



Device-Independent Certification of Entangled Measurements

Rafael Rabelo,¹ Melvyn Ho,¹ Daniel Cavalcanti,¹ Nicolas Brunner,² and Valerio Scarani^{1,3}

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

²*H. H. Wills Physics Laboratory, University of Bristol, Bristol, BS8 1TL, United Kingdom*

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

(Received 16 May 2011; published 25 July 2011)

We present a device-independent protocol to test if a given black-box measurement device is entangled, that is, has entangled eigenstates. Our scheme involves three parties and is inspired by entanglement swapping; the test uses the Clauser-Horne-Shimony-Holt Bell inequality, checked between each pair of parties. In the case where all particles are qubits, we characterize quantitatively the deviation of the measurement device from a perfect Bell-state measurement.

DOI: 10.1103/PhysRevLett.107.050502

PACS numbers: 03.67.Mn, 03.65.Ud, 03.65.Wj

Introduction.—The concept of device-independent information processing relies on performing reliable information tasks on untrustworthy apparatuses. This idea first showed its importance in quantum key distribution, where security and privacy could be tested and assured even in the hypothetical case that the cryptographic devices are provided by some malevolent third party [1–3]. Other tasks were also generalized to the device-independent scenario, such as random number generation [4] and quantum state estimation [5], the latter starting an alternative approach to self-testing [6].

Recently, the task of testing if a measurement device that acts on a bipartite quantum system is *entangled*, that is, if at least one of its eigenstates is not separable (or, more generally, its positive operator-valued measure elements do not factor in the subsystems), was introduced [7]. However, their solution is not device-independent, since further assumptions are required. Here, we present a device-independent realization of this task.

Specifically, in order to show that a measurement is entangled, we are going to assess that it is *entangling* in an entanglement swapping scenario [8]. Suppose A and B are initially not entangled; rather, A is initially entangled with a system C_A and B with a system C_B . Then, if a measurement on $C_A - C_B$ creates entanglement between A and B , that measurement was entangled. To perform a device-independent test means that we cannot *assume* this scenario, but rather, we want to *certify a posteriori* that swapping has indeed happened. Entanglement is checked in a device-independent way using Bell's inequalities. Here we shall use only the Clauser-Horne-Shimony-Holt (CHSH) inequality

$$S = E_{11} + E_{12} + E_{21} - E_{22}, \quad (1)$$

where $E_{xy} = p(a = b|x, y) - p(a \neq b|x, y)$ and $p(a, b|x, y)$ is the probability of getting results a and b given that measurements x and y were performed.

It is important to stress that the only assumption that may go into our test is the existence of two clearly defined

subsystems in Charlie's hands (we shall see later that it can be considered very natural in some implementations and that it can be entirely dispensed with in the idealized cases that we study below). No other assumption needs to be made: For instance, the state could be of arbitrary Hilbert space dimension and could be entangled along any partition.

Protocol.—For each run, Alice chooses at random one out of two measurements A_1 or A_2 with binary outcome $a_i \in \{-1, +1\}$; Bob, one of two measurements B_1 or B_2 , also with binary outcome $b_j \in \{-1, +1\}$; and Charlie, one out of three measurements C_1 , C_2 , or C_3 , with four outcomes $c_k \in \{1, 2, 3, 4\}$. The goal is to *guarantee that C_3 is an entangled measurement*.

On the statistics resulting from a large number of repetitions, the following tests are performed: (i) The cases where Charlie has measured C_1 or C_2 are used to test the CHSH inequality both with Alice (S_{AC}) and with Bob (S_{BC}). For this, Charlie has to define a classical processing that transforms his four outcomes into two bits, one to be correlated with Alice and one with Bob. (ii) When Charlie has measured C_3 , Alice and Bob check the CHSH inequality among themselves, obtaining four numbers $S_{AB|c_3}$ conditioned on the result c_3 obtained by Charlie:

$$\begin{aligned} S_{AB|1} &= -S_{AB|4} = E_{11} + E_{12} + E_{21} - E_{22}, \\ S_{AB|2} &= -S_{AB|3} = E_{11} + E_{12} - E_{21} + E_{22}. \end{aligned} \quad (2)$$

Note that Alice and Bob do not need to know c_3 in each run, since their measurement settings are always the same. The statistics (2) can be checked at the end of the whole experiment. The setup is sketched in Fig. 1.

Now we are going to show that this protocol can lead to a device-independent test of the fact that C_3 is entangled. On the one hand, notice that in quantum physics it is possible to achieve

$$S_{AC} = S_{BC} = S_{AB|c_3} = 2\sqrt{2} \quad \forall c_3 \in \{1, 2, 3, 4\} \quad (3)$$

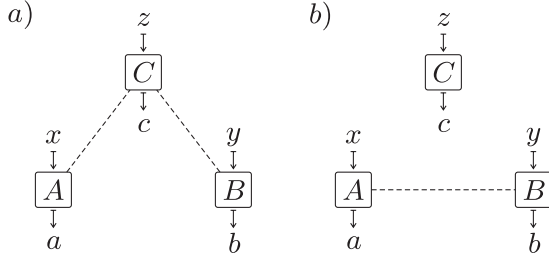


FIG. 1. The scenario consists of three parties A , B , and C , spacelike separated, each holding a black-box device that performs measurements on quantum systems. The protocol is divided into two parts: (a) parties AC and BC evaluate the CHSH inequality, considering measurements $z = 1, 2$ are performed on party C ; (b) given that party C performed measurement $z = 3$, parties AB evaluate the CHSH inequality corresponding to the result c .

already in a four-qubit scenario. The system is prepared in the state $|\Phi^+\rangle_{AC_A} \otimes |\Phi^+\rangle_{BC_B}$. Alice's and Bob's measurements are $A_1 = Z$, $A_2 = X$, $B_1 = (Z + X)/\sqrt{2}$, and $B_2 = (Z - X)/\sqrt{2}$. Charlie's measurements are $C_1 = (Z + X)/\sqrt{2} \otimes Z$ and $C_2 = (Z - X)/\sqrt{2} \otimes X$, and C_3 is the Bell-state measurement, in which outcome $c_3 \in \{1, 2, 3, 4\}$ indicates the projection on one of the Bell states $|\Phi_1\rangle = |\Phi^+\rangle$, $|\Phi_2\rangle = |\Phi^-\rangle$, $|\Phi_3\rangle = |\Psi^+\rangle$, or $|\Phi_4\rangle = |\Psi^-\rangle$.

On the other hand, the observation that either S_{AC} or S_{BC} is *exactly* $2\sqrt{2}$ guarantees in a device-independent way that (i) ρ_{AB} is separable and (ii) Charlie's system can be seen as composite of two subsystems. Indeed, if (say) $S_{AC} = 2\sqrt{2}$, up to local isometries the tripartite state is $\Phi_{AC} \otimes \rho_{A'BC'}$, where $\Phi = |\Phi^+\rangle\langle\Phi^+|$, while A' and C' represent additional degrees of freedom of Alice and Charlie that may even be entangled among themselves and with Bob's system but are not involved in the measurements [9–11]. So, Charlie has two uncorrelated subsystems C and C' . Moreover, if $S_{AB|c_3} > 2$ is observed for any value of c_3 , then $\rho_{AB|c_3}$ must be entangled, which is possible only if C_3 is an entangling measurement given that ρ_{AB} is separable.

In summary, we have shown that

$$(S_{AC} = 2\sqrt{2} \text{ or } S_{BC} = 2\sqrt{2}) \text{ and } S_{AB|c_3} > 2 \Rightarrow C_3 \text{ is entangling and entangled.} \quad (4)$$

This is a device-independent result since only the monogamy induced by the maximal CHSH violation plays a role, without any *a priori* assumption on the state, the Hilbert space dimension, or the measurements.

The criterion (4) can be sharpened by exploiting both S_{AC} and S_{BC} . The idea is that the value of S provides information on the commutator between the two local measurements of each party; so, S_{AC} and S_{BC} constrain $[A_0, A_1]$ and $[B_0, B_1]$, respectively. In turn, something can be inferred on the Bell operator \mathcal{B}_{AB} , which determines the

maximal violation achievable with separable states. Indeed, we can prove that

$$(S_{AC} = 2\sqrt{2} \text{ and } S_{BC} = 2\sqrt{2}) \text{ and } S_{AB|c_3} > \sqrt{2} \rightarrow C_3 \text{ is entangled.} \quad (5)$$

Here is a sketch of the proof (see the appendix for details): One first shows that the first two conditions force the four Bell operators $\mathcal{B}_{AB|c_3}$ to have $2\sqrt{2}$ as the eigenvalue; then, given such an operator, one shows that separable states can reach only the value $\sqrt{2}$, thus generalizing to the device-independent scenario an observation made in earlier works assuming qubits [12].

We have been able to derive only quantitative criteria that rely on at least one between S_{AC} and S_{BC} being exactly $2\sqrt{2}$. The task of relaxing this constraint is left for future work: the main difficulty arising from the fact that, even for the smallest deviation from the ideal values, ρ_{AB} cannot be guaranteed to be separable anymore [13]. Similarly, one cannot guarantee anymore, in a device-independent way, that Charlie has two subsystems: As we mentioned above, this is an assumption that must be made. This assumption may, however, be very natural in some implementations, in which Charlie receives one quantum signal from Alice and one from Bob.

Characterizing a specific measurement.—In the previous section, we have contented ourselves with trying to assess whether the measurement C_3 is entangling and/or entangled or not. However, the protocol that we defined can lead to a much finer statement. Indeed, if one is close to satisfying (3), the measurement C_3 is close to an ideal Bell-state measurement. It should therefore be possible to bound the distance t between the actual and the ideal measurement as a function of the observed violations. The derivation of this bound in a full device-independent scenario, $t \leq f_{DI}(S)$, hits the same difficulties as those encountered in the simpler task of state estimation [5]. Here, we introduce additional assumptions and obtain a bound $t \leq f(S)$. Since obviously $f(S) \leq f_{DI}(S)$, we can conclude that a device-independent estimate of t will be *at least as bad as* $f(S)$.

We go back to the four-qubit scenario described after Eq. (3), and we keep everything as there, except for the measurement C_3 : This is no longer a perfect Bell-state measurement but is still assumed to be projective. One does not know *a priori* which state to associate with each result c_3 ; however, once the measured data have been sorted out according to c_3 , one can check all four versions (2) of the CHSH inequality and associate to each value of c_3 the version that leads to the maximal violation. This amounts to possibly relabeling the outcomes so that the eigenstate $|e_c\rangle$ is the closest to $|\Phi_c\rangle$ for each $c \in \{1, 2, 3, 4\}$. We assume this to be the case from now on.

An operational measure of the distance between C_3 and an ideal Bell-state measurement is the trace distance

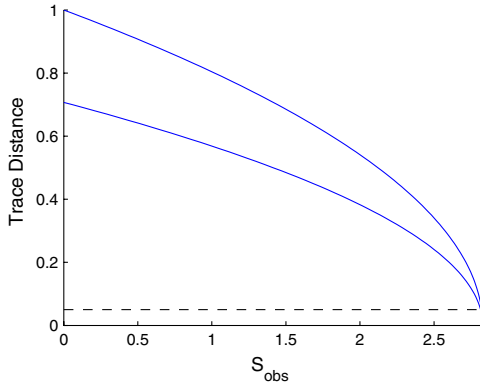


FIG. 2 (color online). In the four-qubit scenario we consider the value of $S_{AB|c}$ as a device-assessment criterion, where the blue lines show the bounds on the trace distance of the measurement device. The violation $S_{\text{obs}} \geq 2.8214$ guarantees the trace distance of the measurement device to be at most 5% from the ideal, as shown by the dashed line.

$$t = \max_c \sqrt{1 - |\langle e_c | \Phi_c \rangle|^2}. \quad (6)$$

This figure of merit represents the worst-case scenario, since we are not specifying in which task the entangled measurement is going to be used after the check.

Now, because of the choice of the local measurements of Alice and Bob, the Bell operators corresponding to the four inequalities (2) read $\mathcal{B}_{AB|c} = 2\sqrt{2}(\Phi_c - \Phi_{5-c})$, where $\Phi_k = |\Phi_k\rangle\langle\Phi_k|$. Therefore

$$S_{AB|c} = 2\sqrt{2}(|\langle e_c | \Phi_c \rangle|^2 - |\langle e_c | \Phi_{(5-c)} \rangle|^2), \quad (7)$$

and the two bounds $0 \leq |\langle e_c | \Phi_{(5-c)} \rangle|^2 \leq 1 - |\langle e_c | \Phi_c \rangle|^2$ lead finally to

$$\sqrt{\frac{1}{2} \left(1 - \max_c \frac{S_{AB|c}}{2\sqrt{2}} \right)} \leq t \leq \sqrt{1 - \min_c \frac{S_{AB|c}}{2\sqrt{2}}}. \quad (8)$$

In particular, the upper bound is the expression $f(S)$ we were looking for, and it indicates how stringent are the requirements for device-independent assessment of a measurement. Recall that the trace distance is also the probability of distinguishing the real case from the ideal one [14]. Requesting that this probability is 5% looks like a pretty loose requirement; but, in order to confirm this assessment in a device-independent way, one will have observe at least $\min_c S_{AB|c} \geq 2.8214$ (Fig. 2). This number is within 0.5% of the maximal value: No experiment has reached such a high violation and precision, even leaving aside that we are considering an entanglement swapping experiment.

Conclusion.—We have presented a proposal for a device-independent test of an entangled measurement. Our proposal requires the use of three parties in an entanglement swapping scenario. There are several extensions and open problems which follow from our Letter.

In particular, our quantitative results rely on the fact that either Alice or Bob violate the CHSH inequality maximally with Charlie; it will be necessary to extend these results to less idealized situations.

One may also wonder if our tripartite scenario is the simplest one. While we do not have a definite answer, we conjecture that it would be impossible to achieve this task in a scenario involving only two parties.

This work was supported by the National Research Foundation and the Ministry of Education, Singapore, and by the United Kingdom EPSRC. We thank the non-local club of CQT and N. Gisin, M. Navascués, S. Pironio, and T. Vértesi for discussions.

Appendix.—Given any two Hermitian operators A_0 and A_1 , with eigenvalues ± 1 , acting on a Hilbert space \mathcal{H} , there is a decomposition of \mathcal{H} into a direct sum of subspaces \mathcal{H}_i such that $\dim(\mathcal{H}_i) \leq 2 \forall i$ and both A_0 and A_1 act within each \mathcal{H}_i , i.e., $\forall |\psi\rangle \in \mathcal{H}_i, A_0|\psi\rangle, A_1|\psi\rangle \in \mathcal{H}_i$ [15]. Thus, the operators A_0 and A_1 can always be written as $A_0 = \sum_i \Pi_i A_0 \Pi_i$ and $A_1 = \sum_i \Pi_i A_1 \Pi_i$, respectively, where Π_i are projectors onto subspaces \mathcal{H}_i . As a consequence, any CHSH operator β acting on the Hilbert space of a 2-qudit system, $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$, can be decomposed into a direct sum of CHSH operators $\beta_{i,j}$, each acting on a 2-qubit subspace $\mathcal{H}_{i,j}$ [16]; that is,

$$\beta = \oplus_{i,j} \beta_{i,j} = \sum_{i,j} (\Pi_i \otimes \Pi_j) \beta (\Pi_i \otimes \Pi_j). \quad (9)$$

To evaluate $S_{\text{Sep}} = \max_{\{\rho \in \mathcal{S}\}} \text{Tr}(\rho \beta)$, where \mathcal{S} is the set of separable states, we first note that, since the trace is linear and \mathcal{S} is a convex set, the maximum is attained over the subset of extremal points. Hence, it suffices to consider the set of pure product states \mathcal{P} . Now, using (9) we have

$$\begin{aligned} S_{\text{Sep}} &= \max_{\{|\phi\rangle \in \mathcal{P}\}} \langle \phi | \beta | \phi \rangle = \max_{\{|\phi\rangle \in \mathcal{P}\}} \langle \phi | \oplus_{i,j} \beta_{i,j} | \phi \rangle \\ &= \max_{\{|\phi_{i,j}\rangle \in \mathcal{P}\}} \sum_{i,j} p_{i,j} \langle \phi_{i,j} | \beta_{i,j} | \phi_{i,j} \rangle, \end{aligned} \quad (10)$$

where $|\phi_{i,j}\rangle = (\Pi_i \otimes \Pi_j) |\phi\rangle / \sqrt{p_{i,j}}$ and $p_{i,j} = \langle \phi | (\Pi_i \otimes \Pi_j) | \phi \rangle$. By convexity, the above expression is upper bounded by the largest mean value among the 2-qubit Bell operators $\beta_{i,j}$ attained by 2-qubit pure product states:

$$\begin{aligned} S_{\text{Sep}} &= \max_{\{|\phi_{i,j}\rangle \in \mathcal{P}\}} \sum_{i,j} p_{i,j} \langle \phi_{i,j} | \beta_{i,j} | \phi_{i,j} \rangle \\ &\leq \sum_{i,j} p_{i,j} \max_{\{|\phi_{i,j}\rangle \in \mathcal{P}\}} \langle \phi_{i,j} | \beta_{i,j} | \phi_{i,j} \rangle \\ &\leq \max_{\{|\phi\rangle \in \mathcal{P}, (i,j)\}} \langle \phi | \beta_{i,j} | \phi \rangle. \end{aligned} \quad (11)$$

According to Ref. [17], the spectral decomposition of any 2-qubit CHSH operator is, up to local unitaries, $\beta = \sum_{i=1}^4 \alpha_i |\Phi_i\rangle\langle\Phi_i|$, where the eigenvectors $|\Phi_i\rangle$ are Bell states and the eigenvalues are functions of the local observables, with $\alpha_1 = -\alpha_3$, $\alpha_2 = -\alpha_4$, and $\alpha_1^2 + \alpha_2^2 = 8$. Let $\alpha_{i,j}$ be the largest eigenvalue of $\beta_{i,j}$. Thus we have

$$\begin{aligned}
S_{\text{Sep}} &= \max_{\{|\phi\rangle \in \mathcal{P}, (i,j)\}} \langle \phi | \beta_{i,j} | \phi \rangle \\
&= \max_{\{|\phi\rangle \in \mathcal{P}, (i,j)\}} \alpha_{i,j} [|\langle \phi | \Phi_1 \rangle|^2 - |\langle \phi | \Phi_3 \rangle|^2] \\
&\quad + \sqrt{8 - \alpha_{i,j}^2} [|\langle \phi | \Phi_2 \rangle|^2 - |\langle \phi | \Phi_4 \rangle|^2]. \quad (12)
\end{aligned}$$

Without loss of generality, we do not consider the local unitaries in the spectral decomposition of β since they can be absorbed into the states $|\phi\rangle$. The largest overlap between a pure product state and a Bell state is $1/2$; thus, we have $S_{\text{Sep}} = \max_{\{(i,j)\}} (\alpha_{i,j} + \sqrt{8 - \alpha_{i,j}^2})/2$.

Note that $\alpha_{i,j} \geq 2$ for all (i,j) . This is because the largest eigenvalue α of β is given by the positive square root of the largest eigenvalue of β^2 , which is lower bounded by 2 [18]. We observe that the above function decreases as α increases. This way, the maximum is attained for the subspace (i,j) such that $\alpha_{i,j}$ is minimum. Then, defining λ as the smallest eigenvalue of β such that $\lambda \geq 2$, we have

$$S_{\text{Sep}} = \frac{\lambda + \sqrt{8 - \lambda^2}}{2}. \quad (13)$$

This generalizes to all dimensions the results of Ref. [12].

Theorem.—If $S_{AC} = S_{BC} = 2\sqrt{2}$, and C_3 is a separable measurement, then $S_{AB|C_3} \leq \sqrt{2}$.

Proof of theorem.—As previously stated, if $S_{AC} = S_{BC} = 2\sqrt{2}$, then, for all subspaces $(i,j)_{AC}$ and $(k,l)_{BC}$ where the initial states shared by parties AC and BC have support, the states are (up to local isometries) maximally entangled and are completely uncorrelated from any other system. Thus, any state steered by measurement C_3 —assuming it is separable—to parties AB will be a product and will have support at most of the same subspaces of \mathcal{H}_A and \mathcal{H}_B where the initial states have support. Moreover, implicit in $S_{AC} = S_{BC} = 2\sqrt{2}$ is the statement that in every subspace $(i,j)_{AC}$ and $(k,l)_{BC}$ where the initial states have support the CHSH operators $\beta_{i,j}$ and $\beta_{k,l}$ have maximal eigenvalues $\alpha_{i,j} = \alpha_{k,l} = 2\sqrt{2}$. This immediately implies that, for the same subspaces, the CHSH operators in parties AB , $\beta_{i,k}$, will also have maximal eigenvalues $\alpha_{i,k} = 2\sqrt{2}$; this follows from Ref. [18].

Thus, we conclude that for all subspaces (i,k) where the final steered (separable) state for AB has support the

2-qubit CHSH operators have the maximum eigenvalue $2\sqrt{2}$. Hence, from (13), we finally get

$$S_{AB|C_3} \leq \sqrt{2}. \quad (14)$$

-
- [1] A. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [2] A. Acín *et al.*, *Phys. Rev. Lett.* **98**, 230501 (2007).
 - [3] S. Pironio *et al.*, *New J. Phys.* **11**, 045021 (2009); L. Masanes, S. Pironio, and A. Acín, *Nature Commun.* **2**, 238 (2011); E. Hänggi and R. Renner, [arXiv:1009.1833v2](#).
 - [4] R. Colbeck, Ph.D. thesis, University of Cambridge [[arXiv:0911.3814](#)]; S. Pironio *et al.*, *Nature (London)* **464**, 1021 (2010).
 - [5] C.E. Bardyn *et al.*, *Phys. Rev. A* **80**, 062327 (2009).
 - [6] D. Mayers and A. Yao, *Quantum Inf. Comput.* **4**, 273 (2004); F. Magniez *et al.*, *Lect. Notes Comput. Sci.* **72**, 4051 (2006).
 - [7] T. Vértesi and M. Navascués, *Phys. Rev. A* **83**, 062112 (2011).
 - [8] M. Zukowski *et al.*, *Phys. Rev. Lett.* **71**, 4287 (1993).
 - [9] S.L. Braunstein, A. Mann, and M. Revzen, *Phys. Rev. Lett.* **68**, 3259 (1992).
 - [10] S. Popescu and D. Rohrlich, *Phys. Lett. A* **169**, 411 (1992).
 - [11] M. McKague, [arXiv:1006.2352](#).
 - [12] M. Seevinck and J. Uffink, *Phys. Rev. A* **76**, 042105 (2007); S.M. Roy, *Phys. Rev. Lett.* **94**, 010402 (2005).
 - [13] A possible way of decreasing the violation between Alice and Charlie consists in keeping the state $\Phi_{AC} \otimes \rho_{A'BC'}$ but changing the measurement so that it starts involving the degrees of freedom A' . There is no way of excluding entanglement between A' and Bob's system.
 - [14] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
 - [15] L. Masanes, *Phys. Rev. Lett.* **97**, 050503 (2006).
 - [16] This holds only if the dimension of the Hilbert space is even; if it is odd, there will be an additional term in the decomposition (besides the 2-qubit Bell operators) which plays no role in the following calculations. Hence, without loss of generality, we assume that the dimension of the Hilbert space is even.
 - [17] V. Scarani and N. Gisin, *J. Phys. A* **34**, 6043 (2001).
 - [18] L.J. Landau, *Phys. Lett. A* **120**, 54 (1987).