Minimum number of experimental settings required to verify bipartite pure states and unitaries

Yunting Li, Haoyu Zhang, Zihao Li, and Huangjun Zhu *

State Key Laboratory of Surface Physics and Department of Physics, Fudan University, Shanghai 200433, China;
Institute for Nanoelectronic Devices and Quantum Computing, Fudan University, Shanghai 200433, China;
and Center for Field Theory and Particle Physics, Fudan University, Shanghai 200433, China

(Received 19 August 2021; accepted 6 December 2021; published 27 December 2021)

Efficient verification of quantum states and gates is crucial to the development of quantum technologies. Although the sample complexities of quantum state verification and quantum gate verification have been studied by many researchers, the number of experimental settings has received little attention and is poorly understood. In this work we study systematically quantum state verification and quantum gate verification with a focus on the number of experimental settings. We show that any bipartite pure state can be verified by only two measurement settings based on local projective measurements. Any bipartite unitary in dimension d can be verified by $2d$ experimental settings based on local operations. In addition, we introduce the concept of entanglement-free verification and clarify its connection with minimal-setting verification. Finally, we show that any two-qubit unitary can be verified with at most five experimental settings; moreover, a generic two-qubit unitary (except for a set of measure zero) can be verified by an entanglement-free protocol based on four settings. In the course of study we clarify the properties of Schmidt coefficients of two-qubit unitaries, which are of independent interest.

DOI: 10.1103/PhysRevA.104.062439

I. INTRODUCTION

Quantum information processing has attracted increasing attention recently due to its great potential and profound implications. To harness the power of quantum information processing, it is crucial to verify the underlying quantum states and devices efficiently based on the accessible measurements. Unfortunately, traditional tomographic approaches are notoriously inefficient since the resource overhead increases exponentially with the system size under consideration. To overcome this problem, a number of alternative approaches have been proposed recently; see Refs. [1–4] for an overview.

Among alternative approaches proposed so far, *quantum state verification* (QSV) is particularly appealing because it can achieve a high efficiency based on local operations and classical communication (LOCC) [5–10]. Notably, efficient verification protocols based on local projective measurements have been constructed for bipartite pure states [5,11–14], stabilizer states [8,10,15–19], hypergraph states [17], weighted graph states [20], and Dicke states [21,22]. Moreover, the efficiency of QSV has been demonstrated in a number of experiments [23–26]. Recently, the idea of QSV was generalized to *quantum gate verification* (QGV) [27–29] (cf. Refs. [30–34]), which enables efficient verification of various quantum gates and quantum circuits based on LOCC. Notably, all bipartite unitaries and Clifford unitaries can be verified with resources that are independent of the system size, while the resources required to verify the generalized controlled-NOT (CNOT) gate and generalized controlled-Z (CZ) gate grow only linearly with the system size. The efficiency of QGV has also been demonstrated in several experiments recently [35,36].

So far most works on QSV and QGV have exclusively focused on the sample efficiency as the main figure of merit. By contrast, the number of experimental settings has received little attention, although this figure of merit is also of key interest to both theoretical study and practical applications. Even for bipartite pure states, it is still not clear how many measurement settings are required to construct a reliable verification protocol. The situation is even worse in the case of bipartite unitaries, not to mention the multipartite scenario. This problem becomes particularly important when it is difficult or slow to switch measurement settings, which is the case in many practical scenarios.

In this work we study systematically QSV and QGV with a focus on the number of experimental settings based on LOCC. We show that any bipartite pure state can be verified by two measurement settings based on nonadaptive local projective measurements. By contrast, at least d experimental settings based on local operations are required to verify each bipartite unitary in dimension d, while $2d$ settings are sufficient. In addition, we introduce the concept of entanglement-free verification, which is of special interest to both theoretical study and practical applications. Moreover, we show that any entanglement-free verification protocol can be turned into a minimal-setting protocol and vice versa.

For each two-qubit unitary, we determine the minimum number of required experimental settings explicitly. Our study shows that any two-qubit unitary can be verified using only five experimental settings, while a generic two-qubit unitary (except for a set of measure zero) can be verified by an entanglement-free protocol based on four settings. Explicit entanglement-free protocols are constructed for CNOT, CZ,

*zhuhuangjun@fudan.edu.cn

controlled-phase (C-Phase), and SWAP gates, respectively. In the course of study we clarify the properties of Schmidt coefficients of two-qubit unitaries and their implications for studying the equivalence relation under local unitary transformations, which are of interest beyond the main focus of this work.

The rest of this paper is organized as follows. In Sec. II we briefly review the basic frameworks of QSV and QGV. In Sec. III we determine the minimum number of measurement settings required to verify each bipartite pure state. In Sec. IV we clarify the relation between minimal-setting verification and entanglement-free verification; in addition, we derive nearly tight lower and upper bounds for the minimum number of settings required to verify each bipartite unitary. In Sec. V we clarify the properties of Schmidt coefficients of two-qubit unitaries. In Sec. VI we determine the minimum number of settings required to verify each two-qubit unitary. Section VII summarizes the paper. To streamline the presentation, some technical proofs are relegated to the Appendixes.

II. QUANTUM STATE AND GATE VERIFICATION

In preparation for the later study, here we briefly review the basic frameworks of QSV [8–10] and QGV [27–29] (cf. Refs. [30–32]).

A. Quantum state verification

Consider a quantum system associated with the Hilbert space $\mathcal{H}$. A quantum device is supposed to produce the target state $|\Psi\rangle$ but actually produces the N states $\rho_1, \rho_2, \ldots, \rho_N$ in N runs. To distinguish the two situations, we can perform a random test in each run. Each test is determined by a test operator E_l, which is associated with a two-outcome measurement of the form $\{E_l, I - E_l\}$, where I is the identity operator. Here the first outcome corresponds to passing the test. To guarantee that the target state can always pass the test, the test operator E_l should satisfy the condition $\langle\Psi|E_l|\Psi\rangle = 1$, which means $E_l|\Psi\rangle = |\Psi\rangle$.

If the test E_l is performed with probability p_l, then the performance of the above verification procedure is determined by the verification operator $\Omega = \sum_l p_l E_l$. Suppose $\langle\Psi|\rho|\Psi\rangle \leqslant 1 - \varepsilon$, then the maximal probability that ρ can pass each test on average is [8–10]

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

where $\beta(\Omega)$ is the second largest eigenvalue of Ω, and $\nu(\Omega) = 1 - \beta(\Omega)$ is the spectral gap from the maximal eigenvalue. Note that a positive spectral gap is necessary and sufficient for verifying the target state reliably, assuming that the total number of tests is not limited.

Let $\varepsilon_j = 1 - \langle\Psi|\rho_j|\Psi\rangle$ be the infidelity of the state prepared in the jth run and let $\bar{\varepsilon} = \sum_j \varepsilon_j/N$ be the average infidelity. Suppose the states $\rho_1, \rho_2, \ldots, \rho_N$ prepared in the N runs are independent of each other. Then the maximal probability that these states can pass all N tests is $[1 - \nu(\Omega)\bar{\varepsilon}]^N$. To ensure the condition $\bar{\varepsilon} < \varepsilon$ with significant level δ, the minimum number of tests required reads [8–10]

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

Not surprisingly, a larger spectral gap means a higher efficiency.

B. Quantum gate verification

Consider a quantum device that is expected to perform the unitary transformation $\mathcal{U}$ associated with the unitary operator U on $\mathcal{H}$, but actually realizes an unknown quantum process Λ. In order to verify whether this quantum process is sufficiently close to the target unitary transformation, we need to construct a set $\mathscr{T} = \{|\psi_j\rangle\}_j$ of test states. In each run we randomly prepare a test state from the set $\mathscr{T}$ and apply the quantum process Λ. Then we verify whether the output state $\Lambda(\rho_j)$ is sufficiently close to the target output state $\mathcal{U}(\rho_j) = U\rho_j U^\dagger$ by virtue of QSV as described in Sec. II A, where $\rho_j = |\psi_j\rangle\langle\psi_j|$ [27,28]. By construction, the target unitary transformation can always pass each test.

Suppose the test state $|\psi_j\rangle$ is chosen with probability $p_j > 0$; denote the verification operator for the output state $\mathcal{U}(\rho_j)$ by Ω_j. Then the average probability that the process Λ can pass each test reads [28]

$$\sum_j p_j \,\mathrm{tr}[\Omega_j \Lambda(\rho_j)]. \quad (3)$$

The target unitary transformation $\mathcal{U}$ can be verified reliably if only $\mathcal{U}$ can pass each test with certainty. To clarify this condition, we need to introduce additional terminology. Let ν_j be the spectral gap of Ω_j. The test state $|\psi_j\rangle$ is effective if $\nu_j > 0$; the set of effective test states is denoted by $\mathscr{T}_{\mathrm{eff}}$. The verification protocol is *ordinary* if $\nu_j > 0$ for each j, in which case every test state is effective, so that $\mathscr{T}_{\mathrm{eff}} = \mathscr{T}$. Otherwise, the verification protocol is *extraordinary*.

A set $\mathscr{T} = \{|\psi_j\rangle\}_j$ in $\mathcal{H}$ can *identify* the unitary transformation $\mathcal{U}$ if the condition

$$\Lambda(|\psi_j\rangle\langle\psi_j|) = \mathcal{U}(|\psi_j\rangle\langle\psi_j|), \quad \forall j \quad (4)$$

implies that $\Lambda = \mathcal{U}$, that is,

$$\Lambda(\rho) = \mathcal{U}(\rho), \quad \forall\rho \in \mathscr{D}(\mathcal{H}), \quad (5)$$

where $\mathscr{D}(\mathcal{H})$ denotes the set of all density operators on the Hilbert space $\mathcal{H}$. In this case, the set $\mathscr{T}$ is referred to as an *identification set* (IS). It turns out the set $\mathscr{T}$ can identify $\mathcal{U}$ iff it can identify any other unitary transformation on $\mathcal{H}$ [32], so it is not necessary to refer to a specific unitary transformation. The significance of ISs to QGV is manifested in the following lemma. Further discussions on ISs will be presented in Sec. IV A.

Lemma 1. If the unitary transformation $\mathcal{U}$ can be verified reliably by a protocol based on the set $\mathscr{T} = \{|\psi_j\rangle\}_j$ of test states, then $\mathscr{T}$ is an IS. If the set $\mathscr{T}_{\mathrm{eff}}$ of effective test states is an IS, then the unitary transformation $\mathcal{U}$ can be verified reliably. If the verification protocol is ordinary, then $\mathcal{U}$ can be verified reliably iff $\mathscr{T}$ is an IS.

Proof. By construction, $\mathcal{U}$ can pass each test with certainty, so any quantum process Λ that satisfies the condition in Eq. (4) can also pass each test with certainty. Suppose

$\mathcal{U}$ can be verified reliably. Then only $\mathcal{U}$ can pass each test with certainty, which implies that $\Lambda = \mathcal{U}$ when Eq. (4) holds. Therefore, $\mathscr{T}$ is an IS.

Conversely, if a quantum process Λ can pass each test with certainty, then we have $\mathrm{tr}[\Omega_j \Lambda(|\psi_j\rangle\langle\psi_j|)] = 1$ for each $|\psi_j\rangle \in \mathscr{T}$, which implies that

$$\Lambda(|\psi_j\rangle\langle\psi_j|) = \mathcal{U}(|\psi_j\rangle\langle\psi_j|), \quad \forall |\psi_j\rangle \in \mathscr{T}_{\mathrm{eff}}, \tag{6}$$

given that $|\psi_j\rangle \in \mathscr{T}_{\mathrm{eff}}$ iff $\nu_j > 0$. Now suppose the set $\mathscr{T}_{\mathrm{eff}}$ of effective test states is an IS, then Eq. (6) implies that $\Lambda = \mathcal{U}$. Therefore, only the target unitary transformation $\mathcal{U}$ can pass each test with certainty, which means $\mathcal{U}$ can be verified reliably. ■

If the verification protocol is ordinary, then $\mathscr{T}_{\mathrm{eff}} = \mathscr{T}$, so the last statement in Lemma 1 follows from the first two statements.

The sample complexity of QGV has been analyzed in Refs. [27–29] based on the idea of channel-state duality, but the details are not necessary to the current study. It turns out the verification of the unitary transformation $\mathcal{U}$ is closely tied to the verification of its Choi state, especially when the verification protocol is balanced, which means $\sum_j p_j \rho_j = I/d$ [28]. However, verification protocols with minimal settings are in general not balanced as we shall see later. This observation shows that some important features in QGV do not have natural analogs in QSV and deserve further studies.

III. VERIFICATION OF BIPARTITE PURE STATES WITH MINIMAL SETTINGS

Given a bipartite or multipartite pure state $|\Psi\rangle$, how many measurement settings are necessary to verify $|\Psi\rangle$ reliably? This problem is trivial if we can perform arbitrary entangling measurements, in which case one setting is enough. Unfortunately, it is not easy to realize entangling measurements in practice, so here we focus on verification protocols based on nonadaptive local projective measurements, which are amenable to experimental realization. This is a fundamental problem in the study of QSV that is of practical interest. However, it is in general very difficult to solve such an optimization problem if not impossible given that the potential choices of measurement settings are countless. Even in the bipartite case, this problem has not been solved in the literature, although it is known that any bipartite pure state can be verified by two distinct tests based on adaptive local projective measurements [12]. Note that one test based on adaptive local projective measurements may entail many different measurement settings, so the result presented in Ref. [12] does not resolve the current problem under consideration.

Here we show that any bipartite pure state can be verified by at most two measurement settings, thereby resolving the minimal-setting problem in the bipartite scenario completely.

Theorem 1. Every bipartite pure product state can be verified by one measurement setting. Every bipartite pure entangled state can be verified by two measurement settings but not one measurement setting.

Proof. Suppose the bipartite system is associated with the bipartite Hilbert space $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$ of dimension $d_{\mathrm{A}} \otimes d_{\mathrm{B}}$. In the Schmidt basis, any bipartite pure state in $\mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$ can be written as

$$|\Psi\rangle = \sum_{j=0}^{r-1} \lambda_j |jj\rangle, \tag{7}$$

where $r = \min\{d_{\mathrm{A}}, d_{\mathrm{B}}\}$, and λ_j are the Schmidt coefficients of $|\Psi\rangle$ arranged in nonincreasing order.

If $|\Psi\rangle$ is a product state, then $\lambda_j = \delta_{j0}$ and $|\Psi\rangle = |00\rangle$. In this case $|\Psi\rangle$ can be verified by a verification protocol composed of the single test $P_0 = |\Psi\rangle\langle\Psi| = |00\rangle\langle 00|$. In addition, P_0 can be realized by one measurement setting, that is, the projective measurement onto the Schmidt basis.

If $|\Psi\rangle$ is entangled, then it cannot be verified by one measurement setting based on a nonadaptive local projective measurement because the pass eigenspace of any such verification operator has dimension at least 2, which means the spectral gap is zero. To prove Theorem 1, it remains to show that $|\Psi\rangle$ can be verified by two measurement settings. Let

$$P_1 := \sum_{j=0}^{r-1} |jj\rangle\langle jj|, \tag{8}$$

$$P_2 := I - |u\rangle\langle u| \otimes I + |u\rangle\langle u| \otimes |v\rangle\langle v|, \tag{9}$$

where

$$|u\rangle := \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |j\rangle, \tag{10}$$

$$|v\rangle := \lambda_0|0\rangle + \lambda_1|1\rangle + \cdots + \lambda_{r-1}|r-1\rangle. \tag{11}$$

Then P_1 and P_2 are two test projectors for $|\Psi\rangle$ that can be realized by nonadaptive local projective measurements. To realize the test P_1, both Alice and Bob perform projective measurements on the Schmidt basis, and the test is passed if they obtain the same outcome j for $j = 0, 1, 2, \ldots, r-1$. To realize P_2, Alice performs the two-outcome projective measurement $\{|u\rangle\langle u|, I - |u\rangle\langle u|\}$ and Bob performs the two-outcome projective measurement $\{|v\rangle\langle v|, I - |v\rangle\langle v|\}$; the test is passed except when Alice obtains the first outcome, while Bob obtains the second outcome.

Now we can construct a simple verification protocol for $|\Psi\rangle$ by performing the two tests P_1 and P_2 with probability $1/2$ each. The resulting verification operator is given by $\Omega = (P_1 + P_2)/2$. According to Lemma 1 in Ref. [22], the spectral gap of Ω is given by $\nu(\Omega) = (1 - \sqrt{q})/2 > 0$ with

$$q = \|\bar{P}_1 \bar{P}_2 \bar{P}_1\| = \frac{r-1}{r}, \tag{12}$$

where $\bar{P}_j = P_j - |\Psi\rangle\langle\Psi|$ for $j = 1, 2$. Therefore, $|\Psi\rangle$ can be verified by the strategy Ω, which can be realized by two measurement settings based on nonadaptive local projective measurements. ■

IV. VERIFICATION OF UNITARY TRANSFORMATIONS WITH MINIMAL SETTINGS

In this section we explore verification protocols of unitary transformations with minimal settings. In addition we introduce the concept of entanglement-free verification and clarify its connection with minimal-setting verification. Verification of bipartite unitaries is then discussed in more detail.

A. Minimal identification sets

Recall that a set of pure states $\mathscr{T} = \{|\psi_j\rangle\}_j$ in $\mathcal{H}$ is an IS if it can identify unitary transformations on $\mathcal{H}$ (cf. Sec. II B) [32]. Here we are particularly interested in ISs with as few elements as possible. The set $\mathscr{T}$ is a *minimal identification set* (MIS) if, in addition, any proper subset is not an IS. MISs are crucial to constructing verification protocols for unitary transformations with minimal settings.

To understand the properties of ISs and MISs, we need to introduce several additional concepts. A set of pure states $\mathscr{T} = \{|\psi_j\rangle\}_j$ in $\mathcal{H}$ is a spanning set if it spans $\mathcal{H}$; it is a basis if it is a spanning set that is also linearly independent. The *transition graph* of the set $\mathscr{T}$ is a graph whose vertices are in one-to-one correspondence with the states $|\psi_j\rangle$; two vertices j, k are adjacent if $\langle\psi_j|\psi_k\rangle \neq 0$. The set $\mathscr{T}$ is connected if its transition graph is connected; note that here the definition is different from the usual definition in topology. The set is a *connected spanning set* if it is a spanning set that is connected; the set $\mathscr{T}$ is a connected linearly independent set (CLIS) if it is a linearly independent set that is connected. A connected basis is a CLIS that is also a connected spanning set. By definition a CLIS can contain at most d states, where d is the dimension of $\mathcal{H}$. Suppose the set $\mathscr{T}$ is nonempty; then a CLIS contained in $\mathscr{T}$ is maximal if it is not contained in any other CLIS contained in $\mathscr{T}$. Note that each state in $\mathscr{T}$ is contained in at least one maximal CLIS. In particular, $\mathscr{T}$ contains at least one maximal CLIS as a subset.

The following result proved in Ref. [32] clarifies the conditions under which a set of pure states can identify unitary transformations on $\mathcal{H}$.

Lemma 2. A set of pure states in $\mathcal{H}$ is an IS iff it is a connected spanning set.

By Lemma 2, at least d test states are required to identify unitaries on $\mathcal{H}$. To saturate the lower bound d, the test states must form a connected basis.

Lemma 3. A set of pure states in $\mathcal{H}$ is a MIS iff it is a connected basis.

Lemma 3 clarifies the properties of MISs; it is a simple corollary of Lemma 2 above and Lemmas 4 and 5 below, which are proved in Appendix A.

Lemma 4. Suppose $\mathscr{T}$ is a connected spanning set in $\mathcal{H}$. Then any maximal CLIS contained in $\mathscr{T}$ is a connected basis.

Lemma 5. Every connected spanning set in $\mathcal{H}$ contains a subset that forms a connected basis. Every set in $\mathcal{H}$ that contains a connected spanning subset is a connected spanning set.

Suppose $\mathscr{T}$ is a connected spanning set that is composed of k pure states. As an implication of Lemma 5, $\mathscr{T}$ contains a connected spanning subset that is composed of k' pure states as long as $d \leqslant k' \leqslant k$. To illustrate the above results, here we present a connected spanning set $\mathscr{S}$ that is composed of the computational basis and one additional state [31]:

$$\mathscr{T} = \{|j\rangle\}_{j=0}^{d-1} \cup \{|\varphi\rangle\}, \tag{13}$$

where

$$|\varphi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle. \tag{14}$$

A connected basis contained in $\mathscr{T}$ can be constructed as follows:

$$\mathscr{S} = \{|j\rangle\}_{j=1}^{d-1} \cup \{|\varphi\rangle\}. \tag{15}$$

According to Lemma 3, $\mathscr{S}$ is also a MIS.

B. Minimal-setting verification and entanglement-free verification

Let U be a unitary operator on $\mathcal{H}$ and $\mathcal{U}$ the associated unitary transformation. Recall that a general verification protocol for U (which means a verification protocol for $\mathcal{U}$) consists of a set of input test states and the verification protocol for the output state associated with each input state. For simplicity, here we assume that each test state is a pure product state, and the verification protocol for each output state is based on nonadaptive local projective measurements. Such verification protocols are most amenable to experimental realization.

We are particularly interested in the minimum number of experimental settings required to verify U by ordinary verification protocols, which is denoted by $\mu(U)$ henceforth. When extraordinary verification protocols are allowed, the minimum number is denoted by $\mu_e(U)$. To be specific, one experimental setting means the preparation of a pure product input state and a nonadaptive local projective measurement on the output state. Note that the number of experimental settings required by any verification protocol is at least the number of test states involved. In conjunction with Lemmas 1 and 2, this observation implies that

$$\mu(U) \geqslant \mu_e(U) \geqslant d \tag{16}$$

for any unitary operator U acting on a d-dimensional Hilbert space. For a simple noncomposite system, the two inequalities can always be saturated, and the verification problem is trivial. In the rest of this paper we shall focus on composite systems and consider only ordinary verification protocols, in which case it is in general highly nontrivial to determine $\mu(U)$. Although it is even more difficult to determine $\mu_e(U)$, our results on $\mu(U)$ provide valuable upper bounds for $\mu_e(U)$, which are nearly tight in the bipartite setting.

A verification protocol for U is *entanglement free* if all input test states and the corresponding output states (after the action of U) are product states; in addition, all measurements are based on local projective measurements. An entanglement-free protocol does not generate any entanglement in the verification procedure and hence the name. Such verification protocols are particularly appealing to both theoretical study and experimental realization. It turns out entanglement-free verification is intimately connected to minimal-setting verification. To clarify this point, we need to introduce some additional terminology.

Denote by Prod the set of pure product states; denote by $\mathrm{Prod}(U)$ the set of product states that remain product states after the action of U:

$$\mathrm{Prod}(U) = \{|\psi\rangle \in \mathrm{Prod} \mid U|\psi\rangle \in \mathrm{Prod}\}. \tag{17}$$

The dimension of the span of the set $\mathrm{Prod}(U)$ is denoted by $d_{\mathrm{Prod}}(U)$,

$$d_{\mathrm{Prod}}(U) = \dim \mathrm{span}(\mathrm{Prod}(U)), \tag{18}$$

which satisfies $0 \leqslant d_{\mathrm{Prod}}(U) \leqslant d$. A state $|\psi\rangle$ in $\mathcal{H}$ satisfies the *product-state constraint* associated with U if $|\psi\rangle \in \mathrm{Prod}(U)$. A set of states satisfies the product-state constraint if it is contained in $\mathrm{Prod}(U)$, so that each state satisfies the constraint.

An entanglement-free IS (EFIS) $\mathscr{T}$ for U is an IS that satisfies the product-state constraint, which implies that $\mathscr{T} \subseteq \mathrm{Prod}(U)$. Similarly, an entanglement-free MIS (EFMIS) is a MIS that satisfies the product-state constraint. Note that the definition of an EFIS (EFMIS) depends on the specific unitary transformation under consideration, although the definition of an IS (MIS) is independent of a specific unitary transformation. The unitary operator U can be verified by an entanglement-free protocol iff it admits an EFMIS, in which case $\mathrm{Prod}(U)$ contains an IS. Lemma 6 and Theorem 2 below further clarify the connections among the product-state constraint as determined by $\mathrm{Prod}(U)$, minimal-setting verification, and entanglement-free verification. The proof of Lemma 6 is presented in Appendix B.

Lemma 6. Suppose U is a unitary operator acting on a composite Hilbert space $\mathcal{H}$ of dimension d. Suppose $\mathscr{T}$ is the set of test states of an entanglement-free verification protocol for U or an ordinary verification protocol composed of d experimental settings based on local operations. Then $\mathscr{T} \subseteq \mathrm{Prod}(U)$.

Theorem 2. Suppose U is a unitary operator on a composite Hilbert space $\mathcal{H}$ of dimension d. Then the following five statements are equivalent:

1. $\mu(U) = d$.
2. $\mathrm{Prod}(U)$ is a connected spanning set.
3. $\mathrm{Prod}(U)$ contains a connected basis as a subset.
4. U admits an EFMIS.
5. U can be verified by an entanglement-free protocol.

Corollary 1. Suppose U is a unitary operator on a composite Hilbert space $\mathcal{H}$ of dimension d. If $\mu(U) = d$ or if U can be verified by an entanglement-free protocol, then $d_{\mathrm{Prod}}(U) = d$.

Corollary 1 is an immediate consequence of Theorem 2.

Proof of Theorem 2. Suppose $\mu(U) = d$. Then U can be verified by an ordinary protocol composed of d experimental settings that are based on local operations. Let $\mathscr{T}$ be the set of test states; then $\mathscr{T}$ forms a connected basis according to Lemmas 1 and 2. In addition, $\mathscr{T} \subseteq \mathrm{Prod}(U)$ according to Lemma 6. Therefore, $\mathrm{Prod}(U)$ is a connected spanning set according to Lemma 5, which confirms the implication $1 \Rightarrow 2$.

Next, suppose $\mathrm{Prod}(U)$ is a connected spanning set. Then $\mathrm{Prod}(U)$ contains a connected basis as a subset according to Lemma 5, which confirms the implication $2 \Rightarrow 3$.

Next, suppose $\mathrm{Prod}(U)$ contains a connected basis $\mathscr{T}$. Then $\mathscr{T}$ satisfies the product-state constraint and is a MIS according to Lemma 3. Therefore, $\mathscr{T}$ is an EFMIS for U, which confirms the implication $3 \Rightarrow 4$.

The implication $4 \Rightarrow 5$ follows from the definition, given that any EFMIS for U can serve as a set of test states of an entanglement-free verification protocol.

Finally, suppose U can be verified by an entanglement-free protocol; let $\mathscr{T}$ be the set of test states. Then $\mathscr{T}$ is an IS contained in $\mathrm{Prod}(U)$ by Lemma 1 and is thus a connected spanning set by Lemma 2. According to Lemma 5, $\mathscr{T}$ contains a connected basis $\mathscr{S}$, which enables us to construct a reliable verification protocol for U using only d experimental settings. Therefore, $\mu(U) = d$, which confirms the implication $5 \Rightarrow 1$ and completes the proof of Theorem 2. ■

C. Minimal settings for verifying bipartite unitaries

In this section we focus on the verification of general bipartite unitaries and show that the minimum number of settings required to verify a generic bipartite unitary grows linearly with the total dimension.

Theorem 3. Suppose U is a unitary operator acting on a d-dimensional bipartite Hilbert space $\mathcal{H}$. Then the minimum number of experimental settings $\mu(U)$ required to verify U satisfies $d \leqslant \mu(U) \leqslant 2d$.

Proof. The inequality $d \leqslant \mu(U)$ follows from the general lower bound in Eq. (16). To prove the upper bound $\mu(U) \leqslant 2d$, note that the MIS $\mathscr{S}$ in Eq. (15) can serve as a set of test states; in addition, all states in $\mathscr{S}$ are product states as long as the computational basis coincides with the standard product basis. According to Theorem 1, the output state associated with each input state can be verified by either one or two measurement settings based on nonadaptive local projective measurements. Therefore, $\mu(U) \leqslant 2d$, which completes the proof of Theorem 3. ■

The following proposition clarifies the relation between $\mu(U)$ and $d_{\mathrm{Prod}}(U)$; see Appendix C for a proof.

Proposition 1. Let U be a unitary operator acting on a d-dimensional bipartite Hilbert space $\mathcal{H}$. If $d_{\mathrm{Prod}}(U) < d$, then

$$\mu(U) = d_{\mathrm{Prod}}(U) + 2[d - d_{\mathrm{Prod}}(U)]. \tag{19}$$

In the case $d_{\mathrm{Prod}}(U) = d$, we have $\mu(U) = d$ if the set Prod(U) is connected and $\mu(U) = d + 1$ otherwise.

V. TWO-QUBIT UNITARIES

In this section we discuss the basic properties of two-qubit unitaries that are relevant to studying the minimal-setting verification and entanglement-free verification presented in the next section. Here the discussion builds on the previous works Refs. [37,38].

A. Canonical form of two-qubit unitaries

Let $\mathcal{H} = \mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$ be the Hilbert space associated with a two-qubit system shared by A and B. According to Refs. [37,38], any two-qubit unitary operator U_{AB} acting on $\mathcal{H}$ can be expressed as follows:

$$U_{\mathrm{AB}} = V_{\mathrm{A}} \otimes W_{\mathrm{B}} U \tilde{V}_{\mathrm{A}} \otimes \tilde{W}_{\mathrm{B}}, \tag{20}$$

where $V_{\mathrm{A}}, W_{\mathrm{B}}, \tilde{V}_{\mathrm{A}}, \tilde{W}_{\mathrm{B}}$ are four qubit unitary operators,

$$\begin{gathered} U = U(\alpha_1, \alpha_2, \alpha_3) = e^{-iH(\alpha_1,\alpha_2,\alpha_3)}, \\ H(\alpha_1, \alpha_2, \alpha_3) = \sum_{k=1}^{3} \alpha_k H_k, \\ 0 \leqslant |\alpha_3| \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4, \\ H_1 = \sigma_1 \otimes \sigma_1, \quad H_2 = \sigma_2 \otimes \sigma_2, \quad H_3 = \sigma_3 \otimes \sigma_3, \end{gathered} \tag{21}$$

and $\sigma_1, \sigma_2, \sigma_3$ are the three Pauli operators. The operator $U(\alpha_1, \alpha_2, \alpha_3)$ can further be expressed as

$$U(\alpha_1, \alpha_2, \alpha_3) = \sum_{k=0}^{3} \zeta_k \sigma_k \otimes \sigma_k, \tag{22}$$

where σ_0 is the identity operator and the coefficients ζ_k are given by

$$\begin{aligned}
\zeta_0 &= \cos\alpha_1 \cos\alpha_2 \cos\alpha_3 - i \sin\alpha_1 \sin\alpha_2 \sin\alpha_3, \\
\zeta_1 &= \cos\alpha_1 \sin\alpha_2 \sin\alpha_3 - i \sin\alpha_1 \cos\alpha_2 \cos\alpha_3, \\
\zeta_2 &= \sin\alpha_1 \cos\alpha_2 \sin\alpha_3 - i \cos\alpha_1 \sin\alpha_2 \cos\alpha_3, \\
\zeta_3 &= \sin\alpha_1 \sin\alpha_2 \cos\alpha_3 - i \cos\alpha_1 \cos\alpha_2 \sin\alpha_3.
\end{aligned} \tag{23}$$

According to the equation

$$\begin{aligned}
\sigma_3^{\mathrm{A}} U(\alpha_1, \alpha_2, -\alpha_3)\sigma_3^{\mathrm{A}} &= U(-\alpha_1, -\alpha_2, -\alpha_3) \\
&= U^*(\alpha_1, \alpha_2, \alpha_3),
\end{aligned} \tag{24}$$

$U(\alpha_1, \alpha_2, -\alpha_3)$ is equivalent to $U^*(\alpha_1, \alpha_2, \alpha_3)$. Therefore, any two-qubit unitary operator is equivalent to $U(\alpha_1, \alpha_2, \alpha_3)$ or $U^*(\alpha_1, \alpha_2, \alpha_3)$ with

$$0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4. \tag{25}$$

Since most quantities we are interested in, such as Schmidt coefficients and the minimum number of experimental settings, are invariant under local unitary transformations and complex conjugation, so we can focus on $U(\alpha_1, \alpha_2, \alpha_3)$ with the parameter range in Eq. (25) in the following discussion.

B. Schmidt coefficients of two-qubit unitaries

To further clarify the properties of two-qubit unitary operators, we need to find suitable invariants. Given a two-qubit unitary operator U acting on the Hilbert space $\mathcal{H} = \mathcal{H}_{\mathrm{A}} \otimes \mathcal{H}_{\mathrm{B}}$, its Choi state

$$|\Psi_U\rangle := U|\Phi\rangle_{\mathrm{AA}'} \otimes |\Phi\rangle_{\mathrm{BB}'} \tag{26}$$

is a four-qubit pure state on $\mathcal{H} \otimes \mathcal{H}$, where

$$|\Phi\rangle_{\mathrm{AA}'} = \frac{1}{\sqrt{2}} \sum_k |k\rangle_{\mathrm{A}} |k\rangle_{\mathrm{A}'}, \quad |\Phi\rangle_{\mathrm{BB}'} = \frac{1}{\sqrt{2}} \sum_k |k\rangle_{\mathrm{B}} |k\rangle_{\mathrm{B}'} \tag{27}$$

are two-qubit maximally entangled states shared by parties AA′ and BB′, respectively. The Schmidt coefficients (rank) of U are defined as the Schmidt coefficients (rank) of $|\Psi_U\rangle$ with respect to the partition between AA′ and BB′. Note that the Schmidt coefficients and Schmidt rank of U are invariant under local unitary transformations.

Let

$$|\tilde{\Phi}_k\rangle = \sigma_k \otimes I|\Phi\rangle, \quad k = 0, 1, 2, 3. \tag{28}$$

Then the set $\{|\tilde{\Phi}_k\rangle\}_{k=0}^{3}$ forms a Bell basis, which is equivalent to the magic basis [39] up to overall phase factors. When $U = U(\alpha_1, \alpha_2, \alpha_3)$ is the canonical two-qubit unitary defined in Sec. V A, by virtue of Eq. (22), the Choi state $|\Psi_U\rangle$ can be expressed as

$$|\Psi_U\rangle = \sum_{k=0}^{3} \zeta_k |\tilde{\Phi}_k\rangle_{\mathrm{AA}'} \otimes |\tilde{\Phi}_k\rangle_{\mathrm{BB}'}. \tag{29}$$

Now it is clear that the Schmidt coefficients of $|\Psi_U\rangle$ with respect to the partition between AA′ and BB′ are $|\zeta_k|$ for $k = 0, 1, 2, 3$, where ζ_k are given in Eq. (23). Therefore, the two-qubit unitary $U(\alpha_1, \alpha_2, \alpha_3)$ has Schmidt coefficients $|\zeta_k|$ for $k = 0, 1, 2, 3$, which satisfy the following normalization condition:

$$|\zeta_0|^2 + |\zeta_1|^2 + |\zeta_2|^2 + |\zeta_3|^2 = 1. \tag{30}$$

Note that $U^*(\alpha_1, \alpha_2, \alpha_3)$ and $U(\alpha_1, \alpha_2, \alpha_3)$ have the same Schmidt coefficients and Schmidt rank. So we can focus on the parameter range in Eq. (25) when studying the Schmidt coefficients and Schmidt rank of $U(\alpha_1, \alpha_2, \alpha_3)$.

The Schmidt rank of $U(\alpha_1, \alpha_2, \alpha_3)$ is determined in Ref. [38] as reproduced in the following lemma, which can also be verified directly by virtue of Eq. (23).

Lemma 7. Suppose $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$. Then the Schmidt rank of $U(\alpha_1, \alpha_2, \alpha_3)$ is 1 if $\alpha_1 = \alpha_2 = \alpha_3 = 0$, is 2 if $\alpha_1 > 0$ and $\alpha_2 = \alpha_3 = 0$, and is 4 if $\alpha_1 \geqslant \alpha_2 > 0$.

The properties of Schmidt coefficients of two-qubit unitaries are summarized in Lemmas 8–10 and Corollary 2 below, which are proved in Appendix D.

Lemma 8. Suppose $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$. Then the Schmidt coefficients of $U(\alpha_1, \alpha_2, \alpha_3)$ satisfy the following relation:

$$|\zeta_0| \geqslant |\zeta_1| \geqslant |\zeta_2| \geqslant |\zeta_3| \geqslant 0. \tag{31}$$

The first inequality saturates iff $\alpha_1 = \pi/4$; the second inequality saturates iff $\alpha_2 = \alpha_1$; the third inequality saturates iff $\alpha_1 = \frac{\pi}{4}$ or $\alpha_3 = \alpha_2$; and the last inequality saturates iff $\alpha_2 = \alpha_3 = 0$.

Lemma 9. Suppose $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$. Then the Schmidt coefficients of $U(\alpha_1, \alpha_2, \alpha_3)$ satisfy the condition $|\zeta_0| > |\zeta_1| = |\zeta_2| = |\zeta_3| > 0$ iff $0 < \alpha_3 = \alpha_2 = \alpha_1 < \pi/4$.

When $\alpha_2 = \alpha_1 = \pi/4$, all Schmidt coefficients of the unitary operator $U(\alpha_1, \alpha_2, \alpha_3)$ are equal to $1/2$ irrespective of the value of α_3 [cf. Eq. (23)]. Such coincidence can also occur when $\alpha_1 = \pi/4$ and $\alpha_2 \leqslant \pi/4$, in which case we have

$$\begin{aligned}
|\zeta_0|^2 = |\zeta_1|^2 &= \tfrac{1}{4}[1 + \cos(2\alpha_2)\cos(2\alpha_3)], \\
|\zeta_2|^2 = |\zeta_3|^2 &= \tfrac{1}{4}[1 - \cos(2\alpha_2)\cos(2\alpha_3)],
\end{aligned} \tag{32}$$

so all Schmidt coefficients of $U(\alpha_1, \alpha_2, \alpha_3)$ are completely determined by the product $\cos(2\alpha_2)\cos(2\alpha_3)$ or any given Schmidt coefficient, as illustrated in Fig. 1. A specific choice of two inequivalent unitary operators with the same Schmidt coefficients is shown in Appendix E. On the other hand, the following lemma shows that such coincidence of Schmidt coefficients cannot occur when $\alpha_1 < \pi/4$.

Lemma 10. Suppose $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$ and $0 \leqslant \alpha_3' \leqslant \alpha_2' \leqslant \alpha_1' \leqslant \pi/4$. Then $U(\alpha_1, \alpha_2, \alpha_3)$ and $U(\alpha_1', \alpha_2', \alpha_3')$ have the same Schmidt coefficients iff one of the following two conditions holds:

$$\alpha_1 = \alpha_1', \quad \alpha_2 = \alpha_2', \quad \alpha_3 = \alpha_3', \tag{33}$$

$$\alpha_1 = \alpha_1' = \frac{\pi}{4}, \quad \cos(2\alpha_2)\cos(2\alpha_3) = \cos(2\alpha_2')\cos(2\alpha_3'). \tag{34}$$

Corollary 2. Suppose U and U' are two two-qubit unitary operators that have the same Schmidt coefficients s_0, s_1, s_2, s_3,

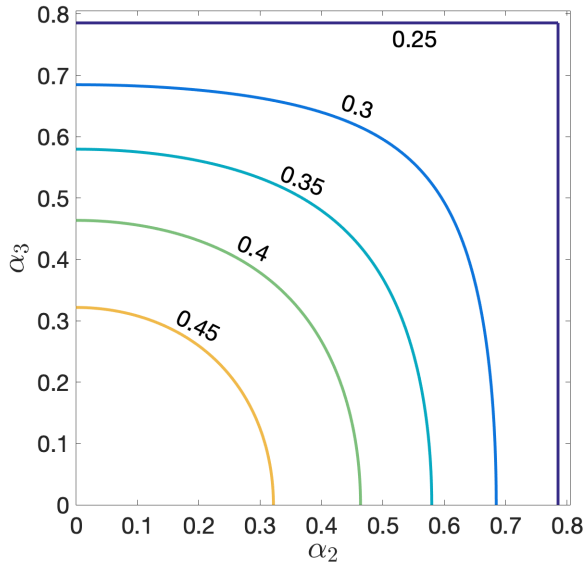

FIG. 1. Contour plot of $|\zeta_0|^2$ in the plane of α_2-α_3, where $|\zeta_0|$ is the largest Schmidt coefficient of $U(\alpha_1 = \pi/4, \alpha_2, \alpha_3)$. The other three Schmidt coefficients are determined by $|\zeta_0|^2$ according to Eq. (32). All unitaries corresponding to a given contour line share the same Schmidt coefficients.

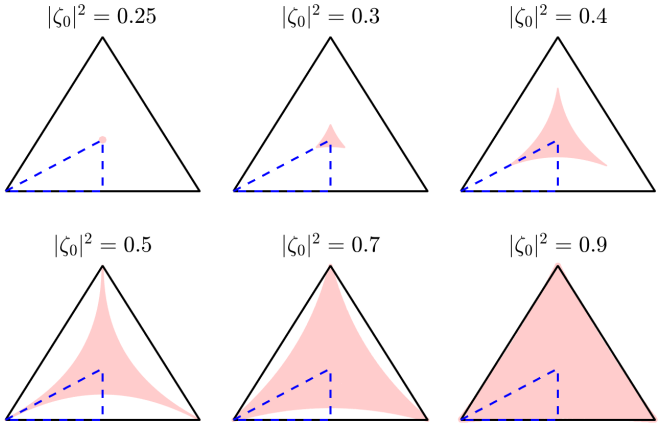

FIG. 2. Accessible Schmidt coefficients of two-qubit unitaries $U(\alpha_1, \alpha_2, \alpha_3)$ for the parameter range $0 \leqslant \alpha_3, \alpha_2, \alpha_1 \leqslant \pi/4$. The red-shaded region in each ternary diagram represents the set of accessible points specified by the barycentric coordinate $(\xi_1, \xi_2, \xi_3) = (|\zeta_1|^2, |\zeta_2|^2, |\zeta_3|^2)/(1 - |\zeta_0|^2)$, where $|\zeta_0|$ is the largest Schmidt coefficient, and $|\zeta_1|, |\zeta_2|, |\zeta_3|$ are the other three Schmidt coefficients; cf. Eq. (23). The left, right, and top corners of the big black triangle correspond to the coordinates (1,0,0), (0,1,0), and (0,0,1), respectively. The shaded region within each blue dashed triangle represents the set of accessible points for the smaller parameter range $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$, in which case $|\zeta_1|, |\zeta_2|, |\zeta_3|$ are in nonincreasing order.

which satisfy $s_0 > s_1 \geqslant s_2 \geqslant s_3$. Then U' is equivalent to either U or U^* under local unitary transformations. In other words, U' can be expressed as

$$U' = V_A \otimes W_B \tilde{U} \tilde{V}_A \otimes \tilde{W}_B, \tag{35}$$

where $\tilde{U} = U$ or U^*, and $V_A, W_B, \tilde{V}_A, \tilde{W}_B$ are suitable qubit unitary operators.

The above analysis clarifies the properties of Schmidt coefficients of two-qubit unitary operators. Given the assumption $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$, the Schmidt coefficients of $U(\alpha_1, \alpha_2, \alpha_3)$ must satisfy the conditions in Eqs. (30) and (31). However, the two conditions are not enough to guarantee the existence of a two-qubit unitary with a given set of Schmidt coefficients. To demonstrate this point, we can determine the ranges of the four Schmidt coefficients of $U(\alpha_1, \alpha_2, \alpha_3)$ by virtue of Eq. (23), with the result

$$\begin{aligned} &\frac{1}{2} \leqslant |\zeta_0| \leqslant 1, \quad 0 \leqslant |\zeta_1| \leqslant \frac{1}{\sqrt{2}}, \\ &0 \leqslant |\zeta_2| \leqslant \frac{1}{2}, \quad 0 \leqslant |\zeta_3| \leqslant \frac{1}{2}. \end{aligned} \tag{36}$$

By contrast, the constraints in Eqs. (30) and (31) alone would imply that $0 \leqslant |\zeta_2| \leqslant 1/\sqrt{3}$.

To further clarify the constraints on the Schmidt coefficients of two-qubit unitaries, it is convenient to introduce some additional variables. Let

$$\xi_j = \frac{|\zeta_j|^2}{1 - |\zeta_0|^2}, \quad j = 1, 2, 3. \tag{37}$$

Geometrically, $(|\zeta_0|^2, |\zeta_1|^2, |\zeta_2|^2, |\zeta_3|^2)$ can be regarded as the barycentric coordinate of a point in a three-dimensional probability simplex according to Eq. (30). The accessible Schmidt coefficients correspond to a subset in the probability simplex. In addition, when $|\zeta_0| < 1$, (ξ_1, ξ_2, ξ_3) is the barycentric coordinate of a point in a two-dimensional probability simplex, which corresponds to a normalized cross section of the three-dimensional probability simplex.

Figure 2 illustrates the accessible region of Schmidt coefficients for six normalized cross sections associated with six distinct values of $|\zeta_0|$, where $|\zeta_0|$ is the largest Schmidt coefficient. The shaded region within each blue dashed triangle represents the set of accessible ordered Schmidt coefficients as determined by (ξ_1, ξ_2, ξ_3) for the parameter range $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$. By contrast, the whole red-shaded region in each ternary diagram represents the set of accessible Schmidt coefficients for the larger parameter range $0 \leqslant \alpha_3, \alpha_2, \alpha_1 \leqslant \pi/4$. In the latter case, Eq. (31) no longer applies, but we have

$$|\zeta_0| \geqslant |\zeta_j|, \quad j = 1, 2, 3, \tag{38}$$

so $|\zeta_0|$ is still the largest Schmidt coefficient.

VI. VERIFICATION OF TWO-QUBIT UNITARIES WITH MINIMAL SETTINGS

A. Product-state constraint

To construct a minimal-setting protocol for verifying the two-qubit unitary $U(\alpha_1, \alpha_2, \alpha_3)$, we first need to clarify the product-state constraint, which is tied to the set $\mathrm{Prod}(U)$ defined in Eq. (17).

To better understand the product-state constraint, it is instructive to consider the magic basis [39], which is composed

of the four maximally entangled states:

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi_2\rangle = \frac{i}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Phi_3\rangle = \frac{i}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Phi_4\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{39}$$

Suppose the input state $|\phi_0\rangle$ has the form $|\phi_0\rangle = \sum_{k=1}^4 \gamma_k|\Phi_k\rangle$ with $\sum_{k=1}^4 |\gamma_k|^2 = 1$. Then the concurrence [39] of the input state reads

$$C(|\phi_0\rangle) = \left|\sum_{k=1}^4 \gamma_k^2\right|. \tag{40}$$

After the action of $U(\alpha_1, \alpha_2, \alpha_3)$, the output state has the expansion

$$|\phi\rangle = \sum_{k=1}^4 e^{-i\lambda_k}\gamma_k|\Phi_k\rangle, \tag{41}$$

where

$$\begin{aligned}\lambda_1 &= \alpha_1 - \alpha_2 + \alpha_3,\\ \lambda_2 &= -\alpha_1 + \alpha_2 + \alpha_3,\\ \lambda_3 &= \alpha_1 + \alpha_2 - \alpha_3,\\ \lambda_4 &= -\alpha_1 - \alpha_2 - \alpha_3.\end{aligned} \tag{42}$$

The concurrence of the output state reads

$$C(|\phi\rangle) = \left|\sum_{k=1}^4 e^{-2i\lambda_k}\gamma_k^2\right|. \tag{43}$$

The product-state constraint demands that $C(|\phi_0\rangle) = 0$ and $C(|\phi\rangle) = 0$:

$$\sum_{k=1}^4 \gamma_k^2 = 0, \quad \sum_{k=1}^4 e^{-2i\lambda_k}\gamma_k^2 = 0. \tag{44}$$

When $0 < \alpha_1 + \alpha_2 < \pi/2$, Eq. (44) is equivalent to the following equations:

$$\begin{aligned}&\gamma_3^2 = r_{31}\gamma_1^2 + r_{32}\gamma_2^2, \quad \gamma_4^2 = r_{41}\gamma_1^2 + r_{42}\gamma_2^2,\\ &r_{31} = \exp[i(2\alpha_2 - 2\alpha_3 + \pi)]\frac{\sin(2\alpha_1 + 2\alpha_3)}{\sin(2\alpha_1 + 2\alpha_2)},\\ &r_{32} = \exp[i(2\alpha_1 - 2\alpha_3 + \pi)]\frac{\sin(2\alpha_2 + 2\alpha_3)}{\sin(2\alpha_1 + 2\alpha_2)},\\ &r_{41} = \exp[i(-2\alpha_1 - 2\alpha_3 + \pi)]\frac{\sin(2\alpha_2 - 2\alpha_3)}{\sin(2\alpha_1 + 2\alpha_2)},\\ &r_{42} = \exp[i(-2\alpha_2 - 2\alpha_3 + \pi)]\frac{\sin(2\alpha_1 - 2\alpha_3)}{\sin(2\alpha_1 + 2\alpha_2)}.\end{aligned} \tag{45}$$

If the product-state constraint holds, then γ_3^2 and γ_4^2 are completely determined by γ_1 and γ_2. Taking into account the normalization condition $\sum_{k=1}^4 |\gamma_k|^2 = 1$ and ignoring the overall phase factors, we can deduce that there are in general two free real parameters.

When $\alpha_1 + \alpha_2 = 0$ or $\alpha_1 + \alpha_2 = \pi/2$, Eq. (45) does not apply, in which case it is more convenient to consider the product-state constraint in the computational basis. Now any two-qubit pure product state can be expressed as

$$|\phi_0\rangle = \begin{pmatrix}a_1\\ a_2\end{pmatrix} \otimes \begin{pmatrix}b_1\\ b_2\end{pmatrix} = \begin{pmatrix}a_1b_1\\ a_1b_2\\ a_2b_1\\ a_2b_2\end{pmatrix}. \tag{46}$$

After the action of $U(\alpha_1, \alpha_2, \alpha_3)$, the output state reads

$$|\phi\rangle = U|\phi_0\rangle = \begin{pmatrix}c_1\\ c_2\\ c_3\\ c_4\end{pmatrix}, \tag{47}$$

where

$$\begin{aligned}c_1 &= (\zeta_0 + \zeta_3)a_1b_1 + (\zeta_1 - \zeta_2)a_2b_2,\\ c_2 &= (\zeta_0 - \zeta_3)a_1b_2 + (\zeta_1 + \zeta_2)a_2b_1,\\ c_3 &= (\zeta_0 - \zeta_3)a_2b_1 + (\zeta_1 + \zeta_2)a_1b_2,\\ c_4 &= (\zeta_0 + \zeta_3)a_2b_2 + (\zeta_1 - \zeta_2)a_1b_1,\end{aligned} \tag{48}$$

and ζ_k for $k = 0, 1, 2, 3$ are defined in Eq. (23). According to Ref. [39], the concurrence C of the output state reads

$$C(|\phi\rangle) = 2|c_1c_4 - c_2c_3|. \tag{49}$$

To satisfy the product-state constraint, the concurrence $C(|\phi\rangle)$ should vanish, which means

$$c_1c_4 - c_2c_3 = 0. \tag{50}$$

B. Minimal setting and entanglement-free verification of two-qubit unitaries

In this section we determine the minimum number of experimental settings required to verify an arbitrary two-qubit unitary and derive a simple criterion for determining whether a general two-qubit unitary can be verified by an entanglement-free protocol. Our main result is summarized in the following theorem.

Theorem 4. Suppose U is a two-qubit unitary operator with Schmidt coefficients s_0, s_1, s_2, s_3 arranged in nonincreasing order. Then

$$\mu(U) = \begin{cases}5 & \text{if } s_0 > s_1 = s_2 = s_3 > 0,\\ 4 & \text{otherwise,}\end{cases} \tag{51}$$

and the unitary operator U can be verified by an entanglement-free protocol unless $s_0 > s_1 = s_2 = s_3 > 0$.

Theorem 4 is a corollary of Lemma 9 in Sec. V B and Theorem 5 below. Define

$$\mathcal{S} := \left\{(\alpha_1, \alpha_2, \alpha_3)\middle| 0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \frac{\pi}{4}\right\}, \tag{52}$$

$$\mathcal{S}_{\mathrm{E}} := \left\{(\alpha, \alpha, \alpha)\middle| 0 < \alpha < \frac{\pi}{4}\right\}, \quad \mathcal{S}_{\mathrm{EF}} := \mathcal{S} \setminus \mathcal{S}_{\mathrm{E}}. \tag{53}$$

Theorem 5. Suppose $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$. Then

$$\mu(U(\alpha_1, \alpha_2, \alpha_3)) = \begin{cases}4 & \text{if } (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{S}_{\mathrm{EF}},\\ 5 & \text{if } (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{S}_{\mathrm{E}}.\end{cases} \tag{54}$$

$U(\alpha_1, \alpha_2, \alpha_3)$ can be verified by an entanglement-free protocol iff $(\alpha_1, \alpha_2, \alpha_3) \in \mathcal{S}_{\mathrm{EF}}$.

Proof. To prove Theorem 5, it suffices to prove Eq. (54), which implies the last statement in the theorem according to

Theorem 2. To prove Eq. (54), we shall first construct a four-setting entanglement-free protocol for verifying $U(\alpha_1, \alpha_2, \alpha_3)$ when $(\alpha_1, \alpha_2, \alpha_3) \in \mathcal{S}_{\mathrm{EF}}$. To this end we need to consider three different cases and construct an EFMIS in each case (cf. Theorem 2).

(1) $\alpha_1 = \alpha_2 = \pi/4$

In this case, according to Eqs. (47)–(50), the product-state constraint under the computational basis reads

$$a_1 a_2 b_1 b_2 \cos(2\alpha_3) = 0. \tag{55}$$

In addition, $|\zeta_0| = |\zeta_1| = |\zeta_2| = |\zeta_3| = 1/2$ according to Eq. (23). So a pure product state satisfies the product-state constraint if one of the reduced states is an eigenstate of σ_3. Based on this observation we can construct an EFMIS as follows:

$$\begin{aligned} |\phi_1\rangle &= |0+\rangle, \quad |\phi_2\rangle = |1+\rangle, \\ |\phi_3\rangle &= |-0\rangle, \quad |\phi_4\rangle = |+0\rangle, \end{aligned} \tag{56}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ are two eigenstates of σ_1. Note that these product states remain as product states after the action of $U(\alpha_1, \alpha_2, \alpha_3)$ as expected. In addition, the transition graph of these states is connected. Therefore, $U(\alpha_1, \alpha_2, \alpha_3)$ can be verified by an entanglement-free protocol based on four experimental settings, which confirms Eq. (54).

(2) $\alpha_1 = \alpha_2 = \alpha_3 = 0$

In this case, $U(\alpha_1, \alpha_2, \alpha_3)$ is equal to the identity, so all product states satisfy the product-state constraint, and it is easy to construct an EFMIS. Actually, the EFMIS constructed in case 1 still works. Therefore, $U(\alpha_1, \alpha_2, \alpha_3)$ can be verified by an entanglement-free protocol based on four experimental settings, which confirms Eq. (54).

(3) $\alpha_1 > \alpha_3$ and $\alpha_2 < \pi/4$.

Now, it is more convenient to consider the magic basis. Suppose the state $|\phi_0\rangle$ has the expansion $|\phi_0\rangle = \sum_{k=1}^4 \gamma_k |\Phi_k\rangle$ with the normalization condition $\sum_{k=1}^4 |\gamma_k|^2 = 1$. Then the product-state constraint is satisfied if the coefficients $\gamma_1^2, \gamma_2^2, \gamma_3^2, \gamma_4^2$ have the form as shown in Appendix F. Moreover, an EFMIS can be constructed as follows (in the magic basis):

$$\begin{aligned} |\phi_1\rangle &= \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \end{pmatrix}, \quad |\phi_2\rangle = \begin{pmatrix} \gamma_1 \\ -\gamma_2 \\ \gamma_3 \\ \gamma_4 \end{pmatrix}, \\ |\phi_3\rangle &= \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ -\gamma_4 \end{pmatrix}, \quad |\phi_4\rangle = \begin{pmatrix} -\gamma_1 \\ \gamma_2 \\ \gamma_3 \\ -\gamma_4 \end{pmatrix}. \end{aligned} \tag{57}$$

Therefore, $U(\alpha_1, \alpha_2, \alpha_3)$ can be verified by an entanglement-free protocol based on four experimental settings, which confirms Eq. (54).

To complete the proof of Theorem 5, it remains to determine $\mu(U(\alpha_1, \alpha_2, \alpha_3))$ in the case $(\alpha_1, \alpha_2, \alpha_3) \in \mathcal{S}_{\mathrm{E}}$, which means $0 < \alpha_1 = \alpha_2 = \alpha_3 < \pi/4$. Suppose the input state $|\phi_0\rangle$ has the expansion $|\phi_0\rangle = \sum_{k=1}^4 \gamma_k |\Phi_k\rangle$ with $\sum_{k=1}^4 |\gamma_k|^2 = 1$ in the magic basis. According to Eq. (45), the product-state constraint amounts to the following equality:

$$(\gamma_1^2, \gamma_2^2, \gamma_3^2, \gamma_4^2) = (\gamma_1^2, \gamma_2^2, -\gamma_1^2 - \gamma_2^2, 0), \tag{58}$$

which implies that $d_{\mathrm{Prod}}(U) = 3$. So $U(\alpha_1, \alpha_2, \alpha_3)$ cannot be verified by an entanglement-free protocol according to Theorem 2. Nevertheless, $U(\alpha_1, \alpha_2, \alpha_3)$ can be verified by a five-setting protocol based on local operations, given that $\mu(U(\alpha_1, \alpha_2, \alpha_3)) = 5$ according to Proposition 1. This result confirms Eq. (54) and completes the proof of Theorem 5. ■

Next, we generalize Theorem 5 to the whole parameter range $0 \leqslant \alpha_3, \alpha_2, \alpha_1 < 2\pi$. Define

$$\tilde{\mathcal{S}} := \{(\alpha_1, \alpha_2, \alpha_3) | 0 \leqslant \alpha_3, \alpha_2, \alpha_1 < 2\pi\}, \tag{59}$$

$$\begin{aligned} \tilde{\mathcal{S}}_{\mathrm{E}} := \Bigg\{ \left(\frac{\pi}{2} k_1 + \frac{\pi}{4} \pm \alpha, \frac{\pi}{2} k_2 + \frac{\pi}{4} \pm \alpha, \frac{\pi}{2} k_3 + \frac{\pi}{4} \pm \alpha \right) \Bigg| \\ 0 < \alpha < \frac{\pi}{4}, \quad k_1, k_2, k_3 = 0, 1, 2, 3 \Bigg\}, \end{aligned} \tag{60}$$

$$\tilde{\mathcal{S}}_{\mathrm{EF}} := \tilde{\mathcal{S}} \setminus \tilde{\mathcal{S}}_{\mathrm{E}}. \tag{61}$$

The following corollary is proved in Appendix G.

Corollary 3. Suppose $0 \leqslant \alpha_3, \alpha_2, \alpha_1 < 2\pi$. Then

$$\mu(U(\alpha_1, \alpha_2, \alpha_3)) = \begin{cases} 4 & \text{if } (\alpha_1, \alpha_2, \alpha_3) \in \tilde{\mathcal{S}}_{\mathrm{EF}}, \\ 5 & \text{if } (\alpha_1, \alpha_2, \alpha_3) \in \tilde{\mathcal{S}}_{\mathrm{E}}. \end{cases} \tag{62}$$

$U(\alpha_1, \alpha_2, \alpha_3)$ can be verified by an entanglement-free protocol iff $(\alpha_1, \alpha_2, \alpha_3) \in \tilde{\mathcal{S}}_{\mathrm{EF}}$.

Theorem 5 and Corollary 3 imply that generic two-qubit unitary transformations (except for a set of measure zero) can be verified by entanglement-free protocols based on four experimental settings. In principle we can reach arbitrarily high precision as long as sufficiently many tests can be performed. Nevertheless, certain special unitary transformations cannot be verified by entanglement-free protocols, in which case five experimental settings are necessary. Note that the minimum number of settings is not continuous, which is expected for a discrete figure of merit. For each unitary U in the later case, we can find a nearby unitary U' that can be verified by an entanglement-free protocol. In this way U can be verified approximately by an entanglement-free protocol. However, the precision is limited by the entanglement infidelity between U' and U; in addition, the target unitary transformation U cannot pass all the tests with certainty. To enhance the precision, we can find a better approximation to U, but the precision is still limited for any given approximation. Although any two-qubit unitary transformation can be verified with five measurement settings (only four settings in the generic case), quite often the sample efficiency can be improved by increasing the number of measurement settings. The tradeoff between the sample efficiency and the number of experimental settings deserves further studies.

C. Examples

In this section we present explicit EFMISs for several well-known two-qubit gates, from which entanglement-free verification protocols can be constructed immediately.

1. CNOT

The CNOT gate is equivalent to $U(\frac{\pi}{4},0,0)$ according to the following decomposition:

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}=V_{\rm A}\otimes W_{\rm B}U\left(\frac{\pi}{4},0,0\right)\tilde{V}_{\rm A}\otimes\tilde{W}_{\rm B},\quad(63)$$

where

$$V_{\rm A}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\i&-i\end{pmatrix},\quad \tilde{V}_{\rm A}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix},$$
$$W_{\rm B}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&i\\-i&-1\end{pmatrix},\quad \tilde{W}_{\rm B}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}.\quad(64)$$

To construct an entanglement-free protocol for verifying the CNOT gate, it suffices to construct an EFMIS. To this end, we can first construct an EFMIS for $U(\frac{\pi}{4},0,0)$ and then apply a suitable local unitary transformation, although it is easy to construct an EFMIS for the CNOT gate directly. According to Eqs. (47)–(50), the product-state constraint for $U(\frac{\pi}{4},0,0)$ under the computational basis can be expressed as

$$\left(a_1^2-a_2^2\right)\left(b_1^2-b_2^2\right)=0.\quad(65)$$

A product state satisfies the constraint iff one of the reduced states is an eigenstate of σ_1. Based on this observation, an EFMIS can be constructed as

$$|\phi_1\rangle=|0+\rangle,\quad |\phi_2\rangle=|1+\rangle,$$
$$|\phi_3\rangle=|-0\rangle,\quad |\phi_4\rangle=|+0\rangle,\quad(66)$$

where $|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$ are the two eigenstates of σ_1. By multiplying the local unitary operator $(\tilde{V}_{\rm A}\otimes\tilde{W}_{\rm B})^\dagger$, we can construct an EFMIS for the CNOT gate as

$$|\tilde{\phi}_1\rangle=|+-\rangle,\quad |\tilde{\phi}_2\rangle=|--\rangle,$$
$$|\tilde{\phi}_3\rangle=|10\rangle,\quad |\tilde{\phi}_4\rangle=|00\rangle.\quad(67)$$

2. CZ

The CZ gate is equivalent to the CNOT gate according to the identity

$$\mathrm{CZ}=(I\otimes H)\mathrm{CNOT}(I\otimes H),\quad(68)$$

where H is the Hadamard gate. Therefore, any EFMIS for the CNOT gate can be turned into an EFMIS for the CZ gate by simply applying the local unitary operator $I\otimes H$. For example, one EFMIS for the CZ gate can be constructed by applying $I\otimes H$ to the states in Eq. (67), which yields

$$|\phi_1\rangle=|+1\rangle,\quad |\phi_2\rangle=|-1\rangle,$$
$$|\phi_3\rangle=|1+\rangle,\quad |\phi_4\rangle=|0+\rangle.\quad(69)$$

3. C-Phase

The C-Phase gate with nontrivial phase $0<\varphi<2\pi$ reads

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&e^{i\varphi}\end{pmatrix}.\quad(70)$$

The conjugate of the C-Phase gate is equivalent to $U(\frac{\varphi}{4},0,0)$ according to the following decomposition:

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&e^{-i\varphi}\end{pmatrix}=V_{\rm A}\otimes W_{\rm B}U\left(\frac{\varphi}{4},0,0\right)\tilde{V}_{\rm A}\otimes\tilde{W}_{\rm B},\quad(71)$$

where

$$V_{\rm A}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\-e^{-i\frac{\varphi}{2}}&e^{-i\frac{\varphi}{2}}\end{pmatrix},\quad \tilde{V}_{\rm A}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&-1\\1&1\end{pmatrix},$$
$$W_{\rm B}=\frac{1}{\sqrt{2}}\begin{pmatrix}e^{i\frac{\varphi}{4}}&e^{i\frac{\varphi}{4}}\\e^{-i\frac{\varphi}{4}}&-e^{-i\frac{\varphi}{4}}\end{pmatrix},\quad \tilde{W}_{\rm B}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}.\quad(72)$$

According to Eqs. (47)–(50), the product-state constraint for $U(\frac{\varphi}{4},0,0)$ under the computational basis can be expressed as

$$\left(a_1^2-a_2^2\right)\left(b_1^2-b_2^2\right)\sin\frac{\varphi}{2}=0.\quad(73)$$

A product state satisfies the constraint if one of the reduced states is an eigenstate of σ_1. So the states in Eq. (66) also form an EFMIS for $U(\frac{\varphi}{4},0,0)$. By applying the local unitary operator $(\tilde{V}_{\rm A}\otimes\tilde{W}_{\rm B})^\dagger$, we can construct an EFMIS for the C-Phase gate (and its conjugate) as

$$|\phi_1\rangle=|-0\rangle,\quad |\phi_2\rangle=|+0\rangle,$$
$$|\phi_3\rangle=-|1+\rangle,\quad |\phi_4\rangle=|0+\rangle.\quad(74)$$

Note that this EFMIS applies to the C-Phase gate with an arbitrary phase. Incidentally, the four states in Eq. (69) also form an EFMIS for the C-Phase gate with an arbitrary phase.

4. SWAP

The SWAP gate is equal to $U(\frac{\pi}{4},\frac{\pi}{4},\frac{\pi}{4})$ up to an overall phase factor according to the following identity:

$$\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}=\frac{1+i}{\sqrt{2}}U\left(\frac{\pi}{4},\frac{\pi}{4},\frac{\pi}{4}\right).\quad(75)$$

Due to this identity, the EFMIS for $U(\frac{\pi}{4},\frac{\pi}{4},\frac{\pi}{4})$ presented in Eq. (56) is also an EFMIS for the SWAP gate. In addition, any product state satisfies the product-state constraint, so any MIS composed of product states is an EFMIS for the SWAP gate.

VII. SUMMARY

We studied systematically QSV and QGV with a focus on the number of experimental settings based on local operations. We showed that any bipartite pure state can be verified by only two measurement settings based on local projective measurements. The minimum number of experimental settings required to verify a bipartite unitary increases linearly with the total dimension. In addition, we introduced the concept of entanglement-free verification, which does not generate any entanglement in the verification procedure. The connection with minimal-setting verification is also clarified. Finally, we determined the minimum number of experimental settings required to verify each two-qubit unitary. It turns

out any two-qubit unitary can be verified using at most five settings based on local operations, and a generic two-qubit unitary requires only four settings. In the course of study we derived a number of results on two-qubit unitaries and their Schmidt coefficients, which are of independent interest. Our work significantly promotes the current understanding on QSV and QGV with respect to the number of required experimental settings, which is instructive for both theoretical studies and practical applications. In addition, our work shows that verification protocols with minimal settings are in general not balanced and thus do not have natural analogs in QSV, which reflects a key distinction between QGV and QSV that is not recognized before. In the future it would be desirable to generalize our results to the multipartite setting.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (Grants No. 92165109 and No. 11875110) and Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01).

APPENDIX A: PROOFS OF LEMMAS 4 AND 5

Proof of Lemma 4. Suppose on the contrary that $\mathscr{S}$ is a maximal CLIS contained in $\mathscr{T}$ and that $\mathscr{S}$ is not a basis for $\mathcal{H}$. Let $\mathcal{H}_1$ be the span of $\mathscr{S}$ and let $\mathcal{H}_2$ be the orthogonal complement of $\mathcal{H}_1$. Then $\mathcal{H}_1$ and $\mathcal{H}_2$ have dimensions at least one; in addition, $\mathscr{T}$ contains a ket $|\psi\rangle$ that is supported neither in $\mathcal{H}_1$ nor in $\mathcal{H}_2$ since otherwise $\mathscr{T}$ cannot be connected. Therefore, $\mathscr{S}\cup\{|\psi\rangle\}\subseteq\mathscr{T}$ is a CLIS that contains $\mathscr{S}$ as a proper subset. This contradiction completes the proof of Lemma 4. ■

Proof of Lemma 5. The first statement in Lemma 5 follows from Lemma 4; note that any maximal CLIS contained in the connected spanning set forms a connected basis. To prove the second statement, suppose $\mathscr{T}$ is a set of kets in $\mathcal{H}$ and contains a connected spanning set $\mathscr{S}$. Then $\mathscr{T}$ is also a spanning set. In addition, each ket in $\mathscr{T}$ is not orthogonal to at least one ket in $\mathscr{S}$. As a consequence, the transition graph of $\mathscr{T}$ is connected given that the transition graph of $\mathscr{S}$ is connected. So $\mathscr{T}$ is itself a connected spanning set, which completes the proof of Lemma 5. ■

APPENDIX B: PROOF OF LEMMA 6

Proof. For an entanglement-free verification protocol, the conclusion follows from the very definition. So it remains to consider the case in which the verification protocol is composed of d experimental settings based on local operations. Then we have $d\leqslant|\mathscr{T}|\leqslant d$, where the lower bound follows from the fact that $\mathscr{T}$ is a spanning set and the upper bound follows from the fact that the number of experimental settings cannot be smaller than the number of test states. It follows that $|\mathscr{T}|=d$ and $\mathscr{T}$ is composed of d product states. In addition, the number of experimental settings is equal to the number of test states. So the output state associated with each input state in $\mathscr{T}$ is also a product state given that at least two measurement settings are required to verify an entangled output state (cf. Theorem 1). Therefore, $\mathscr{T}\subseteq\mathrm{Prod}(U)$, which completes the proof of Lemma 6. ■

APPENDIX C: PROOF OF PROPOSITION 1

Proof. To prove Eq. (19) in Proposition 1, we shall first prove the following inequality:

$$\mu(U)\geqslant d_{\mathrm{Prod}}(U)+2[d-d_{\mathrm{Prod}}(U)]. \tag{C1}$$

Let $\mathscr{T}$ be the set of test states of a verification protocol of U that can be realized by $\mu(U)$ experimental settings. Then $\mathscr{T}$ is a finite spanning set (of $\mathcal{H}$) whose cardinality satisfies $d\leqslant|\mathscr{T}|\leqslant\mu(U)$. Let $\mathscr{T}'=\mathrm{Prod}(U)\cap\mathscr{T}$ and $\mathscr{T}''=\mathscr{T}\setminus\mathscr{T}'$. Then

$$\dim\mathrm{span}(\mathscr{T}')\leqslant d_{\mathrm{Prod}}(U), \tag{C2}$$

$$\dim\mathrm{span}(\mathscr{T}'')\geqslant d-\dim\mathrm{span}(\mathscr{T}')\geqslant d-d_{\mathrm{Prod}}(U). \tag{C3}$$

The output state associated with each input state in $\mathscr{T}'$ is a product state, so one measurement setting is required to verify it. By contrast, the output state associated with each input state in $\mathscr{T}''$ is entangled, so at least two measurement settings are required to verify it according to Theorem 1. Therefore,

$$\begin{aligned}\mu(U)&\geqslant|\mathscr{T}'|+2|\mathscr{T}''|\geqslant\dim\mathrm{span}(\mathscr{T}')+2\dim\mathrm{span}(\mathscr{T}'')\\&\geqslant\dim\mathrm{span}(\mathscr{T}')+2[d-\dim\mathrm{span}(\mathscr{T}')]\\&=2d-\dim\mathrm{span}(\mathscr{T}')\geqslant 2d-d_{\mathrm{Prod}}(U),\end{aligned} \tag{C4}$$

which implies Eq. (C1).

Next, suppose $d_{\mathrm{Prod}}(U)<d$. To prove Eq. (19), it remains to prove the opposite inequality to Eq. (C1). Let $\mathscr{S}$ be a subset of $\mathrm{Prod}(U)$ that is composed of $d_{\mathrm{Prod}}(U)$ linearly independent states. By adding $d-d_{\mathrm{Prod}}(U)-1$ suitable product states, we can construct a set $\mathscr{S}'$ of $d-1$ linearly independent product states. Now we can add a product state that is not in the span of $\mathscr{S}'$ and is not orthogonal to any state in $\mathscr{S}'$. The resulting set $\mathscr{S}''$ forms a connected basis for $\mathcal{H}$ and so can identify unitaries. In addition, the output state associated with each state in $\mathscr{S}$ is a product state and so can be verified by one measurement setting based on a local projective measurement. The output state associated with each state in $\mathscr{S}''\setminus\mathscr{S}$ can be verified by two measurement settings according to Theorem 1. Therefore,

$$\begin{aligned}\mu(U)&\leqslant|\mathscr{S}|+2|\mathscr{S}''\setminus\mathscr{S}|=d_{\mathrm{Prod}}(U)+2[d-d_{\mathrm{Prod}}(U)]\\&=2d-d_{\mathrm{Prod}}(U),\end{aligned} \tag{C5}$$

which implies Eq. (19) given the opposite inequality in Eq. (C1)

Now let us consider the case in which $d_{\mathrm{Prod}}(U)=d$. If the set $\mathrm{Prod}(U)$ is connected, then it contains a connected basis composed of product states by Lemma 5. Moreover, the output state associated with each state in the basis is also a product state and so can be verified by one measurement setting. Therefore, U can be verified by d experimental settings, which means $\mu(U)=d$.

If the set $\mathrm{Prod}(U)$ is not connected, then the set of test states of any valid verification protocol for U contains at least one state not contained in $\mathrm{Prod}(U)$, which implies that $\mu(U)\geqslant d+1$ [cf. the derivation that leads to Eq. (C1)]. To complete the proof of Proposition 1, it remains to construct

a verification protocol for U that requires only $d+1$ experimental settings. Let $\mathscr{S}$ be a subset of $\mathrm{Prod}(U)$ that is composed of $d-1$ linearly independent states. We can add a product state that is not in the span of $\mathscr{S}$ and is not orthogonal to any state in $\mathscr{S}$. The resulting set $\mathscr{S}'$ forms a connected basis for $\mathcal{H}$ and so can identify unitaries. In addition, the output state associated with each state in $\mathscr{S}$ is a product and so can be verified by one measurement setting based on a local projective measurement. The output state associated with the additional product state can be verified by two measurement settings according to Theorem 1. Therefore, U can be verified by $d+1$ experimental settings, that is, $\mu(U)\leqslant d+1$. In conjunction with the opposite inequality derived above, we conclude that $\mu(U)=d+1$ when $d_{\mathrm{Prod}}(U)=d$ and the set $\mathrm{Prod}(U)$ is not connected. ■

APPENDIX D: PROOFS OF LEMMAS 8–10 AND COROLLARY 2

Proof of Lemma 8. Let $c_j=\cos\alpha_j$ and $s_j=\sin\alpha_j$ for $j=1,2,3$. Then the four Schmidt coefficients of $U(\alpha_1,\alpha_2,\alpha_3)$ can be expressed as follows:

$$\begin{aligned}|\zeta_0|&=\sqrt{c_1^2c_2^2c_3^2+s_1^2s_2^2s_3^2},\\ |\zeta_1|&=\sqrt{c_1^2s_2^2s_3^2+s_1^2c_2^2c_3^2},\\ |\zeta_2|&=\sqrt{s_1^2c_2^2s_3^2+c_1^2s_2^2c_3^2},\\ |\zeta_3|&=\sqrt{s_1^2s_2^2c_3^2+c_1^2c_2^2s_3^2}.\end{aligned}\tag{D1}$$

Now the assumption $0\leqslant\alpha_3\leqslant\alpha_2\leqslant\alpha_1\leqslant\pi/4$ implies that

$$0\leqslant s_3\leqslant s_2\leqslant s_1\leqslant\frac{\sqrt{2}}{2}\leqslant c_1\leqslant c_2\leqslant c_3\leqslant 1,\tag{D2}$$

which in turn implies that

$$\begin{aligned}|\zeta_0|^2-|\zeta_1|^2&=\left(c_1^2-s_1^2\right)\left(c_2^2c_3^2-s_2^2s_3^2\right)\geqslant 0,\\ |\zeta_1|^2-|\zeta_2|^2&=\left(c_3^2-s_3^2\right)\left(s_1^2c_2^2-c_1^2s_2^2\right)\geqslant 0,\\ |\zeta_2|^2-|\zeta_3|^2&=\left(c_1^2-s_1^2\right)\left(s_2^2c_3^2-c_2^2s_3^2\right)\geqslant 0.\end{aligned}\tag{D3}$$

Therefore,

$$|\zeta_0|\geqslant|\zeta_1|\geqslant|\zeta_2|\geqslant|\zeta_3|\geqslant 0,\tag{D4}$$

which confirms Eq. (31) in Lemma 8. The first inequality $|\zeta_0|\geqslant|\zeta_1|$ is saturated iff $c_1^2=s_1^2$ or $c_2^2c_3^2=s_2^2s_3^2$, which holds iff $\alpha_1=\pi/4$. The second inequality $|\zeta_1|\geqslant|\zeta_2|$ is saturated iff $c_3^2=s_3^2$ or $s_1^2c_2^2=c_1^2s_2^2$, which holds iff $\alpha_2=\alpha_1$. The third inequality $|\zeta_2|\geqslant|\zeta_3|$ is saturated iff $c_1^2=s_1^2$ or $s_2^2c_3^2=c_2^2s_3^2$, which holds iff $\alpha_1=\frac{\pi}{4}$ or $\alpha_3=\alpha_2$. Finally, the last inequality $|\zeta_3|\geqslant 0$ is saturated iff $s_1^2s_2^2=s_3^2=0$, which holds iff $\alpha_2=\alpha_3=0$. ■

Proof of Lemma 9. If $0<\alpha_1=\alpha_2=\alpha_3<\pi/4$, then Lemma 8 implies that $|\zeta_0|>|\zeta_1|=|\zeta_2|=|\zeta_3|>0$.

Next, suppose $|\zeta_0|>|\zeta_1|=|\zeta_2|=|\zeta_3|>0$. Then the inequality $|\zeta_0|>|\zeta_1|$ implies that $\alpha_1<\pi/4$ according to Lemma 8; in addition, the equalities $|\zeta_1|=|\zeta_2|=|\zeta_3|$ imply that $\alpha_1=\alpha_2=\alpha_3$; finally, the inequality $|\zeta_3|>0$ implies that $\alpha_2>0$. Combining these results we can deduce that $0<\alpha_1=\alpha_2=\alpha_3<\pi/4$, which completes the proof of Lemma 9. ■

Proof of Lemma 10. If the condition in Eq. (33) holds, that is, $\alpha_j=\alpha_j'$ for $j=1,2,3$, then $U(\alpha_1,\alpha_2,\alpha_3)$ and $U(\alpha_1',\alpha_2',\alpha_3')$ have the same Schmidt coefficients. If the condition in Eq. (34) holds, then $U(\alpha_1,\alpha_2,\alpha_3)$ and $U(\alpha_1',\alpha_2',\alpha_3')$ also have the same Schmidt coefficients according to Eq. (32).

To prove the converse implication in Lemma 10, let $C_j=\cos(2\alpha_j)$, $S_j=\sin(2\alpha_j)$, $C_j'=\cos(2\alpha_j')$, and $S_j'=\sin(2\alpha_j')$ for $j=1,2,3$; then the assumptions $0\leqslant\alpha_3\leqslant\alpha_2\leqslant\alpha_1\leqslant\pi/4$ and $0\leqslant\alpha_3'\leqslant\alpha_2'\leqslant\alpha_1'\leqslant\pi/4$ imply that

$$0\leqslant C_1\leqslant C_2\leqslant C_3\leqslant 1,\quad 0\leqslant C_1'\leqslant C_2'\leqslant C_3'\leqslant 1.\tag{D5}$$

In addition, $C_j=0$ iff $\alpha_j=\pi/4$; similarly, $C_j'=0$ iff $\alpha_j'=\pi/4$. Furthermore, according to Eq. (23), the Schmidt coefficients of $U(\alpha_1,\alpha_2,\alpha_3)$ satisfy the following relations:

$$\begin{aligned}|\zeta_0|^2+|\zeta_3|^2&=\tfrac{1}{2}(1-C_1C_2),\\ |\zeta_0|^2-|\zeta_2|^2&=\tfrac{1}{2}C_2(C_1+C_3),\\ |\zeta_0|^2-|\zeta_3|^2&=\tfrac{1}{2}C_3(C_1+C_2),\end{aligned}\tag{D6}$$

and the Schmidt coefficients of $U(\alpha_1',\alpha_2',\alpha_3')$ satisfy similar relations.

Suppose $U(\alpha_1,\alpha_2,\alpha_3)$ and $U(\alpha_1',\alpha_2',\alpha_3')$ have the same Schmidt coefficients. Then Eq. (D6) implies that

$$C_1C_2=C_1'C_2',\quad C_2C_3=C_2'C_3',\quad C_1C_3=C_1'C_3'.\tag{D7}$$

If $\alpha_3\leqslant\alpha_2\leqslant\alpha_1<\pi/4$, so that $C_3\geqslant C_2\geqslant C_1>0$, then Eq. (D7) implies that $C_j'=C_j$ and $\alpha_j'=\alpha_j$ for $j=1,2,3$, which confirms Eq. (33).

If $\alpha_1=\alpha_2=\pi/4$, then we have $C_1=C_2=0$, which implies that $C_1'=C_2'=0$ and $\alpha_1'=\alpha_2'=\alpha_1=\alpha_2=\pi/4$ given Eqs. (D5) and (D7). In this case Eq. (34) holds.

If $\alpha_1=\pi/4$ and $\alpha_3\leqslant\alpha_2<\pi/4$, then $C_1=0$ and $C_3\geqslant C_2>0$, which implies that $C_1'=0$, $C_3',C_2'>0$, and $\alpha_1'=\pi/4$ given Eq. (D7). In addition, by virtue of Eq. (32) we can further derive that $C_2C_3=C_2'C_3'$ since $U(\alpha_1,\alpha_2,\alpha_3)$ and $U(\alpha_1',\alpha_2',\alpha_3')$ have the same Schmidt coefficients. So Eq. (34) also holds in this case. ■

Proof of Corollary 2. As shown in Sec. V A, U is equivalent to $U(\alpha_1,\alpha_2,\alpha_3)$ or $U^*(\alpha_1,\alpha_2,\alpha_3)$ with the constraint $0\leqslant\alpha_3\leqslant\alpha_2\leqslant\alpha_1\leqslant\pi/4$, and U' is equivalent to $U(\alpha_1',\alpha_2',\alpha_3')$ or $U^*(\alpha_1',\alpha_2',\alpha_3')$ with $0\leqslant\alpha_3'\leqslant\alpha_2'\leqslant\alpha_1'\leqslant\pi/4$. By assumption $U(\alpha_1,\alpha_2,\alpha_3)$ and $U(\alpha_1',\alpha_2',\alpha_3')$ have the same Schmidt coefficients s_0,s_1,s_2,s_3, which satisfy $s_0>s_1\geqslant s_2\geqslant s_3$, so we have $\alpha_1<\pi/4$ and $\alpha_1'<\pi/4$ by Lemma 8. In addition, $\alpha_j=\alpha_j'$ for $j=1,2,3$ and $U(\alpha_1,\alpha_2,\alpha_3)=U(\alpha_1',\alpha_2',\alpha_3')$ according to Lemma 10. Therefore, U' is equivalent to either U or U^* under local unitary transformations. ■

APPENDIX E: TWO INEQUIVALENT UNITARY OPERATORS WITH THE SAME SCHMIDT COEFFICIENTS

According to Eq. (32), we can choose the following parameters:

$$\alpha_1=\frac{\pi}{4},\quad \alpha_2=\arccos\sqrt{\frac{11}{16}},\quad \alpha_3=\arccos\sqrt{\frac{17}{24}},\tag{E1}$$

$$\alpha_1'=\frac{\pi}{4},\quad \alpha_2'=\arccos\sqrt{\frac{5}{8}},\quad \alpha_3'=\arccos\sqrt{\frac{13}{16}},\tag{E2}$$

which satisfy $\cos(2\alpha_2')\cos(2\alpha_3') = \cos(2\alpha_2)\cos(2\alpha_3)$. It is easy to verify that the two inequivalent unitary operators $U(\alpha_1, \alpha_2, \alpha_3)$ and $U(\alpha_1', \alpha_2', \alpha_3')$ have the same Schmidt coefficients:

$$\sqrt{\frac{37}{128}}, \quad \sqrt{\frac{37}{128}}, \quad \sqrt{\frac{27}{128}}, \quad \sqrt{\frac{27}{128}}. \tag{E3}$$

APPENDIX F: EFMIS FOR $U(\alpha_1, \alpha_2, \alpha_3)$ WHEN $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$, $\alpha_1 > \alpha_3$, AND $\alpha_2 < \pi/4$

In this Appendix we construct an EFMIS for the unitary $U(\alpha_1, \alpha_2, \alpha_3)$ when $0 \leqslant \alpha_3 \leqslant \alpha_2 \leqslant \alpha_1 \leqslant \pi/4$, $\alpha_1 > \alpha_3$, and $\alpha_2 < \pi/4$, which corresponds to the third case in the proof of Theorem 5.

Suppose in the magic basis the input state $|\phi_0\rangle$ has the expansion $|\phi_0\rangle = \sum_{k=1}^4 \gamma_k |\Phi_k\rangle$, where the coefficients satisfy the normalization condition

$$\sum_{k=1}^4 |\gamma_k|^2 = 1. \tag{F1}$$

Then the product-state constraint holds if the coefficients $\gamma_1^2, \gamma_2^2, \gamma_3^2, \gamma_4^2$ can be expressed as follows:

$$\begin{aligned}
&\gamma_1^2 = e^{2i\alpha_1}\gamma_0^2, \quad \gamma_2^2 = e^{2i\alpha_2}\gamma_0^2,\\
&\gamma_3^2 = \exp[i(2\alpha_1 + 2\alpha_2 - 2\alpha_3 + \pi)]\\
&\qquad \times \frac{\sin(2\alpha_1 + 2\alpha_3) + \sin(2\alpha_2 + 2\alpha_3)}{\sin(2\alpha_1 + 2\alpha_2)}\gamma_0^2,\\
&\gamma_4^2 = \exp[i(-2\alpha_3 + \pi)]\\
&\qquad \times \frac{\sin(2\alpha_1 - 2\alpha_3) + \sin(2\alpha_2 - 2\alpha_3)}{\sin(2\alpha_1 + 2\alpha_2)}\gamma_0^2,
\end{aligned} \tag{F2}$$

where

$$\gamma_0^2 = \frac{\sin(2\alpha_1 + 2\alpha_2)}{2\sin(2\alpha_1 + 2\alpha_2) + 2[\sin(2\alpha_1) + \sin(2\alpha_2)]\cos(2\alpha_3)} \tag{F3}$$

is determined by the normalization condition in Eq. (F1).

Moreover, an EFMIS can be constructed as follows (in the magic basis):

$$\begin{aligned}
|\phi_1\rangle &= \begin{pmatrix}\gamma_1\\ \gamma_2\\ \gamma_3\\ \gamma_4\end{pmatrix}, \quad |\phi_2\rangle = \begin{pmatrix}\gamma_1\\ -\gamma_2\\ \gamma_3\\ \gamma_4\end{pmatrix},\\
|\phi_3\rangle &= \begin{pmatrix}\gamma_1\\ \gamma_2\\ \gamma_3\\ -\gamma_4\end{pmatrix}, \quad |\phi_4\rangle = \begin{pmatrix}-\gamma_1\\ \gamma_2\\ \gamma_3\\ -\gamma_4\end{pmatrix}.
\end{aligned} \tag{F4}$$

The Gram matrix of the four states reads

$$G = \begin{pmatrix} 1 & g_2 & g_4 & h_1 \\ g_2 & 1 & h_2 & -g_3 \\ g_4 & h_2 & 1 & g_1 \\ h_1 & -g_3 & g_1 & 1 \end{pmatrix}, \tag{F5}$$

with $h_1 = g_1 + g_4 - 1$, $h_2 = g_2 + g_4 - 1$ and $g_j = 1 - 2|\gamma_j|^2$ for $j = 1, 2, 3, 4$. Its determinant is $64|\gamma_1\gamma_2\gamma_3\gamma_4|^2 \neq 0$, which implies that the four states in Eq. (F4) span the whole Hilbert space. In addition, we have

$$g_1, g_2, g_3, g_4 \neq 0 \tag{F6}$$

as proved below, which means the corresponding transition graph is connected, so the states in Eq. (F4) indeed form an EFMIS.

Proof of Eq. (F6). We shall prove Eq. (F6) by reduction to absurdity. Suppose $g_1 = 0$ or $g_2 = 0$; then $|\gamma_0|^2 = 1/2$. Let $S_j = \sin(2\alpha_j)$ and $C_j = \cos(2\alpha_j)$ for $j = 1, 2, 3$. From Eq. (F3), we can deduce that

$$(S_1 + S_2)C_3 = 0. \tag{F7}$$

Therefore, $\alpha_1 = \alpha_2 = \alpha_3 = 0$ or $\pi/4$, which contradicts the assumption. This contradiction shows that $g_1 \neq 0$ and $g_2 \neq 0$.

Suppose $g_3 = 0$; then $|\gamma_3|^2 = 1/2$. From Eqs. (F2) and (F3) we can deduce that

$$C_1S_3 + C_2S_3 = C_1S_2 + S_1C_2. \tag{F8}$$

Meanwhile, the assumptions $\alpha_1 > \alpha_3$ and $\alpha_2 < \pi/4$ imply that $C_2 > 0$, $S_2 \geqslant S_3$, $S_1 > S_3$, and

$$C_1S_3 + C_2S_3 < C_1S_2 + S_1C_2, \tag{F9}$$

which contradicts Eq. (F8). This contradiction shows that $g_3 \neq 0$.

Suppose $g_4 = 0$; then $|\gamma_4|^2 = 1/2$. From Eqs. (F2) and (F3) we can deduce that

$$-(C_1 + C_2)S_3 = \sin(2\alpha_1 + 2\alpha_2). \tag{F10}$$

However, this equation cannot hold given the assumptions $\alpha_1 > \alpha_3$ and $\alpha_2 < \pi/4$. This contradiction shows that $g_4 \neq 0$ and completes the proof of Eq. (F6). ■

APPENDIX G: PROOF OF COROLLARY 3

Proof. Corollary 3 follows from Theorem 5 and the following equations:

$$\mu(U(\alpha_1 + \pi/2, \alpha_2, \alpha_3)) = \mu(U(\alpha_1, \alpha_2, \alpha_3)), \tag{G1}$$
$$\mu(U(\alpha_1, \alpha_2 + \pi/2, \alpha_3)) = \mu(U(\alpha_1, \alpha_2, \alpha_3)), \tag{G2}$$
$$\mu(U(\alpha_1, \alpha_2, \alpha_3 + \pi/2)) = \mu(U(\alpha_1, \alpha_2, \alpha_3)), \tag{G3}$$
$$\mu(U(\pi/4 - \alpha_1, \alpha_2, \alpha_3)) = \mu(U(\pi/4 + \alpha_1, \alpha_2, \alpha_3)), \tag{G4}$$
$$\mu(U(\alpha_1, \pi/4 - \alpha_2, \alpha_3)) = \mu(U(\alpha_1, \pi/4 + \alpha_2, \alpha_3)), \tag{G5}$$
$$\mu(U(\alpha_1, \alpha_2, \pi/4 - \alpha_3)) = \mu(U(\alpha_1, \alpha_2, \pi/4 + \alpha_3)). \tag{G6}$$

Equations (G1)–(G3) mean $\mu(U(\alpha_1, \alpha_2, \alpha_3))$ is periodic in $\alpha_1, \alpha_2, \alpha_3$, respectively, with the common period of $\pi/2$. Equations (G4)–(G6) mean $\mu(U(\alpha_1, \alpha_2, \alpha_3))$ is invariant under reflection with respect to the three planes specified by $\alpha_1 = \pi/4$, $\alpha_2 = \pi/4$, $\alpha_3 = \pi/4$, respectively.

Equation (G1) follows from

$$U(\alpha_1, \alpha_2, \alpha_3) = i(\sigma_1 \otimes \sigma_1)U(\alpha_1 + \pi/2, \alpha_2, \alpha_3), \quad \text{(G7)}$$

given that $\mu(U)$ is invariant under local unitary transformations. Equations (G2) and (G3) can be proved in a similar way.

Equation (G4) follows from

$$U(\pi/4 - \alpha_1, \alpha_2, \alpha_3) = -i\sigma_1^{\mathrm{A}} U^*(\pi/4 + \alpha_1, \alpha_2, \alpha_3)\sigma_1^{\mathrm{B}}, \quad \text{(G8)}$$

given that $\mu(U)$ is also invariant under complex conjugation. Equations (G5) and (G6) can be proved in a similar way. ■

[1] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Quantum certification and benchmarking, Nat. Rev. Phys. **2**, 382 (2020).

[2] M. Kliesch and I. Roth, Theory of quantum system certification, PRX Quantum **2**, 010201 (2021).

[3] J. Carrasco, A. Elben, C. Kokail, B. Kraus, and P. Zoller, Theoretical and experimental perspectives of quantum verification, PRX Quantum **2**, 010102 (2021).

[4] X.-D. Yu, J. Shang, and O. Gühne, Statistical methods for quantum state verification and fidelity estimation, arXiv:2109.10805.

[5] 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).

[6] L. Aolita, C. Gogolin, M. Kliesch, and J. Eisert, Reliable quantum certification of photonic state preparations, Nat. Commun. **6**, 8498 (2015).

[7] Y. Takeuchi and T. Morimae, Verification of Many-Qubit States, Phys. Rev. X **8**, 021060 (2018).

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

[9] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario, Phys. Rev. Lett. **123**, 260504 (2019).

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

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

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

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

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

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

[16] A. Kalev, A. Kyrillidis, and N. M. Linke, Validating and certifying stabilizer states, Phys. Rev. A **99**, 042337 (2019).

[17] H. Zhu and M. Hayashi, Efficient Verification of Hypergraph States, Phys. Rev. Appl. **12**, 054047 (2019).

[18] Z. Li, Y.-G. Han, and H. Zhu, Optimal Verification of Greenberger-Horne-Zeilinger States, Phys. Rev. Appl. **13**, 054002 (2020).

[19] N. Dangniam, Y.-G. Han, and H. Zhu, Optimal verification of stabilizer states, Phys. Rev. Res. **2**, 043323 (2020).

[20] M. Hayashi and Y. Takeuchi, Verifying commuting quantum computations via fidelity estimation of weighted graph states, New J. Phys. **21**, 093060 (2019).

[21] Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, and X. Zhang, Efficient Verification of Dicke States, Phys. Rev. Appl. **12**, 044020 (2019).

[22] Z. Li, Y.-G. Han, H.-F. Sun, J. Shang, and H. Zhu, Verification of phased Dicke states, Phys. Rev. A **103**, 022601 (2021).

[23] W.-H. Zhang, C. Zhang, Z. Chen, X.-X. Peng, X.-Y. Xu, P. Yin, S. Yu, X.-J. Ye, Y.-J. Han, J.-S. Xu, *et al.*, Experimental Optimal Verification of Entangled States Using Local Measurements, Phys. Rev. Lett. **125**, 030506 (2020).

[24] L. Lu, L. Xia, Z. Chen, L. Chen, T. Yu, T. Tao, W. Ma, Y. Pan, X. Cai, Y. Lu, *et al.*, Three-dimensional entanglement on a silicon chip, npj Quantum Inf. **6**, 30 (2020).

[25] X. Jiang, K. Wang, K. Qian, Z. Chen, Z. Chen, L. Lu, L. Xia, F. Song, S. Zhu, and X. Ma, Towards the standardization of quantum state verification using optimal strategies, npj Quantum Inf. **6**, 90 (2020).

[26] W.-H. Zhang, X. Liu, P. Yin, X.-X. Peng, G.-C. Li, X.-Y. Xu, S. Yu, Z.-B. Hou, Y.-J. Han, J.-S. Xu, *et al.*, Classical communication enhanced quantum state verification, npj Quantum Inf. **6**, 103 (2020).

[27] Y.-C. Liu, J. Shang, X.-D. Yu, and X. Zhang, Efficient verification of quantum processes, Phys. Rev. A **101**, 042315 (2020).

[28] H. Zhu and H. Zhang, Efficient verification of quantum gates with local operations, Phys. Rev. A **101**, 042316 (2020).

[29] P. Zeng, Y. Zhou, and Z. Liu, Quantum gate verification and its application in property testing, Phys. Rev. Res. **2**, 023306 (2020).

[30] H. F. Hofmann, Complementary Classical Fidelities as an Efficient Criterion for the Evaluation of Experimentally Realized Quantum Operations, Phys. Rev. Lett. **94**, 160504 (2005).

[31] D. M. Reich, G. Gualdi, and C. P. Koch, Minimum number of input states required for quantum gate characterization, Phys. Rev. A **88**, 042309 (2013).

[32] K. Mayer and E. Knill, Quantum process fidelity bounds from sets of input states, Phys. Rev. A **98**, 052326 (2018).

[33] Y.-D. Wu and B. C. Sanders, Efficient verification of bosonic quantum channels via benchmarking, New J. Phys. **21**, 073026 (2019).

[34] A. Elben, B. Vermersch, R. van Bijnen, C. Kokail, T. Brydges, C. Maier, M. K. Joshi, R. Blatt, C. F. Roos, and P. Zoller, Cross-Platform Verification of Intermediate Scale Quantum Devices, Phys. Rev. Lett. **124**, 010504 (2020).

[35] R.-Q. Zhang, Z. Hou, J.-F. Tang, J. Shang, H. Zhu, G.-Y. Xiang, C.-F. Li, and G.-C. Guo, Efficient Experimental Verification of Quantum Gates with Local Operations [Phys. Rev. Lett. (to be published)], arXiv:2107.02365.

[36] M. Luo, X. Zhang, and X. Zhou, Proof-of-principle experimental demonstration of quantum gate verification, arXiv:2107.13466.

[37] B. Kraus and J. I. Cirac, Optimal creation of entanglement using a two-qubit gate, Phys. Rev. A **63**, 062309 (2001).

[38] W. Dür, G. Vidal, and J. I. Cirac, Optimal Conversion of Nonlocal Unitary Operations, Phys. Rev. Lett. **89**, 057901 (2002).

[39] S. Hill and W. K. Wootters, Entanglement of a Pair of Quantum Bits, Phys. Rev. Lett. **78**, 5022 (1997).