Device-independent state estimation based on Bell's inequalities

C.-E. Bardyn,[1,2] T. C. H. Liew,[1] S. Massar,[3] M. McKague,[4] and V. Scarani[1,5]

[1]*Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore*

[2]*Ecole Polytechnique Fédérale de Lausanne (EPFL), 1015 Lausanne, Switzerland*

[3]*Laboratoire d'Information Quantique, CP 225, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, B-1050 Brussells, Belgium*

[4]*Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1*

[5]*Department of Physics, National University of Singapore, Singapore 117542, Singapore*

(Received 10 July 2009; revised manuscript received 28 September 2009; published 14 December 2009)

The only information available about an alleged source of entangled quantum states is the amount S by which the Clauser-Horne-Shimony-Holt inequality is violated: nothing is known about the nature of the system or the measurements that are performed. We discuss how the quality of the source can be assessed in this black-box scenario, as compared to an ideal source that would produce maximally entangled states (more precisely, any state for which $S=2\sqrt{2}$). To this end, we present several inequivalent notions of fidelity, each one related to the use one can make of the source after having assessed it, and we derive quantitative bounds for each of them in terms of the violation S. We also derive a lower bound on the entanglement of the source as a function of S only.

DOI: 10.1103/PhysRevA.80.062327 PACS number(s): 03.67.−a, 03.65.Wj, 03.65.Ud

I. INTRODUCTION

A device, allegedly generating pairs of entangled particles, is for sale. Obviously, the potential *user* wants to check that entanglement is indeed being generated before buying it; but just as obviously, the *vendor* does not want to open the device and reveal its fabrication. For classical devices, such a situation would lead to a complete impasse. Not so, however, for quantum devices: *Bell's inequalities* can act as entanglement witnesses irrespective of the nature of the system under study or of the kind of measurements that are being performed. Thus, suppose that the vendor provides the user with two additional boxes: the measurement devices. Once more, the vendor does not want to open the device and reveal its fabrication. Suppose in addition that the user can choose the measurements: the measurement devices have a knob whose positions correspond to allegedly different measurements (Fig. 1). By operating these devices, the user can reconstruct the statistics $P(a,b|A,B)$ of the observed outputs a and b, conditioned on each choice of knob positions A and B. If the statistics violate some Bell inequality and the measurement has been performed in such a way as to avoid signaling between the measurement boxes, then the user is convinced that the source is indeed producing entangled pairs.

The possibility of such an assessment is already remarkable. However, the user cannot be satisfied with knowing that there is "some entanglement." What is needed is a *quantitative estimate* on how good the source actually is. The amount of violation of a Bell's inequality can provide such a quantitative criterion, provided it is translated into the meaningful figure of merit: fidelity or trace distance to the ideal state or some entanglement measure… The goal of this paper is to provide such quantitative estimates when the Bell inequality under study is the Clauser-Horne-Shimony-Holt (CHSH) inequality [1].

This work is inspired by "device-independent quantum key distribution" [2,3], in which the amount of violation of the CHSH inequality is used to bound the information of an eavesdropper without making any hypothesis on the internal workings of the devices. It is also related to the concept of "dimension witness:" sufficient violation of some Bell inequalities can guarantee that the quantum state has a minimum dimension [4–6]. One possible application of the present work could be to devise improved self-testing of quantum computers [7,8].

II. FORMULATION OF THE PROBLEM

A. Ideal states

As we said, we restrict to the case where the user applies only two measurement settings on each particle and the outcome is binary. In this case, there is only one Bell inequality, namely, CHSH [9]. We further restrict our study in considering only the observed violation S_{obs} of CHSH as quantitative measure, being aware that the statistics $P(a,b|A,B)$ contain further information that might improve the estimates.

Since the source will be characterized by a single scalar quantity, the set of ideal states is the set of states $\mathbf{\Phi}$ such that $S=2\sqrt{2}$ is achievable. This set has been fully characterized [10,11]: it consists of all pure states of the form

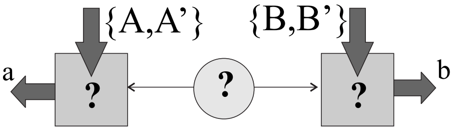

FIG. 1. Device-independent state estimation. The quality of an unknown source of entangled pairs should be established using unknown measurement devices. The only available information is the statistics $P(a,b|A,B)$ of the outcomes (a,b) for measurement settings A,B. This represents the particular case studied in this paper, where both the choice of measurement settings and the outputs are binary.

$\Sigma_j c_j|\Psi_j\rangle$, where $|\Psi_j\rangle$ is a two-qubit maximally entangled state in a four-dimensional subspace, i.e., $|\Psi_j\rangle=\frac{1}{\sqrt{2}}(|2j-1,2j-1\rangle+|2j,2j\rangle)$ up to local unitaries. Since the relative phases of the c_j do not play any role in the violation, we must add mixed states to the set. It is easy to verify that the most general such state can be written as $\boldsymbol{\Phi}=U_AU_B\boldsymbol{\Phi}^+\otimes\boldsymbol{\sigma}U_A^\dagger U_B^\dagger$, where $|\Phi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ is a two-qubit maximally entangled state, $\boldsymbol{\sigma}$ is an arbitrary state, and U_A, U_B are arbitrary local unitaries. In their work on device testing, Mayers and Yao (MY) [7] chose their reference states as those that could be written in the above form with $\boldsymbol{\sigma}$ pure, i.e., even though they did not refer to Bell inequalities, they where considering all pure states that violate CHSH maximally.

B. Figures of merit

The distance between the actual source state, with density matrix $\boldsymbol{\rho}$ and the closest ideal state $\boldsymbol{\Phi}$, is conveniently measured by the trace distance [12,13]

$$\delta_{\text{MY}}(\boldsymbol{\rho})=\min_{\boldsymbol{\Phi}}\ \delta(\boldsymbol{\rho},\boldsymbol{\Phi}), \tag{1}$$

where $\delta(\boldsymbol{\rho},\boldsymbol{\Phi})=\frac{1}{2}\text{Tr}|\boldsymbol{\rho}-\boldsymbol{\Phi}|$. The trace distance has a clear operational interpretation: in whatever task, $\boldsymbol{\rho}$ will behave differently from $\boldsymbol{\Phi}$ with probability at most $\delta(\boldsymbol{\rho},\boldsymbol{\Phi})$. In other words, the real source will differ from an ideal source with probability at most $\delta(\boldsymbol{\rho})$.

The problem we have set out to solve is thus to find a bound of the form

$$\delta_{\text{MY}}(\boldsymbol{\rho})\le\mathcal{D}_{\text{MY}}(S_{\text{obs}}). \tag{2}$$

This bound can in principle be obtained by solving the following optimization problem:

$$\mathcal{D}_{\text{MY}}(S_{\text{obs}})=\max_{\boldsymbol{\rho}:S_{\max}(\boldsymbol{\rho})\ge S_{\text{obs}}}\ \{\min_{\boldsymbol{\Phi}}\ \delta(\boldsymbol{\rho},\boldsymbol{\Phi})\}, \tag{3}$$

where $S_{\max}(\boldsymbol{\rho})$ is the maximum CHSH violation that can be obtained by measuring state $\boldsymbol{\rho}$.

Deriving lower bounds, let alone tight lower bounds, for $\mathcal{D}_{\text{MY}}$ turns out to be much harder than we initially anticipated. In practice, it is simpler to work with the *fidelity* rather than the trace distance: the two measures being related by $\delta\le\sqrt{1-F}$ [13]. In analogy with Eq. (1), we define

$$F_{\text{MY}}(\boldsymbol{\rho})=\max_{\boldsymbol{\Phi}}\ F(\boldsymbol{\rho},\boldsymbol{\Phi})=\max_{\boldsymbol{\Phi}}(\text{Tr}\sqrt{\boldsymbol{\rho}^{1/2}\boldsymbol{\Phi}\boldsymbol{\rho}^{1/2}})^2 \tag{4}$$

and one is then led to search for bounds of the form

$$F_{\text{MY}}(\boldsymbol{\rho})\ge\mathcal{F}_{\text{MY}}(S_{\text{obs}}). \tag{5}$$

For $\mathcal{F}_{\text{MY}}$, we obtain tight lower bounds if the state is restricted to consist of two qubits or (modulo a conjecture of Gisin and Peres) if the state is restricted to be pure. Putting such hypotheses on the source goes against the philosophy of the black box scenario, but it allows us to get a mathematical grasp of the problem. When no restrictions are put on the state, we do not even have a lower bound on $\mathcal{F}_{\text{MY}}$. However, it is possible to introduce other notions of fidelity (see below) which have a clear operational meaning and for which lower bounds can be computed without any hypothesis on the source.

Yet an alternative approach to the source characterization problem would consist in looking for a lower bound to the *entanglement* of the state $\boldsymbol{\rho}$,

$$E(\boldsymbol{\rho})\ge\mathcal{E}(S_{\text{obs}}), \tag{6}$$

where E is an entanglement measure, such as the entanglement of formation, of distillation, etc. [14]. Below, we obtain lower bounds on $\mathcal{E}$.

C. Warm up: Solution assuming two qubits

As a nontrivial warm-up exercise, let us compute the bound Eq. (5) under the assumption that the source emits a pair of qubits and that the measurements are von Neumann measurements. This is an undue restriction for the black-box scenario; we present this calculation because its result is interesting in itself and will be an important tool for the main discussion.

In this case, the set of ideal states is well known: only the maximally entangled states $\boldsymbol{\Phi}=U_AU_B\boldsymbol{\Phi}^+U_A^\dagger U_B^\dagger$ violate CHSH maximally. Therefore, $F_{\text{MY}}(\boldsymbol{\rho})=\max_{\boldsymbol{\Phi}}F(\boldsymbol{\rho},\boldsymbol{\Phi})$ reduces to the so-called *singlet fidelity* of $\boldsymbol{\rho}$. Our approach consists in fixing the singlet fidelity of $\boldsymbol{\rho}$ and computing $S_{\max}(\boldsymbol{\rho})$. To this end, we use the spectral decomposition of the Bell operator

$$\hat{\mathcal{B}}=(\hat{A}+\hat{A}')\otimes\hat{B}+(\hat{A}-\hat{A}')\otimes\hat{B}'. \tag{7}$$

First note that if $F(\boldsymbol{\rho})\le\frac{1}{2}$, the state cannot be entangled, CHSH cannot be violated, and the bound $S_{\max}=2$ can be trivially achieved by the degenerate measurement $\hat{A}=\hat{A}'=\hat{B}=\hat{B}'=\mathbb{1}$. If the inequality is violated, the operators $\hat{A}$, $\hat{A}'$, $\hat{B}$, and $\hat{B}'$ must be linear combinations of the three Pauli matrices. Then the spectral decomposition $\hat{\mathcal{B}}=\Sigma_i\lambda_i|\Phi_i\rangle\langle\Phi_i|$ has the following properties [15]: the $|\Phi_i\rangle$ are a Bell basis (i.e., a basis of maximally entangled states) and the eigenvalues are $\{\lambda_1,\lambda_2,-\lambda_2,-\lambda_1\}$ with $\text{Tr}(\hat{\mathcal{B}}^2)=16$, i.e.,

$$\lambda_1^2+\lambda_2^2=8, \tag{8}$$

which implies the Cirelson bound $|\lambda_i|\le2\sqrt{2}$ [16].

Therefore, for a given $\hat{\mathcal{B}}$, we have

$$S(\boldsymbol{\rho})=\text{Tr}(\boldsymbol{\rho}\hat{\mathcal{B}})=\sum_i\lambda_i\langle\Phi_i|\boldsymbol{\rho}|\Phi_i\rangle. \tag{9}$$

Suppose for definiteness $\lambda_1\ge\lambda_2\ge0$. Then, keeping $F(\boldsymbol{\rho})$ fixed, $S(\boldsymbol{\rho})$ is maximized by choosing $|\Phi_1\rangle$ such that $F(\boldsymbol{\rho},\boldsymbol{\Phi}_1)=F(\boldsymbol{\rho})$. Whereas we have that $S_{\max}(\boldsymbol{\rho})\le\lambda_1F(\boldsymbol{\rho})+\lambda_2[1-F(\boldsymbol{\rho})]$ because the two other eigenvalues are nonpositive. Using Eq. (8), we can set $\lambda_1=2\sqrt{2}\cos x$ and $\lambda_2=2\sqrt{2}\sin x$. The well-known bound $\max_x(a\cos x+b\sin x)=\sqrt{a^2+b^2}$ then leads to $S_{\max}(\boldsymbol{\rho})\le2\sqrt{2}\sqrt{F(\boldsymbol{\rho})^2+[1-F(\boldsymbol{\rho})]^2}$. Finally (Fig. 2),

$$F_{\text{MY}}(\boldsymbol{\rho})\ge(1+\sqrt{[S_{\text{obs}}/2]^2-1})/2\quad\text{(qubits)}. \tag{10}$$

This bound is tight, being achieved by pure nonmaximally entangled states $|\psi\rangle=\cos\theta|00\rangle+\sin\theta|11\rangle$. Indeed, for these

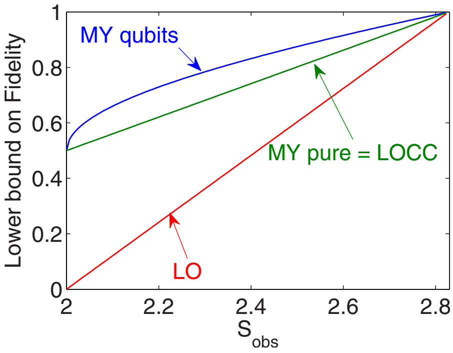

FIG. 2. (Color online) Lower bounds on the fidelity as a function of the observed violation S_{obs} of the CHSH inequality. From top to bottom: F_{MY} assuming two qubits (10); F_{MY} assuming pure states and the Gisin-Peres conjecture (16) equal to F_{LOCC} (20); and F_{LO} (19).

states, $S_{\max}=2\sqrt{1+\sin^2(2\theta)}$ [17,18] and the singlet fidelity is $F=|\langle\psi|\Phi^+\rangle|^2=\frac{1}{2}[1+\sin(2\theta)]$. Furthermore for pairs of pure states, we have the strict equality $\delta=\sqrt{1-F}$, hence Eq. (10) leads to a tight bound for the trace distance as well.

III. BOUNDS ON THE FIDELITY TO THE CLOSEST REFERENCE STATE

A. Structure of the Bell operator

For any two dichotomic operators $\hat{A}$ and $\hat{A}'$, one can find a basis such that both operators are block diagonal, where each block is a 2×2 matrix (see, e.g., [3]). So one has $\hat{A}=\Sigma_\alpha\hat{A}_\alpha$ and $\hat{A}'=\Sigma_\alpha\hat{A}'_\alpha$, where $\hat{A}_\alpha=\Pi_\alpha\hat{A}\Pi_\alpha$, $\hat{A}'_\alpha=\Pi_\alpha\hat{A}'\Pi_\alpha$, and Π_α are orthogonal projectors onto two-dimensional spaces. Of course, a similar decomposition holds for Bob's operators. Therefore, the Bell-CHSH operator can be written as

$$\hat{\mathcal{B}}=\sum_{\alpha,\beta}\hat{\mathcal{B}}_{\alpha,\beta}, \tag{11}$$

where $\hat{\mathcal{B}}_{\alpha,\beta}=\Sigma_i\lambda_i^{\alpha\beta}|\Phi_i^{\alpha\beta}\rangle\langle\Phi_i^{\alpha\beta}|$ are orthogonal two-qubit operators with the same properties as above. Therefore,

$$S(\boldsymbol{\rho})=\sum_{\alpha,\beta}p_{\alpha\beta}\,\text{Tr}(\boldsymbol{\rho}_{\alpha\beta}\hat{\mathcal{B}}_{\alpha\beta})=\sum_{\alpha,\beta}p_{\alpha\beta}S(\boldsymbol{\rho}_{\alpha\beta}), \tag{12}$$

where $p_{\alpha\beta}\boldsymbol{\rho}_{\alpha\beta}=\Pi_\alpha\otimes\Pi_\beta\boldsymbol{\rho}\Pi_\alpha\otimes\Pi_\beta$ and $\boldsymbol{\rho}_{\alpha\beta}$ is a normalized two-qubit state.

B. Complex problem

Given Eq. (12), it may seem that the extension of our result to arbitrary dimensions is just a matter of convex optimization. A closer look shows that one must be much more careful because the above construction does not imply

$$F_{\text{MY}}(\boldsymbol{\rho})\geq\sum_{\alpha,\beta}p_{\alpha\beta}F(\boldsymbol{\rho}_{\alpha\beta})\quad\text{(probably wrong)}, \tag{13}$$

where $F(\boldsymbol{\rho}_{\alpha\beta})$ is the singlet fidelity of $\boldsymbol{\rho}_{\alpha\beta}$. The reason is that in the MY approach, the state must be brought close to a reference state using local unitary operations $U_A\otimes U_B$. Let U_α be the restriction of U_A to the 2×2 block indexed by α and similarly for U_β, and let $\boldsymbol{\Phi}_{\alpha\beta}$ be the maximally entangled state of two qubit such that $F(\boldsymbol{\Phi}_{\alpha\beta},\boldsymbol{\rho}_{\alpha\beta})=F(\boldsymbol{\rho}_{\alpha\beta})$ is the singlet fidelity of $\boldsymbol{\rho}_{\alpha\beta}$. Now, there is no guarantee that U_A and U_B exist, such that $U_\alpha\otimes U_\beta\boldsymbol{\Phi}_{\alpha\beta}U_\alpha^\dagger\otimes U_\beta^\dagger=\boldsymbol{\Phi}^+$ for all α and β, as is required to obtain a reference state according to the MY definition. Moreover, the MY definition of fidelity is a comparison to the whole state $\boldsymbol{\Phi}^+\otimes\boldsymbol{\sigma}$, not only to the two-qubit component $\boldsymbol{\Phi}^+$. In order to make sense of Eq. (13), we will introduce different definitions of fidelity below. Before turning to that, we present the case of pure states of arbitrary dimensions, for which the MY fidelity can be computed.

C. Solution under the restriction to pure states

Let us assume that we know that the source emits a pure state (again an undue restriction for the black box scenario). Using the Schmidt decomposition $|\Psi\rangle=\Sigma_k\lambda_k|k,k\rangle$ with the Schmidt coefficients in decreasing order $\lambda_k\geq\lambda_{k+1}\geq0$, any pure state can be rewritten as $|\Psi\rangle=\Sigma_j\sqrt{p_j}(c_j|2j,2j\rangle+s_j|2j+1,2j+1\rangle)$, with $c_j^2+s_j^2=1$. The MY fidelity can be computed exactly (Appendix A) and one finds

$$F_{\text{MY}}(\Psi)=\sum_j\frac{(\lambda_j+\lambda_{j+1})^2}{2}=\sum_j p_j\frac{(c_j+s_j)^2}{2}. \tag{14}$$

This should now be related to $S_{\max}(\Psi)$. For states of arbitrary dimension, there is no known analytical expression for the maximal violation of CHSH. However, for pure states Ψ, there is a long-standing conjecture by Gisin and Peres [19], whose validity has never been disproved by numerical checks [20]. According to this conjecture, the ordered Schmidt decomposition defines the natural block structure of the CHSH operator. This implies

$$S_{\max}(\Psi)=\sum_j p_j[2\sqrt{1+4c_j^2s_j^2}]. \tag{15}$$

Combining this conjecture with Eq. (14), we find that for pure states, the accessible points in the $(F_{\text{MY}},S_{\max})$ plane are convex combinations of points on the curve given by equality in Eq. (10), yielding (Fig. 2)

$$F_{\text{MY}}(\boldsymbol{\Psi})\geq\frac{1}{4(\sqrt{2}-1)}[S_{\text{obs}}+2\sqrt{2}-4]$$
$$\text{(pure states, modulo Gisin-Peres conjecture)}. \tag{16}$$

This bound is tight if we allow the dimension d to become arbitrarily large (otherwise, the ordering of the λ_k implies constraints on the possible values of $\{p_j,c_j,s_j\}$). Moreover, this bound is weaker than the one obtained under the assumption of two qubits. It should be noted that on the contrary, in device-independent quantum key distribution, the bound for collective attacks is already optimal in the two-qubit case [2,3].

D. Black-box bounds for other fidelities

The MY fidelity is defined to suit the black-box scenario. However, other definitions of fidelity may be meaningful. Here, we consider fidelities defined as

$$F_{\mathcal{L}}(\boldsymbol{\rho}) = \max_{\Lambda \in \mathcal{L}} F(\Lambda(\boldsymbol{\rho}), \boldsymbol{\Phi}^{+}), \tag{17}$$

where $\mathcal{L}$ is a set of completely positive maps which map the Hilbert space of $\boldsymbol{\rho}$ onto a 2×2 dimensional Hilbert space and which cannot increase the entanglement. $F_{\mathcal{L}}$ can be thought of as the best singlet fidelity obtainable under single shot purification of $\boldsymbol{\rho}$ to a two-qubit entangled state using only operations that belong to the family $\mathcal{L}$. We will consider the case where $\mathcal{L}$ consists of all the completely positive maps that can be realized by local operations ($\mathcal{L}$=LO) or by local operations and classical communication ($\mathcal{L}$=LOCC).

These notions of fidelity shed a different light on the task of source characterization. Indeed the Mayers-Yao fidelity and trace distance compare the state produced by the source to the closest ideal state, thereby establishing how much the real state and the ideal state would differ in applications. The new fidelities $F_{\mathcal{L}}$ are relevant to another scenario in which the user may try to improve the source by acting locally on the two subsystems, for instance, by opening the boxes containing the measurement devices and tinkering inside them. But before buying the source, the user wants to perform a fast black-box check to ascertain what will be the performance of the improved source. In other words, by measuring S_{obs} in a black-box scenario, the user can assess how well the source would perform in other scenarios. In this sense, the bounds we derive for these fidelities are real black-box statements, which do not make any hypothesis on the state $\boldsymbol{\rho}$ and on the measurement devices.

These fidelities are related by

$$F_{\text{MY}} \leq F_{\text{LO}} \leq F_{\text{LOCC}}. \tag{18}$$

In Appendix B, we prove that $F_{\text{MY}}(\boldsymbol{\Psi})=F_{\text{LO}}(\boldsymbol{\Psi})$ for pure states while for mixed states, there are explicit cases of strict inequality. We also show (see Fig. 2) that

$$F_{\text{LO}}(\boldsymbol{\rho}) \geq \frac{1}{2(\sqrt{2}-1)}[S_{\text{obs}}-2], \tag{19}$$

$$F_{\text{LOCC}}(\boldsymbol{\rho}) \geq \frac{1}{4(\sqrt{2}-1)}[S_{\text{obs}}+2\sqrt{2}-4]. \tag{20}$$

The bound (19) on F_{LO} is obtained by exhibiting an explicit LO strategy. The proof is lengthy and we give it in Appendix C. We just note here that this bound is surely not tight since it reaches the over pessimistic $F=0$ for $S=2$.

The bound (20) for F_{LOCC} is the same one obtained for F_{MY} on pure states, Eq. (16); we do not know whether this bound is tight. The proof goes as follows. The decomposition Eq. (11) of the Bell-CHSH operator gives us a natural method for projecting $\boldsymbol{\rho}$ onto a two-qubit space: particle A is projected in the Π_α spaces and particle B in the Π_β spaces. Using classical communication (CC) , the actual block (α,β) is made known in both locations. The result of this completely positive map is a state with fidelity $F=p_{\alpha\beta}\Sigma_{\alpha\beta}F(\boldsymbol{\rho}_{\alpha\beta})$, i.e., we obtain a convex combination of points on the curve Eq. (10). The bound (20) is recovered by noticing that, in the LOCC scenario, all the blocks (α,β) for which $S(\boldsymbol{\rho}_{\alpha\beta})=2$ can be brought to have $F=1/2$: indeed, for the blocks where they observe $S=2$, Alice and Bob can swap their local states with those of ancillas prepared in a pure product state.

IV. OTHER FIGURES OF MERIT

The core of our work involved using the fidelity as a figure of merit. Here, we present the consequences of the bounds obtained on the fidelity for other figures of merit.

A. Relation with trace distance

Even if fidelity bounds were found to be tight, the tightness of the bound $\delta \leq \sqrt{1-F}$ on the trace distance would follow only if the states that saturate the bound are pure. However, we are already able to conclude that the bounds $\mathcal{D}(S_{\text{obs}})$ for the trace distance δ put very stringent constraints on the quality of the source.

For instance, our strongest bound Eq. (10) leads to a tight $\delta=\sqrt{1-F}$. If we insert $S_{\text{obs}}=0.99\times 2\sqrt{2}$, we obtain $\delta\approx 10\%$. If the user requests the error rate to be below 1%, the vendor will have to produce extremely good sources—better than any currently available one.

B. Relation with entanglement measures

The bounds for all the $\mathcal{F}_{\mathcal{L}}$ also provide lower bounds on the entanglement of $\boldsymbol{\rho}$. Indeed, consider any entanglement measure E (see [14] for a list). By definition, $\mathcal{L}$ is a set of operations under which E cannot increase and the bounds on $\mathcal{F}_{\mathcal{L}}$ tell us how close the state $\boldsymbol{\rho}$ can be brought to the singlet state using only operations in $\mathcal{L}$. If $\mathcal{L}$=LOCC, each $\boldsymbol{\rho}_{\alpha\beta}$ can further be twirled, leading to the map $\boldsymbol{\rho}\rightarrow p\boldsymbol{\Phi}^{+}+(1-p)\frac{1}{4}$ with $p=[4\mathcal{F}_{\text{LOCC}}(S_{\text{obs}})+1]/3$. For such states, the entanglement measures can generally be computed. For instance, using [21], the entanglement of formation is bounded by

$$E_f \geq h\left(\frac{1}{2}+\frac{1}{4(\sqrt{2}-1)}\sqrt{8(1-\sqrt{2})+4S_{\text{obs}}-S_{\text{obs}}^2}\right).$$

where h is the binary entropy function.

V. CONCLUSION

A theory of black-box source characterization is a step toward the development of device-independent quantum information processing. In the present work, we used only the CHSH inequality: already in this simple case, we have uncovered a rich structure, raised many problems, and solved a few.

In particular, the task of deriving black-box bounds for use in the black-box scenario in full generality is still open; we have been able to derive tight bounds for the Mayers-Yao fidelity either by restricting the dimensions to two qubits (10) or by restricting the state to be pure (16). For arbitrary states, we do not even have a lower bound for the Mayers-Yao fidelity or trace distance. However we have been able to derive unrestricted black-box bounds for use in other scenarios [Eqs. (19) and (20)] where one wants to ascertain how close to an ideal state it would be possible to bring the system by local operations, possibly complemented by classical communication. We have also been able to derive unrestricted black-box lower bounds for the entanglement of the state. Our results indicate that black-box bounds put very stringent demands on the quality of an untrusted source, which could, in particular, have important consequences for self-testing of quantum computers.

ACKNOWLEDGMENTS

This work is supported by the National Research Foundation and Ministry of Education, Singapore, by the Interuniversity Attraction Poles (Belgian Science Policy) Project No. IAP6-10 Photonics@be, by the EU project QAP Contract No. 015848, by NSERC, Ontario-MRI, OCE, QuantumWorks, MITACS, and the Government of Canada. We are grateful to Frédéric Magniez, Mike Mosca, and Jamie Sikora for helpful discussions.

APPENDIX A: CALCULATING F_{MY} FOR PURE STATES

We begin with a state $|\psi\rangle$ in Schmidt form

$$|\psi\rangle = \sum_j \lambda_j |a_j\rangle |b_j\rangle, \tag{A1}$$

while the closest state of the form $|?\rangle \otimes |\phi_+\rangle$ has Schmidt decomposition

$$|\phi\rangle = \sum_j \mu_j |c_j\rangle |d_j\rangle. \tag{A2}$$

with $\mu_{2l}=\mu_{2l+1}$. For concreteness, we may assume that the λ_j's and μ_j's are both in decreasing order

We first show that we may take $|c_j\rangle=|a_j\rangle$ and $|d_j\rangle=|b_j\rangle$. Note that

$$|\langle\psi|\phi\rangle| \leq \sum_{jk} \lambda_j \mu_k |\langle a_j|c_k\rangle||\langle b_j|d_k\rangle|. \tag{A3}$$

Let us define the matrix M by

$$M_{jk} = |\langle a_j|c_k\rangle||\langle b_j|d_k\rangle|. \tag{A4}$$

The values $|\langle a_j|b_k\rangle|$ for various k and fixed j form a vector of norm 1 since $|b_k\rangle$ is a basis and $|a_j\rangle$ has norm 1. The same is true for the values $|\langle b_j|d_k\rangle|$ and if we fix k and vary j instead. Thus, columns (and rows) of M are formed by entrywise products of norm 1 vectors and the sum of each row and column of M is at most 1. This means that we can find a new matrix N with positive entries such that $M+N$ is doubly stochastic. Note that

$$|\langle\psi|\phi\rangle| \leq \sum_{jk} \lambda_j \mu_k (M+N)_{jk}. \tag{A5}$$

By the Birkhoff–von Neumann theorem, we may write $M+N$ as a convex combination of permutation matrices, thus

$$M + N = \sum_m p_m P_m, \tag{A6}$$

with $\Sigma_m p_m=1$ and P_m permutation matrices. Since the combination is convex, there exists some m for which

$$|\langle\psi|\phi\rangle| \leq \sum_{jk} \lambda_j \mu_k (P_m)_{jk}. \tag{A7}$$

The permutations merely reorder the μ_j's and it is easy to prove that the maximum is achieved when the λ_j's and μ_j's are both in decreasing order. Hence, $P_m=I$ satisfies the above equation. We may achieve this by choosing the bases $|c_j\rangle=|a_j\rangle$ and $|d_j\rangle=|b_j\rangle$, so we need not consider any other bases.

We now optimize over μ_j subject to the condition $\mu_{2l}=\mu_{2l+1}$. By the Cauchy-Schwarz inequality, we have

$$\begin{aligned}|\langle\psi|\phi\rangle|^2 &= \left(\sum_l (\lambda_{2l}+\lambda_{2l+1})\mu_{2l}\right)^2 \\ &\leq \left(\sum_l (\lambda_{2l}+\lambda_{2l+1})^2\right)\left(\sum_l \mu_{2l}^2\right),\end{aligned} \tag{A8}$$

with equality when the vectors $(\lambda_{2l}+\lambda_{2l+1})_1$ and $(\mu_{2l})_1$ are collinear. Thus we set

$$\mu_{2l} = \mu_{2l+1} = \frac{\lambda_{2l}+\lambda_{2l+1}}{N}, \tag{A9}$$

with N a normalization constant equal to

$$N = \sqrt{2\sum_l (\lambda_{2l}+\lambda_{2l+1})^2}. \tag{A10}$$

With these values, we obtain

$$F_{\mathrm{MY}}(|\psi\rangle) = |\langle\psi|\phi\rangle|^2 = \sum_l \frac{(\lambda_{2l}+\lambda_{2l+1})^2}{2}. \tag{A11}$$

APPENDIX B: PROOF OF $F_{\mathrm{MY}} \leq F_{\mathrm{LO}}$ WITH EQUALITY FOR PURE STATES

Let ρ be given. Then,

$$F_{\mathrm{LO}}(\rho) = \max_{\Phi\in\mathrm{LO}} F(\Phi(\rho), |\phi_+\rangle\langle\phi_+|) \tag{B1}$$

with LO the set of local operations that take the space AB to a pair of qubits. We may restrict this set to operations which only apply local unitaries and trace out everything but a pair of qubits to obtain

$$F_{\mathrm{LO}}(\rho) \geq \max_{U,V} F(\mathrm{tr}_X(U\otimes V\rho U^\dagger \otimes V^\dagger), |\phi_+\rangle\langle\phi_+|), \tag{B2}$$

where tr_X means tracing out everything but a pair of qubits. Since fidelity only increases when a system is traced out, we have

$$F_{\mathrm{LO}}(\rho) \geq \max_{U,V} F(U\otimes V\rho U^\dagger \otimes V^\dagger, |\phi\rangle\langle\phi| \otimes |\phi_+\rangle\langle\phi_+|) \tag{B3}$$

for all $|\phi\rangle$ and in particular for the $|\phi\rangle$ which maximizes the expression and gives $F_{\mathrm{MY}}(\rho)$. Thus,

$$F_{\mathrm{LO}}(\rho) \geq F_{\mathrm{MY}}(\rho). \tag{B4}$$

Now suppose that $\rho = |\psi\rangle\langle\psi|_{AB}$. We may write an operation in LO as adding a pair of ancillas and a pair of target qubits, applying a pair of unitaries, and tracing out everything but the target qubits. Thus,

$$\begin{aligned} F_{\mathrm{LO}}(|\psi\rangle) = \max_{U,V} F(&\mathrm{tr}_{ABX_aX_b}(U \otimes V|\psi\rangle_{AB}|00\rangle_{X_aX_b}|00\rangle_{Y_aY_b}), \\ &|\phi_+\rangle\langle\phi_+|_{Y_aY_b}). \end{aligned} \tag{B5}$$

Applying Uhlmann's theorem, we obtain

$$\begin{aligned} F_{\mathrm{LO}}(|\psi\rangle) = \max_{U,V,|\phi\rangle} &|\langle\psi|_{AB}\langle 00|_{X_aX_b}\langle 00|_{Y_aY_b}U^\dagger \otimes V^\dagger|\phi\rangle \\ &\otimes |\phi_+\rangle_{Y_aY_b}|^2. \end{aligned} \tag{B6}$$

The right-hand side is equal to $F_{\mathrm{MY}}(|\psi\rangle \otimes |00\rangle \otimes |00\rangle)$ by definition. This in turn is equal to $F_{\mathrm{MY}}(|\psi\rangle)$ since the value of F_{MY} for a pure state is only dependent on the Schmidt decomposition, which the product state ancillas do no change. Thus,

$$F_{\mathrm{LO}}(|\psi\rangle) = F_{\mathrm{MY}}(|\psi\rangle). \tag{B7}$$

For mixed states, there exist cases with a strict inequality. For example, $F_{\mathrm{MY}}(\frac{I}{4}) = \frac{1}{4}$, but $F_{\mathrm{LO}}(\frac{I}{4}) = \frac{1}{2}$ since the class LO allows us to replace the state with $|00\rangle$.

APPENDIX C: PROOF OF THE LOWER BOUND FOR F_{LO}

Here we prove the bound on F_{LO} Eq. (19). The definition of F_{LO} is

$$F_{\mathrm{LO}} = \max_{M_k,N_l} \sum_{k,l} \mathrm{Tr}[M_k \otimes N_L \rho M_k^\dagger \otimes N_l^\dagger \mathbf{\Phi}^+],$$

$$M_k : H_A \to \mathbb{C}^2; \quad \sum_k M_k^\dagger M_k = \mathbb{1}_A,$$

$$N_l : H_B \to \mathbb{C}^2; \quad \sum_l N_l^\dagger N_l = \mathbb{1}_B, \tag{C1}$$

where $\{M_k\}$ ($\{N_l\}$) are completely positive (CP) maps from Alice (Bob's) system to two-dimensional spaces. In general, $\{M_k\}$ and $\{N_l\}$ will depend on ρ.

We will explicitly describe CP maps that achieve Eq. (19), thereby showing that it is a lower bound for F_{LO}. This bound is certainly not tight. This can be seen by the construction we use since the CP maps depend on the measurement operators $\hat{A}$, $\hat{A}'$, $\hat{B}$, and $\hat{B}'$ but not on the state ρ itself. Thus the CP maps do not use all the available information and cannot not be optimal.

The CP maps are constructed as follows:

(1) The operators $\hat{A}$, $\hat{A}'$ (and $\hat{B}$, $\hat{B}'$) are block diagonal, where each block is a 2×2 matrix. We use the projectors $\Pi_\alpha \otimes \Pi_\beta$ to project onto these blocks, obtaining states $\rho_{\alpha\beta}$ with probability $p_{\alpha\beta}$. The Bell operator in block (α,β) has expectation $S(\rho_{\alpha\beta})$.

(2) If $S(\rho_{\alpha\beta}) \leq 2$, then $F \geq 0$. In this case, do nothing.

(3) If $S(\rho_{\alpha\beta}) > 2$, then carry out local rotations, such that after the rotations, the measurements look like

$$\hat{A} = \cos aZ + \sin aX,$$

$$\hat{A}' = \sin aZ + \cos aX,$$

$$|a| \leq \frac{\pi}{4} \tag{C2}$$

and

$$\begin{aligned} \hat{B} &= \cos\left(\frac{\pi}{4} + b\right)X + \sin\left(\frac{\pi}{4} + b\right)Z \\ &= \frac{1}{\sqrt{2}}(\cos b - \sin b)X + \frac{1}{\sqrt{2}}(\cos b + \sin b)Z, \end{aligned}$$

$$\begin{aligned} \hat{B}' &= -\cos\left(\frac{\pi}{4} + b\right)X + \sin\left(\frac{\pi}{4} + b\right)Z \\ &= -\frac{1}{\sqrt{2}}(\cos b - \sin b)X + \frac{1}{\sqrt{2}}(\cos b + \sin b)Z, \end{aligned}$$

$$|b| \leq \frac{\pi}{4}. \tag{C3}$$

The idea of the final rotations is that the operators $\hat{A}$, $\hat{A}'$ (and $\hat{B}$, $\hat{B}'$) define local bases and we rotate the state so that these bases are aligned with the local bases defined by the state $\mathbf{\Phi}^+$.

Note that as both the fidelity and the CHSH violation are linear functions of the density matrix ρ, we can restrict ourselves to pure states. Furthermore, because of the linearity of S and F, we can focus on one block (α,β). Taking the concave hull will yield the set of accessible points. From now on, we drop the indices α,β.

Using Eqs. (C2) and (C3), the Bell operator takes the form

$$\begin{aligned} \hat{B} = \sqrt{2}[&\cos a \cos b(ZZ + XX) + \cos a \sin b(ZZ - XX) \\ &+ \sin a \cos b(ZX + XZ) + \sin a \sin b(-ZX + XZ)]. \end{aligned}$$

The eigenvectors of $\hat{B}$ are denoted $|\Phi_i\rangle$ and its eigenvectors are $\lambda_1, \lambda_2, -\lambda_2, -\lambda_1$ where $0 \leq \lambda_2 \leq 2 \leq \lambda_1 \leq 2\sqrt{2}$. Explicitly, we have

$$\begin{aligned} \lambda_1(a,b) &= 2\sqrt{1 + \cos 2a \cos 2b} \\ &= 2\sqrt{2}\sqrt{\cos^2 a \cos^2 b + \sin^2 a \sin^2 b}, \end{aligned}$$

$$\lambda_2(a,b) = 2\sqrt{1 - \cos 2a \cos 2b}. \tag{C4}$$

The fidelities of the eigenvectors with the $|\Phi^+\rangle$ state are $f_i = |\langle\Phi^+|\Phi_i\rangle|^2$. One finds

$$f_2 = f_3 = 0,$$

$$f_1 + f_4 = 1,$$

$$\Delta f = f_1 - f_4 = \frac{2\sqrt{2}\cos a \cos b}{\lambda_1(a,b)}. \qquad \text{(C5)}$$

The pure state on which the measurements are carried out can be written in the basis $|\Phi_i\rangle$ as

$$|\psi\rangle = c_1|\Phi_1\rangle + c_2|\Phi_2\rangle + c_3|\Phi_3\rangle + c_4|\Phi_4\rangle.$$

The expectation of CHSH is

$$\langle\hat{B}\rangle = S = (|c_1|^2 - |c_4|^2)\lambda_1 + (|c_2|^2 - |c_3|^2)\lambda_2$$

and the fidelity is

$$F = |c_1\sqrt{f_1} + c_4\sqrt{f_4}|^2$$

(where we take the $\sqrt{f_1}$ and $\sqrt{f_4}$ to be the positive square roots of f_1 and f_4).

Note that these expressions would be unchanged if we had a mixture of $|\Phi\rangle_2$, $|\Phi\rangle_3$, and $c_1|\Phi\rangle_1 + c_4|\Phi\rangle_4$. Henceforth, we consider such a mixture. If the state is of the form $|\psi\rangle = |\Phi\rangle_3$ or of the form $|\psi\rangle = |\Phi\rangle_2$, then $S \leq 2$ and therefore, trivially, $F \geq 0$.

We now concentrate on the nontrivial case $|\psi\rangle = c_1|\Phi\rangle_1 + c_4|\Phi\rangle_4$ and $2 < S \leq 2\sqrt{2}$. We will show that in this case

$$\frac{1}{2} + \frac{S}{4\sqrt{2}} \leq F \leq 1. \qquad \text{(C6)}$$

Note that Eq. (C6) and the preceding arguments give us the extremal points in the (S,F) plane we were searching for. Taking the concave hull yields Eq. (19). The concave hull can be attained by taking the angles $a=b=0$ and as state a mixture of $|\phi^+\rangle$ (which has $F=1$ and $S=2\sqrt{2}$ and of $|\Phi_2\rangle$ which has $F=0$ and $S=2$).

Proof of Eq. (C6). To prove Eq. (C6), this recall that $F = |c_1\sqrt{f_1} + c_4\sqrt{f_4}|^2$ and $S = (|c_1|^2 - |c_4|^2)\lambda_1$. We can view $F = |\vec{v}\cdot\vec{w}|^2$ as the scalar product of two vectors $\vec{v} = (c_1, c_4)$ and $\vec{w} = (\sqrt{f_1}, \sqrt{f_4})$. Our argument will be to fix S and to minimize F.

For fixed S, a, and b, the minimum of F is obtained when

$$c_1 = +\sqrt{\frac{1}{2} + \frac{S}{2\lambda_1}}, \quad c_4 = -\sqrt{\frac{1}{2} - \frac{S}{2\lambda_1}}. \qquad \text{(C7)}$$

From now on, we take c_1, c_4 to have this form.

We can then write

$$F = \left(\sqrt{\frac{1}{2} + \frac{S}{2\lambda_1}}\sqrt{\frac{1}{2} + \frac{\Delta f}{2}} - \sqrt{\frac{1}{2} - \frac{S}{2\lambda_1}}\sqrt{\frac{1}{2} - \frac{\Delta f}{2}}\right)^2. \qquad \text{(C8)}$$

From now on, our aim is to choose the measurement angles a, b that minimize Eq. (C8) for fixed S.

First, let us keep S and λ_1 fixed. Then F is minimum when Δf is minimized. We show that this occurs when $|a| = |b|$.

Proof. We consider the (a,b) plane. The vector

$$\vec{n} = (-\cos a \sin a(\cos^2 b - \sin^2 b), \\ -\cos b \sin b(\cos^2 a - \sin^2 a))$$

is normal to the surfaces $\lambda_1 = \text{const}$ and the vector

$$\vec{t} = (\cos b \sin b(\cos^2 a - \sin^2 a), \\ -\cos a \sin a(\cos^2 b - \sin^2 b))$$

is tangent to the surfaces $\lambda_1 = \text{const}$.

Recall Eq. (C5). It then follows that $\vec{t}\cdot(-\sin a \cos b, -\cos a \sin b) = \sin a \sin b(\sin^2 a \cos^2 b - \cos^2 a \sin^2 b)$ is proportional to the change of Δf along the surfaces $\lambda_1 = \text{const}$. Analyzing this function, one finds that the minimum of Δf occurs when $|a| = |b|$. End of proof.

We can thus replace $|a| = |b|$ in Eq. (C8). Then when $S > 2$, the minimum of F occurs when $a = b = 0$. Replacing $a = b = 0$ in Eq. (C8), this is equivalent to proving that when $|a| = |b|$, $F \geq \frac{1}{2} + \frac{S}{4\sqrt{2}}$.

Proof. We use Eq. (C8) to rewrite the inequality $F \geq \frac{1}{2} + \frac{S}{4\sqrt{2}}$ as

$$\frac{1}{2} + \frac{S\Delta f}{2\lambda_1} - 2\sqrt{\frac{1}{4} - \frac{S^2}{4\lambda_1^2}}\sqrt{\frac{1}{4} - \frac{\Delta f^2}{4}} \geq \frac{1}{2} + \frac{S}{4\sqrt{2}}, \qquad \text{(C9)}$$

which we reorganize as

$$\frac{S\Delta f}{2\lambda_1} - \frac{S}{4\sqrt{2}} \geq 2\sqrt{\frac{1}{4} - \frac{S^2}{4\lambda_1^2}}\sqrt{\frac{1}{4} - \frac{\Delta f^2}{4}}. \qquad \text{(C10)}$$

Both the left-hand side and the right-hand side are positive (since it is easily checked that $\Delta f / S_1 \geq 1/2\sqrt{2}$). Hence, this inequality is equivalent to its square, which gives

$$-\frac{S^2\Delta f}{\sqrt{2}\lambda_1} + \frac{S^2}{8} \geq 1 - \Delta f^2 - \frac{S^2}{\lambda_1^2}. \qquad \text{(C11)}$$

Reorganizing terms yields

$$\frac{2(\cos a^2 - 1)^2(S^2 - 4)}{\lambda_1^2} \geq 0, \qquad \text{(C12)}$$

which is manifestly true when $S \geq 2$. End of proof.

End of proof of Eq. (C6).

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

[2] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[3] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[4] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008).

[5] T. Vértesi and K. F. Pál, Phys. Rev. A **79**, 042106 (2009).

[6] J. Briet, H. Buhrman, and B. Toner, e-print arXiv:0901.2009.

[7] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).

[8] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier, in *Self-testing of Quantum Circuits, Proceedings of ICALP2006, Part I*, edited by M. Bugliesi *et al.*, Lecture Notes in Computer Science 4051 (Springer, Berlin, 2006), pp. 72–83.

[9] A. Fine, Phys. Rev. Lett. **48**, 291 (1982).

[10] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).

[11] S. Popescu and D. Rohrlich, Phys. Lett. A **169**, 411 (1992).

[12] C. A. Fuchs and J. van der Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, London, 2000), Chap. 9.

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

[15] V. Scarani and N. Gisin, J. Phys. A **34**, 6043 (2001).

[16] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).

[17] R. F. Werner and M. M. Wolf, Quantum Inf. Comput. **1**(3), 1 (2001).

[18] R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **200**, 340 (1995).

[19] N. Gisin and A. Peres, Phys. Lett. A **162**, 15 (1992).

[20] Y.-C. Liang and A. C. Doherty, Phys. Rev. A **73**, 052116 (2006).

[21] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).