Simultaneous certification of entangled states and measurements in bounded dimensional semiquantum games

Xingjian Zhang[1] and Qi Zhao[1,2,3,*]

[1]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*
[2]*Shanghai Branch, National Laboratory for Physical Sciences at Microscale and Department of Modern Physics,*
University of Science and Technology of China, Shanghai 201315, China
[3]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics,*
University of Science and Technology of China, Shanghai 201315, China

Certification of quantum systems and operations is a central task in quantum information processing. Most current schemes rely on a tomography with fully characterized devices, while this may not be met in real experiments. Device characterizations can be removed with device-independent tests, but it is technically challenging at the moment. In this paper, we investigate the problem of certifying entangled states and measurements via semiquantum games, a type of nonlocal quantum games with well characterized quantum inputs, balancing practicality and device independence. We first design a specific bounded-dimensional semiquantum game, with which any pure entangled state and Bell state measurement operators can be simultaneously certified. Afterward via a duality treatment of state and measurement, we interpret the dual form of this game as a source-independent bounded-dimensional entanglement swapping protocol and show the whole process, including any entangled projector and Bell states, can be certified with this protocol. In particular, our results do not require a complete Bell state measurement, which is beneficial for experiments and practical use.

I. INTRODUCTION

With the rapid development of quantum technologies in state preparation and dynamical evolution, quantum devices are expected to outperform their classical counterparts in the future. However, unexpected and uncharacteristic noise hampers the functioning of quantum devices. Thus certification of states and implemented processes in the quantum devices is a central task in this field. Nonetheless, as a classical being, an observer can only take advantage of classical statistics together with a physical model he or she believes to characterize the system and its dynamical evolution. One way for certification is to employ a full tomography on the system (state tomography) [1–3] or on the process (process tomography) [4–6]. With an information-complete set of measurements (input states), one can reconstruct all the elements in the quantum state operator (quantum process). However, such approaches require a full knowledge on the devices. Unavoidable noise from the real environment can easily nullify the results. The states and measurements used in tomography need to be fully characterized and trusted, while sometimes they might be even more difficult to calibrate than the system or process investigated.

Luckily, quantum physics allows us to break away from the dilemma by Bell nonlocality [7,8]. Violation of a Bell inequality indicates entanglement in a nonlocal system and incompatibility of measurements. In fact, as explicitly pointed out by Mayers and Yao [9], the state and measurements can be uniquely determined to local isometries from certain classical correlations or the system "self-tests" itself [9] without any charactization of the devices but only relying on the validity of quantum physics. In this sense we say the certification is device independent. So far, numerous remarkable results have been derived in the subject of state self-testing [10–17], and physical processes or measurements certification [18–25]. To make self-testing meet a real situation, robust self-testing, allowing the noises and imperfections to some extent, has been investigated, aiming to give a lower bound on the fidelity of the physical system from a reference system (in the sense of local isometries) based on the observed statistics. Much progress has been made in this field, too [14,15,26–28].

Realizing loophole-free device-independent tests are highly challenging in practice, mainly suffering from detection and locality loopholes. Until now, only a few device-independent experiments succeed in closing the detection loophole and the locality loophole simultaneously [29–36]. However, in these demonstrations, either only a modest violation of Bell inequality is obtained, which is far from current robust self-testing requirement [15], or the repetition rate is rather low for practical applications. Besides, not all entangled states can show nonlocal advantages over separable states.

A compromising approach to balancing device independence and practicality is to apply a semi-device-independent scenario. One of the most prominent scenarios is the

*zhaoqithu10@gmail.com

semiquantum game proposed by Buscemi [37]. Semiquantum games are similar to Bell tests, except for that general local quantum inputs are allowed. It has been proved that all entangled states exhibit nonlocality in these games, bridging the gap between the concept of entanglement and nonlocality (see Corollary 1 in Ref. [37]). After the proposal of semiquantum games, focusing on the prepared entangled states, there are results presenting approaches to qualitatively witnessing entanglement [38–42] and quantitatively estimating the amount of entanglement in the system with semiquantum games [43,44]. The use of general quantum inputs make these protocols more flexible than fully device-independent ones. This allows the direct use of general quantum states in a quantum network [45,46]. Moreover, semiquantum games can be loss tolerant [38,45], reducing the detection efficiency requirement. This overcomes the detection-loophole problem in device-independent tasks. However, little attention has been received for channels or measurements in these games, with one exceptional work focusing on the quantum channel with quantum memories [47]. Moreover, it is left open whether we can "uniquely" certify certain systems and operations simultaneously in a manner similar to self-testing in device-independent tests.

In this paper, we consider the certification of entangled states and measurements in semiquantum games with a given dimensional Hilbert space. We design a new type of semiquantum game, showing the plausibility of simultaneous certification of any pure bipartite entangled state in $\mathbb{C}^2 \otimes \mathbb{C}^2$ and Bell state measurement operators. In particular, our design does not rely on a complete Bell state measurement but can be naturally generalized for such a case. Moreover, we transform the setting into the manner of a source-independent entanglement swapping protocol via a duality treatment of state and measurement operator. In its "dual" form of semiquantum game, any entangled projector acting on the bounded dimensional space and Bell states can be certified simultaneously.

II. PRELIMINARY

We first briefly review the concept of semiquantum games in Ref. [37] and results in Ref. [38]. Consider a nonlocal game with two players, Alice and Bob, as shown in Fig. 1. In each round of the game, a referee gives them quantum states $\psi_x^{A_0} \in \mathcal{D}(\mathcal{H}_{A_0})$, $\psi_y^{B_0} \in \mathcal{D}(\mathcal{H}_{B_0})$, $x \in \mathcal{X}$, $y \in \mathcal{Y}$ individually. These inputs can be general quantum states acting on the corresponding Hilbert spaces and are not necessarily pure. Nevertheless, they are all well characterized and trusted. We denote the input systems by the corresponding Hilbert spaces, $\mathcal{H}_{A_0}$, $\mathcal{H}_{B_0}$ for Alice and Bob, respectively. Then they are asked to give classical outputs $a \in \mathcal{A}$, $b \in \mathcal{B}$, and a score $\beta_{a,b}^{x,y}$ is obtained based on the tuple of $\{\psi_x^{A_0}, \psi_y^{B_0}, a, b\}$. In this game, generally, Alice and Bob can first share a bipartite state $\rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, and perform joint positive operator-valued measure measurements (POVMs) on the party they each hold and the received quantum input state, individually. We denote the POVM elements as $M_a^{A_0A}$ acting on $\mathcal{H}_{A_0} \otimes \mathcal{H}_A$ yielding the result a on Alice's side and $M_b^{BB_0}$ acting on $\mathcal{H}_B \otimes \mathcal{H}_{B_0}$ yielding the result b on Bob's side, with $M_a^{A_0A}, M_b^{BB_0} \succeq 0$, $\sum_a M_a^{A_0A} =$
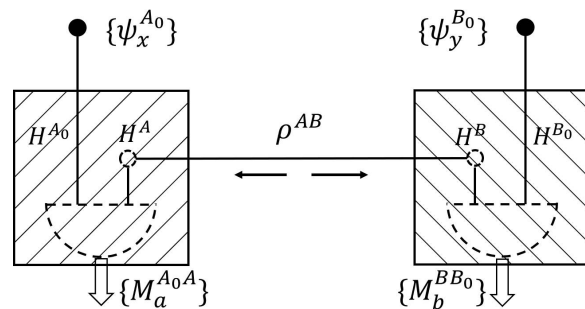

FIG. 1. The semiquantum game. The systems are denoted by their corresponding Hilbert spaces. In this game, from the referee's perspective, well-characterized states $\{\psi_x^{A_0}\}$, $\{\psi_y^{B_0}\}$ are sent to Alice and Bob, respectively, where each of the two players measures the input quantum state received and her or his own party of ρ^{AB} jointly. The joint measurements are expressed as POVMs $\{M_a^{A_0A}\}$, $\{M_b^{BB_0}\}$

I^{A_0A}, $\sum_b M_b^{BB_0} = I^{BB_0}$. The average score is

$$
\begin{aligned}
S &= \sum_{x,y,a,b} \beta_{a,b}^{x,y} P(a, b | \psi_x^{A_0}, \psi_y^{B_0}) \\
&= \sum_{x,y,a,b} \beta_{a,b}^{x,y} \mathrm{Tr}\big[(\psi_x^{A_0} \otimes \rho^{AB} \otimes \psi_y^{B_0})(M_a^{A_0A} \otimes M_b^{BB_0}) \big].
\end{aligned}
$$

(1)

Consider any conventional entanglement witness W, $\mathrm{Tr}[W \rho^T] < 0$ for a specific entangled state ρ^T while $\mathrm{Tr}[W \sigma] \geqslant 0$ for any separable operator σ. The transpose operation does not change the amount of entanglement in the state, and the reason for using a transposed state will be made clear later. It is plausible to transform the entanglement witness W into a semiquantum game and witness entanglement over systems $\mathcal{H}_A$, $\mathcal{H}_B$. Using the technique of partial POVM, we now focus on the effective POVM elements

$$
\tilde{M}_{ab}^{A_0B_0} = \mathrm{Tr}_{AB}\big[(I^{A_0} \otimes \rho^{AB} \otimes I^{B_0})(M_a^{A_0A} \otimes M_b^{BB_0}) \big], \quad (2)
$$

which act on the Hilbert space $\mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0}$. Intuitively, the state information of ρ^{AB} can be cast into the structure of the POVM elements $\tilde{M}_{ab}^{A_0B_0}$. Inputting quantum states can be seen as a tomography process of this effective POVM, hence acquiring information about ρ^{AB}.

To link the entanglement witness with the semiquantum game, consider a decomposition of W with the parameters $\beta^{x,y}$ and quantum inputs $\{\psi_x^{A_0}, \psi_y^{B_0}\}$

$$
W^{A_0B_0} = \sum_{x,y,a,b} \beta_{a,b}^{x,y} \psi_x^{A_0} \otimes \psi_y^{B_0}. \quad (3)
$$

Here we use the superscripts A_0B_0 to denote that the effective entanglement witness now acts on the space $\mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0}$. One can focus on one specific outcome, say, $(a, b) = (0, 0)$, by letting $\beta_{a,b}^{x,y} = \delta_{a,0} \cdot \delta_{b,0} \cdot \beta^{x,y}$ in a semiquantum game. The average score obtained in the game becomes $S = \mathrm{Tr}[W^{A_0B_0} \tilde{M}_{00}^{A_0B_0}]$.

It has been proved in Ref. [38] that a separable σ^{AB} will result in separable effective POVM elements $\tilde{M}_{ab}^{A_0B_0}$ whatever the measurements. In these cases, one will observe a score $S \geqslant 0$. On the other hand, if the shared state between

$\mathcal{H}_A, \mathcal{H}_B$ is the entangled state ρ^{AB}, and the measurement operators are projectors onto the maximally entangled state $M_a^{A_0A} = M_b^{BB_0} = |\Phi^+\rangle\langle\Phi^+|$, then it gives rise to the effective POVM element $\tilde{M}_{ab}^{A_0B_0} = \rho^T/d_A d_B$, where d_A, d_B are dimensions of $\mathcal{H}_A, \mathcal{H}_B$ and $|\Phi^+\rangle = \frac{1}{\sqrt{d}}\sum_{i=1}^{d}|ii\rangle$. In this case a negative score $S < 0$ will be observed, implying entanglement over systems $\mathcal{H}_A, \mathcal{H}_B$.

The results above show that it is viable to witness entanglement in a measurement-device-independent manner with the aid of semiquantum games. Besides, as only the outputs $(a, b) = (0, 0)$ are used, this protocol shares a loss-tolerant feature. Furthermore, these semiquantum games can also be applied to detect detailed entanglement structure [41] and estimate the robustness of entanglement, negativity, and randomness [44].

III. SIMULTANEOUS CERTIFICATION OF ENTANGLED STATE AND MEASUREMENTS

In previous works, only prepared states or channels are characterized via a semiquantum game. To further elaborate the application of semiquantum games, we now investigate the problem of certifying entangled states and joint measurements simultaneously. We first define the concept of entangled measurement operators and entangled measurements:

Definition 1 (Entangled Measurements). A measurement operator $M_{ab}^{AB}(0 \preceq M_{ab}^{AB} \preceq I)$ acting on the system $\mathcal{H}_A \otimes \mathcal{H}_B$ is called entangled if it cannot be expressed as $\sum_{i,j} N_i^A \otimes N_j^B$ with a set of semidefinite positive operators $\{N_i^A, N_j^B | N_i^A \in \mathcal{L}(\mathcal{H}_A), N_j^B \in \mathcal{L}(\mathcal{H}_B), N_i^A, N_j^B \succeq 0\}$; otherwise, it is called a separable measurement operator. A POVM $\{M_{ab}^{AB}\}$ is called entangled if at least one of its measurement operators is entangled.

In the following we may call both entangled states and entangled measurement operators as generally entangled operators. Entangled measurements, especially Bell state measurement (BSM), play an important role in many quantum information processing tasks like entanglement swapping and teleportation. In the measurement-device-independent protocols, entangled measurement operators are essential for a nonlocal behavior, too. We have the following result for semiquantum games:

Theorem 1. In a semiquantum game where the input states and appointed scores form an entanglement witness given by Eq. (3), an observation of an average score $S = \text{Tr}[W\tilde{M}_{00}^{A_0B_0}] < 0$ necessarily indicates that $M_0^{A_0A}(M_0^{BB_0})$ is an entangled POVM operator on systems $\mathcal{H}_{A_0}, \mathcal{H}_A(\mathcal{H}_B, \mathcal{H}_{B_0})$.

The proof is given in Appendix A. This theorem together with previous results show that entangled measurements and state can be witnessed by investigating the effective POVM elements. Now we take one step further and try to certify them via a quantitative investigation on the effective POVM measurement operators $\tilde{M}_{ab}^{A_0B_0}$. We consider the case with a bounded dimensional Hilbert space, specifically the case where the unknown state is a pair of qubits, and we design the semiquantum games such that all quantum inputs are qubits as well, i.e., $\mathcal{H}_A \cong \mathcal{H}_B \cong \mathcal{H}_{A_0} \cong \mathcal{H}_{B_0} \cong \mathbb{C}^2$.

Box 1: Design of the measurement-device-independent game:

Game $\{\psi_x^{A_0}, \psi_y^{B_0}, \beta^{x,y}\}$ is designed such that

- The quantum inputs are sent to the measurement devices at random,

- $\{\psi_x^{A_0}, \psi_y^{B_0}, \beta^{x,y}\}$ are divided into two sets of tuples, $\{\psi_{x_1}^{A_0}, \psi_{y_1}^{B_0}, \beta^{x_1,y_1}\}$ and $\{\psi_{x_2}^{A_0}, \psi_{y_2}^{B_0}, \beta^{x_2,y_2}\}$, where $\{x_1, y_1\} \cup \{x_2, y_2\} = \{x, y\}, \{x_1, y_1\} \cap \{x_2, y_2\} = \emptyset$. They effectively construct the operators

$$W = W_G + W_T = \sum_{x,y} \beta^{x,y} \psi_x^{A_0} \otimes \psi_y^{B_0},$$

$$W_G = |\psi_E\rangle\langle\psi_E| = \sum_{x_1,y_1} \beta^{x_1,y_1} \psi_{x_1}^{A_0} \otimes \psi_{y_1}^{B_0},$$

$$W_T = I^{A_0B_0} - W_G = \sum_{x_2,y_2} \beta^{x_2,y_2} \psi_{x_2}^{A_0} \otimes \psi_{y_2}^{B_0},$$

- $|\psi_E\rangle$ is an entangled pure state,

- The average score obtained in the rounds with input states $\psi_{x_2}^{A_0}, \psi_{y_2}^{B_0}$ is restricted to be

$$S_T = \sum_{x_2,y_2} \beta^{x_2,y_2} P(a = b = 0 | \psi_{x_2}^{A_0}, \psi_{y_2}^{B_0}) = 0.$$

Goal: Maximize the average score $S = \sum_{x,y} \beta^{x,y} P(a = b = 0 | \psi_x^{A_0}, \psi_y^{B_0})$.

In the spirit of measurement-device-independent entanglement witness, we now also focus on one pair of measurement operators corresponding to a single outcome, say, $(a, b) = (0, 0)$, and set the score $\beta_{a,b}^{x,y} = 0$ for $(a, b) \neq (0, 0)$. As only the measurement operators $M_0^{A_0A}, M_0^{BB_0}$ are used, for brevity, we omit the subscripts and denote the measurement operators as M^{A_0A}, M^{BB_0} and the effective POVM element as $\tilde{M}^{A_0B_0}$. We design a measurement-device-independent game as shown in Box 1.

Now we give the main result in this paper:

Theorem 2. Under the condition $\mathcal{H}_A \cong \mathcal{H}_B \cong \mathcal{H}_{A_0} \cong \mathcal{H}_{B_0} \cong \mathbb{C}^2$, the largest score that can be obtained in the game is $S = 1/4$. This score also certifies that $(\rho^{AB})^T \sim |\psi_E\rangle\langle\psi_E|, M^{A_0A}, M^{BB_0} \sim |\Phi^+\rangle\langle\Phi^+|$, where the equivalence refers to a freedom of local unitary operations.

This result shows that any two-qubit entangled pure state $|\psi_E\rangle$ and a pair of BSM operators M^{A_0A}, M^{BB_0} can be certified in the bounded-dimensional semiquantum game. In the following we prove this result.

Proof. The design of the game restricts that the effective POVM operator $\tilde{M}^{A_0B_0}$ must act only on the subspace spanned by $|\psi_E\rangle$, which we denote as span$(|\psi_E\rangle)$. Hence the problem

can be cast into an optimization form:

$$\arg \max_{\rho^{AB}, M^{A_0 A}, M^{BB_0}} \text{Tr}[\tilde{M}^{A_0 B_0} |\psi_E\rangle\langle\psi_E|],$$

Subject to:

$$\tilde{M}^{A_0 B_0} = \text{Tr}_{AB}[(I^{A_0} \otimes \rho^{AB} \otimes I^{B_0})(M^{A_0 A} \otimes M^{BB_0})],$$

$$\text{Tr}[\tilde{M}^{A_0 B_0}(I^{A_0 B_0} - |\psi_E\rangle\langle\psi_E|)] = 0.$$

Here arg refers to the arguments when the maximum of the objective function is taken. Apart from the system dimensions, we do not make assumptions on the measurement operators, $M^{A_0 A}, M^{BB_0}$, which may be general POVM operators, or the state ρ^{AB}, which is in general a mixed state. However, we have the following lemmas showing that only rank-one entangled measurement operators and a pure entangled state may guarantee that $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi_E\rangle))$, where $|\psi_E\rangle$ is entangled:

Lemma 1. For $\mathcal{H}_A \cong \mathcal{H}_B \cong \mathcal{H}_{A_0} \cong \mathcal{H}_{B_0} \cong \mathbb{C}^2$ and $M^{A_0 A}, M^{BB_0}$ rank-one entangled measurement operators over systems $\mathcal{H}_{A_0}, \mathcal{H}_A$ and $\mathcal{H}_{B_0}, \mathcal{H}_B$, a necessary condition for $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi_E\rangle))$ is that ρ^{AB} is a pure state.

Lemma 2. For a pure bipartite entangled quantum state $\rho^{AB} = |\Psi\rangle\langle\Psi| \in \mathcal{D}(\mathbb{C}^2 \otimes \mathbb{C}^2)$ over systems $\mathcal{H}_A, \mathcal{H}_B$, a necessary condition for $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi_E\rangle))$ is that both $M^{A_0 A}$ and M^{BB_0} are rank-one entangled operators over systems $\mathcal{H}_A, \mathcal{H}_{A_0}$ and $\mathcal{H}_B, \mathcal{H}_{B_0}$.

We show the proofs in Appendixes B and C. To see that only rank-one entangled measurement operators and a pure entangled state need to be considered, for a general state ρ^{AB} and POVM elements $M^{A_0 A}, M^{BB_0}$, we can apply spectral decomposition to them,

$$\rho^{AB} = \sum_i |\Psi_i\rangle\langle\Psi_i|,$$

$$M^{A_0 A} = \sum_j |\phi_j\rangle\langle\phi_j|,$$

$$M^{BB_0} = \sum_k |\phi_k\rangle\langle\phi_k|.$$

Here $|\Psi_i\rangle, |\phi_j\rangle, |\phi_k\rangle$ are (subnormalized) orthogonal vectors. The effective POVM $\tilde{M}^{A_0 B_0}$ becomes

$$\tilde{M}^{A_0 B_0} = \sum_{j,k} N_{jk}^{A_0 B_0}$$

$$= \sum_{j,k} \text{Tr}_{AB}[(I^{A_0} \otimes \rho^{AB} \otimes I^{B_0})(|\phi_j\rangle\langle\phi_j| \otimes |\phi_k\rangle\langle\phi_k|)],$$

where $N_{jk}^{A_0 B_0} \succeq 0, \forall j, k$. To restrict that $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi_E\rangle))$, we need all these operators to act on span($|\psi_E\rangle$). Via Lemma 1, ρ^{AB} should be a pure state. Then the problem is reduced to the case in Lemma 2, hence requiring $M^{A_0 A}, M^{BB_0}$ to be necessarily rank-one entangled operators, such that $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi_E\rangle))$.

We now can focus on the case with rank-one measurement operators and a pure state. First we apply the Schmidt decomposition to $|\psi_E\rangle$, and without loss of generality it can be written as $|\psi_E\rangle = \cos\chi |00\rangle + \sin\chi |11\rangle$, where $|0\rangle, |1\rangle$ represent some orthogonal bases in systems A_0, B_0. Since the measurement operators can be treated as (subnormalized) pure bipartite states now, we now denote them

as $M^{A_0 A} = m_a |\phi^{A_0 A}\rangle\langle\phi^{A_0 A}|$, $M^{BB_0} = m_b |\phi^{BB_0}\rangle\langle\phi^{BB_0}|$, where $|\phi^{A_0 A}\rangle, |\phi^{BB_0}\rangle$ are normalized pure states, $0 \leqslant m_a, m_b \leqslant 1$. Furthermore, we express them in the form of

$$|\phi^{A_0 A}\rangle = \sqrt{m_a}(\cos\alpha |0\rangle|\varphi^A\rangle + \sin\alpha |1\rangle|\bar{\varphi}^A\rangle),$$

$$|\phi^{BB_0}\rangle = \sqrt{m_b}(\cos\beta |0\rangle|\varphi^B\rangle + \sin\beta |1\rangle|\bar{\varphi}^B\rangle). \quad (4)$$

In Eq. (4), the state vectors $|0\rangle, |1\rangle$ acting on systems A_0, B_0 are the same as the ones in representing $|\psi_E\rangle$. The vectors $|\varphi^A\rangle, |\bar{\varphi}^A\rangle \in \mathcal{H}_A, |\varphi^B\rangle, |\bar{\varphi}^B\rangle \in \mathcal{H}_B$ are normalized, yet in general $\langle\varphi^A|\bar{\varphi}^A\rangle, \langle\varphi^B|\bar{\varphi}^B\rangle \neq 0$. Therefore, we can express $\tilde{M}^{A_0 B_0} = |\tilde{\Psi}\rangle\langle\tilde{\Psi}|$, where $|\tilde{\Psi}\rangle$ is a subnormalized vector

$$|\tilde{\Psi}\rangle = \sqrt{m_a m_b}(\cos\alpha \cos\beta \langle\Psi|\varphi^A \varphi^B\rangle |00\rangle$$

$$+ \sin\alpha \sin\beta \langle\Psi|\bar{\varphi}^A \bar{\varphi}^B\rangle |11\rangle$$

$$+ \cos\alpha \sin\beta \langle\Psi|\varphi^A \bar{\varphi}^B\rangle |01\rangle$$

$$+ \sin\alpha \cos\beta \langle\Psi|\bar{\varphi}^A \varphi^B\rangle |10\rangle).$$

Requiring $|\tilde{\Psi}\rangle$ to be parallel to $|\psi_E\rangle$ indicates that $\langle\Psi|\varphi^A \bar{\varphi}^B\rangle = \langle\Psi|\bar{\varphi}^A \varphi^B\rangle = 0$. Under this condition we have the following lemma:

Lemma 3. In the condition that $\langle\Psi|\varphi^A \bar{\varphi}^B\rangle = \langle\Psi|\bar{\varphi}^A \varphi^B\rangle = 0$, where $|\varphi^A\rangle, |\bar{\varphi}^A\rangle, |\varphi^B\rangle, |\bar{\varphi}^B\rangle$ are introduced by Eq. (4), we have $|\langle\Psi|\varphi^A \varphi^B\rangle|^2 + |\langle\Psi|\bar{\varphi}^A \bar{\varphi}^B\rangle|^2 \leqslant 1$. The equality is taken iff $\langle\varphi^A|\bar{\varphi}^A\rangle = \langle\varphi^B|\bar{\varphi}^B\rangle = 0$, and the subspaces of the two parties are spanned by $\{|\varphi^A\rangle, |\bar{\varphi}^A\rangle\}, \{|\varphi^B\rangle, |\bar{\varphi}^B\rangle\}$, respectively.

While the lemma is relatively easy to be proved in the Hilbert space with a bounded dimension we now consider, it is worth noting that it does not rely on a restriction of dimensions of $\mathcal{H}_A, \mathcal{H}_B$. We leave the proof for this lemma in the general case in Appendix D.

With this lemma and the requirement that $|\tilde{\Psi}\rangle$ lying parallel to $|\psi_E\rangle$, we can derive that

$$\text{Tr}[\tilde{M}^{A_0 B_0} |\psi_E\rangle\langle\psi_E|]$$

$$\leqslant m_a m_b \frac{\sin^2\alpha \sin^2\beta \cos^2\alpha \cos^2\beta}{\sin^2\alpha \sin^2\beta \cos^2\chi + \cos^2\alpha \cos^2\beta \sin^2\chi}. \quad (5)$$

The equality is reached if and only if $|\langle\Psi|\varphi^A \varphi^B\rangle|^2 + |\langle\Psi|\bar{\varphi}^A \bar{\varphi}^B\rangle|^2 = 1$. The maximum of this expression is $1/4$, taken when $\sin^2\alpha = \sin^2\beta = 1/2$ and $m_a = m_b = 1$, which corresponds to Bell state measurement operators, and $\langle\Psi|\varphi^A \varphi^B\rangle/\langle\Psi|\bar{\varphi}^A \bar{\varphi}^B\rangle = \cos\chi / \sin\chi$, yielding the conclusion that $|\Psi\rangle$ is equivalent to $|\psi_E\rangle$. This finishes our proof.

IV. CERTIFICATION IN A SOURCE-INDEPENDENT ENTANGLEMENT SWAPPING GAME

It is interesting to notice that the entanglement swapping protocol shares a dual form of the semiquantum game if the roles of state and measurements are exchanged, shown in Fig. 2. Suppose there are two independent bipartite states, $\rho^{A_0 A} \in \mathcal{D}(\mathcal{H}_{A_0} \otimes \mathcal{H}_A), \rho^{BB_0} \in \mathcal{D}(\mathcal{H}_B \otimes \mathcal{H}_{B_0})$. Different from the standard entanglement swapping protocol, here the states $\rho^{A_0 A}, \rho^{BB_0}$ and the joint measurement $\{M_i^{AB}\}$ acting on systems A, B are not characterized. We aim to certify the unknown quantum system from the measurement results of $\{M_i^{AB}\}$ and some trusted local ancillary measurements $\{N_a^{A_0}\}, \{N_b^{B_0}\}$ on systems A_0, B_0. For this purpose, we shall
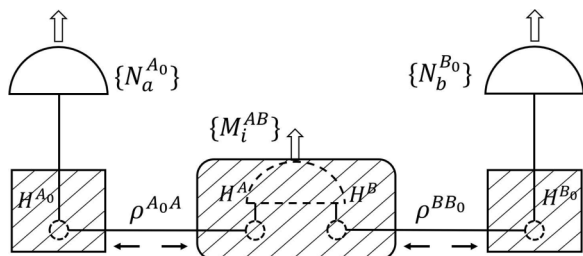
FIG. 2. The uncharacteristic entanglement swapping protocol. In this protocol, two uncharacterized states $\rho^{A_0A} \in \mathcal{D}(\mathcal{H}_{A_0} \otimes \mathcal{H}_A)$, $\rho^{BB_0} \in \mathcal{D}(\mathcal{H}_B \otimes \mathcal{H}_{B_0})$ are prepared. No information is known about the two states except for that they are both a pair of qubits. A so-called Bell state measurement is performed on the systems $\mathcal{H}_A$, $\mathcal{H}_B$. One can use well-characterized local measurements $\{N_a^{A_0}\}$, $\{N_b^{B_0}\}$ on systems A_0, B_0 to certify the results.

construct a game of which the maximum score certifies the underlying states and measurement.

Before we commence, we compare our protocol with some similar scenarios. Our entanglement swapping game is analogous to a (non)bilocal scenario [48,49] and the protocol for self-testing entangled measurements [22]. The common assumption in these scenarios is that the states ρ^{A_0A}, ρ^{BB_0} are independent, ensuring a partition between the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. In large-scale quantum networks with quantum repeaters, scenarios as shown in Fig. 2 are involved. Multiple independent quantum sources will distribute quantum states between adjacent parties, and joint quantum measurements are used to establish correlations between distant parties via entanglement swapping. As local measurements are relatively easy to apply, it might provide insights for further applications in quantum networks by investigating the nonlocal quantum correlations in protocols shown in Fig. 2.

It will be shown that the essence of our result lies in the use of an entangled measurement as well. In the following, we shall consider the case where the joint measurement $\{M_i^{AB}\}$ has only two inputs, $i \in \mathcal{I} = \{0, 1\}$. This is the general condition in a photon-based platform [50]. Because the underlying state $\rho^{A_0A} \otimes \rho^{BB_0}$ is not characterized, we say the protocol shares a source-independent nature [51].

Similarly to the treatment of effective POVM operators, the protocol can be viewed as first preparing a subnormalized positive semidefinite operator on A_0, B_0

$$\tilde{\rho}_i^{A_0B_0} = \mathrm{Tr}_{AB}\big[\big(I^{A_0} \otimes M_i^{AB} \otimes I^{B_0}\big)\big(\rho^{A_0A} \otimes \rho^{BB_0}\big)\big] \quad (6)$$

and measuring the systems A_0, B_0 subsequently. The probability of measurement outcome i on systems A, B is $\mathrm{Tr}[\tilde{\rho}_i^{A_0B_0}]$ and the corresponding state of systems A_0, B_0 becomes $\tilde{\rho}_i^{A_0B_0}/\mathrm{Tr}[\tilde{\rho}_i^{A_0B_0}]$. If we focus on one specific measurement result on systems A, B, with a duality treatment on states and measurements, then the source-independent entanglement swapping protocol can be transformed into the measurement-device-independent-type semiquantum game, except for a difference in the normalization factors of states and measurement operators. Therefore, we may construct a dual semiquantum game to certify the initial systems $\mathcal{H}_{A_0}$, $\mathcal{H}_A$ and $\mathcal{H}_B$, $\mathcal{H}_{B_0}$ and joint measurement operator simultaneously, with measurements on the final systems $\mathcal{H}_{A_0}$, $\mathcal{H}_{B_0}$ only.

With a set of tomographically complete measurements $\{N_a^{A_0}\}$, $\{N_b^{B_0}\}$ we can certify the final state of systems $\mathcal{H}_{A_0}$, $\mathcal{H}_{B_0}$. In a dual semiquantum game, a score $\beta_i^{a,b}$ is appointed to Alice and Bob based on the measurement results of $\{N_a^{A_0}\}$, $\{N_b^{B_0}\}$, $\{M_i^{AB}\}$, and the average score Alice and Bob can get is

$$
\begin{aligned}
S &= \sum_{a,b,i} \beta_i^{a,b} P(a, b, i) \\
&= \sum_{a,b,i} \beta_i^{a,b} \mathrm{Tr}\big[\big(N_a^{A_0} \otimes M_i^{AB} \otimes N_b^{B_0}\big)\big(\rho^{A_0A} \otimes \rho^{BB_0}\big)\big]. \quad (7)
\end{aligned}
$$

We now design a specific game as shown in Box 2.

In order to maximize the score, the operator $\rho_0^{A_0B_0}$ needs to be embedded in the support of $|\psi_E\rangle\langle\psi_E|$, which is much the same as the idea in the measurement-device-independent game. In our proofs for Lemma 1 and Lemma 2, we do not rely on the normalization factors but mainly the orthogonality between different eigenvectors in the spectral decomposition. Hence with a similar route, one can come to the following theorem:

Theorem 3. In the above source-independent entanglement swapping game with the assumption that all systems are two dimensional, the largest score that can be obtained is $1/4$, if and only if $(M_0^{AB})^T = |\psi_E\rangle\langle\psi_E|$, ρ^{A_0A}, $\rho^{BB_0} = |\Phi^+\rangle\langle\Phi^+|$, to local unitary operations.

Box 2: Design of the source-independent entanglement swapping game:

Game $\{N_a^{A_0}, N_b^{B_0}, \beta_i^{a,b}\}$ is designed such that

- The outcomes of local measurements $\{a, b\}$ are divided into two sets of tuples, $\{a_1, b_1\}$ and $\{a_2, b_2\}$, where $\{a_1, b_1\} \cup \{a_2, b_2\} = \{a, b\}$, $\{a_1, b_1\} \cap \{a_2, b_2\} = \emptyset$. There are effective operators constructed as

$$
\begin{aligned}
V &= V_G + V_T = \sum_{a,b,i} \beta_i^{a,b} N_a^{A_0} \otimes N_b^{B_0} \\
&= \delta_{i,0} \sum_{a,b,i} \beta_i^{a,b} N_a^{A_0} \otimes N_b^{B_0},
\end{aligned}
$$

$$V_G = |\psi_E\rangle\langle\psi_E| = \sum_{a_1,b_1} \beta_0^{a_1,b_1} N_{a_1}^{A_0} \otimes N_{b_1}^{B_0},$$

$$V_T = I^{A_0B_0} - V_G = \sum_{a_2,b_2} \beta_0^{a_2,b_2} N_{a_2}^{A_0} \otimes N_{b_2}^{B_0},$$

- $|\psi_E\rangle$ is an entangled projector,

- The average score obtained in the rounds with local measurement outcomes in the set $\{a_2, b_2\}$ is restricted to be

$$S_T = \sum_{a_2,b_2} \beta_0^{a_2,b_2} P(a_2, b_2, i = 0).$$

Goal: Maximize the average score $S = \sum_{a,b} \beta_0^{a,b} P(a, b, i = 0)$.

This theorem actually states that an entangled projector and Bell states can be certified in this game if the state $\tilde{\rho}_i^{A_0 B_0}/\mathrm{Tr}[\tilde{\rho}_i^{A_0 B_0}]$ prepared on the systems A_0, B_0 is a pure entangled state with a probability of 1/4.

It is also plausible to consider the case with a complete joint measurement over systems $\mathcal{H}_A, \mathcal{H}_B$, where under the system dimension restrictions, the measurement outcomes of the joint measurement $\{M_i^{AB}\}$ is in the set $i \in \mathcal{I}_F = \{0, 1, 2, 3\}$. We can use the result to certify the underlying joint measurement and quantum systems by observing all subnormalized operators $\{\tilde{\rho}_i^{A_0 B_0}\}$ with local measurements on systems $\mathcal{H}_{A_0}, \mathcal{H}_{B_0}$. A corollary is as follows:

Corollary 1. Under the assumption that all systems are two-dimensional, if all measurement outcomes of the joint measurement $\{M_i^{AB}\}$ occur with a probability of 1/4 and the corresponding final states $\{\tilde{\rho}_i^{A_0 B_0}/\mathrm{Tr}[\tilde{\rho}_i^{A_0 B_0}]\}$ on the systems $\mathcal{H}_{A_0}, \mathcal{H}_{B_0}$ form a complete set of Bell states under a certain choice of local bases, one can certify that the joint measurement $\{M_i^{AB}\}$ is a set of complete Bell state measurements, and $\rho^{A_0 A}$, ρ^{BB_0} are Bell states.

V. CONCLUSIONS

Via focusing on the effective POVM operator seen from the input ports in a semiquantum game, we show that any pure entangled state and Bell state measurement operators can be certified to local unitary operations. Moreover, we present the certification of Bell states and an entangled joint measurement operator in a source-independent entanglement swapping protocol, following a similar technique. This technique can also be expected to certify other types of semiquantum games, for instance, certification of a quantum memory channel [47].

It is worth noting that our method does not require a complete Bell state measurement. This can be beneficial for experiments, as a complete Bell state measurement is often not easy to achieve in practice (in particular, it is impossible to be carried out in linear optics). Due to a dimension restriction, we cannot treat our certification as a "self-testing" result. We conjecture that the quantum correlation considered in this work is extremal, and the certification results can also be obtained without the dimension restriction. Lemma 3 in our approach relies only on the ranks of the measurement operators and quantum system rather than the system's dimension, which might be a starting point for self-testing. Furthermore, robust semi-device-independent self-testing re-

sults and applications in practical blind quantum computing tasks can be expected [46,52]. We should stress here that as only one measurement outcome is used in the presented certification designs, it might be difficult to use some standard self-testing techniques in the well-studied device-independent protocols, e.g., the SWAP method [26] or the effective dimension reduction with the Jordan's lemma [15], as these methods require unitary operators corresponding to the whole set of measurement operators. This also makes it difficult to construct Bell-like nonlocal inequalities. Mathematically novel new results may be obtained along this direction. Apart from the route to a "standard self-testing" result, it is also intriguing to consider the certification problem in a higher bounded dimension. Some recent works on the prepare-and-measure semi-device-independent protocol have shown novel certification results with a freedom beyond local unitary operations in higher-dimensional systems [53,54]. It would be interesting if similar phenomena also exist in the semiquantum games.

Besides the semiquantum nonlocal game, quantum steering is an another important type of semi-device-independent protocol, which trusts the measurement on one side [55–57]. Quantum steering phenomena rely on quantum correlations which are between entanglement and violation of a Bell inequality. Some quantum states can be certified in these protocols, and it has been shown that the certification of EPR pair via quantum steering has robustness advantage over fully device-independent certification [58]. Quantum steering protocols and semiquantum nonlocal games are suitable for different tasks and practical need. While there are results showing the plausibility to combine the two protocols, yielding new types of quantum correlations [59]. We hope our work can shed light on the further exploration of semiquantum nonlocal games and other semi-device-independent protocols.

Note added. Recently, we became aware of a related work by Ivan Šupić *et al.* [60].

ACKNOWLEDGMENTS

APPENDIX A: PROOF OF THEOREM 1

For convenience, we first restate the theorem in Main text:

Theorem 1. In a semiquantum game where the input states and appointed scores form an entanglement witness, an observation of an average score $S = \mathrm{Tr}[W\tilde{M}_{0,0}^{A_0 B_0}] < 0$ necessarily indicates that $M_a^{A_0 A}$ is an entangled POVM operator on systems A_0 and A, and the same property holds for $M_b^{BB_0}$.

Proof. Suppose the POVM operator $M_a^{A_0 A} = \sum_{\lambda_1, \lambda_2} M_{\lambda_1}^{A_0} \otimes M_{\lambda_2}^{A}, M_{\lambda_1}^{A_0}, M_{\lambda_2}^{A} \geqslant 0, \forall \lambda_1, \lambda_2$, is a separable operator between A_0, A. We do not make constraints on the POVM operator $M_b^{BB_0}$ and the state ρ^{AB}. Then the subnormalized operator

$\tilde{M}_{ab}^{A_0 B_0}$ is

$$
\begin{aligned}
\tilde{M}_{ab}^{A_0 B_0} &= \mathrm{Tr}_{AB}\big[(I^{A_0} \otimes \rho^{AB} \otimes I^{B_0})(M_a^{A_0 A} \otimes M_b^{BB_0})\big] \\
&= \mathrm{Tr}_{AB}\left[(I^{A_0} \otimes \rho^{AB} \otimes I^{B_0})\left(\left(\sum_{\lambda_1,\lambda_2} M_{\lambda_1}^{A_0} \otimes M_{\lambda_2}^A\right) \otimes M_b^{BB_0}\right)\right] \\
&= \sum_{\lambda_1,\lambda_2} M_{\lambda_1}^{A_0} \otimes \mathrm{Tr}_A\big(M_{\lambda_2}^A \cdot \mathrm{Tr}_B\big[(I^A \otimes M_b^{BB_0})(\rho^{AB} \otimes I^{B_0})\big]\big),
\end{aligned}
\tag{A1}
$$

which is a separable operator acting on $\mathcal{H}_{A_0}$, $\mathcal{H}_{B_0}$. Similarly, $\tilde{M}_{ab}^{A_0 B_0}$ is separable if $M_b^{BB_0}$ is separable on B, B_0.

From a qualitative perspective, we can conclude that an entangled $\tilde{M}_{ab}^{A_0 B_0}$ not only indicates the entanglement of ρ^{AB} but also an entangled structure of the measurement operators $M_a^{A_0 A}$, $M_b^{BB_0}$. ∎

APPENDIX B: PROOF OF LEMMA 1

Lemma 1. For $\mathcal{H}_A \cong \mathcal{H}_B \cong \mathcal{H}_{A_0} \cong \mathcal{H}_{B_0} \cong \mathbb{C}^2$, $M^{A_0 A}$, M^{BB_0} rank-one entangled measurement operators over systems $\mathcal{H}_{A_0}$, $\mathcal{H}_A$ and $\mathcal{H}_{B_0}$, $\mathcal{H}_B$, and $\rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, consider the operator

$$
\tilde{M}^{A_0 B_0} = \mathrm{Tr}_{AB}[(I^{A_0} \otimes \rho^{AB} \otimes I^{B_0})(M^{A_0 A} \otimes M^{BB_0})]
\tag{B1}
$$

and a pure entangled state $|\psi\rangle \in \mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0}$. A necessary condition for $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\mathrm{span}(|\psi\rangle))$ is that ρ^{AB} is a pure state.

Proof. We apply the spectra decomposition for ρ^{AB}

$$
\rho^{AB} = \sum_{i=1}^4 \lambda_i |\Psi_i\rangle\langle\Psi_i|,
\tag{B2}
$$

where $\sum_{i=1}^4 \lambda_i = 1$, $\lambda_i \geqslant 0$, $\forall i$. We have

$$
\tilde{M}^{A_0 B_0} = \mathrm{Tr}_{AB}[(I^{A_0} \otimes \rho^{AB} \otimes I^{B_0})(M^{A_0 A} \otimes M^{BB_0})] = \sum_i \lambda_i \mathrm{Tr}_{AB}[(I^{A_0} \otimes |\Psi_i\rangle\langle\Psi_i| \otimes I^{B_0})(M^{A_0 A} \otimes M^{BB_0})]
$$

$$
\equiv \sum_i \lambda_i |\tilde{\Psi}_i\rangle\langle\tilde{\Psi}_i|.
\tag{B3}
$$

Since the entangled measurement operators $M^{A_0 A}$, M^{BB_0} are restricted to be rank-one operators, they can be treated as pure (subnormalized) states, $M^{A_0 A} = m_a |\phi^{A_0 A}\rangle\langle\phi^{A_0 A}|$, $M^{BB_0} = m_b |\phi^{BB_0}\rangle\langle\phi^{BB_0}|$, $0 \leqslant m_a, m_b \leqslant 1$. By applying the Schmidt decomposition, they can be expressed as

$$
\begin{aligned}
|\phi^{A_0 A}\rangle &= \sqrt{m_a}(\cos\alpha |\varphi^{A_0}\rangle|\varphi^A\rangle + \sin\alpha |\varphi^{A_0 \perp}\rangle|\varphi^{A\perp}\rangle), \\
|\phi^{BB_0}\rangle &= \sqrt{m_b}(\cos\beta |\varphi^{B_0}\rangle|\varphi^B\rangle + \sin\beta |\varphi^{B_0 \perp}\rangle|\varphi^{B\perp}\rangle),
\end{aligned}
\tag{B4}
$$

where $\langle\varphi^A|\varphi^{A\perp}\rangle = \langle\varphi^B|\varphi^{B\perp}\rangle = \langle\varphi^{A_0}|\varphi^{A_0 \perp}\rangle = \langle\varphi^{B_0}|\varphi^{B_0 \perp}\rangle = 0$. Since they are restricted to be entangled, we have $\sin\alpha\cos\alpha \neq 0$, $\sin\beta\cos\beta \neq 0$. Then we have

$$
\begin{aligned}
|\tilde{\Psi}_i\rangle = \sqrt{m_a m_b}(&\cos\alpha\cos\beta\langle\Psi_i|\varphi^A\varphi^B\rangle|\varphi^{A_0}\varphi^{B_0}\rangle + \cos\alpha\sin\beta\langle\Psi_i|\varphi^A\varphi^{B\perp}\rangle|\varphi^{A_0}\varphi^{B_0 \perp}\rangle \\
&+ \sin\alpha\cos\beta\langle\Psi_i|\varphi^{A\perp}\varphi^B\rangle|\varphi^{A_0 \perp}\varphi^{B_0}\rangle + \sin\alpha\sin\beta\langle\Psi_i|\varphi^{A\perp}\varphi^{B\perp}\rangle|\varphi^{A_0 \perp}\varphi^{B_0 \perp}\rangle).
\end{aligned}
\tag{B5}
$$

Now $\{|\varphi^A\rangle, |\varphi^{A\perp}\rangle\}$, $\{|\varphi^B\rangle, |\varphi^{B\perp}\rangle\}$ form complete bases for the corresponding spaces, therefore we have

$$
\langle\Psi_i|\varphi^A\varphi^B\rangle^2 + \langle\Psi_i|\varphi^{A\perp}\varphi^{B\perp}\rangle^2 + \langle\Psi_i|\varphi^{A\perp}\varphi^B\rangle^2 + \langle\Psi_i|\varphi^A\varphi^{B\perp}\rangle^2 = 1, \ \forall i.
\tag{B6}
$$

With this complete basis we can represent the eigenvectors of ρ^{AB} as

$$
|\Psi_i\rangle = e^{i\theta_{i_1}}\cos\mu_i\cos\gamma_i|\varphi^A\varphi^B\rangle + e^{i\theta_{i_2}}\cos\mu_i\sin\gamma_i|\varphi^A\varphi^{B\perp}\rangle + e^{i\theta_{i_3}}\sin\mu_i\cos\gamma_i|\varphi^{A\perp}\varphi^B\rangle + e^{i\theta_{i_4}}\sin\mu_i\sin\gamma_i|\varphi^{A\perp}\varphi^{B\perp}\rangle.
\tag{B7}
$$

Hence

$$
\begin{aligned}
|\tilde{\Psi}_i\rangle = \sqrt{m_a m_b}(&e^{i\theta_{i_1}}\cos\mu_i\cos\gamma_i\cos\alpha\cos\beta|\varphi^{A_0}\varphi^{B_0}\rangle + e^{i\theta_{i_2}}\cos\mu_i\sin\gamma_i\cos\alpha\sin\beta|\varphi^{A_0}\varphi^{B_0 \perp}\rangle \\
&+ e^{i\theta_{i_3}}\sin\mu_i\cos\gamma_i\sin\alpha\cos\beta|\varphi^{A_0 \perp}\varphi^{B_0}\rangle + e^{i\theta_{i_4}}\sin\mu_i\sin\gamma_i\sin\alpha\sin\beta|\varphi^{A_0 \perp}\varphi^{B_0 \perp}\rangle).
\end{aligned}
\tag{B8}
$$

In order that $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi\rangle))$, it necessarily restricts that $|\Psi_i\rangle \sim |\Psi_i\rangle$, $\forall i, j$. We can assume that the angle in the phase parameter $\theta_{i_k} = 0$. Now we focus on two vectors, $|\tilde{\Psi}_1\rangle$, $|\tilde{\Psi}_2\rangle$. By $|\tilde{\Psi}_1\rangle \sim |\tilde{\Psi}_2\rangle$ we require

$$\cos \mu_1 \cos \gamma_1 : \cos \mu_1 \sin \gamma_1 : \sin \mu_1 \cos \gamma_1 : \sin \mu_1 \sin \gamma_1 = \cos \mu_2 \cos \gamma_2 : \cos \mu_2 \sin \gamma_2 : \sin \mu_2 \cos \gamma_2 : \sin \mu_2 \sin \gamma_2. \quad \text{(B9)}$$

By spectral decomposition we have $|\Psi_i\rangle$ to be orthogonal to each other, which requires that

$$\cos \mu_1 \cos \gamma_1 \cos \mu_2 \cos \gamma_2 + \cos \mu_1 \sin \gamma_1 \cos \mu_2 \sin \gamma_2 + \sin \mu_1 \cos \gamma_1 \sin \mu_2 \cos \gamma_2 + \sin \mu_1 \sin \gamma_1 \sin \mu_2 \sin \gamma_2 = 0. \quad \text{(B10)}$$

Besides, as $|\psi\rangle$ is entangled, one cannot have both $\sin \mu_i \cos \mu_i = 0$ and $\sin \gamma_i \cos \gamma_i = 0$. Obviously, we cannot have a nontrivial result satisfying all the requirements. Therefore, under the described constraints one cannot have $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi\rangle))$ by measuring a mixed quantum state $\rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

On the other hand, one can obtain an entangled operator $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi\rangle))$ with a pure entangled state $\rho^{AB} = |\Psi\rangle\langle\Psi|$; see the construction yielding the certification result in Theorem 2 in the main text for example. This finishes the proof of Lemma 1. ∎

APPENDIX C: PROOF OF LEMMA 2

Lemma 2. For $\mathcal{H}_A \cong \mathcal{H}_B \cong \mathcal{H}_{A_0} \cong \mathcal{H}_{B_0} \cong \mathbb{C}^2$, a pure entangled state $|\psi\rangle \in \mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0}$, and a pure bipartite entangled quantum state $\rho^{AB} = |\Psi\rangle\langle\Psi|$ over systems $\mathcal{H}_A$, $\mathcal{H}_B$, a necessary condition for $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi\rangle))$ is that both $M^{A_0 A}$ and $M^{B B_0}$ are rank-one entangled operators over systems $\mathcal{H}_A$, $\mathcal{H}_{A_0}$ and $\mathcal{H}_B$, $\mathcal{H}_{B_0}$, where $\tilde{M}^{A_0 B_0}$ is the same operator as in Eq. (B1).

Proof. We assume that the POVM element on Bob's side is a rank-one operator, $M^{B B_0} = |\phi^{B B_0}\rangle\langle\phi^{B B_0}|$, while the element on Alice's side $M^{B B_0}$ is not. We now focus on two eigenvectors of $M^{A_0 A}$, $|\phi_1^{A_0 A}\rangle$, $|\phi_2^{A_0 A}\rangle$. We apply the Schmidt decomposition on these vectors and without loss of generality we write

$$\begin{aligned}
\left|\phi_1^{A_0 A}\right\rangle &= \cos \alpha_1 \left|\varphi_1^{A_0}\right\rangle\left|\varphi_1^A\right\rangle + \sin \alpha_1 \left|\varphi_1^{A_0 \perp}\right\rangle\left|\varphi_1^{A \perp}\right\rangle, \\
\left|\phi_2^{A_0 A}\right\rangle &= \cos \alpha_2 \left|\varphi_2^{A_0}\right\rangle\left|\varphi_2^A\right\rangle + \sin \alpha_2 \left|\varphi_2^{A_0 \perp}\right\rangle\left|\varphi_2^{A \perp}\right\rangle, \\
\left|\phi^{B B_0}\right\rangle &= \cos \beta \left|\varphi^{B_0}\right\rangle\left|\varphi^B\right\rangle + \sin \beta \left|\varphi^{B_0 \perp}\right\rangle\left|\varphi^{B \perp}\right\rangle,
\end{aligned} \quad \text{(C1)}$$

where $\langle\varphi_1^{A_0}|\varphi_1^{A_0 \perp}\rangle = \langle\varphi_1^A|\varphi_1^{A \perp}\rangle = \langle\varphi_2^{A_0}|\varphi_2^{A_0 \perp}\rangle = \langle\varphi_2^A|\varphi_2^{A \perp}\rangle = 0$. Since it is assumed that $\mathcal{H}_{A_0} \cong \mathcal{H}_A \cong \mathbb{C}^2$, using extra degrees of freedom, let

$$\begin{aligned}
\left|\varphi_2^{A_0}\right\rangle &= \cos \gamma \left|\varphi_1^{A_0}\right\rangle + \sin \gamma \left|\varphi_1^{A_0 \perp}\right\rangle, \\
\left|\varphi_2^{A_0 \perp}\right\rangle &= \sin \gamma \left|\varphi_1^{A_0}\right\rangle - \cos \gamma \left|\varphi_1^{A_0 \perp}\right\rangle, \\
\left|\varphi_2^A\right\rangle &= \cos \chi \left|\varphi_1^A\right\rangle + \sin \chi \left|\varphi_1^{A \perp}\right\rangle, \\
\left|\varphi_2^{A \perp}\right\rangle &= \sin \chi \left|\varphi_1^A\right\rangle - \cos \chi \left|\varphi_1^{A \perp}\right\rangle.
\end{aligned} \quad \text{(C2)}$$

By $\langle\phi_1^{A_0 A}|\phi_2^{A_0 A}\rangle = 0$ we have

$$\cos \alpha_1 \cos \alpha_2 \cos \gamma \cos \chi + \cos \alpha_1 \sin \alpha_2 \sin \gamma \sin \chi + \sin \alpha_1 \cos \alpha_2 \sin \gamma \sin \chi + \sin \alpha_1 \sin \alpha_2 \cos \gamma \cos \chi = 0. \quad \text{(C3)}$$

In order that the operator $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\text{span}(|\psi\rangle))$, which is entangled over systems $\mathcal{H}_{A_0}$, $\mathcal{H}_{B_0}$, it is required that $M^{A A_0}$, $M^{B B_0}$ are entangled over systems $\mathcal{H}_A$, $\mathcal{H}_{A_0}$ and $\mathcal{H}_B$, $\mathcal{H}_{B_0}$. Therefore we have $\sin \alpha_1 \cos \alpha_1 \neq 0$, $\sin \alpha_2 \cos \alpha_2 \neq 0$, $\sin \beta \cos \beta \neq 0$.

For the effective POVM operator,

$$\tilde{M}^{A_0 B_0} = \text{Tr}_{AB}[(I^{A_0} \otimes \rho^{AB} \otimes I^{B_0})(M^{A_0 A} \otimes M^{B B_0})] = \sum_i \text{Tr}_{AB}[(I^{A_0} \otimes |\Psi\rangle\langle\Psi| \otimes I^{B_0})(|\phi_i^{A_0 A}\rangle\langle\phi_i^{A_0 A}| \otimes M^{B B_0})]$$

$$\equiv \sum_i |\tilde{\Psi}_i\rangle\langle\tilde{\Psi}_i|, \quad \text{(C4)}$$

with

$$\begin{aligned}
|\tilde{\Psi}_1\rangle &= \cos \alpha_1 \cos \beta \langle\Psi|\varphi_1^A \varphi^B\rangle |\varphi_1^{A_0} \varphi^{B_0}\rangle + \cos \alpha_1 \sin \beta \langle\Psi|\varphi_1^A \varphi^{B \perp}\rangle |\varphi_1^{A_0} \varphi^{B_0 \perp}\rangle \\
&\quad + \sin \alpha_1 \cos \beta \langle\Psi|\varphi_1^{A \perp} \varphi^B\rangle |\varphi_1^{A_0 \perp} \varphi^{B_0}\rangle + \sin \alpha_1 \sin \beta \langle\Psi|\varphi_1^{A \perp} \varphi^{B \perp}\rangle |\varphi_1^{A_0 \perp} \varphi^{B_0 \perp}\rangle,
\end{aligned} \quad \text{(C5)}$$

$$\begin{aligned}
|\tilde{\Psi}_2\rangle &= \cos \alpha_2 \cos \beta \langle\Psi|\varphi_2^A \varphi^B\rangle |\varphi_2^{A_0} \varphi^{B_0}\rangle + \cos \alpha_2 \sin \beta \langle\Psi|\varphi_2^A \varphi^{B \perp}\rangle |\varphi_2^{A_0} \varphi^{B_0 \perp}\rangle \\
&\quad + \sin \alpha_2 \cos \beta \langle\Psi|\varphi_2^{A \perp} \varphi^B\rangle |\varphi_2^{A_0 \perp} \varphi^{B_0}\rangle + \sin \alpha_2 \sin \beta \langle\Psi|\varphi_2^{A \perp} \varphi^{B \perp}\rangle |\varphi_2^{A_0 \perp} \varphi^{B_0 \perp}\rangle \\
&= \big[\cos \alpha_2 \cos \beta \big(\cos \gamma \cos \chi \langle\Psi|\varphi_1^A \varphi^B\rangle + \cos \gamma \sin \chi \langle\Psi|\varphi_1^{A \perp} \varphi^B\rangle \big) \\
&\quad + \sin \alpha_2 \cos \beta \big(\sin \gamma \sin \chi \langle\Psi|\varphi_1^A \varphi^B\rangle - \sin \gamma \cos \chi \langle\Psi|\varphi_1^{A \perp} \varphi^B\rangle \big) \big] |\varphi_1^{A_0} \varphi^{B_0}\rangle
\end{aligned}$$

$$+ \left[\cos \alpha_2 \sin \beta \left(\cos \gamma \cos \chi \langle \Psi | \varphi_1^A \varphi^{B\perp} \rangle + \cos \gamma \sin \chi \langle \Psi | \varphi_1^{A\perp} \varphi^{B\perp} \rangle \right) \right.$$

$$\left. + \sin \alpha_2 \sin \beta \left(\sin \gamma \sin \chi \langle \Psi | \varphi_1^A \varphi^{B\perp} \rangle - \sin \gamma \cos \chi \langle \Psi | \varphi_1^{A\perp} \varphi^{B\perp} \rangle \right) \right] | \varphi_1^{A_0} \varphi^{B_0\perp} \rangle$$

$$+ \left[\cos \alpha_2 \cos \beta \left(\sin \gamma \cos \chi \langle \Psi | \varphi_1^A \varphi^B \rangle + \sin \gamma \sin \chi \langle \Psi | \varphi_1^{A\perp} \varphi^B \rangle \right) \right.$$

$$\left. + \sin \alpha_2 \cos \beta \left(- \cos \gamma \sin \chi \langle \Psi | \varphi_1^A \varphi^B \rangle + \cos \gamma \cos \chi \langle \Psi | \varphi_1^{A\perp} \varphi^B \rangle \right) \right] | \varphi_1^{A_0\perp} \varphi^{B_0} \rangle$$

$$+ \left[\cos \alpha_2 \sin \beta \left(\sin \gamma \cos \chi \langle \Psi | \varphi_1^A \varphi^{B\perp} \rangle + \sin \gamma \sin \chi \langle \Psi | \varphi_1^{A\perp} \varphi^{B\perp} \rangle \right) \right.$$

$$\left. + \sin \alpha_2 \sin \beta \left(- \cos \gamma \sin \chi \langle \Psi | \varphi_1^A \varphi^{B\perp} \rangle + \cos \gamma \cos \chi \langle \Psi | \varphi_1^{A\perp} \varphi^{B\perp} \rangle \right) \right] | \varphi_1^{A_0\perp} \varphi^{B_0\perp} \rangle. \tag{C6}$$

We assume that $|\tilde{\Psi}_1\rangle \in \mathrm{span}(|\psi\rangle)$. In order that $|\tilde{\Psi}_2\rangle \in \mathrm{span}(|\psi\rangle)$ and Eq. (C3) holds, one can only have $\langle \Psi | \varphi_1^A \varphi^B \rangle = \langle \Psi | \varphi_1^{A\perp} \varphi^B \rangle = \langle \Psi | \varphi_1^A \varphi^{B\perp} \rangle = \langle \Psi | \varphi_1^{A\perp} \varphi^{B\perp} \rangle = 0$, which is contradictory to that $\{|\varphi^A\rangle, |\varphi^{A\perp}\rangle\}$, $\{|\varphi^B\rangle, |\varphi^{B\perp}\rangle\}$ are complete bases. Then we can conclude that a general POVM will inevitably result in a mixed $\tilde{M}^{A_0 B_0}$. In summary, under the given constraints, a necessary condition for $\tilde{M}^{A_0 B_0} \in \mathcal{L}(\mathrm{span}(|\psi\rangle))$ is that both $M^{A_0 A}$ and $M^{B B_0}$ are rank-one entangled operators over systems $\mathcal{H}_A$, $\mathcal{H}_{A_0}$ and $\mathcal{H}_B$, $\mathcal{H}_{B_0}$. ∎

APPENDIX D: PROOF OF LEMMA 3

Lemma 3. For rank-one projectors $M^{A_0 A} = |\phi^{A_0 A}\rangle \langle \phi^{A_0 A}| \in \mathcal{L}(\mathcal{H}_{A_0} \otimes \mathcal{H}_A)$, $M^{B B_0} = |\phi^{B B_0}\rangle \langle \phi^{B B_0}| \in \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_{B_0})$, where $\mathcal{H}_{A_0}, \mathcal{H}_{B_0} \cong \mathbb{C}^2$, fix the measurement bases of $\mathcal{H}_{A_0}, \mathcal{H}_{B_0}$ to be $\{|0\rangle, |1\rangle\}_{A_0, B_0}$ and express the projectors as

$$|\phi^{A_0 A}\rangle = \cos \alpha |0\rangle |\varphi^A\rangle + \sin \alpha |1\rangle |\bar{\varphi}^A\rangle, \quad |\phi^{B B_0}\rangle = \cos \beta |0\rangle |\varphi^B\rangle + \sin \beta |1\rangle |\bar{\varphi}^B\rangle. \tag{D1}$$

In the condition that $\langle \Psi | \varphi^A \bar{\varphi}^B \rangle = \langle \Psi | \bar{\varphi}^A \varphi^B \rangle = 0$, we have $|\langle \Psi | \varphi^A \varphi^B \rangle|^2 + |\langle \Psi | \bar{\varphi}^A \bar{\varphi}^B \rangle|^2 \leqslant 1$. The equality is taken iff $\langle \varphi^A | \bar{\varphi}^A \rangle = \langle \varphi^B | \bar{\varphi}^B \rangle = 0$, and the subspaces of the two parties are spanned by $\{|\varphi^A\rangle, |\bar{\varphi}^A\rangle\}$, $\{|\varphi^B\rangle, |\bar{\varphi}^B\rangle\}$, respectively. In particular, no restriction on the dimensions of $\mathcal{H}_A$, $\mathcal{H}_B$ is made.

Proof. In the proof for this lemma, we do not restrict the dimensions of $\mathcal{H}_A$, $\mathcal{H}_B$. Let

$$|\bar{\varphi}^A\rangle = \cos \theta |\varphi^A\rangle + \sin \theta |\varphi^{A\perp}\rangle, \quad |\bar{\varphi}^B\rangle = \cos \gamma |\varphi^B\rangle + \sin \gamma |\varphi^{B\perp}\rangle, \tag{D2}$$

where $|\varphi^{A\perp}\rangle$, $|\varphi^{B\perp}\rangle$ are some states that lay orthogonally to $|\varphi^A\rangle$, $|\varphi^B\rangle$ in the subspaces of Alice and Bob, respectively. Then we have

$$\langle \Psi | \bar{\varphi}^A \bar{\varphi}^B \rangle = \cos \theta \cos \gamma \langle \Psi | \varphi^A \varphi^B \rangle + \cos \theta \sin \gamma \langle \Psi | \varphi^A \varphi^{B\perp} \rangle + \sin \theta \cos \gamma \langle \Psi | \varphi^{A\perp} \varphi^B \rangle + \sin \theta \sin \gamma \langle \Psi | \varphi^{A\perp} \varphi^{B\perp} \rangle. \tag{D3}$$

Since $\langle \Psi | \varphi^A \bar{\varphi}^B \rangle = 0$, we have

$$\cos \gamma \langle \Psi | \varphi^A \varphi^B \rangle + \sin \gamma \langle \Psi | \varphi^A \varphi^{B\perp} \rangle = 0. \tag{D4}$$

Similarly,

$$\cos \theta \langle \Psi | \varphi^A \varphi^B \rangle + \sin \theta \langle \Psi | \varphi^{A\perp} \varphi^B \rangle = 0. \tag{D5}$$

Therefore, we derive the following equation:

$$\langle \Psi | \bar{\varphi}^A \bar{\varphi}^B \rangle = - \cos \theta \cos \gamma \langle \Psi | \varphi^A \varphi^B \rangle + \sin \theta \sin \gamma \langle \Psi | \varphi^{A\perp} \varphi^{B\perp} \rangle. \tag{D6}$$

On the other hand, required by Eq. (D4)(D5), as long as $|\varphi^A\rangle \neq |\bar{\varphi}^A\rangle$, $|\varphi^B\rangle \neq |\bar{\varphi}^B\rangle$, there are following relations:

$$\langle \Psi | \varphi^A \varphi^{B\perp} \rangle = - \frac{\cos \gamma}{\sin \gamma} \langle \Psi | \varphi^A \varphi^B \rangle, \quad \langle \Psi | \varphi^{A\perp} \varphi^B \rangle = - \frac{\cos \theta}{\sin \theta} \langle \Psi | \varphi^A \varphi^B \rangle. \tag{D7}$$

As $|\varphi^A \varphi^B\rangle$, $|\varphi^A \varphi^{B\perp}\rangle$, $|\varphi^{A\perp} \varphi^B\rangle$, $|\varphi^{A\perp} \varphi^{B\perp}\rangle$ are orthogonal to each other, the following inequality holds:

$$|\langle \Psi | \varphi^{A\perp} \varphi^{B\perp} \rangle|^2 \leqslant 1 - |\langle \Psi | \varphi^A \varphi^B \rangle|^2 - |\langle \Psi | \varphi^A \varphi^{B\perp} \rangle|^2 - |\langle \Psi | \varphi^{A\perp} \varphi^B \rangle|^2 = 1 - \left(1 + \frac{\cos^2 \gamma}{\sin^2 \gamma} + \frac{\cos^2 \theta}{\sin^2 \theta} \right) |\langle \Psi | \varphi^A \varphi^B \rangle|^2, \tag{D8}$$

and thereafter

$$|\langle \Psi | \bar{\varphi}^A \bar{\varphi}^B \rangle|^2 = \cos^2 \theta \cos^2 \gamma |\langle \Psi | \varphi^A \varphi^B \rangle|^2 + \sin^2 \theta \sin^2 \gamma |\langle \Psi | \varphi^{A\perp} \varphi^{B\perp} \rangle|^2 - 2 \sin \theta \cos \theta \sin \gamma \cos \gamma \langle \Psi | \varphi^A \varphi^B \rangle \langle \Psi | \varphi^{A\perp} \varphi^{B\perp} \rangle$$

$$\leqslant \cos^2 \theta \cos^2 \gamma |\langle \Psi | \varphi^A \varphi^B \rangle|^2 + \sin^2 \theta \sin^2 \gamma \left[1 - \left(1 + \frac{\cos^2 \gamma}{\sin^2 \gamma} + \frac{\cos^2 \theta}{\sin^2 \theta} \right) |\langle \Psi | \varphi^A \varphi^B \rangle|^2 \right]$$

$$+ 2 \sin \theta \cos \theta \sin \gamma \cos \gamma |\langle \Psi | \varphi^A \varphi^B \rangle| \sqrt{1 - \left(1 + \frac{\cos^2 \gamma}{\sin^2 \gamma} + \frac{\cos^2 \theta}{\sin^2 \theta} \right) |\langle \Psi | \varphi^A \varphi^B \rangle|^2}, \tag{D9}$$

thus

$$|\langle\Psi|\varphi^A\varphi^B\rangle|^2 + |\langle\Psi|\bar{\varphi}^A\bar{\varphi}^B\rangle|^2 \leqslant \sin^2\theta\sin^2\gamma + (1 + \cos^2\theta\cos^2\gamma - \sin^2\theta\sin^2\gamma - \sin^2\theta\cos^2\gamma - \cos^2\theta\sin^2\gamma)|\langle\Psi|\varphi^A\varphi^B\rangle|^2$$

$$+ 2\sin\theta\cos\theta\sin\gamma\cos\gamma|\langle\Psi|\varphi^A\varphi^B\rangle|\sqrt{1 - \left(1 + \frac{\cos^2\gamma}{\sin^2\gamma} + \frac{\cos^2\theta}{\sin^2\theta}\right)|\langle\Psi|\varphi^A\varphi^B\rangle|^2}$$

$$= \sin^2\theta\sin^2\gamma + 2\cos^2\theta\cos^2\gamma|\langle\Psi|\varphi^A\varphi^B\rangle|^2$$

$$+ 2\sin\theta\cos\theta\sin\gamma\cos\gamma|\langle\Psi|\varphi^A\varphi^B\rangle|\sqrt{1 - \left(1 + \frac{\cos^2\gamma}{\sin^2\gamma} + \frac{\cos^2\theta}{\sin^2\theta}\right)|\langle\Psi|\varphi^A\varphi^B\rangle|^2}. \tag{D10}$$

For the right side of this inequality, it can be regarded as a function of the form $f(x) = ax^2 + bx\sqrt{1 - cx^2} + d$, with the variant

$$x = |\langle\Psi|\varphi^A\varphi^B\rangle| \in [0, 1], \tag{D11}$$

and the coefficients

$$a = 2\cos^2\theta\cos^2\gamma,$$
$$b = 2\sin\theta\cos\theta\sin\gamma\cos\gamma,$$
$$c = 1 + \frac{\cos^2\gamma}{\sin^2\gamma} + \frac{\cos^2\theta}{\sin^2\theta},$$
$$d = \sin^2\theta\sin^2\gamma. \tag{D12}$$

In our problem, $c \geqslant 1$, hence it is required that $x^2 \geqslant \frac{1}{c}$. The derivative of $f(x)$ is

$$f'(x) = 2ax + b\sqrt{1 - cx^2} - \frac{bcx^2}{1 - cx^2}. \tag{D13}$$

Let $f'(x) = 0$ and we have

$$x^2 = \frac{1}{2c} \pm \frac{a}{2c}\frac{1}{\sqrt{a^2 + b^2c}}, \tag{D14}$$

where the term $\frac{a}{2c}\frac{1}{\sqrt{a^2+b^2c}} \leqslant \frac{a}{2c}\frac{1}{a} = \frac{1}{2c}$, so we are able to take the value $x = \pm\sqrt{\frac{1}{2c} \pm \frac{a}{2c}\frac{1}{\sqrt{a^2+b^2c}}}$. By some calculation with respect to $f'(x)$, for the maximum value of $f(x)$, we only need to consider its value at the points $x = \sqrt{\frac{1}{c}}$ and $x = \sqrt{\frac{1}{2c} - \frac{a}{2c}\frac{1}{\sqrt{a^2+b^2c}}}$.

(1) $x = \sqrt{\frac{1}{c}}$:
The function value at this point

$$f(x) = \frac{a}{c} + d = \frac{2\cos^2\theta\cos^2\gamma}{1 + \frac{\cos^2\gamma}{\sin^2\gamma} + \frac{\cos^2\theta}{\sin^2\theta}} + \sin^2\theta\sin^2\gamma = \frac{1 + \cos^2\theta\cos^2\gamma}{1 + \frac{\cos^2\gamma}{\sin^2\gamma} + \frac{\cos^2\theta}{\sin^2\theta}} \leqslant 1, \tag{D15}$$

and the equality is taken iff $\cos\theta = \cos\gamma = 0$. This indicates that $\langle\varphi^A|\bar{\varphi}^A\rangle = \langle\varphi^B|\bar{\varphi}^B\rangle = 0$.

(2) $x = \sqrt{\frac{1}{2c} - \frac{a}{2c}\frac{1}{\sqrt{a^2+b^2c}}}$:
The function value at this point

$$f(x) = ax^2 + bx\sqrt{1 - \left(\frac{1}{2} - \frac{a}{2}\frac{1}{\sqrt{a^2+b^2c}}\right)} + d = \frac{a}{2c} + \frac{1}{2c}\frac{b^2c - a^2}{\sqrt{b^2c+a^2}} + d = \frac{1 + \cos\theta\cos\gamma - 2\cos^3\theta\cos^3\gamma}{1 + \frac{\cos^2\gamma}{\sin^2\gamma} + \frac{\cos^2\theta}{\sin^2\theta}} \leqslant 1, \tag{D16}$$

and the equality is taken iff $\cos\theta = \cos\gamma = 0$.

Above all, we come to the conclusion that when $\langle\Psi|\varphi^A\bar{\varphi}^B\rangle = \langle\Psi|\bar{\varphi}^A\varphi^B\rangle = 0$, the inequality $|\langle\Psi|\varphi^A\varphi^B\rangle|^2 + |\langle\Psi|\bar{\varphi}^A\bar{\varphi}^B\rangle|^2 \leqslant 1$ holds, and equality is taken iff $\langle\varphi^A|\bar{\varphi}^A\rangle = \langle\varphi^B|\bar{\varphi}^B\rangle = 0$, and the subspaces of Alice and Bob are spanned by $\{|\varphi^A\rangle, |\bar{\varphi}^A\rangle\}$, $\{|\varphi^B\rangle, |\bar{\varphi}^B\rangle\}$, respectively [notice the inequality scaling (D8)]. ∎

---

[1] M. G. Raymer, M. Beck, and D. F. McAlister, Phys. Rev. Lett. **72**, 1137 (1994).

[2] U. Leonhardt, Phys. Rev. A **53**, 2998 (1996).

[3] U. Leonhardt, *Measuring the Quantum State of Light* (Cambridge University Press, Cambridge, 1997), Vol. 22.

[4] J. F. Poyatos, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **78**, 390 (1997).

[5] I. L. Chuang and M. A. Nielsen, J. Mod. Opt. **44**, 2455 (1997).

[6] G. M. D'Ariano and P. LoPresti, Phys. Rev. Lett. **86**, 4195 (2001).

[7] J. Bell, Phys. Phys. Fiz. **1**, 195 (1964).

[8] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[9] D. Mayers and A. Yao, arXiv:quant-ph/0307205.

[10] T. H. Yang and M. Navascués, Phys. Rev. A **87**, 050102(R) (2013).

[11] A. Coladangelo, K. T. Goh, and V. Scarani, Nat. Commun. **8**, 15485 (2017).

[12] M. McKague, in *Conference on Quantum Computation, Communication, and Cryptography* (Springer, Berlin, 2011), pp. 104–120.

[13] K. F. Pál, T. Vértesi, and M. Navascués, Phys. Rev. A **90**, 042340 (2014).

[14] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, Phys. Rev. A **90**, 042339 (2014).

[15] J. Kaniewski, Phys. Rev. Lett. **117**, 070402 (2016).

[16] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, New J. Phys. **20**, 083041 (2018).

[17] Q. Zhao and Y. Zhou, arXiv:2002.01843.

[18] M. McKague and M. Mosca, in *Conference on Quantum Computation, Communication, and Cryptography* (Springer, Berlin, 2010), pp. 113–130.

[19] C. Bamps and S. Pironio, Phys. Rev. A **91**, 052111 (2015).

[20] I. Šupić, R. Augusiak, A. Salavrakos, and A. Acín, New J. Phys. **18**, 035013 (2016).

[21] J. Kaniewski, Phys. Rev. A **95**, 062323 (2017).

[22] M. O. Renou, J. Kaniewski, and N. Brunner, Phys. Rev. Lett. **121**, 250507 (2018).

[23] J.-D. Bancal, N. Sangouard, and P. Sekatski, Phys. Rev. Lett. **121**, 250506 (2018).

[24] J. Kaniewski, I. Šupić, J. Tura, F. Baccari, A. Salavrakos, and R. Augusiak, Quantum **3**, 198 (2019).

[25] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, Phys. Rev. Lett. **121**, 180505 (2018).

[26] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A **45**, 455304 (2012).

[27] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang, Phys. Rev. A **91**, 022115 (2015).

[28] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, Phys. Rev. Lett. **113**, 040401 (2014).

[29] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán *et al.*, Phys. Rev. Lett. **115**, 250401 (2015).

[30] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán *et al.*, Nature (Lond.) **526**, 682 (2015).

[31] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman *et al.*, Phys. Rev. Lett. **115**, 250402 (2015).

[32] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, Phys. Rev. Lett. **119**, 010402 (2017).

[33] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan *et al.*, Nature (Lond.) **562**, 548 (2018).

[34] M.-H. Li, X. Zhang, W.-Z. Liu, S.-R. Zhao, B. Bai, Y. Liu, Q. Zhao, Y. Peng, J. Zhang, X. Ma *et al.*, arXiv:1902.07529v2.

[35] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji *et al.*, arXiv:1912.11158.

[36] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan *et al.*, arXiv:1912.11159.

[37] F. Buscemi, Phys. Rev. Lett. **108**, 200401 (2012).

[38] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Phys. Rev. Lett. **110**, 060405 (2013).

[39] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **112**, 140506 (2014).

[40] E. Verbanis, A. Martin, D. Rosset, C. C. W. Lim, R. T. Thew, and H. Zbinden, Phys. Rev. Lett. **116**, 190501 (2016).

[41] Q. Zhao, X. Yuan, and X. Ma, Phys. Rev. A **94**, 012343 (2016).

[42] F. Shahandeh, M. J. W. Hall, and T. C. Ralph, Phys. Rev. Lett. **118**, 150505 (2017).

[43] O. Regev and T. Vidick, ACM Trans. Comput. Theory **7**, 15 (2015).

[44] I. Šupić, P. Skrzypczyk, and D. Cavalcanti, Phys. Rev. A **95**, 042340 (2017).

[45] Z.-D. Li, Q. Zhao, R. Zhang, L.-Z. Liu, X.-F. Yin, X. Zhang, Y.-Y. Fei, K. Chen, N.-L. Liu, F. Xu *et al.*, Phys. Rev. Lett. **124**, 160503 (2020).

[46] H.-L. Huang, Q. Zhao, X. Ma, C. Liu, Z.-E. Su, X.-L. Wang, L. Li, N.-L. Liu, B. C. Sanders, C.-Y. Lu, and J.-W. Pan, Phys. Rev. Lett. **119**, 050503 (2017).

[47] D. Rosset, F. Buscemi, and Y.-C. Liang, Phys. Rev. X **8**, 021033 (2018).

[48] C. Branciard, N. Gisin, and S. Pironio, Phys. Rev. Lett. **104**, 170401 (2010).

[49] C. Branciard, D. Rosset, N. Gisin, and S. Pironio, Phys. Rev. A **85**, 032119 (2012).

[50] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Phys. Rev. A **59**, 3295 (1999).

[51] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).

[52] B. W. Reichardt, F. Unger, and U. Vazirani, Nature (Lond.) **496**, 456 (2013).

[53] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Phys. Rev. A **98**, 062307 (2018).

[54] M. Farkas and J. Kaniewski, Phys. Rev. A **99**, 032316 (2019).

[55] E. Schrödinger, in *Mathematical Proceedings of the Cambridge Philosophical Society* (Cambridge University Press, Cambridge, 1935), Vol. 31, pp. 555–563.

[56] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).

[57] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Rev. Mod. Phys. **92**, 015001 (2020).

[58] I. Šupić and M. J. Hoban, New J. Phys. **18**, 075006 (2016).

[59] E. G. Cavalcanti, M. J. W. Hall, and H. M. Wiseman, Phys. Rev. A **87**, 032306 (2013).

[60] I. Šupić, M. J. Hoban, L. D. Colomer, and A. Acín, New J. Phys. **22**, 073006 (2020).