# Optimal verification and fidelity estimation of maximally entangled states

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

[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]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542 Singapore*

(Received 20 February 2019; published 28 May 2019)

We study the verification of maximally entangled states by virtue of the simplest measurement settings: local projective measurements without adaption. We show that optimal protocols are in one-to-one correspondence with complex projective 2-designs constructed from orthonormal bases. Optimal protocols with minimal measurement settings are in one-to-one correspondence with complete sets of mutually unbiased bases. Based on this observation, optimal protocols are constructed explicitly for any local dimension, which can also be applied to estimating the fidelity with the target state and to detecting entanglement. In addition, we show that incomplete sets of mutually unbiased bases are optimal for verifying maximally entangled states when the number of measurement settings is restricted. Moreover, we construct optimal protocols for the adversarial scenario in which state preparation is not trusted. The number of tests has the same scaling behavior as the counterpart for the nonadversarial scenario; the overhead is no more than three times. We also show that the entanglement of the maximally entangled state can be certified with any given significance level using only one test as long as the local dimension is large enough.

DOI: 10.1103/PhysRevA.99.052346

## I. INTRODUCTION

Entanglement is a valuable resource in quantum information processing and a focus of foundational studies. Maximally entangled states are particularly useful because of their applications in many quantum information processing tasks, such as teleportation, dense coding, and quantum cryptography. They are also standard units in entanglement manipulations and transformations and thus play a fundamental role in the resource theory of entanglement [1,2].

In practice, it is not easy to produce perfect maximally entangled states due to various experimental imperfections. It is therefore crucial to efficiently verify the states produced within a given precision based on accessible measurements. Since it is in general very difficult to perform entangling measurements, it is natural to restrict our attention to measurements that can be realized by local operations and classical communication (LOCC) [1], which is a standard paradigm in quantum information processing. This problem has been studied before [3–8], but most previous approaches entail continuous measurements, which are not practical; see Ref. [6] for a preliminary study on the applications of discrete measurements based on symmetric informationally complete measurements [9] and mutually unbiased bases (MUBs) [10–12].

In this work, we propose practical and efficient protocols for verifying maximally entangled states, which require only a few local projective (LP) measurements without adaption. We prove that optimal protocols based on LP measurements are in one-to-one correspondence with weighted complex projective 2-designs constructed from orthonormal bases. Optimal protocols with minimal measurement settings are in one-to-one correspondence with complete sets of MUBs. For any local dimension $d$, optimal protocols can be constructed using at most $\lceil \frac{3}{4}(d-1)^2 \rceil + 1$ distinct measurement settings. These protocols can also be applied to fidelity estimation and entanglement detection. Besides, incomplete sets of MUBs can be used to construct optimal verification protocols when the number of measurement settings is restricted.

Moreover, our approach can be applied to the adversarial scenario in which the states to be verified are prepared by an untrusted party. In this case, our protocols built on LOCC are even optimal among protocols that allow entangling measurements. In addition, we prove that the entanglement of the maximally entangled state can be certified with any given significance level using only one test as long as the local dimension is large enough. Again, entangling measurements are not necessary to achieve this goal. Compared with previous works on single-copy entanglement detection [13,14], our protocol requires a smaller local dimension to achieve a given significance level.

Our study not only provides practical and efficient protocols for verifying maximally entangled states, but also highlights the operational significance of 2-designs and MUBs.

*zhuhuangjun@fudan.edu.cn

†masahito@math.nagoya-u.ac.jp

 ©2019 American Physical Society

The connection between maximally entangled states and maximally incompatible measurements featured in this work is also of intrinsic interest.

## II. VERIFICATION OF PURE STATES

### A. Nonadversarial scenario

Before studying optimal verification of maximally entangle states under LOCC, it is instructive to review the general framework of pure-state verification [8,15], though here we consider more general measurements. Suppose we have a device that is expected to prepare the target state $|\Psi\rangle$. In reality, it turns out the device produces $\sigma_1, \sigma_2, \ldots, \sigma_N$ in $N$ runs. Now our task is to distinguish between the two cases, assuming that either $\sigma_j$ is identical with $|\Psi\rangle\langle\Psi|$ for all $j$ or $\langle\Psi|\sigma_j|\Psi\rangle \leqslant 1-\epsilon$ for all $j$. To this end we can perform two-outcome measurements from a set of accessible measurements. Each two-outcome measurement $\{E_j, 1-E_j\}$ is specified by a test operator $E_j$, which satisfies the condition $0 \leqslant E_j \leqslant 1$ and corresponds to passing the test. It is natural to choose $E_j$ such that the target state $|\Psi\rangle$ always passes the test; that is, $E_j|\Psi\rangle = |\Psi\rangle$ for all $E_j$. For comparison, the maximal probability that $\sigma_j$ can pass the test in the case $\langle\Psi|\sigma_j|\Psi\rangle \leqslant 1-\epsilon$ is given by [8,15]

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

where $\Omega = p_j E_j$ with $p_j$ being the probability of performing the test $E_j$, $\beta(\Omega)$ is the second largest eigenvalue of $\Omega$, and $\nu(\Omega) = 1-\beta(\Omega)$ is the spectral gap from the maximal eigenvalue. Here $\Omega$ is referred to as a verification operator and a strategy.

After $N$ runs, $\sigma_j$ in the bad case can pass all tests with probability at most $[1-\nu(\Omega)\epsilon]^N$. To guarantee significance level $\delta$ (that is, $[1-\nu(\Omega)\epsilon]^N \leqslant \delta$), the minimum number of tests reads

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

Note that passing a single test guarantees the significance level $1-\nu(\Omega)\epsilon$. That is, only one test is required if

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

Here, the meaning of the significance level $\delta$ is that the probability of passing the test is not larger than $\delta$ as long as $\langle\Psi|\sigma_j|\Psi\rangle \leqslant 1-\epsilon$.

The number in Eq. (2) decreases monotonically with $\nu(\Omega)$. If all measurements are accessible, then the best strategy is composed of the test $\{|\Psi\rangle\langle\Psi|, 1-|\Psi\rangle\langle\Psi|\}$ based on an entangling measurement. In this case we have $\Omega = |\Psi\rangle\langle\Psi|$, $\nu(\Omega) = 1$, $N = \lceil \ln\delta/\ln(1-\epsilon)\rceil$, and the condition in Eq. (3) reduces to $\epsilon + \delta \geqslant 1$.

### B. Adversarial scenario

In the adversarial scenario, the states are prepared by a potentially malicious adversary. In this case, we can still verify the target state by first performing a random permutation on $N+1$ systems before applying the strategy $\Omega$ to $N$ systems [15]. Now the performance depends on other eigenvalues of $\Omega$ in addition to $\beta(\Omega)$ (or $\nu(\Omega)$). Denote by $F(N,\delta,\Omega)$ the minimum fidelity of the reduced state of the remaining party with the target state when $N$ tests are passed with significance level $\delta$. Denote by $N(\epsilon,\delta,\Omega)$ the minimum number of tests required to verify the target state within infidelity $\epsilon$ and significance level $\delta$. In general, it is not easy to derive analytical formulas for $F(N,\delta,\Omega)$ and $N(\epsilon,\delta,\Omega)$. Nevertheless, such formulas have been derived in Ref. [15] for two cases most relevant to the current study.

According to Ref. [15], if $\Omega$ is singular (has a zero eigenvalue), then we have

$$F(N,\delta,\Omega) \leqslant 1-\min\left\{\frac{1-\delta}{N\delta\nu(\Omega)}, \frac{1}{(N+1)\delta}, 1\right\}. \quad (4)$$

If in addition $\nu(\Omega) \geqslant 1/2$, then the upper bound is saturated; that is,

$$F(N,\delta,\Omega) = 1-\min\left\{\frac{1-\delta}{N\delta\nu(\Omega)}, \frac{1}{(N+1)\delta}, 1\right\}. \quad (5)$$

The minimum number of tests required to verify $|\Psi\rangle$ within infidelity $\epsilon$ and significance level $\delta$ reads [15]

$$N(\epsilon,\delta,\Omega) = \min\left\{\left\lceil\frac{1-\delta}{\nu(\Omega)\delta\epsilon}\right\rceil, \left\lceil\frac{1}{\delta\epsilon}-1\right\rceil\right\}. \quad (6)$$

Compared with Eq. (2), the scaling with $\delta$ in Eq. (6) is suboptimal. When the strategy $\Omega$ is composed of the entangling test $\{|\Psi\rangle\langle\Psi|, 1-|\Psi\rangle\langle\Psi|\}$ for example, we have $\nu(\Omega) = 1$, and $N(\epsilon,\delta,\Omega)$ is minimized among singular verification strategies. In this case, Eqs. (5) and (6) reduce to

$$F(N,\delta,\Omega) = \max\left\{\frac{(N+1)\delta-1}{N\delta}, 0\right\}, \quad (7)$$

$$N(\epsilon,\delta,\Omega) = \left\lceil\frac{1-\delta}{\delta\epsilon}\right\rceil. \quad (8)$$

Therefore, it is impossible to verify the target state within infidelity $\epsilon < 1$ and significance level $\delta \leqslant 1/2$ using only one test for any singular strategy.

For a given $\beta(\Omega)$, the optimal performance is achieved when the strategy $\Omega$ is *homogeneous* [15], which means it has the form

$$\Omega = |\Psi\rangle\langle\Psi| + \lambda(1-|\Psi\rangle\langle\Psi|), \quad (9)$$

where $\lambda = \beta(\Omega)$. In this case, it is natural to write $F(N,\delta,\lambda)$ and $N(\epsilon,\delta,\lambda)$ in place of $F(N,\delta,\Omega)$ and $N(\epsilon,\delta,\Omega)$. The efficiency of $\Omega$ is determined by Eqs. (7) and (8) when $\lambda = 0$. When $0 < \lambda < 1$, define

$$\eta_k(\lambda) := \frac{k\lambda^{k-1} + (N+1-k)\lambda^k}{N+1}, \quad (10)$$

$$\zeta_k(\lambda) := \frac{(N+1-k)\lambda^k}{N+1}. \quad (11)$$

Then $F(N,\delta,\Omega)$ is given by [15]

$$F(N,\delta,\lambda) = \begin{cases} 0, & \delta \leqslant \lambda^N \\ \delta^{-1}[p_1\zeta_k(\lambda) + p_2\zeta_{k+1}(\lambda)], & \text{otherwise.} \end{cases} \quad (12)$$

Here $k$ is the largest integer that satisfies $\eta_k(\lambda) \geqslant \delta$, and $p_1$ and $p_2$ are probabilities determined by the conditions

$$p_1 + p_2 = 1, \quad p_1\eta_k(\lambda) + p_2\eta_{k+1}(\lambda) = \delta. \quad (13)$$

When $N = 1$, Eq. (12) reduces to

$$F(N,\delta,\lambda) = \begin{cases} 0, & \delta \leqslant \lambda \\ \frac{\lambda(\delta-\lambda)}{\delta(1-\lambda)}, & \lambda \leqslant \delta \leqslant \frac{1+\lambda}{2} \\ \frac{\delta(2-\lambda)-1}{\delta(1-\lambda)}, & \frac{1+\lambda}{2} \leqslant \delta \leqslant 1. \end{cases} \tag{14}$$

Therefore, one test suffices to verify the target state within infidelity $\epsilon$ and significance level $\delta$ (assuming $0 < \epsilon, \delta < 1$) as long as

$$\frac{\lambda(\delta-\lambda)}{\delta(1-\lambda)} \geqslant 1-\epsilon. \tag{15}$$

This condition is also necessary when $\delta \leqslant (1+\lambda)/2$. Note that the requirement $\delta \geqslant \lambda$ is implicitly implied in Eq. (15). As an implication, passing a single test can guarantee significance level

$$\delta \geqslant \frac{\lambda^2}{\lambda - (1-\lambda)(1-\epsilon)}. \tag{16}$$

Suppose $0 < \epsilon, \delta, \lambda < 1$. Then the minimum number $N(\epsilon,\delta,\lambda)$ of tests required to verify $|\Psi\rangle$ within infidelity $\epsilon$ and significance level $\delta$ is given by [15]

$$N(\epsilon,\delta,\lambda) = \left\lceil \min_{k\in\mathbb{Z}^{\geqslant 0}} \tilde{N}(\epsilon,\delta,\lambda,k) \right\rceil = \lceil \tilde{N}(\epsilon,\delta,\lambda,k^*) \rceil, \tag{17}$$

where

$$\tilde{N}(\epsilon,\delta,\lambda,k) := \frac{k\nu^2\delta F + \lambda^{k+1} + \lambda\delta(k\nu-1)}{\lambda\nu\delta\epsilon} \tag{18}$$

with $F = 1-\epsilon$ and $\nu = 1-\lambda$. Here $\mathbb{Z}^{\geqslant 0}$ denotes the set of non-negative integers, and $k^*$ is the largest integer $k$ that satisfies $\delta \leqslant \lambda^k/(F\nu+\lambda) = \lambda^k/(F+\lambda\epsilon)$. In addition, $k^*$ is equal to either $k_- := \lfloor \log_\lambda \delta \rfloor$ or $k_+ := \lceil \log_\lambda \delta \rceil$. In the limit $\delta \to 0$, the number $N(\epsilon,\delta,\lambda)$ can be approximated as follows (assuming that $\lambda$ is lower bounded by a positive constant) [15]:

$$N(\epsilon,\delta,\lambda) \approx \frac{F+\lambda\epsilon}{\lambda\epsilon \ln\lambda} \ln\delta, \tag{19}$$

where $F = 1-\epsilon$. In the high-precision limit $\epsilon, \delta \to 0$, which is the situation of the most interest, we have

$$N(\epsilon,\delta,\lambda) \approx (\lambda\epsilon\ln\lambda)^{-1} \ln\delta \geqslant \mathrm{e}\epsilon^{-1}\ln\delta^{-1}, \tag{20}$$

where the inequality is saturated at $\lambda = 1/\mathrm{e}$, with e being the base of the natural logarithm. Here the number of required tests has the same scaling behaviors with $\epsilon$ and $\delta$ as in the nonadversarial scenario, and the efficiency of the homogeneous strategy is characterized by the function $1/(\lambda\ln\lambda^{-1})$. The optimal performance is achieved when $\lambda = 1/\mathrm{e}$, in which case the overhead is only e times.

## III. LIMITATIONS OF LOCAL OPERATIONS AND CLASSICAL COMMUNICATION

### A. General discussions

To analyze the limitations of local measurements on quantum state verification, we need to introduce several additional concepts. A test operator $E$ is *separable* if it is a linear combination of pure product states with non-negative coefficients. The test $\{E, 1-E\}$ is separable if both $E$ and $1-E$ are separable. A verification strategy is separable if it is composed of separable tests. The strategy is *separable projective* (SP) if, in addition, each test operator is a projector. Any verification strategy realized by LOCC is separable, as illustrated in Fig. 1.

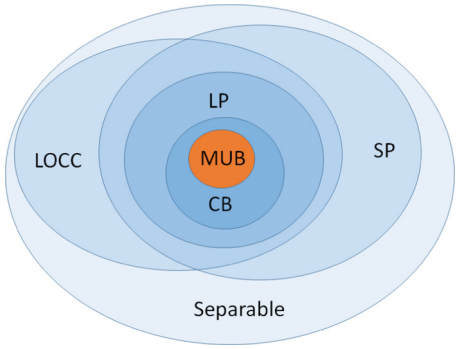


FIG. 1. Hierarchy of separable verification strategies for maximally entangled states. LP, local projective; SP, separable projective; CB, conjugate basis. Optimal CB strategies can achieve the same performance as the optimal separable strategies. Optimal MUB strategies can also achieve the same performance when the local dimension is a prime power.

The robustness of entanglement of a quantum state $\rho$ [1,16–19] is defined as

$$E_{\mathcal{R}}(\rho) := \min\left\{x | x \geqslant 0,\ \exists \text{ a state } \sigma,\ \frac{\rho + x\sigma}{1+x} \in \mathcal{S}\right\}, \tag{21}$$

where $\mathcal{S}$ denotes the set of separable states. If $\sigma$ is required to be the completely mixed state, we get the random robustness [16],

$$R(\rho) := \min\left\{x | x \geqslant 0,\ \frac{D\rho + x}{D(1+x)} \in \mathcal{S}\right\}, \tag{22}$$

where $D$ is the dimension of the whole Hilbert space. Given a pure state $|\Psi\rangle$, the following quantity is closely related to the robustness of entanglement:

$$T(\Psi) := \min\{\mathrm{tr}(E) | E \geqslant |\Psi\rangle\langle\Psi|\}, \tag{23}$$

where the minimization is taken over separable tests of the form $\{E, 1-E\}$. The following lemma is an easy consequence of the definitions of $E_{\mathcal{R}}(\Psi)$ and $T(\Psi)$.

*Lemma 1 (Theorem 2 of Ref. [20], and Ref. [21]).* Any pure state $|\Psi\rangle$ satisfies

$$T(\Psi) \geqslant E_{\mathcal{R}}(\Psi) + 1. \tag{24}$$

Each test operator $E$ of a separable strategy $\Omega$ for $|\Psi\rangle$ satisfies the inequality $\mathrm{tr}(E) \geqslant T(\Psi) \geqslant E_{\mathcal{R}}(\Psi) + 1$, so we have $\mathrm{tr}(\Omega) \geqslant T(\Psi) \geqslant E_{\mathcal{R}}(\Psi) + 1$. Similarly, we have $\mathrm{tr}(\Omega) \geqslant [1 + R(\Psi)]/[1 + R(\Psi)/D]$ if $\Omega$ is homogeneous. This observation implies the following lemma given that $|\Psi\rangle$ is an eigenstate of $\Omega$ with eigenvalue 1.

*Lemma 2.* Any separable strategy $\Omega$ for $|\Psi\rangle$ satisfies

$$\beta(\Omega) \geqslant \frac{T(\Psi)-1}{D-1} \geqslant \frac{E_{\mathcal{R}}(\Psi)}{D-1}, \tag{25}$$

where $D$ is the dimension of the whole Hilbert space. If $\Omega$ is homogeneous, then

$$\beta(\Omega) \geqslant \frac{R(\Psi)}{D + R(\Psi)}. \tag{26}$$

*Lemma 3.* The verification operator $\Omega$ of any SP strategy $\{P_l, p_l\}_{j=1}^g$ for an entangled state $|\Psi\rangle$ satisfies $\beta(\Omega) \geqslant 1/g$. The bound is saturated if and only if (iff) $\bar{P}_l := P_l - |\Psi\rangle\langle\Psi|$ are mutually orthogonal and $p_l = 1/g$ for all $l$.

*Proof.* Since $|\Psi\rangle$ is entangled, all projectors $P_l$ have ranks at least 2; that is, $\bar{P}_l$ have ranks at least 1. Therefore,

$$\beta(\Omega) = \left\| \sum_l p_l \bar{P}_l \right\| \geqslant \max_l p_l \geqslant \frac{1}{g}. \tag{27}$$

Here the second inequality is saturated iff $p_l = 1/g$ for all $l$. In that case, the first inequality is saturated iff $\bar{P}_l$ are mutually orthogonal for all $l$. This observation completes the proof of Lemma 3. ■

An SP strategy $\Omega$ composed of $g$ distinct tests is *parsimonious* if $\beta(\Omega) = 1/g$; that is, $\nu(\Omega) = (g-1)/g$. In this case, by Eq. (2), the number of measurements required to verify $|\Psi\rangle$ within infidelity $\epsilon$ and significance level $\delta$ reads

$$N = \left\lceil \frac{\ln \delta}{\ln[1-(g-1)g^{-1}\epsilon]} \right\rceil \leqslant \left\lceil \frac{g}{(g-1)\epsilon} \ln \delta^{-1} \right\rceil. \tag{28}$$

The counterpart for the adversarial scenario is given by Eq. (6) with $\nu(\Omega) = (g-1)/g$, assuming that $\Omega$ is singular.

### B. Bipartite pure states

Now we turn to a bipartite system with the Hilbert space $\mathcal{H} \otimes \mathcal{H}$ of dimension $D = d^2$. Up to a local unitary transformation, any bipartite pure state can be expressed as

$$|\Psi\rangle = \sum_{j=0}^{d-1} s_j |jj\rangle, \tag{29}$$

where the Schmidt coefficients $s_0 \geqslant s_1 \geqslant \cdots \geqslant s_{d-1}$ are arranged in decreasing order and satisfy the normalization condition $\sum_j s_j^2 = 1$. The robustness and random robustness of entanglement of $|\Psi\rangle$ are well known [1,16–19], as reproduced here:

$$E_{\mathcal{R}}(\Psi) = \left( \sum_j s_j \right)^2 - 1, \quad R(\Psi) = D s_0 s_1. \tag{30}$$

In addition, Theorem 2 of Ref. [21] showed that

$$T(\Psi) = \left( \sum_j s_j \right)^2. \tag{31}$$

By Lemma 2, any separable verification strategy $\Omega$ for $|\Psi\rangle$ satisfies

$$\beta(\Omega) \geqslant \frac{\left(\sum_j s_j\right)^2 - 1}{d^2 - 1}. \tag{32}$$

If $\Omega$ is homogeneous, then we have a stronger conclusion:

$$\beta(\Omega) \geqslant \frac{s_0 s_1}{1 + s_0 s_1}. \tag{33}$$

Here the inequality also follows from the fact that the partial transpose $(|\Psi\rangle\langle\Psi|)^{T_B}$ has an eigenvalue equal to $-s_0 s_1$, while a separable verification operator is necessarily positive partial transpose (PPT).

### C. Maximally entangled states

We are particularly interested in maximally entangled states, which have the form

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_j |jj\rangle \tag{34}$$

up to local unitary transformations. According to Eq. (32) or Eq. (33), any separable strategy $\Omega$ for $|\Phi\rangle$ satisfies

$$\beta(\Omega) \geqslant \frac{1}{d+1}, \quad \nu(\Omega) \leqslant \frac{d}{d+1}. \tag{35}$$

For a homogeneous strategy $\Omega$, Theorem 1 of Ref. [3] showed that

$$\Omega \geqslant \frac{1 + d|\Phi\rangle\langle\Phi|}{d+1}. \tag{36}$$

Also, Ref. [3] showed the existence of a local strategy that saturates the inequality in Eq. (36). The bounds in Eq. (35) are saturated iff the inequality in Eq. (36) is saturated, in which case we have

$$\Omega = \frac{1 + d|\Phi\rangle\langle\Phi|}{d+1}. \tag{37}$$

A separable strategy $\Omega$ for $|\Phi\rangle$ is *optimal* if it saturates the bound $\beta(\Omega) \geqslant 1/(d+1)$ or $\nu(\Omega) \leqslant d/(d+1)$ in Eq. (35); an SP strategy is *perfect* if it is both optimal and parsimonious.

For the optimal strategy, Eq. (2) reduces to

$$N = \left\lceil \frac{\ln \delta}{\ln[1 - d(d+1)^{-1}\epsilon]} \right\rceil \leqslant \left\lceil \frac{d+1}{d\epsilon} \ln \delta^{-1} \right\rceil. \tag{38}$$

In the independent and identically distributed case, this result can be derived from Sec. 4.3.2 and Eq. (36) of Ref. [5]; see Ref. [8] for the case $d = 2$. Notably, thanks to Eq. (3), passing a single test guarantees the significance level $1 - \frac{d}{d+1}\epsilon$ in the nonadversarial scenario. The counterpart for the adversarial scenario is given by Eq. (16) with $\lambda = 1/(d+1)$. These conclusions will have important implications for entanglement detection as we shall see in Secs. IV B and V B. In the large-$d$ limit, we have

$$N = \left\lfloor \frac{\ln \delta}{\ln(1-\epsilon)} \right\rfloor + 1 \leqslant \left\lceil \frac{\ln \delta^{-1}}{\epsilon} \right\rceil. \tag{39}$$

The number of tests is almost the same as what is required by the best strategy based on entangling measurements.

Let $\rho$ be an arbitrary quantum state and

$$F(\rho, |\Phi\rangle\langle\Phi|) := \mathrm{tr}(\rho|\Phi\rangle\langle\Phi|) \tag{40}$$

the fidelity between $\rho$ and $|\Phi\rangle\langle\Phi|$. If $\Omega$ is the optimal strategy given in Eq. (37), then

$$\mathrm{tr}(\rho\Omega) = \frac{1 + dF(\rho, |\Phi\rangle\langle\Phi|)}{d+1} \tag{41}$$

(cf. Theorem 1 in Ref. [3]), so the fidelity can be inferred from the passing probability,

$$F(\rho, |\Phi\rangle\langle\Phi|) = \frac{(d+1)\,\mathrm{tr}(\rho\Omega) - 1}{d}. \tag{42}$$

Therefore, homogeneous verification strategies can also serve for fidelity estimation.

## IV. VERIFICATION OF MAXIMALLY ENTANGLED STATES

### A. Parsimonious and optimal verification strategies

Given any basis $\mathcal{B} = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_d\rangle\}$ for $\mathcal{H}$ (in this paper we only consider orthonormal bases), we can devise a *conjugate-basis* (CB) test as follows: Alice performs the projective measurement on the basis $\mathcal{B}$, while Bob performs the projective measurement on the conjugate basis $\mathcal{B}^* = \{|\psi^*\rangle : |\psi\rangle \in \mathcal{B}\}$, where $|\psi^*\rangle$ denotes the complex conjugate of $|\psi^*\rangle$ (with respect to the given computational basis used to define $|\Phi\rangle$). The CB test is passed if Alice and Bob obtain the same outcome; in other words, the pass eigenspace is spanned by $|\psi\rangle \otimes |\psi^*\rangle$ for all $|\psi\rangle \in \mathcal{B}$, and the test projector has the form

$$P(\mathcal{B}) := \sum_{|\psi\rangle\in\mathcal{B}} |\psi\rangle\langle\psi| \otimes |\psi^*\rangle\langle\psi^*|, \tag{43}$$

which has rank $d$. A similar idea was used to construct general tests from positive operator-valued measures on $\mathcal{H}$ (see Eq. (13) of Ref. [5]), while the test here is simpler and easier to realize. Note that $P(\mathcal{B})|\Phi\rangle = |\Phi\rangle$ for any orthonormal basis $\mathcal{B}$ of $\mathcal{H}$, so $|\Phi\rangle$ can pass the test with certainty as desired. A CB strategy $\{P(\mathcal{B}_l), p_l\}_l$ is composed of CB tests, where $\mathcal{B}_l$ are bases for $\mathcal{H}$, and $p_l$ form a probability distribution. The resulting verification operator reads

$$\Omega = \sum_l p_l P_l = \sum_l p_l \sum_{|\psi\rangle\in\mathcal{B}_l} |\psi\rangle\langle\psi| \otimes |\psi^*\rangle\langle\psi^*|. \tag{44}$$

*Proposition 1.* Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two orthonormal bases for $\mathcal{H}$. Then $\bar{P}(\mathcal{B}_1)$ and $\bar{P}(\mathcal{B}_2)$ are orthogonal iff $\mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased.

Here $\bar{P}(\mathcal{B}) = P(\mathcal{B}) - |\Phi\rangle\langle\Phi|$. Proposition 1 is an implication of the following inequality:

$$\begin{aligned}\mathrm{tr}[\bar{P}(\mathcal{B}_1)\bar{P}(\mathcal{B}_2)] + 1 &= \mathrm{tr}[P(\mathcal{B}_1)P(\mathcal{B}_2)] \\ &= \sum_{|\psi\rangle\in\mathcal{B}_1, |\varphi\rangle\in\mathcal{B}_2} |\langle\psi|\varphi\rangle|^4 \geqslant 1,\end{aligned} \tag{45}$$

which is saturated iff $\mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased; that is, $|\langle\psi|\varphi\rangle|^2 = 1/d$ for all $|\psi\rangle \in \mathcal{B}_1$ and $|\varphi\rangle \in \mathcal{B}_2$ [10]. Lemma 3 and Proposition 1 together yield Proposition 2.

*Proposition 2.* Let $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_g$ be $g$ bases for $\mathcal{H}$. The CB strategy $\{P(\mathcal{B}_l), p_l\}$ is parsimonious iff $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_g$ are mutually unbiased and all $p_l$ are equal to $1/g$. The strategy is perfect iff, in addition, $g = d + 1$, so that $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_g$ form a complete set of MUBs.

An MUB strategy is a CB strategy based on MUBs and with uniform probabilities, which is parsimonious by Proposition 2. If a set of $g$ MUBs is available, then the number of tests required to verify $|\Phi\rangle$ within infidelity $\epsilon$ and significance level $\delta$ in the nonadversarial scenario is given by Eq. (2) with $\nu(\Omega) = (g-1)/g$; that is, $\beta(\Omega) = 1/g$. Incidentally, the maximally entangled state $|\Phi\rangle$ is equivalent to a qudit graph state for which we have introduced a general verification protocol called the cover protocol [15]; see also Ref. [22] when $d = 2$. In retrospect, the cover protocol in this special case is equivalent to an MUB strategy constructed from two bases (that is $g = 2$).

For $d \geqslant 2$, there exist at least three bases that are mutually unbiased [10]. Define operators $Z$ and $X$ as follows:

$$Z|j\rangle = \omega^j|j\rangle, \quad X|j\rangle = |j+1\rangle, \quad \omega = \mathrm{e}^{2\pi\mathrm{i}/d}, \tag{46}$$

where $j \in \mathbb{Z}_d$ and $\mathbb{Z}_d$ is the ring of integers modulo $d$. Then the two operators $Z$ and $X$ generate the Heisenberg-Weyl group (up to phase factors), which reduces to the Pauli group in the case of a qubit. The respective eigenbases of the three operators $Z$, $X$, and $XZ$ are mutually unbiased [10], and a parsimonious strategy can be constructed using the three bases; here the test projectors can be expressed explicitly as in Eq. (48) below. So the maximally entangled state $|\Phi\rangle$ in any dimension $d$ can be verified within infidelity $\epsilon$ and significance level $\delta$ with only

$$\left\lceil \frac{\ln\delta}{\ln(1-2\epsilon/3)} \right\rceil \leqslant \left\lceil \frac{3}{2\epsilon} \ln\delta^{-1} \right\rceil \tag{47}$$

tests according to Eq. (28). This number is only 50% more than the number required by the best strategy based on entangling measurements.

If $d$ has the prime-power decomposition $d = \prod_{j=1}^r p_j^{n_j}$, where $p_j$ are distinct primes and $n_j$ are positive integers, then at least $\min_j(p_j^{n_j} + 1)$ bases can be found that are mutually unbiased. In particular, a complete set of $d + 1$ MUBs can be constructed when the dimension is a prime power [10–12]. When the dimension $d$ is a prime, for example, the respective eigenbases of $Z, X, XZ, XZ^2, \ldots, XZ^{d-1}$ form a complete set of MUBs. In this case, the $d + 1$ test projectors can be expressed as

$$P_0 = \frac{1}{d}\sum_{k=0}^{d-1}(Z \otimes Z^{-1})^k = \sum_j |jj\rangle\langle jj|, \tag{48a}$$

$$P_{m+1} = \frac{1}{d}\sum_{k=0}^{d-1}(XZ^m \otimes XZ^{-m})^k, \quad m = 0, 1, \ldots, d-1. \tag{48b}$$

The resulting verification protocol is perfect, and the number of tests required to verify $|\Phi\rangle$ attains the lower bound in Eq. (38). When $d = 2$, the three test projectors read

$$\frac{1+Z^{\otimes 2}}{2}, \quad \frac{1+X^{\otimes 2}}{2}, \quad \frac{1-Y^{\otimes 2}}{2}, \tag{49}$$

with $Y = \mathrm{i}XZ$, which reproduce the result in Ref. [8].

When a complete set of MUBs is not available, we can still devise optimal verification protocols for $|\Phi\rangle$ using (weighted complex projective) 2-designs. Let $P_+$ be the projector onto the symmetric subspace of $\mathcal{H}^{\otimes 2}$. A weighted set of kets $\{|\psi_\xi\rangle, w_\xi\}$ in $\mathcal{H}$ with $w_\xi \geqslant 0$ and $\sum_\xi w_\xi = d$ is a *2-design* [23–25] if $\sum_\xi w_\xi(|\psi_\xi\rangle\langle\psi_\xi|)^{\otimes 2} = 2P_+/(d+1)$; that is

$$\sum_\xi w_\xi(|\psi_\xi\rangle\langle\psi_\xi|) \otimes (|\psi_\xi^*\rangle\langle\psi_\xi^*|) = \frac{1}{d+1}(1 + d|\Phi\rangle\langle\Phi|). \tag{50}$$

Let $\{\mathcal{B}_l, p_l\}_l$ be a weighted set of kets with the uniform weight $p_l$ for all kets in basis $l$ and $\sum_l p_l = 1$; note that

the total weight is $d\sum_l p_l = d$. Then $\{\mathcal{B}_l, p_l\}_l$ forms a 2-design iff $\Omega = \sum_l p_l P(\mathcal{B}_l) = (1 + d|\Phi\rangle\langle\Phi|)/(d+1)$. This observation confirms the following result.

*Proposition 3.* A CB strategy $\{P(\mathcal{B}_l), p_l\}$ is optimal iff $\{\mathcal{B}_l, p_l\}_l$ forms a 2-design.

Propositions 2 and 3 together imply the following result first derived in Ref. [26] (cf. Theorem 3.2 there): at least $d+1$ bases are needed for constructing a 2-design in dimension $d$; if the lower bound is saturated, then all bases are mutually unbiased and have the same weight. When $d$ is a prime power, the lower bound can always be saturated [10,12,27,28]. When $d+1$ is a prime power, a 2-design can be constructed from $d+2$ bases according to Ref. [26], so an optimal CB strategy can be constructed using only $d+2$ measurement settings. When $d = 6$, for example, a 2-design can be constructed from eight bases, although a complete set of MUBs is not expected to exist.

*Proposition 4.* For any maximally entangled state with local dimension $d \geqslant 3$, an optimal verification protocol can be devised with at most $\lceil \frac{3}{4}(d-1)^2 \rceil + 1$ distinct CB tests.

*Proof.* According to Theorem 4.1 and Proposition 4.3 in Ref. [26], a (weighted) 2-design can be constructed explicitly from $\lceil \frac{3}{4}(d-1)^2 \rceil + 1$ bases, from which we can devise an optimal verification protocol with $\lceil \frac{3}{4}(d-1)^2 \rceil + 1$ distinct CB tests by Proposition 3. ■

Thanks to Proposition 4, the number of tests required to verify $|\Phi\rangle$ within infidelity $\epsilon$ and significance level $\delta$ can always attain the lower bound in Eq. (38). Propositions 2, 3, and 4 highlight the significance of MUBs and 2-designs for the verification, fidelity estimation, and entanglement detection of the maximally entangled state $|\Phi\rangle$.

Next, we show that all parsimonious strategies based on LP measurements (that is, projective measurements on product bases) and all optimal strategies (including perfect strategies) based on SP measurements are actually CB strategies. These results further strengthen the significance of MUBs and 2-designs. The following two theorems are proved in the Appendix.

*Theorem 1.* An LP strategy $\{P_l, p_l\}_{j=1}^g$ with $g \geqslant 2$ is parsimonious iff $p_l = 1/g$ and $P_l = P(\mathcal{B}_l)$, where the $g$ bases $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_g$ are mutually unbiased. The strategy is perfect iff, in addition, $g = d+1$, so that $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_g$ form a complete set of MUBs.

*Remark 1.* An LP strategy is a strategy based on LP measurements, in which each test is realized by performing an LP measurement and then selecting suitable outcomes; cf. Eq. (A2) in the Appendix. By definition, each LP test projector on $\mathcal{H}^{\otimes 2}$ is diagonal in some product basis.

*Theorem 2.* An SP strategy $\{P_l, p_l\}_{j=1}^g$ is optimal iff there exist $g$ bases $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_g$ such that $P_l = P(\mathcal{B}_l)$ and $\{\mathcal{B}_l, p_l\}_l$ forms a 2-design. The strategy is perfect iff, in addition, $g = d+1$, $p_l = 1/(d+1)$, and $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_g$ form a complete set of MUBs.

Theorem 2 is quite surprising given that no obvious bases are involved in the definition of SP strategies. In addition to the applications in state verification, Theorem 2 also sheds light on the existence problem on MUBs.

*Corollary 1.* There exists a complete set of MUBs in dimension $d$ iff there exist $d+1$ separable projectors $P_1, P_2, \ldots, P_{d+1}$ such that $P_j \geqslant |\Phi\rangle\langle\Phi|$ for all $j$ and that $P_j - |\Phi\rangle\langle\Phi|$ are mutually orthogonal.

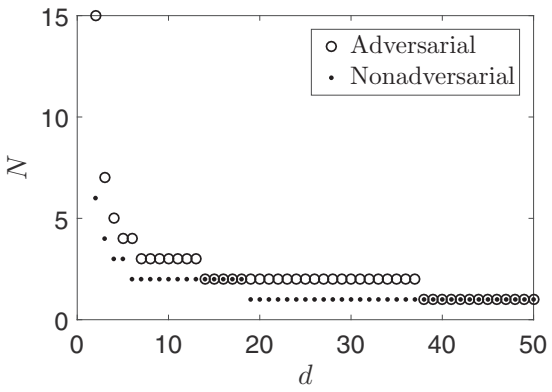


FIG. 2. Certification of the entanglement of maximally entangled states in the adversarial scenario and nonadversarial scenario. Here $d$ is the local dimension and $N$ is the number of tests required to certify the entanglement with significance level $\delta = 0.1$. In the nonadversarial scenario, the optimal strategy $\Omega$ with $\beta(\Omega) = 1/(d+1)$ is applied [cf. Eq. (37)]. In the adversarial scenario, a homogeneous strategy $\Omega'$ with $\beta(\Omega') = 2/(d+1)$ is applied. In both scenarios, one test is sufficient when $d$ is large enough.

### B. Applications to entanglement detection

Note that $\rho$ is entangled when the fidelity $F(\rho, |\Phi\rangle\langle\Phi|)$ is larger than $1/d$. Given a verification strategy $\Omega$, to certify the entanglement of $|\Phi\rangle$ with significance level $\delta$, the number of tests is given by Eq. (2) with $\epsilon = (d-1)/d$; that is,

$$N_{\mathrm{E}} = \left\lceil \frac{\ln \delta}{\ln[1 - d^{-1}(d-1)\nu(\Omega)]} \right\rceil \geqslant \left\lceil \frac{\ln \delta^{-1}}{\ln d} \right\rceil. \tag{51}$$

In particular, passing a single test can guarantee the significance level $1 - \frac{d-1}{d}\nu(\Omega)$ in the nonadversarial scenario, which also follows from Eq. (3). The bound in Eq. (51) can be attained by the strategy $\Omega = |\Phi\rangle\langle\Phi|$ based on the entangling measurement $\{|\Phi\rangle\langle\Phi|, 1 - |\Phi\rangle\langle\Phi|\}$. In this case, the entanglement of $|\Phi\rangle$ can be certified using only one test for any given significance level $\delta$ if the local dimension satisfies the condition $d \geqslant \delta^{-1}$.

In practice, it is more convenient to apply strategies based on local measurements. If $\Omega$ is the optimal local strategy with $\nu(\Omega) = d/(d+1)$ (for example, the strategy based on a complete set of MUBs), then Eq. (51) reduces to

$$N_{\mathrm{E}} = \left\lceil \frac{\ln \delta}{\ln 2 - \ln(d+1)} \right\rceil. \tag{52}$$

Surprisingly, the entanglement of $|\Phi\rangle$ can be certified with only one test based on local measurements when

$$d \geqslant 2\delta^{-1} - 1, \tag{53}$$

as illustrated in Fig. 2. If $\Omega$ is a parsimonious strategy with $g$ distinct tests, then $\nu(\Omega) = (g-1)/g$, so that Eq. (51) reduces to

$$N_{\mathrm{E}} = \left\lceil \frac{\ln \delta}{\ln(g+d-1) - \ln(gd)} \right\rceil, \tag{54}$$

which approaches $\lfloor \ln \delta^{-1}/\ln g \rfloor + 1$ in the large-$d$ limit. Again, one test is sufficient when $g > \delta^{-1}$ and $d$ is large enough.

Recently, Ref. [13] (see also Ref. [14]) showed that the entanglement of certain multipartite states, such as linear cluster states and tensor powers of the singlet, can be certified using only one test. In general it is not easy to make a fair comparison between their results and our results because the problems considered and starting points in the two works are different. With this caveat in mind, we present the following observations. In the case of the singlet, the protocol in Ref. [13] is similar to the protocol in Ref. [8] and is a special case of our general protocol based on complete sets of MUBs [see Eq. (49)]. Reference [13] essentially demonstrates that the entanglement of the singlet can be certified to any given significance if the number of copies is large enough, though the collection of singlets is considered as a whole and single-copy detection means a single copy of such a collection. According to Eq. (10) in Ref. [13], to achieve significance level $\delta$ (corresponding to confidence level $1-\delta$), the number of required tests satisfies

$$N \geqslant \frac{\ln \delta}{\ln \frac{2}{3}} = \frac{\log_2 \delta}{\log_2 \frac{2}{3}}, \tag{55}$$

which corresponds to a local dimension of

$$2^N \geqslant \delta^{-1/\log_2(3/2)} \approx \delta^{-1.71} \tag{56}$$

if these singlets are considered as a bipartite maximally entangled state. This dimension is in general much larger than the counterpart in Eq. (53) required by our protocol. When $\delta = 0.05$, for example, the smallest local dimension required by Ref. [13] is $2^N = 256$, while it is only 39 for our optimal protocol. Our protocol is more efficient because it involves collective measurements across different copies if the maximally entangled state is composed of many copies of two-qubit Bell states.

## V. VERIFICATION OF MAXIMALLY ENTANGLED STATES IN THE ADVERSARIAL SCENARIO

### A. Optimal verification strategies

In the adversarial scenario, the efficiency of a verification strategy $\Omega$ will depend on smaller eigenvalues as well as $\beta(\Omega)$. In this case, singular verification strategies are not efficient for high-precision verification according to Eqs. (6) and (8), even for the strategy $\Omega$ based on the entangling test $\{|\Phi\rangle\langle\Phi|, 1-|\Phi\rangle\langle\Phi|\}$, which is optimal for the nonadversarial scenario when there is no restriction on the measurements. Here we construct optimal protocols for the adversarial scenario.

If there is no restriction on the measurements, the optimal strategy can always be chosen to be homogeneous. In the high-precision limit, a strategy $\Omega$ is optimal in the adversarial scenario if it is homogeneous with $\beta(\Omega) = 1/\mathrm{e}$ [15]. For the maximally entangled state $|\Phi\rangle$, we can construct a homogeneous strategy $\Omega$ with $\beta(\Omega) = 1/(d+1)$ according to Sec. IV A. To construct the optimal strategy, it suffices to add the trivial test with a suitable probability $p$. Here "trivial test" refers to the test associated with the identity operator, so that all states can pass the test for sure [15]. Note that

$$|\Phi\rangle\langle\Phi| + \lambda(1-|\Phi\rangle\langle\Phi|) = (1-p)\frac{1+d|\Phi\rangle\langle\Phi|}{d+1} + p \tag{57}$$

if

$$p = \frac{(d+1)\lambda - 1}{d}. \tag{58}$$

In this way, any homogeneous strategy $\Omega$ that satisfies the condition $1/(d+1) \leqslant \beta(\Omega) < 1$ can be constructed by virtue of local projective measurements. In particular, we can construct a homogeneous strategy $\Omega$ with $\beta(\Omega) = 1/\mathrm{e}$ by choosing $p = (d+1-\mathrm{e})/(\mathrm{e}d)$. Then the number of tests attains the minimum in the high-precision limit; that is,

$$N(\epsilon, \delta, \lambda) \approx \mathrm{e}\epsilon^{-1} \ln \delta^{-1}. \tag{59}$$

In general, the optimal value of $\beta(\Omega)$ depends on the target infidelity $\epsilon$ and significance level $\delta$. For high-precision verification, nevertheless, this value is close to $1/\mathrm{e}$ [15]. Such strategies can also be constructed by virtue of local projective measurements.

### B. Applications to entanglement detection

Recall that a bipartite state $\rho$ is entangled whenever $\langle\Phi|\rho|\Phi\rangle > 1/d$. Given a strategy $\Omega$ for the maximally entangled state $|\Phi\rangle$, the number of tests required to certify its entanglement with significance level $\delta$ is $N(\epsilon, \delta, \Omega)$ with $\epsilon = (d-1)/d$. Now the analysis in Sec. V A is not so relevant because $\epsilon$ is quite large. Nevertheless, singular verification strategies are still not efficient when $\delta$ is small.

If $\Omega$ is the strategy based on the entangling test $\{|\Phi\rangle\langle\Phi|, 1-|\Phi\rangle\langle\Phi|\}$, then $\nu(\Omega) = 1$, and the number of tests is given by Eq. (8) with $\epsilon = (d-1)/d$; that is,

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

When $\delta \ll 1$, we have $N(\epsilon, \delta, \Omega) \approx d/[(d-1)\delta]$, so the number of tests is approximately inversely proportional to $\delta$. If $\Omega$ is a parsimonious strategy composed of $g$ distinct tests with $g \leqslant d$ as constructed in Sec. IV A, then the number of tests is determined by Eq. (6) with $\nu(\Omega) = (g-1)/g$ and $\epsilon = (d-1)/d$, that is,

$$N(\epsilon, \delta, \Omega) = \min\left\{ \left\lceil \frac{gd(1-\delta)}{(g-1)(d-1)\delta} \right\rceil, \left\lceil \frac{d}{(d-1)\delta} - 1 \right\rceil \right\}, \tag{61}$$

which is approximately equal to the number in Eq. (60).

As in Sec. V A, the optimal strategy for certifying the entanglement of $|\Phi\rangle$ can be chosen to be homogeneous. Given a homogeneous strategy $\Omega$ with $\beta(\Omega) = \lambda$, the number of required tests is $N(\epsilon, \delta, \lambda)$ presented in Eq. (17) with $\epsilon = (d-1)/d$ [15]. When $\delta \ll \lambda$, we have

$$N(\epsilon, \delta, \lambda) \approx \frac{1+(d-1)\lambda}{(d-1)\lambda \ln \lambda} \ln \delta \tag{62}$$

according to Eq. (19). The minimum of the right-hand side is attained when $\lambda$ is the unique solution, denoted by $\lambda_*$, of the following equation:

$$1 + (d-1)\lambda + \ln \lambda = 0. \tag{63}$$

It is not easy to derive an analytical formula for $\lambda_*$, but it is easy to compute $\lambda_*$ numerically. In addition, it is easy to prove that $\lambda_* \geqslant 1/(d+1)$ when $d \geqslant 4$, so the optimal strategy can be realized by LOCC. When $d = 2, 3$, the optimal value of $\lambda$ under LOCC is $1/(d+1)$. When $d \geqslant 3$ and $\lambda = 1/(d-1)$, we have

$$N(\epsilon, \delta, \lambda) \approx \frac{2\ln \delta^{-1}}{\ln(d-1)}, \tag{64}$$

so the choice $\lambda = 1/(d-1)$ is reasonably good for practical purposes. It should be pointed out that the above equation is derived under the assumption $\delta \ll \lambda = 1/(d-1)$.

In the rest of this section we show that for any given significance level $0 < \delta < 1$, the entanglement of the maximally entangled state $|\Phi\rangle$ can be certified using only one test as long as the local dimension $d$ is large enough. To verify this claim, we may assume that $0 < \delta \leqslant 1/2$ without loss of generality because the number of tests cannot increase when $\delta$ increases.

*Theorem 3.* In the adversarial scenario, the entanglement of the $d \times d$ maximally entangled state $|\Phi\rangle$ can be certified with significance level $0 < \delta \leqslant 1/2$ using only one test based on a homogeneous strategy $\Omega$ iff

$$d \geqslant d_* := \left\lceil \frac{2 + 2\sqrt{1-\delta} - \delta}{\delta} \right\rceil, \tag{65}$$

$$\lambda_- \leqslant \beta(\Omega) \leqslant \lambda_+, \tag{66}$$

where

$$\lambda_\pm = \frac{(d+1)\delta \pm \sqrt{(d+1)^2\delta^2 - 4d\delta}}{2d}. \tag{67}$$

*Proof.* Let $\lambda = \beta(\Omega)$. If the entanglement of $|\Phi\rangle$ can be certified with significance level $0 < \delta \leqslant 1/2$ using only one test, then $\lambda > 0$ by Eq. (60); see also the conclusion presented after Eq. (8). In addition, Eq. (15) with $\epsilon = (d-1)/d$ has to hold, which means $\lambda < \delta$ and

$$d \geqslant \frac{\delta(1-\lambda)}{\lambda(\delta - \lambda)}. \tag{68}$$

The minimum value of the right-hand side is attained when $\lambda = 1 - \sqrt{1-\delta}$, in which case the above equation reduces to

$$d \geqslant \frac{2 + 2\sqrt{1-\delta} - \delta}{\delta}, \tag{69}$$

which implies Eq. (65). In addition, Eq. (68) implies that

$$d\lambda^2 - (d+1)\delta\lambda + \delta \leqslant 0, \tag{70}$$

from which we can deduce that $\lambda_- \leqslant \lambda = \beta(\Omega) \leqslant \lambda_+$, which confirms Eq. (66).

Conversely, if $d \geqslant d_*$ and $\lambda_- \leqslant \lambda = \beta(\Omega) \leqslant \lambda_+$, then Eqs. (15) and (68) hold. Therefore, the homogeneous strategy $\Omega$ can be applied to certify the entanglement of $|\Phi\rangle$ with only one test. ■

Note that the bound in Eq. (65) is equivalent to the condition $\delta \geqslant 4d/(d+1)^2$. When this condition is satisfied, then $\lambda_+$ ($\lambda_-$) is monotonically increasing (decreasing) in $d$ and $\delta$. In conjunction with the assumption $0 < \delta \leqslant 1/2$, we can deduce that

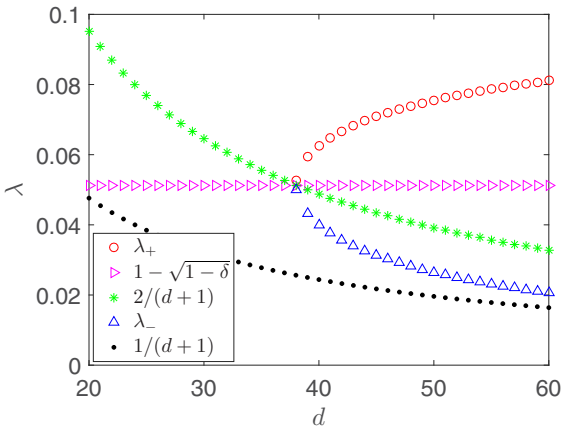


FIG. 3. Entanglement certification of maximally entangled states in the adversarial scenario using only one test. Here the significance level is set at $\delta = 0.1$. When the local dimension satisfies $d \geqslant 38$, the entanglement can be certified by any homogeneous strategy $\Omega$ with $\lambda_- \leqslant \beta(\Omega) \leqslant \lambda_+$ [cf. Eqs. (66) and (67)], including the specific choice $\beta(\Omega) = 2/(d+1)$ or $\beta(\Omega) = 1 - \sqrt{1-\delta}$. The plot also shows that $\lambda_- \geqslant 1/(d+1)$, which means all such strategies can be realized by virtue of local projective measurements.

$$\frac{1}{d+1} < \frac{1}{d} < \frac{d+1-\sqrt{d^2-6d+1}}{4d} \leqslant \lambda_- \leqslant \lambda_+ \leqslant \frac{d+1+\sqrt{d^2-6d+1}}{4d} < \frac{d-1}{2d}, \tag{71}$$

$$\frac{\delta}{d} < \lambda_- \leqslant \lambda_+ < \delta. \tag{72}$$

In addition, we have

$$\lambda_- \leqslant \frac{2}{d+1} \leqslant 1 - \sqrt{1-\delta} \leqslant \lambda_+, \tag{73}$$

where the middle inequality is saturated when the inequality $\delta \geqslant 4d/(d+1)^2$ is saturated, in which case all the inequalities in Eq. (73) are saturated (cf. Fig. 3).

If Eq. (65) is not satisfied, then the entanglement of $|\Phi\rangle$ cannot be certified with only one test even if entangling measurements are accessible given that the optimal performance can always be achieved by a homogeneous strategy. Conversely, if Eq. (65) is satisfied, then the entanglement of $|\Phi\rangle$ can be certified with only one test by a homogeneous strategy constructed from local projective measurements. Actually, all homogeneous strategies that can certify the entanglement with one test can be realized by local measurements thanks to Eq. (71). Notably, the homogeneous strategy $\Omega$ with $\beta(\Omega) = 1 - \sqrt{1-\delta}$ or with $\beta(\Omega) = 2/(d+1)$ can achieve the optimal performance and can be realized by local measurements in view of Eq. (73). For example, the entanglement of $|\Phi\rangle$ can be certified with significance level $\delta = 0.1$ using one test iff $d \geqslant 38$, as illustrated in Figs. 2 and 3. When $\delta \ll 1$, we have $d_* \approx (4/\delta) - 2$, so the threshold dimension is about two times the counterpart $(2/\delta) - 1$ for the nonadversarial scenario [cf. Eq. (53)].

## VI. SUMMARY

We studied systematically efficient verification of maximally entangled states based on local projective measurements. We proved that optimal strategies are in one-to-one correspondence with weighted complex projective 2-designs, while perfect strategies are in one-to-one correspondence with complete sets of MUBs. Based on this observation, optimal protocols are constructed for maximally entangled states of any local dimension, and near-optimal protocols are constructed using only three measurement settings. Besides state verification, these protocols are also very useful for fidelity estimation and entanglement detection. Moreover, our approach can be applied to the adversarial scenario. In this case, we can construct protocols based on local projective measurements that are optimal even among protocols that allow entangling measurements. In addition, we proved that the entanglement of the maximally entangled state can be certified with any given significance level using only one test when the local dimension is large enough. Our work is of interest not only to practical quantum information processing, but also to foundational studies on the connections between quantum states and quantum measurements.

## ACKNOWLEDGMENTS

H.Z. is grateful to Zihao Li and Yun-Guang Han for comments. This work is supported by the National Natural Science Foundation of China (Grant No. 11875110). M.H. was supported in part by the Fund for the Promotion of Joint International Research (Fostering Joint International Research) Grant No. 15KK0007, Japan Society for the Promotion of Science (JSPS) Grants-in-Aid for Scientific Research (A) No. 17H01280 and (B) No. 16KT0017, and the Kayamori Foundation of Informational Science Advancement.

## APPENDIX: PROOFS OF THEOREMS 1 AND 2

*Proof of Theorem 1.* The "if" part of the theorem follows from Proposition 2. Conversely, if the LP strategy $\{P_l, p_l\}_{j=1}^{g}$ is parsimonious, then $p_l = 1/g$ and $\bar{P}_l$ are mutually orthogonal according to Lemma 3. In view of Lemma 5 below, there must exist $g$ bases $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_g$ that are mutually unbiased and such that $P_l = P(\mathcal{B}_l)$. Therefore, the LP strategy is actually a CB strategy, which is perfect iff the bases form a complete set of MUBs. ∎

*Proof of Theorem 2.* The "if" part follows from Propositions 3 and 2. Conversely, if the SP strategy $\{P_l, p_l\}_{j=1}^{g}$ is optimal, then $\sum_l p_l \operatorname{tr}(P_l) = d$, which implies that all $P_l$ have rank $d$ by Lemma 4 below. So each $P_l$ has the form $P_l = P(\mathcal{B}_l)$ for some basis $\mathcal{B}_l$ by Lemma 7 below, and the SP strategy is actually a CB strategy. Now the theorem follows from Propositions 3 and 2. ∎

*Lemma 4.* Any separable projector $P \geqslant |\Phi\rangle\langle\Phi|$ has rank at least $d$.

*Proof.* $\operatorname{rank}(P) \geqslant \operatorname{rank}(\operatorname{tr}_{\mathrm{B}} P) \geqslant \operatorname{rank}(\operatorname{tr}_{\mathrm{B}} |\Phi\rangle\langle\Phi|) = d$. Alternatively, this conclusion follows from the observation that $\operatorname{tr}(P) \geqslant E_{\mathcal{R}}(\Phi) + 1 = d$. ∎

*Lemma 5.* Suppose $P_1, P_2 \geqslant |\Phi\rangle\langle\Phi|$ are two LP projectors. Then $\bar{P}_1$ and $\bar{P}_2$ are orthogonal iff $P_1 = P(\mathcal{B}_1)$ and $P_2 = P(\mathcal{B}_2)$, where $\mathcal{B}_1$ and $\mathcal{B}_2$ are two bases for $\mathcal{H}$ that are mutually unbiased.

*Proof.* The "if" part follows from Proposition 1. Concerning the converse, suppose $P_l$ is diagonal in the product basis $\mathcal{B}_l \times \mathcal{B}_l'$ for $l = 1, 2$. Then $P_l \geqslant P(\mathcal{B}_l)$ by Lemma 6 below, so $\bar{P}_l \geqslant \bar{P}(\mathcal{B}_l)$. If $\bar{P}_1$ and $\bar{P}_2$ are orthogonal, then $\bar{P}(\mathcal{B}_1)$ and $\bar{P}(\mathcal{B}_2)$ are orthogonal, so $\mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased by Proposition 1. In addition,

$$1 = \operatorname{tr}(P_1 P_2) \geqslant \operatorname{tr}[P_1 P(\mathcal{B}_2)] = \operatorname{rank}(P_1)/d, \tag{A1}$$

which implies that $P_1$ has rank $d$ in view of Lemma 4, so that $P_1 = P(\mathcal{B}_1)$. By the same token, $P_2 = P(\mathcal{B}_2)$. ∎

*Lemma 6.* Suppose $P \geqslant |\Phi\rangle\langle\Phi|$ is an LP projector that is diagonal in the product basis $\mathcal{B} \times \mathcal{B}'$; then $P \geqslant P(\mathcal{B})$.

*Proof.* Suppose $\mathcal{B} = \{|\psi_j\rangle\}_{j=1}^{d}$ and $\mathcal{B}' = \{|\phi_j\rangle\}_{j=1}^{d}$; then $P$ has the form

$$P = \sum_j \sum_{k \in A_j} |\psi_j\rangle\langle\psi_j| \otimes |\phi_k\rangle\langle\phi_k|, \tag{A2}$$

where $A_j$ are subsets of $\{1, 2, \ldots, d\}$. In addition,

$$\begin{aligned} 1 = \langle\Phi|P|\Phi\rangle &= \sum_j \sum_{k \in A_j} |\langle\psi_j, \phi_k|\Phi\rangle|^2 \\ &= \frac{1}{d} \sum_j \sum_{k \in A_j} |\langle\phi_k|\psi_j^*\rangle|^2 \leqslant 1. \end{aligned} \tag{A3}$$

Here the upper bound is saturated iff each $|\psi_j^*\rangle$ is supported in the span of $\{|\phi_k\rangle\}_{k \in A_j}$. It follows that $|\psi_j^*\rangle\langle\psi_j^*| \leqslant \sum_{k \in A_j} |\phi_k\rangle\langle\phi_k|$, so that

$$\begin{aligned} P(\mathcal{B}) &= \sum_j |\psi_j\rangle\langle\psi_j| \otimes |\psi_j^*\rangle\langle\psi_j^*| \\ &\leqslant \sum_j \sum_{k \in A_j} |\psi_j\rangle\langle\psi_j| \otimes |\phi_k\rangle\langle\phi_k| = P, \end{aligned} \tag{A4}$$

which completes the proof. ∎

*Lemma 7.* Any rank-$d$ separable projector $P$ on $\mathcal{H}^{\otimes 2}$ that satisfies $P \geqslant |\Phi\rangle\langle\Phi|$ has the form $P = P(\mathcal{B})$, where $\mathcal{B}$ is an orthonormal basis for $\mathcal{H}$.

*Remark 2.* The support of $P(\mathcal{B})$ contains exactly $d$ product states, namely, $|\psi\rangle\langle\psi| \otimes |\psi^*\rangle\langle\psi^*|$ for $|\psi\rangle \in \mathcal{B}$. So the basis $\mathcal{B}$ in Lemma 7 is uniquely determined by $P$, assuming that two bases $\mathcal{B}, \mathcal{B}'$ for $\mathcal{H}$ are deemed identical if they differ only by the ordering or overall phase factors of kets [note that such bases yield the same test projector, that is, $P(\mathcal{B}') = P(\mathcal{B})$]. Then the mapping from bases for $\mathcal{H}$ to projectors on $\mathcal{H}^{\otimes 2}$ as defined by $P(\mathcal{B})$ in Eq. (43) is injective.

*Proof of Lemma 7.* By assumption $P$ is a linear combination of pure product states with positive coefficients,

$$P = \sum_j c_j |\varphi_j\rangle\langle\varphi_j| \otimes |\phi_j\rangle\langle\phi_j|, \tag{A5}$$

where $|\varphi_j\rangle$ and $|\phi_j\rangle$ are normalized kets, $c_j > 0$, and $\sum_j c_j = \operatorname{tr}(P) = d$. We have

$$1 = \langle\Phi|P|\Phi\rangle = \frac{1}{d} \sum_j c_j |\langle\phi_j^*|\varphi_j\rangle|^2 \leqslant \frac{1}{d} \sum_j c_j = 1, \tag{A6}$$

which implies that $|\phi_j\rangle = |\varphi_j^*\rangle$ for all $j$. So there exist $d$ kets, say, $|\varphi_1\rangle, \ldots, |\varphi_d\rangle$, such that $|\varphi_j\rangle \otimes |\varphi_j^*\rangle$ for $j = 1, 2, \ldots, d$ span the support of $P$. In addition, $|\Phi\rangle$ has the form $|\Phi\rangle = \sum_{j=1}^{d} a_j |\varphi_j\rangle \otimes |\varphi_j^*\rangle$. This equality can hold iff $\mathcal{B} := \{|\varphi_j\rangle\}_{j=1}^{d}$ is an orthonormal basis for $\mathcal{H}$ and $a_j = 1/\sqrt{d}$ for $j = 1, 2, \ldots, d$. Now $\{|\varphi_j\rangle \otimes |\varphi_j^*\rangle\}_{j=1}^{d}$ is an orthonormal basis in the support of $P$, so $P = P(\mathcal{B})$. ■


[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. 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).

[4] M. Hayashi, B.-S. Shi, A. Tomita, K. Matsumoto, Y. Tsuda, and Y.-K. Jiang, Hypothesis testing for an entangled state produced by spontaneous parametric down-conversion, Phys. Rev. A **74**, 062321 (2006).

[5] M. Hayashi, Group theoretical study of LOCC-detection of maximally entangled states using hypothesis testing, New J. Phys. **11**, 043028 (2009).

[6] M. Hayashi, Discrete realization of group symmetric LOCC-detection of maximally entangled state, arXiv:0810.3381.

[7] M. Hayashi and M. Owari, Tight asymptotic bounds on local hypothesis testing between a pure bipartite state and the white noise state, IEEE Trans. Inf. Theory **63**, 4008 (2017).

[8] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements, Phys. Rev. Lett. **120**, 170502 (2018).

[9] C. A. Fuchs, M. C. Hoang, and B. C. Stacey, The SIC question: History and state of play, Axioms **6**, 21 (2017).

[10] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, On mutually unbiased bases, Int. J. Quantum Inf. **08**, 535 (2010).

[11] I. D. Ivanović, Geometrical description of quantal state determination, J. Phys. A: Math. Gen. **14**, 3241 (1981).

[12] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, Ann. Phys. **191**, 363 (1989).

[13] A. Dimić and B. Dakić, Single-copy entanglement detection, npj Quantum Inf. **4**, 11 (2018).

[14] V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, and B. Dakić, Experimental few-copy multi-particle entanglement detection, arXiv:1809.05455.

[15] H. Zhu and M. Hayashi, Efficient verification of pure quantum states with applications to hypergraph states, arXiv:1806.05565.

[16] G. Vidal and R. Tarrach, Robustness of entanglement, Phys. Rev. A **59**, 141 (1999).

[17] A. W. Harrow and M. A. Nielsen, Robustness of quantum gates in the presence of noise, Phys. Rev. A **68**, 012308 (2003).

[18] M. Steiner, Generalized robustness of entanglement, Phys. Rev. A **67**, 054305 (2003).

[19] F. G. S. L. Brandão, Quantifying entanglement with witness operators, Phys. Rev. A **72**, 022310 (2005).

[20] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani, Bounds on Multipartite Entangled Orthogonal State Discrimination using Local Operations and Classical Communication, Phys. Rev. Lett. **96**, 040501 (2006).

[21] M. Owari and M. Hayashi, Two-way classical communication remarkably improves local distinguishability, New J. Phys. **10**, 013006 (2008).

[22] M. Hayashi and T. Morimae, Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing, Phys. Rev. Lett. **115**, 220502 (2015).

[23] G. Zauner, Quantum designs: Foundations of a noncommutative design theory, Int. J. Quantum Inf. **09**, 445 (2011).

[24] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, J. Math. Phys. **45**, 2171 (2004).

[25] A. J. Scott, Tight informationally complete quantum measurements, J. Phys. A: Math. Gen. **39**, 13507 (2006).

[26] A. Roy and A. J. Scott, Weighted complex projective 2-designs from bases: Optimal state determination by orthogonal measurements, J. Math. Phys. **48**, 072110 (2007).

[27] A. Klappenecker and M. Rötteler, Mutually unbiased bases are complex projective 2-designs, in *IEEE International Symposium on Information Theory (ISIT): Adelaide, Australia, 4-9 September, 2005* (IEEE, Piscataway, NJ, 2005), pp. 1740–1744.

[28] H. Zhu, Mutually unbiased bases as minimal Clifford covariant 2-designs, Phys. Rev. A **91**, 060301(R) (2015).