

Physical characterization of quantum devices from nonlocal correlations

Jean-Daniel Bancal,¹ Miguel Navascués,² Valerio Scarani,^{1,3} Tamás Vértesi,⁴ and Tzyh Haur Yang¹

¹Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore

²School of Physics, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom

³Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542, Singapore

⁴Institute for Nuclear Research, Hungarian Academy of Sciences, P.O. Box 51, H-4001 Debrecen, Hungary

(Received 22 July 2014; published 18 February 2015)

In the device-independent approach to quantum information theory, quantum systems are regarded as black boxes that, given an input (the measurement setting), return an output (the measurement result). These boxes are then treated regardless of their actual internal working. In this paper we develop SWAP, a theoretical concept that, in combination with the tool of semidefinite methods for the characterization of quantum correlations, allows us to estimate physical properties of the black boxes from the observed measurement statistics. We find that the SWAP tool provides bounds orders of magnitude better than previously known techniques (e.g., for a Clauser-Horne-Shimony-Holt violation larger than 2.57, SWAP predicts a singlet fidelity greater than 70%). This method also allows us to deal with hitherto intractable cases such as robust device-independent self-testing of nonmaximally entangled two-qutrit states in the Collins-Gisin-Linden-Massar-Popescu scenario (for which Jordan's lemma does not apply) and the device-independent certification of entangled measurements. We further apply the SWAP method to relate nonlocal correlations to work extraction and quantum dimensionality, hence demonstrating that this tool can be used to study a wide variety of properties relying on the sole knowledge of accessible statistics.

DOI: [10.1103/PhysRevA.91.022115](https://doi.org/10.1103/PhysRevA.91.022115)

PACS number(s): 03.65.Ta, 03.67.Mn

I. INTRODUCTION

In the past few years, several tasks for which quantum physics offers an advantage over classical methods have been found possible without assuming knowledge of the inner working of the devices involved, i.e., in a device-independent manner. This is the case of key distribution [1–5] and randomness certification [6,7], for instance (see also [8,9] and references therein for more examples).

In a device-independent experiment, also known as a Bell-type experiment, conclusions are not drawn from the knowledge that specific resources are used by the devices—the content of the devices might not be known *a priori*—but only from the observed relation between their inputs and outputs. Therefore, such devices are referred to as black boxes. Any actual physical realization of black boxes providing an advantage over classical devices must, however, use some quantum resource. For instance, the violation of a bipartite Bell inequality requires two black boxes to share an entangled quantum state. Some knowledge about the underlying quantum state can thus be inferred from the observed correlations only.

Several works have shown that, beyond the mere presence of entanglement, other quantum features such as genuine entanglement [10], the dimension of the underlying Hilbert space [11], or the overlap between measurements [12] can also be witnessed from correlations only. Moreover, quantitative statements have also been obtained, for instance, on the amount of entanglement [13,14]. However, even quantifying these aspects never fully characterizes the underlying quantum realization: Several states have the same negativity or Hilbert space dimension and several sets of measurements can have the same overlap. In fact, all of these estimations could be deduced if one were able to identify which states and measurements are performed by the black boxes in the first place. This is the subject of this paper (see Fig. 1).

The question of identifying quantum states and measurements from correlations only was originally addressed in two inequivalent ways. The first criterion is due to Refs. [15–17], where it is shown that if the Clauser-Horne-Shimony-Holt (CHSH) inequality [18] is violated maximally (given by the famous value of $2\sqrt{2}$ [19]), then the state being measured is equivalent to a maximally entangled state and the measurements are anticommuting on both Alice's and Bob's part. The other criterion that certifies the same state and measurements is due to Mayers and Yao [20] (see also [21]).

These pioneering works showed that there exist lists of statistical data in the device-independent framework that allow one to identify the quantum state and measurement operators involved in the actual experiments. Moreover, the process can tolerate a small amount of external noise. This notion of determining approximately the state and measurement operators involved via nonlocality detection is known as device-independent self-testing (or simply self-testing for short) and it has inspired a number of works on the subject [13,22–25]. However, the weak noise tolerance exhibited by the self-testing protocols proposed so far makes them inapplicable in realistic experimental situations. Moreover, all of them are specific to a given Bell inequality [13,22,24], or family of Bell inequalities [25], and thus cannot be applied to arbitrary states or measurements.

In this paper, building on the method sketched in Ref. [26], we present the SWAP method, a unified tool that allows one to guess the state, measurements, or other general properties of the quantum systems inside the boxes from the experimentally accessible correlations. The process is algorithmic, i.e., it is completely automated, and makes use of the Navascués-Pironio-Acín (NPA) hierarchy for the characterization of quantum correlations [27]. To illustrate the power of this method, we apply it to estimate different physical properties in standard Bell scenarios.

The structure of this paper is as follows. First, we recall the formal definition of self-testing. Then, in Sec. III we explain the main idea behind our method: an effective description, in the language of moment matrices, of the process of exchanging the content of black boxes with a trusted finite-dimensional system. This idea, together with the NPA hierarchy [27,28], allows us to estimate quantum monotones via convex optimization [29], in the same way that we would calculate such monotones had we known the exact mathematical representation of the state and measurement operators involved in the nonlocality experiment. We also indicate in this section how our results can be easily generalized to the case where black boxes are not independently and identically distributed. In Sec. IV we demonstrate that the method improves the noise tolerance of previous self-testing protocols by several orders of magnitude. Next we show how the method can be applied to Bell-type scenarios for which, due to their complexity, no robust device-independent protocols (no matter how fragile to noise) could be derived before. These are self-testing of states with measurements having more than two possible outcomes (Sec. V A), the certification of entangled measurements (Sec. V B), and the estimation of the amount of work extractable from nonlocal quantum systems (Sec. V C).

II. SELF-TESTING

Let Alice and Bob be two distant observers conducting measurements on a shared quantum system. If Alice (Bob) makes no assumption on the inner mechanisms of their experimental devices, she (he) has to regard each of her (his) devices as a black box where she (he) inputs a symbol x (y), the measurement setting, and obtains an output a (b), the measurement outcome. In these conditions, Alice and Bob can make a frequency analysis to estimate $p(a,b|x,y)$, the probability that they observe results a,b when they input x,y . The question of self-testing is whether the user can deduce, from the knowledge of these conditional probabilities only, the state and measurements used inside their boxes (see Fig. 1).

According to quantum theory, there exist a state ρ and measurement operators $\{E_a^x, F_b^y\}$ such that $p(a,b|x,y) = \text{tr}(\rho E_a^x \otimes F_b^y)$. Assuming that all physical implementations of a positive operator valued measure (POVM) involve a projective measurement over a dilated space, the operators $\{E_a^x, F_b^y\}$ can be taken as projectors. The underlying quantum

state ρ to which both parties have access in their laboratories can, in principle, be mixed. For simplicity, for all subsequent discussions, we will take it to be pure, i.e., $\rho = |\Psi\rangle\langle\Psi|$. However, as the reader can appreciate, all results presented in this paper hold independently of this assumption.

Now suppose that, after many runs of an experiment, the parties observe a probability distribution that is compatible with some specific state and measurements $(|\bar{\psi}\rangle, \{\bar{E}_a^x, \bar{F}_b^y\})$ defined in $\mathbb{C}^d \otimes \mathbb{C}^d$:

$$p(a,b|x,y) = \langle \bar{\psi} | \bar{E}_a^x \otimes \bar{F}_b^y | \bar{\psi} \rangle. \quad (1)$$

In general, this observation does not imply that the actual state $|\psi\rangle$ and measurements $\{E_a^x, F_b^y\}$ used by the black boxes are these: Since correlations admit in general several possible quantum realizations, the actual states and measurements could be different. Remarkably, however, for some $p(a,b|x,y)$ it turns out that the guessed state and measurements $(|\bar{\psi}\rangle, \{\bar{E}_a^x, \bar{F}_b^y\})$ are the only possible ones, up to local unitaries and the addition of irrelevant degrees of freedom. In this case, the observation of $p(a,b|x,y)$ certifies that the states and measurements used by the boxes are the guessed ones.

Technically, this is captured by the following self-testing statement: The correlations $p(a,b|x,y)$ allow for self-testing if for every quantum realization $(|\psi\rangle, \{E_a^x, F_b^y\})$ compatible with $p(a,b|x,y)$ there exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$ such that

$$\Phi|\psi\rangle = |\bar{\psi}\rangle_{A'B'} \otimes |\text{junk}\rangle_{AB}, \quad (2)$$

$$\Phi(E_a^x \otimes F_b^y |\psi\rangle) = (\bar{E}_a^x \otimes \bar{F}_b^y |\bar{\psi}\rangle)_{A'B'} \otimes |\text{junk}\rangle_{AB}, \quad (3)$$

where A' and B' are two ancillary qudits. The isometry must be seen as a virtual protocol: It does not need to be implemented in the laboratory as part of the procedure of self-testing; all that must be done in the laboratory is to query the boxes and derive $p(a,b|x,y)$.

Intuitively, the isometry consists of local swaps that put the relevant degrees of freedom from the boxes into the ancillas, which have the right dimension for a comparison with the desired state and measurement to be possible. Indeed, the intuition of the SWAP was already mentioned in the work of Mayers and Yao [20]. However, it was not exploited to derive a general method as we are going to do here.

III. METHOD

We first present the SWAP method with a specific example and then show how a general construction is possible for any self-testing scenario. Finally we show how to remove the assumptions of infinitely many runs and the assumption that the behavior of the devices is the same in each run and uncorrelated among the runs (the latter being usually referred to as the assumption of independent and identical distribution (i.i.d.) by analogy with sampling of probability distributions).

A. Example: Self-testing of qubit states

1. Construction of the SWAP operator

Since the swaps are local operations, it is enough to show how to construct one for Alice (the same construction applies

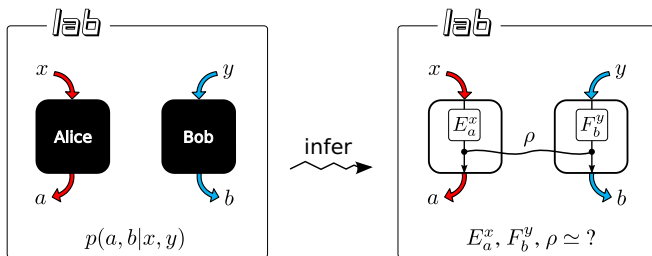


FIG. 1. (Color online) We are interested in certifying the physical properties of black boxes. This amounts to questioning the nature of the underlying quantum state ρ and of the measurement operators E_a^x, F_b^y , which are necessary for some boxes to produce the observed statistics $p(a,b|x,y)$.

to the other parties. If the state we wish to self-test is a qubit state, the local ancilla A' is a qubit. To construct the SWAP, we start by temporarily assuming that the state inside the box is indeed a qubit and then relax this assumption.

If the state inside Alice's box is a qubit, the SWAP operator between her system and ancilla can be written as the concatenation of three controlled-NOT (CNOT) gates with alternate controls:

$$S_{AA'} = UVU, \quad (4)$$

where

$$\begin{aligned} U &= \mathbb{I} \otimes |0\rangle\langle 0| + \sigma_x \otimes |1\rangle\langle 1|, \\ V &= |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_x \end{aligned} \quad (5)$$

are the CNOT gates with the ancilla and the system, respectively, as control. For simplicity, in this introduction we assume further that the operators σ_z and σ_x are part of the set of operators we want to self-test (see Sec. IV D for an example when this is not the case). For instance,

$$\sigma_z = \bar{A}_0 \equiv \bar{E}_{a=+1}^0 - \bar{E}_{a=-1}^0, \quad (6)$$

$$\sigma_x = \bar{A}_1 \equiv \bar{E}_{a=+1}^1 - \bar{E}_{a=-1}^1. \quad (7)$$

The trick is now to rewrite U and V with \bar{A}_0 and \bar{A}_1 on the side of the system and then to replace them by the real A_0 and A_1 operators defined analogously from the actual projectors E_a^x . This gives

$$\begin{aligned} U &= \mathbb{I} \otimes |0\rangle\langle 0| + A_1 \otimes |1\rangle\langle 1|, \\ V &= \frac{\mathbb{I} + A_0}{2} \otimes \mathbb{I} + \frac{\mathbb{I} - A_0}{2} \otimes \sigma_x. \end{aligned} \quad (8)$$

At this point, we have dropped the requirement that the system is a qubit. Nevertheless, these two operators are still unitary because, by assumption, $A_x^2 = \mathbb{I}$.

Finally, the guess for the SWAP operator is just (4) with the expressions (8) for U and V . Using the same construction for Bob's side, the final guess for the SWAP operator is

$$S = S_{AA'} \otimes S_{BB'} \quad (9)$$

A few remarks are in order here. First, note that $S_{AA'} = VUV$ would be an equally valid choice instead of (4). However, in several situations it can be preferable to use (4). For instance, if the ancilla is initialized in the state $|0\rangle$, then the action of the first U is equivalent to the identity. Then $S_{AA'}$ reduces to UV , which leads to simpler numerical computations than VUV . We refer to UV as a partial SWAP.

Second, note that the SWAP defined here explicitly depends on the measurement operators used by the individual parties. This guarantees that the result of applying this SWAP operator to the measured state is identical for all unitarily equivalent quantum representations.

2. State certification with the semidefinite program hierarchy

Once the SWAP operator is defined, the next step of the method describes how to use the knowledge of the correlations $p(a,b|x,y)$. For this, consider the self-testing of the state (2); the self-testing of measurements (3) follows a similar path and

will be sufficiently illustrated by our example in Sec. IV C. A possible figure of merit is the fidelity

$$F = \langle \bar{\psi} | \rho_{\text{SWAP}} | \bar{\psi} \rangle, \quad (10)$$

where ρ_{SWAP} is the state of the ancillas after the SWAP. The relation between this figure of merit and the trace distance between the desired and actual states is discussed in Sec. IV A.

Explicitly, if the initial dummy states of the ancillas are denoted by $\rho_{A'}$ and $\rho_{B'}$, we have

$$\rho_{\text{SWAP}} = \text{tr}_{AB}[\mathcal{S}(|\psi\rangle\langle\psi|)_{AB} \otimes \rho_{A'} \otimes \rho_{B'} \mathcal{S}^\dagger], \quad (11)$$

where the SWAP operator \mathcal{S} is defined by Eq. (9). Having expressed \mathcal{S} in terms of four of the desired operators A_0, A_1, B_0 and B_1 , we find ρ_{SWAP} to be a 4×4 matrix whose entries are linear combinations of expectation values such as $\langle \psi | A_x \otimes \mathbb{I} | \psi \rangle$, $\langle \psi | A_0 A_1 \otimes \mathbb{I} | \psi \rangle$, $\langle \psi | A_x \otimes B_y | \psi \rangle$, etc. Consequently, our estimate f on the singlet fidelity F attainable via isometries (10) is a linear combination of operator averages of the form $c_t = \langle \psi | t(A_x, B_y) | \psi \rangle$, where t is a product of the operators A_x, B_y .

Self-testing is perfect, i.e., (2) holds exactly, if we find $f = 1$; but the method automatically deals with imperfect cases, that is, it is robust by construction. So we are finally left to estimate the minimal possible value of f compatible with $p(a,b|x,y)$ and with quantum physics. In other words, we must solve the problem

$$\begin{aligned} \min_d \quad & f(d) = \langle \bar{\psi} | \rho_{\text{SWAP}}(d) | \bar{\psi} \rangle \\ \text{s.t.} \quad & d \in \mathcal{Q}, \\ & \frac{1}{4} \{ 1 + (-1)^a d_{A_x} + (-1)^b d_{B_y} + (-1)^{a+b} d_{A_x B_y} \} \\ & = p(a,b|x,y), \end{aligned} \quad (12)$$

where the maximization $d \in \mathcal{Q}$ is performed over the set \mathcal{Q} of all vectors $d = (d_{\mathbb{I}}, d_{A_0}, \dots)$ that admit a quantum representation, i.e., for which there exist a state $|\psi\rangle$ and dichotomic operators A_x, B_y such that $d_t = \langle \psi | t(A_x, B_y) | \psi \rangle$ for all products t . Note that in the optimization problem above we assumed for simplicity a probability distribution $p(a,b|x,y)$ with dichotomic settings $a, b \in \{0,1\}$.

Optimizations over the set of quantum momenta are computationally hard [30] and, in some scenarios, conjectured to be undecidable [31]. That is why we propose to relax the above problem to an optimization over the sets \mathcal{Q}^S , defined in Ref. [27] as outer approximations of the quantum set. Let S be a set of products of the operators A_x, B_y and let d be a complex vector whose entries are labeled by products of the form $s^\dagger t$, with $s, t \in S$ (objects such as d will be called moment vectors). We define $\Gamma^S(d)$ as a matrix whose rows and columns are numbered by products belonging to S and such that $\Gamma_{s,t} = d_{s^\dagger t}$. It can be shown that $d \in \mathcal{Q}$ implies that $\Gamma^S(d)$ is positive semidefinite. The relaxation we propose to attack problem (12) is thus

$$\begin{aligned} f^S = \min_d \quad & f(d) \\ \text{s.t.} \quad & \Gamma^S(d) \geq 0, \\ & \frac{1}{4} \{ 1 + (-1)^a d_{A_x} + (-1)^b d_{B_y} + (-1)^{a+b} d_{A_x B_y} \} \\ & = p(a,b|x,y). \end{aligned} \quad (13)$$

$$\Phi(E_a^x \otimes F_b^y |\psi\rangle) = (\bar{E}_a^x \otimes \bar{F}_b^y |\bar{\psi}\rangle)_{A'B'} \otimes |junk\rangle_{AB}$$

This last problem can be formulated as a semidefinite program (SDP) [29], a type of convex optimization for which there exist efficient numerical solvers to find global minima and which also return sound error bounds on the optimal guess. A note on notation is in order: Whenever S corresponds to the set of all products of n or fewer measurement operators, we will denote the corresponding set Q^S by Q^n . It can be verified that if certain conjectures in von Neumann algebras hold [32], the sequence of sets $(Q^n)_n$ converges to Q [28].

We stress that the bound on F obtained through this method is a bound on the fidelity of the swapped state not only with respect to the target state $|\bar{\psi}\rangle$, but also with the actual state $|\psi\rangle$. Indeed, ρ_{SWAP} is obtained from $|\psi\rangle$ via a local unitary. Moreover, this bound is a lower bound in two respects: For one, the choice of S may not be optimal, i.e., there could be a better guess for the SWAP operator; for the other, the minimum is taken over a larger set of correlations than those allowed by quantum physics.

One further clarification is in order: The SDP above (13) assesses the quality of the state inside the box with respect to the reference state $|\bar{\psi}\rangle$ modulo local isometries, as opposed to local unitaries. Indeed, note that the swapped state ρ_{SWAP} depends both on the initial state ρ and on the ancillas $\rho_{A'}, \rho_{B'}$ and it could be the case that the ancillas also contribute by some amount to this fidelity. For instance, a fully mixed measured state cannot have a fidelity larger than $1/4$ with any pure state $|\bar{\psi}\rangle$; however, pure ancillas can always reach a fidelity of $1/2$. This distinction between isometries and unitaries must be taken into account for a proper physical interpretation of the magnitudes derived in this paper.

Note that whenever both the state and measurements are perfectly self-tested, however, the state can be assessed up to local unitaries as well. Indeed, the action of the SWAP operators can then only be perfect and therefore the state that is certified only comes from inside the box.

B. General construction

Here we present a constructive approach to the SWAP method, which is applicable (though not guaranteed to be optimal) to general Bell inequalities and Bell-type scenarios involving an arbitrary number of parties, inputs, and outputs.

1. Mathematical guess and convergence conditions for the SWAP method

Self-testing requires postulating an initial mathematical guess $(|\bar{\psi}\rangle, \{\bar{E}_a^x, \bar{F}_b^y\})$ on the physics behind a Bell experiment. The self-testing procedure then assesses whether the guess is (close to) correct or not. For instance, in a situation in which we wish to estimate device independently how close a state prepared in a laboratory is to the one that we intended to produce and how close the measurements performed are to the ones we wished to implement, the guessed states or measurements are simply given by the ones we intended to produce or perform. If, however, we just have access to some distributions $p(a, b|x, y)$, close to the boundary of the set of quantum correlations, and we wish to guess the state and measurements involved, the correlations $p(a, b|x, y)$ must violate some Bell inequality \mathcal{B} nearly maximally. Hence, we can apply the heuristics described in Ref. [33] to determine

the quantum state and measurement operators that maximize \mathcal{B} and take that to be our mathematical guess. Note that as long as robust self-testing is possible, the guess does not need to be exact, i.e., it is enough that $\bar{p}(a, b|x, y) = \langle \bar{\psi} | \bar{E}_a^x \otimes \bar{F}_b^y | \bar{\psi} \rangle \approx p(a, b|x, y)$.

Let us now discuss the conditions under which our method will certify that $p(a, b|x, y)$ self-tests the mathematical guess $(|\bar{\psi}\rangle, \{\bar{E}_a^x, \bar{F}_b^y\})$ in a robust way. Following the notation of [34], we say that $p(a, b|x, y)$ is a relativistic quantum distribution if there exist a state $|\psi\rangle \in \mathcal{H}$ and projection operators $\mathcal{E}_a^x, \mathcal{F}_b^y \in B(\mathcal{H})$, with $\sum_a \mathcal{E}_a^x = \sum_b \mathcal{F}_b^y = \mathbb{I}$, and $[\mathcal{E}_a^x, \mathcal{F}_b^y] = 0$, for all x, y, a, b such that $p(a, b|x, y) = \langle \psi | \mathcal{E}_a^x \mathcal{F}_b^y | \psi \rangle$. Note that the definition of relativistic quantum distributions follows from a relaxation of the tensor structure of Alice's and Bob's projection operators. Now, given $p(a, b|x, y)$, consider the following three conditions.

(i) The mathematical guess is finite dimensional ($d < \infty$).

(ii) For any sequence of relativistic quantum realization $(|\psi_N\rangle, \{\mathcal{E}_{a,N}^x, \mathcal{F}_{b,N}^y\})_N$ with $\lim_{N \rightarrow \infty} \langle \psi_N | \mathcal{E}_{a,N}^x \mathcal{F}_{b,N}^y | \psi_N \rangle = \bar{p}(a, b|x, y)$ and any polynomial Q of Alice's and Bob's measurement operators, the identity

$$\begin{aligned} \lim_{N \rightarrow \infty} \langle \psi_N | Q(\{\mathcal{E}_{a,N}^x, \mathcal{F}_{b,N}^y\}) | \psi_N \rangle \\ = \langle \bar{\psi} | Q(\{\bar{E}_a^x \otimes \mathbb{I}, \mathbb{I} \otimes \bar{F}_b^y\}) | \bar{\psi} \rangle \end{aligned} \quad (14)$$

holds.

(iii) Neither Alice's nor Bob's operators can be simultaneously block diagonalized, i.e.,

$$\bar{E}_a^x \neq \oplus_k \bar{E}_a^x(k), \quad \bar{F}_b^y \neq \oplus_\ell \bar{F}_b^y(\ell). \quad (15)$$

If the above conditions apply, then our method will return a sequence of bounds on the desired property (e.g., the fidelity with respect to a reference state), which will converge to the optimal value as the experimental data $p(a, b|x, y)$ approach $\bar{p}(a, b|x, y)$. This follows from the explicit construction of the SWAP operator given in the next section and from the convergence of the SDP hierarchies for noncommutative polynomial optimization [35].

Actually, it is generally enough that Eq. (17) hold for polynomials Q of bounded degree. For instance, in the previous section, the expression for the singlet fidelity just involved monomials of degree smaller than or equal to 8. Note also that not satisfying condition (ii) might prohibit convergence of our method and hence perfect self-testing of the desired property. However, any bound produced by our method is valid regardless of this condition.

On the other hand, if condition (iii) is dropped, then either $\{\bar{E}_a^x\}$ or $\{\bar{F}_b^y\}$ can be expressed as a direct sum of elements of the form $\mathbb{I}_{d_k} \otimes \bar{R}_k$, where \bar{R}_k denotes an irreducible representation and d_k is the degeneracy of that representation. In that case, convergence is not guaranteed in general, but it can still occur provided the magnitudes we try to estimate only concern the nontrivial parts of such a block structure.

For example, let Alice's operators be the direct sum of two nonequivalent irreducible blocks of the same dimension and let $|\bar{\psi}\rangle = |\bar{\psi}_1\rangle \oplus |\bar{\psi}_2\rangle = |0\rangle \otimes |\bar{\psi}_1\rangle + |1\rangle \otimes |\bar{\psi}_2\rangle$ be a decomposition of the state of our mathematical guess on these two blocks. Note that the mixed state

$|0\rangle\langle 0| \otimes |\bar{\psi}_1\rangle\langle \bar{\psi}_1| + |1\rangle\langle 1| \otimes |\bar{\psi}_2\rangle\langle \bar{\psi}_2|$ would give rise to the same statistics $\bar{p}(a,b|x,y)$. Hence our bounds for the fidelity $\langle \bar{\psi} | \rho | \bar{\psi} \rangle$ do not converge to 1. However, one can show that the block fidelity

$$\frac{\langle 0 | \langle \bar{\psi}_1 | \rho | 0 \rangle | \bar{\psi}_1 \rangle}{|\langle \bar{\psi}_1 | \bar{\psi}_1 \rangle|^2} + \frac{\langle 1 | \langle \bar{\psi}_2 | \rho | 1 \rangle | \bar{\psi}_2 \rangle}{|\langle \bar{\psi}_2 | \bar{\psi}_2 \rangle|^2} \quad (16)$$

still converges.¹

Note that such block fidelity allows for partial self-testing of nonextremal correlations. Thus, it could be used to demonstrate, for instance, that a rank-2 mixed state belongs to the space spanned by its two eigenvectors, even though this mixed state itself cannot be perfectly self-tested.

For our method to achieve perfect self-testing, we require that the mathematical guess be finite dimensional. Moreover, we require that the distribution $\bar{p}(a,b|x,y)$ generated by the finite-dimensional model $(|\bar{\psi}\rangle, \{\bar{E}_a^x, \bar{F}_b^y\} \subset B(\mathbb{C}^d \otimes \mathbb{C}^d))$ be such that, for any sequence of quantum distributions $[p_N(a,b|x,y) = \langle \psi_N | E_{a,N}^x \otimes F_{b,N}^y | \psi_N \rangle]_N$, with $\lim_{N \rightarrow \infty} p_N(a,b|x,y) = \bar{p}(a,b|x,y)$, there exist isometries $(W_N)_N$ satisfying

$$\begin{aligned} \lim_{N \rightarrow \infty} W_N P(\{E_{a,N}^x\}) \otimes Q(\{F_{b,N}^y\}) |\psi_N\rangle \\ = P(\{\bar{E}_a^x\}) \otimes Q(\{\bar{F}_b^y\}) |\bar{\psi}\rangle \otimes |\text{junk}\rangle \end{aligned} \quad (17)$$

for any pair of polynomials P and Q of Alice's and Bob's measurement operators. Note that, if we further demand the isometries $(W_N)_N$ to be local, this is a strengthening of the self-testing conditions (2) and (3). Then, under the assumption that Kirchberg's conjecture is true [32] [i.e., that $(Q^n)_n$ converges to Q], our method will return a sequence of bounds on the desired property (e.g., the fidelity with respect to a reference state), which will converge to the optimal value as the experimental data $p_N(a,b|x,y)$ approach $p(a,b|x,y)$.

Not satisfying condition (17) might prohibit perfect self-testing of the desired property by our method. However, any bound it produces is valid regardless of this condition.

2. Construction of a unitary SWAP operator and the SDP

Since the swaps are local, let us focus again on the construction of the SWAP operator $\mathcal{S}_{AA'}$ on Alice's side and omit the subscripts unless they are required. If both A and A' are qudits, an expression for the SWAP operator is

$$\mathcal{S}_{AA'} = TUVU, \quad (18)$$

¹To see this, consider the following swap operator: $S = |0\rangle\langle 0| \otimes S_1 + |1\rangle\langle 1| \otimes S_2$, where S_1 and S_2 are swaps between each of the blocks and an external register. Let also T be a CNOT gate that copies the information about which block is occupied into an additional flag register. Applying both S and T to the case in which the measured state is either $|\bar{\psi}_1\rangle \oplus |\bar{\psi}_2\rangle$ or $|0\rangle\langle 0| \otimes |\bar{\psi}_1\rangle\langle \bar{\psi}_1| + |1\rangle\langle 1| \otimes |\bar{\psi}_2\rangle\langle \bar{\psi}_2|$ results in external registers being left in the state $\rho = |0\rangle\langle 0| \otimes |\bar{\psi}_1\rangle\langle \bar{\psi}_1| + |1\rangle\langle 1| \otimes |\bar{\psi}_2\rangle\langle \bar{\psi}_2|$, which has a block fidelity of 1. The fact that both S and T follow the block structure guarantees, by the Artin-Wedernburn lemma [36], that they can be obtained as polynomials of the measurement operators, as required.

with

$$\begin{aligned} T &= \mathbb{I} \otimes \sum_{k=0}^{d-1} |-k\rangle\langle k|, \\ U &= \sum_{k=0}^{d-1} P^k \otimes |k\rangle\langle k|, \\ V &= \sum_{k=0}^{d-1} |k\rangle\langle k| \otimes P^{-k}, \end{aligned} \quad (19)$$

where

$$P = \sum_{k=0}^{d-1} |k+1\rangle\langle k| \quad (20)$$

and additions inside kets are modulo d . As before, the idea of the construction consists in mimicking these operators.

We can assume that the algebra generated by the $\{\bar{E}_a^x\}$ is irreducible, i.e., that condition (15) holds (the case of many irreducible representations can be treated similarly). By the Artin-Wedernburn theorem [36], any matrix in $\mathbb{C}^d \times \mathbb{C}^d$ on Alice's side is thus an element of the algebra generated by the $\{\bar{E}_a^x\}$. In particular, the operator P in Eq. (20) can be expressed as a linear combination $P(\bar{E}_a^x)$ of products of Alice's projector operators.

However, contrary to the case of qubits, if in this expression the guesses $\{\bar{E}_a^x\}$ are replaced by arbitrary measurement operators $\{E_a^x\}$, the resulting operator $P(E_a^x)$ need not be unitary in general. Still, by the polar decomposition [36], there always exist a unitary² \hat{P} such that

$$\hat{P}^\dagger P(E_a^x) \geq 0. \quad (21)$$

Moreover, it is guaranteed that $\hat{P} = P(E_a^x)$ whenever the right-hand side operator is itself unitary.

Similarly, the projectors $\{|k\rangle\langle k|\}_{k=0}^{d-1}$ on system A in Eq. (20) can be replaced by $\{E_k^0\}_k$, provided there are d such projectors and the $\{\bar{E}_k^0\}_{k=0}^{d-1}$ are rank-1. If one or several of the projectors in Alice's measurement model are degenerate, then we must break the degeneracy via the addition of new noncommuting variables. For instance, suppose that \bar{E}_k^0 has rank n_k . Then we must find a self-adjoint element $X_k(\bar{E}_a^x)$ of Alice's algebra of observables such that $\bar{E}_k^0 X_k(\bar{E}_a^x) \bar{E}_k^0 = \sum_{s=1}^{n_k} \lambda_{k,s} |k_s\rangle\langle k_s|$ has n_k different eigenvalues $\lambda_{k,1} > \lambda_{k,2} > \dots > \lambda_{k,n_k}$. Again, this is always possible by virtue of the Artin-Wedernburn theorem [36]. Now we introduce n new noncommuting variables $\{E_{k,j}^0\}_{j=1}^{n_k}$, which will play the role of $\{|k_j\rangle\langle k_j|\}_{j=1}^{n_k}$. These

²Technically, there always exist an isometry with the said property. However, any isometry $V \in B(\mathcal{H})$ in infinite dimensions can be viewed as a unitary operator in $\mathcal{H} \otimes \mathbb{C}^2$. Indeed, let $V^\dagger V = \mathbb{I}$ and define $U = (\mathbb{I} - VV^\dagger) \otimes |0\rangle\langle 1| + V^\dagger \otimes |1\rangle\langle 1| + V \otimes |0\rangle\langle 0|$. Then $UU^\dagger = U^\dagger U = \mathbb{I}$ and $U|\psi\rangle|0\rangle = (V|\psi\rangle)|0\rangle$. At the level of the moment matrices, we can thus assume that such isometries are unitaries.

variables must satisfy

$$\begin{aligned} E_{k,j}^0 E_{k,l}^0 &= \delta_{j,l} E_{k,j}^0, \quad \sum_{j=1}^{n_k} E_{k,j}^0 = E_k^0, \quad [E_{k,j}^0, E_k^0 X_k E_k^0] = 0, \\ \frac{1}{2}(\lambda_{k,j} + \lambda_{k,j+1}) E_{k,j}^0 &\geq E_k^0 X_k (E_a^x) E_{k,j}^0, \quad j = 1, \dots, n_k - 1 \\ E_k^0 X_k (E_a^x) E_{k,j}^0 &\geq \frac{1}{2}(\lambda_{k,j-1} + \lambda_{k,j}) E_{k,j}^0, \quad j = 2, \dots, n_k. \end{aligned} \quad (22)$$

As with \hat{P} , the existence of the projectors $\{E_{k,j}^0\}$ does not impose extra conditions and can always be taken for granted.

Now we can collect all the elements of the construction of the SWAP operator on Alice's side:

- (i) Guess the operators \bar{E}_a^x .
- (ii) Construct P given in Eq. (20) as linear combinations of products of the \bar{E}_a^x . Similarly, for each degenerate projector E_k^0 , find $X_k(\bar{E}_a^x)$ such that $\bar{E}_k^0 X_k(\bar{E}_a^x) \bar{E}_k^0$ is nondegenerate in the support of \bar{E}_k^0 .
- (iii) Formally replace \bar{E}_a^x by the unknown E_a^x in those expressions to obtain the expressions of $P(E_a^x)$ and $X_k(E_a^x)$ (if needed).
- (iv) Define the SWAP operator as (18), in which U and V are given by the expressions (20) with $|k\rangle\langle k|$ replaced by E_k^0 or $E_{k,j}^0$ and P replaced by \hat{P} (on the original system). These otherwise undefined operators are constrained in terms of the E_a^x by (21) and (22).

The inclusion of $\hat{P}_A, \hat{P}_B, E_{k,j}^0$ in the moment matrix, together with the extra semidefinite constraints (21) and (22), is known as the technique of localizing matrices [35]. We review it here.

Let $g = \sum_u g_u u$ be a polynomial of Alice's and Bob's measurement operators (with the u being operator products) and let d be a moment vector. Then the localizing matrix $\Gamma^S(g, d)$ is a matrix whose rows and columns are numbered by elements of the set of products S and such that $\Gamma_{s,t}^S(g, d) = \sum_u g_u d_{s^\dagger u t}$. It can be verified that if d is such that it admits a quantum representation where the polynomial g is a non-negative operator, then $\Gamma_{s,t}^S(g, d)$ must be positive semidefinite.

In our scenario, we must guarantee that the optimization is done over all quantum representations such that (21) and (22) hold. Such constraints hence translate to

$$\Gamma^{S'}(\hat{P}_A^\dagger P_A(E_a^x), d) \geq 0, \quad \Gamma^{S'}(\hat{P}_B^\dagger P_B(F_b^y), d) \geq 0, \quad (23)$$

plus the constraints associated with conditions (22). Here S' is chosen as big as possible, but such that all entries of the localizing matrices can be written as linear combinations of moment vectors defined over SS^\dagger . Note that requiring $\Gamma^{S'}(\hat{P}_A^\dagger P_A(E_a^x))$ to be positive also implies that it must be Hermitian. The semidefinite program to place a lower bound on the fidelity of the swapped state with respect to the reference state $|\bar{\psi}\rangle$ is then

$$\begin{aligned} f^S &= \min \quad \langle \bar{\psi} | \rho_{\text{SWAP}}(d) | \bar{\psi} \rangle \\ \text{s.t.} \quad &\Gamma^S(d) \geq 0, \\ &d_{E_a^x F_b^y} = p(a, b|x, y), \quad \Gamma^{S'}(\hat{P}_A^\dagger P_A(E_a^x), d) \geq 0, \\ &\Gamma^{S'}(\hat{P}_B^\dagger P_B(F_b^y), d) \geq 0, \end{aligned} \quad (24)$$

plus extra constraints in the case that a subset of the \bar{E}_k^0 (\bar{F}_k^0) is degenerate. Note that whenever the reference state and measurements are chosen real, it is sufficient to perform this optimization over real SDP matrices because the objective function is a combination of moments with real coefficients.

C. Finite-size fluctuations beyond the assumption of independent and identical distribution

All the previous discussion implicitly assumed that the behavior of the devices is the same in each run and is uncorrelated among the runs, i.e. satisfy the assumption of i.i.d.. Moreover, we presented the case for infinitely many runs of the experiment such that $p(a, b|x, y)$ can be estimated exactly. In this section we remove both assumptions by presenting a finite-size analysis inspired by [37]. As one of the outcomes, we prove that the asymptotic bounds can be computed under the assumption of independent and identical distribution without loss of generality.

Suppose that Alice and Bob have sequentially distributed pairs of black boxes. We allow for the possibility that different pairs of boxes exhibit different statistics, which can in turn depend on Alice's and Bob's past measurement history. Now let g be a function of the underlying state and measurement operators in each realization for which the SWAP tool, or any other method, establishes that $g(|\psi\rangle, E_a^x, F_b^y) > g^*$ for some g^* whenever the violation of a specific Bell inequality \mathcal{B} via independent and identically distributed pairs is greater than V_0 . Then, given a Bell violation $V > V_0$ obtained with nonindependent and identically distributed boxes, we wish to disprove the following hypothesis.

Hypothesis Φ . All the distributed pairs contain quantum states and operators $(|\psi\rangle, E_a^x, F_b^y)$ such that $g(|\psi\rangle, E_a^x, F_b^y) \leq g^*$.

To do this, the idea is to define a statistical parameter T that both parties can estimate during the course of the experiment and such that $P(T > 1/\delta | \Phi) < \delta$. If the observed value t is such that $t > 1/\delta_0$ for some threshold δ_0 , the parties can conclude that hypothesis Φ is not likely to be true. Let us construct this parameter T .

Let $\Psi \equiv (\bar{\psi}, \bar{E}_a^x, \bar{F}_b^y)$ be a particular quantum model with \mathcal{B} violation $V > V_0$. Under the assumption that Alice and Bob can choose their measurement settings x, y randomly and independently of their boxes, any Bell inequality \mathcal{B} can be written as $\langle B(a, b, x, y) \rangle \leq V_0$, with $B(a, b, x, y)$ being an arbitrary real function of the inputs and outputs of the problem that will depend on Alice's and Bob's distribution $p(x)p(y)$ of the inputs.

Let $|B(a, b, x, y)| \leq K$ for all inputs and outputs. Following the lines of [37], we define the normalized form of $B(a, b, x, y)$ as $\tilde{B}(a, b, x, y) \equiv \frac{B(a, b, x, y) + K}{V_0 + K}$. Clearly, $\langle \tilde{B}(a, b, x, y) \rangle_\Psi > 1$ and $\tilde{B}(a, b, x, y) \geq 0$ for all x, y, a, b . Also, $\langle \tilde{B}(a, b, x, y) \rangle \leq 1$ for any pair of boxes satisfying hypothesis Φ .

Next choose $0 < \epsilon < 1$ such that

$$R(a, b, x, y) \equiv (1 - \epsilon) + \epsilon \tilde{B}(a, b, x, y) \quad (25)$$

satisfies

$$\langle \ln[R(a, b, x, y)] \rangle_\Psi > 0. \quad (26)$$

That such an ϵ exists follows from the observation that, for $\epsilon \ll 1$,

$$\langle \ln[1 - \epsilon + \epsilon \tilde{B}(a, b, x, y)] \rangle_\Psi \approx \epsilon \langle [\tilde{B}(a, b, x, y) - 1] \rangle_\Psi > 0. \quad (27)$$

Note that, by construction, $\langle R(a, b, x, y) \rangle \leq 1$ under hypothesis Φ .

Now suppose that Alice and Bob conduct the Bell experiment n times, choosing their inputs x, y with probability $p(x)p(y)$ each time, thus obtaining the experimental data $\{a_k, b_k, x_k, y_k\}_{k=1}^n$. Define the positive random variable $T \equiv \prod_{k=1}^n R_k$, with $R_k \equiv R(a_k, b_k, x_k, y_k)$. Under hypothesis Φ , it can be seen that $\langle T \rangle \leq 1$ [37] and so, by Markov's inequality, $P(T \geq \delta) \leq 1/\delta$.

However, in the event that Alice and Bob are actually being distributed n independent copies of box Ψ , by the central limit theorem, the random variable $X \equiv \ln(T) = \sum_{k=1}^n \ln(R_k)$ is expected to take values in the range $n\langle \ln(R) \rangle_\Psi \pm O(\sqrt{n})$. From Eq. (26) we thus have that, with very high probability, T will grow exponentially with n . In a few experiments, Alice and Bob will hence observe a ridiculously high value of T and therefore conclude that hypothesis Φ must be abandoned.

A rough estimate on the probability of (wrongly) accepting hypothesis Φ when n independent copies of Ψ are actually distributed can be established via Chebyshev's inequality, which states that for any random variable Z , $P(|Z - \langle Z \rangle| \geq \epsilon) \leq \frac{\langle Z^2 \rangle - \langle Z \rangle^2}{\epsilon^2}$. Let $\delta_0 > 0$ define the criterion used to reject hypothesis Φ , i.e., Alice and Bob will reject Φ if and only if $T > 1/\delta_0$. Suppose also that n is large enough to guarantee that $\langle X \rangle_\Psi = n\langle \ln(R) \rangle_\Psi \geq \ln(\delta_0^{-1})$. Then the probability $P(T \leq \delta_0^{-1})$ that Φ is accepted satisfies

$$\begin{aligned} P(T \leq \delta_0^{-1}) &= P(\langle X \rangle - X \geq \langle X \rangle - \ln(\delta_0^{-1})) \\ &\leq P(|\langle X \rangle - X| \geq |\langle X \rangle - \ln(\delta_0^{-1})|) \\ &\leq \frac{\langle \ln^2(R) \rangle_\Psi - \langle \ln(R) \rangle_\Psi^2}{n[\langle \ln(R) \rangle_\Psi - \ln(\delta_0^{-1})/n]^2}, \end{aligned} \quad (28)$$

which tends to zero as $O(1/n)$.

In order to reject hypotheses such as the singlet fidelity of the state inside the boxes is smaller than f^* for each realization, it is thus enough to estimate the maximal Bell violation \mathcal{B} compatible with fidelity f^* in the independent and identically distributed case. The method so far described, though, is based on the estimation of the violation of a single Bell inequality. One could ask what happens, then, when we consider additional parameters in our independent and identically distributed analysis, such as the whole probability distribution $p(a, b|x, y)$. As we will see below, the minimum singlet fidelity for a given CHSH violation substantially increases when the experimental distribution is isotropic (see Sec. IV A for details).

In fact, one can show, following an argument similar to that presented in Refs. [38,39], that such improved bounds can be demonstrated by monitoring some other Bell inequality \mathcal{B}' , described by the dual of our SDP program (24). One can thus also consider these improved bounds in the presence of

finite statistics by applying the analysis above to the new Bell inequality \mathcal{B}' .³

Note that ruling out hypothesis Φ guarantees that at least one of the pairs is of the desired kind, i.e., has $g > g^*$. In a case where n runs have taken place, one might want to guarantee that at least a significant fraction of these n runs satisfy $g > g^*$. We leave this general question open for further study. In the special case where the finite statistics experiment was realized with independent and identically distributed boxes, however, our argument already guarantees that with large probability all boxes are of good quality. In view of these reflections, in the rest of the article we will always work in the asymptotic case of infinitely many runs and the independent and identically distributed behavior of the boxes will be taken for granted.

IV. MORE ROBUST BOUNDS FOR KNOWN SELF-TESTING SCENARIOS

The remainder of the paper is devoted to discussing several explicit examples of self-testing. We start with examples that are already known in the literature to have robust self-testing and show how our method obtains much stronger bounds.

A. Singlet fidelity from the CHSH inequality

The first reported example of self-testing, though it was not called that, is that the maximal violation of the CHSH inequality self-tests the maximally entangled state of two qubits [16,17]. The CHSH expression is

$$\mathcal{I}_{\text{CHSH}} = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle. \quad (29)$$

For simplicity of notation, we work with a guessed ideal case in which both Alice's and Bob's observables are the same, i.e.,

$$\bar{A}_0 = \bar{B}_0 = \sigma_z, \quad \bar{A}_1 = \bar{B}_1 = \sigma_x. \quad (30)$$

This requires writing the maximally entangled two-qubit state as

$$|\bar{\Psi}\rangle = \cos\left(\frac{\pi}{8}\right)|\Phi^-\rangle + \sin\left(\frac{\pi}{8}\right)|\Psi^+\rangle. \quad (31)$$

Having set this, we choose the initial states of the ancilla qubits to be $|0\rangle_{A'}$ and $|0\rangle_{B'}$ and then go through the procedure described in Sec. III A without modification to obtain after

³In practice, the whole distribution $p(a, b|x, y)$ is generally not accessible. Rather, frequencies $f(a, b|x, y)$ can be observed. One may thus be tempted to use these frequencies in place of the distribution p itself in order to guess the new Bell inequality \mathcal{B}' . These frequencies, however, typically do not satisfy the no-signaling condition and thus do not belong to any level of the NPA relaxation. Therefore, they cannot be set as constraints in our SDP program. One should thus not apply the SDP to the observed frequencies directly, but rather to some quantum point p chosen reasonably close to f (if no quantum point is statistically close to f , then the validity of the experiment may be questioned). The bound obtained with the inequality found in this way will be valid independently of how the frequencies were approximated.

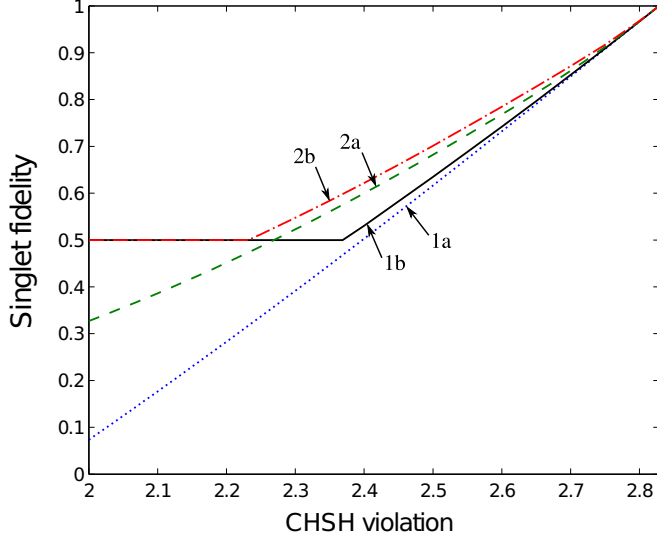


FIG. 2. (Color online) Minimal singlet fidelity as a function of CHSH violation. Curves 1 (2) correspond to lower bounds on the fidelity for generic (isotropic) boxes. Curves a (b) were obtained with the unmodified (improved) SWAP operator.

some algebra

$$\begin{aligned}
 F = & \frac{1}{2} + \frac{1}{2\sqrt{2}}\mathcal{I}_{\text{CHSH}} - \frac{1}{8}[\langle A_0, A_1 | [B_0, B_1] \rangle \\
 & + \frac{1}{8\sqrt{2}}[3\langle A_1 B_1 \rangle - 2\langle A_0 B_1 \rangle - 2\langle A_1 B_0 \rangle \\
 & + \langle A_0 A_1 A_0 (B_1 - 2B_0) \rangle \\
 & + (\langle A_1 - 2A_0 \rangle B_0 B_1 B_0) - \langle A_0 A_1 A_0 B_0 B_1 B_0 \rangle]. \quad (32)
 \end{aligned}$$

It is presently not difficult to check, with the tools used in the proof of the Tsirelson bound, that $F = 1$ indeed if $\mathcal{I}_{\text{CHSH}} = 2\sqrt{2}$.⁴ Our goal, however, is to go beyond the ideal case and obtain a lower bound on F via the SDP.

The constraint can be the value of $\mathcal{I}_{\text{CHSH}}$ alone or all the statistics $p(a, b|x, y)$ collected during the experiment. The second case takes advantage of more information than the first one and thus provides a better bound. This is illustrated by curves 1a and 2a in Fig. 2.

As mentioned previously, there is no guarantee that the SWAP operator we used [defined by Eqs. (4) and (8)] is optimal. In fact, we have found better bounds by tweaking the standard method in two ways. First, we consider SWAP operators that depend on the Bell violation. The first dependence we consider consists in using the dichotomic operator A_2 satisfying

$$A_2\{\cos[\zeta_A(V)]A_0 + \sin[\zeta_A(V)]A_1\} \geq 0, \quad (33)$$

where $\zeta_A(V)$ is an arbitrary function of the CHSH violation V , as Alice's logical NOT operator. For $V = 2\sqrt{2}$ choosing

⁴Looking for the eigenvalues of the square of the CHSH operator, one finds that $\mathcal{I}_{\text{CHSH}} = 2\sqrt{2}$ can only be obtained if $\langle [A_0, A_1][B_0, B_1] \rangle = -4$. Together with the unitarity of the operators, this implies that $A_0 A_1 = -A_1 A_0$, i.e., $A_0 A_1 A_0 = -A_1$, and the same for Bob. By replacing all these results in Eq. (32), one finds $F = 1$.

$\zeta_A(V) = \pi/2$ allows one to recover $A_2 = A_1$ so that the NOT operator returns the correct SWAP operator in the case of maximal CHSH violation. Similarly, we can parametrize an auxiliary operator for Bob by a function $\zeta_B(V)$.

The intuition behind this SWAP ansatz is that, even though Alice and Bob are preparing the maximally entangled state, their measurement devices are somehow tilted, thus explaining why they do not achieve the optimal CHSH value. The resulting fidelity will have the same expression as in Eq. (32), but with A_1, B_1 replaced by A_2, B_2 .

We introduce a second parameter in the SWAP operator by considering combinations of UVU with the identity, i.e., we define

$$\mathcal{S}_{AA'} = \cos \xi_A \mathbb{1} + i \sin \xi_A UVU \quad (34)$$

and similarly for Bob. For every value of ξ_A , $\mathcal{S}_{AA'}$ is still a unitary operator and setting $\xi_A = \pi/2$ recovers the previous choice of SWAP operator.

The second tweak that we apply on the standard SWAP method takes advantage of the fact that since we are only interested in certifying the quality of the measured state up to local isometries, it is sufficient to place a lower bound on its fidelity with respect to any reference state of the form

$$|\psi_{ME}\rangle = W_A \otimes W_B |\bar{\psi}\rangle, \quad (35)$$

where W_A and W_B are arbitrary single-qubit unitaries.

Altogether, we thus looked for parameters $\zeta_A, \zeta_B, \xi_A, \xi_B$ and unitaries W_A, W_B that could improve the bounds 1a and 2a in Fig. 2. The result of this optimization is shown in the same figure with curves 1b and 2b.

The new curves display a different behavior in two regions. When $\mathcal{I}_{\text{CHSH}} \gtrsim 2.37$ (or $\mathcal{I}_{\text{CHSH}} \gtrsim 2.23$ in the isotropic case), an appropriate choice of $\zeta_A, \zeta_B, W_A, W_B$ together with $\xi_A = \xi_B = \pi/2$ results in an improved bound on the fidelity compared to the standard SWAP procedure. For lower CHSH violations, however, the best choice of SWAP operator is obtained with $\xi_A = \xi_B = 0$, resulting in a singlet fidelity of $1/2$. This value is thus obtained by comparing the ancilla rather than the state inside the box to the singlet (or equivalently by considering the local isometry that maps every local Hilbert space to the pure state $|0\rangle$). It thus corresponds to a trivial singlet fidelity, which can be certified up to local isometries regardless of the measured state. Clearly, any self-testing performed up to local isometries admits a trivial fidelity bound of this kind.

One can check that the curve 1a can be saturated by some two-qubit states and measurements when the standard SWAP operation (4) and (8) and reference state $|\bar{\psi}\rangle$ are used. This bound is thus tight under this condition. Therefore, a modification of the SWAP procedure was necessary to improve this bound. It would be interesting to see if the improved bounds can be improved further or if they are close to optimal.

The fact that the bounds obtained in the isotropic and generic cases differ in the first region suggests that the CHSH inequality is not optimal to place a bound on the singlet fidelity of singlets subject to uniform noise. Upon examination of the dual of our SDP, we find that a better Bell expression to consider is of the form

$$I_{\alpha, \beta} = \alpha \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \beta \langle A_1 B_1 \rangle, \quad (36)$$

where $\alpha, \beta > 0$ are parameters that depend on the quality of the statistics. Note that an inequality of the same form, but with different values for the coefficients α, β , was also shown to be relevant for randomness certification in the presence of a Werner state [38,40].

Comparison with previous bounds on the singlet fidelity from the CHSH violation

Previous to this work, most self-testing bounds were given in terms of the norm of the difference between the desired state $|\bar{\psi}\rangle_{A'B'} \otimes |\text{junk}\rangle_{AB}$ and the actual one after the isometry $|\psi\rangle_{A'B'AB}$, i.e., in the form

$$|||\psi\rangle - |\bar{\psi}\rangle \otimes |\text{junk}\rangle|| \leq t. \quad (37)$$

As a consequence,

$$t^2 \geq 2 - 2s,$$

where the scalar product $s = \langle \psi | \bar{\psi} \otimes \text{junk} \rangle$ can be taken as real and positive since everything is defined up to a local unitary, so in particular it is possible to add a suitable global phase.

In this paper we work with the singlet fidelity evaluated on the swapped state, i.e., $F = \langle \bar{\psi} | \rho_{\text{SWAP}} | \bar{\psi} \rangle$. In Appendix A we show that both quantities are related through

$$s^2 \geq 2F - 1. \quad (38)$$

For a CHSH violation of $2\sqrt{2} - \epsilon$, curve 1b in Fig. 2 gives a lower bound of approximately $F \gtrsim 1 - 1.1\epsilon$. We thus have that

$$\begin{aligned} |||\psi\rangle - |\bar{\psi}\rangle \otimes |\text{junk}\rangle||^2 &= 2(1 - s) \\ &\leq 2 - 2\sqrt{2F - 1} \\ &\lesssim 2.2\epsilon. \end{aligned} \quad (39)$$

In the work of McKague *et al.* [22], the values of t are given explicitly by replacing ϵ_1 and ϵ_2 with the values given in Theorem 2 by Clauser, Horne, Shimony, and Holt and in Theorem 3 by Mayers and Yao, which gives

$$|||\psi\rangle - |\bar{\psi}\rangle \otimes |\text{junk}\rangle||^2 \lesssim 100\sqrt{\epsilon}. \quad (40)$$

Note that this bound is not linear in ϵ and thus seems harder to compare with (39). However, one can see that this bound quickly becomes trivial. Indeed, already for $\epsilon \simeq 2.2 \times 10^{-5}$, it yields a distance larger than $2 - \sqrt{2}$, the distance between the singlet state and a product state.

In the work of Reichardt *et al.* [24], the bounds are not explicitly given, but can be reconstructed. The relevant result for comparison with our work is Lemma 4.2 in the long version [41], which refers to the single CHSH game (i.e., before the extension to parallel repetition that constitutes the main result of their work). Using their notation,

$$\begin{aligned} |||\bar{\psi}\rangle - |\psi^*\rangle \otimes |\psi^\times\rangle||^2 &= \sum_{c,i,j} ||\psi_{cij}||^2 ||\tilde{\psi}_{cij} - e^{i\phi_{cij}} |\psi^*\rangle||^2 \\ &\stackrel{(*)}{\leq} 72284 \sum_{c,i,j} ||\psi_{cij}||^2 \beta_{ij} \stackrel{(**)}{\lesssim} 10^5 \epsilon, \end{aligned} \quad (41)$$

where $(*)$ is from the end of proof of Proposition 4.5 and $(**)$ is from Eq. (4.4), using $72284 * \sqrt{2} \approx 10^5$.

We see that our results are orders of magnitude better than the best previous results in the literature. Note also that no other results allow us to establish a nontrivial bound for the singlet fidelity in the best CHSH experiment realized so far [42]. Curve 1b in Fig. 2, on the other hand, allows one to certify a singlet fidelity greater than 99%.

B. Singlet fidelity from Mayers and Yao

The work of Mayers and Yao, where the term “self-testing” was first used, reported another criterion to self-test the maximally entangled state of two qubits. This time $|\bar{\psi}\rangle = |\Phi^+\rangle$ and the measurements are the same as (30), but there is a third setting on Alice’s side, ideally

$$\bar{A}_2 = \frac{\sigma_z + \sigma_x}{\sqrt{2}}. \quad (42)$$

The ideal Mayers-Yao statistics, which self-tests $|\Phi^+\rangle$ with $F = 1$, are given by

$$\begin{aligned} \langle A_0 B_0 \rangle &= \langle A_1 B_1 \rangle = 1, \\ \langle A_0 B_1 \rangle &= \langle A_1 B_0 \rangle = 0, \\ \langle A_2 B_0 \rangle &= \langle A_2 B_1 \rangle = \frac{1}{\sqrt{2}}. \end{aligned} \quad (43)$$

As for the CHSH example, we can just use the SWAP operator defined by (4) and (8) to obtain

$$\begin{aligned} F &= \frac{1}{4}(1 + \langle A_0 B_0 \rangle) \\ &\quad + \frac{1}{16} \{ \langle [A_0, A_1][B_0, B_1] \rangle \\ &\quad + \langle (A_1 - A_0 A_1 A_0)(B_1 - B_0 B_1 B_0) \rangle \}. \end{aligned} \quad (44)$$

Notice that the setting A_2 does not appear in the construction of the SWAP operator or consequently in F , but it fulfills the crucial role of inducing constraints on higher moments of A_0, A_1, B_0, B_1 in the SDP matrix.

For definiteness, we study the robustness of a mixture of ideal Mayers-Yao statistics (weight v) with white noise (weight $1 - v$), that is, the statistics are given by the correlations (43) multiplied each by v . These are the correlations expected from using the prescribed measurements on a Werner state $\rho_W = v|\Phi^+\rangle\langle\Phi^+| + (1 - v)\mathbb{1}/4$ with visibility v .

Figure 3 shows the bound on the fidelity that we are able to certify from a direct application of our method for different values of v . We compare it to the analogous bound obtained from the CHSH violation achievable by the state and the actual fidelity of the Werner state. None of the lower bounds come close to the actual fidelity, thus suggesting that different measurements are necessary to optimally bound the singlet fidelity of Werner states in a device-independent manner.

C. Complementary qubit measurements from the CHSH violation

Suppose that, rather than verifying that $|\psi\rangle$ is close to $|\bar{\psi}\rangle$, we are interested in certifying to what degree Bob’s input y is able to switch between the qubit dichotomic measurements σ_z, σ_x . For that, we envision a virtual experiment in which we hand Bob a trusted qubit in a state $|\varphi\rangle$ unknown to him. We let Bob turn on an interaction between the trusted system and his box and only then we

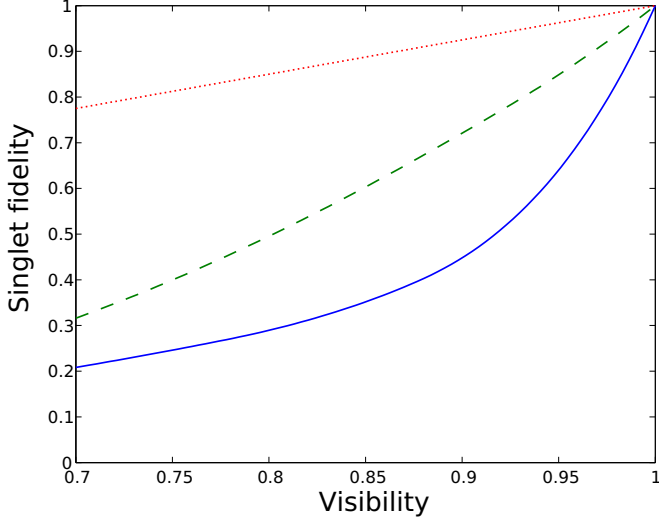


FIG. 3. (Color online) Lower bounds on the singlet fidelity of Werner states certified by the Mayers-Yao test (solid line). Same bound as certified by the CHSH test is reported here from Fig. 2 for comparison (dashed line). The dotted line is the actual fidelity of the Werner state itself.

tell Bob which symbol $y = 0, 1$ to input. If the resulting statistics $P(b|y, |\varphi\rangle)$ satisfy $P(b|0, |\varphi\rangle) = \langle \varphi | \frac{\mathbb{I} + (-1)^b \sigma_z}{2} | \varphi \rangle$ and $P(b|1, |\varphi\rangle) = \langle \varphi | \frac{\mathbb{I} + (-1)^b \sigma_x}{2} | \varphi \rangle$, we conclude that Bob's input indeed allows him to switch between the Pauli measurements σ_z, σ_x .

Considering that Bob uses the SWAP operator specified in Eqs. (4) and (8) as an interaction between the state $|\varphi\rangle$ and his box, he will observe outcome b , when later performing measurement y , with probability

$$P(b|y, |\varphi\rangle) = \text{tr}(M_b^y S \rho_{AB} \otimes |\varphi\rangle_{B'} \langle \varphi| S^\dagger), \quad (45)$$

where S is given by Eq. (9). To quantify the hypothesis $B_0 = \sigma_z, B_1 = \sigma_x$, we define the figure of merit

$$\tau \equiv \frac{1}{2} \{ P(0|0, |0\rangle) + P(1|0, |1\rangle) + P(0|1, |+\rangle) + P(1|1, |-\rangle) \} - 1, \quad (46)$$

which compares statistics obtained when using different states for the ancillas. Here τ is a number ranging from -1 to $+1$ and $\tau = 1$ is achievable only in the ideal case. As before, $P(b|y, |\varphi\rangle)$ depends linearly on the moment vector c . For example,

$$P(0|0, |0\rangle) = \langle \psi | \left(\frac{\mathbb{I} + B_0}{2} \right) | \psi \rangle + \langle \psi | \left(\frac{\mathbb{I} - B_0}{2} \right) \times B_1 \left(\frac{\mathbb{I} + B_0}{2} \right) B_1 \left(\frac{\mathbb{I} - B_0}{2} \right) | \psi \rangle. \quad (47)$$

Consequently, $\tau = \tau(d)$ and so a lower bound on this quantity can be estimated with an SDP for measurements that are compatible with some Bell violation. The result of this computation for the case of measurements leading to some

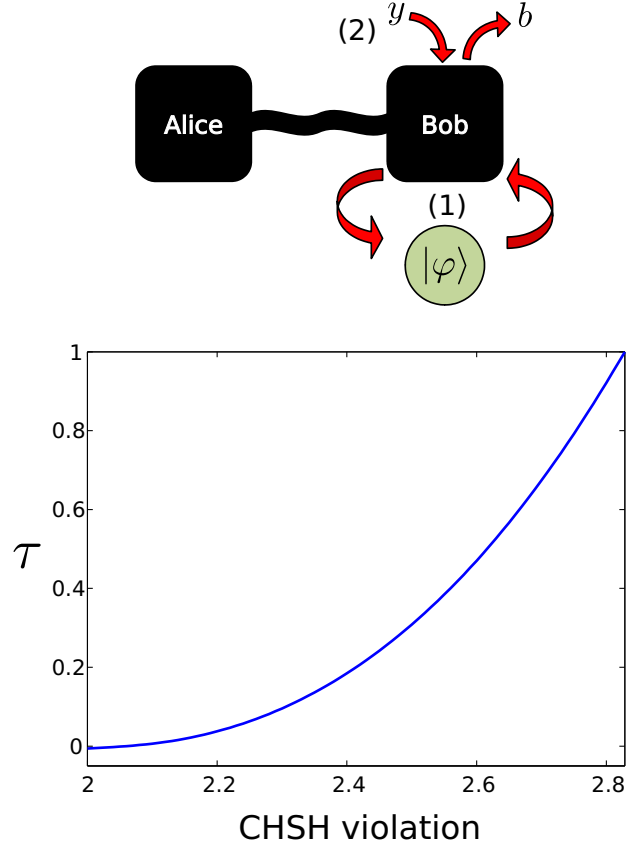


FIG. 4. (Color online) Estimation of Bob's measurements. The protocol works in two steps. (1) We implement a full SWAP of Bob's box and his trusted qubit, which we prepare in state $|\varphi\rangle$. (2) We implement measurement B_y and study the resulting statistics.

CHSH violation is shown in Fig. 4, where τ indeed tends to 1 as the CHSH parameter gets closer to $2\sqrt{2}$.

D. Fidelity of partially entangled two-qubit pure states

In Secs. IV A and IV B we have used quantum nonlocality to certify how close Alice's and Bob's state $|\psi\rangle$ is to a maximally entangled qubit pair. Here we show how our method can be used to certify nonmaximally entangled qubit pairs as well. This problem was first considered in Ref. [25], where an analytic estimate on the state fidelity was obtained. Here, using the SWAP concept, we derive a much better bound.

The scenario is similar to that used above to self-test the singlet state. The only difference is that we will use a tilted CHSH inequality of the form

$$\mathcal{B}_\alpha = \alpha \langle A_0 \rangle + \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle, \quad (48)$$

where $0 \leq \alpha \leq 2$. The maximum quantum violation of this inequality [43] is given by $\sqrt{8 + 2\alpha^2}$ and the corresponding optimal qubit strategy is

$$\begin{aligned} \bar{A}_0 &= \sigma_z, & \bar{A}_1 &= \sigma_x, \\ \bar{B}_0 &= \cos \mu \sigma_z + \sin \mu \sigma_x, \\ \bar{B}_1 &= \cos \mu \sigma_z - \sin \mu \sigma_x, \\ |\bar{\psi}\rangle &= \cos \theta |00\rangle + \sin \theta |11\rangle, \end{aligned} \quad (49)$$

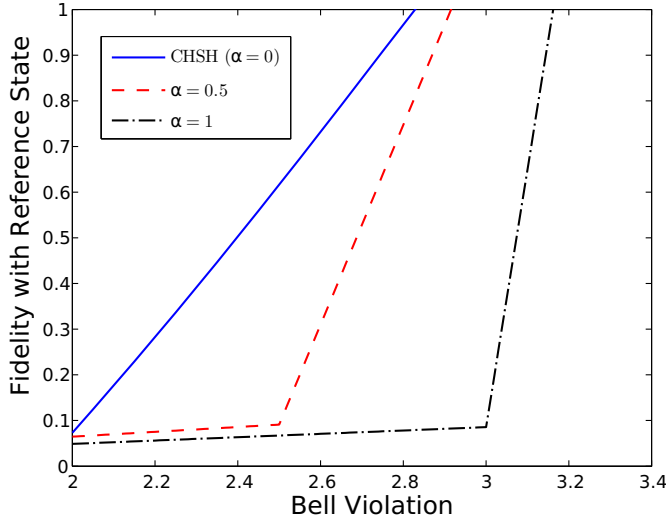


FIG. 5. (Color online) The solid line refers to the standard CHSH case, which obviously recovers the line in Fig. 2. The dashed line refers to the case when $\alpha = 0.5$ and the local bound is 2.5, explaining the discontinuity. The dot-dashed line refers to the case when $\alpha = 1$ and the local bound is 3.

where $\sin 2\theta = \sqrt{(1 - \alpha^2/4)/(1 + \alpha^2/4)}$ and $\tan \mu = \sin 2\theta$. Thus, we can use the appropriate inequality with the corresponding value of α to device-independently certify a reference state of the form $|\bar{\psi}\rangle = \cos \theta |00\rangle + \sin \theta |11\rangle$. The details on the construction of the SWAP operator are similar to those in Sec. IV A and can be found in Appendix B.

Figure 5 shows a plot of the minimal fidelity with $|\bar{\psi}\rangle$ for different values of α and different Bell inequality violations. The curves are approximately linear, between the local bound and maximum quantum bound. Since the local and quantum bound coincide at $\alpha = 2$, the line gets steeper. This is expected because, as α increases, the range of tolerable error gets smaller. However, it is interesting to note that the robustness is always close to linear for the three cases.

V. OTHER ROBUST SELF-TESTING SCENARIOS

A. Fidelity of a pure two-qutrit state from the Collins-Gisin-Linden-Massar-Popescu inequality

So far, our studied cases concern scenarios where Alice and Bob each have two inputs and two outputs and they want to certify their state against an entangled pair of qubits. In this section we illustrate how to extend these ideas to higher-dimensional scenarios. It is unclear how one can generalize the methods sketched in Refs. [22,24,25] for such a purpose. However, using the SWAP method above, it is easy to do so.

The relevant Bell inequality for this case is the CGLMP inequality [44]; it requires two measurement settings on each side, with three measurement outcomes. The inequality reads

$$\begin{aligned} \mathcal{B}_{\text{CGLMP}}(p) = & p(a < b | x = 1, y = 1) \\ & + p(a > b | x = 0, y = 1) \\ & + p(a \geq b | x = 1, y = 0) \\ & + p(a < b | x = 0, y = 0) \geq 1. \end{aligned} \quad (50)$$

The maximum quantum violation is conjectured [45] and verified numerically [27] to be $\mathcal{B}_{\text{CGLMP}}(p) = (12 - \sqrt{33})/9 \approx 0.6950$. Moreover, it is believed that the maximal quantum violation can only be achieved with the (nonmaximally entangled) state and measurement operators described in Refs. [44,45]. Here we will prove this conjecture true.

First of all, let us reexpress the state and measurement of [44,45] in real form. This can be achieved by choosing the first measurements of Alice's and Bob's to be $\bar{E}_m^0 = \bar{F}_m^0 = |m\rangle\langle m|$ for $m = 0, 1, 2$, the second ones $\bar{E}_m^1 = \bar{F}_m^1 = |\alpha_m\rangle\langle\alpha_m|$ with

$$|\alpha_m\rangle = \frac{1}{3}(2|m\rangle + 2|m+1\rangle - |m+2\rangle), \quad (51)$$

and the state $|\bar{\psi}\rangle$ to be measured is as follows:

$$\begin{aligned} |\bar{\psi}\rangle = & \frac{1}{3\sqrt{2+\gamma^2}}[(\gamma + \sqrt{3})(|00\rangle + |11\rangle + |22\rangle) \\ & + \gamma(|01\rangle + |12\rangle + |20\rangle) \\ & + (\gamma - \sqrt{3})(|02\rangle + |10\rangle + |21\rangle)]. \end{aligned} \quad (52)$$

Here all additions performed inside the kets are modulo 3.

The above measurements and states shall then be our reference system. To certify the state, as usual, Alice and Bob will each attach a trusted qutrit to the entangled pair. The next step is to construct CNOT operators with which to build a partial SWAP (see Sec. III). The key point is how to build the translation operator P from the measurement projectors defined in Eq. (52). There are many choices to do so; we chose the simplest combination

$$P = \sum_{i=0}^2 \bar{E}_i^0 \left(-\frac{1}{2} \bar{E}_i^1 - 2\bar{E}_{i+1}^1 + \bar{E}_{i+2}^1 \right), \quad (53)$$

which indeed is a translation operator mapping $|0\rangle \rightarrow |1\rangle \rightarrow |2\rangle \rightarrow |0\rangle$. Here addition of indices is modulo 3. Since Alice's and Bob's optimal operators are identical, the above formula also applies to Bob's settings if we replace E by F .

The choice above in Eq. (53) is a valid unitary operator only for the optimal strategy $E_a^0 = |a\rangle\langle a|$ and $E_a^1 = |\alpha_a\rangle\langle\alpha_a|$. In a device-independent scenario there is no guarantee that this choice still defines a valid unitary operator. We therefore introduce an extra auxiliary (non-Hermitian) operator \hat{P}_A with the constraint that $\hat{P}_A^\dagger P(E_a^x) \geq 0$. For Bob's side, the SWAP operators are defined exactly the same way as above for Alice. Thus, we require also another auxiliary operator \hat{P}_B . We therefore use two localizing matrices $\Gamma(\hat{P}_A^\dagger P(E_a^x), d)$ and $\Gamma(\hat{P}_B^\dagger P(F_a^x), d)$ to self-test the CGMLP inequality. As mentioned in Sec. III B 2, all three semidefinite matrices can be taken as real here since for any feasible point \vec{d} of the corresponding complex SDP, the real vector $\text{Re}\{\vec{d}\}$ returns the same state fidelity and the real matrices $\Gamma(\text{Re}\{\vec{d}\}, \bar{\Gamma}(\hat{P}_A^\dagger P(E_a^x), \text{Re}\{\vec{d}\}), \bar{\Gamma}(\hat{P}_B^\dagger P(F_a^x), \text{Re}\{\vec{d}\}))$ are also positive semidefinite and satisfy the appropriate linear constraints.

Figure 6 shows a plot of the minimum fidelity with respect to the reference state $|\bar{\psi}\rangle$ as a function of the CGLMP violation. One can see that, as the violation tends to the quantum minimum (≈ 0.6950), the fidelity of the general black box with respect to the reference state (nonmaximally entangled state) tends to 1. This shows that any quantum system violating the CGLMP inequality maximally is equivalent via local

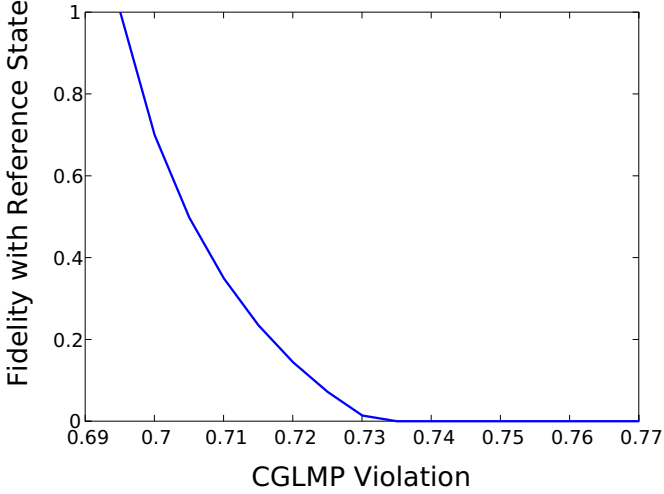


FIG. 6. (Color online) Minimum fidelity of the state swapped out of the operators defined above. The blue line represents the minimum fidelity obtained from the SDP hierarchy. The hierarchy we used is the smallest hierarchy possible for the problem to be defined.

isometries to the nonmaximally entangled state described in Ref. [45]. This proves the conjecture that only nonmaximally entangled states can violate CGLMP maximally.

B. Certification of entangled measurements

In Ref. [46] an entanglement-swapping-based protocol to certify entangled measurements in a device-independent way is presented. In this protocol, four parties A, B, C_A , and C_B are allowed to conduct one out of two possible dichotomic measurements in their respective subsystems. By showing a maximal violation of the CHSH inequality between parties A, C_A and B, C_B , the state shared by Alice and Bob is certified to be separable. Then parties C_A, C_B are brought together and a collective measurement C with four possible outcomes is conducted on the joint C_A - C_B system. As shown in Ref. [46], if, conditioned on any of C 's outcome, Alice and Bob observe an absolute value for the CHSH inequality larger than $\sqrt{2}$, then measurement C must be entangled.

Unfortunately, the previous protocol relies on the assumption that parties A, C_A or B, C_B violate the CHSH inequality maximally. This assumption is crucial to identify the degrees of freedom in parties C_A and C_B on which to test for the effect of measurement C . Indeed, the maximal violation of both CHSH inequalities identifies one qubit on each of these systems on which the authors of [46] show that the action of measurement C is entangled. Without this identification, the experimental statistics can always be modeled with a separable POVM between two parts C_A and C_B of the joint system C . Indeed, consider the situation where C_A and C_B , in addition to the degrees of freedom relevant for their CHSH measurement, share extra pairs of maximally entangled states. Then, at the time of conducting measurement C , C_A can use the maximally entangled states to teleport her internal state to C_B , who in turn conducts measurement C on his side. The resulting POVM allows one to implement effectively measurement C on C_A 's and C_B 's internal states and is achievable via one-way

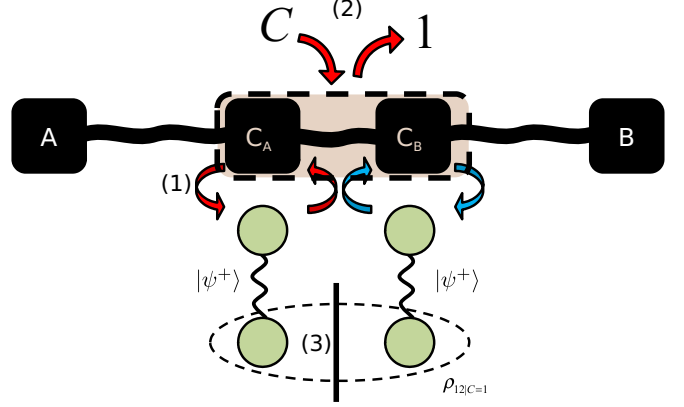


FIG. 7. (Color online) Certification of nonseparability of the measurement C . The scheme works as follows. (1) We perform a (local) SWAP between the boxes C_A, C_B and two particles, each maximally entangled with particles 1 and 2, respectively. (2) We perform measurement C and postselect on the result $c = 1$. (3) We minimize the negativity of the state $\rho_{12|c=1}$.

local operations and classical communication (and is hence separable). Therefore, we say that a measurement is entangled if one can identify local degrees of freedom on which its action is entangled.

In order to single out appropriate degrees of freedom where to test the action of measurement C for nonmaximal CHSH violations, we make use of the SWAP tool (see Fig. 7). Namely, we present a trusted qubit system to each of C_A and C_B that we SWAP inside the two parties' boxes with the help of the unitary swaps \mathcal{S}_A and \mathcal{S}_B . These local unitaries define a qubit degree of freedom inside each party's system. We then test whether the action of measurement C on these particular degrees of freedom is entangled by analyzing the state of two additional qubits (systems 1 and 2 in Fig. 7) initially chosen to be maximally entangled with the two swapped qubits.

We choose to analyze the state of these two qubits conditioned on one of the possible outcomes of the joint measurement C (as opposed to conditioning on four possible outcomes as in Ref. [46]). It is thus sufficient to consider that C can produce either the value $c = +1$ or the value $c = -1$, where $+1$ denotes success of the measurement, i.e., projection onto one Bell state, and -1 denotes projection onto one of the three remaining Bell states. The state of interest is then $\rho_{12|c=1}$. Obviously, if C can be described as a separable operator on the degrees of freedom considered, $\rho_{12|c=1}$ cannot be entangled at the end of the procedure. We can quantify the entanglement of the state $\rho_{12|c=1}$ via its negativity \mathcal{N} [47], which, although nonlinear in the components of $\rho_{12|c=1}$, can be estimated via the SDP [14].

This negativity can be bounded as a function of the following three inequalities:

$$\begin{aligned} \mathcal{B}_1 &= \langle A_0 C_0^A \rangle + \langle A_0 C_1^A \rangle + \langle A_1 C_0^A \rangle - \langle A_1 C_1^A \rangle \leq 2, \\ \mathcal{B}_2 &= \langle B_0 C_0^B \rangle + \langle B_0 C_1^B \rangle + \langle B_1 C_0^B \rangle - \langle B_1 C_1^B \rangle \leq 2, \\ \mathcal{B}_3 &= \langle (1+C)(A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1) \rangle \\ &\quad - 2\langle C \rangle \leq 2, \end{aligned} \quad (54)$$

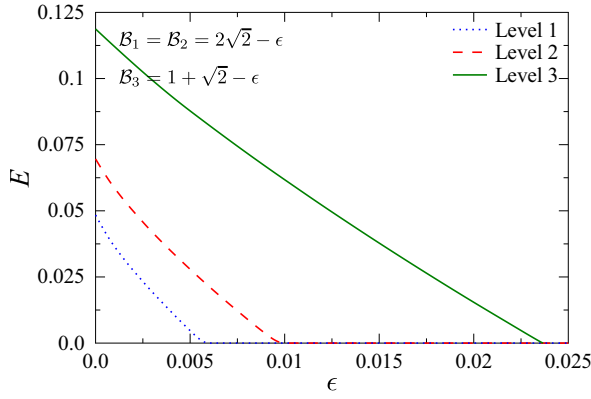


FIG. 8. (Color online) Certification of nonseparability of measurement C . We minimize the quantity $E = P(c = 1)\mathcal{N}(\rho_{12|c=1})$ as a function of the value ϵ , where $\mathcal{N}(\rho_{12|c=1})$ denotes the negativity of the state $\rho_{12|c=1}$. The curves correspond to different levels of the NPA hierarchy [27,28]. A value $E > 0$ signals that Charlie's measurement C is entangled.

by solving the following SDP program:

$$\begin{aligned}
 f^S = \min \quad & \text{tr}(\sigma_-) \\
 \text{s.t.} \quad & \Gamma^S(d) \geq 0, \\
 & \rho_{12|c=1} = g(d), \\
 & \rho_{12|c=1}^{T_1} = \sigma_+ - \sigma_-, \\
 & \sigma_{\pm} \geq 0, \\
 & \sum_i f_i^{B_j}(d_i) = B_j, \quad j = 1, 2, 3,
 \end{aligned} \quad (55)$$

where $\rho_{12|c=1}$ is a function of the entries of the moment matrix $\Gamma^S(d)$, which we denote by $g(d)$. The optimization runs over the moments d and the Hermitian matrices σ_{\pm} . Above we made use of the variational formula for the negativity of a bipartite state [47]. Note that T_1 denotes the partial transpose with respect to the first subsystem (cf. also [14]) and $f_i^{B_j}$ are the coefficients of the Bell inequality B_j .

Figure 8 shows the minimum value of $E \equiv P(c = 1)\mathcal{N}(\rho_{12|c=1})$ when the Bell violations are chosen to be the ones expected from perfect measurements on two Werner states $\rho = V|\psi^-\rangle\langle\psi^-| + (1 - V)\mathbb{1}/4$ with $\epsilon = 2\sqrt{2}(1 - V)$ up to first order in ϵ , i.e., $B_1 = B_2 = 2\sqrt{2} - \epsilon$ and $B_3 = 1 + \sqrt{2} - \epsilon$. The values in Fig. 8 were obtained by using the SEDUMI [48] package in MATLAB. The three distinct curves correspond to different relaxations of the SDP problem with respective dimensions 144, 168, and 200 of the moment matrix $\Gamma^S(c)$. At the highest NPA level 3 (corresponding to a 200-dimensional moment matrix), we find that for $\epsilon < 0.023$ the action of measurement C on the degrees of freedom identified by the SWAP operators cannot be described by a separable POVM. In the figure we may also observe that as ϵ goes to zero measurement C tends to act as a Bell state measurement providing (close to) $E = 1/8$.

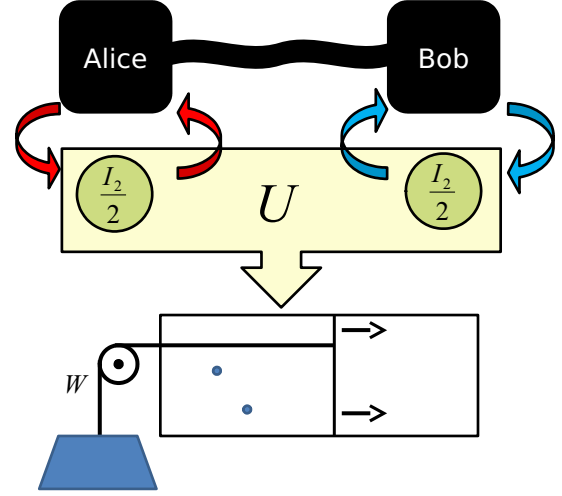


FIG. 9. (Color online) Non-locality and work. We let the boxes interact unitarily with two maximally mixed qubits, representing the position of two particles in a Szilard engine. The resulting pure state can then be rotated so that both particles end up on the left side of the engine with very high probability, hence producing storable work.

C. The SWAP and maximally mixed states: Work extraction and dimension estimates

The relation between work and information has been a matter of scientific debate since the dawn of statistical mechanics. In this regard, it has been shown in Refs. [49,50] that the knowledge of the state of a quantum system, as measured by the smooth minimum and maximum entropies, can be used to generate work. Since the SWAP tool allows us to acquire knowledge about the state inside the box, it is hence not surprising that it can also place a lower bound on its potential for work extraction.

In Fig. 9 we use local SWAP operators over two maximally mixed trusted qubits initially inside a Szilard engine in contact with a bath at temperature T . Since by definition the state of a maximally mixed qubit is completely unknown, such states can be considered as a free resource. After the interaction with the box, the state of the two qubits gets purified and they can be rotated to one of the sides of the box with high probability, thus pulling a weight. Under the assumption that the energy operator of the system inside the box is fully degenerate, it can be proven that the amount of work extracted in this way is related to the difference between the maximum and minimum eigenvalues of ρ_{SWAP} (see Appendix C). This difference can be estimated via semidefinite programming. Figure 10 shows a plot of the CHSH violation vs the minimum amount of work extractable via this scheme. Notice that work extraction is possible as long as the system is nonlocal. Also, for the maximal CHSH violation, the amount of work extractable per KT is $W/KT = 2 \ln(2)$, the work content of two pure qubits [51,52].

In more complex nonlocality scenarios, similar optimizations over the spectrum of the swapped state could also give clues about the dimensionality of the state inside Alice's and Bob's boxes. In Ref. [53] it is proven that a state $\rho \in B(\mathcal{H})$ can be transformed into a state $\sigma \in B(\mathcal{H})$ by means of unitary transformations over ρ and maximally mixed ancillas if and

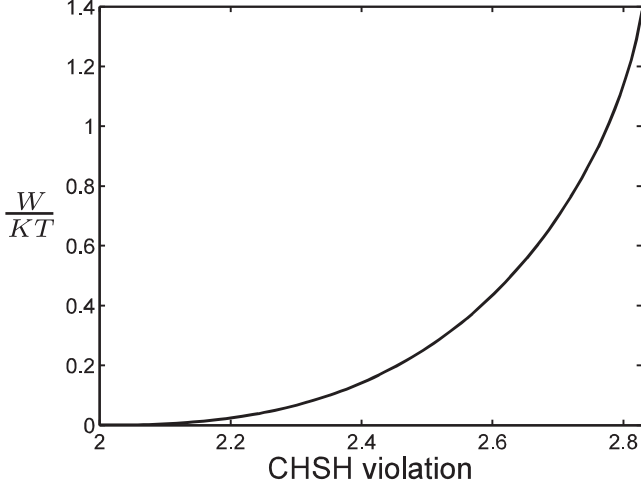


FIG. 10. Extractable work per KT as a function of the CHSH violation of an isotropic box.

only if ρ majorizes σ , i.e., if $\sum_{i=1}^k \lambda_i(\rho) \geq \sum_{i=1}^k \lambda_i(\sigma)$, for all k [here $\lambda_i(M)$ denotes the i th greatest eigenvalue of the matrix M]. Now let $\rho_{\text{box}} \in B(\mathbb{C}^D)$ be the state inside the box(es) and consider the transformation $\rho = \rho_{\text{box}} \otimes (\mathbb{I}_d/d) \rightarrow \sigma = (\mathbb{I}/D) \otimes \rho_{\text{SWAP}}$ that results from applying a SWAP operator between the box and a trusted qudit in the maximally mixed state, followed by the replacement of the state inside the box by a maximally mixed qudit. From [53] it follows that $\lambda_1(\rho)/d \geq \lambda_1(\rho_{\text{SWAP}})/D$ and so D satisfies

$$D \geq d\lambda_1(\rho_{\text{SWAP}}). \quad (56)$$

By minimizing $\lambda_1(\rho_{\text{SWAP}})$, we could hence (in principle) place a lower bound on the dimensionality D of the system inside the box.

VI. CONCLUSION

To appreciate and ultimately certify a quantum experiment, a considerable amount of detailed information about the internal workings of the experimental setup is generally needed. For instance, in typical ion-trap experiments [54] the state of the ions is considered to be (approximately) embedded in a two-dimensional Hilbert space and the behavior of the ion when subject to sequential laser pulses is well known. Without this knowledge, it would be difficult to make sense of most ion-trap experiments. Remarkably, there exist situations where this kind of information is not required in order to take advantage of a (possibly complex) system.

In this paper we have introduced the SWAP tool to characterize quantum systems in arbitrary Bell-type scenarios. We showed that it provides much stronger bounds for known self-testing procedures compared to previously known techniques. We also showed that it provides robust self-testing in different contexts, such as the self-testing of qutrit states and of entangled measurements. Finally, we used the SWAP tool to relate nonlocal correlations to work extraction and quantum dimension, demonstrating that the tool can be used to study a wide variety of properties. All of these results are naturally

noise tolerant and were obtained from the sole knowledge of accessible statistics.

The generality of the method exposed here raises the following questions. How far can one go with the device-independent approach? Are Hilbert spaces necessary at all? Could the whole field of quantum information science be reformulated as a theory of black boxes?

ACKNOWLEDGMENTS

This work was funded by the Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 Grant No. MOE2012-T3-1-009) and by the National Research Foundation of Singapore. M.N. acknowledges support from the John Templeton Foundation, the ERC Advanced Grant NLST, EPSRC DIQIP, the European Commission STREP “RAQUEL,” and the MINECO Project No. FIS2008-01236, with the support of FEDER funds. T.V. acknowledges financial support from a János Bolyai Grant of the Hungarian Academy of Sciences, the Hungarian National Research Fund OTKA (Grant No. PD101461), and the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project.

APPENDIX A: PROOF OF RELATION (38)

In order to relate both quantities, we express $|\psi\rangle$ in the Schmidt decomposition

$$|\psi\rangle = \sum_{i \geq 1} \sqrt{p_i} |\psi_i\rangle_{A'B'} |\phi_i\rangle_{AB}. \quad (A1)$$

A singlet fidelity F with respect to $A'B'$ hence implies

$$\sum_{i \geq 1} p_i |\langle \bar{\psi} | \psi_i \rangle|^2 = F. \quad (A2)$$

Notice that the left-hand side has an upper bound of p_1 (assuming that the Schmidt coefficients are ordered decreasingly, i.e., that p_1 is the maximum).

On the other hand, we have that

$$p_1 |\langle \bar{\psi} | \psi_1 \rangle|^2 + 1 - p_1 \geq \sum_i p_i |\langle \bar{\psi} | \psi_i \rangle|^2 = F. \quad (A3)$$

Combining the last inequality with $p_1 \geq F$, we get that

$$p_1 |\langle \bar{\psi} | \psi_1 \rangle|^2 \geq 2F - 1. \quad (A4)$$

Finally, note that

$$\begin{aligned} s^2 &= \max_{|\text{junk}\rangle} |\langle \psi | (|\bar{\psi}\rangle \otimes |\text{junk}\rangle)|^2 \\ &\geq p_1 |\langle \psi_1 | \bar{\psi} \rangle|^2 \geq 2F - 1, \end{aligned} \quad (A5)$$

where the inequality follows from taking $|\text{junk}\rangle = |\phi_1\rangle$.

APPENDIX B: NONMAXIMALLY ENTANGLED STATE CERTIFICATION WITH THE TILTED CHSH INEQUALITY

For convenience, we shall work in the local basis such that Bob’s optimal measurements are $\bar{B}_0 = \sigma_z$ and $\bar{B}_1 = \cos(2\mu)\sigma_z - \sin(2\mu)\sigma_x$. Note that \bar{B}_1 is no longer σ_x , as in the CHSH case, thus the SWAP operator defined in Eq. (4) no longer works for Bob. We will have to construct the analog of σ_x by combining the operators B_0 and B_1 . We thus

introduce an auxiliary dichotomic operator B_2 , with $B_2^2 = \mathbb{I}$, and impose relations between B_0, B_1, B_2 such that B_2 behaves as if it were $[\cos(2\mu)B_0 - B_1]/\sin(2\mu)$. Following Sec. III, the appropriate constraint is

$$B_2 \frac{\cos(2\mu)B_0 - B_1}{\sin(2\mu)} \geq 0. \quad (\text{B1})$$

This will force B_2 to share the same eigenvectors as $[\cos(2\mu)B_0 - B_1]/\sin(2\mu)$ and will identify both operators in the optimal case. The SWAP operators in this case will then be $\mathcal{S}_B = U'_B V'_B U'_B$, with

$$U'_B = (\mathbb{I} \otimes |0\rangle\langle 0| + B_2 \otimes |1\rangle\langle 1|),$$

$$V'_B = \left(\frac{\mathbb{I} + B_0}{2} \otimes \mathbb{I} + \frac{\mathbb{I} - B_0}{2} \otimes \sigma_x \right), \quad (\text{B2})$$

while \mathcal{S}_A is the same as in Eq. (4).

With the introduction of this extra auxiliary operator, our moment matrix is now enlarged with effectively two operators on Alice's side (A_0, A_1) and three operators on Bob's side (B_0, B_1, B_2). The constraint (B1) is enforced by imposing that the localizing matrix defined by

$$\Gamma \left(B_2 \frac{\cos(2\mu)B_0 - B_1}{\sin(2\mu)} \right)_{ss'}$$

$$= \frac{\cos(2\mu)}{\sin(2\mu)} d_{s^\dagger B_2 B_0 s'} - \frac{1}{\sin(2\mu)} d_{s^\dagger B_2 B_1 s'} \quad (\text{B3})$$

is positive semidefinite.

APPENDIX C: WORK EXTRACTION

Let ρ_{AB} , with spectral decomposition $\rho_{AB} = \sum_{k=1}^4 \lambda_k |\psi_k\rangle\langle\psi_k|$, describe the state of two particles in a Szilard engine of length L and area A , with $\lambda_i \geq \lambda_{i+1}$. Denoting by L (R) the state corresponding to a particle being on the left (right) of the Szilard engine, we can always apply

a unitary U over the state ρ_{AB} such that $U|\psi_1\rangle = |L, L\rangle$, $U|\psi_2\rangle = |R, L\rangle$, $U|\psi_3\rangle = |L, R\rangle$, and $U|\psi_4\rangle = |R, R\rangle$. It follows that a population of N particle pairs in a Szilard engine, initially in state $\rho_{AB}^{\otimes N}$, can be brought to a situation where $N_L = N(\lambda_1 - \lambda_4 + 1)$ particles are on the left side of the engine and $N_R = N(\lambda_4 - \lambda_1 + 1)$ are on the right side. If we place a movable wall connected to a weight on the left side of the engine (in contact with a bath at temperature T), the pressure over the wall is equal to

$$P = \frac{N_L K T}{A z} - \frac{N_R K T}{A(L - z)}, \quad (\text{C1})$$

where z denotes the position of the piston. At constant temperature, the equilibrium position of the piston is $z_{\text{eq}} = \frac{N_L L}{N_L + N_R}$. The work extracted in the process of moving the piston from $z = L/2$ to z_{eq} is

$$W = \int_{L/2}^{z_{\text{eq}}} P A dz$$

$$= K T \left\{ N_L \ln \left(\frac{2N_L}{N_L + N_R} \right) + N_R \ln \left(\frac{2N_R}{N_L + N_R} \right) \right\}$$

$$\equiv W(\lambda_1 - \lambda_4). \quad (\text{C2})$$

Finally, the minimum value of $\lambda_4 - \lambda_1$ can be extracted from ρ_{SWAP} via the following SDP:

$$\min \quad \mu_1 - \mu_4$$

$$\text{s.t.} \quad \rho_{\text{SWAP}} - \mu_4 \mathbb{I} \geq 0,$$

$$\mu_1 \mathbb{I} - \rho_{\text{SWAP}} \geq 0. \quad (\text{C3})$$

Since

$$\rho_{\text{SWAP}} - \mu_4 \mathbb{I} \geq 0 \Rightarrow \text{Re}\{\rho_{\text{SWAP}}\} - \mu_4 \mathbb{I} \geq 0,$$

$$\mu_1 \mathbb{I} - \rho_{\text{SWAP}} \geq 0 \Rightarrow \mu_1 \mathbb{I} - \text{Re}\{\rho_{\text{SWAP}}\} \geq 0, \quad (\text{C4})$$

it follows that the free variables in the corresponding SDP can be taken as real, as in the previous examples.

-
- [1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007).
 - [2] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *New J. Phys.* **11**, 045021 (2009).
 - [3] Ll. Masanes, S. Pironio, and A. Acín, *Nat. Commun.* **2**, 238 (2011).
 - [4] E. Hänggi and R. Renner, *arXiv:1009.1833*.
 - [5] S. Pironio, Ll. Masanes, A. Leverrier and A. Acín, *Phys. Rev. X* **3**, 031007 (2013).
 - [6] R. Colbeck and A. Kent, *J. Phys. A: Math. Theor.* **44**, 095305 (2011).
 - [7] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Nature (London)* **464**, 1021 (2010).
 - [8] V. Scarani, *Acta Phys. Slovaca* **62**, 347 (2012).
 - [9] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Rev. Mod. Phys.* **86**, 419 (2014).
 - [10] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, *Phys. Rev. Lett.* **106**, 250404 (2011).
 - [11] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Methot, and V. Scarani, *Phys. Rev. Lett.* **100**, 210503 (2008).
 - [12] M. Tomamichel and E. Hänggi, *J. Phys. A: Math. Theor.* **46**, 055301 (2013).
 - [13] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, *Phys. Rev. A* **80**, 062327 (2009).
 - [14] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, *Phys. Rev. Lett.* **111**, 030501 (2013).
 - [15] B. S. Tsirelson, *Hadronic J. Suppl.* **8**, 329 (1993).
 - [16] S. J. Summers and R. F. Werner, *Commun. Math. Phys.* **110**, 247 (1987) (Theorem 2.3).
 - [17] S. Popescu and D. Rohrlich, *Phys. Lett. A* **169**, 411 (1992).
 - [18] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).
 - [19] B. S. Cirel'son, *Lett. Math. Phys.* **4**, 93 (1980).
 - [20] D. Mayers and A. Yao, *Quantum Inf. Comput.* **4**, 273 (2004).
 - [21] T. Franz, F. Furrer, and R. F. Werner, *Phys. Rev. Lett.* **106**, 250502 (2011).

- [22] M. McKague, T. H. Yang, and V. Scarani, *J. Phys. A: Math. Theor.* **45**, 455304 (2012).
- [23] C. A. Miller and Y. Shi, [arXiv:1207.1819](#).
- [24] B. W. Reichardt, F. Unger, and U. Vazirani, *Nature (London)* **496**, 456 (2013).
- [25] T. H. Yang and M. Navascués, *Phys. Rev. A* **87**, 050102(R) (2013).
- [26] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués, *Phys. Rev. Lett.* **113**, 040401 (2014).
- [27] M. Navascués, S. Pironio, and A. Acín, *Phys. Rev. Lett.* **98**, 010401 (2007).
- [28] M. Navascués, S. Pironio, and A. Acín, *New J. Phys.* **10**, 073013 (2008).
- [29] S. P. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, 2004).
- [30] T. Ito, H. Kobayashi, and K. Matsumoto, in *IEEE 27th Conference on Computational Complexity* (IEEE, Piscataway, NJ, 2012), p. 217.
- [31] T. Fritz, T. Netzer, and A. Thom, *Proc. Amer. Math. Soc.* **142**, 4265 (2014).
- [32] N. Ozawa, *J. Math. Phys.* **54**, 032202 (2013).
- [33] K. F. Pál and T. Vértesi, *Phys. Rev. A* **82**, 022116 (2010).
- [34] M. Navascués, T. Cooney, D. Pérez-García, and I. Villanueva, *Found. Phys.* **42**, 985 (2012).
- [35] S. Pironio, M. Navascués, and A. Acín, *SIAM J. Optim.* **20**, 2157 (2010).
- [36] M. Takesaki, *Theory of Operator Algebras I* (Springer, Berlin, 1979).
- [37] Y. Zhang, S. Glancy, and E. Knill, *Phys. Rev. A* **84**, 062118 (2011).
- [38] O. Nieto-Silleras, S. Pironio, and J. Silman, *New J. Phys.* **16**, 013035 (2014).
- [39] J.-D. Bancal, L. Sheridan, and V. Scarani, *New J. Phys.* **16**, 033011 (2014).
- [40] J.-D. Bancal and V. Scarani, in *Proceedings of the 9th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC'14)* (Schlors Dagstuhl-Leibniz-Zentrum, Dagstuhl, Germany, 2014), Vol. 27, pp. 1–16.
- [41] B. W. Reichardt, F. Unger, and U. Vazirani, [arXiv:1209.0448](#).
- [42] B. G. Christensen *et al.*, *Phys. Rev. Lett.* **111**, 130406 (2013).
- [43] A. Acín, S. Massar, and S. Pironio, *Phys. Rev. Lett.* **108**, 100402 (2012).
- [44] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, *Phys. Rev. Lett.* **88**, 040404 (2002).
- [45] A. Acín, T. Durt, N. Gisin, and J. I. Latorre, *Phys. Rev. A* **65**, 052325 (2002).
- [46] R. Rabelo, M. Ho, D. Cavalcanti, N. Brunner, and V. Scarani, *Phys. Rev. Lett.* **107**, 050502 (2011).
- [47] G. Vidal and R. F. Werner, *Phys. Rev. A* **65**, 032314 (2002).
- [48] J. F. Sturm, *Optim. Methods Softw.* **11**, 625 (1999).
- [49] L. Szilard, *Z. Phys.* **53**, 840 (1929).
- [50] O. C. O. Dahlsten, R. Renner, E. Rieper, and V. Vedral, *New J. Phys.* **13**, 053015 (2011).
- [51] C. H. Bennett, *Int. J. Theor. Phys.* **21**, 905 (1982).
- [52] R. P. Feynman, A. J. Hey, and R. W. Allen, *Feynman Lectures on Computation* (Perseus, Cambridge, MA, 2000).
- [53] M. Horodecki, P. Horodecki, and J. Oppenheim, *Phys. Rev. A* **67**, 062104 (2003).
- [54] D. Leibfried, R. Blatt, C. Monroe, and D. Wineland, *Rev. Mod. Phys.* **75**, 281 (2003).