} \ln \delta^{-1} \rceil$	$\lceil 2(\ln 2)^{-1}\epsilon^{-1} \ln \delta^{-1} \rceil$
Qudit stabilizer states (d odd prime)	$\frac{d-1}{d}$	yes	$\lceil \frac{d}{d-1}\epsilon^{-1} \ln \delta^{-1} \rceil$	$\lceil \mathrm{e}\epsilon^{-1} \ln \delta^{-1} \rceil$
Hypergraph state $\lvert G\rangle$	$\chi(G)^{-1}$	no	$\lceil \chi(G)\epsilon^{-1} \ln \delta^{-1} \rceil$	$\lfloor [\chi(G) + \mathrm{e} - 1]\epsilon^{-1} \ln \delta^{-1} \rfloor$
Weighted graph state $\lvert G\rangle$	$\chi(G)^{-1}$	no	$\lceil \chi(G)\epsilon^{-1} \ln \delta^{-1} \rceil$	$\lfloor [\chi(G) + \mathrm{e} - 1]\epsilon^{-1} \ln \delta^{-1} \rfloor$
Dicke states ($n = 3$)	$\frac{1}{3}$	no	$\lceil 3\epsilon^{-1} \ln \delta^{-1} \rceil$	$\lfloor 4.1\epsilon^{-1} \ln \delta^{-1} \rfloor$
Dicke states ($n \geqslant 4$)	$(n-1)^{-1}$	no	$\lceil (n-1)\epsilon^{-1} \ln \delta^{-1} \rceil$	$\lfloor (n + \mathrm{e} - 2)\epsilon^{-1} \ln \delta^{-1} \rfloor$

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 toward 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], stabilizer states (including graph states) [43,49], hypergraph states [49], 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

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle \tag{153}$$

up to some local unitary transformations. According to Refs. [39,44], the maximum spectral gap of any verification strategy Ω based on LOCC or separable measurements is

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

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

$$N_{\mathrm{NA}} = \left\lceil \frac{\ln \delta}{\ln[1 - d(d+1)^{-1}\epsilon]} \right\rceil \leqslant \left\lceil \frac{d+1}{d\epsilon} \ln \delta^{-1} \right\rceil. \tag{155}$$

Here, the upper bound is nearly tight when ϵ is small, so we will neglect such small difference in favor of a simpler expression in the following discussions. In addition, the verification operator Ω 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 as

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

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

By adding the trivial test with a suitable probability, any homogeneous strategy Ω with $\nu(\Omega) \leqslant d/(d+1)$ [that is, $\beta(\Omega) \geqslant 1/(d+1)$] can be constructed using LOCC. In particular, we can construct a homogeneous strategy Ω with $\beta(\Omega) = 1/\mathrm{e}$, which is optimal for high-precision verification in the adversarial scenario according to Sec. VI. Then the number of required tests satisfies

$$N \leqslant \lceil \mathrm{e}\epsilon^{-1} \ln \delta^{-1} \rceil \tag{157}$$

by Theorem 3. When $\delta \leqslant 1/\mathrm{e}$, the above bound can be strengthened by Eq. (75), which yields $N < \mathrm{e}\epsilon^{-1} \ln \delta^{-1}$. This bound is nearly tight in the high-precision limit.

Equations (154)–(157) above also apply to the n-qudit GHZ state for $n \geqslant 3$ 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 Ω with spectral gap $(1 + s_0 s_1)^{-1}$, which attains the maximum over separable measurements [46]. For a general bipartite pure state, the spectral gap achievable so far is [45,47]

$$\nu(\Omega) = \frac{2}{2 + s_0^2 + s_1^2} \geqslant \frac{2}{3}. \tag{158}$$

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

$$N_{\mathrm{NA}} = \left\lceil \frac{2 + s_0^2 + s_1^2}{2\epsilon} \ln \delta^{-1} \right\rceil \leqslant \left\lceil \frac{3}{2\epsilon} \ln \delta^{-1} \right\rceil. \tag{159}$$

Moreover, this strategy can be turned into a homogeneous strategy with the same spectral gap [45], which is useful for fidelity estimation by Eqs. (8) and (9). The standard deviation of this estimation satisfies

$$\Delta F = \frac{\sqrt{p(1-p)}}{\nu(\Omega)\sqrt{N}} \leqslant \frac{\sqrt{(1-F)(F+2^{-1})}}{\sqrt{N}}, \tag{160}$$

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

By adding the trivial test with a suitable probability, any homogeneous strategy Ω with $\nu(\Omega) \leqslant 2/(2 + s_0^2 + s_1^2)$ can be constructed using LOCC [45]. In particular, we can construct a homogeneous strategy Ω with $\beta(\Omega) = 1/\mathrm{e}$ [that is, $\nu(\Omega) = 1 - (1/\mathrm{e})$], 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 [37,38,58], which is different from what we consider here.

D. Stabilizer states

For stabilizer states, which are equivalent to graph states under local Clifford transformations [59,60], 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 as [43]

$$\Omega_{\rm PLM} = |G\rangle\langle G| + \frac{2^{n-1}-1}{2^n-1}(1-|G\rangle\langle G|), \tag{161}$$

which is homogeneous with

$$\beta(\Omega_{\rm PLM}) = \frac{2^{n-1}-1}{2^n-1} \leqslant \frac{1}{2}, \quad \nu(\Omega_{\rm PLM}) = \frac{2^{n-1}}{2^n-1} \geqslant \frac{1}{2}. \tag{162}$$

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

$$\lceil 2^{1-n}(2^n-1)\epsilon^{-1}\ln\delta^{-1}\rceil \leqslant \lceil 2\epsilon^{-1}\ln\delta^{-1}\rceil, \tag{163}$$

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

$$\Delta F = \frac{\sqrt{p(1-p)}}{\nu\sqrt{N}} \leqslant \frac{\sqrt{1-F^2}}{\sqrt{N}}, \tag{164}$$

where $p = {\rm tr}(\Omega\sigma) = \nu F + \beta$, $\nu = \nu(\Omega_{\rm PLM}) \geqslant 1/2$, and $\beta = \beta(\Omega_{\rm PLM}) \leqslant 1/2$.

When adapted to the adversarial scenario, the strategy in Eq. (161) is nearly optimal thanks to Theorem 3 and Eq. (78); the number of required tests satisfies

$$N \leqslant \left\lceil \frac{\ln\delta}{(\beta\ln\beta)\epsilon} \right\rceil \leqslant \left\lceil \frac{2\ln\delta^{-1}}{(\ln 2)\epsilon} \right\rceil < \left\lceil \frac{2.89\ln\delta^{-1}}{\epsilon} \right\rceil. \tag{165}$$

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 ϵ and δ are both optimal. Previously, the best protocol for the adversarial scenario (without using our recipe) required $\lceil m^3/(\delta\epsilon)\rceil$ tests ($\lceil n^3/(\delta\epsilon)\rceil$ tests in the worst case) when $|G\rangle$ is a graph state whose underlying graph G is m-colorable [15,49].

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 qubit 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 $\mathbb{Z}_d^n$, where $\mathbb{Z}_d$ is the field of integers modulo d. Note that $\mathbb{Z}_d^n$ 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 $K_r^d = 1$ for $r = 1, 2, \ldots, n$. Each stabilizer operator in S has the form $\prod_{r=1}^n K_r^{k_r}$ with $\mathbf{k} := (k_1, k_2, \ldots, k_n) \in \mathbb{Z}_d^n$. If $\mathbf{k} = (0, 0, \ldots, 0)$, then this stabilizer operator is equal to the identity operator; otherwise, it has d distinct eigenvalues ω^j for $j = 0, 1, \ldots, d-1$, where $\omega = {\rm e}^{2\pi{\rm i}/d}$ is a primitive dth root of unity.

For each nonzero element $\mathbf{k}$ 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 as

$$P_{\mathbf{k}} = \frac{1}{d}\sum_{j=0}^{d-1}\left(\prod_{r=1}^n K_r^{k_r}\right)^j. \tag{166}$$

Note that $j\mathbf{k}$ for $j \in \mathbb{Z}_d$ will lead to the same measurement and test operator. Moreover, $P_{\mathbf{k}'} = P_{\mathbf{k}}$ iff $\mathbf{k}' = j\mathbf{k}$ for some $j \in \mathbb{Z}_d$ with $j \neq 0$ (this conclusion may fail if d is not a prime, 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 $P_{\mathbf{k}}$ randomly each with probability $(d-1)/(d^n-1)$. The resulting verification operator reads as

$$\begin{aligned}\Omega &= \frac{1}{d^n-1}\sum_{\mathbf{k}\in\mathbb{Z}_d^n,\ \mathbf{k}\neq(0,0,\ldots,0)} P_{\mathbf{k}} \\ &= |G\rangle\langle G| + \frac{d^{n-1}-1}{d^n-1}(1-|G\rangle\langle G|),\end{aligned} \tag{167}$$

which is homogeneous with

$$\beta(\Omega) = \frac{d^{n-1}-1}{d^n-1} \leqslant \frac{1}{d}, \quad \nu(\Omega) = \frac{d^n-d^{n-1}}{d^n-1} \geqslant \frac{d-1}{d}. \tag{168}$$

The number of tests required by this protocol is

$$\left\lceil \frac{d^n-1}{d^n-d^{n-1}}\epsilon^{-1}\ln\delta^{-1} \right\rceil \leqslant \left\lceil \frac{d}{d-1}\epsilon^{-1}\ln\delta^{-1} \right\rceil, \tag{169}$$

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. (9), the standard deviation of this estimation satisfies

$$\Delta F = \frac{\sqrt{p(1-p)}}{\nu\sqrt{N}} \leqslant \frac{\sqrt{(1-F)[F+(d-1)^{-1}]}}{\sqrt{N}} \tag{170}$$

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

By adding the trivial test with a suitable probability we can construct any homogeneous verification operator Ω for

$|G\rangle$ with $\frac{d^{n-1}-1}{d^n-1} \leqslant \beta(\Omega) < 1$ using LOCC. When d is an odd prime, we can construct a homogeneous verification operator Ω with $\beta(\Omega) = 1/\mathrm{e}$, which is optimal for the adversarial scenario in the high-precision limit. Then the number of required tests satisfies $N \leqslant \lceil \mathrm{e}\epsilon^{-1} \ln \delta^{-1} \rceil$ as in Eq. (157).

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, ρ 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 δ, we need to guarantee $\langle G|\rho|G\rangle > 1/d$ with significance level δ. Given a verification strategy Ω, then it suffices to perform

$$N = \left\lceil \frac{\ln \delta}{\ln[1-(d-1)\nu(\Omega)/d]} \right\rceil \tag{171}$$

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

$$N \leqslant \left\lceil \frac{\ln \delta}{\ln[1-(d-1)^2/d^2]} \right\rceil = \left\lceil \frac{\ln \delta}{\ln[(2d-1)/d^2]} \right\rceil. \tag{172}$$

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

In the adversarial scenario, we can construct a homogeneous strategy Ω with $\beta(\Omega) = 2/(d+1)$ using local projective measurements according to the above analysis. Thanks to Corollary 6 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 $\delta \geqslant 4d/(d+1)^2$, that is, $d \geqslant (2+2\sqrt{1-\delta}-\delta)/\delta$ (cf. Theorem 3 in Ref. [44]). According to Corollary 5, the lower bound for δ cannot be decreased if $d \geqslant 5$ 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 $e \in E$ [5,6,49]. 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

$$\nu(\Omega) = \chi(G)^{-1} \geqslant [\Delta(G)+1]^{-1} \geqslant n^{-1}, \tag{173}$$

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

$$N_{\mathrm{NA}} = \lceil \chi(G)\epsilon^{-1} \ln \delta^{-1} \rceil \leqslant \lceil n\epsilon^{-1} \ln \delta^{-1} \rceil. \tag{174}$$

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 Ω_p with $p = \nu/\mathrm{e}$ [49]. In the adversarial scenario, the number of tests required by Ω_p satisfies

$$N \leqslant \frac{[\chi(G)+\mathrm{e}-1]\ln(F\delta)^{-1}}{\epsilon} \leqslant \frac{(n+\mathrm{e}-1)\ln(F\delta)^{-1}}{\epsilon}, \tag{175}$$

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 $(2\ln 2)n^3\epsilon^{-18}$ tests when $\delta = \epsilon$ and $4n\epsilon \leqslant 1$ (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]. 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. X D and its generalization in Sec. X E, 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 [50]. 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, $\nu(\Omega) = \chi(G)^{-1} \geqslant n^{-1}$, 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 Ω_p with $p = \nu/\mathrm{e}$. Then the number of tests required by Ω_p to verify $|G\rangle$ in the adversarial scenario satisfies

$$N \leqslant \frac{[\chi(G)+\mathrm{e}-1]\ln(F\delta)^{-1}}{\epsilon} \leqslant \frac{(n+\mathrm{e}-1)\ln(F\delta)^{-1}}{\epsilon} \tag{176}$$

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. [50] is based on an earlier version of this paper for dealing with the adversarial scenario (see 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. (176). 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 multipartite quantum states which are useful for quantum metrology. The n-qubit Dicke state with k excitations reads as

$$|D_n^k\rangle = \binom{n}{k}^{-1/2} \sum_{x\in B_{n,k}} |x\rangle, \tag{177}$$

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 $n \geqslant 3$ and $1 \leqslant k \leqslant n-1$. 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

$$\nu(\Omega) = \begin{cases} \frac{1}{3}, & n = 3, \\ \frac{1}{n-1}, & n \geqslant 4. \end{cases} \tag{178}$$

To verify the Dicke state within infidelity ϵ and significance level δ, the number of required tests reads as

$$N_{\mathrm{NA}} = \begin{cases} \lceil 3\epsilon^{-1} \ln \delta^{-1} \rceil, & n = 3, \\ \lceil (n-1)\epsilon^{-1} \ln \delta^{-1} \rceil, & n \geqslant 4. \end{cases} \tag{179}$$

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

$$N \leqslant \begin{cases} 4.1\epsilon^{-1} \ln \delta^{-1}, & n = 3, \\ (n + \mathrm{e} - 2)\epsilon^{-1} \ln \delta^{-1}, & n \geqslant 4. \end{cases} \tag{180}$$

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).

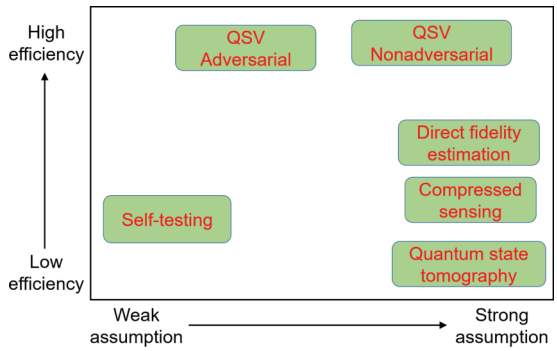

FIG. 10. Qualitative comparison among various approaches for estimating or verifying quantum states with respect to the efficiency and the strength of assumptions. Thanks to the recipe proposed in Sec. IX, QSV in the adversarial scenario can achieve nearly the same efficiency as QSV in the nonadversarial scenario, although the underlying assumptions are much weaker.

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 [37,38]. 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 scaling of resource costs. Nevertheless, it can reduce

the resource overhead significantly by exploiting the structure of quantum states of low ranks [35].

DFE, QSV, and self-testing address a different type of question: 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 [36]. QSV tries to decide whether the fidelity (infidelity) is larger (smaller) than a given threshold, which is usually easier than fidelity estimation [39,40,43]. 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 [37,38].

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. [36] 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 [38]); 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 10 qubits. For example, the resource required to self-test Dicke states increases exponentially with the number of qubits [62,63]. 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. III B 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. IX, 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. 10. 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 [38], 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). M.H. 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 A: PROOF OF EQ. (1)

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

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

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

Therefore,

$$\begin{aligned} \max_{\langle\Psi|\sigma|\Psi\rangle \leqslant 1-\epsilon} \mathrm{tr}(\Omega\sigma) &= \max_{x_j \geqslant 0,\, \sum_j x_j = 1,\, x_1 \leqslant 1-\epsilon} \sum_j \lambda_j x_j \\ &= \max_{0 \leqslant x_1 \leqslant 1-\epsilon} x_1 + \lambda_2(1 - x_1) = 1 - \nu(\Omega)\epsilon, \end{aligned} \tag{A2}$$

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

APPENDIX B: PROOFS OF LEMMAS 1 TO 6

In this Appendix we prove Lemmas 1 to 6 in Sec. V.

1. Proofs of Lemmas 1 to 3

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

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

To compute $\eta(N, 0, \Omega)$, we need to determine those $\mathbf{k} \in \mathscr{S}_N$ at which $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0$. By Eq. (27), this condition is satisfied iff $k_1 = 0$, or $\lambda_i = 0$ and $k_i \geqslant 1$ for some $2 \leqslant i \leqslant D$. In the first case, we have $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leqslant \beta^N$, and the inequality is saturated when $\mathbf{k} = (0, N+1, 0, \ldots, 0)$. In the second case, we have

$$\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \frac{k_i \lambda_i^{k_i - 1}}{N+1} \prod_{j\neq i, k_j > 0} \lambda_j^{k_j} \leqslant \frac{1}{N+1}, \tag{B2}$$

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

Next, consider the proofs of Lemmas 2 and 3. From the definitions in Eqs. (20) and (34) together with the results in Eqs. (32) and (33), we can deduce the following relations:

$$\zeta(N, \delta, \Omega) = \min_{\delta' \geqslant \delta} \tilde{\zeta}(N, \delta', \Omega) \leqslant \tilde{\zeta}(N, \delta, \Omega), \tag{B3a}$$

$$\eta(N, f, \Omega) = \max_{f' \leqslant f} \tilde{\eta}(N, f', \Omega) \geqslant \tilde{\eta}(N, f, \Omega), \tag{B3b}$$

$$F(N, \delta, \Omega) = \min_{\delta' \geqslant \delta} \tilde{F}(N, \delta', \Omega) \leqslant \tilde{F}(N, \delta, \Omega), \tag{B3c}$$

$$\mathcal{F}(N, f, \Omega) = \min_{f' \geqslant f} \tilde{\mathcal{F}}(N, f', \Omega) \leqslant \tilde{\mathcal{F}}(N, f, \Omega). \tag{B3d}$$

Therefore, Lemmas 2 and 3 are immediate consequences of Lemma 13 below.

Lemma 13. The following statements hold:

(1) $\tilde{\zeta}(N, \delta, \Omega)$ is convex and nondecreasing in δ for $0 \leqslant \delta \leqslant 1$ and is strictly increasing for $\delta_{\mathrm{c}} \leqslant \delta \leqslant 1$.

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

(3) $\tilde{F}(N, \delta, \Omega)$ is nondecreasing in δ for $0 < \delta \leqslant 1$ and is strictly increasing for $\delta_{\mathrm{c}} \leqslant \delta \leqslant 1$.

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

Here, δ_{c} is defined in Eq. (31). The convexity of $\tilde{\zeta}(N, \delta, \Omega)$ means

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

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

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

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

Proof of Lemma 13. The convexity of $\tilde{\zeta}(N, \delta, \Omega)$ in δ can be proved by virtue of the definition in Eq. (34). Suppose $0 \leqslant \delta_1 < \delta_2 \leqslant 1$ and $0 < s < 1$; let $\delta = (1-s)\delta_1 + s\delta_2$. If $\delta_1 > \delta_{\mathrm{c}}$, then there exist two quantum states ρ_1 and ρ_2 that satisfy

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

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

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

so that

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

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

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

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

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

To prove the monotonicity of $\tilde{\zeta}(N,\delta,\Omega)$ with δ, let δ_1,δ_2 be real numbers that satisfy $\delta_c \leqslant \delta_1 < \delta_2 \leqslant 1$. Then there exists a quantum state ρ_2 with $p_{\rho_2}=\delta_2$ and $f_{\rho_2}=\tilde{\zeta}(N,\delta_2,\Omega)>0$. Let s be the solution to the equation $\delta_1=(1-s)\delta_c+s\delta_2$; then $0\leqslant s<1$. Let $\rho=(1-s)\rho_c+s\rho_2$; then $p_\rho=\delta_1$, so that

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

Therefore, $\tilde{\zeta}(N,\delta,\Omega)$ is strictly increasing in δ when $\delta_c\leqslant\delta\leqslant 1$. As a corollary, $\tilde{\zeta}(N,\delta,\Omega)$ is nondecreasing in δ for $0\leqslant\delta\leqslant 1$ given that $\tilde{\zeta}(N,\delta,\Omega)=0$ for $0\leqslant\delta\leqslant\delta_c$.

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

To prove the monotonicity of $\tilde{\eta}(N,f,\Omega)$ over f, choose $0\leqslant f_1<f_2\leqslant 1$. Then there exists a quantum state ρ_1 such that $f_{\rho_1}=f_1$ and $p_{\rho_1}=\tilde{\eta}(N,f_1,\Omega)<1$. Choose $\varrho=(|\Psi\rangle\langle\Psi|)^{\otimes(N+1)}$; then $f_\varrho=p_\varrho=1$. Let s be the solution to the equation $f_2=(1-s)f_1+s$; note that $0<s\leqslant 1$ because of the assumption $f_1<f_2\leqslant 1$. Let $\rho_2=(1-s)\rho_1+s\varrho$; then $f_{\rho_2}=f_2$, so that

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

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

Next, consider statement 3 in Lemma 13. Suppose δ_1,δ_2 are real numbers that satisfy $\delta_c\leqslant\delta_1<\delta_2\leqslant 1$. Then $\tilde{F}(N,\delta_2,\Omega)\geqslant F(N,\delta_2,\Omega)>0$ and there is a quantum state ρ_2 such that $p_{\rho_2}=\delta_2$ and $f_{\rho_2}=\delta_2\tilde{F}(N,\delta_2,\Omega)$. By assumption, δ_1 can be expressed as a convex sum of δ_2 and δ_c, that is, $\delta_1=s\delta_2+(1-s)\delta_c$, where s satisfies $0\leqslant s<1$. Let $\rho_1=s\rho_2+(1-s)\rho_c$, 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

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

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

Finally, consider statement 4 in Lemma 13. Suppose f_1 and f_2 are real numbers that satisfy $0<f_1<f_2\leqslant 1$ and let $s=f_1/f_2$. Then $0<s<1$ and there exists a quantum state ρ_2 such that $f_{\rho_2}=f_2$ and $p_{\rho_2}=f_2/\tilde{\mathcal{F}}(N,f_2,\Omega)$. Let $\rho_1=s\rho_2+(1-s)\rho_c$, where ρ_c is a quantum state that satisfies $p_{\rho_c}=\delta_c$ and $f_{\rho_c}=0$. Then we have

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

so that

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

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

2. Proofs of Lemmas 4 to 7

Proof of Lemma 4. To prove Eq. (38a) in the lemma, let $f_1=\zeta(N,\delta,\Omega)$ and $\delta_1=\eta(N,f_1,\Omega)$. If δ satisfies the condition $0\leqslant\delta\leqslant\delta_c$, then $f_1=0$ and $\delta_1=\delta_c$ according to Lemma 1, which confirms Eq. (38a).

Now, suppose $\delta_c<\delta\leqslant 1$; then $\max\{\delta,\delta_c\}=\delta$. In addition, there exists a quantum state ρ on $\mathcal{H}^{\otimes(N+1)}$ such that $p_\rho=\delta$ and $f_\rho=f_1$, which implies that $\delta_1=\eta(N,f_1,\Omega)\geqslant\delta$. Meanwhile, there exists a state ρ' such that $f_{\rho'}=f_1$ and $p_{\rho'}=\delta_1$, which implies that $\zeta(N,\delta_1,\Omega)\leqslant f_1=\zeta(N,\delta,\Omega)$. Since $\zeta(N,\delta,\Omega)$ is strictly increasing in δ for $\delta_c\leqslant\delta\leqslant 1$ according to Lemma 3, we conclude that $\delta_1\leqslant\delta$. 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 $\delta_1\geqslant\delta_c$ and there exists a quantum state ρ on $\mathcal{H}^{\otimes(N+1)}$ such that $f_\rho=f$ and $p_\rho=\delta_1$, which implies that $f_1=\zeta(N,\delta_1,\Omega)\leqslant f$. Meanwhile, there exists a state ρ' such that $p_{\rho'}=\delta_1$ and $f_{\rho'}=f_1$, which implies that $\eta(N,f_1,\Omega)\geqslant\delta_1=\eta(N,f,\Omega)$. Since $\eta(N,\delta,\Omega)$ is strictly increasing in f for $0\leqslant f\leqslant 1$ according to Lemma 3, we conclude that $f_1\geqslant f$. This observation implies that $f_1=f$ and confirms Eq. (38b) given the opposite inequality derived above. ■

Proof of Lemma 5. Recall that $\zeta(N,\delta,\Omega)$ is convex and nondecreasing in δ according to Lemma 3. In addition, $\zeta(N,\delta,\Omega)$ is a piecewise-linear function of δ, and each turning point is equal to $\eta_{\mathbf{k}}$ for some $\mathbf{k}\in\mathscr{S}_N$ at which we have $\zeta(N,\delta=\eta_{\mathbf{k}},\Omega)=\zeta_{\mathbf{k}}$ (cf. Lemma 14 below). Here, $\eta_{\mathbf{k}}$ and $\zeta_{\mathbf{k}}$ are shorthand for $\eta_{\mathbf{k}}(\boldsymbol{\lambda})$ and $\zeta_{\mathbf{k}}(\boldsymbol{\lambda})$, respectively, which are defined in Eq. (27). To prove Eq. (39a), it suffices to prove the inequality $\zeta_{\mathbf{k}}\geqslant\zeta(N-1,\eta_{\mathbf{k}},\Omega)$ for each turning point.

If $k_1=0$, then $\zeta_{\mathbf{k}}=0$, which implies that $\eta_{\mathbf{k}}\leqslant\delta_c$ according to Lemma 1, so that $\zeta(N-1,\eta_{\mathbf{k}},\Omega)=0\leqslant\zeta_{\mathbf{k}}$. If $k_1\geqslant 1$, let $\mathbf{k}'=(k_1-1,k_2,\ldots,k_D)$. Then

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

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

$$\zeta(N-1,\eta_{\mathbf{k}},\Omega)\leqslant\zeta(N-1,\eta_{\mathbf{k}',N-1},\Omega)\leqslant\zeta_{\mathbf{k}',N-1}\leqslant\zeta_{\mathbf{k}}, \tag{B17}$$

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

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

Alternatively, Eq. (39c) can be derived from Lemmas 1, 3, 4, and Eq. (39a). To be specific, if $f = 0$, then we have $\eta(N, f, \Omega) < \eta(N-1, f, \Omega)$ according to Lemma 1, so Eq. (39c) holds with strict inequality. If $f > 0$, then

$$\eta(N, f, \Omega) > \eta(N, 0, \Omega) = \delta_{\rm c}, \tag{B18}$$

$$\eta(N-1, f, \Omega) > \eta(N-1, 0, \Omega) > \delta_{\rm c}, \tag{B19}$$

according to Lemmas 1 and 3, where $\delta_{\rm c}$ is given in Eq. (31). In addition, Eq. (39a) and Lemma 4 imply that

$$\begin{aligned}&\zeta(N, \eta(N-1, f, \Omega), \Omega) \geqslant \zeta(N-1, \eta(N-1, f, \Omega), \Omega)\\ &= f = \zeta(N, \eta(N, f, \Omega), \Omega).\end{aligned} \tag{B20}$$

In conjunction with Lemma 3, this equation implies that

$$\eta(N, f, \Omega) \leqslant \eta(N-1, f, \Omega) \tag{B21}$$

and confirms Eq. (39c). If the inequality in Eq. (39c) is saturated, then the inequality in Eq. (B20) is saturated, so that $\eta(N-1, f, \Omega) \leqslant \delta_{\rm c}$ 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 6. Lemma 6 follows from the definition of $N(\epsilon, \delta, \Omega)$ in Eq. (23) and the fact that the following four inequalities are equivalent:

$$F(N, \delta, \Omega) \geqslant 1 - \epsilon, \tag{B22}$$

$$\zeta(N, \delta, \Omega) \geqslant \delta(1-\epsilon), \tag{B23}$$

$$\eta(N, \delta(1-\epsilon), \Omega) \leqslant \delta, \tag{B24}$$

$$\mathcal{F}(N, \delta(1-\epsilon), \Omega) \geqslant (1-\epsilon). \tag{B25}$$

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 $\delta > \delta_{\rm c}$ if either inequality is satisfied. ■

Proof of Lemma 7. Equation (43b) is an immediate consequence of Eqs. (36a) and (43a); Eq. (43c) is an immediate consequence of Eqs. (23) and (43b). So, to prove Lemma 7, it suffices to prove Eq. (43a).

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

$$\begin{aligned}&\zeta(N, \delta, \Omega)\\ &= \min_{\{c_{\mathbf{k}}\}} \left\{ \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}} \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \middle| \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}} \eta_{\mathbf{k}}(\boldsymbol{\lambda}) \geqslant \delta \right\}\\ &\geqslant \min_{\{c_{\mathbf{k}}\}} \left\{ \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}} \zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \tilde{\Omega}) \middle| \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}} \eta_{\mathbf{k}}(\boldsymbol{\lambda}) \geqslant \delta \right\}\\ &\geqslant \min_{\{c_{\mathbf{k}}\}} \left\{ \zeta\left(N, \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}} \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \tilde{\Omega}\right) \middle| \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}} \eta_{\mathbf{k}}(\boldsymbol{\lambda}) \geqslant \delta \right\}\\ &= \min_{\delta' \geqslant \delta} \zeta(N, \delta', \tilde{\Omega}) = \zeta(N, \delta, \tilde{\Omega}),\end{aligned} \tag{B26}$$

which confirms Eq. (43a). Here, $\{c_{\mathbf{k}}\}$ is a probability distribution on $\mathscr{S}_N$; the first inequality in Eq. (B26) follows from the assumption that $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \geqslant \zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \tilde{\Omega})$ for all $\mathbf{k} \in \mathscr{S}_N$, and the second inequality follows from the convexity of $\zeta(N, \delta', \tilde{\Omega})$ in δ' (cf. Lemma 3); the last equality follows from the monotonicity of $\zeta(N, \delta', \tilde{\Omega})$ in δ'. ■

By Eq. (37) in the main text, $\zeta(N, \delta, \Omega)$ and $\eta(N, f, \Omega)$ are piecewise linear functions, whose turning points correspond to the extremal points of the region $R_{N,\Omega}$, which have the form $(\eta_{\mathbf{k}}(\boldsymbol{\lambda}), \zeta_{\mathbf{k}}(\boldsymbol{\lambda}))$ for certain $\mathbf{k} \in \mathscr{S}_N$. In conjunction with the monotonicity and convexity (concavity) of $\zeta(N, \delta, \Omega)$ $[\eta(N, f, \Omega)]$ stated in Lemma 3 (see also Lemma 4), we can deduce the following conclusion. Here, $\delta_{\rm c}$ is defined in Eq. (31).

Lemma 14. $\zeta(N, \delta, \Omega)$ for $\delta_{\rm c} \leqslant \delta \leqslant 1$ and $\eta(N, f, \Omega)$ for $0 \leqslant f \leqslant 1$ can be expressed as follows:

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

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

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

$$\delta_{\rm c} = a_0 < a_1 < \cdots < a_{m-1} < a_m = 1, \tag{B29}$$

$$0 = b_0 < b_1 < \cdots < b_{m-1} < b_m = 1, \tag{B30}$$

$$0 = \frac{b_0}{a_0} < \frac{b_1}{a_1} < \cdots < \frac{b_{m-1}}{a_{m-1}} < \frac{b_m}{a_m} = 1. \tag{B31}$$

Note that we can choose strict inequalities $\delta > a_j$ and $f > b_l$ in Lemma 14 if $\delta > \delta_{\rm c}$ and $f > 0$. If Ω is a nonsingular homogeneous strategy defined in Eq. (44), for example, then $\delta_{\rm c} = \lambda^N$, $m = N+1$, $a_j = \eta_{N+1-j}(\lambda)$, and $b_j = \zeta_{N+1-j}(\lambda)$; cf. Theorem 1 in the main text.

Lemma 14 is very helpful to understanding the properties of $\zeta(N, \delta, \Omega)$ and $\eta(N, f, \Omega)$, although, in general, it is not easy to determine the values of m, $\mathbf{k}^{(j)}$, a_j, and b_j. Geometrically, (a_j, b_j) happen to be the extremal points of the region $R_{N,\Omega}$. When $\delta_{\rm c} = \tau^N$, which can happen iff $\tau = \beta > 0$, $R_{N,\Omega}$ has no other extremal point; when $\delta_{\rm c} > \tau^N$, $R_{N,\Omega}$ 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 E.

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 $j, k \in \mathbb{Z}^{\geqslant 0}$ and $0 < \lambda < 1$, define

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

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

where $\eta_k(\lambda)$ and $\zeta_k(\lambda)$ are defined in Eq. (47), assuming that N is a positive integer. To simplify the notations, we shall use η_k, ζ_k, g_k, g_{kj} as shorthand for $\eta_k(\lambda)$, $\zeta_k(\lambda)$, $g_k(\lambda)$, $g_{kj}(\lambda)$ if there is no danger of confusions. Geometrically, g_{jk} and g_{kj} denote the slope of the line passing through the two points (η_j, ζ_j) and (η_k, ζ_k).

Lemma 15. Suppose $0 < \lambda < 1$ and $j, k \in \mathbb{Z}^{\geqslant 0}$ 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 $0 \leqslant \lambda < 1$ and $k \in \{1, 2, \ldots, N+1\}$. Then

$$\frac{1}{1-\lambda^N} \leqslant \frac{1-\zeta_k(\lambda)}{1-\eta_k(\lambda)} \leqslant \frac{1+N(1-\lambda)}{N(1-\lambda)} = \frac{1+N\nu}{N\nu}. \quad \text{(C3)}$$

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

When $0 \leqslant \lambda < 1$ (and N is a positive integer), Lemma 16 implies that

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

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

Lemma 17. Suppose $0 < \lambda \leqslant 1$, $\nu = 1-\lambda$, and a is a real number. Then

$$\lambda^{-a} - a\nu - 1 \geqslant 0 \quad \text{if } a \geqslant 0 \quad \text{or } a \leqslant -1, \quad \text{(C5)}$$

$$\lambda^{-a} - a\nu - 1 \leqslant 0 \quad \text{if } -1 \leqslant a \leqslant 0. \quad \text{(C6)}$$

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 $0 < \lambda < 1$, $0 \leqslant \delta \leqslant 1$, and $k \in \mathbb{Z}^{\geqslant 0}$. Then $\zeta(N, \delta, \lambda, k)$ increases strictly monotonically with δ when $k \leqslant N+1$. 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. (53) in the main text. Note that $\zeta(N, \delta, \lambda, k) = 1$ is independent of N and λ when $\delta = 1$ and $k = 0$.

Lemma 19. Suppose $0 < \lambda < 1$ and $0 < \delta \leqslant 1$. Then

$$\max_{k \in \mathbb{Z}^{\geqslant 0}} \zeta(N, \delta, \lambda, k) = \zeta(N, \delta, \lambda, k_*), \quad \text{(C7)}$$

$$\begin{aligned} &\max\{0, \zeta(N, \delta, \lambda, k_*)\} \\ &= \max\left\{0, \max_{k \in \{0,1,\ldots,N\}} \zeta(N, \delta, \lambda, k)\right\} \\ &= \max\{0, \zeta(N, \delta, \lambda, k_+), \zeta(N, \delta, \lambda, k_-)\}, \end{aligned} \quad \text{(C8)}$$

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

$$\zeta(N, \delta, \lambda, k_*) \leqslant 0, \quad 0 \leqslant \delta \leqslant \lambda^N, \quad \text{(C9)}$$

$$\zeta(N, \delta, \lambda, k_*) > 0, \quad \lambda^N < \delta \leqslant 1. \quad \text{(C10)}$$

Lemma 20. Suppose $0 < \epsilon, \delta, \lambda < 1$ and $k \in \mathbb{Z}^{\geqslant 0}$. Then $\tilde{N}(\epsilon, \delta, \lambda, k) > 0$ and it decreases strictly monotonically with ϵ and δ. If $\delta \leqslant \lambda^k/(F + \lambda\epsilon)$, then $\tilde{N}(\epsilon, \delta, \lambda, k) > k-1$. Given $k \geqslant 1$, then $\tilde{N}(\epsilon, \delta, \lambda, k) \leqslant \tilde{N}(\epsilon, \delta, \lambda, k-1)$ iff $\delta \leqslant \lambda^k/(F + \lambda\epsilon)$. In addition,

$$\min_{k \in \mathbb{Z}^{\geqslant 0}} \tilde{N}(\epsilon, \delta, \lambda, k) = \tilde{N}(\epsilon, \delta, \lambda, k^*) \quad \text{(C11)}$$

$$= \min\{\tilde{N}_+(\epsilon, \delta, \lambda), \tilde{N}_-(\epsilon, \delta, \lambda)\} \quad \text{(C12)}$$

$$= \begin{cases} \tilde{N}_-(\epsilon, \delta, \lambda), & \delta \geqslant \frac{\lambda^{k_+}}{F+\lambda\epsilon}, \\ \tilde{N}_+(\epsilon, \delta, \lambda), & \delta \leqslant \frac{\lambda^{k_+}}{F+\lambda\epsilon}, \end{cases} \quad \text{(C13)}$$

where k^* is the largest integer k that satisfies the inequality $\delta \leqslant \lambda^k/(F + \lambda\epsilon)$ and $\tilde{N}_\pm(\epsilon, \delta, \lambda) = \tilde{N}(\epsilon, \delta, \lambda, k_\pm)$ 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. (63).

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

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

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 15. According to Eqs. (C1) and (C2) as well as the definitions of $\eta_k(\lambda)$ and $\zeta_k(\lambda)$ in Eq. (47), we have

$$g_k(\lambda) = \frac{\lambda[1 + (N-k)\nu]}{\nu(N\lambda + k\nu)}, \quad \text{(C15)}$$

$$g_k(\lambda) - g_{k+1}(\lambda) = \frac{(N+1)\lambda}{[N\lambda + (k+1)\nu](N\lambda + k\nu)} > 0, \quad \text{(C16)}$$

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

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

$$g_{kj}(\lambda) = \sum_{m=k}^{j-1} \frac{\eta_m(\lambda) - \eta_{m+1}(\lambda)}{\eta_k(\lambda) - \eta_j(\lambda)} g_m(\lambda). \quad \text{(C17)}$$

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

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

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

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

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

$$\eta_1(\lambda) = \frac{1+N\lambda}{N+1}, \quad \zeta_1(\lambda) = \frac{N\lambda}{N+1}, \quad \text{(C20)}$$

so that

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

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 $\lambda^{-a} - a\nu - 1 = 0$ if $\lambda = 1$, or $a = 0$, or $a = -1$. The derivative of $\lambda^{-a} - a\nu - 1$ over λ reads as $a(1 - \lambda^{-a-1})$, and it satisfies

$$a(1 - \lambda^{-a-1}) \leqslant 0 \quad \text{if } a \geqslant 0 \quad \text{or } a \leqslant -1, \quad \text{(C22)}$$

$$a(1 - \lambda^{-a-1}) \geqslant 0 \quad \text{if } -1 \leqslant a \leqslant 0, \quad \text{(C23)}$$

which imply the inequalities in Eqs. (C5) and (C6) given that $\lambda^{-a} - a\nu - 1 = 0$ when $\lambda = 1$. If $a \neq -1, 0$, then the inequality in Eq. (C22) is saturated iff $\lambda = 1$, and the same holds for the inequality in Eq. (C23). Therefore, both Eqs. (C5) and (C6) are saturated iff $\lambda = 1$, which completes the proof of Lemma 17. ■

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

According to the following equation

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

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

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

which is saturated iff $\delta = 1$ and $k = 0$. To this end, it suffices to consider the two special cases $\delta = 0$ and 1 since the left-hand side in Eq. (C25) is linear in δ. In the first case, the inequality is strict. In the second case, according to Lemma 17 with $a = -(k + 1)$, we have

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

and the inequality is saturated iff $k = 0$. This observation confirms the inequality in Eq. (C25) and the saturation condition, which in turn confirms Lemma 18. ■

Proof of Lemma 19. When $k - 1 \in \mathbb{Z}^{\geqslant 0}$, by the definition of $\zeta(N, \delta, \lambda, k)$ in Eq. (53), we can derive

$$\zeta(N, \delta, \lambda, k) - \zeta(N, \delta, \lambda, k-1) = \frac{\lambda^k[k + (N+1-k)\lambda] - (N+1)\lambda\delta}{(k\nu + N\lambda)[(k-1)\nu + N\lambda]}. \tag{C27}$$

So $\zeta(N, \delta, \lambda, k) \geqslant \zeta(N, \delta, \lambda, k-1)$ iff $\delta \leqslant \eta_k$ and the inequality is saturated only when $\delta = \eta_k$. Therefore, the maximum of $\zeta(N, \delta, \lambda, k)$ over $k \in \mathbb{Z}^{\geqslant 0}$ is attained when k is the largest integer that satisfies $\eta_k \geqslant \delta$, that is, $k = k_*$, which confirms Eq. (C7).

Before proving Eq. (C8), we first prove Eqs. (C9) and (C10). According to Eq. (53) 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 $0 < \delta \leqslant \lambda^N$, then we have $k_* \geqslant N + 1$, which implies that $\zeta_{k_*}(\lambda) \leqslant 0$ and $\zeta_{k_*+1}(\lambda) < 0$. Therefore, $\zeta(N, \delta, \lambda, k_*) \leqslant 0$, which confirms Eq. (C9). Conversely, if $\lambda^N < \delta \leqslant 1$, then $k_* \leqslant N$, which implies that $\zeta_{k_*}(\lambda) > 0$ and $\zeta_{k_*+1}(\lambda) \geqslant 0$. So $\zeta(N, \delta, \lambda, k_*) > 0$, which confirms Eq. (C10).

Alternatively, to prove Eq. (C9), we can prove that $\zeta(N, \delta, \lambda, k) \leqslant 0$ for $k \in \mathbb{Z}^{\geqslant 0}$. Given that $\zeta(N, \delta, \lambda, k)$ is a linear function of δ, it suffices to prove the result when $\delta = 0$ and λ^N. According to Eq. (53), we have

$$\zeta(N, \delta = 0, \lambda, k) = -\frac{\lambda^{k+1}}{\nu(k\nu + N\lambda)} < 0, \tag{C28}$$

$$\zeta(N, \delta = \lambda^N, \lambda, k) = \frac{\lambda\{\lambda^N[1 + (N-k)\nu] - \lambda^k\}}{\nu(k\nu + N\lambda)} \leqslant 0, \tag{C29}$$

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 $0 < \delta \leqslant \lambda^N$, then Eq. (C8) follows from Eq. (C7) and the fact that $\zeta(N, \delta, \lambda, k_*) \leqslant 0$. If instead $\lambda^N < \delta \leqslant 1$, then we have $0 \leqslant k_+ \leqslant N$ and $0 \leqslant k_- \leqslant N - 1$; in addition, $\eta_{k_-}(\lambda) \geqslant \delta$ and $\eta_{1+k_+}(\lambda) < \delta$. 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, we first consider the monotonicity of $\tilde{N}(\epsilon, \delta, \lambda, k)$ defined in Eq. (63) for $0 < \epsilon, \delta \leqslant 1$, $0 < \lambda < 1$, and $k \in \mathbb{Z}^{\geqslant 0}$. The partial derivative of $\tilde{N}(\epsilon, \delta, \lambda, k)$ over ϵ reads as

$$\frac{\partial \tilde{N}(\epsilon, \delta, \lambda, k)}{\partial \epsilon} = -\frac{\lambda^{k+1} + \delta(k\nu - \lambda)}{\lambda\nu\delta\epsilon^2} \leqslant 0, \tag{C30}$$

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 ϵ for $0 < \epsilon \leqslant 1$ 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 δ reads as

$$\frac{\partial \tilde{N}(\epsilon, \delta, \lambda, k)}{\partial \delta} = -\frac{\lambda^k}{\nu\delta^2\epsilon} < 0. \tag{C31}$$

So, $\tilde{N}(\epsilon, \delta, \lambda, k)$ is strictly decreasing in δ for $0 < \delta \leqslant 1$. According to the above analysis,

$$\tilde{N}(\epsilon, \delta, \lambda, k) \geqslant \tilde{N}(\epsilon = 1, \delta = 1, \lambda, k) = \frac{\lambda^k + k\nu - 1}{\nu} \geqslant 0. \tag{C32}$$

Here, the first inequality is saturated iff $\epsilon = \delta = 1$, or $\delta = 1$ and $k = 0$; the second inequality is saturated iff $k = 0, 1$ (cf. Lemma 17). So $\tilde{N}(\epsilon, \delta, \lambda, k) > 0$, 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 ϵ and δ.

Next, suppose $0 < \epsilon, \delta < 1$. If $\delta \leqslant \lambda^k/(F + \lambda\epsilon)$ and $k = 0$, then $\tilde{N}(\epsilon, \delta, \lambda, k) > k > k - 1$ according to the first statement in Lemma 20. If instead $\delta = \lambda^k/(F + \lambda\epsilon)$ and $k \geqslant 1$, 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 $\delta \leqslant \lambda^k/(F + \lambda\epsilon)$ given that $\tilde{N}(\epsilon, \delta, \lambda, k)$ is monotonically deceasing in δ.

Next, if $k \geqslant 1$, then

$$\tilde{N}(\epsilon, \delta, \lambda, k) - \tilde{N}(\epsilon, \delta, \lambda, k-1) = \frac{\nu\delta(F\nu + \lambda) + \lambda^{k+1} - \lambda^k}{\lambda\nu\delta\epsilon} = \frac{\delta(F + \lambda\epsilon) - \lambda^k}{\lambda\delta\epsilon}, \tag{C34}$$

so $\tilde{N}(\epsilon, \delta, \lambda, k) \leqslant \tilde{N}(\epsilon, \delta, \lambda, k-1)$ iff $\delta \leqslant \lambda^k/(F + \lambda\epsilon)$. Consequently, the minimum of $\tilde{N}(\epsilon, \delta, \lambda, k)$ over $k \in \mathbb{Z}^{\geqslant 0}$ is attained when k is the largest integer that satisfies the inequality $\delta \leqslant \lambda^k/(F + \lambda\epsilon)$, that is, $k = k^*$, which confirms Eq. (C11).

In addition, we have

$$\frac{\lambda^{k_+ + 1}}{F + \lambda\epsilon} < \lambda^{k_+} \leqslant \delta \leqslant \lambda^{k_-} < \frac{\lambda^{k_-}}{F + \lambda\epsilon}, \tag{C35}$$

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 21. 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. (63) and (64), we have

$$\begin{aligned}\tilde{N}_-(\epsilon,\delta,\lambda) &= \frac{k_-\nu^2\delta F + \lambda^{k_-+1} + \lambda\delta(k_-\nu - 1)}{\lambda\nu\delta\epsilon} \\ &= \frac{F\nu+\lambda}{\lambda\epsilon}k_- + \frac{\lambda^{k_-+1} - \lambda\delta}{\lambda\nu\delta\epsilon} \\ &= \frac{F\nu+\lambda}{\lambda\epsilon}k_- + \frac{\lambda^{k_- - \log_\lambda\delta+1} - \lambda}{\lambda\nu\epsilon}. \end{aligned} \tag{C36}$$

So, the inequality in Eq. (C14) is equivalent to the following inequality:

$$\lambda^{1-b} - \lambda - \nu b \leqslant 0, \tag{C37}$$

where $b = \log_\lambda\delta - k_- = \log_\lambda\delta - \lfloor\log_\lambda\delta\rfloor$, which satisfies $0 \leqslant b < 1$. Equation (C37) holds because $\lambda^{1-b} - \lambda - \nu b$ is strictly convex in b (given the assumption $0 < \lambda < 1$) and it is equal to 0 when $b = 0$ and 1 (the function is well defined when $b = 1$ although this value cannot be attained here). In addition, the inequality in Eq. (C37) 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 iff $\log_\lambda\delta$ is an integer. ■

2. Proofs of Theorems 1–3 and Eq. (72)

Proof of Theorem 1. According to Lemma 2, we have $F(N,\delta,\lambda) = \zeta(N,\delta,\lambda)/\delta$. If $\delta \leqslant \delta_c = \lambda^N$, then we have $\zeta(N,\delta,\lambda) = 0$ by Eq. (32). If $\delta > \lambda^N$, then

$$\zeta(N,\delta,\lambda) = \min_{0\leqslant k<j\leqslant N+1}(c_j\zeta_j + c_k\zeta_k), \tag{C38}$$

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

$$c_j + c_k = 1, \quad c_j\eta_j + c_k\eta_k = \delta, \tag{C39}$$

which yield

$$c_j = \frac{\eta_k - \delta}{\eta_k - \eta_j}, \quad c_k = \frac{\delta - \eta_j}{\eta_k - \eta_j}. \tag{C40}$$

Therefore,

$$\begin{aligned} c_j\zeta_j + c_k\zeta_k &= \frac{\eta_k - \delta}{\eta_k - \eta_j}\zeta_j + \frac{\delta - \eta_j}{\eta_k - \eta_j}\zeta_k \\ &= \zeta_j + g_{kj}(\delta - \eta_j) = \zeta_k + g_{kj}(\delta - \eta_k), \end{aligned} \tag{C41}$$

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

If $j > k+1$, then $\eta_{j-1} < \delta$ or $\eta_{k+1} \geqslant \delta$, 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 15. Therefore, the minimum in Eq. (C38) can be attained when $j = k+1$ and $\eta_{k+1} < \delta \leqslant \eta_k$, in which case $k = k_*$ is the largest integer that satisfies the condition $\eta_k \geqslant \delta$. In addition, we have $c_k = c_k(\delta,\lambda)$ and $c_j = 1 - c_k(\delta,\lambda)$, so that

$$\zeta(N,\delta,\lambda) = c_j\zeta_j + c_k\zeta_k = \zeta(N,\delta,\lambda,k_*), \tag{C42}$$

which confirms Eq. (54). ■

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

$$\zeta(N,\delta,\lambda) \geqslant F\delta, \tag{C43}$$

where $F\delta > 0$. According to Corollary 1 in the main text, Eq. (C43) is equivalent to

$$\max_{k\in\mathbb{Z}^{\geqslant 0}}\zeta(N,\delta,\lambda,k) \geqslant F\delta. \tag{C44}$$

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. (53) we can deduce that the inequality $\zeta(N,\delta,\lambda,k) \geqslant F\delta$ is satisfied iff

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

So, Eq. (C43) is satisfied iff

$$N \geqslant \min_{k\in\mathbb{Z}^{\geqslant 0}}\tilde{N}(\epsilon,\delta,\lambda,k), \tag{C46}$$

which implies Theorem 2 given Lemma 20. ■

Proof of Eq. (72). The equality in Eq. (72) follows from Theorem 2 and Corollary 4, note that

$$\tilde{N}(\epsilon,\delta,\lambda,1) = \frac{\nu^2\delta F + \lambda^2 - \lambda^2\delta}{\lambda\nu\delta\epsilon}. \tag{C47}$$

To prove the lower bound in Eq. (72), we first compute the derivative of $\tilde{N}(\epsilon,\delta,\lambda,1)$ over λ, with the result

$$\frac{\partial\tilde{N}(\epsilon,\delta,\lambda,1)}{\partial\lambda} = \frac{(1-\delta)\lambda^2 - \delta F\nu^2}{\lambda^2\nu^2\epsilon\delta}. \tag{C48}$$

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

$$\lambda = \lambda_* := \frac{\sqrt{\delta F}}{\sqrt{1-\delta} + \sqrt{\delta F}}. \tag{C49}$$

Therefore,

$$N(\epsilon,\delta,\lambda) \geqslant \tilde{N}(\epsilon,\delta,\lambda,1) \geqslant \tilde{N}(\epsilon,\delta,\lambda_*,1) = \frac{2\sqrt{(1-\delta)F}}{\epsilon\sqrt{\delta}}, \tag{C50}$$

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

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

$$\begin{aligned} F(N,\delta,\lambda) &\geqslant \frac{(N-k_+)\lambda}{k_+ + (N-k_+)\lambda} = \frac{\lceil\frac{k_+F}{\lambda\epsilon}\rceil\lambda}{k_+ + \lceil\frac{k_+F}{\lambda\epsilon}\rceil\lambda} \\ &\geqslant \frac{\frac{k_+F}{\epsilon}}{k_+ + \frac{k_+F}{\epsilon}} = F = 1 - \epsilon, \end{aligned} \tag{C51}$$

which implies that $N(\epsilon,\delta,\lambda) \leqslant N$ and confirms the upper bound in Eq. (73).

Next, let $N = k_- + \lceil\frac{k_-F}{\lambda\epsilon}\rceil$. If $k_- = 0$, then we have $N = 0 < N(\epsilon,\delta,\lambda)$. If $k_- \geqslant 1$, then $N - 1 \geqslant k_- \geqslant 1$. By virtue of

Corollary 3 we can deduce that

$$F(N-1,\delta,\lambda) \leqslant \frac{(N-1-k_-)\lambda}{k_- + (N-1-k_-)\lambda} = \frac{\left(\left\lceil \frac{k_- F}{\lambda\epsilon}\right\rceil - 1\right)\lambda}{k_- + \left(\left\lceil \frac{k_- F}{\lambda\epsilon}\right\rceil - 1\right)\lambda} < \frac{\frac{k_- F}{\epsilon}}{k_- + \frac{k_- F}{\epsilon}} = 1-\epsilon, \tag{C52}$$

which implies that $N(\epsilon,\delta,\lambda) \geqslant N$ and confirms the lower bound in Eq. (73).

If $\log_\lambda \delta$ is an integer, then $k_+ = k_-$, so the lower bound and upper bound in Eq. (73) 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 21 imply that

$$N(\epsilon,\delta,\lambda) = \lceil \min\{\tilde{N}_+(\epsilon,\delta,\lambda), \tilde{N}_-(\epsilon,\delta,\lambda)\}\rceil \leqslant \lceil \tilde{N}_-(\epsilon,\delta,\lambda)\rceil \leqslant \left\lceil \frac{\log_\lambda \delta}{\lambda\epsilon} - \frac{\nu k_-}{\lambda}\right\rceil, \tag{C53}$$

which confirms Eq. (74). If $\log_\lambda \delta$ 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 Ω 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. (37) and the observation that $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 1/2$ for all $\mathbf{k} \in \mathscr{S}_1$ with $k_1 = 1$ given the assumption $N = 1$. Here, $\mathscr{S}_1$ is defined in the paragraph before Eq. (25) in the main text. Geometrically, this fact means that all points $(\eta_{\mathbf{k}}(\boldsymbol{\lambda}), \zeta_{\mathbf{k}}(\boldsymbol{\lambda}))$ for $\mathbf{k} \in \mathscr{S}_1$ with $k_1 = 1$ lie on a line segment.

To be specific, recall that $\zeta(N,\delta,\Omega) \leqslant \zeta(N,\delta,\beta)$. When $\beta \geqslant 1/2$, Eq. (106) holds because the opposite inequality $\zeta(N,\delta,\Omega) \geqslant \zeta(N,\delta,\beta)$ also holds. In view of Lemma 7, to verify this claim, it suffices to prove that

$$\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \geqslant \zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \beta) \quad \forall\, \mathbf{k} \in \mathscr{S}_1. \tag{D1}$$

The assumption $\mathbf{k} \in \mathscr{S}_1$ means $k_j \geqslant 0$ and $\sum_j k_j = 2$. When $k_1 = 2$, we have $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = \eta_{\mathbf{k}}(\boldsymbol{\lambda}) = 1$, so Eq. (D1) holds. When $k_1 = 0$, we have $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0$, while $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leqslant \beta$ according to Lemma 1, so that $\zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \beta) = 0$ (cf. Theorem 1) and Eq. (D1) also holds. When $k_1 = 1$, according to Eq. (27), we have

$$\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \frac{1+\lambda_j}{2}, \quad \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = \frac{\lambda_j}{2} \tag{D2}$$

for some $2 \leqslant j \leqslant D$. If $(1+\lambda_j)/2 \leqslant \beta$, then we have $\zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \beta) = 0$ according to Eq. (94), so Eq. (D1) holds. If $(1+\lambda_j)/2 \geqslant \beta$ (note that $\lambda_j \leqslant \beta$), then

$$\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \beta) = \frac{\lambda_j}{2} - \frac{\beta(1+\lambda_j-2\beta)}{2(1-\beta)} = \frac{(2\beta-1)(\beta-\lambda_j)}{2(1-\beta)} \geqslant 0. \tag{D3}$$

Therefore, Eq. (D1) holds for all $\mathbf{k} \in \mathscr{S}_1$, which implies that $\zeta(N,\delta,\Omega) \geqslant \zeta(N,\delta,\beta)$. In conjunction with the opposite inequality, we can deduce that $\zeta(N,\delta,\Omega) = \zeta(N,\delta,\beta)$, 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 $\tilde{\Omega}$ be a verification operator with three distinct eigenvalues $1, \beta, \tau$ (the eigenvalue 1 is nondegenerate); then we have $\zeta(N,\delta,\Omega) \leqslant \zeta(N,\delta,\tilde{\Omega})$. In addition, it is straightforward to verify Eq. (107) if Ω is replaced by $\tilde{\Omega}$. To prove Eq. (107), it suffices to prove that $\zeta(N,\delta,\Omega) \geqslant \zeta(N,\delta,\tilde{\Omega})$. Thanks to Lemma 7, this condition can be simplified to

$$\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \geqslant \zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \tilde{\Omega}) \quad \forall\, \mathbf{k} \in \mathscr{S}_1. \tag{D4}$$

When $k_1 = 2$, we have $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = \eta_{\mathbf{k}}(\boldsymbol{\lambda}) = 1$, so Eq. (D4) holds. When $k_1 = 0$, we have $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0$ and $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leqslant \beta$ according to Eq. (27), so

$$\zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \tilde{\Omega}) \leqslant \zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \beta) = 0, \tag{D5}$$

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

$$\zeta(N, \delta = \eta_{\mathbf{k}}(\boldsymbol{\lambda}), \tilde{\Omega}) = \frac{\lambda_j}{2} = \zeta_{\mathbf{k}}(\boldsymbol{\lambda}); \tag{D6}$$

recall that Eq. (107) holds if Ω is replaced by $\tilde{\Omega}$. This observation confirms Eq. (D4) and implies the inequality $\zeta(N,\delta,\Omega) \geqslant \zeta(N,\delta,\tilde{\Omega})$. In conjunction with the opposite inequality, we conclude that $\zeta(N,\delta,\Omega) = \zeta(N,\delta,\tilde{\Omega})$, 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. (20c), to prove the inequality in Eq. (111) in the lemma, it suffices to find a permutation-invariant quantum state ρ on $\mathcal{H}^{\otimes(N+1)}$ such that $p_\rho = \delta$ and

$$f_\rho = p_\rho - \frac{1}{N+1} \tag{E1}$$

for each δ in the interval $1/(N+1) \leqslant \delta \leqslant \delta^*$. Since p_ρ and f_ρ are linear in ρ, it suffices to find such a state in the two cases $\delta = 1/(N+1)$ and $\delta = \delta^*$, respectively. When $\delta = 1/(N+1)$, we can choose the state $\rho = \rho_{\mathbf{k}}$ with $\mathbf{k} = (N, 0, \ldots, 0, 1)$, in which case $p_\rho = 1/(N+1)$ and $f_\rho = 0$ by Eq. (27), so Eq. (E1) holds as desired; note that Ω is singular by assumption, which means $\tau = \lambda_D = 0$.

In the case $\delta = \delta^*$, we can choose the state $\rho = \rho_{\mathbf{k}_1}$ with $\mathbf{k}_1 := (N, 1, 0, \ldots, 0)$. Then Eq. (27) [cf. Eq. (47)] yields

$$p_\rho = \eta_{\mathbf{k}_1}(\boldsymbol{\lambda}) = \frac{1+N\beta}{N+1} = \frac{1+N(1-\nu)}{N+1} = \delta^*, \quad f_\rho = \zeta_{\mathbf{k}_1}(\boldsymbol{\lambda}) = \frac{N\beta}{N+1} = \frac{N(1-\nu)}{N+1}. \tag{E2}$$

Therefore,

$$p_\rho - f_\rho = \eta_{\mathbf{k}_1}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}_1}(\boldsymbol{\lambda}) = \frac{1}{N+1}, \tag{E3}$$

and Eq. (E1) holds again. This observation completes the proof of Lemma 8. ■

Proof of Theorem 5. To prove the inequality in Eq. (112) in the theorem, let $\rho = \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}} \rho_{\mathbf{k}}$ as in Eq. (25), where $c_{\mathbf{k}}$

form a probability distribution on $\mathscr{S}_N$. If $p_\rho = 1$, then $c_{\mathbf{k}} = \delta_{\mathbf{k},\mathbf{k}_0}$ with $\mathbf{k}_0 := (N+1, 0, \ldots, 0)$, in which case we have $F_\rho = f_\rho = 1$ and $F(N, \delta = 1, \Omega) = 1$, so Eq. (112) holds. If $0 < p_\rho < 1$, then $c_{\mathbf{k}_0} < 1$ and

$$\begin{aligned}\frac{1-p_\rho}{1-f_\rho} &= \frac{1-\sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-\sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda})} \\ &= \frac{1-c_{\mathbf{k}_0}-\sum_{\mathbf{k}\in\mathscr{S}_N^*} c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-c_{\mathbf{k}_0}-\sum_{\mathbf{k}\in\mathscr{S}_N^*} c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda})} \\ &= \frac{1-\sum_{\mathbf{k}\in\mathscr{S}_N^*} c'_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-\sum_{\mathbf{k}\in\mathscr{S}_N^*} c'_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda})} \\ &= \frac{\sum_{\mathbf{k}\in\mathscr{S}_N^*} c'_{\mathbf{k}}[1-\eta_{\mathbf{k}}(\boldsymbol{\lambda})]}{\sum_{\mathbf{k}\in\mathscr{S}_N^*} c'_{\mathbf{k}}[1-\zeta_{\mathbf{k}}(\boldsymbol{\lambda})]},\end{aligned} \tag{E4}$$

where $\mathscr{S}_N^* := \mathscr{S}_N \setminus \{\mathbf{k}_0\}$ is the subset of $\mathscr{S}_N$ without the vector $\mathbf{k}_0 := (N+1, 0, \ldots, 0)$, and $c'_{\mathbf{k}} := c_{\mathbf{k}}/(1-c_{\mathbf{k}_0})$ form a probability distribution on $\mathscr{S}_N^*$. By virtue of Lemma 23 below, we can deduce that

$$\frac{1-p_\rho}{1-f_\rho} \geqslant \min_{\mathbf{k}\in\mathscr{S}_N^*} \frac{1-\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-\zeta_{\mathbf{k}}(\boldsymbol{\lambda})} = \frac{N\nu}{N\nu+1}, \tag{E5}$$

so that

$$f_\rho \geqslant p_\rho - \frac{1-p_\rho}{N\nu} \tag{E6}$$

and

$$F_\rho = \frac{f_\rho}{p_\rho} \geqslant 1 - \frac{1-p_\rho}{N\nu p_\rho}. \tag{E7}$$

Here, Eqs. (E6) and (E7) also hold when $p_\rho = 1$. By the definition of $F(N, \delta, \Omega)$ in Eq. (20c), we conclude that

$$F(N, \delta, \Omega) \geqslant 1 - \frac{1-\delta}{N\nu\delta}. \tag{E8}$$

Incidentally, this bound is negative and thus trivial when $\delta < 1/(N\nu+1)$; in particular, it is negative when $\delta \leqslant \beta^N$ since $\beta^N < 1/(N\nu+1)$ according to Eq. (C4).

Now, we show that the inequality in Eq. (112) [same as Eq. (E8)] is saturated when $\delta \geqslant \delta^*$. Since $\delta^* = \eta_{\mathbf{k}_1}(\boldsymbol{\lambda})$ with $\mathbf{k}_1 = (N, 1, 0, \ldots, 0)$, it suffices to show that the inequality in Eq. (E6) can be saturated whenever $p_\rho \geqslant \eta_{\mathbf{k}_1}(\boldsymbol{\lambda})$. When $c_{\mathbf{k}} = \delta_{\mathbf{k},\mathbf{k}_0}$, that is, $\rho = \rho_{\mathbf{k}_0} = (|\Psi\rangle\langle\Psi|)^{\otimes(N+1)}$, we have $p_\rho = 1$ and $f_\rho = 1$, so Eq. (E6) is saturated. When $c_{\mathbf{k}} = \delta_{\mathbf{k},\mathbf{k}_1}$, that is, $\rho = \rho_{\mathbf{k}_1}$, we have $p_\rho = \eta_{\mathbf{k}_1}(\boldsymbol{\lambda}) = \delta^*$ and $f_\rho = \zeta_{\mathbf{k}_1}(\boldsymbol{\lambda})$ [cf. Eq. (E2)], so Eq. (E6) is also saturated. Since both p_ρ and f_ρ are linear in ρ, it follows that the inequality in Eq. (E6) can be saturated by a convex combination of $\rho_{\mathbf{k}_0}$ and $\rho_{\mathbf{k}_1}$ whenever $p_\rho \geqslant \eta_{\mathbf{k}_1}(\boldsymbol{\lambda})$.

Next, we prove Eq. (113) in the case $\nu \geqslant 1/2$, that is, $\beta \leqslant 1/2$. To this end, note that

$$\begin{aligned}p_\rho - f_\rho &= \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}}\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}}\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \\ &= \sum_{\mathbf{k}\in\mathscr{S}_N} c_{\mathbf{k}}[\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}}(\boldsymbol{\lambda})] \leqslant \frac{1}{N+1},\end{aligned} \tag{E9}$$

where the last inequality follows from Lemma 22 below. Therefore,

$$F_\rho \geqslant 1 - \frac{1}{(N+1)p_\rho} \tag{E10}$$

whenever $p_\rho > 0$, which implies that

$$F(N, \delta, \Omega) \geqslant 1 - \frac{1}{(N+1)\delta} \tag{E11}$$

and confirms Eq. (113). If in addition Ω is singular and δ satisfies $1/(N+1) \leqslant \delta \leqslant \delta^*$, then this bound is saturated according to Lemma 8. ■

2. Auxiliary lemmas

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

Lemma 22. $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) \leqslant 1/(N+1)$ for all $\mathbf{k} \in \mathscr{S}_N$ if $\beta \leqslant 1/2$.

Proof. If $\mathbf{k} = \mathbf{k}_0$, then $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 1$, so we have $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0 \leqslant 1/(N+1)$. If $\mathbf{k} \neq \mathbf{k}_0$, then Eq. (27) implies that

$$\begin{aligned}\eta_{\mathbf{k}}(\boldsymbol{\lambda}) - \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) &= \sum_{i\geqslant 2|k_i\geqslant 1} \frac{k_i}{(N+1)} \lambda_i^{k_i-1} \prod_{j\neq i|k_j\geqslant 1} \lambda_j^{k_j} \\ &\leqslant \frac{N+1-k_1}{N+1}\beta^{N-k_1} \\ &\leqslant \frac{N+1-k_1}{N+1}\left(\frac{1}{2}\right)^{N-k_1} \leqslant \frac{1}{N+1}.\end{aligned} \tag{E12}$$

The first inequality follows from the facts that $\lambda_j \leqslant \beta$ for all $j \geqslant 2$ and that $0 \leqslant N - k_1 \leqslant N$; the second inequality follows from the assumption $\beta \leqslant 1/2$. ■

Define

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) := \frac{1-\eta_{\mathbf{k}}(\boldsymbol{\lambda})}{1-\zeta_{\mathbf{k}}(\boldsymbol{\lambda})}, \quad \mathbf{k} \in \mathscr{S}_N^* \tag{E13}$$

where $\mathscr{S}_N^* = \mathscr{S}_N \setminus \{\mathbf{k}_0\}$ is the subset of $\mathscr{S}_N$ without the vector $\mathbf{k}_0 = (N+1, 0, \ldots, 0)$.

Lemma 23. For each $\mathbf{k} \in \mathscr{S}_N^*$, we have

$$\frac{N\nu}{N\nu+1} \leqslant \xi_{\mathbf{k}}(\boldsymbol{\lambda}) \leqslant 1 - \tau^N, \tag{E14}$$

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

The lower bound in Eq. (E14) can be expressed as

$$\frac{N\nu}{N\nu+1} = \frac{1-\eta_{\mathbf{k}_1}(\boldsymbol{\lambda})}{1-\zeta_{\mathbf{k}_1}(\boldsymbol{\lambda})}, \tag{E15}$$

where $\mathbf{k}_1 := (N, 1, 0, \ldots, 0)$. According to Eq. (C4), we have

$$\frac{N\nu}{N\nu+1} < 1 - \beta^N \leqslant 1 - \tau^N. \tag{E16}$$

Lemma 23 implies that the region $R_{N,\Omega}$ is contained in the triangle determined by the following three lines:

$$\begin{aligned} f &= 0, \\ 1-p &= (1-\tau^N)(1-f), \\ 1-p &= \frac{N\nu}{N\nu+1}(1-f). \end{aligned} \tag{E17}$$

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 23. The assumption $\mathbf{k} \in \mathscr{S}_N^*$ implies that $\sum_j k_j = N+1$ and $k_1 \leqslant N$. Thanks to Lemma 24 below, we have

$$\begin{aligned} \xi_{\mathbf{k}}(\boldsymbol{\lambda}) &\geqslant \xi_{\mathbf{k}}(1,\beta,\ldots,\beta) = \xi_{(k_1,N-k_1+1)}(1,\beta) \\ &= \frac{1-\eta_{N-k_1+1}(\beta)}{1-\zeta_{N-k_1+1}(\beta)} \geqslant \frac{N\nu}{N\nu+1}, \end{aligned} \tag{E18}$$

where the second inequality follows from Lemma 16 in Appendix C. Note that the definition of $\xi_{\mathbf{k}}(\boldsymbol{\lambda})$ [as well as that of $\eta_{\mathbf{k}}(\boldsymbol{\lambda})$ and $\zeta_{\mathbf{k}}(\boldsymbol{\lambda})$] can be extended as long as $\mathbf{k}$ and $\boldsymbol{\lambda}$ have the same number of components.

By the same token, we have

$$\begin{aligned} \xi_{\mathbf{k}}(\boldsymbol{\lambda}) &\leqslant \xi_{\mathbf{k}}(1,\tau,\ldots,\tau) = \xi_{(k_1,N-k_1+1)}(1,\tau) \\ &= \frac{1-\eta_{N-k_1+1}(\tau)}{1-\zeta_{N-k_1+1}(\tau)} \leqslant 1-\tau^N, \end{aligned} \tag{E19}$$

where the two inequalities follow from Lemma 24 and Lemma 16, respectively. ■

It is instructive to take a look at the special scenario in which $\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0$ (cf. the proof of Lemma 1 in Appendix B), which means $k_1 = 0$, or $\lambda_i = 0$ and $k_i \geqslant 1$ for some $2 \leqslant i \leqslant D$. In the first case, we have $\tau^N \leqslant \eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leqslant \beta^N$ by Eq. (27), so that

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) = 1-\eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leqslant 1-\tau^N, \tag{E20}$$

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) \geqslant 1-\beta^N \geqslant \frac{N\nu}{N\nu+1}, \tag{E21}$$

where the last inequality follows from Eq. (C4). In the second case, we have $\tau = 0$ and

$$\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \frac{k_i \lambda_i^{k_i-1}}{N+1} \prod_{j\neq i, k_j>0} \lambda_j^{k_j} \leqslant \frac{1}{N+1}, \tag{E22}$$

which implies that

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) = 1-\eta_{\mathbf{k}}(\boldsymbol{\lambda}) \leqslant 1 = 1-\tau^N, \tag{E23}$$

$$\xi_{\mathbf{k}}(\boldsymbol{\lambda}) \geqslant \frac{N}{N+1} \geqslant \frac{N\nu}{N\nu+1}. \tag{E24}$$

These results are compatible with Lemma 23 as expected.

Lemma 24. Suppose $\mathbf{k} = (k_1, k_2, \ldots, k_m)$ is a sequence of $m \geqslant 2$ non-negative integers that satisfies $k_1 \leqslant N$ and $\sum_j k_j = N+1$, where N is a positive integer. Let $\boldsymbol{u}, \boldsymbol{v}$ be two m-component vectors that satisfy $0 \leqslant \boldsymbol{u} \leqslant \boldsymbol{v} \leqslant 1$ and $u_1 = v_1 = 1$. Then we have $\xi_{\mathbf{k}}(\boldsymbol{u}) \geqslant \xi_{\mathbf{k}}(\boldsymbol{v})$.

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

Proof. The assumption $0 \leqslant \boldsymbol{u} \leqslant \boldsymbol{v} \leqslant 1$ and Eq. (27) imply that $\zeta_{\mathbf{k}}(\boldsymbol{u}) \leqslant \zeta_{\mathbf{k}}(\boldsymbol{v}) \leqslant k_1/(N+1) < 1$, so $\xi_{\mathbf{k}}(\boldsymbol{u})$ is continuous in $\boldsymbol{u}$ for $0 \leqslant \boldsymbol{u} \leqslant 1$ by the definition in Eq. (E13). Therefore, it suffices to prove the lemma when $0 < \boldsymbol{u} \leqslant \boldsymbol{v} \leqslant 1$, in which case $\eta_{\mathbf{k}}(\boldsymbol{u})$ and $\zeta_{\mathbf{k}}(\boldsymbol{u})$ can be expressed as follows:

$$\eta_{\mathbf{k}}(\boldsymbol{u}) = \theta \sum_j \frac{k_j}{u_j}, \quad \zeta_{\mathbf{k}}(\boldsymbol{u}) = \theta k_1, \tag{E25}$$

where $\theta := (\prod_i u_i^{k_i})/(N+1)$.

For $j \geqslant 2$, calculation shows that

$$\begin{aligned} \frac{\partial \eta_{\mathbf{k}}(\boldsymbol{u})}{\partial u_j} &= \theta\left(\frac{k_j}{u_j}\sum_i \frac{k_i}{u_i} - \frac{k_j}{u_j^2}\right), \\ \frac{\partial \zeta_{\mathbf{k}}(\boldsymbol{u})}{\partial u_j} &= \theta \frac{k_1 k_j}{u_j}. \end{aligned} \tag{E26}$$

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 θ. In addition,

$$\begin{aligned} \frac{\partial \xi_{\mathbf{k}}(\boldsymbol{u})}{\partial u_j} &= -\frac{\theta k_j u_j \sum_{i>1} \frac{k_i}{u_i} - \theta k_j + \theta^2 k_1 k_j}{(1-\theta k_1)^2 u_j^2} \\ &= -\frac{\theta k_j \left[u_j \sum_{i>1, i\neq j} \frac{k_i}{u_i} + (k_j - 1) + \theta k_1\right]}{(1-\theta k_1)^2 u_j^2} \leqslant 0; \end{aligned} \tag{E27}$$

note that $1-\theta k_1 \geqslant 1/(N+1) > 0$. The inequality in Eq. (E27) is strict except when $k_j = 0$, in which case $\xi_{\mathbf{k}}(\boldsymbol{u})$ is independent of u_j, and so are $\eta_{\mathbf{k}}(\boldsymbol{u})$ and $\zeta_{\mathbf{k}}(\boldsymbol{u})$ [cf. Eq. (27) in the main text]. Therefore, $\xi_{\mathbf{k}}(\boldsymbol{u})$ is nonincreasing in u_j for all $j \geqslant 2$, which means $\xi_{\mathbf{k}}(\boldsymbol{u}) \geqslant \xi_{\mathbf{k}}(\boldsymbol{v})$ whenever $0 < \boldsymbol{u} \leqslant \boldsymbol{v} \leqslant 1$ and $u_1 = v_1 = 1$. The condition $0 < \boldsymbol{u} \leqslant \boldsymbol{v} \leqslant 1$ can be relaxed to $0 \leqslant \boldsymbol{u} \leqslant \boldsymbol{v} \leqslant 1$ by continuity. ■

APPENDIX F: PROOFS OF LEMMA 9 AND THEOREM 6

1. Auxiliary lemmas

Before proving Lemma 9 and Theorem 6, wee need to introduce a few auxiliary notations and results.

Denote by $\bar{\mathscr{S}}_N$ the convex hull of $\mathscr{S}_N$, then $\bar{\mathscr{S}}_N$ is composed of real vectors $\mathbf{k} = (k_1, k_2, \ldots, k_D)$ that satisfy $\sum_{j=1}^D k_j = N+1$ and $k_j \geqslant 0$ for $j = 1, 2, \ldots D$. When Ω is positive definite, that is, $\tau(\Omega) > 0$, we can extend the definition of $\eta_{\mathbf{k}}(\boldsymbol{\lambda})$ and $\zeta_{\mathbf{k}}(\boldsymbol{\lambda})$ over $\mathbf{k}$ to $\bar{\mathscr{S}}_N$ [cf. Eq. (27)]. Since all eigenvalues λ_j of Ω for $j = 1, 2, \ldots, D$ are positive, we have $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) > 0$ for all $\mathbf{k} \in \bar{\mathscr{S}}_N$. The following analogs of $\zeta(N, \delta, \Omega)$ and $\eta(N, f, \Omega)$ [cf. Eq. (37)] will play key roles in proving Lemma 9 and Theorem 6. Define

$$\bar{\zeta}(N,\delta,\Omega) := \begin{cases} \min_{\mathbf{k}\in\bar{\mathscr{S}}_N}\{\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) | \eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \delta\}, & \beta^N \leqslant \delta \leqslant 1, \\ 0, & 0 \leqslant \delta \leqslant \beta^N, \end{cases} \tag{F1}$$

$$\bar{\eta}(N,f,\Omega) := \max_{\mathbf{k}\in\bar{\mathscr{S}}_N}\{\eta_{\mathbf{k}}(\boldsymbol{\lambda}) | \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = f\}, \quad 0 \leqslant f \leqslant 1, \tag{F2}$$

where β is the second largest eigenvalue of Ω. Incidentally, $\eta(N, f=0, \Omega) = \delta_c = \beta^N$ since $\tau > 0$; see Lemma 1.

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

$$\zeta(N,\delta,\Omega) \geqslant \bar{\zeta}(N,\delta,\Omega), \tag{F3}$$

$$\eta(N,f,\Omega) \leqslant \bar{\eta}(N,f,\Omega). \tag{F4}$$

Proof. When δ satisfies $0 \leqslant \delta \leqslant \beta^N$, by definition we have $\bar{\zeta}(N,\delta,\Omega) = 0 \leqslant \zeta(N,\delta,\Omega)$, so Eq. (F3) holds. When $\delta > \beta^N$, by Lemma 14 in Appendix B, we can find vectors $\mathbf{q}_0, \mathbf{q}_1 \in \mathscr{S}_N$ such that $\beta^N \leqslant \eta_0 < \eta_1 \leqslant 1$, $\eta_0 < \delta \leqslant \eta_1$, $0 \leqslant \zeta_0 < \zeta_1 \leqslant 1$, and $0 \leqslant F_0 < F_1 \leqslant 1$, where $\eta_j = \eta_{\mathbf{q}_j}(\boldsymbol{\lambda})$, $\zeta_j = \zeta_{\mathbf{q}_j}(\boldsymbol{\lambda})$, 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 non-negative coefficients determined by the requirements $c_0 + c_1 = 1$ and $c_0\eta_0 + c_1\eta_1 = \delta$, that is,

$$c_0 = \frac{\eta_1 - \delta}{\eta_1 - \eta_0}, \quad c_1 = \frac{\delta - \eta_0}{\eta_1 - \eta_0}. \tag{F5}$$

If $\delta = \eta_1$, then $\zeta(N,\delta,\Omega) = \zeta_1$ and Eq. (F3) holds because of the relation $\mathscr{S}_N \subset \bar{\mathscr{S}}_N$. 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 (η_0, ζ_0) and (η_1, ζ_1), which has slope $(\zeta_1 - \zeta_0)/(\eta_1 - \eta_0)$.

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

$$\mathbf{k}(t) = \mathbf{q}_0(1-t) + \mathbf{q}_1 t = \mathbf{q}_0 + (\mathbf{q}_1 - \mathbf{q}_0)t, \tag{F6}$$

$$\eta(t) = \eta_{\mathbf{k}(t)}(\boldsymbol{\lambda}), \quad \zeta(t) = \zeta_{\mathbf{k}(t)}(\boldsymbol{\lambda}). \tag{F7}$$

Note that $\mathbf{k}(t) \in \bar{\mathscr{S}}_N$ for $0 \leqslant t \leqslant 1$; 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 (η_0, ζ_0) and (η_1, ζ_1). The explicit expressions of $\eta(t)$ and $\zeta(t)$ can be derived by virtue of Eq. (27), with the result

$$\eta(t) = \theta(t)\sum_j \frac{k_j(t)}{\lambda_j}, \quad \zeta(t) = \theta(t)k_1(t), \tag{F8}$$

where

$$\theta(t) = \frac{1}{N+1}\prod_j \lambda_j^{k_j(t)}. \tag{F9}$$

Let

$$F(t) = \frac{\zeta(t)}{\eta(t)} = \frac{k_1(t)}{\sum_j \frac{k_j(t)}{\lambda_j}}; \tag{F10}$$

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

Let t_δ be the smallest value of t such that $\eta(t) = \delta$; then $\bar{\zeta}(N,\delta,\Omega) \leqslant \zeta(t_\delta)$. So, Eq. (F3) would follow if we can prove that $\zeta(t_\delta) \leqslant \zeta(N,\delta,\Omega)$.

To achieve our goal, we shall prove that the parametric curve $(\eta(t), \zeta(t))$ for $0 \leqslant t \leqslant t_\delta$ lies below the line segment passing through the two points (η_0, ζ_0) and (η_1, ζ_1). To this end, we need to analyze the convexity (or concavity) property of the curve, which depends on the second derivative

$$\frac{d^2\zeta(t)}{d\eta(t)^2} = \frac{\zeta''(t)\eta'(t) - \eta''(t)\zeta'(t)}{\eta'(t)^3}. \tag{F11}$$

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

$$\eta'(t) = \frac{d\eta(t)}{dt} = \eta(t)\sum_j (q_{1j} - q_{0j})\ln\lambda_j + \theta(t)\sum_j \frac{q_{1j} - q_{0j}}{\lambda_j} = \theta(t)\left[\frac{\eta(t)}{\theta(t)}\ln\frac{\theta_1}{\theta_0} + \left(\frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0}\right)\right], \tag{F12}$$

$$\zeta'(t) = \frac{d\zeta(t)}{dt} = \zeta(t)\sum_j (q_{1j} - q_{0j})\ln\lambda_j + \theta(t)(q_{11} - q_{01}) = \theta(t)\left[k_1(t)\ln\frac{\theta_1}{\theta_0} + (q_{11} - q_{01})\right], \tag{F13}$$

$$\eta''(t) = \frac{d^2\eta(t)}{dt^2} = \theta(t)\left(\ln\frac{\theta_1}{\theta_0}\right)\left[\frac{\eta(t)}{\theta(t)}\ln\frac{\theta_1}{\theta_0} + 2\left(\frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0}\right)\right], \tag{F14}$$

$$\zeta''(t) = \frac{d^2\zeta(t)}{dt^2} = \theta(t)\left(\ln\frac{\theta_1}{\theta_0}\right)\left[k_1(t)\ln\frac{\theta_1}{\theta_0} + 2(q_{11} - q_{01})\right], \tag{F15}$$

where

$$\theta_0 = \theta(t=0) = \frac{1}{N+1}\prod_j \lambda_j^{q_{0j}}, \quad \theta_1 = \theta(t=1) = \frac{1}{N+1}\prod_j \lambda_j^{q_{1j}}. \tag{F16}$$

Note that

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

Therefore,

$$\begin{aligned}
\zeta''(t)\eta'(t) - \eta''(t)\zeta'(t) &= \theta(t)^2\left(\ln\frac{\theta_1}{\theta_0}\right)^2\left[(q_{11} - q_{01})\frac{\eta(t)}{\theta(t)} - \left(\frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0}\right)k_1(t)\right] \\
&= \theta(t)^2\left(\ln\frac{\theta_1}{\theta_0}\right)^2\left\{(q_{11} - q_{01})\left[\frac{\eta_0}{\theta_0} + \left(\frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0}\right)t\right] - \left(\frac{\eta_1}{\theta_1} - \frac{\eta_0}{\theta_0}\right)[q_{01} + (q_{11} - q_{01})t]\right\} \\
&= \theta(t)^2\left(\ln\frac{\theta_1}{\theta_0}\right)^2\left(\frac{\eta_0 q_{11}}{\theta_0} - \frac{\eta_1 q_{01}}{\theta_1}\right) = \theta(t)^2\left(\ln\frac{\theta_1}{\theta_0}\right)^2\frac{\eta_0\eta_1}{\theta_0\theta_1}\left(\frac{\theta_1 q_{11}}{\eta_1} - \frac{\theta_0 q_{01}}{\theta_0}\right) = \theta(t)^2\left(\ln\frac{\theta_1}{\theta_0}\right)^2\frac{\eta_0\eta_1}{\theta_0\theta_1}(F_1 - F_0) \geqslant 0.
\end{aligned} \tag{F18}$$

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 positive constant. When $t = 0$, we have

$$\eta'(0) = \eta_0\left[\ln\frac{\theta_1}{\theta_0} + \left(\frac{\eta_1\theta_0}{\theta_1\eta_0} - 1\right)\right] > \eta_0\left[\ln\frac{\theta_1}{\theta_0} + \left(\frac{\theta_0}{\theta_1} - 1\right)\right] \geqslant 0 \tag{F19}$$

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 $0 \leqslant t \leqslant 1$. If $\eta'(t) > 0$ in this interval, then $\frac{d^2\zeta(t)}{d\eta(t)^2} \geqslant 0$ and $\zeta(t)$ is a convex function of $\eta(t)$ for $0 \leqslant t \leqslant 1$, so the parametric curve $(\eta(t), \zeta(t))$ lies below the line segment that connects the two points (η_0, ζ_0) and (η_1, ζ_1), which implies the inequality $\zeta(t_\delta) \leqslant \zeta(N, \delta, \Omega)$ and Eq. (F3). Here, t_δ is the smallest value of t such that $\eta(t) = \delta$. Otherwise, $\eta'(t)$ has a unique zero point $0 < t_2 \leqslant 1$. If $t_2 = 1$, then the same conclusion holds. If $t_2 < 1$, then $\eta'(t) > 0$ for $0 \leqslant t < t_2$ and $\eta'(t) < 0$ for $t_2 < t \leqslant 1$, 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 $0 \leqslant t \leqslant t_3$ and that $t_\delta < t_3$. To prove Eq. (F3), it suffices to prove the inequality $\zeta(t_3) \leqslant \zeta_1$, that is, $F(t_3) \leqslant F_1$, given that $\eta(t_3) = \eta_1$.

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

$$\frac{dF(t)}{dt} = \frac{\theta(t)^2}{\eta(t)^2}\frac{\eta_0\eta_1}{\theta_0\theta_1}(F_1 - F_0) > 0. \tag{F20}$$

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 $0 \leqslant t \leqslant 1$, which implies that $F(t_3) \leqslant F(1) = F_1$ and that $\zeta(t_3) \leqslant \zeta(1) = \zeta_1$. Therefore, the parametric curve $(\eta(t), \zeta(t))$ for $0 \leqslant t \leqslant t_3$ lies below the line segment that connects the two points (η_0, ζ_0) and (η_1, ζ_1), which implies that $\zeta(t_\delta) \leqslant \zeta(N, \delta, \Omega)$ and confirms Eq. (F3).

Equation (F4) can be proved using a similar reasoning used for proving Eq. (F3). When $f = 0$, we have

$$\bar{\eta}(N, f, \Omega) = \max_{\mathbf{k}\in\bar{\mathscr{T}}_N}\{\eta_{\mathbf{k}}(\boldsymbol{\lambda})|\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0\} \geqslant \max_{\mathbf{k}\in\mathscr{S}_N}\{\eta_{\mathbf{k}}(\boldsymbol{\lambda})|\zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = 0\} = \eta(N, f, \Omega), \tag{F21}$$

which confirms Eq. (F4); here, the inequality follows from the fact that $\mathscr{S}_N$ is contained in $\bar{\mathscr{T}}_N$. When $f > 0$, we can choose $\mathbf{q}_0, \mathbf{q}_1 \in \mathscr{S}_N$ and define $\eta_0, \zeta_0, \eta_1, \zeta_1, \eta(t), \zeta(t)$ in a similar way to the proof of Eq. (F3), but with the requirement $\eta_0 < \delta \leqslant \eta_1$ replaced by $\zeta_0 < f \leqslant \zeta_1$. Since the case $f = \zeta_1$ is trivial, we can assume $\zeta_0 < f < \zeta_1$. Then Eqs. (F6)–(F20) still apply. According to Eq. (F18) and the equation

$$\frac{d^2\eta(t)}{d\zeta(t)^2} = -\frac{\zeta''(t)\eta'(t) - \eta''(t)\zeta'(t)}{\zeta'(t)^3}, \tag{F22}$$

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

$$\zeta'(0) = \theta_0\left[q_{01}\ln\frac{\theta_1}{\theta_0} + (q_{11} - q_{01})\right] \geqslant \theta_0\left[q_{01}\left(1 - \frac{\theta_0}{\theta_1}\right) + (q_{11} - q_{01})\right] = \theta_0\frac{q_{11}\theta_1 - q_{01}\theta_0}{\theta_1} = \theta_0\frac{\zeta_1 - \zeta_0}{\theta_1} > 0. \tag{F23}$$

In addition, $\theta(t) > 0$, and $\zeta'(t)/\theta(t)$ is a linear and thus monotonic function of t according to Eq. (F13). Therefore, $\zeta'(t)$ has at most one zero point in the interval $0 \leqslant t \leqslant 1$ as is the case for $\eta'(t)$. Now, Eq. (F4) can be proved using a similar reasoning as presented after Eq. (F19), though "convex" is replaced by "concave." ■

Lemma 26. Suppose $1 > x_1 \geqslant x_2 \geqslant \ldots, x_m > 0$ and $c \leqslant 0$. Then

$$\max_{a_1,a_2,\ldots,a_m\geqslant 0}\left\{\sum_j \frac{a_j}{x_j}\middle|\sum_j a_j\ln x_j = c\right\} = \frac{c}{y\ln y}, \tag{F24}$$

where $y = x_1$ if $x_1\ln x_1^{-1} \leqslant x_m\ln x_m^{-1}$ 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 $a_1, a_2, \ldots, a_m \geqslant 0$ 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,

$$\max_{a_1,a_2,\ldots,a_m\geqslant 0}\left\{\sum_j \frac{a_j}{x_j}\middle|\sum_j a_j\ln x_j = c\right\} = \max_j \frac{c}{x_j\ln x_j} = \max\left\{\frac{c}{x_1\ln x_1}, \frac{c}{x_m\ln x_m}\right\} = \frac{c}{y\ln y}. \tag{F26}$$

Here, the second equality follows from the assumption $1 > x_1 \geqslant x_2 \geqslant \ldots x_m > 0$ and the fact that the function $c/(x\ln x)$ is convex in x for $0 < x < 1$, given that c 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 25,

$$\mathcal{F}(N, f, \Omega) = \frac{f}{\eta(N, f, \Omega)} \geqslant \frac{f}{\bar{\eta}(N, f, \Omega)} = \min_{\mathbf{k}\in\bar{\mathscr{T}}_N|\zeta_{\mathbf{k}}(\boldsymbol{\lambda})=f}\frac{\zeta_{\mathbf{k}}(\boldsymbol{\lambda})}{\eta_{\mathbf{k}}(\boldsymbol{\lambda})} = \min_{\mathbf{k}\in\bar{\mathscr{T}}_N|\zeta_{\mathbf{k}}(\boldsymbol{\lambda})=f}\frac{k_1}{\sum_j(k_j/\lambda_j)} = \min_{\mathbf{k}\in\bar{\mathscr{T}}_N|\zeta_{\mathbf{k}}(\boldsymbol{\lambda})=f}\frac{k_1}{k_1 + \sum_{j=2}^D(k_j/\lambda_j)}. \tag{F27}$$

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

$$f = \zeta_{\mathbf{k}}(\boldsymbol{\lambda}) = \frac{k_1}{N+1}\prod_j \lambda_j^{k_j} \leqslant \prod_{j=2}^{D} \lambda_j^{k_j} \leqslant \beta^{N+1-k_1}, \tag{F28}$$

which implies that $N + 1 - k_1 \leqslant \ln f/\ln\beta = \log_\beta f$, that is, $k_1 \geqslant N + 1 - (\ln f/\ln\beta)$. In addition, the above equation implies that $0 \geqslant \sum_{j=2}^{D} k_j \ln\lambda_j \geqslant \ln f$, which in turn implies that $\sum_{j=2}^{D}(k_j/\lambda_j) \leqslant \ln f/(\tilde{\beta}\ln\tilde{\beta})$ in view of Lemma 26. Therefore,

$$\begin{aligned}\mathcal{F}(N, f, \Omega) &\geqslant \min_{\mathbf{k}\in\mathscr{T}_N|\zeta_{\mathbf{k}}(\boldsymbol{\lambda})=f} \frac{k_1}{k_1 + (\tilde{\beta}\ln\tilde{\beta})^{-1}\ln f} \\ &\geqslant \frac{N+1-(\ln\beta)^{-1}\ln f}{N+1-(\ln\beta)^{-1}\ln f - h\ln f},\end{aligned} \tag{F29}$$

which confirms Eq. (121).

Next, let us prove Eq. (120). If $\delta \leqslant \beta^N$, then we have $\tau\delta \leqslant \beta^{N+1}$ and $N + 1 - (\ln\beta)^{-1}\ln(\tau\delta) \leqslant 0$, so the bound in Eq. (120) is either zero or negative and is thus trivial. If $\delta > \beta^N$, then Lemma 25 implies that

$$\begin{aligned}F(N, \delta, \Omega) &= \frac{\zeta(N, \delta, \Omega)}{\delta} \geqslant \frac{\bar{\zeta}(N, \delta, \Omega)}{\delta} \\ &= \min_{\mathbf{k}\in\mathscr{T}_N|\eta_{\mathbf{k}}(\boldsymbol{\lambda})=\delta} \frac{k_1}{k_1 + \sum_{j=2}^{D}(k_j/\lambda_j)}.\end{aligned} \tag{F30}$$

The condition $\eta_{\mathbf{k}}(\boldsymbol{\lambda}) = \delta$ entails the following inequality:

$$\begin{aligned}\tau\delta = \tau\eta_{\mathbf{k}}(\boldsymbol{\lambda}) &= \frac{\tau}{N+1}\left(\prod_j \lambda_j^{k_j}\right)\left(\sum_j \frac{k_j}{\lambda_j}\right) \leqslant \prod_{j=2}^{D}\lambda_j^{k_j} \\ &\leqslant \beta^{N+1-k_1}.\end{aligned} \tag{F31}$$

Now, Eq. (120) can be proved using a similar reasoning that leads to Eq. (F29), but with f replaced by $\tau\delta$. ■

Proof of Theorem 6. Equation (124) follows from Eq. (30) and Theorem 3 in the main text. The lower bound in Eq. (125) follows from Eq. (124) given that $\tilde{\beta} = \beta = \lambda_2$ or $\tilde{\beta} = \tau = \lambda_D$.

To prove the upper bounds in Eq. (125), let $f = F\delta$ with $F = 1 - \epsilon$ and

$$N = \left\lceil \frac{hF\ \ln f^{-1}}{\epsilon} + \frac{\ln f}{\ln\beta} - 1 \right\rceil; \tag{F32}$$

then $N \geqslant 1$ since

$$\frac{hF\ \ln f^{-1}}{\epsilon} + \frac{\ln f}{\ln\beta} > \frac{F\ \ln F}{\epsilon\beta\ \ln\beta} + \frac{\ln F}{\ln\beta} > 1. \tag{F33}$$

Here, the second inequality is equivalent to

$$F\ \ln F + \epsilon\beta\ \ln F - \epsilon\beta\ \ln\beta < 0. \tag{F34}$$

To prove this inequality, note that for a given $0 < F < 1$, the left-hand side is maximized when $\beta = F/\mathrm{e}$. So

$$F\ \ln F + \epsilon\beta\ \ln F - \epsilon\beta\ \ln\beta \leqslant \frac{F(1 - F + \mathrm{e}\ \ln F)}{\mathrm{e}} < 0. \tag{F35}$$

In addition, Lemma 9 implies that

$$\begin{aligned}\mathcal{F}(N, f, \Omega) &\geqslant \frac{N+1-(\ln\beta)^{-1}\ln f}{N+1-(\ln\beta)^{-1}\ln f - h\ln f} \\ &\geqslant \frac{hF\epsilon^{-1}\ln f^{-1}}{hF\epsilon^{-1}\ln f^{-1} - h\ \ln f} = 1 - \epsilon.\end{aligned} \tag{F36}$$

In conjunction with Lemma 6, this equation implies that $N(\epsilon, \delta, \Omega) \leqslant N$, which confirms the first upper bound in Eq. (125). Moreover, we have $h > |1/\ln\beta|$ since $0 < \beta < 1$ and $|\tilde{\beta}\ \ln\tilde{\beta}| \leqslant |\beta\ \ln\beta| < |\ln\beta|$. Therefore,

$$\begin{aligned}N &= \left\lceil \frac{h(1-\epsilon)\ln f^{-1}}{\epsilon} + \frac{\ln f}{\ln\beta} - 1 \right\rceil \\ &< \frac{h\ \ln f^{-1}}{\epsilon} - h\ \ln f^{-1} + \frac{\ln f}{\ln\beta} \\ &< \frac{h\ \ln f^{-1}}{\epsilon} = \frac{h\ \ln(F\delta)^{-1}}{\epsilon},\end{aligned} \tag{F37}$$

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 $\mathcal{F}(N, f, \Omega)$ replaced by $F(N, \delta, \Omega)$ ■

APPENDIX G: PROOFS OF LEMMAS 10–12

Proof of Lemma 10. By Eqs. (138) and (139) in the main text, it is clear that $p_*(\nu, 1-\nu)$ is nondecreasing in ν, and $h_*(\nu, 1-\nu)$ is nonincreasing in ν. If $1 - \mathrm{e}^{-1} \leqslant \nu \leqslant 1$, then

$$\nu h_*(\nu, 1-\nu) = \mathrm{e}\nu \geqslant \mathrm{e}(1-\mathrm{e}^{-1}) = \mathrm{e} - 1 > 1, \tag{G1}$$

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

$$\nu h_*(\nu, 1-\nu) = \nu[(1-\nu)\ln(1-\nu)^{-1}]^{-1}, \tag{G2}$$

so that

$$\lim_{\nu\to 0} \nu h_*(\nu, 1-\nu) = \lim_{\nu\to 0} \nu[(1-\nu)\ln(1-\nu)^{-1}]^{-1} = 1. \tag{G3}$$

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

In addition,

$$\nu h(p, \nu, 1-\nu) = \nu\left(\beta_p \ln\beta_p^{-1}\right)^{-1}, \tag{G4}$$

where $\beta_p = 1 - \nu + p\nu$ satisfies $0 < \beta_p < 1$. The derivative of $\nu h(p, \nu, 1-\nu)$ over ν reads as

$$\frac{d}{d\nu}\left(\frac{\nu}{\beta_p \ln\beta_p^{-1}}\right) = -\frac{(1-p)\nu + \ln(1-\nu+p\nu)}{[(1-\nu+p\nu)\ln(1-\nu+p\nu)]^2} > 0, \tag{G5}$$

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 ν. Incidentally, the derivative in Eq. (G5) approaches $\frac{1}{2}$ in the limit $\nu \to 0$. ■

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

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

$$\beta'_q \ln {\beta'_q}^{-1} < \beta_q \ln \beta_q^{-1} \leqslant \tau_q \ln \tau_q^{-1}, \tag{G6}$$

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

In addition, the inequalities $\tau_p \leqslant \beta_p \leqslant \beta'_p$ imply that

$$\beta_p \ln {\beta_p}^{-1} \geqslant \min\left\{\beta'_p \ln {\beta'_p}^{-1}, \tau_p \ln \tau_p^{-1}\right\} \tag{G7}$$

and that

$$\begin{aligned} h(p,\nu',\tau) &= \left[\min\left\{\beta'_p \ln {\beta'_p}^{-1}, \tau_p \ln \tau_p^{-1}\right\}\right]^{-1} \\ &\geqslant \left[\min\left\{\beta_p \ln \beta_p^{-1}, \tau_p \ln \tau_p^{-1}\right\}\right]^{-1} = h(p,\nu,\tau). \end{aligned} \tag{G8}$$

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

$$h_*(\nu',\tau) = h(p,\nu',\tau) \geqslant h(p,\nu,\tau) \geqslant h_*(\nu,\tau). \tag{G9}$$

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

Next, suppose $\tau \leqslant \tau' \leqslant \beta$. Then we have $\tau_q \leqslant \tau'_q \leqslant \beta_q$, $\beta_q \geqslant 1/\mathrm{e}$, and

$$\tau'_q \ln {\tau'_q}^{-1} \geqslant \min\left\{\beta_q \ln \beta_q^{-1}, \tau_q \ln \tau_q^{-1}\right\} = \beta_q \ln \beta_q^{-1}, \tag{G10}$$

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

In addition, the inequalities $\tau_p \leqslant \tau'_p \leqslant \beta_p$ imply that

$$\tau'_p \ln {\tau'_p}^{-1} \geqslant \min\left\{\beta_p \ln \beta_p^{-1}, \tau_p \ln \tau_p^{-1}\right\} \tag{G11}$$

and that

$$\begin{aligned} h(p,\nu,\tau') &= \left[\min\left\{\beta_p \ln \beta_p^{-1}, \tau'_p \ln {\tau'_p}^{-1}\right\}\right]^{-1} \\ &\leqslant \left[\min\left\{\beta_p \ln \beta_p^{-1}, \tau_p \ln \tau_p^{-1}\right\}\right]^{-1} = h(p,\nu,\tau). \end{aligned} \tag{G12}$$

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

$$h_*(\nu,\tau) = h(p,\nu,\tau) \geqslant h(p,\nu,\tau') \geqslant h_*(\nu,\tau'). \tag{G13}$$

So $h_*(\nu,\tau)$ is also nonincreasing in τ, 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 $\nu h_*(\nu,\tau) \geqslant \nu h_*(\nu,1-\nu) > 1$, which confirms statement 3 in Lemma 11. In addition, the following equations

$$\lim_{\nu\to 0} \nu h_*(\nu,\tau) \geqslant \lim_{\nu\to 0} \nu h_*(\nu,1-\nu) = 1, \tag{G14}$$

$$\lim_{\nu\to 0} \nu h_*(\nu,\tau) \leqslant \lim_{\nu\to 0} \nu h(\nu,\nu,\tau) = 1 \tag{G15}$$

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

$$\nu h(p,\nu,\tau) = \max\left\{\nu\left(\beta_p \ln \beta_p^{-1}\right)^{-1}, \nu\left(\tau_p \ln \tau_p^{-1}\right)^{-1}\right\}, \tag{G16}$$

where $\beta_p = 1-\nu+p\nu$. It is clear that $\nu(\tau_p \ln \tau_p^{-1})^{-1}$ increases strictly monotonically with ν. The same conclusion holds for $\nu(\beta_p \ln \beta_p^{-1})^{-1}$ according to the derivative in Eq. (G5). Therefore, $\nu h(p,\nu,\tau)$ increases strictly monotonically with ν, which confirms statement 7 in Lemma 11.

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

$$\nu' h_*(\nu',\tau) \leqslant \nu' h(q,\nu',\tau) < \nu h(q,\nu,\tau) = \nu h_*(\nu,\tau), \tag{G17}$$

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

Proof of Lemma 12. Recall that $p_*(\nu)$ is the smallest value of $p > 0$ that satisfies the conditions $\beta_p \geqslant 1/\mathrm{e}$ and $p \ln p = \beta_p \ln \beta_p$ [see Eq. (146)]. Let $q = p_*(\nu)$; then $0 < q \leqslant 1/\mathrm{e}$. Suppose $0 < \nu' < \nu$ and $\beta' = 1-\nu'$. Then $1 > \beta' > \beta \geqslant 0$ and $1 > \beta'_q > \beta_q \geqslant 1/\mathrm{e}$, so that

$$\beta'_q \ln {\beta'_q}^{-1} < \beta_q \ln \beta_q^{-1} = q \ln q^{-1}, \tag{G18}$$

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

Next, let us consider the monotonicity of $h(\mathrm{e}^{-1}\nu,\nu)$ and $\nu h(\mathrm{e}^{-1}\nu,\nu)$. By definition we have

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

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

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

In addition, $\mathrm{e}(\ln \frac{\mathrm{e}}{\nu})^{-1}$ is strictly increasing in ν for the interval $0 < \nu \leqslant 1$. Meanwhile, we have

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

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

$$\begin{aligned} &\mathrm{e}\beta_{p_0} - (\mathrm{e}-\nu^2)\ln(\mathrm{e}\beta_{p_0}) \\ &\quad = \mathrm{e} - \mathrm{e}\nu + \nu^2 - (\mathrm{e}-\nu^2)\ln(\mathrm{e}-\mathrm{e}\nu+\nu^2) \\ &\quad \geqslant \mathrm{e} - \mathrm{e}\nu + \nu^2 - (\mathrm{e}-\nu^2)(1-\nu) \\ &\quad = (2-\nu)\nu^2 > 0. \end{aligned} \tag{G22}$$

Here, the first inequality follows from the inequality below

$$\ln(\mathrm{e} - \mathrm{e}\nu + \nu^2) \leqslant 1-\nu, \tag{G23}$$

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

Finally, we are ready to prove Eq. (148). The first inequality there follows from the definition of $h_*(\nu)$. To prove the rest inequalities, note that

$$\ln \beta_{p_0}^{-1} = -\ln(1-\nu+\mathrm{e}^{-1}\nu^2) \geqslant \nu, \tag{G24}$$

$$\beta_{p_0} \ln \beta_{p_0}^{-1} \geqslant (1-\nu+\mathrm{e}^{-1}\nu^2)\nu \tag{G25}$$

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

$$p_0 \ln\left(p_0^{-1}\right) = \frac{\nu}{\mathrm{e}} \ln \frac{\mathrm{e}}{\nu} \geqslant (1-\nu+\mathrm{e}^{-1}\nu^2)\nu. \tag{G26}$$

Therefore,

$$\nu h(\mathrm{e}^{-1}\nu, \nu) \leqslant (1-\nu+\mathrm{e}^{-1}\nu^2)^{-1} \leqslant 1+(\mathrm{e}-1)\nu \leqslant \mathrm{e}, \tag{G27}$$

which confirms Eq. (148) in Lemma 12. Here, the second inequality follows from the inequality below

$$\begin{aligned}&(1-\nu+\mathrm{e}^{-1}\nu^2)[1+(\mathrm{e}-1)\nu] \\ &\quad = 1+\mathrm{e}^{-1}\nu(1-\nu)(\mathrm{e}^2-2\mathrm{e}+\nu-\mathrm{e}\nu) \geqslant 1,\end{aligned} \tag{G28}$$

given that $0 < \nu \leqslant 1$. ■

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 Ω 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 $0 \leqslant Q_k \leqslant 1$. 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

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

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 Ω. 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 Ω 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. ■

[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, Multiparty 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**, 113022 (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 (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).

[23] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. G. Rarity, and M. S. Tame, Experimental verification of multipartite entanglement in quantum networks, Nat. Commun. **7**, 13251 (2016).

[24] D. Markham and A. Krause, A simple protocol for certifying graph states and applications in quantum networks, arXiv:1801.05057.

[25] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Bell's theorem without inequalities, Am. J. Phys. **58**, 1131 (1990).

[26] V. Scarani, A. Acín, E. Schenck, and M. Aspelmeyer, Nonlocality of cluster states of qubits, Phys. Rev. A **71**, 042325 (2005).

[27] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, Bell Inequalities for Graph States, Phys. Rev. Lett. **95**, 120405 (2005).

[28] M. Gachechiladze, C. Budroni, and O. Gühne, Extreme Violation of Local Realism in Quantum Hypergraph States, Phys. Rev. Lett. **116**, 070401 (2016).

[29] R. H. Dicke, Coherence in spontaneous radiation processes, Phys. Rev. **93**, 99 (1954).

[30] H. Häffner, W. Hänsel, C. F. Roos, J. Benhelm, D. Chek-al-kar, M. Chwalla, T. Körber, U. D. Rapol, M. Riebe, P. O. Schmidt, C. Becher, O. Gühne, W. Dür, and R. Blatt, Scalable multiparticle entanglement of trapped ions, Nature (London) **438**, 643 (2005).

[31] L. Pezzè, A. Smerzi, M. K. Oberthaler, R. Schmied, and P. Treutlein, Quantum metrology with nonclassical states of atomic ensembles, Rev. Mod. Phys. **90**, 035005 (2018).

[32] F. Verstraete, V. Murg, and J. I. Cirac, Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems, Adv. Phys. **57**, 143 (2008).

[33] R. Orús, A practical introduction to tensor networks: Matrix product states and projected entangled pair states, Ann. Phys. **349**, 117 (2014).

[34] *Quantum State Estimation*, Lecture Notes in Physics, Vol. 649, edited by M. G. A. Paris and J. Řeháček (Springer, Berlin, 2004).

[35] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, Quantum State Tomography Via Compressed Sensing, Phys. Rev. Lett. **105**, 150401 (2010).

[36] S. T. Flammia and Y.-K. Liu, Direct Fidelity Estimation from Few Pauli Measurements, Phys. Rev. Lett. **106**, 230501 (2011).

[37] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inf. Comput. **4**, 273 (2004).

[38] I. Šupić and J. Bowles, Self-testing of quantum systems: a review, arXiv:1904.10042.

[39] M. Hayashi, K. Matsumoto, and Y. Tsuda, A study of LOCC-detection of a maximally entangled state using hypothesis testing, J. Phys. A: Math. Gen. **39**, 14427 (2006).

[40] M. Hayashi, Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing, New J. Phys. **11**, 043028 (2009).

[41] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, Reliable quantum certification of photonic state preparations, Nat. Commun. **6**, 8498 (2015).

[42] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States, Phys. Rev. X **8**, 021060 (2018).

[43] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements, Phys. Rev. Lett. **120**, 170502 (2018).

[44] H. Zhu and M. Hayashi, Optimal verification and fidelity estimation of maximally entangled states, Phys. Rev. A **99**, 052346 (2019).

[45] Z. Li, Y.-G. Han, and H. Zhu, Efficient verification of bipartite pure states, Phys. Rev. A **100**, 032316 (2019).

[46] K. Wang and M. Hayashi, Optimal verification of two-qubit pure states, Phys. Rev. A **100**, 032315 (2019).

[47] X.-D. Yu, J. Shang, and O. Gühne, Optimal verification of general bipartite pure states, npj Quantum Inf. **5**, 112 (2019).

[48] Z. Li, Y.-G. Han, and H. Zhu, Optimal Verification of Greenberger-Horne-Zeilinger States, arXiv:1909.08979.

[49] H. Zhu and M. Hayashi, Efficient Verification of Hypergraph States, Phys. Rev. Appl. **12**, 054047 (2019).

[50] M. Hayashi and Y. Takeuchi, Verifying commuting quantum computations via fidelity estimation of weighted graph states, New J. Phys. **21**, 093060 (2019).

[51] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang, Efficient Verification of Dicke States, Phys. Rev. Appl. **12**, 044020 (2019).

[52] W.-H. Zhang, Z. Chen, X.-X. Peng, X.-Y. Xu, P. Yin, X.-J. Ye, J.-S. Xu, G. Chen, C.-F. Li, and G.-C. Guo, Experimental Optimal Verification of Entangled States using Local Measurements, arXiv:1905.12175.

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

[54] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario, Phys. Rev. Lett. **123**, 260504 (2019).

[55] A. Dimić and B. Dakić, Single-copy entanglement detection, npj Quantum Inf. **4**, 11 (2018).

[56] H. Zhu and H. Zhang, Efficient verification of quantum gates with local operations, arXiv:1910.14032.

[57] Y.-C. Liu, J. Shang, X.-D. Yu, and X. Zhang, Efficient and practical verification of quantum processes, arXiv:1910.13730.

[58] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. **8**, 15485 (2017).

[59] D. Schlingemann, Stabilizer codes can be realized as graph codes, Quantum Inf. Comput. **2**, 307 (2002).

[60] M. Grassl, A. Klappenecker, and M. Rötteler, Graphs, quadratic forms, and quantum codes, in *Proceedings of the 2002 IEEE International Symposium on Information Theory* (IEEE Information Theory Society, Lausanne, Switzerland, 2002).

[61] L. Hartmann, J. Calsamiglia, W. Dür, and H. J. Briegel, Weighted graph states and applications to spin chains, lattices and gases, J. Phys. B: At. Mol. Opt. Phys. **40**, S1 (2007).

[62] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, Self-testing multipartite entangled states through projections onto two systems, New J. Phys. **20**, 083041 (2018).

[63] M. Fadel, Self-testing Dicke states, arXiv:1707.01215.