Oblivious communication game, self-testing of projective and nonprojective measurements, and certification of randomness

A. K. Pan*
National Institute of Technology Patna, Ashok Rajpath, Patna, Bihar 800005, India

(Received 1 November 2020; revised 13 January 2021; accepted 9 August 2021; published 23 August 2021)

We provide an interesting two-party parity-oblivious communication game whose success probability is solely determined by the Bell expression. The parity-oblivious condition in an operational quantum theory implies the preparation noncontextuality in an ontological model of it. We find that the aforementioned Bell expression has two upper bounds in an ontological model: the usual local bound and a nontrivial preparation noncontextual bound arising from the nontrivial parity-oblivious condition, which is smaller that the local bound. We first demonstrate the communication game when both Alice and Bob perform three measurements of dichotomic observables in their respective sites. The optimal quantum value of the Bell expression in this scenario enables us to device-independently self-test the maximally entangled state and trine set of observables, three-outcome qubit positive-operator-valued measures and 1.58 bits of local randomness. Further, we generalize the above communication game in that both Alice and Bob perform the same but arbitrary (odd) number ($n > 3$) of measurements. Based on the optimal quantum value of the relevant Bell expression for any arbitrary n, we also demonstrate device-independent self-testing of the state and measurements.

DOI: 10.1103/PhysRevA.104.022212

I. INTRODUCTION

The Bell theorem [1] is at the heart of quantum foundations. This no-go proof asserts that every quantum statistics cannot be accounted for by any ontological model satisfying locality. Later, it was found that Bell's theorem certifies the nonlocal correlation in a device-independent way in that no characterization of devices needs to be assumed. Besides the immense impact of Bell's theorem on conceptual foundations of quantum theory, the device-independent quantum certification based on it has led to many potential practical applications (for a review see [2]) in quantum information processing tasks.

Another pertinent no-go proof in quantum foundations, the Kochen-Specker (KS) [3] theorem, proves an inconsistency between the quantum theory and noncontextual ontological models. While the demonstration of Bell's theorem requires two or more spacelike separated systems, the KS theorem can also be demonstrated for a single system having dimension of the Hilbert space $d \geqslant 3$. However, the traditional KS notion of noncontextuality is merely applicable to the deterministic ontological models of quantum theory and the ontic states strictly provide the values corresponding to the sharp projective measurements only. The notion of KS noncontextuality was further generalized by Spekkens [4] for positive-operator-valued measures (POVMs) in any arbitrary operational theory. He also extended the formulation to the transformation and preparation noncontextuality. In the present work, the notion of preparation contextuality plays an important role.

The communication games [5–27] are widely used tools for studying the fundamental limiting features of an operational theory in terms of their ability to process information. In such a game, two or more parties jointly perform a given task with the highest possible efficiency despite the amount and type of communication being constrained by some rules. In terms of the nature of communication from sender to receiver, there are two major classes of games: one in which the dimension of the communicated system in classical or quantum theory is bounded and another in which the obliviousness condition on the communication is imposed without any restriction on the dimension of the system and/or on the amount of communication. There is yet another class of games using energy constraints [22] and information content constraints [27]. Both classes of communication games can be played either in the prepare-and-measure scenario or in the entanglement-assisted scenario [17–21,23–26]. The well-known parity-oblivious random access code [17–20,23] is one such communication game.

In this work, we provide an interesting two-party oblivious communication game in which the sender (Alice) is allowed to communicate any amount of information but that should not reveal the parity information of the inputs to the receiver (Bob). We demonstrate that the success probability of this parity-oblivious communication game is solely dependent on a suitable Bell expression. Note here that obliviousness in an operational theory can equivalently be represented as obliviousness at the level of ontic states if the ontological model of that operational theory is preparation noncontextual [17]. In this connection, it is also worthwhile to note that, in two-input–two-output Bell scenario the preparation noncontextuality assumption in an ontological model of quantum theory can also be viewed as a locality condition [28,29].

*akp@nitp.ac.in

We call it a trivial preparation noncontextuality condition. However, in a two-party Bell scenario beyond the two-input–two-output one there could be certain forms of oblivious condition which can lead to nontrivial restriction on the choices of inputs. In such a case the upper bound of the Bell expression may be reduced from the trivial case (the local bound), which we term here a nontrivial preparation noncontextual bound. Thus, for a specific choice of states and measurements, it is possible that the optimal quantum value of the Bell expression may not be large enough to exhibit nonlocality, but the nonclassicality in the form of nontrivial preparation contextuality may still be revealed. In quantum theory, the optimal value of the Bell expressions enables one to self-test the state and measurements.

Specifically, we propose an entanglement-assisted parity-oblivious communication game in that both Alice and Bob receive inputs $x, y \in \{1, 2, \ldots, n\}$ with odd $n \geqslant 3$ and according to which they perform local measurements on their respective sites. Each of the local measurements produces dichotomic outputs $a, b \in \{0, 1\}$. The inputs of Alice satisfy a parity-oblivious condition and this in turn provides that a functional relationship between Alice's observables has to be satisfied. We show that the success probability of the communication game is solely determined by the value of a family of Bell expressions (say, $\mathcal{B}_n$) which has a local bound and a nontrivial preparation noncontextual bound. We demonstrate that an optimal quantum value $(\mathcal{B}_n)_Q^{\text{opt}}$ enables one to device-independently self-test the entangled state and a set of projective measurements.

We first demonstrate the communication game for $n = 3$, which allows us to self-test a trine set of observables and entangled state. We then show that a simple modification of the aforementioned game can certify the three-outcome qubit POVMs, which in turn can be used to certify 1.58 bits of local randomness. Further, we generalize the aforementioned three-input game to any (odd) arbitrary n input game and optimal quantum success probability enables the self-testing of a maximally entangled state and a set of observables. We further discuss that such a generalization does not enable us to certify the randomness.

The plan of the paper is the following. In Sec. II we provide the preliminaries of the oblivious communication game, the notion of preparation noncontextuality in an ontological model, the self-testing protocols, and the device-independent randomness certification. In Sec. III we provide a specific entanglement-assisted parity-oblivious game in which Alice and Bob perform three measurements each and optimization of the success probability of that game. In Sec. IV we provide the self-testing protocol that certifies the entangled state and the trine set of observables. The self-testing of three-outcome POVMs and local randomness is provided in Sec. V. The generalization of the communication game for any arbitrary odd n is provided in Sec. VI. We summarize our results in Sec. VII.

II. PRELIMINARIES

Before presenting the main results, we briefly summarize the notion of preparation noncontextuality in an ontological model, the parity-oblivious communication game, the device-independent self-testing, and certifications randomness.

A. Operational theory and ontological model

We invoke an elegant framework of an ontological model [4,30] of quantum theory to introduce the notion of noncontextuality from a modern perspective. Given a preparation procedure P and a measurement procedure M, an operational theory assigns a probability $p(k|P, M)$ of obtaining a particular outcome k. In quantum theory, a preparation procedure P produces a density matrix ρ and a measurement procedure M (in general described by POVMs E_k) provides the probability of a particular outcome k being given by $p(k|P, M) = \text{Tr}[\rho E_k]$, the Born rule.

In an ontological model of quantum theory, it is assumed that whenever ρ is prepared by P, a probability distribution $\mu_P(\lambda|\rho)$ in the ontic space Λ is prepared, satisfying $\int_\Lambda \mu_P(\lambda|\rho)d\lambda = 1$, where $\lambda \in \Lambda$. The probability of obtaining an outcome k is given by a response function $\xi_M(k|\lambda, E_k)$ satisfying $\sum_k \xi_M(k|\lambda, E_k) = 1$, where a measurement operator E_k is realized through M. A viable ontological model should reproduce the Born rule, i.e., for all ρ, E_k, and k, $\int_\Lambda \mu_P(\lambda|\rho)\xi_M(k|\lambda, E_k)d\lambda = \text{Tr}[\rho E_k]$.

An ontological model of an operational theory can be assumed to be noncontextual in the following way [4]: If two experimental procedures are equivalent in operational theory, then they can be represented noncontextually in an ontological model. Then an ontological model of quantum theory is assumed to be preparation noncontextual for all M and k,

$$p(k|P, M) = p(k|P', M) \Rightarrow \mu_P(\lambda|\rho) = \mu_{P'}(\lambda|\rho), \quad (1)$$

where ρ is prepared by two distinct preparation procedures P and P' [4,31,32]. We will shortly see that in a preparation noncontextual ontological model the parity-oblivious constraint in a communication game in operational quantum theory implies an equivalent obliviousness condition at the level of ontic states.

B. Oblivious communication games

Consider a scenario where two distant parties, Alice and Bob, collaborate to perform a common task through a one-way communication [5–10,12–16]. Alice (Bob) receives an input $x \in \{1, \ldots, n_A\}$ ($y \in \{1, \ldots, n_B\}$) with probability distribution $p_A(x)$ [$p_B(y)$]. Bob's task is to guess a function of their interest $f(x, y)$ with the help of Alice's communication. For this, he encodes his answer in an output variable, say, $b \in \{0, 1\}$. Let $p(b|x, y)$ represent the probability of obtaining a binary output b given inputs x and y. The input may also contain the output of Alice. The guessing probability of the function $f(x, y)$ is a linear function of the observed probabilities $\{p(b|x, y)\}$. Thus, any linear figure of merit can be expressed as

$$\mathbb{P} = \sum_{x,y} \mathcal{C}^b_{x,y} p_A(x) p_B(y) p(b = f(x, y)|x, y), \quad (2)$$

where $\mathcal{C}^b_{x,y}$ is the payoff function of the game which quantifies the normalized weightage for guessing the correct $f(x, y)$. The quantum advantage of a communication game over clas-

sical resources becomes trivial if Alice is allowed to send her input x to Bob. However, if some constraints are imposed on the communication from Alice to Bob, then the supremacy of quantum resources may be exhibited. One such constraint can be bounding the dimension of the input. Another one, in which we are particularly interested here, is the parity-obliviousness condition [17–21,23–26,33,34]. Such a condition implies that there is no restriction on the number of communications, but that should not covey the information about a particular property of the inputs.

In an operational theory, Alice prepares the inputs x by the preparation procedures P_x and upon receiving the input y, Bob performs the measurement of M_y. Consider that there are L subsets having the same number of elements of the input $P_l \subset P_x$ with $l = 1, 2, 3, \ldots, L$. An oblivious condition demands that an input is not distinguishable whether it has come from $P_l \subset P_x$ or from $P_{l'} \subset P_x$ even when Alice's communication is not restricted. For our purpose it will be enough to consider the input of Alice as being uniformly distributed so that $p_A(x) = 1/|P_x|$, where $|P_x|$ is the cardinality of the set. Then, for an oblivious game for all l, l', y, and b we can write

$$\sum_{P_x \in P_l} p(P_x|b, M_y) = \sum_{P_x \in P_{l'}} p(P_x|b, M_y). \tag{3}$$

Using the Bayes rule, one can write $p(P_x|b, M_y) = p(b|P_x, M_y)p(x, y)/p(b|M_y)$. By noting that $p(x, y) = p_A(x)p_B(y)$, Eq. (3) can be written as

$$\sum_{P_x \in P_l} p(b|P_x, M_y) = \sum_{P_x \in P_{l'}} p(b|P_x, M_y) \tag{4}$$

for all l, l', y, and b. This means that the two input sets P_l and P_l' cannot be distinguished by any outcome b and any measurement M_y in an operational theory. This takes the form of the premise of the notion of preparation noncontextuality given in Eq. (1). Assuming preparation noncontextuality in an ontological model of the above operational theory, we can write

$$\sum_{P_x \in P_l} \mu(\lambda|P_x) = \sum_{P_x \in P_{l'}} \mu(\lambda|P_x), \tag{5}$$

where $\lambda \in \Lambda$ is the ontic state and Λ is the ontic state space. Using the Bayes rule once again, it can be shown that

$$\sum_{P_x \in P_l} \mu(P_x|\lambda) = \sum_{P_x \in P_{l'}} \mu(P_x|\lambda), \tag{6}$$

which implies that for preparation noncontextual models, the satisfaction of the obliviousness condition in an operational theory provides an equivalent representation at the level of the ontic states. In other words, the obliviousness condition must be satisfied at the level of ontic states λ too for the preparation noncontextual model. In this work, we consider a particular obliviousness condition, the parity-obliviousness one, in which no parity information of the inputs will be transmitted to Bob due to Alice's communication. Similarly, for preparation noncontextual ontological models, the ontic state λ cannot contain any information about the parity.

C. Device-independent self-testing

Self-testing in its traditional form is a device-independent protocol that aims to uniquely characterize the nature of the target quantum state and measurements solely from the correlations. Essentially, this requires finding a suitable Bell inequality whose maximum violation is achieved uniquely by the target state and measurements involved. Given the communication game discussed above, the observed joint probability in quantum theory can be obtained from the Born rule and is given by $p(ab|x, y) = \mathrm{Tr}[\rho_{AB}(A_{a|x} \otimes B_{b|y})]$, where $\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$ is an entangled state and $\{A_{a|x}\}$ and $\{B_{b|y}\}$ are the sets of local measurements that belong to Alice and Bob, respectively.

The aim of the self-testing is to find the suitable correlations which can uniquely be realized by the target state and measurements. The traditional self-testing scenario was first proposed by Mayers and Yao [35]. Later, McKague and Mosca [36] used this isometric embedding to develop a generalized Mayers-Yao test [37]. Since then, many works on this topic have been reported [38–47]. Related works, such as certification of binary outcomes, also have been reported [48]. Another interesting proposal for device-independent self-testing of Pauli observables was put forwarded in [44,45] using three Clauser-Horne-Shimony-Holt inequalities. For a recent review, see Ref. [49].

However, although device-independent scenario uses minimal assumptions, conclusive experimental certification are challenging. To circumvent this issue, semi-device-independent self-testing protocols have been proposed [50–58] where the entanglement is not required and the dimensions of the system are known. Such protocols are claimed to be more appealing for experimentalists compared to fully device-independent Bell tests. In this work, based on the optimal quantum success probability of a suitable communication game, we provide schemes to device-independently self-test the entangled state, a specific set of projective measurements, and the three-outcome extremal qubit POVMs.

D. Certification of randomness

Randomness is a powerful resource having a wide field of applicability ranging from scientific research to daily life. Classical algorithms, however powerful they may be, can only produce a pseudorandom number, whose unpredictability relies on the complexity of the generator [59]. In contrast, quantum theory provides intrinsic randomness through the unpredictability of the Born rule. Device-independent randomness generation relies on a fundamental relation between the nonlocality of quantum theory and its random character, which is usually expressed in terms of a trade-off between the probability of guessing correctly the outcomes of measurements performed on quantum systems and the amount of violation of a given Bell inequality [1,2,60].

Such a strategy of certifying device-independent randomness was first put forward by Colbeck [61]. Adopting a strategy similar to that in [62], the relation between randomness and violation of Bell's inequality is established through nonlocal guessing games. The joint probability $P(ab|x, y)$ can be obtained when Alice and Bob perform measurements according to the given inputs. In our case, we have inputs

$x, y \in 1, 2, \ldots, n$ and outputs $a, b \in \{0, 1\}$. Then there will be a number $2n^2$ of joint probabilities that can be viewed as a component of a vector $\mathbf{P} = \{p(a, b|x, y)\}$, which is referred to as behavior which characterizes the systems of Alice and Bob [63]. In our communication game, it is assumed that $\mathbf{P}$ is given, which means it is a promise on the behavior. In the nonlocal guessing game there is another party, Eve, whose goal is to guess Alice's outcome for a certain input (say, x^*) with the highest possible probability. A strategy of Eve can be that she prepares the quantum state $|\Psi_{ABE}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ for Alice and Bob so that $|\Psi_{AB}\rangle$ can be obtained by tracing out her system. Given inputs x and y, Alice and Bob measure sets of POVMs $\{A_{a|x}\}$ and $\{B_{b|y}\}$, respectively. Thus, $P(ab|x, y) = \mathrm{Tr}[(A_{a|x} \otimes B_{b|y} \otimes \mathbb{I})\rho_{ABE}]$. Given a special input x^*, the local guessing probability can be written as

$$G = \max_F P(a, a|A_{x^*}, F) = \max_F \mathrm{Tr}[(A_{a|x^*} \otimes \mathbb{I} \otimes F_a)\rho_{ABE}], \tag{7}$$

where $F = \{F_a\}$ is the POVM of Eve whose measurement result provides her the best guess of Alice's outcome. The min-entropy can be used as a measure of randomness so that an amount of randomness $H_{\min}(a|x) = -\log_2 G$ is generated by Alice.

Quite a number of works in this direction have been reported [58,64–70] and verified experimentally [71–73]. Note that the device-independent randomness certification faces practical challenges that arise with the loophole-free violation of Bell's inequality by lowering the bit rate. In recent times, loophole-free Bell tests have been realized [74–76] which in turn enable experimental demonstrations of device-independent random number certification [71,72]. However, such implementation still remains a difficult task to perform commonly. To tackle this practical issue, the device-independent self-testing of a random number generator in a prepare-and-measure scenario was proposed in [77]. Semi-device-independent randomness certification protocols [78–81] in a prepare-and-measure scenario have also been proposed where the dimension of the quantum system is known. Here we demonstrate the device-independent certification of randomness using the optimal success probability of our communication game.

III. PARITY-OBLIVIOUS COMMUNICATION GAME AND RELEVANT BELL INEQUALITY

Equipped with preliminary ideas about the ontological model and oblivious communication game, we are now in a position to introduce a specific parity-oblivious communication game. We first provide a parity-oblivious communication game where Alice and Bob have inputs $x, y \in \{1, 2, 3\}$ and outputs $a, b \in \{0, 1\}$. These correspond to the measurements of dichotomic observables of A_x and B_y by Alice and Bob, respectively. Using her output, Alice prepares six input states $x^i \in (x, a) \equiv \{10, 11, 20, 21, 30, 31\}$, where $i = 1, 2, \ldots, 6$. For our purpose we consider a uniform distribution of inputs of Alice and also for Bob, so $p_A(x) = p_B(y) = \frac{1}{3}$. The winning rule of the game is that Bob's output must be $b = \delta_{x,y} \oplus_2 a$. In an operational theory the success probability of this communication game is

$$\mathbb{P}_3 = \frac{1}{9} \sum_{x,y=1}^{3} p(b = \delta_{x,y} \oplus_2 a)|x, y). \tag{8}$$

When there is no restriction on the inputs, the success probability can be cast as

$$\mathbb{P}_3 = \frac{1}{2}\left(1 + \frac{\langle \mathcal{B}_3 \rangle}{9}\right), \tag{9}$$

where

$$\mathcal{B}_3 = A_1 \otimes (-B_1 + B_2 + B_3) + A_2 \otimes (B_1 - B_2 + B_3) + A_3 \otimes (B_1 + B_2 - B_3). \tag{10}$$

The correlation $\langle A_x B_x \rangle = \sum_{a,b} (-1)^{a \oplus_2 b} P(ab|x, y)$. The local bound of the Bell expression is $(\mathcal{B})_{\text{local}} \leqslant 5$.

We now impose the parity-oblivious restriction on communication. Consider an input set divided into two subsets having equal numbers of elements; the even parity set $P_l = \{x^i : x \oplus_2 a = 0\}$ and the odd parity set $P_{l'} = \{x^i : x \oplus_2 a = 1\}$. The parity-obliviousness condition demands that

$$\sum_{x^i \in P_l} p(b|x^i, y) = \sum_{x^i \in P_{l'}} p(b|x^i, y). \tag{11}$$

As already mentioned, the parity obliviousness in an operational theory implies a similar consequence at the level of ontic states if the ontological model is preparation noncontextual.

In quantum theory, Alice encodes her input string of x^i into pure quantum states ρ_{x^i} prepared by a procedure P_{x^i}. Bob performs a two-outcome measurement B_y for every $y \in \{1, 2, 3\}$ and reports outcome b as his output. If Alice and Bob share an entangled state $|\psi_{AB}\rangle$ then Alice can steer the states x^i to Bob by measuring three dichotomic observables A_x on her particle corresponding to the input $x \in \{1, 2, 3\}$. For example, $\rho_{11} = \mathrm{Tr}_A[(\Pi^+_{A_1} \otimes \mathbb{I})\rho_{AB}(\Pi^+_{A_1} \otimes \mathbb{I})]/\mathrm{Tr}[\rho_{AB}(\Pi^+_{A_1} \otimes \mathbb{I})]$, where $\Pi^+_{A_1} = (\mathbb{I} + A_1)/2$ is the projector of Alice's observable A_1. Also, $\rho_{21} = \mathrm{Tr}_A[(\Pi^-_{A_2} \otimes \mathbb{I})\rho_{AB}(\Pi^-_{A_2} \otimes \mathbb{I})]/\mathrm{Tr}[\rho_{AB}(\Pi^-_{A_2} \otimes \mathbb{I})]$ and $\rho_{31} = \mathrm{Tr}_A[(\Pi^+_{A_3} \otimes \mathbb{I})\rho_{AB}(\Pi^+_{A_3} \otimes \mathbb{I})]/\mathrm{Tr}[\rho_{AB}(\Pi^+_{A_3} \otimes \mathbb{I})]$. Note that $\rho_{x1} + \rho_{x0} = \mathbb{I}$ with $x = 1, 2, 3$. The parity-oblivious condition in quantum theory reads

$$\sum_{x^i|x \oplus_2 a=0} \rho_{x^i} = \sum_{x^i|x \oplus_2 a=1} \rho_{x^i}. \tag{12}$$

This explicitly means that $\rho_{11} + \rho_{20} + \rho_{31} = \rho_{10} + \rho_{21} + \rho_{30}$. It is straightforward to see that the parity-oblivious condition given by Eq. (12) provides a nontrivial functional relation $\sum_{x=1}^{3} A_x = 0$ between the observables that has to be satisfied in quantum theory.

Equivalently, in an ontological model of quantum theory, the preparation noncontextuality assumption provides

$$\sum_{x^i|x \oplus_2 a=0} \mu(\lambda|P_{x^i}) = \sum_{x^i|x \oplus_2 a=1} \mu(\lambda|P_{x^i}). \tag{13}$$

In a preparation noncontextual ontological model the equivalent condition of $\sum_{x=1}^{3} A_x = 0$ needs to be used to derive

the upper bound of the Bell expression $\mathcal{B}_3$. Imposing this nontrivial condition in an ontological model, the local bound of $\mathcal{B}_3$ gets reduced to the nontrivial preparation noncontextual bound $(\mathcal{B}_3)_{pnc} \leqslant 4$. Importantly, the choice of Alice's observable optimizes the quantum value of $(\mathcal{B}_3)_Q = 6$, which satisfies the parity-oblivious condition in quantum theory.

In order to derive an optimal quantum value of the Bell expression $\mathcal{B}_3$, we use a sum-of-square (SOS) approach [82] so that $(\mathcal{B}_3)_Q \leqslant \beta_3$ for all possible quantum states and measurement operators A_x and B_y, where β_3 is the upper bound on the quantum value of $(\mathcal{B}_3)_Q$. This is equivalent to showing that there is a positive-semidefinite operator $\gamma_3 \geqslant 0$ that can be expressed as $\langle\gamma_3\rangle_Q = \beta_3 - (\mathcal{B}_3)_Q$. This can be proved by considering a set of suitable positive operators L_y, which consists of polynomial functions of A_x and B_y, so that

$$\gamma_3 = \frac{1}{2}\sum_{y=1}^{3} \omega_y L_y^\dagger L_y, \tag{14}$$

where the L_y are positive operators. For the Bell expression given by Eq. (10), we choose the operators L_y as

$$L_y|\psi\rangle = \frac{1}{\omega_y}\left(\sum_{x=1}^{3} \alpha_3^{x,y} A_x\right)|\psi\rangle - B_y|\psi\rangle, \tag{15}$$

where $\alpha_3^{x,y} = 1$ (-1) when $x \neq y$ $(x = y)$. Also,

$$\omega_y = \left\|\sum_{x=1}^{3} \alpha_3^{x,y} A_x|\psi\rangle\right\|, \tag{16}$$

where $\|\cdot\|$ is the Euclidean norm of a vector. Plugging Eq. (15) into Eq. (14) and by noting that $A_x^\dagger A_x = B_y^\dagger B_y = \mathbb{I}$ we get

$$\langle\gamma_3\rangle_Q = -(\mathcal{B}_3)_Q + \sum_{y=1}^{3} \omega_y, \tag{17}$$

which can be rewritten as

$$(\mathcal{B}_3)_Q = \sum_{y=1}^{3} \omega_y - \langle\gamma_3\rangle_Q. \tag{18}$$

In order to maximize $(\mathcal{B}_3)_Q$, we write

$$\max[(\mathcal{B}_3)_Q] \leqslant \max\left(\sum_{y=1}^{3} \omega_y\right) + \max(-\langle\gamma_3\rangle_Q). \tag{19}$$

We separately derive $\max(\sum_{y=1}^{3} \omega_y)$ and $\max(-\langle\gamma_3\rangle_Q)\forall\psi, A_x, B_y$. To maximize $\sum_{y=1}^{3} \omega_y$, we use the concavity inequality [83] $\sum_{y=1}^{3} \omega_y \leqslant \sqrt{3\sum_{y=1}^{3}(\omega_y)^2}$. From the definition of ω_y in Eq. (16) we can write $(\omega_1)^2 = \langle\psi|(-A_1 + A_2 + A_3)^2|\psi\rangle = 3 + \langle\psi|(-\{A_1, A_2\} + \{A_2, A_3\} - \{A_1, A_3\})|\psi\rangle$. The quantities $(\omega_2)^2$ and $(\omega_3)^2$ can also be written in a similar manner. Using them, we have

$$\sum_{y=1}^{3} \omega_y \leqslant \sqrt{3(9 - \langle\Delta_3\rangle)}, \tag{20}$$

where the quantity Δ_3 is explicitly written as

$$\Delta_3 = \{A_1, A_2\} + \{A_2, A_3\} + \{A_1, A_3\}. \tag{21}$$

Here $\{\}$ denotes anticommutation. This means that minimizing $\langle\Delta_3\rangle$ provides $\max(\sum_{y=1}^{3} \omega_y)$.

For dichotomic observables satisfying $A_x^2 = \mathbb{I}$, by considering $|\psi'\rangle = (A_1 + A_2 + A_3)|\psi\rangle$ (where $|\psi\rangle$ is a nonzero vector), we can write

$$\langle\Delta_3\rangle = -3 + \langle\psi'|\psi'\rangle. \tag{22}$$

Note that the inner product $\langle\psi'|\psi'\rangle$ is in general non-negative. It becomes zero only when $|\psi'\rangle$ is a zero vector. The minimum value of $\langle\Delta_3\rangle$ is obtained when the inner product is zero; however, since $|\psi\rangle$ is nonzero then $A_1 + A_2 + A_3 = 0$ needs to be satisfied. We obtain $\max(\sum_{y=1}^{3} \omega_y) = 6$. This also ensures that each of the ω_y is equal to 2, thereby implying $\langle\{A_x, A_x'\}\rangle = -1$ for $x \neq x'$.

We now consider $\max(-\langle\gamma_3\rangle_Q)\forall\psi, A_x, B_y$. Since γ_3 is a positive operator, $\max(-\langle\gamma_3\rangle_Q) = 0$ for any $|\psi\rangle$. This means that $\langle\psi L_y^\dagger L_y|\psi\rangle = 0$, and consequently $L_y|\psi\rangle = 0$, i.e.,

$$\sum_{x=1}^{3} \alpha_3^{x,y} A_x|\psi\rangle = \omega_y B_y|\psi\rangle. \tag{23}$$

Altogether, from Eq. (19) we thus have the optimal value $(\mathcal{B}_3)_Q^{\text{opt}} = 6$. It can be found from Eq. (23) that Bob's observables satisfy the relation $B_y = -A_x$ when $x = y$. This in turn provides the success probability $(\mathbb{P}_3)_Q^{\text{opt}} = \frac{5}{6}$ compared to the nontrivial preparation noncontextual bound $(\mathbb{P}_3)_{pnc} = \frac{13}{18}$.

One of Alice's choices of observables can even be found for a qubit system is given by

$$A_1 = \sigma_z, \quad A_2 = \frac{\sqrt{3}}{2}\sigma_x - \frac{1}{2}\sigma_z, \quad A_3 = -\frac{\sqrt{3}}{2}\sigma_x - \frac{1}{2}\sigma_z,$$

which are the trine-spin axes satisfying $\vec{a}_x\vec{a}_{x'} = -\frac{1}{2}$, for $x \neq x'$, where $\vec{a}_x$ is the Bloch vector. As already mentioned, from Eq. (23) one finds $B_y = -A_x$ if $x = y$. This provides $\langle A_x \otimes B_y\rangle = -1$ $(\frac{1}{2})$ when $x = y$ $(x \neq y)$ and the state required for obtaining the optimal value is

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{24}$$

The optimal quantum value of the Bell expression $\mathcal{B}_3$ enables us to self-test the entangled state and projective measurements of the trine set of observables from the observed statistics. In the following, we provide the device-independent self-testing protocols based on $\mathcal{B}_3^{\text{opt}}$.

IV. SELF-TESTING OF STATE AND TRINE SET OF OBSERVABLES

As mentioned earlier, for self-testing of the state and measurements, one requires correlations $p(ab|x, y)$ which can be reproduced uniquely by the state and measurements (up to a certain equivalence class). Hence the target state and measurements can be certified from the correlation alone. In other words, the self-testing technique implies the existence of local unitaries along with axillary systems so that the target state and measurements can be inferred from the physical state and

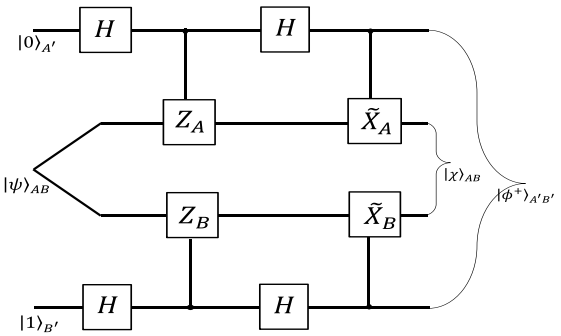

FIG. 1. Circuit based on Bell's inequality in Eq. (10) for self-testing a two-qubit maximally entangled state and trine set of measurements. The operations Z_A, Z_B, $\tilde{X}_B$, and $\tilde{X}_B$ are defined in the text and H is the Hadamard gate. A detailed derivation is in Appendix A.

measurements. In our scenario when Alice and Bob perform three measurements each, we can find that the measurements can be expressed using only real numbers. However, we will see when Alice and Bob perform more than three measurements each, the observables required to achieve a optimum quantum value of the Bell expressions cannot be expressed using the real numbers only. In such a case the correlations are invariant under complex conjugation or transposition [36,45,49]. Since a transpose is not a valid unitary map, the self-testing protocol needs to be suitably modified in this case [36,45,49], which is provided in Sec. VI.

Let us first provide the self-testing protocol based on the optimal value $(\mathcal{B}_3)_Q^{\text{opt}}$. The measurement can be considered projective as according to the Naimark dilation theorem any nonprojective measurement can be considered a projective measurement over a dilated Hilbert space. For our purpose, we invoke the SWAP circuit scheme [35–37] to demonstrate that the optimal quantum value $(\mathcal{B}_3)_Q^{\text{opt}}$ implies the existence of an isometry Φ so that $\Phi : \mathcal{H}_A \otimes \mathcal{H}_B \to (\mathcal{H}_A \otimes \mathcal{H}_{A'}) \otimes (\mathcal{H}_B \otimes \mathcal{H}_{B'})$ and $|\psi\rangle_{AB} \to |\chi\rangle_{AB} \otimes |\phi^+\rangle_{A'B'}$. Here primed and nonprimed symbols denote the reference and physical systems, respectively.

In order to find the self-testing properties, let us define the observables $Z_A = A_1, X_A = A_3 - A_2, Z_B = -B_1$, and $X_B = B_2 - B_3$. Further we define $\tilde{X}_A = X_A/\|X_A\| = (A_3 - A_2)/\sqrt{3}$ and $\tilde{X}_B = X_B/\|X_B\| = (B_2 - B_3)/\sqrt{3}$. We derive the properties

$$Z_A|\psi\rangle_{AB} = Z_B|\psi\rangle_{AB}, \quad \tilde{X}_A|\psi\rangle_{AB} = \tilde{X}_B|\psi\rangle_{AB}, \tag{25}$$

$$\{Z_A, \tilde{X}_A\}|\psi\rangle_{AB} = \{Z_B, \tilde{X}_B\}|\psi\rangle_{AB} = 0. \tag{26}$$

Details of the derivation of Eqs. (25) and (26) can be found in Appendix A.

If $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is the state and $A_x \in \mathcal{H}_A$ and $B_y \in \mathcal{H}_B$ (where $x, y = 1, 2, 3$) are the observables providing the optimal value of $\mathcal{B}_3$, then from the circuit given in Fig. 1 it can be proved that there exist a local unitary operation Φ and ancilla state $|00\rangle_{A'B'}$ such that

$$\Phi(|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = |\chi\rangle_{AB} \otimes |\phi^+\rangle_{A'B'}, \tag{27}$$

where $|\chi\rangle_{AB} = \frac{1+Z_A}{\sqrt{2}}|\psi\rangle_{AB}$ is the so-called junk state. This is obtained by using the self-testing properties given by Eqs. (25) and (26). Corresponding to the measurements using the SWAP circuit, one gets

$$\Phi(B_y|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = |\chi\rangle \otimes (\mathbb{I} \otimes B'_y)|\phi^+\rangle_{A'B'}, \tag{28}$$

$$\Phi(A_x|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = |\chi\rangle \otimes (A'_x \otimes \mathbb{I})|\phi^+\rangle_{A'B'}, \tag{29}$$

$$\Phi(A_xB_y|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = |\chi\rangle \otimes (A'_x \otimes B'_y)|\phi^+\rangle_{A'B'}. \tag{30}$$

Details of the calculation are given in Appendix A. This thus demonstrates that the self-testing protocol based on the Bell expression $\mathcal{B}_3$ given in Eq. (10) provides the equivalence between the reference and physical experiments. This in turn device-independently certifies the maximally entangled state and trine set of observables.

V. CERTIFYING THREE-OUTCOME POVMS AND RANDOMNESS

In this section we first argue how a simple modification of the earlier game and an optimal quantum value in that case certify a three-outcome extremal qubit POVM and more than one bit of local randomness. For this we keep the original game as it is but introduce an additional input $x = 4$ to Alice. This can be used to certify the three-outcome POVMs. Let us first explain the scenario. Alice receives an additional input $x = 4$ according to which she performs the measurement of a three-outcome extremal POVMs, say, $A_4 = \{A_{k|4}\}$, where $k = 1, 2, 3$. This means that each of the $A_{k|4}$ is a projector satisfying $\sum_k A_{k|4} = \mathbb{I}$. Let Alice's measurement on her system produce the outcomes with the same probability and having no pattern. The question is whether such an unpredictability of the outcomes is genuine or someone (say, an adversary Eve) may be able to guess Alice's outcomes. To examine the presence of Eve, the unpredictability of Alice's outcomes has to be certified in a device-independent way. Alice then performs certain tests for the device-independent certification of Eve's guessing probabilities of her outcomes. This in turn requires the certification of three-outcome POVMs and in that case the upper bound of Eve's guessing probability needs to be $\frac{1}{3}$. The first test is the maximization of the Bell expression $\mathbb{B}_3$, which has already been shown, and the second test is the minimization of the probability of other events.

We first show that a modified Bell expression of $\mathcal{B}_3$ can be used to self-test three-outcome POVMs without invoking the role of Eve. However, while demonstrating the certification of randomness, we explicitly consider Eve's role. Following Acín *et al.* [68], let us define a modified Bell expression $\mathcal{B}'_3$ as

$$\mathcal{B}'_3 = \mathcal{B}_3 - \alpha \sum_{k=1}^{3} P(k, +|x = 4, y = k), \tag{31}$$

where α is strictly positive. As the last term on the right-hand side is always negative, both $\mathcal{B}'_3$ and $\mathcal{B}_3$ have the same classical upper bound. Equivalently, $(\mathcal{B}'_3)_Q$ cannot be larger than $(\mathcal{B}_3)_Q^{\text{opt}} = 6$ and there is only way to obtain equality when the probability $P(k, +|x = 4, y = k) = \text{Tr}[(A_{k|4} \otimes \Pi^+_{B_k})\rho_{AB}]$ equals zero for every k. Here $\Pi^+_{B_k}$ is the projector correspond-

ing to Bob's observables. This is possible when the POVM elements $\{A_{k|4}\}$ are antialigned with three $\Pi^{+}_{B_k}$ of Bob. Since $\Pi^{+}_{B_k}$ are certified by the optimal value of $(\mathcal{B}_3)^{\text{opt}}_{Q} = 6$ and they are positive projectors of the trine set of observables, we can then have $A_{k|4} = \frac{2}{3}\Pi^{-}_{A_k} = \frac{1}{3}(\mathbb{I} - A_k)$, with $k = 1, 2, 3$. Thus the modified Bell expression $(\mathcal{B}'_3)^{\text{opt}}_{Q} = 6$ certifies the three-outcome POVMs. If Alice performs the POVM $A_4 = \{A_{k|4}\}$ on her subsystem, then the probability of each outcome provides the same probability $\frac{1}{3}$ and generates the $\log_2 3$ bit of local randomness.

However, in general, in randomness certification protocols Eve's role is crucial. Her strategy may be to use a POVM $F = \{F_k\}$ so that she can model her measurement in a way that whenever Alice obtains the outcome k Eve perfectly guesses that outcome. Then Eve's probability of perfectly guessing Alice's outcome is given by [68]

$$G = \max_{F} \sum_{k} P(k, k|A_{k|3}, F). \tag{32}$$

If Eve's guessing probability is found to be $G = \frac{1}{3}$, then the unpredictability of Alice's outcomes is certified. In order to certify this in a device-independent way, in general one can write a family of qubit POVMs operators $A_4 = \{A_{k|4}\}$ as

$$A_{k|4} = \gamma^0_k \mathbb{I} + \gamma^1_k \sigma_z + \gamma^2_k \sigma_y + \gamma^4_k \sigma_x, \tag{33}$$

where σ_x, σ_z, and σ_y are the Pauli operators. It can be readily checked that to satisfy $A_{k|4} = \frac{2}{3}\Pi^{-}_{A_k}$ the coefficients γ^j_k with $j = 0, 1, 2, 3$ take the form

$$\gamma^0_k = P(k|A_{k|4}), \quad \gamma^1_k = E_{k|3,1}, \quad \gamma^2_k = \sum_{j=1}^{3} E_{b|3,j}, \tag{34}$$

$$\gamma^3_k = \frac{1}{\sqrt{3}}(E_{k|3,2} - E_{k|3,3}), \tag{35}$$

where $E_{k|x,y} = \sum_k kP(k, b|x, y)$.

Let us now consider the action of Eve here. In a nonlocal guessing game, Eve tries to guess Alice's output with the highest possible accuracy, as summarized in Sec. II. Thus the inclusion of Eve's system modifies the isometry as $\Phi : \mathcal{H}_A \otimes H_B \otimes H_E \to (\mathcal{H}_A \otimes \mathcal{H}_{A'}) \otimes (H_B \otimes \mathcal{H}_{B'}) \otimes H_E$ so that $\Phi(|\psi_{ABE}\rangle \otimes |00\rangle_{A'B'}) = |\chi\rangle_{ABE} \otimes |\psi^+\rangle_{A'B'}$. Now, on the support of $\mathcal{H}_A \otimes \mathcal{H}_{A'}$, each element $\{A_{k|4}\}$ of A_4 can be represented by an operator $\tilde{A}_{k|4} \in \mathcal{H}_A \otimes \mathcal{H}_{A'}$ so that

$$\tilde{A}_{k|4} = \sum_{j=0}^{3} \tilde{A}^j_{k|4} \otimes \sigma_j, \tag{36}$$

where $\sigma_0 = \mathbb{I}$ and $j = 1, 2, 3$ correspond to Pauli operators. From the self-testing relations given by Eq. (28) we have

$$\begin{aligned}
\gamma^0_k &= \langle\psi|\tilde{A}_{k|4} \otimes \mathbb{I}|\psi\rangle = \langle\chi|\tilde{A}^0_{k|4}|\chi\rangle,\\
\gamma^1_k &= \langle\psi|\tilde{A}_{k|4} \otimes B_1|\psi\rangle = \langle\chi|\tilde{A}^1_{k|4}|\chi\rangle,\\
\gamma^2_k &= \langle\psi|\tilde{A}_{k|4} \otimes (B_1 + B_2 + B_3)|\psi\rangle = \langle\chi|\tilde{A}^2_{k|4}|\chi\rangle,\\
\gamma^3_k &= \tfrac{1}{3}\langle\psi|\tilde{A}_{k|4} \otimes \otimes B_2 - B_3|\psi\rangle = \langle\chi|\tilde{A}^3_{k|4}|\chi\rangle.
\end{aligned} \tag{37}$$

Here $|\psi\rangle \equiv |\chi\rangle_{ABE} \otimes |\psi^+\rangle_{A'B'}$. This thus self-tests the three-outcome extremal qubit POVMs $A_{k|4} = \frac{2}{3}\Pi^{-}_{A_k}$ with $k = 1, 2, 3$.

We now proceed to generate the certified randomness of more than one bit, building upon the work of Acín *et al.* [68]. This is to show that for a quantum state $|\psi\rangle_{ABE}$ shared by Alice, Bob, and Eve and for A_x and B_y $(x, y = 1, 2, 3)$ local to Alice and Bob, respectively, a POVM $\{F_k\}$ is local to Eve. If the optimal violation of $\mathcal{B}_3$ is obtained, this then certifies the local guessing probability $G = \frac{1}{3}$. In order to show this, by assuming a normalized state $|\phi^k_{A'}\rangle = F_k|\chi\rangle/\sqrt{q_k}$ and without loss of generality, by taking Eve's measurement F_k as projective, we can write

$$\gamma^j_k = \sum_{k'} \langle\chi|F_{k'}\tilde{A}^j_{k|4}F_{k'}|\chi\rangle \tag{38}$$

$$= \sum_{k'} q_{k'}\langle\phi^{k'}_{A'}|\tilde{A}^j_{k|4}|\phi^{k'}_{A'}\rangle = \sum_{k'} q_{k'}\beta^{j,k'}_k, \tag{39}$$

where $k = 1, 2, 3$. This can be interpreted as a convex combination of original POVMs $\{A_{k|4}\}$ in terms of the POVMs $\{\tilde{A}_{k|4}\}$ with respective weight q_k so that $A_{k|4} = \sum_{k'}\sum_j q_{k'}\beta^{j,k'}_k\sigma_j$; however, since $A_{k|4}$ is extremal, we have $\beta^{j,k'}_k = \gamma^j_k$ for all k'. This then implies that $\beta^{0,k}_k = \gamma^0_k = \frac{1}{3}$ for all k. We then have the local guessing probability

$$\begin{aligned}
G &= \sum_k P(k, k|A_{k|4}, F_k) = \sum_k \langle\psi|\tilde{A}_{k|4}F_k|\psi\rangle\\
&= \sum_k \langle\chi|\tilde{A}^0_{k|4}F_k|\chi\rangle = \sum_k q_k\beta^{0,k}_k = \frac{1}{3}.
\end{aligned} \tag{40}$$

This then certifies $H_\infty = \log_2 3$ bits of randomness from one entanglement bit. It was proved by D'Ariano *et al.* [84] that there exist d^2 extremal POVMs for d-dimensional space. Using this fact, Acín *et al.* [68] argued that at most $2\log_2 d$ $(4\log_2 d)$ bits of local (global) randomness can be certified from an entangled state of dimension $\mathcal{C}^d \otimes \mathcal{C}^d$. For the case of a qubit system, Acín *et al.* [68] demonstrated an interesting protocol to certify two bits of local randomness based on a simultaneous maximal quantum violation of three Clauser-Horne-Shimony-Holt inequalities. They [68] had conjectured that the maximum quantum violation of Gisin's elegant Bell inequality [85] can also be used to certify two bits of randomness in a device-independent way, which was proved by Andersson *et al.* [70] by providing the self-testing properties of elegant Bell inequality [41]. Here we use fewer observables for Alice and Bob and device-independently certify $\log_2 3$ bits of local randomness.

VI. GENERALIZATION OF THE GAME FOR ANY ARBITRARY ODD *n*

We now generalize the parity-oblivious communication game where Alice and Bob have inputs $x, y \in \{1, 2, \ldots, n\}$ and outputs $a, b \in \{0, 1\}$. Alice prepares $2n$ input states $x^i \in (x, a) \equiv \{1, 2, \ldots, n\} \times \{0, 1\}$ and sends to Bob. We consider a uniform distribution of inputs of Alice and also for Bob, so that $p_A(x) = p_B(y) = 1/n$. The condition of winning the game remains the same as before, i.e., $b = \delta_{x,y} \oplus_2 a$. In such a case the success probability is given by

$$\mathbb{P}_n = \frac{1}{2} + \frac{\langle\mathcal{B}_n\rangle}{2n^2}, \tag{41}$$

where $\mathcal{B}_n$ is the Bell expression given by

$$\mathcal{B}_n = \sum_{x,y=1x\neq y}^{n} A_{n,x} \otimes B_{n,y} - \sum_{x,y=1;x=y}^{n} A_{n,x} \otimes B_{n,y}. \quad (42)$$

In order to find the quantum upper bound of the Bell expression $\mathcal{B}_n$, we again use the SOS approach. This is equivalent to showing that there is a positive-semidefinite operator $\gamma_n \geqslant 0$, where

$$\gamma_n = \frac{1}{2}\sum_{y=1}^{3} \omega_{n,y} L_{n,y}^{\dagger} L_{n,y}, \quad (43)$$

where the $L_{n,y}$ are positive operators and polynomial functions of $A_{n,x}$ and $B_{n,y}$. For the Bell expression given by Eq. (42), the operators $L_{n,y}$ can be written as

$$L_{n,y}|\psi\rangle = \frac{1}{\omega_{n,y}} \sum_{x=1}^{n} \alpha_n^{x,y} A_{n,x}|\psi\rangle - B_{n,y}|\psi\rangle, \quad (44)$$

where $\alpha_n^{x,y} = 1$ (-1) when $x \neq y$ $(x = y)$ and $\omega_{n,y} = \| \sum_{x=1}^{n} \alpha_n^{x,y} A_{n,x}|\psi\rangle \|$. Plugging Eq. (44) into Eq. (43) and noting that $A_{n,x}^{\dagger} A_{n,x} = B_{n,y}^{\dagger} B_{n,y} = \mathbb{I}$, we get $\langle\gamma_n\rangle_Q = -(\mathcal{B}_n)_Q + \sum_{y=1}^{n} \omega_{n,y}$. To obtain a maximum value of $(\mathcal{B}_n)_Q$ we can write

$$\max[(\mathcal{B}_n)_Q] \leqslant \max\left(\sum_{y=1}^{n} \omega_{n,y}\right) + \max(-\langle\gamma_n\rangle_Q). \quad (45)$$

To maximize $\sum_{y=1}^{n} \omega_{n,y}$ we again use the concavity inequality $\sum_{y=1}^{n} \omega_{n,y} \leqslant \sqrt{n \sum_{y=1}^{n} \omega_{n,y}^2}$, where

$$\sum_{y=1}^{n} \omega_{n,y}^2 = n^2 + \sum_{y=1}^{n} \Bigg\langle \Bigg[\left\{ \alpha_n^{1,y} A_{n,1}, \sum_{x=2}^{n} \alpha_n^{x,y} A_{n,x} \right\} + \left\{ \alpha_n^{2,y} A_{n,2}, \sum_{x\neq 2;x=1}^{n} \alpha_n^{x,y} A_{n,x} \right\} + \cdots + \left\{ \alpha_n^{n,y} A_{n,n}, \sum_{x=1}^{n-1} \alpha_n^{x,y} A_{n,x} \right\} \Bigg] \Bigg\rangle, \quad (46)$$

which can be written in a simplified form as

$$\sum_{y=1}^{n} \omega_{n,y}^2 = n^2 + (n-4)\langle\Delta_n\rangle, \quad (47)$$

where

$$\Delta_n = \left\{ A_{n,1}, \sum_{x=2}^{n} A_{n,x} \right\} + \left\{ A_{n,2}, \sum_{x=3}^{n} A_{n,x} \right\} + \cdots + \{A_{n,n-2}, (A_{n,n-1} + A_{n,n})\} + \{A_{n,n-1}, A_{n,n}\}. \quad (48)$$

By considering $(\sum_{x=1}^{n} A_{n,x})^2 = n\mathbb{I} + \Delta_n$ for dichotomic observables that satisfy the parity-oblivious condition, the optimal quantum value of $\langle\Delta_n\rangle = -n$. This in turn provides $\max(\sum_{y=1}^{n} \omega_{n,y}) = 2n$.

Since γ_n is a positive operator, $\max(-\langle\gamma_n\rangle_Q) = 0$ for every $|\psi\rangle$, provided for all y, $L_{n,y}|\psi\rangle = 0$, i.e.,

$$\sum_{x=1}^{n} \alpha_n^{x,y} A_{n,x}|\psi\rangle = \omega_{n,y} B_{n,y}|\psi\rangle \quad (49)$$

Altogether, from Eq. (45) we have

$$(\mathcal{B})_Q^{\text{opt}} = 2n. \quad (50)$$

One of the choices of the observables can be found for the qubit system,

$$A_{n,1} = \sigma_z, \quad \{A_{n,i}\}_{i=2,\ldots,(n+1)/2} = \nu_{n,i}\sigma_x - \beta_{n,i}\sigma_y - \frac{\sigma_z}{(n-1)}, \quad \{A_{n,j}\}_{j=(n+3)/2,\ldots,n} = -\nu_{n,j}\sigma_x + \beta_{n,j}\sigma_y - \frac{\sigma_z}{(n-1)}, \quad (51)$$

with $\nu_{n,i}^2 + \beta_{n,i}^2 + \frac{1}{(n-1)^2} = 1$. Also, $\nu_{n,i} = \nu_{n,j}$ and $\beta_{n,i} = \beta_{n,j}$ when $i = (n+1)/2$ and $j = (n+3)/2$. In quantum theory, such choices of observables satisfy

$$A_{n,1} + \sum_{i=2}^{(n-1)/2} A_{n,i} + \sum_{j=(n+1)/2}^{n} A_{n,j} = 0 \quad (52)$$

and consequently the corresponding projectors satisfy the relation

$$\frac{2}{n}\left(P_{A,1}^{+(-)} + \sum_{i=2}^{(n-1)/2} P_{A_{n,i}}^{+(-)} + \sum_{j=(n+1)/2}^{n} P_{A_{n,j}}^{+(-)} \right) = \mathbb{I}. \quad (53)$$

This in turn satisfies the parity-oblivious condition of the game. The required state is a maximally entangled state given by Eq. (24). Using Eq. (49), we can obtain Bob's choice of observables for optimal violation. It can be seen that Bob's observables satisfy the same condition of Alice as given by Eq. (52).

Using the parity-oblivious condition given by Eq. (53), the preparation noncontextuality bound of $\mathcal{B}_n$ can be derived, which is $(\mathcal{B}_n)_{pnc} \leqslant 2n-2$, which is violated by quantum theory. The proof is similar to the case for $n = 3$, which can be seen as follows. Substituting the condition given in Eq. (52) into the generalized Bell expression in Eq. (42), we have $\mathcal{B}_n = 2\sum_{x=y=1}^{n} A_x B_y$. Using Eq. (52) again, it is straightforward to derive the aforementioned upper bound of $(\mathcal{B}_n)_{pnc}$ in a preparation noncontextual model. However, there is flexibility to choose a different form of the observables satisfying the same condition of Eq. (53). In Appendix B we provide a self-testing protocol for certifying the maximally entangled state and observables based on the optimal quantum value of the generalized Bell expression in Eq. (42).

Now one may be wondering whether it is possible to certify n-outcome POVMs and $\log_2 n$ bits of randomness for an arbitrary (odd) n scenario similar to that for $n = 3$. We discuss that this is not the case. Following the $n = 3$ case, let us consider the action of the $(n+1)$th measurement $A_{n,n+1}$ of Alice which is an n-outcome qubit POVM $\{A_{k|n+1}\}$. As already used earlier, a shifted Bell expression of Eq. (42) can be written as

$$\mathcal{B}_n' = \mathcal{B}_n - \alpha' \sum_{k=1}^{n} P(k, +|x = n+1, y = k), \quad (54)$$

where α' is a strictly positive quantity. As the last term on the right-hand side is always non-negative, the preparation noncontextual bounds of both $\mathcal{B}_n'$ and $\mathcal{B}_n$ remain $2n-2$. Similarly, the quantum value of $\mathcal{B}_n'$ cannot exceed $2n$. There is only one way to obtain a maximum value of $(\mathcal{B}_n')_Q$ when

for every k the probability $P(a = k, b = +|x = n + 1, y = k)$ equals zero. This is possible when the POVM elements of the measurement $\{A_{k|n+1}\}$ is antialigned with n projective measurements of Bob's side. Such POVM elements can then be written as $A_{k|n+1} = \frac{2}{n}\Pi^{-}_{A_k}$, with $\frac{2}{n}\sum_{k=1}^{n}\Pi^{-}_{A_k} = \mathbb{I}$. We already have the parity-oblivious condition in Eq. (53) where such a condition is satisfied for qubit observables.

Note here that every element of the POVMs $\{A_{k|n+1}\}$ is effectively a projector. One may expect to certify n outcome qubit POVMs as in the $n = 3$ case and consequently $\log_2 n$ bits of randomness. However, $\{A_{k|n+1}\}$ is not an extremal set of POVMs if (odd) $n > 3$. It is known that the extremal POVMs for qubit systems have at most four outcomes and nonextremal POVMs can be simulated by convex combination of extremal POVMs [86]. This indicates that the certification of unbounded randomness is not possible using our generalized version of the game for arbitrary n. However, the optimal quantum success probability for the arbitrary n case enables device-independent self-testing of the entangled state and measurements.

VII. CONCLUSION

We have provided an interesting oblivious communication game played between two parties, Alice and Bob, who receive an arbitrary (odd) number n of inputs. In particular, we provided an entanglement-assisted parity-oblivious game where Alice is allowed to communicate any amount of information but that should not reveal the parity information of the inputs to Bob. Such an oblivious condition in an operational theory implies obliviousness at the level of ontic states for a preparation noncontextual ontological model [17]. We showed that given any arbitrary n the success probability of our game is solely dependent on a relevant Bell expression $\mathcal{B}_n$. We demonstrated that the upper bound $\mathcal{B}_n$ can be reduced from the trivial case (the local bound), which we termed here a nontrivial preparation noncontextual bound. The aforementioned Bell expression is optimized using the SOS approach and it is found that a two-qubit maximally entangled state and an interesting set of observables in the qubit system will suffice for the purpose of optimization. Interestingly, the set of observables leading to the optimal value satisfies the required parity-oblivious condition of Alice's inputs. This provides a functional relationship between Alice's choice of observables, which in turn reduces the local bound to the nontrivial preparation noncontextual bound of $\mathcal{B}_n$. Thus, for specific choices of states and measurements, it is possible that an optimal quantum value of $(\mathcal{B}_n)^{\text{opt}}_Q$ may not be enough to exhibit nonlocality, but the nonclassicality in the form of nontrivial preparation contextuality may be demonstrated.

Using the optimal quantum value $(\mathcal{B}_3)^{\text{opt}}_Q = 6$ for the $n = 3$ case, we demonstrated the self-testing of a two-qubit maximally entangled state and trine-spin observables. We used it to certify the three-outcome extremal POVMs, which in turn enabled us to certify the $\log_2 3$ bits of local randomness. Further, we generalized our scheme for any arbitrary (odd) number of inputs n of Alice and Bob and demonstrated that the optimal quantum value of the Bell expression $(\mathcal{B}_n)^{\text{opt}}_Q$ can be obtained for a qubit system local to Alice and Bob. One may intend to examine the possibility of certifying n-outcome POVMs by using a modified version of the Bell expression and its optimal quantum value $(\mathcal{B}'_n)^{\text{opt}}_Q$. Since extremal POVMs for qubit systems have at most four outcomes and nonextremal POVMs can be simulated by convex combination of extremal measurements, then the certification of n-outcome POVMs is not possible. Finally, we may remark that since the generalized Bell expression can be optimized for qubit systems, then the parity-oblivious communication game presented here can be tested using the existing technologies.

ACKNOWLEDGMENT

The author acknowledges support through Project No. DST/ICPS/QuEST/Theme 1/2019/4.

APPENDIX A: SELF-TESTING OF STATE AND MEASUREMENTS BASED ON THE OPTIMAL VALUE OF $\mathcal{B}_3$

We provide the detailed derivation of self-testing of the maximally entangled state and trine set of spin observables for the $n = 3$ scenario based on the optimal quantum violation of Bell's inequality (10). Specifically, we prove here Eqs. (27)–(30) by using the self-testing circuit in Fig. 1. The self-testing relations given by Eqs. (25) and (26) are derived as follows. We define $Z_A = A_1$, $\tilde{X}_A = (A_3 - A_2)/\sqrt{3}$, $Z_B = -B_1$, and $\tilde{X}_B = (B_2 - B_3)/\sqrt{3}$. From Eq. (18) the optimal quantum violation ensures that $A_1B_1|\psi\rangle_{AB} = A_2B_2|\psi\rangle_{AB} = A_3B_3|\psi\rangle_{AB} = -|\psi\rangle_{AB}$. Using $|\psi_{AB}\rangle = -A_1B_1|\psi_{AB}\rangle$, we have $A_1|\psi_{AB}\rangle = -B_1|\psi_{AB}\rangle$ and hence

$$Z_A|\psi\rangle_{AB} = Z_B|\psi\rangle_{AB}. \tag{A1}$$

Similarly, we can write

$$\begin{aligned}\tilde{X}_A\tilde{X}_B|\psi\rangle_{AB} &= \tfrac{1}{3}(A_3B_2 - A_3B_3 - A_2B_2 + A_2B_3)|\psi\rangle_{AB}\\ &= \tfrac{1}{3}(2 + A_3B_2 + A_2B_3)|\psi\rangle_{AB}.\end{aligned} \tag{A2}$$

We prove that $(A_3B_2 + A_2B_3)|\psi\rangle_{AB} = |\psi\rangle_{AB}$. Note that the optimal violation provides $A_1 + A_2 + A_3 = 0$ to hold for Alice's observables and $B_1 + B_2 + B_3 = 0$ for Bob's observables. Then, by considering $A_1(B_1 + B_2 + B_3)|\psi\rangle_{AB} = 0$, we get $(A_1B_2 + A_1B_3)|\psi\rangle_{AB} = |\psi\rangle_{AB}$. Similarly, we get five more relations as $(A_2B_1 + A_2B_3)|\psi\rangle_{AB} = |\psi\rangle_{AB}$, $(A_3B_1 + A_3B_2)|\psi\rangle_{AB} = |\psi\rangle_{AB}$, $(A_2B_1 + A_3B_1)|\psi\rangle_{AB} = |\psi\rangle_{AB}$, $(A_1B_2 + A_3B_2)|\psi\rangle_{AB} = |\psi\rangle_{AB}$, and $(A_2B_3 + A_1B_3)|\psi\rangle_{AB} = |\psi\rangle_{AB}$. Using these relations, it can be proved that $(A_3B_2 + A_2B_3)|\psi\rangle_{AB} = |\psi\rangle_{AB}$. In fact, it can be proved that each of $A_xB_y|\psi\rangle_{AB}$ is equal to the other for any x *not* equal to y.

From Eq. (A2) we then have $\tilde{X}_A\tilde{X}_B|\psi\rangle_{AB} = |\psi\rangle_{AB}$, i.e.,

$$\tilde{X}_A|\psi\rangle_{AB} = \tilde{X}_B|\psi\rangle_{AB}. \tag{A3}$$

Using the aforementioned relations, it can be shown that

$$\begin{aligned}&(Z_A\tilde{X}_A + \tilde{X}_AZ_A)|\psi\rangle_{AB}\\ &\quad= \tfrac{1}{3}(A_1B_3 + A_3B_1 - A_1B_2 - A_2B_1)|\psi\rangle_{AB} = 0\end{aligned} \tag{A4}$$

and

$$(Z_B\tilde{X}_B + \tilde{X}_B Z_B)|\psi\rangle_{AB} = \tfrac{1}{3}(B_1B_3 + B_3B_1 - B_1B_2 - B_2B_1)|\psi\rangle_{AB} = 0. \quad \text{(A5)}$$

We then have

$$\{Z_A, \tilde{X}_A\}|\psi\rangle_{AB} = \{Z_B, \tilde{X}_B\}|\psi\rangle_{AB} = 0. \quad \text{(A6)}$$

Equations (A1), (A3), and (A6) are the self-testing properties provided in Eqs. (25) and (26).

Using the isometry described in Fig. 1, we can write

$$\Phi(|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = \tfrac{1}{4}[(1+Z_A)(1+Z_B)|\psi\rangle_{AB}|00\rangle + \tilde{X}_B(1+Z_A)(1-Z_B)|\psi\rangle_{AB}|01\rangle + X_A(1-Z_A)(1+Z_B)|\psi\rangle_{AB}|10\rangle + \tilde{X}_A\tilde{X}_B(1-Z_A)(1-Z_B)|\psi\rangle_{AB}|11\rangle], \quad \text{(A7)}$$

which can be recast using the self-testing properties given by Eqs. (25) and (26) as

$$\Phi(|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = \frac{1}{4}[2(1+Z_A)|\psi\rangle_{AB} \otimes (|00\rangle + |11\rangle)] \equiv \frac{1+Z_A}{\sqrt{2}}|\psi\rangle_{AB} \otimes |\phi^+\rangle_{A'B'}. \quad \text{(A8)}$$

Identifying $|\chi\rangle_{AB} = \frac{1+Z_A}{\sqrt{2}}|\psi\rangle_{AB}$, we have Eq. (27). This implies the self-testing of a two-qubit maximally entangled state using the optimal quantum value of the Bell expression in Eq. (10).

Now, for self-testing of measurements, we note that $B_1 = -Z_B$, $B_2 = (\sqrt{3}/2)\tilde{X}_B + \frac{1}{2}Z_B$, and $B_3 = -(\sqrt{3}/2)\tilde{X}_B + \frac{1}{2}Z_B$. Similar relations can be written for A_1, A_2, and A_3. It is then enough to demonstrate how the local isometry works for Z_B, X_B, X_A, and Z_A. We thus show the following by using the self-testing circuit:

$$\Phi(\tilde{X}_A|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = \tfrac{1}{4}[(1+Z_A)\tilde{X}_A(1+Z_B)|\psi\rangle_{AB}|00\rangle + \tilde{X}_B(1+Z_A)\tilde{X}_A(1-Z_B)|\psi\rangle_{AB}|01\rangle + \tilde{X}_A(1-Z_A)\tilde{X}_A(1+Z_B)|\psi\rangle_{AB}|10\rangle + \tilde{X}_A\tilde{X}_B(1-Z_A)\tilde{X}_A(1-Z_B)|\psi\rangle_{AB}|11\rangle]. \quad \text{(A9)}$$

The first term $(1+Z_A)\tilde{X}_A(1+Z_B)|\psi\rangle_{AB}|00\rangle = (\tilde{X}_A + \tilde{X}_AZ_B + Z_A\tilde{X}_A + Z_A\tilde{X}_AZ_B)|\psi\rangle|00\rangle$. Using $Z_A|\psi\rangle = Z_B|\psi\rangle$ and $\{Z_A, \tilde{X}_A\}|\psi\rangle_{AB} = 0$, we find $(\tilde{X}_A + \{Z_A, \tilde{X}_A\} - \tilde{X}_A)|\psi\rangle_{AB}|00\rangle = 0$. The second term is given by $(\tilde{X}_B\tilde{X}_A - \tilde{X}_B\tilde{X}_AZ_B + \tilde{X}_BZ_A\tilde{X}_A - \tilde{X}_BZ_A\tilde{X}_AZ_B)|\psi\rangle_{AB}|01\rangle = (2 + Z_A + Z_B)|\psi\rangle_{AB}|01\rangle = 2(1+Z_A)|\psi\rangle_{AB}|01\rangle$. The third term $(\tilde{X}_A\tilde{X}_A + \tilde{X}_AZ_A\tilde{X}_A - \tilde{X}_A\tilde{X}_AZ_B - \tilde{X}_AZ_A\tilde{X}_AZ_B)|\psi\rangle_{AB}|10\rangle = 2(1+Z_A)|\psi\rangle_{AB}|01\rangle$. Similarly, the fourth term $(\tilde{X}_A\tilde{X}_B\tilde{X}_A - \tilde{X}_A\tilde{X}_B\tilde{X}_AZ_B - \tilde{X}_A\tilde{X}_BZ_A\tilde{X}_A + \tilde{X}_A\tilde{X}_BZ_A\tilde{X}_AZ_B)|\psi\rangle_{AB}|11\rangle$ can be written as $(\tilde{X}_A + \tilde{X}_BZ_B - \tilde{X}_AZ_A - \tilde{X}_A\tilde{X}_B\tilde{X}_A)|\psi\rangle_{AB}|11\rangle$ by using Eqs. (A1) and (A3). Further using them along with $\{Z_A, \tilde{X}_A\}|\psi\rangle_{AB} = 0$ from Eq. (A6), we have $(\tilde{X}_A - \{\tilde{X}_B, Z_B\} - \tilde{X}_A)|\psi\rangle_{AB}|11\rangle = 0$.

Using those, Eq. (A9) can then be written as

$$\Phi(\tilde{X}_A|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = \frac{1+Z_A}{\sqrt{2}}|\psi\rangle_{AB}\frac{(|01\rangle + |10\rangle)}{\sqrt{2}} = |\chi\rangle_{AB} \otimes (\sigma_x \otimes \mathbb{I})|\phi^+\rangle_{A'B'}. \quad \text{(A10)}$$

Following steps similar to those above, we have

$$\Phi(\tilde{X}_B|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = \tfrac{1}{4}[(1+Z_A)(1+Z_B)\tilde{X}_B|\psi\rangle|00\rangle + \tilde{X}_B(1+Z_A)(1-Z_B)\tilde{X}_B|\psi\rangle|01\rangle + X_A(1-Z_A)(1+Z_B)\tilde{X}_B|\psi\rangle|10\rangle + \tilde{X}_A\tilde{X}_B(1-Z_A)(1-Z_B)\tilde{X}_B|\psi\rangle|11\rangle] \equiv |\chi\rangle_{AB} \otimes (\mathbb{I} \otimes \sigma_x)|\phi^+\rangle_{A'B'} \quad \text{(A11)}$$

and

$$\Phi(Z_A|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = |\chi\rangle_{AB} \otimes (\sigma_z \otimes \mathbb{I})|\phi^+\rangle_{A'B'}, \quad \text{(A12)}$$

$$\Phi(Z_B|\psi\rangle_{AB} \otimes |00\rangle_{A'B'}) = |\chi\rangle_{AB} \otimes (\mathbb{I} \otimes \sigma_z)|\phi^+\rangle_{A'B'}. \quad \text{(A13)}$$

Using the results in Eqs. (A11)–(A13), it is straightforward to show that

$$\Phi(B_y|\psi\rangle) = |\chi\rangle_{AB} \otimes (\mathbb{I} \otimes B'_y)|\phi^+\rangle_{A'B'}, \quad \text{(A14)}$$

$$\Phi(A_x|\psi\rangle) = |\chi\rangle_{AB} \otimes (A'_x \otimes \mathbb{I})|\phi^+\rangle_{A'B'}. \quad \text{(A15)}$$

Similarly, a few more steps are required to show that

$$\Phi(A_x \otimes B_y|\psi\rangle) = |\chi\rangle_{AB} \otimes (A'_x \otimes B'_y)|\phi^+\rangle_{A'B'}. \quad \text{(A16)}$$

We have thus self-tested the measurements and Eqs. (A14)–(A16) are Eqs. (28)–(30).

APPENDIX B: SELF-TESTING FOR THE CASE OF $n = 5$

We note that there are different forms of choices of observable available that satisfy the oblivious condition given by Eq. (52). One of the choices is presented in Eq. (51). We can choose another set of observables by keeping the parity-oblivious condition and consequently the functional relation between the observables of Alice and Bob intact. As already mentioned in the main text, such a functional relation fixes the optimal quantum value of the Bell expression (42). We provide the self-testing scheme for $n = 5$, which can be straightforwardly generalized for any odd n. The alternative choices for $n = 5$ are

$$A_{5,1} = \sigma_z, \quad A_{5,2} = \nu_{5,1}\sigma_x - \beta_{5,1}\sigma_y - \frac{\sigma_z}{4},$$
$$A_{5,3} = -\nu_{5,1}\sigma_x - \beta_{5,1}\sigma_y - \frac{\sigma_z}{4},$$
$$A_{5,4} = \nu_{5,1}\sigma_x + \beta_{5,1}\sigma_y - \frac{\sigma_z}{4}, \quad A_{5,5} = -\nu_{5,1}\sigma_x + \beta_{5,1}\sigma_y - \frac{\sigma_z}{4}, \tag{B1}$$

satisfying the parity-oblivious condition $\sum_{n=1}^{5} A_{5,n} = 0$. Here $|\nu_{5,n}|^2 + |\beta_{5,n}|^2 + \frac{1}{16} = 1$.

Following the usual SWAP circuit in Fig. 2, we show that the maximum violation of $\mathcal{B}_5$ implies the existence of an isometry Φ so that $\Phi : \mathcal{H}_A \otimes \mathcal{H}_B \to (\mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_{A''}) \otimes (\mathcal{H}_B \otimes \mathcal{H}_{B'} \otimes \mathcal{H}_{B''})$ and $|\psi\rangle_{AB} \to |\xi\rangle_{ABA'B'} \otimes |\phi^+\rangle_{A''B''}$. Let us define the observables $Z_A = A_{5,1}$, $X_A = A_{5,2} - A_{5,3} + A_{5,4} - A_{5,5}$, and $Y_A = -A_{5,2} - A_{5,3} + A_{5,4} + A_{5,5}$ along with $Z_B = -B_{5,1}$, $X_B = -B_{5,2} + B_{5,3} - B_{5,4} + B_{5,5}$, and $Y_B = -B_{5,2} - B_{5,3} + B_{5,4} + B_{5,5}$ satisfying following properties. The observables X_A, X_B, Y_A, and Y_B may not be Hermitian, but one can define the following Hermitian operators, for example, $\tilde{X}_A = X_A/\|X_A\|$. The self-testing relations are

$$Z_A|\psi\rangle = Z_B|\psi\rangle, \quad \tilde{X}_A|\psi\rangle = \tilde{X}_B|\psi\rangle, \quad \tilde{Y}_A|\psi\rangle = -\tilde{Y}_B|\psi\rangle, \tag{B2}$$

$$\{Z_A, \tilde{X}_A\}|\psi\rangle\{\tilde{Y}_A, \tilde{X}_A\}|\psi\rangle = \{Z_A, \tilde{Y}_A\}|\psi\rangle = 0, \tag{B3}$$

$$\{Z_B, \tilde{X}_B\}|\psi\rangle\{\tilde{Y}_B, \tilde{X}_B\}|\psi\rangle = \{Z_B, \tilde{Y}_B\}|\psi\rangle = 0. \tag{B4}$$

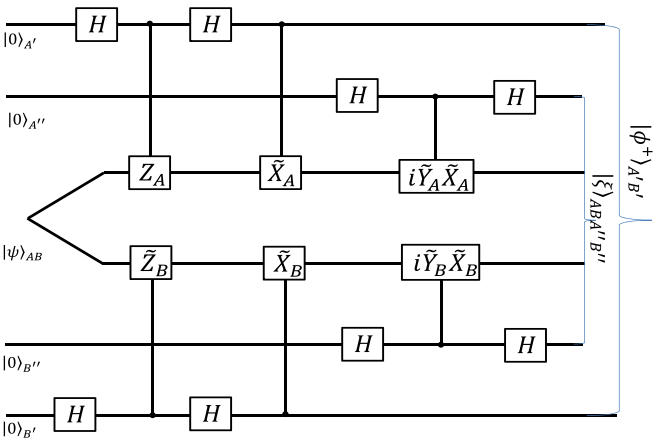

FIG. 2. Self-testing scheme based on the optimal quantum value of $\mathbb{B}_5$ which can be obtained by setting $n = 5$ in Eq. (10). Details of the SWAP isometry are given in the text.

Using the above relations, we can also have

$$\tilde{Y}_A\tilde{X}_A|\psi\rangle = \tilde{Y}_B\tilde{X}_B|\psi\rangle, \tag{B5}$$

which provides $\tilde{Y}_A\tilde{X}_A\tilde{Y}_B\tilde{X}_B|\psi\rangle = -|\psi\rangle$. Using the circuit in Fig. 2, we demonstrate the self-testing of the two-qubit maximally entangled state using the isometry $\Phi(|\psi\rangle_{AB} \otimes |00\rangle_{A'B'} \otimes |00\rangle_{A''B''})$.

It is already shown in Appendix A that, due to the action of the first two pairs of Hadamard operations and controlled gate operations of Z_A, $\tilde{X}_A$, Z_B, and $\tilde{X}_B$, the state evolves to

$$|\chi\rangle_{AB} \otimes |\phi^+\rangle_{A'B'} \otimes |00\rangle_{A''B''}, \tag{B6}$$

where $|\chi\rangle_{AB} = \frac{1+Z_A}{\sqrt{2}}|\psi\rangle_{AB}$. After the third pair of Hadamard gates, the state evolves to $|\xi\rangle_{AB} \otimes |\phi^+\rangle_{A'B'} \otimes |++\rangle_{A''B''}$ and applying the final set of controlled gates and finally using Eq. (B5), the state in Eq. (B6) evolves to

$$|\chi\rangle_{AB} \otimes |\phi^+\rangle_{A'B'} \otimes \tfrac{1}{2}[|00\rangle_{A''B''} + i\tilde{Y}_B\tilde{X}_B|01\rangle_{A''B''} + i\tilde{Y}_B\tilde{X}_B|10\rangle_{A''B''} - |11\rangle_{A''B''}]. \tag{B7}$$

Considering the action of the final pair of Hadamard gates, we find that the self-testing of the entangled state is given by

$$\Phi(|\psi\rangle_{AB} \otimes |00\rangle_{A'B'} \otimes |00\rangle_{A''B''}) = |\xi\rangle_{ABA''B''} \otimes |\phi^+\rangle_{A'B'}, \tag{B8}$$

where $|\xi\rangle_{ABA''B''}$ is the so-called junk state that is given by

$$|\xi\rangle_{ABA''B''} = \tfrac{1}{2}[|\chi\rangle_{AB} \otimes (\mathbb{I} + i\tilde{Y}_A\tilde{X}_A)|00\rangle_{A''B''} + |\chi\rangle_{AB} \otimes (\mathbb{I} - i\tilde{Y}_A\tilde{X}_A)|11\rangle_{A''B''}]. \tag{B9}$$

Now, for the local unitary evolutions provided in Fig. 2 and using self-testing relations given by Eqs. (B2) and (B3), it is straightforward to demonstrate that

$$\Phi(\tilde{X}_A|\psi\rangle_{AB} \otimes |00\rangle_{A'B'} \otimes |00\rangle_{A''B''}) = |\xi\rangle_{ABA''B''} \otimes (\mathbb{I} \otimes \sigma_x)|\phi^+\rangle_{A'B'}, \tag{B10}$$

$$\Phi(Z_A|\psi\rangle_{AB} \otimes |00\rangle_{A'B'} \otimes |00\rangle_{A''B''}) = |\xi\rangle_{ABA''B''} \otimes (\mathbb{I} \otimes \sigma_z)|\phi^+\rangle_{A'B'}, \tag{B11}$$

$$\Phi(\tilde{X}_B|\psi\rangle_{AB} \otimes |00\rangle_{A'B'} \otimes |00\rangle_{A''B''}) = |\xi\rangle_{ABA''B''} \otimes (\sigma_x \otimes \mathbb{I})|\phi^+\rangle_{A'B'}, \tag{B12}$$

$$\Phi(Z_B|\psi\rangle_{AB} \otimes |00\rangle_{A'B'} \otimes |00\rangle_{A''B''}) = |\xi\rangle_{ABA''B''} \otimes (\sigma_z \otimes \mathbb{I})|\phi^+\rangle_{A'B'}. \tag{B13}$$

However, for $\Phi(\tilde{Y}_A|\psi\rangle_{AB} \otimes |00\rangle_{A'B'} \otimes |00\rangle_{A''B''})$, the derivation is a little involved and we provide a modified version of the derivation. The state just before the final pair of Hadamard gates can be written as

$$\tfrac{1}{2}[|\chi\rangle_{AB} \otimes |00\rangle_{A''B''} + i\tilde{Y}_B\tilde{X}_B|\chi\rangle_{AB} \otimes |01\rangle_{A''B''} + i\tilde{Y}_A\tilde{X}_A|\chi\rangle_{AB} \otimes |10\rangle_{A''B''} - \tilde{Y}_A\tilde{X}_A\tilde{Y}_B\tilde{X}_B|\chi\rangle_{AB} \otimes |11\rangle_{A''B''}]|\phi^+\rangle_{A'B'}. \tag{B14}$$

Using Eq. (B5) and after the action of the final pair of Hadamard gates we finally have

$$\begin{aligned}&\Phi(\tilde{Y}_A|\psi\rangle_{AB}\otimes|00\rangle_{A'B'}\otimes|00\rangle_{A''B''})\\&=\tfrac{1}{2}[|\chi\rangle_{AB}\otimes(\mathbb{I}+i\tilde{Y}_A\tilde{X}_A)|00\rangle_{A''B''}\\&-|\chi\rangle_{AB}\otimes(\mathbb{I}-i\tilde{Y}_A\tilde{X}_A)|11\rangle_{A''B''}]\otimes(\sigma_y\otimes\mathbb{I})|\phi^+\rangle_{A'B'}\\&\equiv\sigma_z^{A''}|\xi\rangle_{ABA''B''}\otimes(\sigma_y\otimes\mathbb{I})|\phi^+\rangle_{A'B'}.\end{aligned}\tag{B15}$$

Similarly, following the earlier steps, it can be easily seen that

$$\begin{aligned}&\Phi(\tilde{Y}_B|\psi\rangle_{AB}\otimes|00\rangle_{A'B'}\otimes|00\rangle_{A''B''})\\&=\sigma_z^{B''}|\xi\rangle_{ABA''B''}\otimes(\mathbb{I}\otimes\sigma_y)|\phi^+\rangle_{A'B'}.\end{aligned}\tag{B16}$$

In order to take care of the conjugation issue involved with σ_y, the observable $\sigma_z^{B''}$ has to be suitably used.

APPENDIX C: SKETCH REGARDING THE SELF-TESTING FOR THE CASE OF (ODD) $n > 5$

Now, for the self-testing purpose in the case of $n > 5$ it is convenient to use a different set of observables which also satisfy the required parity-oblivious condition in Eq. (52). We choose the following set of observables. When $n = 4l + 5$ with $l = 0, 1, 2, \ldots,$

$$\begin{aligned}A_{n,1}&=\sigma_z,\quad \{A_{n,2+4m}\}=\nu_{n,m}\sigma_x-\beta_{n,m}\sigma_y-\frac{\sigma_z}{n-1},\\\{A_{n,3+4m}\}&=-\nu_{n,m}\sigma_x-\beta_{n,m}\sigma_y-\frac{\sigma_z}{n-1},\\\{A_{n,4+4m}\}&=\nu_{n,m}\sigma_x+\beta_{n,m}\sigma_y-\frac{\sigma_z}{n-1},\\\{A_{n,5+4m}\}&=-\nu_{n,m}\sigma_x+\beta_{n,m}\sigma_y-\frac{\sigma_z}{n-1},\end{aligned}\tag{C1}$$

where $m = 0, 1, 2, \ldots, n-5$ and $|\nu_{n,m}|^2 + |\beta_{n,m}|^2 + 1/(n-1)^2 = 1$. For $n = 4l + 7$ along with the above set of observables, we additionally require

$$\begin{aligned}A_{n,(n-1)}&=\alpha'_n\sigma_x-\beta'_n\sigma_y-\frac{\sigma_z}{n-1},\\A_{n,n}&=-\alpha'_n\sigma_x+\beta'_n\sigma_y-\frac{\sigma_z}{n-1},\end{aligned}\tag{C2}$$

where $|\alpha'_n|^2 + |\beta'_n|^2 + 1/(n-1)^2 = 1$. By suitably summing and subtracting the observables in Eqs. (C1) and (C2) one obtains Z_A, Z_B, X_A, X_B, Y_A, and Y_B, which will provide the self-testing relations (B2)–(B5).

[1] J. Bell, On the Einstein Podolsky Rosen paradox, Physics **1**, 195 (1964).

[2] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[3] S. Kochen and E. P. Specker, The problem of hidden variables in quantum mechanics, J. Math. Mech. **17**, 59 (1967).

[4] R. W. Spekkens, Contextuality for preparations, transformations, and unsharp measurements, Phys. Rev. A **71**, 052108 (2005).

[5] R. Raz, *Proceedings of the 31st Annual ACM Symposium on Theory of Computing, Atlanta, 1999* (ACM, New York, 1999), pp. 358–367.

[6] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Quantum Fingerprinting, Phys. Rev. Lett. **87**, 167902 (2001).

[7] R. de Wolf, Quantum communication and complexity, Theor. Comput. Sci. **287**, 337 (2002).

[8] C. Brukner, M. Zukowski, and A. Zeilinger, Quantum Communication Complexity Protocol with Two Entangled Qutrits, Phys. Rev. Lett. **89**, 197901 (2002).

[9] G. Brassard, Quantum communication complexity, Found. Phys. **33**, 1593 (2003).

[10] C. Brukner, M. Zukowski, J.-W. Pan, and A. Zeilinger, Quantum Communication Complexity Protocol with Two Entangled Qutrits, Phys. Rev. Lett. **92**, 127901 (2004).

[11] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, Quantum random access codes with shared randomness, arXiv:0810.2937.

[12] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Nonlocality and communication complexity, Rev Mod. Phys. **82**, 665 (2010).

[13] J. Oppenheim and S. Wehner, The uncertainty principle determines the nonlocality of quantum mechanics, Science **19**, 330 (2010).

[14] H. Buhrman, Ł. Czekaj, A. Grudka, M. Horodecki, P. Horodecki, M. Markiewicz, F. Speelman, and S. Strelchuk, Quantum communication complexity advantage implies violation of a Bell inequality, Proc. Natl. Acad. Sci. USA **113**, 3191 (2016).

[15] D. Martinez, A. Tavakoli, M. Casanova, G. Canas, B. Marques, and G. Lima, High-Dimensional Quantum Communication Complexity beyond Strategies Based on Bell's Theorem, Phys. Rev. Lett. **121**, 150504 (2018).

[16] A. Tavakoli, M. Zukowski, and C. Brukner, Does violation of a Bell inequality always imply quantum advantage in a communication complexity problem?, Quantum **4**, 316 (2020).

[17] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, G. J. Pryde, Preparation Contextuality Powers Parity-Oblivious Multiplexing, Phys. Rev. Lett. **102**, 010401 (2009).

[18] M. Banik, S. S. Bhattacharya, A. Mukherjee, A. Roy, A. Ambainis, and A. Rai, Limited preparation contextuality in quantum theory and its relation to the Cirel'son bound, Phys. Rev. A **92**, 030103(R) (2015).

[19] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Quantum Random Access Codes Using Single d-Level Systems, Phys. Rev. Lett. **114**, 170502 (2015).

[20] A. Chailloux, I. Kerenidis, S. Kundu, and J. Sikora, Optimal bounds for parity-oblivious random access codes, New J. Phys. **18**, 045003 (2016).

[21] A. Hameedi, A. Tavakoli, B. Marques, and M. Bourennane, Communication Games Reveal Preparation Contextuality, Phys. Rev. Lett. **119**, 220402 (2017).

[22] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Semi-device-independent framework based on natural physical assumptions, Quantum **1**, 33 (2017).

[23] S. Ghorai and A. K. Pan, Optimal quantum preparation contextuality in an n-bit parity-oblivious multiplexing task, Phys. Rev. A **98**, 032110 (2018).

[24] A. Ambainis, M. Banik, A. Chaturvedi, D. Kravchenko, and A. Rai, Parity oblivious d-level random access codes and class of noncontextuality inequalities, Quantum Inf. Process. **18**, 111 (2019).

[25] D. Saha, P. Horodecki, and M. Pawłowski, State independent contextuality advances one-way communication, New J. Phys. **21**, 093057 (2019).

[26] D. Saha and A. Chaturvedi, Preparation contextuality as an essential feature underlying quantum communication advantage, Phys. Rev. A **100**, 022108 (2019).

[27] A. Tavakoli, E. Z. Cruzeiro, J. B. Brask, N. Gisin, and N. Brunner, Informationally restricted quantum correlations, Quantum **4**, 332 (2020).

[28] M. F. Pusey, Robust preparation noncontextuality inequalities in the simplest scenario, Phys. Rev. A **98**, 022112 (2018).

[29] A. Tavakoli and R. Uola, Measurement incompatibility and steering are necessary and sufficient for operational contextuality, Phys. Rev. Res. **2**, 013011 (2020).

[30] N. Harrigan and R. Spekkens, Einstein, incompleteness, and the epistemic view of quantum states, Found. Phys. **40**, 125 (2010).

[31] A. K. Pan, Revealing universal quantum contextuality through communication games, Sci. Rep. **9**, 17631 (2019).

[32] A. K. Pan, Two definitions of maximally ψ-epistemic ontological model and preparation non-contextuality, Europhys. Lett. **133**, 50004 (2021).

[33] A. Kumari and A. K. Pan, Sharing nonlocality and nontrivial preparation contextuality using the same family of Bell expressions, Phys. Rev. A **100**, 062130 (2019).

[34] A. K. Pan and S. S. Mahato, Device-independent certification of the Hilbert-space dimension using a family of Bell expressions, Phys. Rev. A **102**, 052221 (2020).

[35] D. Mayers and A. Yao, *Proceedings of the 39th IEEE Conference on Foundations of Computer Science, Palo Alto, 1998* (IEEE, New York, 1998).

[36] M. McKague and M. Mosca, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by W. van Dam, V. M. Kendon, and S. Severini, Lecture Notes in Computer Science Vol. 6519 (Springer, Berlin, 2010), p. 113.

[37] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inf. Comput. **4**, 273 (2004).

[38] M. McKague, T. H. Yang, and V. Scarani, Robust self-testing of the singlet, J. Phys. A: Math. Theor. **45**, 455304 (2012).

[39] X. Wu, J. D. Bancal, M. McKague, and V. Scarani, Device-independent parallel self-testing of two singlets, Phys. Rev. A **93**, 062121 (2016).

[40] M. McKague, Self-testing in parallel, New J. Phys. **18**, 045013 (2016).

[41] O. Andersson, P. Badziag, I. Bengtsson, I. Dumitru, and A. Cabello, Self-testing properties of Gisin's elegant Bell inequality, Phys. Rev. A **96**, 032119 (2017).

[42] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. **8**, 15485 (2017).

[43] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, Self-testing multipartite entangled states through projections onto two systems, New J. Phys. **20**, 083041 (2018).

[44] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Device-Independent Entanglement Certification of All Entangled States, Phys. Rev. Lett. **121**, 180503 (2018).

[45] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Self-testing of Pauli observables for device-independent entanglement certification, Phys. Rev. A **98**, 042336 (2018).

[46] T. Coopmans, J. Kaniewski, and C. Schaffner, Robust self-testing of two-qubit states, Phys. Rev. A **99**, 052123 (2019).

[47] A. Tavakoli, M. Farkas, D. Rosset, J.-D. Bancal, and J. Kaniewski, Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments: Bell inequalities, device-independent certification and applications, Sci. Adv. **7**, eabc3847 (2021).

[48] M. T. Quintino, C. Budroni, E. Woodhead, A. Cabello, and D. Cavalcanti, Device-Independent Tests of Structures of Measurement Incompatibility, Phys. Rev. Lett. **123**, 180401 (2019).

[49] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, Quantum **4**, 337 (2020).

[50] A. Tavakoli, J. Kaniewski, T. Vertesi, D. Rosset, and N. Brunner, Self-testing quantum states and measurements in the prepare-and-measure scenario, Phys. Rev. A **98**, 062307 (2018).

[51] M. Farkas and J. Kaniewski, Self-testing mutually unbiased bases in the prepare-and-measure scenario, Phys. Rev. A **99**, 032316 (2019).

[52] K. Mohan, A. Tavakoli, and N. Brunner, Sequential random access codes and self-testing of quantum measurement instruments, New J. Phys. **21**, 083034 (2019).

[53] P. Mironowicz and M. Pawłowski, Experimentally feasible semi-device-independent certification of four-outcome positive-operator-valued measurements, Phys. Rev. A **100**, 030301(R) (2019).

[54] A. Tavakoli, M. Smania, T. Vertesi, N. Brunner, and M. Bourennane, Self-testing non-projective quantum measurements in prepare-and-measure experiments, Sci. Adv. **6**, eaaw6664 (2020).

[55] M. Smania, P. Mironowicz, M. Nawareg, M. Pawłowski, A. Cabello, and M. Bourennane, Experimental certification of an informationally complete quantum measurement in a device-independent protocol, Optica **7**, 123 (2020).

[56] N. Miklin, J. J. Borkała, and M. Pawłowski, Semi-device-independent self-testing of unsharp measurements, Phys. Rev. Res. **2**, 033014 (2020).

[57] E. S. Gómez, S. Gómez, P. González, G. Cañas, J. F. Barra, A. Delgado, G. B. Xavier, A. Cabello, M. Kleinmann, T. Vértesi, and G. Lima, Device-Independent Certification of a Nonprojective Qubit Measurement, Phys. Rev. Lett. **117**, 260401 (2016).

[58] S. Gómez, A. Mattar, E. S. Gómez, D. Cavalcanti, O. Jiménez Farías, A. Acín, and G. Lima, Experimental nonlocality-based randomness generation with nonprojective measurements, Phys. Rev. A **97**, 040102(R) (2018).

[59] M. Matsumoto and T. Nishimura, Dynamic creation of pseudorandom number generators, ACM Trans. Model. Comput. Simul. **8**, 3 (1998).

[60] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).

[61] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2006; arXiv:0911.3814.

[62] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[63] O. Nieto-Silleras, S. Pironio, and J. Silman, Using complete measurement statistics for optimal device-independent randomness evaluation, New J. Phys. **16**, 013035 (2014).

[64] A. Acín, S. Massar, and S. Pironio, Randomness versus Nonlocality and Entanglement, Phys. Rev. Lett. **108**, 100402 (2012).

[65] R. Colbeck and R. Renner, Free randomness can be amplified, Nat. Phys. **8**, 450 (2012).

[66] S. Pironio and S. Massar, Security of practical private randomness generation, Phys. Rev. A **87**, 012336 (2013).

[67] J. D. Bancal, L. Sheridan, and V. Scarani, More randomness from the same data, New J. Phys. **16**, 033011 (2014).

[68] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A **93**, 040102(R) (2016).

[69] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín, Unbounded randomness certification using sequences of measurements, Phys. Rev. A **95**, 020102(R) (2017).

[70] O. Andersson, P. Badziag, I. Dumitru, and A. Cabello, Device-independent certification of two bits of randomness from one entangled bit and Gisin's elegant Bell inequality, Phys. Rev. A **97**, 012314 (2018).

[71] 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.*, Device independent quantum random number generation, Nature (London) **562**, 548 (2018).

[72] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Experimentally generated randomness certified by the impossibility of superluminal signals, Nature (London) **556**, 223 (2018).

[73] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu, C. A. Miller, A. Mink, and E. Knill, Experimental Low-Latency Device-Independent Quantum Randomness, Phys. Rev. Lett. **124**, 010505 (2020).

[74] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán *et al.*, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature (London) **526**, 682 (2015).

[75] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. A. Larsson, C. Abellan *et al.*, Significant-Loophole-Free Test of Bells Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (2015).

[76] 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.*, Strong Loophole-Free Test of Local Realism, Phys. Rev. Lett. **115**, 250402 (2015).

[77] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Self-Testing Quantum Random Number Generator, Phys. Rev. Lett. **114**, 150501 (2015).

[78] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, Phys. Rev. A **84**, 034301 (2011).

[79] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Semi-device independent random number expansion protocol with n to 1 quantum random access codes, Phys. Rev. A **85**, 052308 (2012).

[80] Y.-Q. Zhou, H.-W. Li, Y.-K. Wang, D.-D. Li, F. Gao, and Q.-Y. Wen, Semi-device-independent randomness expansion with partially free random sources, Phys. Rev. A **92**, 022331 (2015).

[81] A. K. Pan, Semi-device-independent randomness certification using Mermin's proof of Kochen-Specker contextuality, Eur. Phys. J. D **75**, 98 (2021).

[82] C. Bamps and S. Pironio, Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing, Phys. Rev. A **91**, 052111 (2015).

[83] C. J. Bradley, *Introduction to Inequalities* (United Kingdom Mathematics Trust, Leeds, 2006).

[84] G. M. D'Ariano, P. L. Presti, and P. Perinotti, Classical randomness in quantum measurements, J. Phys. A: Math. Gen. **38**, 5979 (2005).

[85] N. Gisin, in *Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle: Essays in Honour of Abner Shimony*, edited by W. C. Myrvold and J. Christian, The Western Ontario Series in Philosophy of Science Vol. 73 (Springer, Dordrecht, 2009), p. 125.

[86] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Simulating Positive-Operator-Valued Measures with Projective Measurements, Phys. Rev. Lett. **119**, 190501 (2017).