Efficient certification of high-dimensional entanglement

Yiwen Wu,[1, 2, 3] Zihao Li,[1, 2, 3] and Huangjun Zhu[1, 2, 3, *]

[1]State Key Laboratory of Surface Physics, Department of Physics,
and Center for Field Theory and Particle Physics, Fudan University, Shanghai 200433, China
[2]Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China
[3]Shanghai Research Center for Quantum Sciences, Shanghai 201315, China

(Dated: August 8, 2025)

High-dimensional entanglement (HDE) is a valuable resource in quantum information processing, and efficient certification of HDE is crucial to many applications. In this work, we propose a simple and general framework for certifying HDE in general bipartite pure states under restricted operations, such as local operations and classical communication (LOCC). On this basis we show that HDE in general bipartite pure states can be certified efficiently. Moreover, the sample cost for certifying a given degree of HDE even decreases monotonically with the local dimensions. In addition, for a general two-qubit pure state, we construct an optimal entanglement certification strategy based on separable operations, which can be realized by LOCC when the target state has sufficiently high entanglement. The core concept of our framework is versatile and can be extended to certify a wide range of critical resources under restricted operations.

I. INTRODUCTION

Quantum entanglement is a characteristic of quantum mechanics and a valuable resource in many tasks in quantum information processing [1]. *High-dimensional entanglement* (HDE) [2, 3], which involves quantum systems with higher local dimensions compared with qubits, may further offer enhanced information capacity and improved noise resilience and has thus attracted increasing attention recently. It is especially valuable for important tasks such as quantum cryptography [4, 5], quantum communication [6–8], and quantum computation [9–11]. Moreover, HDE is tied to the classical hardness in simulating quantum systems and may even serve as a benchmark for quantum technologies [12–14]. Therefore, efficient certification of HDE is of intrinsic interest to both theoretical studies and practical applications [15, 16]. However, traditional tomographic approaches are too resource-intensive for this task for large and intermediate quantum systems.

To address the challenge in HDE certification, a number of alternative approaches have emerged recently, including fidelity-based Schmidt number witnesses [17–22], correlation-based approaches [23–28], entropic steering criteria [29, 30], and methods based on positive maps (such as the reduction map) [31–33] and hypothesis testing [34]. In addition, several verification protocols have been demonstrated in experiments across various platforms, including photonic systems [17–20, 23, 25, 28, 34] and cold atoms [21, 30]. Despite this progress, little is known about the sample complexity of certifying HDE and the construction of optimal or nearly optimal certification protocols.

In this work, inspired by the idea of *quantum state verification* (QSV) [35–40], we propose a simple and general framework for certifying HDE under restricted operations, such as *local operations and classical communication* (LOCC) and separable operations. To rigorously quantify the capabilities of these operations in certifying HDE, we introduce the concept of separation probabilities. Then, we determine the separation probabilities of maximally entangled states and derive nearly tight upper and lower bounds for general bipartite pure states. Based on these findings, we show that HDE in general bipartite pure states can be certified efficiently using LOCC. Notably, the sample cost for certifying a given degree of HDE even decreases monotonically with the local dimensions. The same conclusion still holds even if the strategy is required to be homogeneous [37, 38]. In addition, we construct an optimal entanglement certification strategy for any two-qubit pure state using separable operations, and show that this optimal strategy can be realized by LOCC when the target state has sufficiently high entanglement. This study also shows that optimal strategies for entanglement certification are in general different from the counterparts for QSV. The versatility of our framework extends beyond HDE certification. The basic idea may find applications in certifying many other important resources, such as coherence and nonstabilizerness, under restricted operations.

The rest of this paper is organized as follows. In Sec. II we introduce necessary preliminaries on HDE and QSV. In Sec. III we propose a simple and general framework for certifying entanglement under restricted operations and introduce the concept of separation probabilities. In Sec. IV we show that HDE in general bipartite pure states can be certified efficiently after clarifying the properties of separation probabilities. In Sec. V we construct an optimal entanglement certification strategy for a general two-qubit pure state based on separable operations and show that this strategy can be realized by LOCC when the target state has a high concurrence. Section VI summarizes this paper.

[*] zhuhuangjun@fudan.edu.cn

II. PRELIMINARIES

Let $\mathcal{H}$ be the Hilbert space of a quantum system under consideration and denote by $\mathcal{D}(\mathcal{H})$ the set of all quantum states on $\mathcal{H}$. Given any pure state $|\Psi\rangle$ in $\mathcal{H}$ we use $\Psi = |\Psi\rangle\langle\Psi|$ to denote the corresponding density operator. Given a closed subset $\mathcal{S}$ in $\mathcal{D}(\mathcal{H})$, denote by $F(\Psi, \mathcal{S})$ the maximum fidelity between $|\Psi\rangle$ and states in $\mathcal{S}$, that is,

$$F(\Psi, \mathcal{S}) = \max_{\sigma\in\mathcal{S}} \langle\Psi|\sigma|\Psi\rangle. \tag{1}$$

Denote by $\tilde{\mathcal{S}}$ the subset of pure states in $\mathcal{S}$, that is,

$$\tilde{\mathcal{S}} := \{\sigma \in \mathcal{S} \mid \mathrm{tr}(\sigma^2) = 1\}, \tag{2}$$

which is also a closed subset in $\mathcal{D}(\mathcal{H})$. Given a positive integer k, let $[k]$ be a shorthand for $\{1, 2, \ldots, k\}$.

A. Schmidt number and high-dimensional entanglement

Here we assume that $\mathcal{H} = \mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ is the Hilbert space of a bipartite quantum system shared by Alice and Bob; let $d_A = \dim(\mathcal{H}_A)$, $d_B = \dim(\mathcal{H}_B)$, $D = \dim(\mathcal{H}_{AB}) = d_A d_B$, and $d = \min\{d_A, d_B\}$. To simplify the following discussion, in this paper we shall assume that $d = d_A \le d_B$ without loss of generality. In addition, denote by $\mathrm{U}(\mathcal{H})$ the group of unitary operators on $\mathcal{H}$ and by $\mathrm{U}(d)$ the group of unitary operators on a d-dimensional Hilbert space.

A bipartite pure state $|\Psi\rangle \in \mathcal{H}_{AB}$ is a product state if it can be expressed in the form $|\Psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ with $|\psi_A\rangle \in \mathcal{H}_A$ and $|\psi_B\rangle \in \mathcal{H}_B$. Otherwise, $|\Psi\rangle$ is entangled. The state $|\Psi\rangle$ is maximally entangled if the reduced state $\rho_A = \mathrm{tr}_B(|\Psi\rangle\langle\Psi|)$ is a completely mixed state, in which case any other state in $\mathcal{D}(\mathcal{H}_{AB})$ can be generated from $|\Psi\rangle$ under LOCC (see Sec. II B). For example, here is a typical maximally entangled state:

$$|\Phi\rangle = \sum_{j=0}^{d-1} \frac{1}{\sqrt{d}} |jj\rangle. \tag{3}$$

A mixed state on $\mathcal{H}_{AB}$ is separable if it is a convex combination of pure product states and entangled otherwise [41]. A mixed state is maximally entangled if every pure state in its support is maximally entangled. The structures of such states were clarified in Refs. [42, 43]. The set of separable states on $\mathcal{H}_{AB}$ is denoted by $\mathcal{S}_{\mathrm{sep}}(\mathcal{H}_{AB})$ henceforth, which can be abbreviated as $\mathcal{S}_{\mathrm{sep}}$ if there is no danger of confusion.

Any bipartite pure state $|\Psi\rangle$ in $\mathcal{H}_{AB}$ has a *Schmidt decomposition* [44] of the form

$$|\Psi\rangle = \sum_{j=0}^{d-1} \sqrt{s_j} |\psi_j^A\rangle \otimes |\psi_j^B\rangle, \tag{4}$$

where $\{|\psi_j^A\rangle\}_{j=0}^{d-1}$ forms an orthonormal basis of $\mathcal{H}_A$, $\{|\psi_j^B\rangle\}_{j=0}^{d-1}$ is a set of orthonormal states in $\mathcal{H}_B$, and $\{s_j\}_{j=0}^{d-1}$ is the set of *Schmidt coefficients*, also known as *Schmidt spectrum*, which satisfies $\sum_{j=0}^{d-1} s_j = 1$. Without loss of generality, we assume that $s_0 \ge s_1 \ge \cdots \ge s_{d-1} \ge 0$ throughout this paper. Although the above decomposition is not necessarily unique, the set of Schmidt coefficients is uniquely determined by $|\Psi\rangle$. For example, all the Schmidt coefficients are equal to $1/d$ whenever $|\Psi\rangle$ is maximally entangled, and vice versa. The Schmidt vector of $|\Psi\rangle$ is defined as $\mathbf{s}_\Psi := (s_0, s_1, \ldots, s_{d-1})$. The *Schmidt rank* of $|\Psi\rangle$ is defined as the number of nonzero Schmidt coefficients and is denoted by $\mathrm{SR}(\Psi)$ henceforth; it is equal to the rank of $\rho_A = \mathrm{tr}_B(|\Psi\rangle\langle\Psi|)$ and also the rank of $\rho_B = \mathrm{tr}_A(|\Psi\rangle\langle\Psi|)$.

Given $r \in [d]$, let $\mathcal{S}_r$ be the subset of quantum states in $\mathcal{D}(\mathcal{H}_{AB})$ that can be expressed as convex combinations of pure states with Schmidt rank at most r. Note that $\mathcal{S}_r$ is a proper subset of $\mathcal{S}_{r+1}$ for $r \in [d-1]$, and $\mathcal{S}_1$ coincides with the set $\mathcal{S}_{\mathrm{sep}}$ of separable states. The *Schmidt number* of $\sigma \in \mathcal{D}(\mathcal{H}_{AB})$ is defined as the smallest integer r such that $\mathcal{S}_r$ contains σ and is denoted by $\mathrm{SN}(\sigma)$. By definition, the Schmidt number of a pure state is equal to its Schmidt rank.

As the simplest measure for quantifying HDE, the Schmidt number is discrete and not so robust to perturbation or noise. To remedy this problem, a family of continuous entanglement measures were introduced by Vidal [45]. Suppose $|\Psi\rangle$ has Schmidt spectrum $\{s_j\}_{j=0}^{d-1}$. Define $\mathcal{E}_r(\Psi)$ as the sum of the $d-r$ smallest Schmidt coefficients, that is,

$$\mathcal{E}_r(\Psi) := \sum_{j=r}^{d-1} s_j, \quad r \in [d-1]. \tag{5}$$

Note that $\mathcal{E}_r(\Psi)$ only depends on the nonzero Schmidt coefficients of $|\Psi\rangle$ and is independent of the local dimensions (once the set of nonzero Schmidt coefficients is fixed). The above definition can be extended to mixed states via the convex-roof construction. An ensemble of pure states $\{|\Psi_l\rangle, p_l\}_l$ is a convex decomposition of $\sigma \in \mathcal{D}(\mathcal{H}_{AB})$ if $\sum_l p_l |\Psi_l\rangle\langle\Psi_l| = \sigma$. Denote by $\mathbb{D}(\sigma)$ the set of all convex decompositions of σ into pure states. Then $\mathcal{E}_r(\sigma)$ can be defined as follows:

$$\mathcal{E}_r(\sigma) := \inf_{\{|\Psi_l\rangle, p_l\}_l \in \mathbb{D}(\sigma)} \sum_l p_l \mathcal{E}_r(\Psi_l), \tag{6}$$

where the infimum is taken over all convex decompositions of σ. Based on this definition we can introduce a subset of quantum states with limited HDE:

$$\mathcal{S}_{\mathcal{E}_r}(E) := \{\sigma \in \mathcal{D}(\mathcal{H}_{AB}) \mid \mathcal{E}_r(\sigma) \le E\}, \tag{7}$$

which will be useful for formulating robust HDE certification. Note that $\mathcal{S}_{\mathcal{E}_r}(0)$ coincides with $\mathcal{S}_r$.

Next, we clarify the basic properties of the entanglement measure $\mathcal{E}_r$ that are relevant to the current study.

Propositions 1-4 below are proved in Appendix A, although Proposition 2 is known before [2, 46].

Proposition 1. *Suppose $r \in [d-1]$; then*

$$0 \le \mathcal{E}_r(\sigma) \le \frac{d-r}{d} \quad \forall\, \sigma \in \mathcal{D}(\mathcal{H}_{AB}), \tag{8}$$

where the lower bound is saturated iff $\mathrm{SN}(\sigma) \le r$, and the upper bound is saturated iff σ is maximally entangled.

Note that Proposition 1 is compatible with the fact that $\mathcal{S}_{\mathcal{E}_r}(0) = \mathcal{S}_r$. Next, we clarify the maximum fidelity between two bipartite pure states with given Schmidt spectra.

Proposition 2. *Suppose $|\Psi\rangle$ and $|\Upsilon\rangle$ are two pure states in $\mathcal{H}_{AB}$ that have Schmidt spectra $\{s_j\}_{j=0}^{d-1}$ and $\{t_j\}_{j=0}^{d-1}$, respectively. Then*

$$|\langle\Psi|\Upsilon\rangle| \le \sum_{j=0}^{d-1} \sqrt{s_j t_j}, \tag{9}$$

and the inequality is saturated if $|\Psi\rangle = \sum_{j=0}^{d-1} \sqrt{s_j}|jj\rangle$ and $|\Upsilon\rangle = \sum_{j=0}^{d-1} \sqrt{t_j}|jj\rangle$.

As a simple corollary of Proposition 2 we can deduce that

$$|\langle\Psi|\Phi\rangle| \le \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \sqrt{s_j}, \tag{10}$$

and the inequality is saturated if $|\Psi\rangle = \sum_{j=0}^{d-1} \sqrt{s_j}|jj\rangle$. By virtue of Proposition 2 we can derive the following proposition.

Proposition 3. *Suppose $|\Psi\rangle \in \mathcal{H}_{AB}$ has Schmidt spectrum $\{s_j\}_{j=0}^{d-1}$, $r \in [d-1]$, and $E' = \mathcal{E}_r(\Psi)$. Then*

$$F(\Psi, \mathcal{S}_r) = F\big(\Psi, \tilde{\mathcal{S}}_r\big) = 1 - \mathcal{E}_r(\Psi), \tag{11}$$

$$\begin{aligned} &F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) = F\big(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E)\big) \\ &= \begin{cases} \Big[\sqrt{E'E} + \sqrt{(1-E')(1-E)}\Big]^2 & 0 \le E < E', \\ 1 & E \ge E'. \end{cases} \end{aligned} \tag{12}$$

In addition, $F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E))$ and $F(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E))$ are nondecreasing and concave in E.

Note that the maximum fidelities $F(\Psi, \mathcal{S}_r) = F(\Psi, \tilde{\mathcal{S}}_r)$ and $F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) = F(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E))$ are independent of the local dimensions once the set of nonzero Schmidt coefficients of $|\Psi\rangle$ is fixed. Proposition 3 endows $\mathcal{E}_r(\Psi)$ with a simple operational interpretation, which will be discussed further in Sec. II B. In addition, $F(\Psi, \mathcal{S}_1) = F(\Psi, \mathcal{S}_{\mathrm{sep}}) = s_0$ coincides with the largest Schmidt coefficient of $|\Psi\rangle$ and is closely tied to the geometric measure of entanglement [47].

Proposition 4. *Suppose $|\Psi\rangle, |\Upsilon\rangle \in \mathcal{H}_{AB}$ and $r \in [d-1]$. Then*

$$\begin{aligned} |\mathcal{E}_r(\Psi) - \mathcal{E}_r(\Upsilon)| &\le \ell(r,d)\sqrt{2 - 2|\langle\Psi|\Upsilon\rangle|} \\ &\le \ell(r,d)\||\Psi\rangle - |\Upsilon\rangle\|_2, \end{aligned} \tag{13}$$

where

$$\ell(r,d) := \begin{cases} 1 & r \le d/2, \\ \frac{2\sqrt{r(d-r)}}{d} & r > d/2. \end{cases} \tag{14}$$

Proposition 4 shows that $\mathcal{E}_r(\Psi)$ is a Lipschitz function with Lipschitz constant $\ell(r,d) \le 1$.

B. Transformations of bipartite pure states under LOCC

To understand the transformations of bipartite pure states under LOCC, we first need to introduce the concept of *majorization* [48]. Suppose $\mathbf{x} = (x_0, x_1, \ldots, x_{d-1})$ and $\mathbf{y} = (y_0, y_1, \ldots, y_{d-1})$ are two d-dimensional real vectors. Let $\mathbf{x}^{\downarrow}$ be the vector obtained by arranging the components of $\mathbf{x}$ in nonincreasing order, which means $x_0^{\downarrow} \ge x_1^{\downarrow} \ge \cdots \ge x_{d-1}^{\downarrow}$; define $\mathbf{y}^{\downarrow}$ in a similar way. Then $\mathbf{x}$ is *majorized* by $\mathbf{y}$, denoted by $\mathbf{x} \prec \mathbf{y}$, if

$$\sum_{j=0}^{k} x_j^{\downarrow} \le \sum_{j=0}^{k} y_j^{\downarrow}, \quad k = 0, 1, \ldots, d-1, \tag{15}$$

and the inequality is saturated when $k = d-1$. A function f defined on a subset of $\mathbb{R}^d$ is *Schur convex* (*concave*) if $f(\mathbf{x}) \le f(\mathbf{y})$ $[f(\mathbf{x}) \ge f(\mathbf{y})]$ whenever $\mathbf{x} \prec \mathbf{y}$.

As a generalization, given two pure states $|\Psi\rangle$ and $|\Upsilon\rangle$ in $\mathcal{H}_{AB}$, $|\Psi\rangle$ is *majorized* by $|\Upsilon\rangle$ if the Schmidt vector of $|\Psi\rangle$ is majorized by the Schmidt vector of $|\Upsilon\rangle$, that is, $\mathbf{s}_\Psi \prec \mathbf{s}_\Upsilon$. A function f defined on pure states in $\mathcal{H}_{AB}$ is *Schur convex* (*concave*) if it is invariant under local unitary transformations and is Schur convex (concave) when regarded as a function of the Schmidt vector. For example, each entanglement measure $\mathcal{E}_r$ defined in Eq. (5) is Schur concave.

Now, we can formulate the majorization criterion on the transformations of bipartite pure states under LOCC originally established by Nielsen [49].

Proposition 5. *Suppose $|\Psi\rangle$ and $|\Upsilon\rangle$ are two pure states in $\mathcal{H}_{AB}$. Then $|\Psi\rangle$ can be transformed into $|\Upsilon\rangle$ under LOCC iff $|\Psi\rangle$ is majorized by $|\Upsilon\rangle$.*

Proposition 5 in particular implies that the Schmidt number and the entanglement measure $\mathcal{E}_r$ cannot increase under LOCC. If the majorization condition does not hold, then $|\Psi\rangle$ can be transformed into $|\Upsilon\rangle$ only probabilistically under LOCC. The maximum success probability $p(\Psi \to \Upsilon)$ is determined by Vidal [45]:

$$p(\Psi \to \Upsilon) = \min_r \frac{\mathcal{E}_r(\Psi)}{\mathcal{E}_r(\Upsilon)}. \tag{16}$$

This result highlights the importance of the family of entanglement measures $\mathcal{E}_r$ in understanding bipartite entanglement transformations under LOCC.

C. Quantum state verification

Before introducing the framework of HDE certification, we briefly review the general framework of QSV [36–38]. A device is supposed to produce the target quantum state $|\Psi\rangle \in \mathcal{H}$, but actually produces N states $\sigma_1, \sigma_2, \ldots, \sigma_N$ in N runs. We assume that either $\sigma_j = |\Psi\rangle\langle\Psi|$ for all j or $\langle\Psi|\sigma_j|\Psi\rangle \leq 1-\varepsilon$ for all j. Now our task is to distinguish the two cases with a given significance level δ. To this end, for each σ_j we can perform a binary measurement $\{\Pi_l, \mathbb{1} - \Pi_l\}$ chosen randomly with probability p_l from a given set of measurements. Here the first outcome Π_l corresponds to passing the test, while the second outcome corresponds to failing the test. To guarantee that the target state can always pass the test, the test operator Π_l should satisfy the condition $\Pi_l|\Psi\rangle = |\Psi\rangle$.

The performance of the above verification strategy is characterized by the verification operator $\Omega = \sum_l p_l \Pi_l$. When $\langle\Psi|\sigma|\Psi\rangle \leq 1-\varepsilon$, the maximum probability that σ can pass one test on average reads [36–38]

$$\max_{\langle\Psi|\sigma|\Psi\rangle\leq 1-\varepsilon} \operatorname{tr}(\Omega\sigma) = 1-\varepsilon+\beta(\Omega)\varepsilon = 1-\nu(\Omega)\varepsilon, \quad (17)$$

where $\beta(\Omega)$ is the second largest eigenvalue of Ω, and $\nu(\Omega) := 1-\beta(\Omega)$ is the *spectral gap* from the maximum eigenvalue 1. After N runs, the probability that "bad" states σ_j pass all the tests is at most $[1-\nu(\Omega)\varepsilon]^N$. To verify the target state $|\Psi\rangle$ within infidelity ε and significance level δ using the strategy Ω, the minimum number of tests required is [36–38]

$$N = \left\lceil \frac{\ln\delta}{\ln[1-\nu(\Omega)\varepsilon]} \right\rceil \approx \left\lceil \frac{1}{\nu(\Omega)} \varepsilon^{-1} \ln\left(\delta^{-1}\right) \right\rceil, \quad (18)$$

which is inversely proportional to the spectral gap $\nu(\Omega)$.

To minimize the number N of tests, we need to maximize the spectral gap $\nu(\Omega)$. If there is no restriction on the measurements, then the best strategy is to perform the test $\{|\Psi\rangle\langle\Psi|, \mathbb{1} - |\Psi\rangle\langle\Psi|\}$, which means $\Omega = |\Psi\rangle\langle\Psi|$, $\nu(\Omega) = 1$, and $N \approx \varepsilon^{-1}\ln(\delta^{-1})$. In most cases of practical interest, however, the target state $|\Psi\rangle$ is entangled, and it is extremely difficult to perform the entangling measurement mentioned above. Therefore, it is of paramount importance to determine the efficiency limit of restricted operations, such as LOCC or separable operations as a relaxation. A verification operator Ω for $|\Psi\rangle$ is called local if the corresponding strategy can be realized by LOCC. The verification operator Ω is separable if both Ω and $\mathbb{1} - \Omega$ are proportional to separable states. Define $\nu_{\mathrm{LC}}(\Psi)$ as the maximum spectral gap that can be achieved by LOCC and $\beta_{\mathrm{LC}}(\Psi) = 1 - \nu_{\mathrm{LC}}(\Psi)$. Define $\nu_{\mathrm{sep}}(\Psi)$ and $\beta_{\mathrm{sep}}(\Psi)$ as the counterparts for separable operations.

Next, the verification operator Ω for $|\Psi\rangle$ is *homogeneous* [37, 38] if it has the form

$$\Omega = |\Psi\rangle\langle\Psi| + \beta(\Omega)(\mathbb{1} - |\Psi\rangle\langle\Psi|), \quad (19)$$

where $\beta(\Omega) \in [0, 1)$. In this case, the probability $\operatorname{tr}(\Omega\sigma)$ is completely determined by the fidelity $\langle\Psi|\sigma|\Psi\rangle$. Such a verification strategy is also useful for fidelity estimation. In analogy to $\nu_{\mathrm{LC}}(\Psi)$, we define $\nu^{\mathrm{H}}_{\mathrm{LC}}(\Psi)$ as the maximum spectral gap of homogeneous verification operators that can be realized by LOCC and let $\beta^{\mathrm{H}}_{\mathrm{LC}}(\Psi) = 1 - \nu^{\mathrm{H}}_{\mathrm{LC}}(\Psi)$. As the counterparts for separable operations, $\nu^{\mathrm{H}}_{\mathrm{sep}}(\Psi)$ and $\beta^{\mathrm{H}}_{\mathrm{sep}}(\Psi)$ can be defined in a similar way. Here the argument Ψ can be omitted if there is no danger of confusion.

D. Verification of bipartite pure states

In this subsection we summarize the main results on the verification of bipartite pure states. Our discussion is mainly based on Refs. [50–53]. Nevertheless, some results presented here were not clearly stated before.

Suppose $|\Psi\rangle \in \mathcal{H}_{AB}$ is a bipartite pure state, then the spectral gaps $\nu_{\mathrm{LC}}(\Psi)$, $\nu_{\mathrm{sep}}(\Psi)$, $\nu^{\mathrm{H}}_{\mathrm{LC}}(\Psi)$, and $\nu^{\mathrm{H}}_{\mathrm{sep}}(\Psi)$ are completely determined by the nonzero Schmidt coefficients of $|\Psi\rangle$ as we shall see shortly. In addition, they are closely tied to important entanglement measures known as the robustness and random robustness [50, 51, 54]. Propositions 6-9 below are proved in Appendix B.

Proposition 6. *Suppose $|\Psi\rangle \in \mathcal{H}_{AB}$; then the spectral gaps $\nu_{\mathrm{LC}}(\Psi)$, $\nu_{\mathrm{sep}}(\Psi)$, $\nu^{\mathrm{H}}_{\mathrm{LC}}(\Psi)$, and $\nu^{\mathrm{H}}_{\mathrm{sep}}(\Psi)$ only depend on the nonzero Schmidt coefficients of $|\Psi\rangle$ and are independent of the local dimensions.*

Thanks to Proposition 6, without loss of generality, we can assume that $|\Psi\rangle$ has the following Schmidt decomposition:

$$|\Psi\rangle = \sum_{j=0}^{d-1} \sqrt{s_j}\,|jj\rangle. \quad (20)$$

Then one can construct the following three verification operators for $|\Psi\rangle$, which are optimal or nearly optimal:

$$\Omega_{\mathrm{sep}} := |\Psi\rangle\langle\Psi| + \sum_{j,k=0,\, j\neq k}^{d-1} \sqrt{s_j s_k}\,|jk\rangle\langle jk|, \quad (21)$$

$$\Omega^{\mathrm{H}}_{\mathrm{sep}} := |\Psi\rangle\langle\Psi| + \frac{\sqrt{s_0 s_1}}{1+\sqrt{s_0 s_1}}(\mathbb{1} - |\Psi\rangle\langle\Psi|), \quad (22)$$

$$\Omega^{\mathrm{H}}_{\mathrm{LC}} := |\Psi\rangle\langle\Psi| + \frac{s_0 + s_1}{2 + s_0 + s_1}(\mathbb{1} - |\Psi\rangle\langle\Psi|). \quad (23)$$

Here, Ω_{sep} was introduced in Ref. [50] and is tied to the computation of the robustness of entanglement [54]; $\Omega^{\mathrm{H}}_{\mathrm{sep}}$ is tied to the random robustness; $\Omega^{\mathrm{H}}_{\mathrm{LC}}$ was introduced in Ref. [52]. The next proposition follows from Refs. [50, 52] as shown in Appendix B.

Proposition 7. *Suppose $|\Psi\rangle\in\mathcal{H}_{AB}$ is given in Eq. (20); then $\Omega_{\rm sep}$ is a separable verification operator of $|\Psi\rangle$, $\Omega_{\rm sep}^{\rm H}$ is a separable homogeneous verification operator of $|\Psi\rangle$, and $\Omega_{\rm LC}^{\rm H}$ is a local homogeneous verification operator of $|\Psi\rangle$. In addition,*

$$\beta(\Omega_{\rm sep})=\sqrt{s_0s_1},\qquad \nu(\Omega_{\rm sep})=1-\sqrt{s_0s_1},\tag{24}$$

$$\beta(\Omega_{\rm sep}^{\rm H})=\frac{\sqrt{s_0s_1}}{1+\sqrt{s_0s_1}},\quad \nu(\Omega_{\rm sep}^{\rm H})=\frac{1}{1+\sqrt{s_0s_1}},\tag{25}$$

$$\beta(\Omega_{\rm LC}^{\rm H})=\frac{s_0+s_1}{2+s_0+s_1},\quad \nu(\Omega_{\rm LC}^{\rm H})=\frac{2}{2+s_0+s_1}.\tag{26}$$

Proposition 8. *Suppose $|\Psi\rangle\in\mathcal{H}_{AB}$ is given in Eq. (20) and has Schmidt rank r. Then*

$$\frac{\left(\sum_j\sqrt{s_j}\right)^2-1}{r^2-1}\leq\beta_{\rm sep}\leq\beta_{\rm LC}\leq\frac{s_0+s_1}{2+s_0+s_1}\leq\frac{1}{3},\tag{27}$$

$$\frac{\sqrt{s_0s_1}}{1+\sqrt{s_0s_1}}=\beta_{\rm sep}^{\rm H}\leq\beta_{\rm LC}^{\rm H}\leq\frac{s_0+s_1}{2+s_0+s_1}\leq\frac{1}{3}.\tag{28}$$

The inequalities in Eqs. (27) and (28) are equivalent to the following inequalities:

$$\frac{2}{3}\leq\frac{2}{2+s_0+s_1}\leq\nu_{\rm LC}\leq\nu_{\rm sep}\leq\frac{r^2-\left(\sum_j\sqrt{s_j}\right)^2}{r^2-1},\tag{29}$$

$$\frac{2}{3}\leq\frac{2}{2+s_0+s_1}\leq\nu_{\rm LC}^{\rm H}\leq\nu_{\rm sep}^{\rm H}=\frac{1}{1+\sqrt{s_0s_1}}.\tag{30}$$

According to Ref. [52], the verification strategy $\Omega_{\rm LC}^{\rm H}$ can be realized using adaptive local projective measurements based on 2-designs [55–57] and two-way communication. It is not clear if this strategy can be realized in a simpler way. As an alternative, Refs. [51, 52] proposed a simpler verification strategy using only two local projective tests based on MUB and one-way communication. Recall that two bases $\{|\psi_j\rangle\}_{j=0}^{d-1}$ and $\{|\varphi_j\rangle\}_{j=0}^{d-1}$ on $\mathcal{H}_A$ are mutually unbiased if $|\langle\psi_j|\varphi_k\rangle|^2=1/d$ for all $j,k=0,1,\ldots,d-1$. To be concrete, we assume that the MUB is composed of the computational basis $\{|j\rangle\}_{j=0}^{d-1}$ and the Fourier basis $\{|u_j\rangle\}_{j=0}^{d-1}$, where $|u_j\rangle=\sum_{k=0}^{d-1}\omega^{jk}|k\rangle/\sqrt{d}$ with $\omega=\mathrm{e}^{2\pi\mathrm{i}/d}$. Let $M=\sqrt{d}\,\mathrm{diag}(\sqrt{s_0},\ldots,\sqrt{s_{d-1}})$ and $|v_j\rangle=M|u_j^*\rangle$. Then the verification operator tied to the MUB strategy is a convex sum of two test projectors and can be expressed as follows:

$$\Omega_{\rm MUB}:=\frac{1}{2}\sum_{j=0}^{d-1}|jj\rangle\langle jj|+\frac{1}{2}\sum_{j=0}^{d-1}|u_jv_j\rangle\langle u_jv_j|.\tag{31}$$

In addition, Ref. [52] showed that

$$\beta(\Omega_{\rm MUB})=\frac{1}{2},\quad \nu(\Omega_{\rm MUB})=\frac{1}{2}.\tag{32}$$

Moreover, $\nu(\Omega_{\rm MUB})$ attains the maximum among all strategies composed of two distinct tests based on local projective measurements. So the MUB strategy is quite appealing to practical applications.

Next, suppose $|\Psi\rangle\in\mathcal{H}_{AB}$ is maximally entangled, which means $s_j=1/d$ for $j=0,1,\ldots,d-1$. Then the first three inequalities in Eq. (27) and the first two inequalities in Eq. (28) are saturated. In addition, the verification operators $\Omega_{\rm sep}^{\rm H}$ and $\Omega_{\rm LC}^{\rm H}$ coincide and are optimal among separable verification operators. Moreover, the optimal separable verification operator is unique when $d=d_A=d_B$ according to Proposition 9 below.

Proposition 9. *Suppose $|\Psi\rangle\in\mathcal{H}_{AB}$ is a maximally entangled state. Then*

$$\beta_{\rm sep}=\beta_{\rm LC}=\beta_{\rm sep}^{\rm H}=\beta_{\rm LC}^{\rm H}=\frac{1}{d+1}.\tag{33}$$

If in addition $d=d_A=d_B$ and Ω is a separable verification operator of $|\Psi\rangle$. Then $\beta(\Omega)=1/(d+1)$ iff

$$\Omega=\Omega_{\rm opt}:=|\Psi\rangle\langle\Psi|+\frac{1}{d+1}(\mathbb{1}-|\Psi\rangle\langle\Psi|),\tag{34}$$

which is automatically local and homogeneous.

When $d=d_A=d_B$, $\mathcal{H}_A$ and $\mathcal{H}_B$ are isomorphic. According to Ref. [51], the optimal verification strategy $\Omega_{\rm opt}$ in Eq. (34) can be realized using local projective measurements based on 2-designs. Suppose $|\Psi\rangle=|\Phi\rangle$ and $\{\mathcal{B}_l,p_l\}_l$ is a weighted set of orthonormal bases in $\mathcal{H}_A$ that forms a complex projective 2-design. Then $\Omega_{\rm opt}$ can be realized as follows:

$$\Omega_{\rm opt}=\sum_l p_l\Pi(\mathcal{B}_l),\quad \Pi(\mathcal{B}_l)=\sum_{|\psi\rangle\in\mathcal{B}_l}|\psi\rangle\langle\psi|\otimes|\psi^*\rangle\langle\psi^*|,\tag{35}$$

where $|\psi^*\rangle$ denotes the complex conjugate of $|\psi\rangle$ with respect to the computational basis, and the test $\Pi(\mathcal{B}_l)$ can be realized by conjugate-basis measurements. To construct such an optimal strategy, we need at least $d+1$ distinct local projective tests because at least $d+1$ bases are required to construct a 2-design in dimension d [58]. The lower bound can be saturated when the local dimension d is a prime power, in which case a 2-design can be constructed from a complete set of $d+1$ MUB (with uniform weights) [59–61].

III. ENTANGLEMENT AND RESOURCE CERTIFICATION

In this section we introduce a general framework for certifying quantum resources under restricted operations. For concreteness, we shall focus on entanglement certification under LOCC or separable operations in the following discussions, but generalization to other resources, such as quantum coherence and nonstabilizerness, is immediate.

Let $\mathcal{H}$ be a bipartite or multipartite Hilbert space and $|\Psi\rangle\in\mathcal{H}$ the target state of practical interest. Let $\mathcal{S}$ be a closed convex subset of quantum states in $\mathcal{D}(\mathcal{H})$ that represents the set of separable states or states with limited entanglement. Here our main concern is bipartite entanglement and we are particularly interested in the sets $\mathcal{S}_r$ and $\mathcal{S}_{\mathcal{E}_r}(E)$ defined in Sec. II A, but the following analysis has a much wider scope of applications.

A. Basic framework

A device is supposed to produce the target state $|\Psi\rangle \in \mathcal{H}$, but may actually produce states $\sigma_1, \sigma_2, \dots, \sigma_N \in \mathcal{S}$ in N runs. Now, our task is to distinguish the two situations as efficiently as possible. To this end we can devise a family of binary tests $\{\Pi_l, \mathbb{1} - \Pi_l\}_l$ as in QSV, such that the target state can always pass each test, that is, $\Pi_l|\Psi\rangle = |\Psi\rangle$. Suppose the test $\{\Pi_l, \mathbb{1} - \Pi_l\}$ is chosen randomly with probability p_l; then the performance of this strategy is determined by the verification operator $\Omega = \sum_l p_l \Pi_l$ as in QSV. More precisely, the performance is determined by the *separation probability* $P_\Omega(\Psi, \mathcal{S})$ defined as follows:

$$P_\Omega(\Psi, \mathcal{S}) := \max_{\sigma\in\mathcal{S}} \operatorname{tr}(\Omega\sigma). \tag{36}$$

The smaller the separation probability $P_\Omega(\Psi, \mathcal{S})$, the better the strategy Ω can distinguish the target state $|\Psi\rangle$ from states in the set $\mathcal{S}$. After N runs, the states in the set $\mathcal{S}$ can pass all tests with probability at most $P_\Omega^N(\Psi, \mathcal{S})$. When $P_\Omega(\Psi, \mathcal{S}) < 1$, to certify the target state $|\Psi\rangle$ with significance level δ, which means $P_\Omega^N(\Psi, \mathcal{S}) \le \delta$, it suffices to choose

$$N = \left\lceil \frac{\ln\delta}{\ln P_\Omega(\Psi, \mathcal{S})} \right\rceil = \left\lceil \frac{\ln(\delta^{-1})}{\ln\bigl[P_\Omega^{-1}(\Psi, \mathcal{S})\bigr]} \right\rceil. \tag{37}$$

To minimize the number of tests required, we need to minimize $P_\Omega(\Psi, \mathcal{S})$ over all accessible strategies. Here we are particularly interested in strategies that can be realized by LOCC. The *separation probability* of $|\Psi\rangle$ with respect to the set $\mathcal{S}$ is defined as

$$P_{\mathrm{LC}}(\Psi, \mathcal{S}) := \min_\Omega P_\Omega(\Psi, \mathcal{S}) = \min_\Omega \max_{\sigma\in\mathcal{S}} \operatorname{tr}(\Omega\sigma), \tag{38}$$

where the minimization is taken over all local strategies. It can be written as $P(\Psi, \mathcal{S})$ if there is no danger of confusion. If Ω is an optimal strategy, then the number of tests required reads

$$N = \left\lceil \frac{\ln\delta}{\ln P(\Psi, \mathcal{S})} \right\rceil = \left\lceil \frac{\ln(\delta^{-1})}{\ln[P^{-1}(\Psi, \mathcal{S})]} \right\rceil. \tag{39}$$

Therefore, the separation probability $P(\Psi, \mathcal{S})$ determines how well we can certify the target state $|\Psi\rangle$ against the set $\mathcal{S}$ under LOCC and is thus of special interest to both theoretical studies and practical applications. When $\mathcal{S} = \mathcal{S}_{\mathrm{sep}}$, the notation $P(\Psi, \mathcal{S})$ can be abbreviated as $P(\Psi)$ for simplicity.

The separation probability $P_{\mathrm{LC}}^{\mathrm{H}}(\Psi, \mathcal{S})$ is defined in analogy to $P_{\mathrm{LC}}(\Psi, \mathcal{S})$ in Eq. (38) except that the minimization is taken over all homogeneous strategies that can be realized by LOCC. It can be abbreviated as $P^{\mathrm{H}}(\Psi, \mathcal{S})$ if there is no danger of confusion. In addition, $P_{\mathrm{sep}}(\Psi, \mathcal{S})$ and $P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S})$ can be defined by replacing LOCC with separable operations.

B. Basic properties of the separation probabilities

Here we clarify the basic properties of the separation probabilities based on LOCC. Suppose $\mathcal{S}$ is a closed convex subset of $\mathcal{D}(\mathcal{H})$ that is invariant under local unitary transformations. Propositions 10-14 below can be verified by straightforward calculations. Similar results also apply to separation probabilities based on separable operations.

Proposition 10. *Suppose Ω is a verification operator of $|\Psi\rangle \in \mathcal{H}$; then*

$$P_\Omega(\Psi, \mathcal{S}) \le \nu(\Omega) F(\Psi, \mathcal{S}) + \beta(\Omega), \tag{40}$$

where the inequality is saturated when Ω is homogeneous.

Proposition 10 is a simple corollary of the following inequality:

$$\Omega \le |\Psi\rangle\langle\Psi| + \beta(\Omega)(\mathbb{1} - |\Psi\rangle\langle\Psi|) = \nu(\Omega)|\Psi\rangle\langle\Psi| + \beta(\Omega)\mathbb{1}, \tag{41}$$

and the inequality is saturated when Ω is homogeneous. In turn it implies the following proposition.

Proposition 11. *Suppose $|\Psi\rangle \in \mathcal{H}$; then*

$$F(\Psi, \mathcal{S}) \le P(\Psi, \mathcal{S}) \le \nu(\Psi) F(\Psi, \mathcal{S}) + \beta(\Psi), \tag{42}$$

$$P^{\mathrm{H}}(\Psi, \mathcal{S}) = \nu^{\mathrm{H}}(\Psi) F(\Psi, \mathcal{S}) + \beta^{\mathrm{H}}(\Psi). \tag{43}$$

Next, we show that pure states that are equivalent under local unitary transformations share the same separation probabilities. In addition, their optimal verification operators are connected by local unitary transformations.

Proposition 12. *Suppose Ω is a (homogeneous) verification operator of $|\Psi\rangle \in \mathcal{H}$ and $U \in \mathrm{U}(\mathcal{H})$. Then $U\Omega U^\dagger$ is a (homogeneous) verification operator of $U|\Psi\rangle$. If U is a local unitary, then*

$$\begin{aligned} P_{U\Omega U^\dagger}\bigl(U\Psi U^\dagger, \mathcal{S}\bigr) &= P_\Omega(\Psi, \mathcal{S}), \\ P\bigl(U\Psi U^\dagger, \mathcal{S}\bigr) &= P(\Psi, \mathcal{S}), \\ P^{\mathrm{H}}\bigl(U\Psi U^\dagger, \mathcal{S}\bigr) &= P^{\mathrm{H}}(\Psi, \mathcal{S}). \end{aligned} \tag{44}$$

Thanks to Proposition 12, we can focus on a particular representative within each equivalent class when studying the separation probabilities. In addition, Proposition 12 implies the following two propositions.

Proposition 13. *Suppose Ω is a verification operator of the state $|\Psi\rangle \in \mathcal{H}$, $U \in \mathrm{U}(\mathcal{H})$, $U|\Psi\rangle = |\Psi\rangle$, $\Omega_1 = U\Omega U^\dagger$, and $\Omega_2 = (\Omega + \Omega_1)/2$. Then Ω_1 and Ω_2 are verification operators of $|\Psi\rangle$ and $\beta(\Omega_2) \le \beta(\Omega_1) = \beta(\Omega)$. If U is a local unitary, then*

$$P_{\Omega_2}(\Psi, \mathcal{S}) \le P_{\Omega_1}(\Psi, \mathcal{S}) = P_\Omega(\Psi, \mathcal{S}). \tag{45}$$

Let $\mathrm{U_L}(\mathcal{H})$ be the group composed of all local unitaries in $\mathrm{U}(\mathcal{H})$ and $\tilde{\mathrm{U}}_{\mathrm{L}}(\mathcal{H})$ the group generated by $\mathrm{U_L}(\mathcal{H})$ and complex conjugation (with respect to the computational basis).

Proposition 14. *Suppose $|\Psi\rangle \in \mathcal{H}$ is invariant under a subgroup G of $\tilde{\mathrm{U}}_{\mathrm{L}}(\mathcal{H})$. Then there exists an optimal local verification operator Ω of $|\Psi\rangle$ which is G-invariant, that is,*

$$P_\Omega(\Psi,\mathcal{S}) = P(\Psi,\mathcal{S}), \quad U\Omega U^\dagger = \Omega \quad \forall U \in G. \tag{46}$$

Thanks to Proposition 14, to determine the separation probability of $|\Psi\rangle$ or to construct an optimal verification operator, it suffices to consider verification operators that share the same symmetry as $|\Psi\rangle$. This simple observation is very helpful for studying the separation probabilities of bipartite and multipartite quantum states.

IV. CERTIFICATION OF HIGH-DIMENSIONAL ENTANGLEMENT

In this section we consider the certification of HDE in general bipartite pure states in the bipartite Hilbert space $\mathcal{H}_{AB}$ and clarify the basic properties of separation probabilities. The following proposition is proved in Appendix C.

Proposition 15. *Suppose $|\Psi\rangle \in \mathcal{H}_{AB}$, $\mathcal{S} = \mathcal{S}_r$ or $\mathcal{S} = \mathcal{S}_{\mathcal{E}_r}(E)$ with $r \in [d-1]$, and $0 \le E < \mathcal{E}_r(\Psi)$. Then the separation probabilities $P_{\mathrm{LC}}(\Psi,\mathcal{S})$, $P_{\mathrm{sep}}(\Psi,\mathcal{S})$, $P^{\mathrm{H}}_{\mathrm{LC}}(\Psi,\mathcal{S})$, and $P^{\mathrm{H}}_{\mathrm{sep}}(\Psi,\mathcal{S})$ are independent of the local dimensions as long as the nonzero Schmidt coefficients of $|\Psi\rangle$ are fixed.*

Thanks to Proposition 15, to determine the separation probabilities of $|\Psi\rangle$ we can consider any bipartite pure state that has the same nonzero Schmidt coefficients as $|\Psi\rangle$, which is very helpful for simplifying the analysis.

A. HDE in maximally entangled states

To start with, here we focus on the maximally entangled state $|\Phi\rangle \in \mathcal{H}_{AB}$ defined in Eq. (3), assuming that $d = d_A = d_B$. Any other maximally entangled state in $\mathcal{H}_{AB}$ is equivalent to $|\Phi\rangle$ under local unitary transformations. Note that $|\Phi\rangle$ is invariant under arbitrary unitary transformations of the form $U\otimes U^*$ with $U \in \mathrm{U}(d)$. Moreover, any operator on $\mathcal{H}_{AB}$ that shares this symmetry is a linear combination of $|\Phi\rangle\langle\Phi|$ and the identity operator. Therefore, by Proposition 14, to construct an optimal verification operator, it suffices to consider homogeneous verification operators. Moreover, the verification operator Ω_{opt} defined in Proposition 9 with $|\Psi\rangle = |\Phi\rangle$ is optimal for HDE certification among all verification operators based on separable operations, including LOCC.

Now, suppose $\mathcal{S}$ is a closed convex subset of $\mathcal{D}(\mathcal{H}_{AB})$ that is invariant under local unitary transformations. Then, by Proposition 11 with $\beta(\Phi) = \beta(\Omega_{\mathrm{opt}}) = 1/(d+1)$ and $\nu(\Phi) = \nu(\Omega_{\mathrm{opt}}) = d/(d+1)$, the separation probability $P(\Phi,\mathcal{S})$ reads

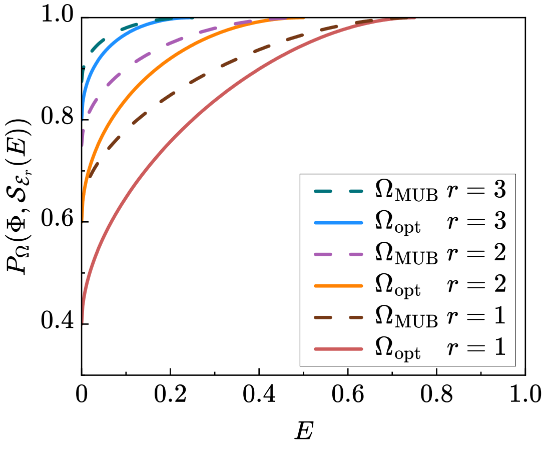

FIG. 1. The separation probabilities $P_\Omega(\Phi,\mathcal{S}_{\mathcal{E}_r}(E))$ achieved by the MUB strategy Ω_{MUB} and optimal strategy Ω_{opt} as functions of E for $d = 4$ and $r = 1, 2, 3$.

$$P(\Phi,\mathcal{S}) = P_{\Omega_{\mathrm{opt}}}(\Phi,\mathcal{S}) = \frac{d}{d+1}F(\Phi,\mathcal{S}) + \frac{1}{d+1}. \tag{47}$$

The following theorem is a simple corollary of Eq. (47) and Proposition 3.

Theorem 1. *Suppose $r \in [d-1]$ and $0 \le E < (d-r)/d$. Then*

$$P(\Phi,\mathcal{S}_r) = \frac{r+1}{d+1}, \tag{48}$$

$$P(\Phi,\mathcal{S}_{\mathcal{E}_r}(E)) = \frac{\left[\sqrt{(d-r)E} + \sqrt{r(1-E)}\right]^2 + 1}{d+1}. \tag{49}$$

In conjunction with Eq. (39), it is straightforward to determine the number of tests required to certify the lower bound $r+1$ for the Schmidt number with significance level δ:

$$N = \left\lceil \left(\ln\frac{d+1}{r+1}\right)^{-1} \ln(\delta^{-1}) \right\rceil. \tag{50}$$

This number increases monotonically with r, but decreases monotonically with d. When $d+1 \ge (r+1)/\delta$, we have $N = 1$, hence HDE can be certified using a single test when d is sufficiently large compared with r. This conclusion is robust to noise thanks to the formula for $P(\Phi,\mathcal{S}_{\mathcal{E}_r}(E))$ in Eq. (49), as illustrated in Fig. 1. Note that the separation probability $P(\Phi,\mathcal{S}_{\mathcal{E}_r}(E))$ is nondecreasing in r and E and concave in E. In the special case $r = 1$ and $E = 0$, which means $\mathcal{S}_{\mathcal{E}_r}(E) = \mathcal{S}_r = \mathcal{S}_{\mathrm{sep}}$, we obtain the separation probability for certifying entanglement and the corresponding number of required tests:

$$P(\Phi) = \frac{2}{d+1}, \quad N = \left\lceil \left(\ln\frac{d+1}{2}\right)^{-1} \ln(\delta^{-1}) \right\rceil. \tag{51}$$

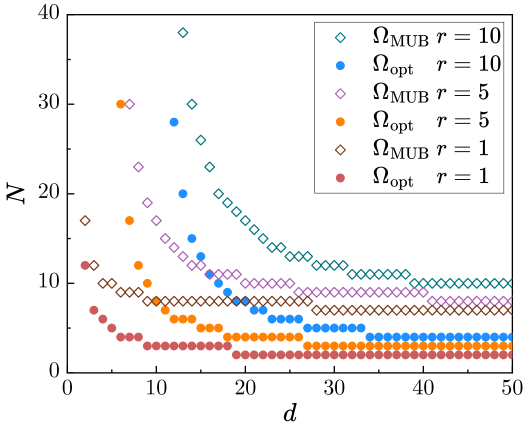

FIG. 2. Certification of the Schmidt number of the $d \times d$ maximally entangled state based on the two strategies $\Omega_{\rm MUB}$ and $\Omega_{\rm opt}$. The figure shows the number of tests required by each strategy to certify the lower bound $r+1$ for the Schmidt number with significance level $\delta = 0.01$.

To realize the optimal strategy $\Omega_{\rm opt}$ discussed above, we need to construct at least $d+1$ distinct local projective tests, which might be quite challenging. For comparison, next, we turn to the simpler strategy $\Omega_{\rm MUB}$ originally introduced for QSV in Refs. [51, 52] as mentioned in Sec. II D, which is based on only two distinct local projective tests. Previously, similar strategies have been explored for certifying HDE [18, 20, 23, 24], but the distinction between $\Omega_{\rm MUB}$ and $\Omega_{\rm opt}$ is not clear. The following proposition clarifies the separation probabilities achieved by $\Omega_{\rm MUB}$; it may be regarded as a special case of Proposition 17 presented in Sec. IV B.

Proposition 16. *Suppose $r \in [d-1]$ and $0 \le E < (d-r)/d$. Then*

$$P_{\Omega_{\rm MUB}}(\Phi, \mathcal{S}_r) = \frac{r+d}{2d}, \tag{52}$$

$$P_{\Omega_{\rm MUB}}(\Phi, \mathcal{S}_{\mathcal{E}_r}(E)) = \frac{\left[\sqrt{(d-r)E} + \sqrt{r(1-E)}\right]^2 + d}{2d}. \tag{53}$$

In conjunction with Eq. (39), it is straightforward to determine the number of tests required by the strategy $\Omega_{\rm MUB}$ to certify the Schmidt number of the maximally entangled state $|\Phi\rangle$. Figure 2 illustrates the performance of $\Omega_{\rm MUB}$ in comparison with $\Omega_{\rm opt}$. Although $\Omega_{\rm MUB}$ is not as efficient as $\Omega_{\rm opt}$, still it enables us to certify HDE using a constant sample cost.

B. HDE in general bipartite pure states

Now, we turn to a general bipartite pure state $|\Psi\rangle$ in $\mathcal{H}_{AB}$, without assuming $d_A = d_B$. Since $|\Psi\rangle$ lacks the high degree of symmetry enjoyed by the maximally entangled state $|\Phi\rangle$, it is in general extremely difficult to derive an exact formula for the separation probabilities $P_{\rm LC}(\Psi, \mathcal{S})$ and $P_{\rm sep}(\Psi, \mathcal{S})$ with $\mathcal{S} = \mathcal{S}_r$ or $\mathcal{S} = \mathcal{S}_{\mathcal{E}_r}(E)$, assuming that $r \in [d-1]$ and $0 \le E < \mathcal{E}_r(\Psi)$. Nevertheless, we can clarify their key properties and derive nearly tight upper and lower bounds. Theorems 2-5 below are proved in Appendix D.

Theorem 2. *Suppose $|\Psi\rangle \in \mathcal{H}_{AB}$, $r \in [d-1]$, $0 \le E < (d-r)/d$, and $\mathcal{S} = \mathcal{S}_r$ or $\mathcal{S} = \mathcal{S}_{\mathcal{E}_r}(E)$. Then the separation probabilities $P_{\rm LC}(\Psi, \mathcal{S})$ and $P_{\rm sep}(\Psi, \mathcal{S})$ are Schur convex in $|\Psi\rangle$ and do not decrease if $|\Psi\rangle$ is subjected to LOCC. In addition,*

$$P_{\rm LC}(\Phi, \mathcal{S}) = P_{\rm sep}(\Phi, \mathcal{S}) \le P_{\rm sep}(\Psi, \mathcal{S}) \le P_{\rm LC}(\Psi, \mathcal{S}), \tag{54}$$

$$P_{\rm LC}(\Phi, \mathcal{S}) = P_{\rm sep}(\Phi, \mathcal{S}) \le P^{\rm H}_{\rm sep}(\Psi, \mathcal{S}) \le P^{\rm H}_{\rm LC}(\Psi, \mathcal{S}). \tag{55}$$

According to Theorem 2, if $|\Psi\rangle$ is subjected to LOCC, then it is more difficult to distinguish the resulting state from states with no or limited entanglement as expected. However, the situation is quite different if we restrict the analysis to homogeneous verification strategies. Notably, the separation probability $P^{\rm H}_{\rm sep}(\Psi, \mathcal{S}_r)$ is not necessarily Schur convex. For example, consider the following two two-qutrit states:

$$\begin{aligned} |\Psi_1\rangle &= \sqrt{\frac{2}{5}}|00\rangle + \sqrt{\frac{2}{5}}|11\rangle + \sqrt{\frac{1}{5}}|22\rangle, \\ |\Psi_2\rangle &= \sqrt{\frac{3}{5}}|00\rangle + \sqrt{\frac{1}{5}}|11\rangle + \sqrt{\frac{1}{5}}|22\rangle, \end{aligned} \tag{56}$$

where $|\Psi_1\rangle$ is majorized by $|\Psi_2\rangle$, which means $|\Psi_1\rangle$ can be transformed into $|\Psi_2\rangle$ under LOCC by Proposition 5. On the other hand, when $r=2$, from Theorem 3 below, we can deduce that

$$P^{\rm H}_{\rm sep}(\Psi_2, \mathcal{S}_r) = \frac{4+\sqrt{3}}{5+\sqrt{3}} < P^{\rm H}_{\rm sep}(\Psi_1, \mathcal{S}_r) = \frac{6}{7}. \tag{57}$$

Therefore, $P^{\rm H}_{\rm sep}(\Psi, \mathcal{S}_r)$ is not Schur convex.

Next, suppose $|\Psi\rangle$ has Schmidt spectrum $\{s_j\}_{j=0}^{d-1}$ with $s_0 \ge s_1 \ge \cdots \ge s_{d-1} \ge 0$. Here, we provide a number of informative upper and lower bounds for four types of separation probabilities and show that HDE in a general bipartite pure state can be certified efficiently. Define

$$\begin{aligned} P^{\rm LB}_{\rm sep}(\Psi, \mathcal{S}_r) &= 1 - \mathcal{E}_r(\Psi), \\ P^{\rm UB}_{\rm LC}(\Psi, \mathcal{S}_r) &= 1 - \frac{2\mathcal{E}_r(\Psi)}{2+s_0+s_1}, \\ P^{\rm LB}_{\rm sep}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) &= f_r(\Psi, E), \\ P^{\rm UB}_{\rm LC}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) &= \frac{2f_r(\Psi, E) + s_0 + s_1}{2+s_0+s_1}, \end{aligned} \tag{58}$$

where $\mathcal{E}_r(\Psi) = \sum_{j=r}^{d-1} s_j$ and $f_r(\Psi, E) = F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E))$ as determined in Eq. (12) of Proposition 3. The following theorem is a direct consequence of Propositions 3, 8, 10, and 11 as shown in Appendix D.

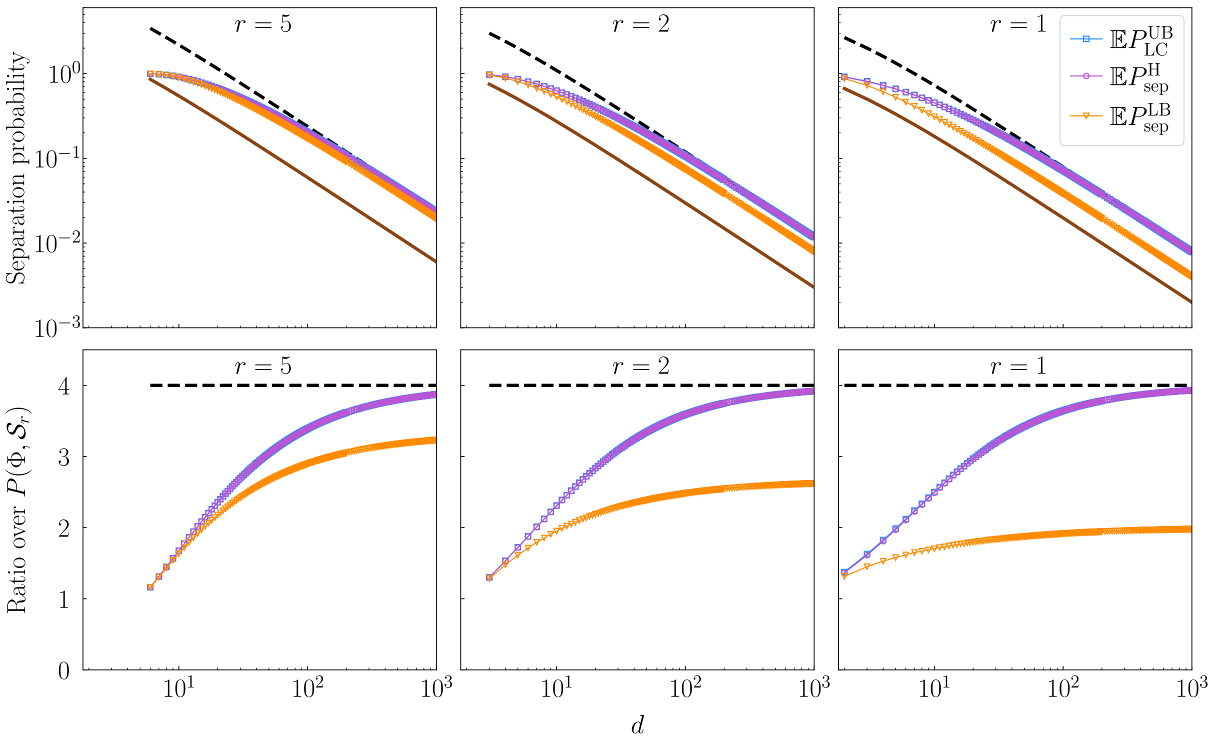

FIG. 3. The mean separation probabilities (upper plots) and their ratios over $P(\Phi, \mathcal{S}_r) = P_{\mathrm{sep}}(\Phi, \mathcal{S}_r) = (r+1)/(d+1)$ (lower plots) as functions of $d = d_A = d_B$ for $r = 1, 2, 5$. Here $\mathbb{E}P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r)$ is an upper bound for $\mathbb{E}P_{\mathrm{LC}}^{\mathrm{H}}(\Psi, \mathcal{S}_r)$ and $\mathbb{E}P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_r)$, while $\mathbb{E}P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_r)$ is a lower bound for $\mathbb{E}P_{\mathrm{sep}}(\Psi, \mathcal{S}_r)$ and $\mathbb{E}P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_r)$. Note that $\mathbb{E}P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r)$ and $\mathbb{E}P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_r)$ almost coincide. The brown solid line and black dashed line in each plot denote the lower bound $P(\Phi, \mathcal{S}_r)$ and upper bound $4P(\Phi, \mathcal{S}_r)$, respectively, as presented in Theorem 4. For each local dimension d, 10000 Haar-random pure states are sampled.

Theorem 3. *Suppose* $|\Psi\rangle \in \mathcal{H}_{AB}$ *has Schmidt spectrum* $\{s_j\}_{j=0}^{d-1}$, $r \in [d-1]$, *and* $0 \leq E < \mathcal{E}_r(\Psi)$. *Then*

$$P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_r) \leq P_{\mathrm{sep}}(\Psi, \mathcal{S}_r) \leq P_{\mathrm{LC}}(\Psi, \mathcal{S}_r) \leq P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r) \leq \frac{2}{1+s_0} P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_r), \tag{59}$$

$$1 - \frac{\mathcal{E}_r(\Psi)}{1+\sqrt{s_0 s_1}} = P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_r) \leq P_{\mathrm{LC}}^{\mathrm{H}}(\Psi, \mathcal{S}_r) \leq P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r) \leq \frac{3}{2+s_0} P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_r), \tag{60}$$

$$P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) \leq P_{\mathrm{sep}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) \leq P_{\mathrm{LC}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) \leq P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) \leq \frac{2}{1+s_0} P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)), \tag{61}$$

$$\frac{f_r(\Psi, E) + \sqrt{s_0 s_1}}{1+\sqrt{s_0 s_1}} = P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) \leq P_{\mathrm{LC}}^{\mathrm{H}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) \leq P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) \leq \frac{3}{2+s_0} P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)). \tag{62}$$

If $|\Psi\rangle = \sum_{j=0}^{d-1} \sqrt{s_j}\,|jj\rangle$ as in Eq. (20), then $P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r)$ and $P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E))$ correspond to the separation probabilities of the local homogeneous verification operator $\Omega_{\mathrm{LC}}^{\mathrm{H}}$ defined in Eq. (23), which is reproduced from Ref. [52]. By contrast, $P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_r)$ and $P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E))$ correspond to the separation probabilities of the verification operator $\Omega = |\Psi\rangle\langle\Psi|$, which is in general not separable. Nevertheless, for some bipartite entangled pure states, these separation probabilities can also be attained by a separable verification operator, as we shall see in Sec. V. The separation probabilities $P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_r)$ and $P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E))$ can be attained by the optimal separable homogeneous verification operator $\Omega_{\mathrm{sep}}^{\mathrm{H}}$ in Eq. (22) (see also Proposition 7).

Next, we clarify the separation probabilities of the strategy Ω_{MUB} defined in Eq. (31) for certifying the Schmidt number of the state $|\Psi\rangle$ in Eq. (20). Let

$$|\tilde{\Psi}\rangle = \sum_{j=0}^{r-1} \sqrt{\frac{(1-E)s_j}{1-\mathcal{E}_r(\Psi)}}\,|jj\rangle + \sum_{j=r}^{d-1} \sqrt{\frac{E s_j}{\mathcal{E}_r(\Psi)}}\,|jj\rangle; \tag{63}$$

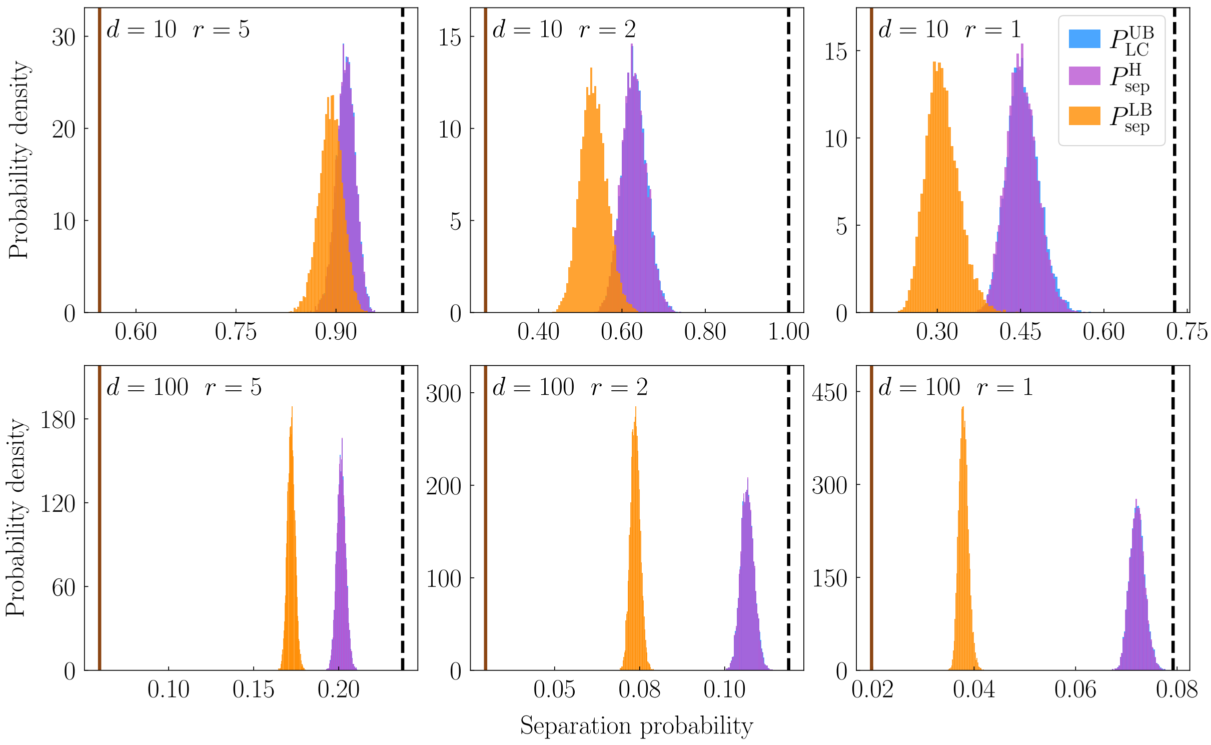

FIG. 4. Distributions of the separation probabilities and relevant bounds for Haar-random pure states with $d = d_A = d_B = 10, 100$ and $r = 1, 2, 5$. Note that the distributions of $P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r)$ and $P_{\mathrm{sep}}^{\mathrm{H}}(\Psi, \mathcal{S}_r)$ are almost indistinguishable. The brown solid line and black dashed line in each plot denote the values $P(\Phi, \mathcal{S}_r)$ and $4P(\Phi, \mathcal{S}_r)$, respectively (cf. Fig. 3). For each local dimension d, 10000 Haar-random pure states are sampled.

then $\tilde{\Psi} \in \mathcal{S}_{\mathcal{E}_r}(E)$ and

$$\operatorname{tr}\bigl(\Omega_{\mathrm{MUB}} |\tilde{\Psi}\rangle\langle\tilde{\Psi}|\bigr) = \frac{f_r(\Psi, E) + 1}{2}. \tag{64}$$

Therefore, the inequality in Eq. (40) of Proposition 10 is saturated when $\Omega = \Omega_{\mathrm{MUB}}$ and $\mathcal{S} = \mathcal{S}_{\mathcal{E}_r}(E)$, given that $\nu(\Omega_{\mathrm{MUB}}) = \beta(\Omega_{\mathrm{MUB}}) = 1/2$. In conjunction with the observation $\mathcal{S}_r = \mathcal{S}_{\mathcal{E}_r}(0)$, we can immediately deduce the following proposition.

Proposition 17. *Suppose $|\Psi\rangle \in \mathcal{H}_{AB}$ has Schmidt spectrum $\{s_j\}_{j=0}^{d-1}$, $r \in [d-1]$, and $0 \leq E < \mathcal{E}_r(\Psi)$. Then*

$$P_{\Omega_{\mathrm{MUB}}}(\Psi, \mathcal{S}_r) = 1 - \frac{\mathcal{E}_r(\Psi)}{2}, \tag{65}$$

$$P_{\Omega_{\mathrm{MUB}}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) = \frac{f_r(\Psi, E) + 1}{2}. \tag{66}$$

In conjunction with Eq. (58) we can derive the following relations:

$$P_{\Omega_{\mathrm{MUB}}}(\Psi, \mathcal{S}_r) = \frac{P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_r) + 1}{2}, \tag{67}$$

$$P_{\Omega_{\mathrm{MUB}}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) = \frac{P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) + 1}{2}. \tag{68}$$

These equations mean $P_{\Omega_{\mathrm{MUB}}}(\Psi, \mathcal{S}_r) - P_{\mathrm{sep}}(\Psi, \mathcal{S}_r) < 1/2$ and the inequality still holds if $\mathcal{S}_r$ is replaced by $\mathcal{S}_{\mathcal{E}_r}(E)$.

Next, we consider the general behavior of the separation probabilities for a Haar-random bipartite pure state $|\Psi\rangle \in \mathcal{H}_{AB}$. With high probability we have $s_0, s_1 \sim 1/d$, $\mathcal{E}_r(\Psi) \sim (d-r)/d$, and $P_{\mathrm{sep}}^{\mathrm{LB}}(\Psi, \mathcal{S}_r)$, $P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r) \sim r/d$ for $r < (d-3)/4$. Therefore, HDE can be certified efficiently by LOCC, which is corroborated by rigorous analytical derivation and extensive numerical simulations as shown below.

Theorem 4. *Suppose $|\Psi\rangle$ is a Haar-random pure state in $\mathcal{H}_{AB}$ and $r \in [d-1]$. Then*

$$\begin{aligned}\frac{r+1}{d+1} &\leq \mathbb{E}P_{\mathrm{sep}}(\Psi, \mathcal{S}_r) \leq \mathbb{E}P_{\mathrm{LC}}(\Psi, \mathcal{S}_r) \leq \mathbb{E}P_{\mathrm{LC}}^{\mathrm{H}}(\Psi, \mathcal{S}_r) \\ &\leq \mathbb{E}P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r) \leq \frac{4(r+1)}{d+1} = 4P(\Phi, \mathcal{S}_r).\end{aligned} \tag{69}$$

Theorem 5. *Suppose $|\Psi\rangle$ is a Haar-random pure state in $\mathcal{H}_{AB}$, $r \in [d-1]$, and $\epsilon \geq 0$. Then the separation probability $P_{\mathrm{LC}}^{\mathrm{H}}(\Psi, \mathcal{S}_r)$ satisfies*

$$\Pr\left\{P_{\mathrm{LC}}^{\mathrm{H}}(\Psi, \mathcal{S}_r) \geq \frac{4(r+1)}{d+1} + \epsilon\right\} \leq 2\exp\left(-\frac{D\epsilon^2}{50\pi}\right), \tag{70}$$

where $D = \dim(\mathcal{H}_{AB})$, and the same result still holds *if $P_{\rm LC}^{\rm H}(\Psi,\mathcal{S}_r)$ is replaced by $P_{\rm LC}(\Psi,\mathcal{S}_r)$, $P_{\rm sep}^{\rm H}(\Psi,\mathcal{S}_r)$, or $P_{\rm sep}(\Psi,\mathcal{S}_r)$.*

As a complement to Theorems 4 and 5, Fig. 3 shows the mean separation probability $\mathbb{E}P_{\rm sep}^{\rm H}(\Psi,\mathcal{S}_r)$ as a function of d for $r=1,2,5$. Also shown are the upper bound $\mathbb{E}P_{\rm LC}^{\rm UB}(\Psi,\mathcal{S}_r)$ for $\mathbb{E}P_{\rm LC}^{\rm H}(\Psi,\mathcal{S}_r)$ and $\mathbb{E}P_{\rm sep}^{\rm H}(\Psi,\mathcal{S}_r)$ and the lower bound $\mathbb{E}P_{\rm sep}^{\rm LB}(\Psi,\mathcal{S}_r)$ for $\mathbb{E}P_{\rm sep}(\Psi,\mathcal{S}_r)$ and $\mathbb{E}P_{\rm sep}^{\rm H}(\Psi,\mathcal{S}_r)$. This figure indicates that

$$\mathbb{E}P_{\rm LC}^{\rm UB}(\Psi,\mathcal{S}_r)\approx\mathbb{E}P_{\rm LC}^{\rm H}(\Psi,\mathcal{S}_r)\approx\mathbb{E}P_{\rm sep}^{\rm H}(\Psi,\mathcal{S}_r), \qquad (71)$$

so the verification strategy in Eq. (23) is nearly optimal among local homogeneous strategies for the Haar-random pure state $|\Psi\rangle$. In addition, the values in the above equation are close to the upper bound $4P(\Phi,\mathcal{S}_r)$ when d is sufficiently large compared with r, in which case the last two inequalities in Eq. (69) are approximately saturated. Figure 4 shows the probability density distributions of $P_{\rm LC}^{\rm UB}(\Psi,\mathcal{S}_r)$, $P_{\rm sep}^{\rm H}(\Psi,\mathcal{S}_r)$, and $P_{\rm sep}^{\rm LB}(\Psi,\mathcal{S}_r)$. All these distributions are concentrated within the interval $[P(\Phi,\mathcal{S}_r),4P(\Phi,\mathcal{S}_r)]$ and become increasingly concentrated as d increases. These results further demonstrate that HDE in general bipartite pure states can be certified efficiently.

V. CERTIFICATION OF ENTANGLEMENT IN TWO-QUBIT PURE STATES

In this section, we construct an optimal separable strategy and two nearly optimal local strategies for certifying the entanglement of a general two-qubit pure state. When the state has sufficiently high concurrence, we further show that the optimal separable strategy can also be implemented by LOCC.

Up to a local unitary transformation, any two-qubit entangled pure state can be expressed as follows:

$$|\Psi_\theta\rangle=\cos\theta|00\rangle+\sin\theta|11\rangle,\quad 0<\theta\leq\frac{\pi}{4}. \qquad (72)$$

Note that $|\Psi_\theta\rangle$ is invariant under the swap operation and complex conjugation (with respect to the computational basis). In addition, $|\Psi_\theta\rangle$ is invariant under any local unitary transformation of the form $V_\zeta\otimes V_\zeta^*$, where

$$V_\zeta=|0\rangle\langle0|+{\rm e}^{-{\rm i}\zeta}|1\rangle\langle1|,\quad 0\leq\zeta<2\pi. \qquad (73)$$

Therefore, we can restrict our attention to verification operators that enjoy the same symmetry when searching for an optimal strategy.

Given $0<\theta\leq\pi/4$ and $0\leq p\leq1$, define the following verification operators:

$$\Omega_0:=|\Psi_\theta\rangle\langle\Psi_\theta|+\cos\theta\sin\theta(|01\rangle\langle01|+|10\rangle\langle10|), \qquad (74)$$

$$\Omega_1:=|\Psi_\theta\rangle\langle\Psi_\theta|+\frac{\cos\theta\sin\theta}{1+\cos\theta\sin\theta}(\mathbb{1}-|\Psi_\theta\rangle\langle\Psi_\theta|), \qquad (75)$$

$$\Omega(\theta,p):=p\Omega_1+(1-p)\Omega_0. \qquad (76)$$

Note that $\Omega_0=\Omega(\theta,0)$ and $\Omega_1=\Omega(\theta,1)$. In addition, Ω_0, Ω_1, and $\Omega(\theta,p)$ are invariant under the swap operation, complex conjugation, and any local unitary transformation of the form $V_\zeta\otimes V_\zeta^*$. Furthermore, by virtue of the PPT criterion [62, 63], it is straightforward to verify that both Ω_0 and Ω_1 are separable. Here Ω_1 is the optimal QSV strategy proposed in Ref. [64], which can be implemented by local operations with two-way classical communication, and Ω_0 is a separable strategy proposed in the proofs of Lemma 1 and Theorem 2 of Ref. [50]; however, no LOCC implementation of Ω_0 has been found. To simplify the following discussion, the separation probability $P_{\Omega(\theta,p)}(\Psi_\theta)$ will be abbreviated as $P(\theta,p)$ henceforth.

By virtue of Theorem 3 and the above observation, we can immediately derive the following proposition, which clarifies the separation probability associated with an optimal homogeneous strategy that can be realized by separable operations or LOCC. The result is illustrated in Fig. 6.

Proposition 18. *Suppose $0<\theta\leq\pi/4$. Then the local strategy Ω_1 defined in Eq. (75) is optimal among all separable homogeneous strategies for $|\Psi_\theta\rangle$. The separation probabilities $P_{\rm sep}^{\rm H}(\Psi_\theta)$ and $P_{\rm LC}^{\rm H}(\Psi_\theta)$ read*

$$P_{\rm sep}^{\rm H}(\Psi_\theta)=P_{\rm LC}^{\rm H}(\Psi_\theta)=P_{\Omega_1}(\Psi_\theta)=\frac{\cos^2\theta+\cos\theta\sin\theta}{1+\cos\theta\sin\theta}. \qquad (77)$$

If $0\leq E<\sin^2\theta$, then

$$\begin{aligned}P_{\rm sep}^{\rm H}(\Psi_\theta,\mathcal{S}_{\mathcal{E}_1}(E))&=P_{\rm LC}^{\rm H}(\Psi_\theta,\mathcal{S}_{\mathcal{E}_1}(E))=P_{\Omega_1}(\Psi_\theta,\mathcal{S}_{\mathcal{E}_1}(E))\\&=\frac{\cos^2(\theta-\theta_E)+\cos\theta\sin\theta}{1+\cos\theta\sin\theta},\end{aligned} \qquad (78)$$

where $\theta_E=\arcsin\sqrt{E}$.

Next, we turn to general verification strategies. For $0<\theta\leq\pi/4$ and $0\leq p\leq1$, define

$$\begin{aligned}\kappa(\theta)&:=\cos\theta\sin\theta,\\ q(\theta)&:=\max\left\{\frac{(1+\kappa)(2\kappa-\cos^2\theta)}{\kappa(2\kappa+\sin^2\theta)},0\right\},\\ a^*(\theta,p)&:=\begin{cases}0 & q(\theta)\leq p\leq1,\\ \arctan\sqrt{h(\theta,p)} & 0\leq p<q(\theta),\end{cases}\\ h(\theta,p)&:=\frac{(1+\kappa)(2\kappa-\cos^2\theta)-p\kappa(2\kappa+\sin^2\theta)}{(1+\kappa)(2\kappa-\sin^2\theta)-p\kappa(2\kappa+\cos^2\theta)},\end{aligned} \qquad (79)$$

where the arguments θ and p can be omitted to simplify the notation. Here $q(\theta)=0$ when $0<\theta\leq\arctan(1/2)$ and $q(\theta)$ increases from 0 to 1 when θ increases from $\arctan(1/2)$ to $\pi/4$. In addition, if $\arctan(1/2)<\theta\leq\pi/4$ and $0\leq p<q(\theta)$, then we have $0<h(\theta,p)\leq1$ and thus $0<a^*(\theta,p)\leq\pi/4$. Lemmas 1-3 below are proved in Appendix E.

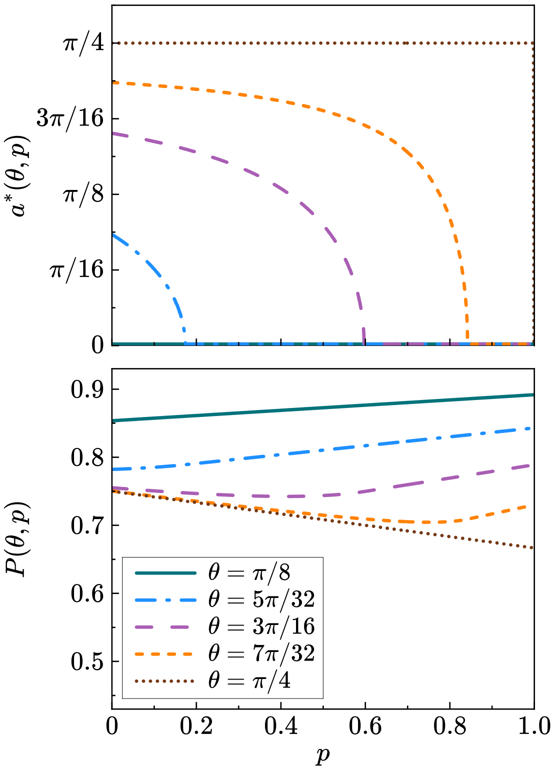

FIG. 5. The function $a^*(\theta,p)$ and the separation probability $P(\theta,p)=P_{\Omega(\theta,p)}(\Psi_\theta)$ for certifying the entanglement of $|\Psi_\theta\rangle$. For a given value of θ, $P(\theta,p)$ is convex in p and has a unique minimizer in p.

Lemma 1. *Suppose $0<\theta\leq\pi/4$. Then, for some $0\leq p\leq 1$, $\Omega(\theta,p)$ is an optimal separable verification operator of the target state $|\Psi_\theta\rangle$, that is,*

$$P_{\rm sep}(\Psi_\theta)=\min_{0\leq p\leq 1}P(\theta,p). \tag{80}$$

Lemma 2. *Suppose $0<\theta\leq\pi/4$ and $0\leq p\leq 1$. Then*

$$\begin{aligned}P(\theta,p)&=\max_{0\leq a\leq\pi/2}\operatorname{tr}\big[\Omega(\theta,p)\rho_a^{\otimes 2}\big]=\operatorname{tr}\big[\Omega(\theta,p)\rho_{a^*}^{\otimes 2}\big]\\&=\begin{cases}\cos^2\theta+\frac{p\cos\theta\sin^3\theta}{1+\cos\theta\sin\theta} & 0<\theta<\pi/4,\ q(\theta)\leq p\leq 1,\\ \frac{9-p}{12} & \theta=\pi/4,\end{cases}\end{aligned} \tag{81}$$

where $\rho_a=|\psi_a\rangle\langle\psi_a|$ and $|\psi_a\rangle=\cos a|0\rangle+\sin a|1\rangle$; in addition, $P(\theta,p)$ is strictly increasing in p for $p\in[q(\theta),1]$. If $p<1$ or $\theta<\pi/4$, then the maximum over a is attained iff $a=a^*$. If $\arctan(1/2)<\theta<\pi/4$, then $P(\theta,p)$ is strictly convex in p for $p\in[0,q(\theta)]$.

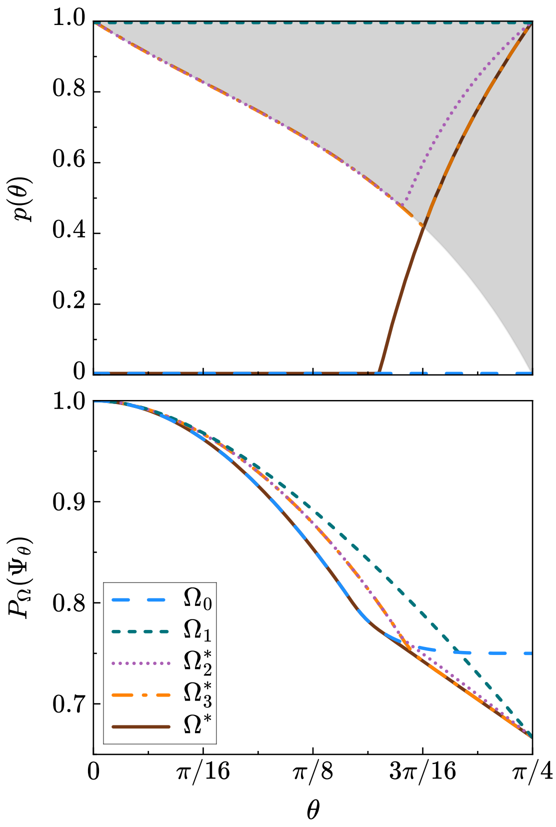

FIG. 6. Several verification strategies $\Omega(\theta,p(\theta))$ of $|\Psi_\theta\rangle$ encoded by θ and $p(\theta)$ according to Eq. (76) (upper plot) and their separation probabilities (lower plot). Here Ω^*, Ω_2^*, and Ω_3^* are shorthands of $\Omega(\theta,p^*(\theta))$, $\Omega(\theta,p_2^*(\theta))$, and $\Omega(\theta,p_3^*(\theta))$, respectively. Verification stategies associated with the shaded region in the upper plot can be realized by LOCC.

The dependence of $P(\theta,p)$ on θ and p is illustrated in Fig. 5. As a simple corollary of Eq. (79) and Lemma 2, the separation probability $P_{\Omega_0}(\Psi_\theta)=P(\theta,0)$ reads

$$P_{\Omega_0}(\Psi_\theta)=\begin{cases}\cos^2\theta & 0<\theta\leq\arctan(1/2),\\ \frac{3\cos^2\theta\sin^2\theta}{4\cos\theta\sin\theta-1} & \arctan(1/2)<\theta\leq\pi/4,\end{cases} \tag{82}$$

as illustrated in Fig. 6. By virtue of Lemmas 1 and 2, we can further determine the separation probability $P_{\rm sep}(\Psi_\theta)$ and identify an optimal separable verification operator. Let θ^* be the unique root of the following equation:

$$17-9\cos(4\theta)-25\sin(2\theta)+3\sin(6\theta)=0,\qquad\theta\in[0,\pi/4]; \tag{83}$$

note that $\theta^*>\arctan(1/2)$ and $\theta^*\approx 0.51095$.

Lemma 3. *Suppose $0<\theta\leq\pi/4$ and $0\leq p\leq 1$. Then the separation probability $P(\theta,p)$ is convex in p and has a unique minimizer $p^*(\theta)$, which is contained in $[0,q(\theta)]$. The probability $P(\theta,p)$ is strictly decreasing (increasing)* *in p for $p \in [0, p^*(\theta)]$ ($p \in [p^*(\theta), 1]$). In addition,*

$$p^*(\theta) = \begin{cases} 0 & 0 < \theta \leq \theta^*, \\ 1 & \theta = \pi/4. \end{cases} \tag{84}$$

If $\theta^* < \theta < \pi/4$, then $p^*(\theta)$ coincides with the unique zero of the partial derivative $\partial P(\theta, p)/\partial p$ over $p \in (0, q(\theta))$.

As a simple corollary of Lemmas 1-3 and Eq. (82), the following theorem determines the separation probability $P_{\rm sep}(\Psi_\theta)$. The variations of $p^*(\theta)$ and $P_{\rm sep}(\Psi_\theta)$ are illustrated in Fig. 6 together with several related quantities.

Theorem 6. *Suppose $0 < \theta \leq \pi/4$. Then $\Omega(\theta, p^*(\theta))$ is an optimal separable strategy for certifying the entanglement of $|\Psi_\theta\rangle$, that is, $P_{\rm sep}(\Psi_\theta) = P(\theta, p^*(\theta))$. In addition,*

$$P_{\rm sep}(\Psi_\theta) = \begin{cases} \cos^2\theta & 0 < \theta \leq \arctan(1/2), \\ \frac{3\cos^2\theta\sin^2\theta}{4\cos\theta\sin\theta - 1} & \arctan(1/2) < \theta \leq \theta^*, \\ 2/3 & \theta = \pi/4. \end{cases} \tag{85}$$

Thanks to Lemma 3 and Theorem 6, the optimal separable strategy for certifying the entanglement of $|\Psi_\theta\rangle$ is unique if we focus on strategies of the form $\Omega(\theta, p)$. Notably, Ω_0 is optimal when $0 < \theta \leq \theta^*$, while Ω_1 is optimal only when $\theta = \pi/4$, although it is an optimal separable strategy for QSV whenever $0 < \theta \leq \pi/4$. In general, the optimal separable strategy for entanglement certification and the counterpart for QSV are different except when $\theta = \pi/4$. Moreover, when $0 < \theta \leq \arctan(1/2)$, the separable strategy Ω_0 even achieves the same separation probability as the globally optimal strategy $\Omega = |\Psi_\theta\rangle\langle\Psi_\theta|$, which is nonseparable. This result is in sharp contrast with the counterpart in QSV, in which the maximum spectral gap cannot be attained by separable operations for any entangled pure state.

In the rest of this section, we turn to certification strategies for $|\Psi_\theta\rangle$ based on LOCC. Now, the problem is much more tricky because it is not clear what strategies of the form $\Omega(\theta, p)$ can be realized by LOCC. Nevertheless, we can pinpoint a specific parameter region in which this is the case. Note that, if $\Omega(\theta, p)$ can be realized by LOCC, then $\Omega(\theta, p')$ for $p' \in [p, 1]$ can also be realized by LOCC given that $\Omega(\theta, 1)$ can be realized by LOCC according to Wang and Hayashi [64]. In addition, we can prove the following proposition as shown in Appendix E 4.

Proposition 19. *Suppose $0 < \theta \leq \pi/4$ and $\tilde{p}(\theta) \leq p \leq 1$ with*

$$\tilde{p}(\theta) := 1 - \frac{\tan\theta}{\cos^2\theta + \cos\theta\sin\theta}. \tag{86}$$

Then $\Omega(\theta, p)$ can be realized by LOCC.

Note that $\tilde{p}(\theta)$ is strictly decreasing in θ, $\tilde{p}(\pi/4) = 0$, and $\lim_{\theta\to 0}\tilde{p}(\theta) = 1$ as illustrated in Fig. 6. Thanks to Proposition 19, we can construct two efficient strategies for certifying the entanglement of $|\Psi_\theta\rangle$ based on LOCC. Let $\theta_2^* = \arctan[(\sqrt{5} - 1)/2]$ and define

$$p_2^*(\theta) := \max\{\tilde{p}(\theta), q(\theta)\} = \begin{cases} \tilde{p}(\theta) & 0 < \theta \leq \theta_2^*, \\ q(\theta) & \theta_2^* < \theta \leq 1, \end{cases} \tag{87}$$

$$p_3^*(\theta) := \max\{\tilde{p}(\theta), p^*(\theta)\}. \tag{88}$$

Then

$$0 \leq p^*(\theta) \leq p_3^*(\theta) \leq p_2^*(\theta) \leq 1, \tag{89}$$

given that $0 \leq \tilde{p}(\theta) \leq 1$ and $0 \leq p^*(\theta) \leq q(\theta) \leq 1$. So the corresponding strategies $\Omega(\theta, p_2^*(\theta))$ and $\Omega(\theta, p_3^*(\theta))$ can be realized by LOCC. By virtue of Lemma 2 we can derive an explicit formula for the separation probability of $\Omega(\theta, p_2^*(\theta))$:

$$\begin{aligned} P(\theta, p_2^*(\theta)) &= \cos^2\theta + \frac{p_2^*\cos\theta\sin^3\theta}{1 + \cos\theta\sin\theta} \\ &= \begin{cases} \cos^2\theta + \frac{(1-\tan\theta)\tan\theta\sin^2\theta}{1+\tan\theta} & 0 < \theta \leq \theta_2^*, \\ \cos^2\theta + \frac{(2\tan\theta-1)\sin^2\theta}{(\tan\theta+2)\tan\theta} & \theta_2^* < \theta \leq \pi/4. \end{cases} \end{aligned} \tag{90}$$

In conjunction with Lemma 3 we can deduce that

$$\begin{aligned} &P_{\rm sep}(\Psi_\theta) = P(\theta, p^*(\theta)) \leq P(\theta, p_3^*(\theta)) \leq P(\theta, p_2^*(\theta)) \\ &\leq P(\theta, 1) = P_{\Omega_1}(\Psi_\theta) = \frac{\cos^2\theta + \cos\theta\sin\theta}{1 + \cos\theta\sin\theta}. \end{aligned} \tag{91}$$

This equation means the strategy $\Omega(\theta, p_3^*(\theta))$ is no worse than $\Omega(\theta, p_2^*(\theta))$, which in turn is no worse than Ω_1, although Ω_1 is the optimal local strategy for QSV. Actually, both strategies $\Omega(\theta, p_2^*(\theta))$ and $\Omega(\theta, p_3^*(\theta))$ are nearly optimal as illustrated in Fig. 6. This observation also shows that the optimal local strategy for entanglement certification is in general different from the counterpart for QSV except when $\theta = \pi/4$, which echoes the result on separable operations as mentioned above.

Finally, numerical calculation shows that $\tilde{p}(\theta) \leq p^*(\theta)$, which means $p_3^*(\theta) = p^*(\theta)$ when $\theta_3^* \leq \theta \leq \pi/4$ for some threshold $\theta_3^* \approx 0.59079$. In this case, the concurrence of the target state $|\Psi_\theta\rangle$ satisfies

$$C(\Psi_\theta) = 2\sin\theta\cos\theta \geq 2\sin\theta_3^*\cos\theta_3^* \approx 0.92521. \tag{92}$$

So the optimal separable entanglement certification strategy $\Omega(\theta, p^*(\theta))$ for $|\Psi_\theta\rangle$ can be realized by LOCC when $\theta_3^* \leq \theta \leq \pi/4$, that is, $C(\Psi_\theta) \geq 2\sin\theta_3^*\cos\theta_3^*$, which means the target state $|\Psi_\theta\rangle$ has sufficiently high entanglement.

VI. SUMMARY

Inspired by QSV, we proposed a simple and general framework for certifying HDE under restricted operations and introduced the concept of separation probabilities.

As concrete examples, separation probabilities associated with the sets $\mathcal{S}_{\rm sep}$, $\mathcal{S}_r$, and $\mathcal{S}_{\mathcal{E}_r}(E)$ were discussed in detail. On this basis, we showed that HDE in general bipartite pure states, including the maximally entangled states in particular, can be certified efficiently using LOCC. Notably, the sample cost for certifying a given degree of HDE even decreases monotonically with the local dimensions. For a general two-qubit pure state, we constructed an optimal entanglement certification strategy based on separable operations and clarified the properties of the separation probabilities. In addition, we showed that this optimal strategy can be realized by LOCC when the target state has sufficiently high entanglement. Our work offers a new perspective on and a practical approach for HDE certification. The basic idea may also find applications in certifying many other important resources, such as coherence and nonstabilizerness, which deserves further studies.

ACKNOWLEDGMENT

This work is supported by Shanghai Science and Technology Innovation Action Plan (Grant No. 24LZ1400200), Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), and the National Key Research and Development Program of China (Grant No. 2022YFA1404204).

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[2] B. M. Terhal and P. Horodecki, Schmidt number for density matrices, Phys. Rev. A **61**, 040301 (2000).

[3] M. Erhard, M. Krenn, and A. Zeilinger, Advances in high-dimensional quantum entanglement, Nat. Rev. Phys. **2**, 365 (2020).

[4] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, Entanglement's benefit survives an entanglement-breaking channel, Phys. Rev. Lett. **111**, 010501 (2013).

[5] M. Huber and M. Pawłowski, Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement, Phys. Rev. A **88**, 032309 (2013).

[6] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, High-dimensional quantum communication: Benefits, progress, and future challenges, Adv. Quantum Technol. **2**, 1900038 (2019).

[7] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, Overcoming noise in entanglement distribution, Phys. Rev. X **9**, 041042 (2019).

[8] X.-M. Hu, C. Zhang, Y. Guo, F.-X. Wang, W.-B. Xing, C.-X. Huang, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, X. Gao, M. Pivoluska, and M. Huber, Pathways for entanglement-based quantum communication in the face of high noise, Phys. Rev. Lett. **127**, 110505 (2021).

[9] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White, Simplifying quantum logic using higher-dimensional Hilbert spaces, Nat. Phys. **5**, 134 (2009).

[10] M. Van den Nest, Universal quantum computation with little entanglement, Phys. Rev. Lett. **110**, 060504 (2013).

[11] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, Qudits and high-dimensional quantum computing, Front. Phys. **8**, 589504 (2020).

[12] L. Amico, R. Fazio, A. Osterloh, and V. Vedral, Entanglement in many-body systems, Rev. Mod. Phys. **80**, 517 (2008).

[13] F. Verstraete, V. Murg, and J. Cirac, Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems, Adv. Phys. **57**, 143 (2008).

[14] J. Eisert, M. Cramer, and M. B. Plenio, Colloquium: Area laws for the entanglement entropy, Rev. Mod. Phys. **82**, 277 (2010).

[15] O. Gühne and G. Tóth, Entanglement detection, Phys. Rep. **474**, 1 (2009).

[16] N. Friis, G. Vitagliano, M. Malik, and M. Huber, Entanglement certification from theory to experiment, Nat. Rev. Phys. **1**, 72 (2019).

[17] Y. Guo, X.-M. Hu, B.-H. Liu, Y.-F. Huang, C.-F. Li, and G.-C. Guo, Experimental witness of genuine high-dimensional entanglement, Phys. Rev. A **97**, 062309 (2018).

[18] J. Bavaresco, N. Herrera Valencia, C. Klöckl, M. Pivoluska, P. Erker, N. Friis, M. Malik, and M. Huber, Measurements in two bases are sufficient for certifying high-dimensional entanglement, Nat. Phys. **14**, 1032 (2018).

[19] Y. Chen, S. Ecker, J. Bavaresco, T. Scheidl, L. Chen, F. Steinlechner, M. Huber, and R. Ursin, Verification of high-dimensional entanglement generated in quantum interference, Phys. Rev. A **101**, 032302 (2020).

[20] N. Herrera Valencia, V. Srivastav, M. Pivoluska, M. Huber, N. Friis, W. McCutcheon, and M. Malik, High-dimensional pixel entanglement: Efficient generation and certification, Quantum **4**, 376 (2020).

[21] N. Euler and M. Gärttner, Detecting high-dimensional entanglement in cold-atom quantum simulators, PRX Quantum **4**, 040338 (2023).

[22] N. K. H. Li, M. Huber, and N. Friis, High-dimensional entanglement witnessed by correlations in arbitrary bases, npj Quantum Inf. **11**, 50 (2025).

[23] Z. Huang, L. Maccone, A. Karim, C. Macchiavello, R. J. Chapman, and A. Peruzzo, High-dimensional entanglement certification, Sci. Rep. **6**, 27637 (2016).

[24] P. Erker, M. Krenn, and M. Huber, Quantifying high dimensional entanglement with two mutually unbiased bases, Quantum **1**, 22 (2017).

[25] Y. Guo, B.-C. Yu, X.-M. Hu, B.-H. Liu, Y.-C. Wu, Y.-F. Huang, C.-F. Li, and G.-C. Guo, Measurement-device-independent quantification of irreducible high-dimensional entanglement, npj Quantum Inf. **6**, 52 (2020).

[26] N. Wyderka and A. Ketterer, Probing the geometry of correlation matrices with randomized measurements, PRX Quantum **4**, 020325 (2023).

[27] S. Liu, Q. He, M. Huber, O. Gühne, and G. Vitagliano, Characterizing entanglement dimensionality from randomized measurements, PRX Quantum **4**, 020324 (2023).

[28] O. Lib, S. Liu, R. Shekel, Q. He, M. Huber, Y. Bromberg, and G. Vitagliano, Experimental certification of high-dimensional entanglement with randomized measurements, Phys. Rev. Lett. **134**, 210202 (2025).

[29] J. Schneeloch and G. A. Howland, Quantifying high-dimensional entanglement with Einstein-Podolsky-Rosen correlations, Phys. Rev. A **97**, 042338 (2018).

[30] M. Dąbrowski, M. Mazelanik, M. Parniak, A. Leszczyński, M. Lipka, and W. Wasilewski, Certification of high-dimensional entanglement and Einstein-Podolsky-Rosen steering with cold atomic quantum memory, Phys. Rev. A **98**, 042126 (2018).

[31] A. Sanpera, D. Bruß, and M. Lewenstein, Schmidt-number witnesses and bound entanglement, Phys. Rev. A **63**, 050301 (2001).

[32] B. Mallick, A. G. Maity, N. Ganguly, and A. S. Majumdar, Higher-dimensional-entanglement detection and quantum-channel characterization using moments of generalized positive maps, Phys. Rev. A **112**, 012416 (2025).

[33] C. Yi, X. Li, and H. Zhu, Certifying entanglement dimensionality by reduction moments (2025), arXiv:2501.15360 [quant-ph].

[34] X.-M. Hu, W.-B. Xing, Y. Guo, M. Weilenmann, E. A. Aguilar, X. Gao, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, Z. Wang, and M. Navascués, Optimized detection of high-dimensional entanglement, Phys. Rev. Lett. **127**, 220501 (2021).

[35] 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).

[36] S. Pallister, N. Linden, and A. Montanaro, Optimal verification of entangled states with local measurements, Phys. Rev. Lett. **120**, 170502 (2018).

[37] H. Zhu and M. Hayashi, Efficient verification of pure quantum states in the adversarial scenario, Phys. Rev. Lett. **123**, 260504 (2019).

[38] H. Zhu and M. Hayashi, General framework for verifying pure quantum states in the adversarial scenario, Phys. Rev. A **100**, 062335 (2019).

[39] J. Morris, V. Saggio, A. Gočanin, and B. Dakić, Quantum verification and estimation with few copies, Adv. Quantum Technol. **5**, 2100118 (2022).

[40] X.-D. Yu, J. Shang, and O. Gühne, Statistical methods for quantum state verification and fidelity estimation, Adv. Quantum Technol. **5**, 2100126 (2022).

[41] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40**, 4277 (1989).

[42] Z. G. Li, M. J. Zhao, S. M. Fei, H. Fan, and W. M. Liu, Mixed maximally entangled states, Quantum Info. Comput. **12**, 63–73 (2012).

[43] H. Zhu, Zero uncertainty states in the presence of quantum memory, npj Quantum Inf. **7**, 47 (2021).

[44] A. Peres and L. E. Ballentine, Quantum theory: Concepts and methods, Am. J. Phys. **63**, 285 (1995).

[45] G. Vidal, Entanglement of pure states for a single copy, Phys. Rev. Lett. **83**, 1046 (1999).

[46] M. Horodecki and P. Horodecki, Reduction criterion of separability and limits for a class of distillation protocols, Phys. Rev. A **59**, 4206 (1999).

[47] T.-C. Wei and P. M. Goldbart, Geometric measure of entanglement and applications to bipartite and multipartite quantum states, Phys. Rev. A **68**, 042307 (2003).

[48] R. Bhatia, *Matrix Analysis* (Springer, 1996).

[49] M. A. Nielsen, Conditions for a class of entanglement transformations, Phys. Rev. Lett. **83**, 436 (1999).

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

[51] H. Zhu and M. Hayashi, Optimal verification and fidelity estimation of maximally entangled states, Phys. Rev. A **99**, 052346 (2019).

[52] Z. Li, Y.-G. Han, and H. Zhu, Efficient verification of bipartite pure states, Phys. Rev. A **100**, 032316 (2019).

[53] X.-D. Yu, J. Shang, and O. Gühne, Optimal verification of general bipartite pure states, npj Quantum Inf. **5**, 112 (2019).

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

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

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

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

[58] 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).

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

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

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

[62] A. Peres, Separability criterion for density matrices, Phys. Rev. Lett. **77**, 1413 (1996).

[63] M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: Necessary and sufficient conditions, Phys. Lett. A **223**, 1 (1996).

[64] K. Wang and M. Hayashi, Optimal verification of two-qubit pure states, Phys. Rev. A **100**, 032315 (2019).

[65] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, 1985).

[66] M. Ledoux, *The Concentration of Measure Phenomenon* (American Mathematical Society, 2001).

[67] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

[68] Z.-W. Liu, S. Lloyd, E. Zhu, and H. Zhu, Entanglement, quantum randomness, and complexity beyond scrambling, JHEP **2018** (7), 41.

CONTENTS

In this appendix, we prove the results presented in the main text, including Propositions 1-4, 6-9, 15 and 19, Theorems 2-5, and Lemmas 1-3. Following the notation in the main text, $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ denotes a bipartite Hilbert space with local dimensions $d = d_A, d_B$ $(d_A \leq d_B)$ and total dimension $D = d_A d_B = d d_B$. In addition, $|\Phi\rangle$ and $|\Psi_\theta\rangle$ denote the maximally entangled state defined in Eq. (3) and the two-qubit pure state defined in Eq. (72), respectively, while $|\Psi\rangle$ denotes a general bipartite pure state.

Appendix A: Proofs of Propositions 1-4

Proof of Proposition 1. First, suppose $\sigma = |\Psi\rangle\langle\Psi|$ is a pure state with Schmidt spectrum $\{s_j\}_{j=0}^{d-1}$, which is arranged in nonincreasing order, that is, $s_0 \geq s_1 \geq \cdots \geq s_{d-1}$. Then $\mathcal{E}_r(\sigma) = \mathcal{E}_r(\Psi) = \sum_{j=r}^{d-1} s_j$ satisfies the inequalities in Eq. (8), that is, $0 \leq \mathcal{E}_r(\sigma) \leq (d-r)/d$. The lower bound is saturated iff $s_r = s_{r+1} = \cdots = s_{d-1} = 0$, that is, $\mathrm{SN}(\sigma) \leq r$; the upper bound is saturated iff $s_0 = s_1 = \cdots = s_{d-1} = 1/d$, in which case $|\Psi\rangle$ is maximally entangled.

Next, we turn to a general density operator σ in $\mathcal{D}(\mathcal{H}_{AB})$. Now, Eq. (8) still holds because $\mathcal{E}_r$ is defined via the convex-roof construction. If $\mathrm{SN}(\sigma) \leq r$, then σ can be expressed as a convex sum of states in $\mathcal{S}_r$, which means $\mathcal{E}_r(\sigma) = 0$. Conversely, if $\mathcal{E}_r(\sigma) = 0$, then σ can be expressed as a convex sum of states in $\mathcal{S}_r$, which means $\mathrm{SN}(\sigma) \leq r$. If σ is maximally entangled, then every pure state $|\Upsilon\rangle$ in its support is maximally entangled, that is, $\mathcal{E}_r(\Upsilon) = (d-r)/d$. Therefore, $\mathcal{E}_r(\sigma) = (d-r)/d$ and the upper bound in Eq. (8) is saturated. Conversely, if $\mathcal{E}_r(\sigma) = (d-r)/d$, then every pure state $|\Upsilon\rangle$ in the support of σ satisfies $\mathcal{E}_r(\Upsilon) = (d-r)/d$ and is thus maximally entangled. Therefore, σ is also maximally entangled. □

Proof of Proposition 2. Expand $|\Psi\rangle$ and $|\Upsilon\rangle$ in the computational basis:

$$|\Psi\rangle = \sum_{j=0}^{d-1}\sum_{k=0}^{d_B-1} A_{jk}|jk\rangle, \quad |\Upsilon\rangle = \sum_{j=0}^{d-1}\sum_{k=0}^{d_B-1} B_{jk}|jk\rangle, \tag{A1}$$

where A and B are the coefficient matrices. Then $\{s_j\}_{j=0}^{d-1}$ and $\{t_j\}_{j=0}^{d-1}$ are the singular value spectra of A and B, respectively. In addition, by virtue of von Neumann's trace theorem in matrix analysis [65] we can deduce that

$$|\langle\Psi|\Upsilon\rangle| = \left|\mathrm{tr}\bigl(A^\dagger B\bigr)\right| \leq \sum_{j=0}^{d-1}\sqrt{s_j t_j}, \tag{A2}$$

which confirms the inequality in Eq. (9). In addition, this inequality is indeed saturated when $|\Psi\rangle = \sum_{j=0}^{d-1}\sqrt{s_j}\,|jj\rangle$ and $|\Upsilon\rangle = \sum_{j=0}^{d-1}\sqrt{t_j}\,|jj\rangle$, which completes the proof of Proposition 2. □

Proof of Proposition 3. The first equality in Eq. (11) holds because $\mathcal{S}_r$ is the convex hull of $\tilde{\mathcal{S}}_r$. By virtue of Proposition 2 the second equality in Eq. (11) can be proved as follows:

$$F\bigl(\Psi, \tilde{\mathcal{S}}_r\bigr) = \max_{\Upsilon\in\tilde{\mathcal{S}}_r} |\langle\Psi|\Upsilon\rangle|^2 = \max_{t_j\geq 0,\, \sum_{j=0}^{r-1} t_j = 1}\left(\sum_{j=0}^{r-1}\sqrt{s_j t_j}\right)^2 = \sum_{j=0}^{r-1} s_j = 1 - \mathcal{E}_r(\Psi). \tag{A3}$$

Next, we turn to Eq. (12). If $E \geq E' = \mathcal{E}_r(\Psi) = \sum_{j=r}^{d-1} s_j$, then $\Psi \in \tilde{\mathcal{S}}_{\mathcal{E}_r}(E)$ and $F(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E)) = 1$. If instead $0 \leq E < E'$, then

$$F\bigl(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E)\bigr) = \max_{\Upsilon\in\tilde{\mathcal{S}}_{\mathcal{E}_r}(E)} |\langle\Psi|\Upsilon\rangle|^2 = \max_{t_j\geq 0,\, \sum_{j=r}^{d-1} t_j \leq E}\left(\sum_{j=0}^{d-1}\sqrt{s_j t_j}\right)^2 = \left[\sqrt{E'E} + \sqrt{(1-E')(1-E)}\right]^2. \tag{A4}$$

In both cases, the second equality in Eq. (12) holds. Now it is straightforward to verify that $F(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E))$ is nondecreasing and concave in E. Note that the monotonicity of $F(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E))$ also holds by definition.

To prove the first equality in Eq. (12), suppose $F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) = \langle\Psi|\sigma|\Psi\rangle$ with $\sigma \in \mathcal{S}_{\mathcal{E}_r}(E)$, which means $\mathcal{E}_r(\sigma) \leq E$. Let $\sigma = \sum_l p_l|\Psi_l\rangle\langle\Psi_l|$ be an optimal decomposition of σ into pure states such that $\mathcal{E}_r(\sigma) = \sum_l p_l\mathcal{E}_r(\Psi_l)$. Then

$$F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) = \langle\Psi|\sigma|\Psi\rangle = \sum_l p_l|\langle\Psi|\Psi_l\rangle|^2 \leq \sum_l p_l F\bigl(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(\mathcal{E}_r(\Psi_l))\bigr) \leq F\bigl(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(\mathcal{E}_r(\sigma))\bigr) \leq F\bigl(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E)\bigr), \tag{A5}$$

where the first inequality holds because $\Psi_l \in \tilde{\mathcal{S}}_{\mathcal{E}_r}(\mathcal{E}_r(\Psi_l))$ by definition, while the second and third inequalities hold because $F(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E))$ is concave and nondecreasing in E as proved above. Therefore, $F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) = F(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E))$, which confirms the first equality in Eq. (12), given that $F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) \geq F(\Psi, \tilde{\mathcal{S}}_{\mathcal{E}_r}(E))$ by definition. Consequently, $F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E))$ is also nondecreasing and concave in E, which completes the proof of Proposition 3. □

Proof of Proposition 4. Let $E=\mathcal{E}_r(\Psi)$, $E'=\mathcal{E}_r(\Upsilon)$, $a=\arcsin\sqrt{E}$, and $b=\arcsin\sqrt{E'}$; then $0\leq E,E'\leq (d-r)/d$ and $0\leq \sin(a+b)\leq 1$. If in addition $r>d/2$, then $\sin(a+b)\leq 2\sqrt{r(d-r)}/d$. Therefore, $0\leq\sin(a+b)\leq \ell(r,d)$ for $r\in[d-1]$.

On the other hand, we have

$$\begin{aligned}|E-E'|&=|\mathcal{E}_r(\Psi)-\mathcal{E}_r(\Upsilon)|=\left|\sin^2 a-\sin^2 b\right|=\left|\sin^2 a\cos^2 b-\sin^2 b\cos^2 a\right|=|\sin(a+b)\sin(a-b)|\\&=\left|2\sin(a+b)\sin\left(\frac{a-b}{2}\right)\cos\left(\frac{a-b}{2}\right)\right|\leq\left|2\sin(a+b)\sin\left(\frac{a-b}{2}\right)\right|\leq 2\ell(r,d)\left|\sin\left(\frac{a-b}{2}\right)\right|.\end{aligned}\tag{A6}$$

Furthermore, by virtue of Proposition 3 we can deduce that

$$|\langle\Psi|\Upsilon\rangle|\leq\sqrt{E'E}+\sqrt{(1-E')(1-E)}=\sin a\sin b+\cos a\cos b=\cos(a-b),\tag{A7}$$

$$\sqrt{2-2|\langle\Psi|\Upsilon\rangle|}\geq\sqrt{2-2\cos(a-b)}=2\left|\sin\left(\frac{a-b}{2}\right)\right|.\tag{A8}$$

The above equations together imply that

$$|\mathcal{E}_r(\Psi)-\mathcal{E}_r(\Upsilon)|\leq\ell(r,d)\sqrt{2-2|\langle\Psi|\Upsilon\rangle|}\leq\ell(r,d)\||\Psi\rangle-|\Upsilon\rangle\|_2,\tag{A9}$$

which confirms Eq. (13) and completes the proof of Proposition 4. Here the last inequality follows from the equation below:

$$\||\Psi\rangle-|\Upsilon\rangle\|_2^2=2-\langle\Psi|\Upsilon\rangle-\langle\Upsilon|\Psi\rangle\geq 2-2|\langle\Psi|\Upsilon\rangle|.\tag{A10}$$

□

Appendix B: Proofs of Propositions 6-9

Proposition 6 is a simple corollary of the following lemma.

Lemma 4. *Suppose $\mathcal{H}_{AB}=\mathcal{H}_A\otimes\mathcal{H}_B$ and $\mathcal{H}'_{AB}=\mathcal{H}'_A\otimes\mathcal{H}'_B$ are two bipartite Hilbert spaces and the two states $|\Psi\rangle\in\mathcal{H}_{AB}$ and $|\Psi'\rangle\in\mathcal{H}'_{AB}$ have the same nonzero Schmidt coefficients (including the multiplicities). Then*

$$\nu_{\rm LC}(\Psi)=\nu_{\rm LC}(\Psi'),\quad \nu_{\rm sep}(\Psi)=\nu_{\rm sep}(\Psi'),\tag{B1}$$

$$\nu_{\rm LC}^{\rm H}(\Psi)=\nu_{\rm LC}^{\rm H}(\Psi'),\quad \nu_{\rm sep}^{\rm H}(\Psi)=\nu_{\rm sep}^{\rm H}(\Psi').\tag{B2}$$

Proof of Lemma 4. Without loss of generality we can assume that $\mathcal{H}_A\leq\mathcal{H}'_A$ and $\mathcal{H}_B\leq\mathcal{H}'_B$. If $\mathcal{H}_A=\mathcal{H}'_A$ and $\mathcal{H}_B=\mathcal{H}'_B$, then $|\Psi\rangle$ and $|\Psi'\rangle$ are equivalent under a local unitary transformation, and there is a one-to-one correspondence between local (separable) verification operators of $|\Psi\rangle$ and the counterparts of $|\Psi'\rangle$ under the same local unitary transformation. The same conclusion holds if we restrict to homogeneous verification operators. So Eqs. (B1) and (B2) hold as expected.

In general, by applying a suitable local unitary transformation if necessary, we can assume that $|\Psi'\rangle$ is supported in $\mathcal{H}_{AB}$ and is identical to $|\Psi\rangle$ when regarded as a pure state in $\mathcal{H}_{AB}$. Then any local verification operator of $|\Psi\rangle$ is also a local verification operator of $|\Psi'\rangle$, which implies that $\nu_{\rm LC}(\Psi)\leq\nu_{\rm LC}(\Psi')$. To prove the opposite inequality, let Q_A (Q_B) be the projector onto $\mathcal{H}_A$ ($\mathcal{H}_B$) as a subspace of $\mathcal{H}'_A$ ($\mathcal{H}'_B$) and let $Q=Q_A\otimes Q_B$. If Ω' is a local verification operator of $|\Psi'\rangle$, then $\Omega=Q\Omega'Q$ is a local verification operator of $|\Psi\rangle$ with $\nu(\Omega)\geq\nu(\Omega')$. Therefore, we have $\nu_{\rm LC}(\Psi)\geq\nu_{\rm LC}(\Psi')$, which implies the first equality in Eq. (B1) given the opposite inequality proved above.

Next, we turn to Eq. (B2). If Ω' is a local homogeneous verification operator of $|\Psi'\rangle$, then $\Omega=Q\Omega'Q$ is a local homogeneous verification operator of $|\Psi\rangle$ with $\nu(\Omega)\geq\nu(\Omega')$, which implies that $\nu_{\rm LC}^{\rm H}(\Psi)\geq\nu_{\rm LC}^{\rm H}(\Psi')$. Conversely, if Ω is a local homogeneous verification operator of $|\Psi\rangle$, then $\Omega'=\Omega+\beta(\Omega)(\mathbb{1}'-Q)$ is a local homogeneous verification operator of $|\Psi'\rangle$ with $\nu(\Omega')=\nu(\Omega)$. Therefore, $\nu_{\rm LC}^{\rm H}(\Psi)\leq\nu_{\rm LC}^{\rm H}(\Psi')$, which implies the first equality in Eq. (B2) given the opposite inequality proved above.

The above reasoning still applies when local operations are replaced by separable operations, so the second inequalities in Eqs. (B1) and (B2) also hold, which completes the proof of Lemma 4. □

Proof of Proposition 7. By construction it is clear that $\Omega_{\rm sep}$ is a verification operator of $|\Psi\rangle$, while $\Omega_{\rm sep}^{\rm H}$ and $\Omega_{\rm LC}^{\rm H}$ are homogeneous verification operators of $|\Psi\rangle$. According to the proofs of Lemma 1 and Theorem 2 of Ref. [50] (see also

Ref. [54]), the two operators $\Omega_{\rm sep}$ and $\mathbb{1}-\Omega_{\rm sep}$ are separable. Therefore, $\Omega_{\rm sep}$ is a separable verification operator of $|\Psi\rangle$. In addition, we have

$$(1+\sqrt{s_0s_1})\Omega_{\rm sep}^{\rm H}=\Omega_{\rm sep}+\sqrt{s_0s_1}\sum_{j=0}^{d-1}|jj\rangle\langle jj|+\sum_{j,k=0,\, j\neq k}^{d-1}(\sqrt{s_0s_1}-\sqrt{s_js_k})|jk\rangle\langle jk|+\sqrt{s_0s_1}\sum_{j=0}^{d-1}\sum_{k=d}^{d_B-1}|jk\rangle\langle jk|, \tag{B3}$$

$$(1+\sqrt{s_0s_1})\big(\mathbb{1}-\Omega_{\rm sep}^{\rm H}\big)=\mathbb{1}-|\Psi\rangle\langle\Psi|=\mathbb{1}-\Omega_{\rm sep}+\sum_{j,k=0,\, j\neq k}^{d-1}\sqrt{s_js_k}\,|jk\rangle\langle jk|, \tag{B4}$$

which imply that $\Omega_{\rm sep}^{\rm H}$ and $\mathbb{1}-\Omega_{\rm sep}^{\rm H}$ are separable given that $\Omega_{\rm sep}$ and $\mathbb{1}-\Omega_{\rm sep}$ are separable. Therefore, $\Omega_{\rm sep}^{\rm H}$ is a separable homogeneous verification operator of $|\Psi\rangle$.

Next, according to Refs. [52], the verification operator $\Omega_{\rm LC}^{\rm H}$ can be realized by LOCC. So $\Omega_{\rm LC}^{\rm H}$ is a local homogeneous verification operator of $|\Psi\rangle$.

Equations (24)-(26) follow from the definitions of the verification operators $\Omega_{\rm sep}$, $\Omega_{\rm sep}^{\rm H}$, and $\Omega_{\rm LC}^{\rm H}$ in Eqs. (21)-(23), which completes the proof of Proposition 7. □

Proof of Proposition 8. Thanks to Proposition 6, we can assume that $r=d=d_A=d_B$ without loss of generality.

According to Lemma 2 of Ref. [51], any separable verification operator Ω of $|\Psi\rangle$ satisfies

$$\beta(\Omega)\geq\frac{\mathcal{E}_R(\Psi)}{d_Ad_B-1}=\frac{\big(\sum_j\sqrt{s_j}\big)^2-1}{r^2-1}, \tag{B5}$$

which implies the first inequality in Eq. (27). Here $\mathcal{E}_R(\Psi)=(\sum_j\sqrt{s_j})^2-1$ is the robustness of entanglement [54]. If in addition Ω is homogeneous, then

$$\beta(\Omega)\geq\frac{R(\Psi)}{d_Ad_B+R(\Psi)}=\frac{\sqrt{s_0s_1}}{1+\sqrt{s_0s_1}}, \tag{B6}$$

where $R(\Psi)=d_Ad_B\sqrt{s_0s_1}$ is the random robustness [54]. The above inequality is saturated when $\Omega=\Omega_{\rm sep}^{\rm H}$ thanks to Proposition 7. Therefore, $\beta_{\rm sep}^{\rm H}=\sqrt{s_0s_1}/(1+\sqrt{s_0s_1})$, which confirms the first equality in Eq. (28). The third inequality in Eq. (27) and the second inequality in Eq. (28) also follow from Proposition 7. The inequalities $\beta_{\rm sep}\leq\beta_{\rm LC}$ and $\beta_{\rm sep}^{\rm H}\leq\beta_{\rm LC}^{\rm H}$ in Eqs. (27) and (28) hold by definition. The inequality $(s_0+s_1)/(2+s_0+s_1)\leq 1/3$ holds because $2/d\leq s_0+s_1\leq 1$. This observation completes the proof of Proposition 8. □

Proof of Proposition 9. By assumption $|\Psi\rangle$ is maximally entangled, which means $\mathrm{SR}(\Psi)=d=d_A$, $s_j=1/d$ for $j=0,1,\ldots,d-1$. So the first three inequalities in Eq. (27) and the first two inequalities in Eq. (28) are saturated, which implies Eq. (33). In addition, the verification operator $\Omega_{\rm opt}$ defined in Eq. (34) is separable and local. If $\Omega=\Omega_{\rm opt}$, then it is obvious that $\beta(\Omega)=1/(d+1)$.

Next, suppose $d=d_A=d_B$ and Ω is a separable verification operator of $|\Psi\rangle$ with $\beta(\Omega)=1/(d+1)$. To prove Eq. (34) we can assume that $|\Psi\rangle=|\Phi\rangle$ without loss of generality. Then $\mathcal{H}_A$ and $\mathcal{H}_B$ are isomorphic and $|\Psi\rangle$ is invariant under local unitary transformations of the form $U\otimes U^*$ for $U\in\mathrm{U}(d)$, where U^* denotes the complex conjugation of U with respect to the Schmidt basis. Let

$$\Omega^{\rm H}=\int(U\otimes U^*)\Omega(U\otimes U^*)^\dagger dU, \tag{B7}$$

where the integration is taken over the normalized Haar measure on $\mathrm{U}(d)$. Then $\Omega^{\rm H}$ is a separable homogeneous verification operator of $|\Psi\rangle$. In addition, we have

$$\mathrm{tr}\big(\Omega^{\rm H}\big)=\mathrm{tr}(\Omega),\quad \frac{1}{d+1}\leq\beta\big(\Omega^{\rm H}\big)\leq\beta(\Omega)=\frac{1}{d+1}, \tag{B8}$$

which implies that $\beta\big(\Omega^{\rm H}\big)=\beta(\Omega)=1/(d+1)$. Therefore, Ω is necessarily homogeneous and we have

$$\Omega=\Omega^{\rm H}=|\Psi\rangle\langle\Psi|+\frac{1}{d+1}(\mathbb{1}-|\Psi\rangle\langle\Psi|), \tag{B9}$$

which confirms Eq. (34) and completes the proof of Proposition 9. □

Appendix C: Proof of Proposition 15

Proposition 15 is a simple corollary of Lemma 5 below.

Lemma 5. *Suppose $\mathcal{H}_{AB}=\mathcal{H}_A\otimes\mathcal{H}_B$ and $\mathcal{H}'_{AB}=\mathcal{H}'_A\otimes\mathcal{H}'_B$ are two bipartite Hilbert spaces and the two states $|\Psi\rangle\in\mathcal{H}_{AB}$ and $|\Psi'\rangle\in\mathcal{H}'_{AB}$ have the same nonzero Schmidt coefficients (including multiplicities). Suppose $r\in[d-1]$, $0\leq E<\mathcal{E}_r(\Psi)$, $\mathcal{S}$ is one of the sets $\mathcal{S}_r$ or $\mathcal{S}_{\mathcal{E}_r}(E)$, and $\mathcal{S}'$ is the counterpart with $\mathcal{H}_{AB}$ replaced by $\mathcal{H}'_{AB}$. Then*

$$P_{\rm LC}(\Psi,\mathcal{S})=P_{\rm LC}(\Psi',\mathcal{S}'),\quad P_{\rm sep}(\Psi,\mathcal{S})=P_{\rm sep}(\Psi',\mathcal{S}'), \tag{C1}$$

$$P^{\rm H}_{\rm LC}(\Psi,\mathcal{S})=P^{\rm H}_{\rm LC}(\Psi',\mathcal{S}'),\quad P^{\rm H}_{\rm sep}(\Psi,\mathcal{S})=P^{\rm H}_{\rm sep}(\Psi',\mathcal{S}'). \tag{C2}$$

Proof of Lemma 5. As in the proof of Lemma 4 we can assume that $\mathcal{H}_A\leq\mathcal{H}'_A$ and $\mathcal{H}_B\leq\mathcal{H}'_B$, then $\mathcal{S}\subseteq\mathcal{S}'$. If $\mathcal{H}_A=\mathcal{H}'_A$ and $\mathcal{H}_B=\mathcal{H}'_B$, then $|\Psi\rangle$ and $|\Psi'\rangle$ are equivalent under local unitary transformations, so Eqs. (C1) and (C2) hold as expected.

In general, by applying a suitable local unitary transformation if necessary, we can assume that $|\Psi'\rangle$ is supported in $\mathcal{H}_{AB}$ and is identical to $|\Psi\rangle$ when regarded as a pure state in $\mathcal{H}_{AB}$. Then any local verification operator Ω of $|\Psi\rangle$ is also a local verification operator of $|\Psi'\rangle$ (via the natural embedding). In addition, we have $P_\Omega(\Psi,\mathcal{S})=P_\Omega(\Psi',\mathcal{S}')$ by Lemma 7 below, which implies that $P_{\rm LC}(\Psi,\mathcal{S})\geq P_{\rm LC}(\Psi',\mathcal{S}')$.

To prove the opposite inequality, let Q_A (Q_B) be the projector onto $\mathcal{H}_A$ ($\mathcal{H}_B$) as a subspace of $\mathcal{H}'_A$ ($\mathcal{H}'_B$) and let $Q=Q_A\otimes Q_B$. If Ω' is a local verification operator of $|\Psi'\rangle$, then $Q\Omega'Q$ can be regarded as a local verification operator of $|\Psi\rangle$. In addition, we have

$$P_{Q\Omega'Q}(\Psi,\mathcal{S})=\max_{\sigma\in\mathcal{S}}\operatorname{tr}(Q\Omega'Q\sigma)=\max_{\sigma\in\mathcal{S}}\operatorname{tr}(\Omega'\sigma)\leq\max_{\sigma\in\mathcal{S}'}\operatorname{tr}(\Omega'\sigma)=P_{\Omega'}(\Psi',\mathcal{S}'), \tag{C3}$$

which implies that $P_{\rm LC}(\Psi,\mathcal{S})\leq P_{\rm LC}(\Psi',\mathcal{S}')$. In conjunction with the opposite inequality proved above, we can deduce that $P_{\rm LC}(\Psi,\mathcal{S})=P_{\rm LC}(\Psi',\mathcal{S}')$, which confirms the first equality in Eq. (C1). The second equality in Eq. (C1) follows from a similar reasoning.

Equation (C2) follows from Propositions 3, 11 and Lemma 4, which completes the proof of Lemma 5. □

In the rest of this appendix, we prove two auxiliary lemmas employed in the proof of Lemma 5.

Lemma 6. *Suppose $|\Psi\rangle\in\mathcal{H}_{AB}$, $r\in[d-1]$, $0\leq E<\mathcal{E}_r(\Psi)$, and Ω is a verification operator of $|\Psi\rangle$. Then $P_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))$ and $P(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))$ are nondecreasing and concave in E.*

Proof of Lemma 6. The monotonicity of $P_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))$ and $P(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))$ is evident by definition. To prove their concavity, it suffices to prove the following inequalities:

$$P_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))\geq qP_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_1))+(1-q)P_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_2)), \tag{C4}$$

$$P(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))\geq qP(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_1))+(1-q)P(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_2)), \tag{C5}$$

assuming that $0\leq E_1,E_2<\mathcal{E}_r(\Psi)$, $0\leq q\leq 1$, and $qE_1+(1-q)E_2=E$. Suppose $P_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_j))=\operatorname{tr}(\Omega\rho_j)$ with $\rho_j\in\mathcal{S}_{\mathcal{E}_r}(E_j)$ for $j=1,2$. Then we have

$$qP_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_1))+(1-q)P_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_2))=q\operatorname{tr}(\Omega\rho_1)+(1-q)\operatorname{tr}(\Omega\rho_2)=\operatorname{tr}\{\Omega[q\rho_1+(1-q)\rho_2]\}\leq P_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E)), \tag{C6}$$

where the inequality holds because $q\rho_1+(1-q)\rho_2\in\mathcal{S}_{\mathcal{E}_r}(E)$ by the definition of the entanglement measure $\mathcal{E}_r(\cdot)$. The above equation confirms Eq. (C4) and the concavity of $P_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))$. Next, suppose Ω' is an optimal strategy for certifying the target state $|\Psi\rangle$ against $\mathcal{S}_{\mathcal{E}_r}(E)$. Then

$$\begin{aligned}P(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))=P_{\Omega'}(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))&\geq qP_{\Omega'}(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_1))+(1-q)P_{\Omega'}(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_2))\\&\geq qP(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_1))+(1-q)P(\Psi,\mathcal{S}_{\mathcal{E}_r}(E_2)),\end{aligned} \tag{C7}$$

where the first inequality follows from the concavity of $P_{\Omega'}(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))$ as proved above, and the second inequality holds by definition. This observation confirms Eq. (C5) and the concavity of $P(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))$ and completes the proof of Lemma 6. □

Lemma 7. *Suppose $\mathcal{H}_{AB}=\mathcal{H}_A\otimes\mathcal{H}_B$ and $\mathcal{H}'_{AB}=\mathcal{H}'_A\otimes\mathcal{H}'_B$ are two bipartite Hilbert spaces with $\mathcal{H}_A\leq\mathcal{H}'_A$ and $\mathcal{H}_B\leq\mathcal{H}'_B$, Ω is a verification operator of $|\Psi\rangle\in\mathcal{H}_{AB}$, $\mathcal{S}$ is one of the sets $\mathcal{S}_r$ or $\mathcal{S}_{\mathcal{E}_r}(E)$ with $r\in[d-1]$ and $0\leq E<\mathcal{E}_r(\Psi)$, and $\mathcal{S}'$ is the counterpart with $\mathcal{H}_{AB}$ replaced by $\mathcal{H}'_{AB}$. Then*

$$P_\Omega(\Psi,\mathcal{S})=P_\Omega(\Psi,\mathcal{S}'). \tag{C8}$$

Proof of Lemma 7. Let $P_\Omega = P_\Omega(\Psi, \mathcal{S})$ and $P'_\Omega = P_\Omega(\Psi, \mathcal{S}')$; then $P'_\Omega \geq P_\Omega \geq 0$ given that $\mathcal{S} \subseteq \mathcal{S}'$. If $P'_\Omega = 0$, then $P_\Omega = P'_\Omega = 0$. Otherwise, let Q_A (Q_B) be the projector onto $\mathcal{H}_A$ ($\mathcal{H}_B$) as a subspace of $\mathcal{H}'_A$ ($\mathcal{H}'_B$) and let $Q = Q_A \otimes Q_B$. Suppose $P'_\Omega = \operatorname{tr}(\Omega\rho)$ with $\rho \in \mathcal{S}'$. Let $q = \operatorname{tr}(Q\rho Q)$ and $\varrho = Q\rho Q/q$ (note that $0 < q \leq 1$); then

$$P'_\Omega = \operatorname{tr}(\Omega\rho) = q\operatorname{tr}(\Omega\varrho) \leq \operatorname{tr}(\Omega\varrho). \tag{C9}$$

If $\mathcal{S} = \mathcal{S}_r$, then $\rho \in \mathcal{S}'_r$, $\varrho \in \mathcal{S}_r$, and the above equation implies that $P'_\Omega \leq P_\Omega$, which confirms Eq. (C8) given that the opposite inequality holds by definition.

Next, suppose $\mathcal{S} = \mathcal{S}_{\mathcal{E}_r}(E)$. Then $\rho \in \mathcal{S}'_{\mathcal{E}_r}(E)$ and $q\mathcal{E}_r(\varrho) \leq \mathcal{E}_r(\rho) \leq E$. In addition, we have

$$\begin{aligned} P'_\Omega &= q\operatorname{tr}(\Omega\varrho) \leq qP_\Omega(\Psi, \mathcal{S}_{\mathcal{E}_r}(\mathcal{E}_r(\varrho))) \leq (1-q)P_\Omega(\Psi, \mathcal{S}_{\mathcal{E}_r}(0)) + qP_\Omega(\Psi, \mathcal{S}_{\mathcal{E}_r}(\mathcal{E}_r(\varrho))) \\ &\leq P_\Omega(\Psi, \mathcal{S}_{\mathcal{E}_r}(q\mathcal{E}_r(\varrho))) \leq P_\Omega(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) = P_\Omega, \end{aligned} \tag{C10}$$

given that $P_\Omega(\Psi, \mathcal{S}_{\mathcal{E}_r}(E))$ is nondecreasing and concave in E by Lemma 6. In conjunction with the opposite inequality $P'_\Omega \geq P_\Omega$ mentioned above, this equation implies Eq. (C8) and completes the proof of Lemma 7. □

Appendix D: Proofs of results on general bipartite pure states

In this appendix we prove Theorems 2-5, which are tied to entanglement certification of general bipartite pure states.

1. Proof of Theorem 2

Proof of Theorem 2. Suppose $|\Upsilon\rangle$ is another quantum state in $\mathcal{H}_{AB}$. According to Proposition 5, $|\Psi\rangle$ is majorized by $|\Upsilon\rangle$ iff there exists a local channel Λ that can transform $|\Psi\rangle$ into $|\Upsilon\rangle$, that is, $\Lambda(|\Psi\rangle\langle\Psi|) = |\Upsilon\rangle\langle\Upsilon|$. Here we assume that both conditions hold in the following analysis.

Let Ω_Υ be an arbitrary verification operator of $|\Upsilon\rangle$; then $0 \leq \Omega_\Upsilon \leq \mathbb{1}$ and $\operatorname{tr}(\Omega_\Upsilon|\Upsilon\rangle\langle\Upsilon|) = 1$. Let $\Omega_\Psi = \Lambda^\dagger(\Omega_\Upsilon)$; then

$$0 \leq \Omega_\Psi \leq \mathbb{1}, \quad \operatorname{tr}(\Omega_\Psi|\Psi\rangle\langle\Psi|) = \operatorname{tr}[\Omega_\Upsilon\Lambda(|\Psi\rangle\langle\Psi|)] = \operatorname{tr}(\Omega_\Upsilon|\Upsilon\rangle\langle\Upsilon|) = 1. \tag{D1}$$

Therefore, Ω_Ψ is a verification operator of $|\Psi\rangle$. If Ω_Υ can be realized by LOCC (separable operations), then Ω_Ψ can also be realized by LOCC (separable operations). Moreover, the separation probability achieved by Ω_Ψ can be bounded from above as follows:

$$P_{\Omega_\Psi}(\Psi, \mathcal{S}) = \max_{\sigma\in\mathcal{S}} \operatorname{tr}(\Omega_\Psi\sigma) = \max_{\sigma\in\mathcal{S}} \operatorname{tr}[\Omega_\Upsilon\Lambda(\sigma)] \leq \max_{\sigma\in\mathcal{S}} \operatorname{tr}(\Omega_\Upsilon\sigma) = P_{\Omega_\Upsilon}(\Upsilon, \mathcal{S}). \tag{D2}$$

Here the inequality holds because $\Lambda(\sigma) \in \mathcal{S}$ whenever $\sigma \in \mathcal{S}$. Therefore,

$$P_{\mathrm{LC}}(\Psi, \mathcal{S}) \leq P_{\mathrm{LC}}(\Upsilon, \mathcal{S}), \quad P_{\mathrm{sep}}(\Psi, \mathcal{S}) \leq P_{\mathrm{sep}}(\Upsilon, \mathcal{S}), \tag{D3}$$

which means $P_{\mathrm{LC}}(\Psi, \mathcal{S})$ and $P_{\mathrm{sep}}(\Psi, \mathcal{S})$ are Schur convex in $|\Psi\rangle$ and do not decrease if $|\Psi\rangle$ is subjected to LOCC.

The equality in Eq. (54) holds because the local homogeneous verification operator Ω_{opt} in Proposition 9 is optimal among separable verification operators; the first inequality holds because the maximally entangled state $|\Phi\rangle$ is majorized by any pure state in $\mathcal{H}_{AB}$, and the second inequality holds by definition. Equation (55) is a simple corollary of Eq. (54) given that $P^{\mathrm{H}}_{\mathrm{LC}}(\Psi, \mathcal{S}) \geq P^{\mathrm{H}}_{\mathrm{sep}}(\Psi, \mathcal{S}) \geq P_{\mathrm{sep}}(\Psi, \mathcal{S})$ by definition. This observation completes the proof of Theorem 2. □

2. Proof of Theorem 3

Proof of Theorem 3. By virtue of Propositions 3 and 11 we can deduce that

$$P_{\mathrm{sep}}(\Psi, \mathcal{S}_r) \geq F(\Psi, \mathcal{S}_r) = 1 - \mathcal{E}_r(\Psi), \quad P_{\mathrm{sep}}(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) \geq F(\Psi, \mathcal{S}_{\mathcal{E}_r}(E)) = f_r(\Psi, E), \tag{D4}$$

which, together with the definitions in Eq. (58), confirm the first inequalities in Eqs. (59) and (61). By virtue of Propositions 3, 8, and 11 we can deduce that

$$P_{\rm sep}^{\rm H}(\Psi,\mathcal{S}_r)=\nu_{\rm sep}^{\rm H}(\Psi)F(\Psi,\mathcal{S}_r)+\beta_{\rm sep}^{\rm H}(\Psi)=\frac{[1-\mathcal{E}_r(\Psi)]+\sqrt{s_0s_1}}{1+\sqrt{s_0s_1}}=1-\frac{\mathcal{E}_r(\Psi)}{1+\sqrt{s_0s_1}}, \tag{D5}$$

$$P_{\rm sep}^{\rm H}(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))=\nu_{\rm sep}^{\rm H}(\Psi)F(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))+\beta_{\rm sep}^{\rm H}(\Psi)=\frac{f_r(\Psi,E)+\sqrt{s_0s_1}}{1+\sqrt{s_0s_1}}, \tag{D6}$$

which confirm the equalities in Eqs. (60) and (62).

The second inequalities in Eqs. (59) and (61) and the first inequalities in Eqs. (60) and (62) hold by definition.

The first upper bounds for $P_{\rm LC}(\Psi,\mathcal{S}_r)$, $P_{\rm LC}^{\rm H}(\Psi,\mathcal{S}_r)$, $P_{\rm LC}(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))$, and $P_{\rm LC}^{\rm H}(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))$ correspond to the separation probabilities achieved by the following local homogeneous verification operator [see Eq. (23)]:

$$\Omega=|\Psi\rangle\langle\Psi|+\frac{s_0+s_1}{2+s_0+s_1}(\mathbb{1}-|\Psi\rangle\langle\Psi|). \tag{D7}$$

In conjunction with Propositions 3 and 10 we can deduce that

$$P_{\rm LC}(\Psi,\mathcal{S}_r)\leq P_{\rm LC}^{\rm H}(\Psi,\mathcal{S}_r)\leq P_\Omega(\Psi,\mathcal{S}_r)=\nu(\Omega)F(\Psi,\mathcal{S}_r)+\beta(\Omega)\leq\frac{2[1-\mathcal{E}_r(\Psi)]+s_0+s_1}{2+s_0+s_1}=1-\frac{2\mathcal{E}_r(\Psi)}{2+s_0+s_1}, \tag{D8}$$

$$P_{\rm LC}(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))\leq P_{\rm LC}^{\rm H}(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))\leq P_\Omega(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))=\nu(\Omega)F(\Psi,\mathcal{S}_{\mathcal{E}_r}(E))+\beta(\Omega)\leq\frac{2f_r(\Psi,E)+s_0+s_1}{2+s_0+s_1}, \tag{D9}$$

which, together with the definitions in Eq. (58), confirm the third inequalities in Eqs. (59) and (61) and the second inequalities in Eqs. (60) and (62).

Finally, by virtue of the inequalities $f_r(\Psi,E)\geq f_r(\Psi,0)=1-\mathcal{E}_r(\Psi)\geq s_0$ we can deduce that

$$1-\frac{2\mathcal{E}_r(\Psi)}{2+s_0+s_1}\leq 1-\frac{\mathcal{E}_r(\Psi)}{1+s_0}=\frac{1-\mathcal{E}_r(\Psi)}{1+s_0}+\frac{s_0}{1+s_0}\leq\frac{2[1-\mathcal{E}_r(\Psi)]}{1+s_0}, \tag{D10}$$

$$1-\frac{2\mathcal{E}_r(\Psi)}{2+s_0+s_1}\leq\frac{3}{2+s_0}\left[1-\frac{\mathcal{E}_r(\Psi)}{1+\sqrt{s_0s_1}}\right]-\frac{1-\mathcal{E}_r(\Psi)-s_0}{2+s_0}\leq\frac{3}{2+s_0}\left[1-\frac{\mathcal{E}_r(\Psi)}{1+\sqrt{s_0s_1}}\right], \tag{D11}$$

$$\frac{2f_r(\Psi,E)+s_0+s_1}{2+s_0+s_1}\leq\frac{f_r(\Psi,E)+s_0}{1+s_0}\leq\frac{2f_r(\Psi,E)}{1+s_0}, \tag{D12}$$

$$\frac{2f_r(\Psi,E)+s_0+s_1}{2+s_0+s_1}\leq\frac{3}{2+s_0}\frac{f_r(\Psi,E)+\sqrt{s_0s_1}}{1+\sqrt{s_0s_1}}-\frac{f_r(\Psi,E)-s_0}{2+s_0}\leq\frac{3}{2+s_0}\frac{f_r(\Psi,E)+\sqrt{s_0s_1}}{1+\sqrt{s_0s_1}}, \tag{D13}$$

which confirm the last inequalities in Eqs. (59)-(62) and complete the proof of Theorem 3. □

3. Auxiliary lemmas

Before proving Theorems 4 and 5, here we need to introduce two auxiliary lemmas.

Denote by S_{n-1} the $(n-1)$-dimensional unit sphere in $\mathbb{R}^n$. A function $f:S_{n-1}\to\mathbb{R}$ is a Lipschitz (continuous) function with Lipschitz constant η if

$$|f(x)-f(y)|\leq\eta\|x-y\|_2\quad\forall\, x,y\in S_{n-1}, \tag{D14}$$

where $\|\cdot\|_2$ denotes the Euclidean norm.

Lemma 8. (Levy's lemma) [66, 67] *Suppose $f:S_{n-1}\to\mathbb{R}$ is a Lipschitz function with Lipschitz constant η, and $x\in S_{n-1}$ is drawn uniformly at random. Then*

$$\Pr\{f(x)-\mathbb{E}f\geq\epsilon\}\leq 2\exp\left(-\frac{n\epsilon^2}{25\pi\eta^2}\right). \tag{D15}$$

Next, define the following function on pure states in $\mathcal{H}_{AB}$:

$$U_r(\Psi):=1-\frac{\mathcal{E}_r(\Psi)}{1+s_0(\Psi)},\quad |\Psi\rangle\in\mathcal{H}_{AB},\quad r\in[d-1], \tag{D16}$$

which can also be regarded as a function defined on a $(2D-1)$-dimensional real unit sphere, where $D = \dim(\mathcal{H}_{AB})$. Here $s_0(\Psi)$ is the largest Schmidt coefficient of $|\Psi\rangle$, recall that the Schmidt coefficients are arranged in nonincreasing order by default. The function $U_r(\Psi)$ is an upper bound for $P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r)$ according to the following equation:

$$P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r) = 1 - \frac{2\mathcal{E}_r(\Psi)}{2 + s_0(\Psi) + s_1(\Psi)} \leq 1 - \frac{\mathcal{E}_r(\Psi)}{1 + s_0(\Psi)} = U_r(\Psi), \tag{D17}$$

where the inequality holds because $s_0(\Psi) \geq s_1(\Psi)$.

Lemma 9. *Suppose $|\Psi\rangle \in \mathcal{H}_{AB}$ and $r \in [d-1]$. Then $U_r(\Psi)$ is a Lipschitz function with Lipschitz constant 2. If $|\Psi\rangle$ is a Haar-random pure state in $\mathcal{H}_{AB}$, then*

$$\mathbb{E}U_r(\Psi) < \frac{4(r+1)}{d+1}. \tag{D18}$$

Proof of Lemma 9. Let $|\Upsilon\rangle \in \mathcal{H}_{AB}$ be another pure state; let $s_0(\Psi)$ and $s_0(\Upsilon)$ be the largest Schmidt coefficients of $|\Psi\rangle$ and $|\Upsilon\rangle$, respectively. Then we have

$$\begin{aligned} U_r(\Upsilon) - U_r(\Psi) &= \frac{\mathcal{E}_r(\Psi)}{1+s_0(\Psi)} - \frac{\mathcal{E}_r(\Upsilon)}{1+s_0(\Upsilon)} = \frac{\mathcal{E}_r(\Psi)}{1+s_0(\Psi)} - \frac{\mathcal{E}_r(\Upsilon)}{1+s_0(\Psi)} + \frac{\mathcal{E}_r(\Upsilon)}{1+s_0(\Psi)} - \frac{\mathcal{E}_r(\Upsilon)}{1+s_0(\Upsilon)} \\ &= \frac{\mathcal{E}_r(\Psi) - \mathcal{E}_r(\Upsilon)}{1+s_0(\Psi)} + \frac{\mathcal{E}_r(\Upsilon)[s_0(\Upsilon) - s_0(\Psi)]}{[1+s_0(\Psi)][1+s_0(\Upsilon)]} \leq \frac{\||\Psi\rangle - |\Upsilon\rangle\|_2}{1+s_0(\Psi)} + \frac{\mathcal{E}_r(\Upsilon)\||\Psi\rangle - |\Upsilon\rangle\|_2}{[1+s_0(\Psi)][1+s_0(\Upsilon)]} \leq 2\||\Psi\rangle - |\Upsilon\rangle\|_2, \end{aligned} \tag{D19}$$

where the inequalities hold because $s_0(\Psi) = 1 - \mathcal{E}_1(\Psi)$, $0 \leq \mathcal{E}_r(\Psi) \leq 1$, and $\mathcal{E}_r(\Psi)$ is a Lipschitz function with Lipschitz constant 1 by Propositions 1 and 4. By symmetry the above equation still holds if $|\Psi\rangle$ and $|\Upsilon\rangle$ are exchanged. Therefore, $U_r(\Psi)$ is a Lipschitz function with Lipschitz constant 2.

Next, we turn to Eq. (D18), assuming that $|\Psi\rangle$ is a Haar-random pure state in $\mathcal{H}_{AB}$. Let $\{s_j = s_j(\Psi)\}_{j=0}^{d-1}$ denote the Schmidt spectrum of $|\Psi\rangle$. By definition we have

$$U_r(\Psi) = 1 - \frac{\mathcal{E}_r(\Psi)}{1+s_0} = 1 - \frac{\sum_{j=r}^{d-1} s_j}{1+s_0} = \frac{\sum_{j=0}^{r-1} s_j}{1+s_0} + \frac{s_0}{1+s_0} \leq \frac{d}{d+1}\sum_{j=0}^{r-1} s_j + \frac{s_0}{1+s_0}, \tag{D20}$$

where the inequality holds because $s_0 \geq 1/d$. Therefore,

$$\mathbb{E}U_r(\Psi) \leq \frac{d}{d+1}\mathbb{E}\sum_{j=0}^{r-1} s_j + \mathbb{E}\frac{s_0}{1+s_0} < \frac{4r}{d+1} + \frac{4}{d+1} = \frac{4(r+1)}{d+1}, \tag{D21}$$

which confirms Eq. (D18). Here the second inequality holds because

$$\mathbb{E}\sum_{j=0}^{r-1} s_j \leq r\mathbb{E}s_0 \leq \frac{4r}{d}, \quad \mathbb{E}\frac{s_0}{1+s_0} \leq \frac{\mathbb{E}s_0}{1+\mathbb{E}s_0} \leq \frac{4}{d+4} < \frac{4}{d+1}, \tag{D22}$$

given that $\mathbb{E}s_0 \leq 4/d$ by Lemma 22 in Ref. [68] and that the function $s_0/(1+s_0)$ is concave in s_0. □

4. Proof of Theorem 4

Proof of Theorem 4. The first inequality in Eq. (69) follows from Theorem 1 given that $P_{\mathrm{sep}}(\Psi, \mathcal{S}_r) \geq P_{\mathrm{sep}}(\Phi, \mathcal{S}_r)$ for all $|\Psi\rangle \in \mathcal{H}_{AB}$ by Theorem 2. The second, third, and fourth inequalities in Eq. (69) hold by definition. The last inequality in Eq. (69) holds because $P_{\mathrm{LC}}^{\mathrm{UB}}(\Psi, \mathcal{S}_r) \leq U_r(\Psi)$ by Eq. (D17) and $\mathbb{E}U_r(\Psi) < 4(r+1)/(d+1)$ by Lemma 9. □

5. Proof of Theorem 5

Proof of Theorem 5. Equation (70) in Theorem 5 can be proved as follows:

$$\Pr\biggl\{P_{\mathrm{LC}}^{\mathrm{H}}(\Psi, \mathcal{S}_r) \geq \frac{4(r+1)}{d+1} + \epsilon\biggr\} \leq \Pr\biggl\{U_r(\Psi) \geq \frac{4(r+1)}{d+1} + \epsilon\biggr\} \leq \Pr\{U_r(\Psi) \geq \mathbb{E}U_r(\Psi) + \epsilon\} \leq 2\exp\biggl(-\frac{D\epsilon^2}{50\pi}\biggr). \tag{D23}$$

Here the first two inequalities follow from the facts that $P^{\mathrm{H}}_{\mathrm{LC}}(\Psi,\mathcal{S}_r)\leq P^{\mathrm{UB}}_{\mathrm{LC}}(\Psi,\mathcal{S}_r)\leq U_r(\Psi)$ by Eq. (D17) and that $\mathbb{E}U_r(\Psi)<4(r+1)/(d+1)$ by Lemma 9; the last inequality follows from Lemma 8 (Levy's lemma) with $n=2D$ and $\eta=2$ given that $U_r(\Psi)$ is a Lipschitz function with Lipschitz constant 2 by Lemma 9 again.

By definition we have $P_{\mathrm{sep}}(\Psi,\mathcal{S}_r)\leq P_{\mathrm{LC}}(\Psi,\mathcal{S}_r)\leq P^{\mathrm{H}}_{\mathrm{LC}}(\Psi,\mathcal{S}_r)$ and $P_{\mathrm{sep}}(\Psi,\mathcal{S}_r)\leq P^{\mathrm{H}}_{\mathrm{sep}}(\Psi,\mathcal{S}_r)\leq P^{\mathrm{H}}_{\mathrm{LC}}(\Psi,\mathcal{S}_r)$, so Eq. (70) still holds if $P^{\mathrm{H}}_{\mathrm{LC}}(\Psi,\mathcal{S}_r)$ is replaced by $P_{\mathrm{LC}}(\Psi,\mathcal{S}_r)$, $P^{\mathrm{H}}_{\mathrm{sep}}(\Psi,\mathcal{S}_r)$, or $P_{\mathrm{sep}}(\Psi,\mathcal{S}_r)$, which completes the proof of Theorem 5. □

Appendix E: Proofs of results on two-qubit pure states

In this appendix we prove Lemmas 1-3 and Proposition 19, which are tied to entanglement certification of two-qubit pure states.

1. Proof of Lemma 1

Proof of Lemma 1. Recall that the target state $|\Psi_\theta\rangle$ is invariant under swap, complex conjugation (with respect to the computational basis), and any unitary transformation of the form $V_\zeta\otimes V_\zeta^*$, where $V_\zeta=|0\rangle\langle 0|+\mathrm{e}^{-\mathrm{i}\zeta}|1\rangle\langle 1|$ and $0\leq\zeta<2\pi$. Therefore, according to Proposition 14, we can restrict our attention to verification operators that enjoy the same symmetry when searching for an optimal verification operator. Following a similar analysis presented in Ref. [36] we can deduce that any such verification operator has the following form:

$$\Omega=|\Psi_\theta\rangle\langle\Psi_\theta|+\lambda_2|\Psi_\theta^\perp\rangle\langle\Psi_\theta^\perp|+\lambda_3(|01\rangle\langle 01|+|10\rangle\langle 10|),\quad 0\leq\lambda_2,\lambda_3\leq 1, \tag{E1}$$

where $|\Psi_\theta^\perp\rangle=\sin\theta|00\rangle-\cos\theta|11\rangle$ is orthogonal to the target state $|\Psi_\theta\rangle$.

Now, suppose Ω is associated with a separable verification strategy, then both Ω and $\mathbb{1}-\Omega$ are separable operators. In the case of two qubits under consideration, a positive operator is separable iff it is positive after partial transpose with respect to either party, say Bob. Simple calculation shows that Ω^{T_B} has the following four eigenvalues:

$$\cos^2\theta+\lambda_2\sin^2\theta,\quad \sin^2\theta+\lambda_2\cos^2\theta,\quad \lambda_3+(1-\lambda_2)\cos\theta\sin\theta,\quad \lambda_3-(1-\lambda_2)\cos\theta\sin\theta. \tag{E2}$$

The verification strategy Ω is separable iff all these eigenvalues lie in the interval $[0,1]$, which amounts to the following conditions:

$$\lambda_3+(1-\lambda_2)\cos\theta\sin\theta\leq 1,\quad \lambda_3-(1-\lambda_2)\cos\theta\sin\theta\geq 0, \tag{E3}$$

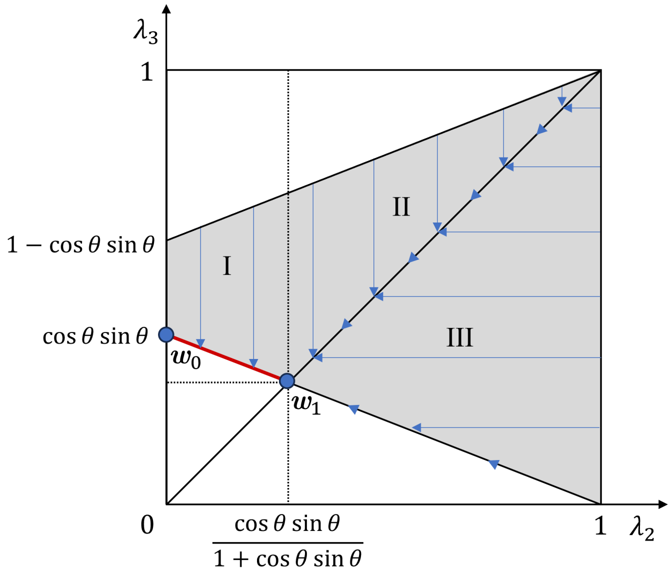

FIG. 7. Verification operators of $|\Psi_\theta\rangle$ that have the form Eq. (E1). Separable verification operators correspond to points in the shaded region, which is constrained by Eq. (E3). The blue arrows indicate optimization directions along which the separation probability is nonincreasing. One point on the red line segment $(\boldsymbol{w}_0,\boldsymbol{w}_1)$ corresponds to an optimal verification operator.

as illustrated in Fig. 7. Note that the separation probability $P_\Omega(\Psi_\theta)$ is nondecreasing in λ_2 and λ_3; in addition, the first inequality is satisfied automatically when the second inequality is saturated. To construct an optimal separable verification operator, it suffices to consider the case in which the second inequality is saturated, that is,

$$\lambda_2 + \frac{\lambda_3}{\cos\theta\sin\theta} = 1. \tag{E4}$$

If $\lambda_2 \geq \lambda_3$, then $\beta(\Omega) = \lambda_2$ and $\nu(\Omega) = 1 - \lambda_2$, which means $\operatorname{tr}(\Omega\sigma) \leq \cos^2\theta + \lambda_2\sin^2\theta$ for any $\sigma \in \mathcal{S}_{\text{sep}}$ by Proposition 10, and the upper bound can be attained when $\sigma = |00\rangle\langle 00|$. So the separation probability $P_\Omega(\Psi_\theta)$ reads

$$P_\Omega(\Psi_\theta) = \max_{\sigma\in\mathcal{S}_{\text{sep}}} \operatorname{tr}(\Omega\sigma) = \cos^2\theta + \lambda_2\sin^2\theta, \tag{E5}$$

which increases monotonically with λ_2, assuming that $\lambda_2 \geq \lambda_3$. To construct an optimal separable verification operator, therefore, it suffices to consider the parameter range defined by the following conditions:

$$\lambda_2 + \frac{\lambda_3}{\cos\theta\sin\theta} = 1, \quad 0 \leq \lambda_2 \leq \lambda_3, \tag{E6}$$

which corresponds to the red line segment in Fig. 7. The two endpoints of this line segment read

$$\boldsymbol{w}_0 := (0, \cos\theta\sin\theta), \quad \boldsymbol{w}_1 := \left(\frac{\cos\theta\sin\theta}{1+\cos\theta\sin\theta}, \frac{\cos\theta\sin\theta}{1+\cos\theta\sin\theta}\right), \tag{E7}$$

which correspond to the verification operators Ω_0 and Ω_1 defined in Eqs. (74) and (75), respectively. It follows that an optimal separable verification operator can be constructed from a convex combination of Ω_0 and Ω_1. In other words, for some $p \in [0,1]$, $\Omega(\theta,p)$ is an optimal separable verification operator of the target state $|\Psi_\theta\rangle$, which amounts to Eq. (80). This observation completes the proof of Lemma 1. □

2. Proof of Lemma 2

Proof of Lemma 2. Let

$$|\psi_{a,\xi}\rangle = \cos a|0\rangle + \sin a\, \mathrm{e}^{\mathrm{i}\xi}|1\rangle, \quad \rho_{a,\xi} = |\psi_{a,\xi}\rangle\langle\psi_{a,\xi}|, \quad 0 \leq a \leq \pi/2, \quad 0 \leq \xi < 2\pi. \tag{E8}$$

When $\xi = 0$, $|\psi_{a,\xi}\rangle$ and $\rho_{a,\xi}$ can be abbreviated as $|\psi_a\rangle$ and ρ_a, respectively. Then $P(\theta,p)$ can be expressed as follows:

$$P(\theta,p) = \max_{0\leq a,b\leq\pi/2,\, 0\leq\xi_1,\xi_2<2\pi} \operatorname{tr}[\Omega(\theta,p)\rho_{a,\xi_1}\otimes\rho_{b,\xi_2}] = \max_{0\leq a,b\leq\pi/2} \operatorname{tr}[\Omega(\theta,p)(\rho_a\otimes\rho_b)], \tag{E9}$$

where the second equality holds because all entries of $\Omega(\theta,p)$ in the computational basis are nonnegative. In addition, direct calculation yields

$$\begin{aligned}\operatorname{tr}[\Omega(\theta,p)(\rho_a\otimes\rho_b)] = {} & (\cos\theta\cos a\cos b + \sin\theta\sin a\sin b)^2 + \frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}(\sin\theta\cos a\cos b - \cos\theta\sin a\sin b)^2 \\ & + \cos\theta\sin\theta\left(1 - \frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}\right)\left(\cos^2 a\sin^2 b + \sin^2 a\cos^2 b\right).\end{aligned} \tag{E10}$$

Let $u = (\cos^2 a + \cos^2 b)/2$ and $v = (\cos^2 a - \cos^2 b)/2$. Then $\operatorname{tr}[\Omega(\theta,p)(\rho_a\otimes\rho_b)]$ can also be expressed as follows:

$$\begin{aligned}\operatorname{tr}[\Omega(\theta,p)(\rho_a\otimes\rho_b)] = {} & \left[\cos\theta\sqrt{(u+v)(u-v)} + \sin\theta\sqrt{(1-u-v)(1-u+v)}\right]^2 \\ & + \frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}\left[\sin\theta\sqrt{(u+v)(u-v)} - \cos\theta\sqrt{(1-u-v)(1-u+v)}\right]^2 \\ & + 2\cos\theta\sin\theta\left(1 - \frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}\right)[u - (u+v)(u-v)].\end{aligned} \tag{E11}$$

Its partial derivative over v reads

$$\frac{\partial\operatorname{tr}[\Omega(\theta,p)(\rho_a\otimes\rho_b)]}{\partial v} = -2\gamma v, \tag{E12}$$

where

$$\begin{aligned}\gamma &= 1+\cos\theta\sin\theta(\tan a\tan b+\cot a\cot b)+\frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}[1-\cos\theta\sin\theta(\tan a\tan b+\cot a\cot b)]\\ &\quad -2\cos\theta\sin\theta\left(1-\frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}\right)\geq 1+\frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}\geq 1.\end{aligned}\tag{E13}$$

Therefore, $\mathrm{tr}[\Omega(\theta,p)(\rho_a\otimes\rho_b)]$ is strictly increasing in v when $v\leq 0$, and strictly decreasing in v when $v\geq 0$. To evaluate the last maximization in Eq. (E9), we can take $v=0$, that is, $b=a$, which confirms the first equality in Eq. (81).

Now, direct calculation yields

$$\begin{aligned}\mathrm{tr}\big[\Omega(\theta,p)\rho_a^{\otimes 2}\big] &= \big(\cos\theta\cos^2 a+\sin\theta\sin^2 a\big)^2+2\cos\theta\sin\theta\cos^2 a\sin^2 a\\ &\quad +\frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}\Big[\big(\sin\theta\cos^2 a-\cos\theta\sin^2 a\big)^2-2\cos\theta\sin\theta\cos^2 a\sin^2 a\Big].\end{aligned}\tag{E14}$$

To determine the maximum of $\mathrm{tr}[\Omega(\theta,p)\rho_a^{\otimes 2}]$ over a, we can take its partial derivative with respect to a:

$$\frac{\partial\,\mathrm{tr}[\Omega(\theta,p)\rho_a^{\otimes 2}]}{\partial a}=4\cos a\sin a\big[g_1(\theta,p)\cos^2 a-g_2(\theta,p)\sin^2 a\big],\tag{E15}$$

where

$$\begin{aligned}g_1(\theta,p)&=2\cos\theta\sin\theta-\cos^2\theta-\frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}\big(2\cos\theta\sin\theta+\sin^2\theta\big),\\ g_2(\theta,p)&=2\cos\theta\sin\theta-\sin^2\theta-\frac{p\cos\theta\sin\theta}{1+\cos\theta\sin\theta}\big(2\cos\theta\sin\theta+\cos^2\theta\big).\end{aligned}\tag{E16}$$

In conjunction with the assumptions $0<\theta\leq\pi/4$ and $0\leq p\leq 1$ we can deduce that

$$g_2(\theta,p)\geq g_2(\theta,1)=\frac{\cos(2\theta)+\sin(2\theta)-1}{2+\sin(2\theta)}\geq 0,\quad g_2(\theta,p)-g_1(\theta,p)=\frac{\cos(2\theta)[2+(1-p)\sin(2\theta)]}{2+\sin(2\theta)}\geq 0.\tag{E17}$$

Here the first inequality is saturated iff $p=1$, the second inequality is saturated iff $\theta=\pi/4$, and the third inequality is saturated iff $\theta=\pi/4$.

If $q(\theta)\leq p\leq 1$, where $q(\theta)$ is defined in Eq. (79) and satisfies $q(\theta)\leq 1$, then $g_1(\theta,p)\leq 0$, so $\mathrm{tr}[\Omega(\theta,p)\rho_a^{\otimes 2}]$ is nonincreasing in a and is thus maximized when $a=0=a^*(\theta,p)$. Therefore,

$$P(\theta,p)=\mathrm{tr}[\Omega(\theta,p)|00\rangle\langle 00|]=\cos^2\theta+\frac{p\cos\theta\sin^3\theta}{1+\cos\theta\sin\theta},\tag{E18}$$

which confirms the second equality in Eq. (81) and shows that $P(\theta,p)$ is strictly increasing in p; this result also confirms the third equality in Eq. (81) except when $\theta=\pi/4$. If in addition $p<1$ or $\theta<\pi/4$, then $g_2(\theta,p)>0$, so $\mathrm{tr}[\Omega(\theta,p)\rho_a^{\otimes 2}]$ is strictly decreasing in a, and its maximum over $a\in[0,\pi/2]$ is attained iff $a=a^*(\theta,p)$.

If instead $0\leq p<q(\theta)$, then $p<1$, $g_2(\theta,p)>0$, $0\leq g_1(\theta,p)\leq g_2(\theta,p)$, and $g_1(\theta,p)/g_2(\theta,p)=h(\theta,p)$, where $h(\theta,p)$ is defined in Eq. (79). In addition, the function $g_1(\theta,p)\cos^2 a-g_2(\theta,p)\sin^2 a$ is strictly decreasing in a for $a\in[0,\pi/2]$ and is equal to 0 when $a=\arctan\sqrt{h(\theta,p)}=a^*(\theta,p)$ [see Eq. (79)]. Therefore, the maximum of $\mathrm{tr}[\Omega(\theta,p)\rho_a^{\otimes 2}]$ over $a\in[0,\pi/2]$ is attained iff $a=\arctan\sqrt{h(\theta,p)}=a^*(\theta,p)$, which confirms the second equality in Eq. (81).

Next, we prove the third equality in Eq. (81) when $\theta=\pi/4$. In this case, $q(\theta)=1$, $h(\theta,p)=1$ for $p\in[0,1)$, and

$$a^*(\theta,p)=\begin{cases}\pi/4 & p\in[0,1),\\ 0 & p=1,\end{cases}\tag{E19}$$

so $\mathrm{tr}\big[\Omega(\theta,p)\rho_{a^*}^{\otimes 2}\big]=(9-p)/12$, which confirms the third equality in Eq. (81).

Finally, we turn to the convexity of the separation probability $P(\theta,p)$, assuming that $\arctan(1/2)<\theta<\pi/4$ and $0\leq p\leq q(\theta)$. Then the maximum of $\mathrm{tr}[\Omega(\theta,p)\rho_a^{\otimes 2}]$ over $a\in[0,\pi/2]$ is attained iff $a=\arctan\sqrt{h(\theta,p)}=a^*(\theta,p)$. In addition, according to Eq. (79) and the following equation

$$\frac{\partial h(\theta,p)}{\partial p}=\frac{(\sin^4\theta-\cos^4\theta)}{g_2^2(\theta,p)(1+\cos\theta\sin\theta)}<0,\tag{E20}$$

$h(\theta,p)$ and $a^*(\theta,p)$ are strictly decreasing in p. Suppose $0\le p_1<p_2\le q(\theta)$, $0<x<1$, and $p=xp_1+(1-x)p_2$; then

$$\begin{aligned}P(\theta,p)&=\operatorname{tr}\Big[\Omega(\theta,p)\rho_{a^*(\theta,p)}^{\otimes 2}\Big]=x\operatorname{tr}\Big[\Omega(\theta,p_1)\rho_{a^*(\theta,p)}^{\otimes 2}\Big]+(1-x)\operatorname{tr}\Big[\Omega(\theta,p_2)\rho_{a^*(\theta,p)}^{\otimes 2}\Big]\\&<x\operatorname{tr}\Big[\Omega(\theta,p_1)\rho_{a^*(\theta,p_1)}^{\otimes 2}\Big]+(1-x)\operatorname{tr}\Big[\Omega(\theta,p_2)\rho_{a^*(\theta,p_2)}^{\otimes 2}\Big]=xP(\theta,p_1)+(1-x)P(\theta,p_2).\end{aligned}\tag{E21}$$

So $P(\theta,p)$ is strictly convex in p for $p\in[0,q(\theta)]$, which completes the proof of Lemma 2. □

3. Proof of Lemma 3

Proof of Lemma 3. By definition we have $P(\theta,p)=P_{\Omega(\theta,p)}(\Psi_\theta)=\max_{\sigma\in\mathcal{S}_{\rm sep}}\operatorname{tr}[\Omega(\theta,p)\sigma]$, so $P(\theta,p)$ is convex in p given that $\Omega(\theta,p)$ is linear in p by construction.

If $0<\theta\le\arctan(1/2)$, then $q(\theta)=0$ and $P(\theta,p)$ is strictly increasing in p by Lemma 2 and thus has a unique minimizer at $p=0$, that is $p^*(\theta)=0$, which confirms Eq. (84) for $\theta\in(0,\arctan(1/2)]$. If $\theta=\pi/4$, then $q(\theta)=1$ and $P(\theta,p)=(9-p)/12$ is strictly decreasing in p and thus has a unique minimizer at $p=1$, that is $p^*(\theta)=1$, which confirms Eq. (84) again. In both cases, we have $p^*(\theta)\in[0,q(\theta)]$.

Next, suppose $\arctan(1/2)<\theta<\pi/4$; then $0<q(\theta)<1$. According to Lemma 2, $P(\theta,p)$ is strictly increasing in p for $p\in[q(\theta),1]$ and strictly convex in p for $p\in[0,q(\theta)]$. Therefore, $P(\theta,p)$ has a unique minimizer and $p^*(\theta)\in[0,q(\theta)]$; in addition, $P(\theta,p)$ is strictly decreasing (increasing) in p for $p\in[0,p^*(\theta)]$ ($p\in[p^*(\theta),1]$). In conjunction with Eq. (79) we can further deduce that

$$P_p(\theta,0)=\frac{\sin(2\theta)[17-9\cos(4\theta)-25\sin(2\theta)+3\sin(6\theta)]}{8[2\sin(2\theta)-1]^2[2+\sin(2\theta)]},\tag{E22}$$

$$P_p(\theta,p)=\frac{\cos\theta\sin^3\theta}{1+\cos\theta\sin\theta}>0\quad\forall p\in[q(\theta),1],\tag{E23}$$

where $P_p(\theta,p)$ is a shorthand for $\partial P(\theta,p)/\partial p$. Note that $P_p(\theta,p)$ is continuous in p for $p\in[0,1]$.

If $\arctan(1/2)<\theta\le\theta^*$, then $P_p(\theta,p)\ge P_p(\theta,0)\ge 0$ for $p\in[0,1]$; note that $P_p(\theta^*,0)=0$ according to the definition of θ^* based on Eq. (83). Therefore, $P(\theta,p)$ is strictly increasing in p for $p\in[0,1]$, which means $p^*(\theta)=0$ and confirms Eq. (84) for $\theta\in(0,\theta^*]$ given the above analysis.

If $\theta^*<\theta<\pi/4$, then $P_p(\theta,p=0)<0$, while $P_p(\theta,p=q(\theta))>0$. So $P_p(\theta,p)=0$ has a unique zero for $p\in(0,q(\theta))$, which necessarily coincides with the minimizer $p^*(\theta)$. This observation completes the proof of Lemma 3. □

4. Proof of Proposition 19

To prove Proposition 19, we need to introduce a verification strategy for $|\Psi_\theta\rangle$ constructed by Wang and Hayashi [64], assuming that $0<\theta\le\pi/4$. First, Ref. [64] constructed the following five test operators for $|\Psi_\theta\rangle$ using LOCC:

$$\begin{aligned}T_1^{A\to B}&=\eta|0\rangle\langle 0|\otimes|0\rangle\langle 0|+|\tilde\psi_+\rangle\langle\tilde\psi_+|\otimes|+\rangle\langle +|+|\tilde\psi_-\rangle\langle\tilde\psi_-|\otimes|-\rangle\langle -|,\\T_2^{A\to B}&=\eta|0\rangle\langle 0|\otimes|0\rangle\langle 0|+|\tilde\varphi_+\rangle\langle\tilde\varphi_+|\otimes|\top\rangle\langle\top|+|\tilde\varphi_-\rangle\langle\tilde\varphi_-|\otimes|\perp\rangle\langle\perp|,\\T_1^{B\to A}&=\eta|0\rangle\langle 0|\otimes|0\rangle\langle 0|+|+\rangle\langle +|\otimes|\tilde\psi_+\rangle\langle\tilde\psi_+|+|-\rangle\langle -|\otimes|\tilde\psi_-\rangle\langle\tilde\psi_-|,\\T_2^{B\to A}&=\eta|0\rangle\langle 0|\otimes|0\rangle\langle 0|+|\top\rangle\langle\top|\otimes|\tilde\varphi_+\rangle\langle\tilde\varphi_+|+|\perp\rangle\langle\perp|\otimes|\tilde\varphi_-\rangle\langle\tilde\varphi_-|,\\T_3&=|0\rangle\langle 0|\otimes|0\rangle\langle 0|+|1\rangle\langle 1|\otimes|1\rangle\langle 1|,\end{aligned}\tag{E24}$$

where

$$\begin{aligned}&|+\rangle=\frac{1}{\sqrt2}(|0\rangle+|1\rangle),\quad|-\rangle=\frac{1}{\sqrt2}(|0\rangle-|1\rangle),\quad|\top\rangle=\frac{1}{\sqrt2}(|0\rangle+\mathrm{i}|1\rangle),\quad|\perp\rangle=\frac{1}{\sqrt2}(|0\rangle-\mathrm{i}|1\rangle),\\&|\tilde\psi_\pm\rangle=\frac{(1-\eta)\cos\theta}{\sqrt{1-\eta\cos^2\theta}}|0\rangle\pm\frac{\sin\theta}{\sqrt{1-\eta\cos^2\theta}}|1\rangle,\quad|\tilde\varphi_\pm\rangle=\frac{(1-\eta)\cos\theta}{\sqrt{1-\eta\cos^2\theta}}|0\rangle\pm\mathrm{i}\frac{\sin\theta}{\sqrt{1-\eta\cos^2\theta}}|1\rangle.\end{aligned}\tag{E25}$$

Note that $|\tilde\psi_\pm\rangle$ and $|\tilde\varphi_\pm\rangle$ are not normalized. Based on these test operators, Ref. [64] constructed the following verification strategy for $|\Psi_\theta\rangle$:

$$\Omega_{\rm WH}(\theta,\eta,p')=\frac{1-p'}{4}\big(T_1^{A\to B}+T_2^{A\to B}+T_1^{B\to A}+T_2^{B\to A}\big)+p'T_3,\tag{E26}$$

which can be realized by LOCC.

Now, suppose $\tilde{p}(\theta) \leq p \leq 1$, where $\tilde{p}(\theta)$ is defined in Eq. (86). Let

$$\eta = 1 - \tan\theta, \quad p' = \cos\theta\sin\theta\left(\frac{\cos^2\theta + \cos\theta\sin\theta}{1+\cos\theta\sin\theta}p + \tan\theta - 1\right); \tag{E27}$$

then $0 \leq p' \leq \sin^2\theta/(1+\cos\theta\sin\theta) \leq 1/3$, and it is straightforward to verify the following equality:

$$\Omega(\theta, p) = \Omega_{\mathrm{WH}}(\theta, \eta, p'). \tag{E28}$$

So the verification strategy $\Omega(\theta, p)$ can be realized by LOCC, which completes the proof of Proposition 19.