Device-Independent Entanglement Certification of All Entangled States

Joseph Bowles,[1] Ivan Šupić,[1] Daniel Cavalcanti,[1] and Antonio Acín[1,2]
[1]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
[2]ICREA-Institució Catalana de Recerca i Estudis Avançats, Pg. Lluis Companys 23, Barcelona 08010, Spain

(Received 27 March 2018; published 29 October 2018)

We present a method to certify the entanglement of all entangled quantum states in a device-independent way. This is achieved by placing the state in a quantum network and constructing a correlation inequality based on an entanglement witness for the state. Our method is device independent, in the sense that entanglement can be certified from the observed statistics alone, under minimal assumptions on the underlying physics. Conceptually, our results borrow ideas from the field of self-testing to bring the recently introduced measurement-device-independent entanglement witnesses into the fully device-independent regime.

DOI: 10.1103/PhysRevLett.121.180503

Introduction.—The certification of entanglement is a vital task in quantum information processing for which much effort has been put into developing optimal methods [1]. Typically, one uses an approach based on entanglement witnesses [2]; since every entangled state violates a suitably chosen entanglement witness, one can in principle certify the entanglement of any entangled state. This approach, however, requires the precise knowledge of the measurements performed during the certification. At best, this means that much effort has to be put into the characterization of the experimental setup and sources of error must be known and accounted for. At worst, if the system under investigation is highly complex or poorly understood, the method may not be applicable or a false positive certification may result [3].

A solution to this problem recently came from the field of device-independent (DI) quantum information [4–7]. Here, the aim is to certify physical properties of quantum systems without requiring precise knowledge of the underlying physics, that is, by treating all devices as black boxes processing classical information. In the case of entanglement certification, one requires that the state under investigation violates a Bell inequality [4,8], a linear function of the observed experimental probabilities that is bounded for all separable states. Since the Bell inequality is a function of the observed probabilities only, and independent of the specific physical realization, entanglement can be certified without any assumptions on the performed measurements, making this approach practically attractive.

The advantages of this approach, however, come at a price: not all entangled states are capable of violating a Bell inequality [9–17]. For example, the two-qubit isotropic state,

$$\varrho(p) = p|\Phi^+\rangle\langle\Phi^+| + (1-p)\frac{\mathbb{1}}{4}, \tag{1}$$

where $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, is entangled for $p \geq 1/3$; however Bell inequality violation with projective measurements is impossible if $p \lesssim 0.68$ [18] ($p \lesssim 0.45$ in the case of general measurements [18,19]). For a large class of states, a device-independent entanglement detection method based on the violation of a standard Bell inequality therefore cannot be used.

This naturally leads to the question of whether the entanglement of all entangled states can be certified device independent using an alternative approach. In this Letter, we show the answer to be "yes" by considering networks of quantum states. Network scenarios have already been shown to be useful for DI entanglement certification, through the phenomenon of activation of Bell nonlocality [20–22]. In the present Letter, we propose a method of entanglement certification where the state under investigation is placed in a network featuring additional bipartite auxiliary states. The certification of entanglement is achieved via the violation of a correlation inequality based on an entanglement witness for the state and borrows ideas from the fields of self-testing, semiquantum games and measurement-device-independent (MDI) entanglement witnesses [23–26]. Moreover, our construction is fully DI, requiring knowledge of the observed statistics only.

Previous work.—In the standard scenario for DI entanglement certification, two parties, Alice and Bob, share a bipartite quantum state ϱ^{AB} and wish to ensure that it is entangled. As mentioned, one way to achieve this is via a Bell test, in which each party treats his or her subsystem as a black box on which he or she performs a number of possible measurements labeled by the classical variables,

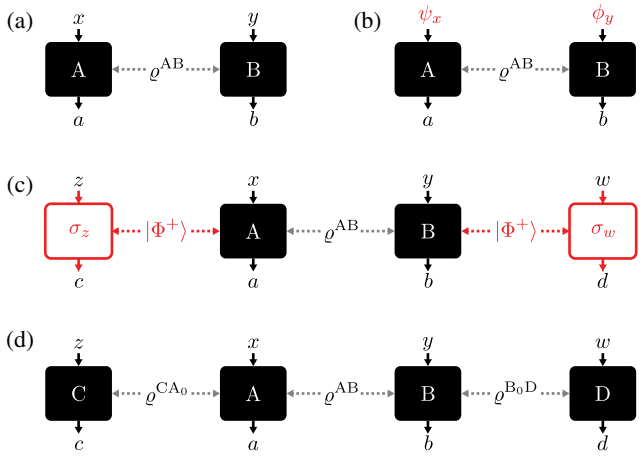

FIG. 1. Scenarios for entanglement certification. Red denotes trusted states/devices. (a) Standard Bell scenario for device-independent entanglement certification. The estimated probabilities $p(ab|xy)$ are tested for the violation of a Bell inequality in order to certify the entanglement of the state ϱ^{AB}. (b) Scenario for MDI entanglement certification. Here, the inputs are given by trusted quantum states ψ_x and ϕ_y. (c) Equivalent MDI scenario in which the inputting of the states ψ_x and ϕ_y in scenario (b) is replaced by giving Alice and Bob each one half of a maximally entangled state and performing local measurements on them. (d) Our proposal for DI entanglement certification. The entangled state ϱ^{AB} to be detected is placed in a network containing additional auxiliary entangled states. Using self-testing techniques, these entangled states are certified to be maximally entangled and perform the expected measurements as required in (c).

x for Alice and y for Bob, obtaining outcomes a and b, respectively [see Fig. 1(a)]. At the end of the experiment, they estimate the joint probabilities $p(a,b|x,y)$ of obtaining outcomes a and b for measurements x and y. A DI certification of entanglement is a proof of the entanglement of ϱ^{AB}, which follows from the probabilities $p(a,b|x,y)$ alone, i.e., without requiring assumptions about the specific physical system under investigation or the form of the measurement operators. This is equivalent to proving that the probabilities $p(a,b|x,y)$ cannot be produced by any separable state, and can be achieved via Bell inequality violation, since separable states always produce local statistics, Bell inequality violation certifies the entanglement of the state ϱ^{AB}.

As noted, there exist entangled states which do not violate any Bell inequality [9–17]. Hence, the entanglement of many states cannot be certified in this scenario. One partial solution to this problem came in the form of MDI entanglement witnesses (MDIEWs) [24,26]. Here, the Bell test scenario is modified so that the measurement inputs are given by quantum states ψ_x and ϕ_y, as opposed to the classical labels x and y [see Fig. 1(b)]. In the general construction, the set of quantum inputs for each party should be informationally complete on the local Hilbert spaces of the state under investigation. With this, a Bell-like correlation inequality can be constructed from every entanglement witness and the entanglement of all entangled states can be certified.

However, this approach is not DI since it assumes the knowledge of the input states. In what follows, we show how one can remove this assumption and achieve a fully DI certification for all entangled states. Here we concentrate on the case of two-qubit systems for the sake of simplicity. Generalizations to higher dimensions and multipartite states will be discussed in a later section and more in detail in a longer, technical version of this Letter [27]. For two-qubit states, a convenient choice of a tomographically complete set of states to use in an MDIEW protocol are the eigenstates of the Pauli matrices, i.e.,

$$\{\psi_x\} = \{\phi_y\} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |R\rangle, |L\rangle\}, \quad (2)$$

being $|+/-\rangle = (1/\sqrt{2})(|0\rangle \pm |1\rangle)$ and $|R/L\rangle = (1/\sqrt{2})(|0\rangle \pm i|1\rangle)$. Our starting point is to see that the inputting of the states ψ_x and ϕ_y is mathematically equivalent to the following [see Fig. 1(c)]. Prepare two ancilla states both in the state $|\Phi^+\rangle$ and give one qubit of each to Alice and to Bob. On the remaining two qubits, perform one of the three Pauli measurements, specified by $z = 1, 2, 3$ and $w = 1, 2, 3$. Conditioned on the choice of Pauli measurements and the corresponding outcomes, Alice and Bob's qubits are projected in one of the states in Eq. (2). This replacement is not DI, as it still assumes the form of the maximally entangled states and measurements on them. However, it is possible to use self-testing techniques to achieve a DI certification of these states and measurements [28,29]. The main idea of our protocol is to incorporate these self-testing techniques into the MDI protocol for entanglement detection and promote it into a fully DI protocol that detects any entangled state.

DI entanglement certification in networks.—We are now ready to define our scenario. We extend the standard Bell scenario to involve two more parties, Charlie and Daisy [see Fig. 1(d)]. As before, the aim is to certify the entanglement of the state ϱ^{AB} shared between Alice and Bob; however we now introduce two auxiliary states, ϱ^{CA_0}, shared between Charlie and Alice and ϱ^{B_0D} shared between Bob and Daisy. Denoting the set of linear operators on Hilbert space $\mathcal{H}$ by $\mathcal{B}(\mathcal{H})$, we have $\varrho^{AB} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$, $\varrho^{CA_0} \in \mathcal{B}(\mathcal{H}_C \otimes \mathcal{H}_{A_0})$, and $\varrho^{B_0D} \in \mathcal{B}(\mathcal{H}_{B_0} \otimes \mathcal{H}_D)$. We work in a DI scenario in the sense that we assume (i) the validity of quantum theory, but not the precise form of the states and measurements, and (ii) that the network of Fig. 1(d) correctly describes the experimental setup. Note that since we are only interested in certifying the entanglement of ϱ^{AB}, no restrictions are placed on the states ϱ^{CA_0} and ϱ^{B_0D}, in particular they may (and indeed will) be entangled. We now move to the central result of our work.

Main result

The entanglement of any entangled state ϱ^{AB} can be certified in the scenario of Fig. 1(d) as follows:

(i) The parties perform local measurements on their subsystems to obtain the statistics $p(c,a,b,d|z,x,y,w)$.

(ii) The following is then verified:

Self-testing–The marginal distributions $p(c,a|z,x)$ and $p(b,d|y,w)$ maximally violate a Bell inequality that certifies that the auxiliary states each contain a maximally entangled state and that Charlie and Daisy each perform Pauli measurements on their subsystems.

Entanglement certification–The correlations violate an additional inequality $\mathcal{I}[p(c,a,b,d|z,x,y,w)] \geq 0$ that certifies ϱ^{AB} is entangled.

Let us first discuss step (i), considering two-qubit systems. Charlie and Daisy have a choice of three measurements z, $w = 1, 2, 3$ with outcomes c, $d = \pm 1$. Alice and Bob have a choice of seven measurements x, $y = 1, 2, 3, 4, 5, 6, \star$ with outcomes a, $b = \pm 1$. The auxiliary states are chosen to be $\varrho^{CA_0} = \varrho^{B_0D} = |\Phi^+\rangle\langle\Phi^+|$. Charlie's measurements are given by the three Pauli observables σ_z, σ_x, σ_y, for $z = 1, 2, 3$. Alice's measurements for the inputs $x = 1, \ldots, 6$ are given by the rotated Pauli observables $(\sigma_z \pm \sigma_x)/\sqrt{2}$, $(\sigma_z \pm \sigma_y)/\sqrt{2}$, $(\sigma_x \pm \sigma_y)/\sqrt{2}$ acting on the $\mathcal{H}_{A_0}$ space. For the input $x = \star$, Alice's measurement is given by $\{|\Phi^+\rangle\langle|\Phi^+|, \mathbb{1} - |\Phi^+\rangle\langle\Phi^+|\}$ acting on the joint space $\mathcal{H}_{A_0} \otimes \mathcal{H}_A$. Measurements for Bob and Daisy are chosen analogously.

The Bell inequality we use for our self-testing in step (ii) of the protocol is as follows (here we focus on Charlie and Alice). Denote the expectation value of the measurements x and y by $E_{x,y}$. Consider the Bell inequality

$$\begin{aligned}\mathcal{J} = {} & E_{1,1} + E_{1,2} + E_{2,1} - E_{2,2} \\ & + E_{1,3} + E_{1,4} - E_{3,3} + E_{3,4} \\ & + E_{2,5} + E_{2,6} - E_{3,5} + E_{3,6} \leq 6. \end{aligned} \tag{3}$$

This bound follows from the fact that each line of the above is a CHSH Bell inequality [30]: each is upper bounded by 2. Using the state ϱ^{CA_0} and measurements described above, one achieves a maximal violation of each CHSH inequality and so $\mathcal{J} = 6\sqrt{2}$. Note that each of Charlie's measurements appears in exactly two of the lines. Since the maximum violation of a single CHSH inequality requires two anticommuting measurements [31–33], one would expect that the maximum violation of Eq. (3) requires three anticommuting measurements for Charlie. This is indeed the case, as described in the following lemma (see [34] for related results).

Lemma 1. Let Charlie and Alice share the state $|\psi\rangle \in \mathcal{H}_C \otimes \mathcal{H}_{A_0}$ and denote by Z^C, X^C, Y^C three ± 1 outcome observables for Charlie. If one observes a Bell inequality violation of $\mathcal{J} = 6\sqrt{2}$, then there exist local auxiliary states $|00\rangle \in [\mathcal{H}_{C''} \otimes \mathcal{H}_{C'}] \otimes [\mathcal{H}_{A_0''} \otimes \mathcal{H}_{A_0'}]$ and a local unitary $U = U_C \otimes U_A$ such that

$$U[|\psi\rangle \otimes |00\rangle] = |\xi\rangle \otimes |\Phi^+\rangle^{C'A'}, \tag{4}$$

$$U[\mathsf{X}^C|\psi\rangle \otimes |00\rangle] = |\xi\rangle \otimes \sigma_x^{C'}|\Phi^+\rangle^{C'A'}, \tag{5}$$

$$U[\mathsf{Z}^C|\psi\rangle \otimes |00\rangle] = |\xi\rangle \otimes \sigma_z^{C'}|\Phi^+\rangle^{C'A'}, \tag{6}$$

$$U[\mathsf{Y}^C|\psi\rangle \otimes |00\rangle] = \sigma_z^{C''}|\xi\rangle \otimes \sigma_y^{C'}|\Phi^+\rangle^{C'A'}, \tag{7}$$

where $|\xi\rangle$ takes the form

$$|\xi\rangle = |\xi_0\rangle^{CA} \otimes |00\rangle^{C''A''} + |\xi_1\rangle^{CA} \otimes |11\rangle^{C''A''}. \tag{8}$$

Here we use superscript to denote the Hilbert space on which an operator acts nontrivially. For example $\mathsf{X}^C|\psi\rangle \equiv (\mathsf{X}^C \otimes \mathbb{1}^{A_0})|\psi\rangle$. The above lemma can be understood as follows. The observation $\mathcal{J} = 6\sqrt{2}$ implies that the state $|\psi\rangle$ must contain a two-qubit maximally entangled subspace and that two of Charlie's measurements must be given by the observables σ_x and σ_z in this space [Eq. (4) to (6)]. From Eq. (7), the third measurement of Charlie is equivalent to first measuring the observable σ_z on the state $|\xi\rangle$, and then measuring either σ_y or $-\sigma_y$ on his half of the maximally entangled state depending on this first outcome. We can therefore understand the above as Charlie measuring either $\{\sigma_x, \sigma_y, \sigma_z\}$ or $\{\sigma_x, -\sigma_y, \sigma_z\}$ on the maximally entangled state, with some unknown probability that depends on the precise (unknown) form of $|\xi\rangle$. This reflects the fact that the only two nonunitarily equivalent sets of mutually anticommuting measurements on a qubit are given by $\{\sigma_x, \pm\sigma_y, \sigma_z\}$, which are related via transposition (or equivalently complex conjugation) in the computational basis. A full proof of Lemma 1 can be found in Ref. [27].

Strictly speaking we have not self-tested the three Pauli measurements on the maximally entangled state due to the additional σ_z measurement in Eq. (7). However, this does not prevent us from using the MDIEW technique. The intuitive reason for this is as follows. Since the measurements $\{\sigma_x, \sigma_y, \sigma_z\}$ and $\{\sigma_x, -\sigma_y, \sigma_z\}$ are related via transposition, the states that Alice receives for the input to the MDIEW protocol [see Eq. (2)] are essentially either ψ_x or ψ_x^T with some unknown probability. Using transposed quantum inputs ψ_x^T for Alice in a MDIEW protocol with a product state $\varrho^{AB} = \sigma_A \otimes \sigma_B$ is mathematically equivalent to using the standard inputs ψ_x on the state $\sigma_A^T \otimes \sigma_B$. However, since this state remains a separable, this cannot lead to false positive entanglement detection.

We now move to entanglement certification part of step (ii) of the protocol. Fix an entangled two-qubit quantum state $\tilde{\varrho}^{AB}$ for which to perform the entanglement certification. The correlation inequalities we consider are constructed from an entanglement witness for the state $\tilde{\varrho}^{AB}$ and are

inspired from those found in [23,24,26]. For every entangled $\tilde{\varrho}^{\mathrm{AB}}$ there exists a Hermitian linear operator $\mathcal{W}$, called an entanglement witness, such that $\mathrm{tr}(\mathcal{W}\varrho^{\mathrm{AB}}) \geq 0$ for every separable state ϱ^{AB} and $\mathrm{tr}(\mathcal{W}\tilde{\varrho}^{\mathrm{AB}}) < 0$. Consider the projectors $\pi_{c|j} = \frac{1}{2}[\mathbb{1} + c\sigma_j]$ with $c = \pm 1$ and $j = 1, 2, 3$, that is, projectors onto the plus and minus eigenspaces of the Pauli observables. Since these form a basis of the set of Hermitian matrices, any entanglement witness for a two-qubit state may be decomposed as

$$\mathcal{W} = \sum_{cdzw} \omega_{cd}^{zw} \pi_{c|z} \otimes \pi_{d|w}. \tag{9}$$

The inequality we consider is then

$$\mathcal{I} = \sum_{cdzw} \omega_{cd}^{zw} p(c, +, +, d|z, x = \star, y = \star, w) \geq 0, \tag{10}$$

which is satisfied if ϱ^{AB} is a separable state; however it can be violated using $\tilde{\varrho}^{\mathrm{AB}}$. To see this, write the probabilities arising from the network of Fig. 1(c) as

$$\begin{aligned} &p(c, +, +, d|z, x = \star, y = \star, w) \\ &\quad = \mathrm{tr}[\mathsf{M}_{c|z}^{\mathrm{C}} \otimes \mathsf{M}_{+|\star}^{\mathrm{A}_0\mathrm{A}} \otimes \mathsf{M}_{+|\star}^{\mathrm{BB}_0} \otimes \mathsf{M}_{d|w}^{\mathrm{D}} \varrho^{\mathrm{CA}_0} \otimes \varrho^{\mathrm{AB}} \otimes \varrho^{\mathrm{B}_0\mathrm{D}}], \end{aligned} \tag{11}$$

where the $\mathsf{M}_{i|j}$ are the local measurement operators. Since there are no restrictions on the auxiliary states or measurements, we may assume that these states are pure and the measurements $\mathsf{M}_{c|u}^{\mathrm{C}}$ and $\mathsf{M}_{d|w}^{\mathrm{D}}$ projective without a loss of generality. We may therefore write

$$\begin{aligned} &p(c, +, +, d|z, x = \star, y = \star, w) \\ &\quad = \mathrm{tr}[\mathbb{1} \otimes \mathsf{M}_{+|\star}^{\mathrm{A}_0\mathrm{A}} \otimes \mathsf{M}_{+|\star}^{\mathrm{BB}_0} \otimes \mathbb{1} |\psi\rangle\langle\psi|_{c|z}^{\mathrm{CA}_0} \otimes \varrho^{\mathrm{AB}} \otimes |\psi\rangle\langle\psi|_{d|w}^{\mathrm{B}_0\mathrm{D}}], \end{aligned} \tag{12}$$

where $|\psi\rangle_{c|z} = \mathsf{M}_{c|z}^{\mathrm{C}} |\psi\rangle^{\mathrm{CA}_0}$ and $|\psi\rangle_{d|w} = \mathsf{M}_{d|w}^{\mathrm{D}} |\psi\rangle^{\mathrm{B}_0\mathrm{D}}$. From step (ii), we may use Lemma 1 to replace the auxiliary states and measurements in the above, e.g., $|\psi\rangle_{c|z} = U^{\dagger}[|\xi\rangle \otimes \pi_{c|z}^{\mathrm{C}'} |\Phi^+\rangle]$ for $z = 1, 2$. After some work (see Supplemental Material F of Ref. [27] for details) one obtains

$$\mathcal{I} = \mathrm{tr}[\mathcal{W}\Lambda(\varrho^{\mathrm{AB}})], \tag{13}$$

where $\Lambda(\cdot)$ can be shown to be a local positive map on all separable states. One thus has that $\Lambda(\varrho^{\mathrm{AB}})$ is separable if ϱ^{AB} is separable, and so $\mathcal{I} \geq 0$ for all separable ϱ^{AB}. The proof of this follows the same structure as the MDIEW technique; however one must take a bit more care due to the additional complications implied by Lemma 1.

It remains to show that one can violate $\mathcal{I}$ using the state $\tilde{\varrho}^{\mathrm{AB}}$. First generate auxiliary states $\varrho^{\mathrm{CA}_0} = \varrho^{\mathrm{B}_0\mathrm{D}} = |\Phi^+\rangle\langle\Phi^+|$ and perform the measurements detailed in step (i) so that the self-testing conditions of step (ii) are satisfied. One then has

$$p(c, +, +, d|z, x = \star, y = \star, w) = \tag{14}$$

$$\begin{aligned} &\mathrm{tr}[\pi_{c|z} \otimes |\Phi^+\rangle\langle\Phi^+| \otimes |\Phi^+\rangle\langle\Phi^+| \otimes \pi_{d|w} |\Phi^+\rangle \\ &\quad \times \langle\Phi^+| \otimes \tilde{\varrho}^{\mathrm{AB}} \otimes |\Phi^+\rangle\langle\Phi^+|] \\ &= \frac{1}{4}\mathrm{tr}[|\Phi^+\rangle\langle\Phi^+| \otimes |\Phi^+\rangle\langle\Phi^+| \pi_{c|z}^T \otimes \tilde{\varrho}^{\mathrm{AB}} \otimes \pi_{d|w}^T] \end{aligned} \tag{15}$$

$$= \frac{1}{16}\mathrm{tr}[\pi_{c|z} \otimes \pi_{d|w} \tilde{\varrho}^{\mathrm{AB}}], \tag{16}$$

where we have used $\mathrm{tr}_{\mathrm{A}}[|\Phi^+\rangle\langle\Phi^+| \pi_{i|j}^{\mathrm{A}} \otimes \mathbb{1}] = \frac{1}{2}\pi_{i|j}^T$ in the second and third line. One thus has

$$\mathcal{I} = \frac{1}{16} \sum_{czdw} \omega_{cd}^{zw} \mathrm{tr}[\pi_{c|z} \otimes \pi_{d|w} \tilde{\varrho}^{\mathrm{AB}}] \tag{17}$$

$$\mathcal{I} = \frac{1}{16}\mathrm{tr}[\mathcal{W}\tilde{\varrho}^{\mathrm{AB}}] < 0, \tag{18}$$

hence certifying the entanglement of $\tilde{\varrho}^{\mathrm{AB}}$.

High dimension and multipartite states.—Our method can be used to certify the entanglement of bipartite states of any dimension. Every bipartite entangled state of dimension $d \times d$ violates an entanglement witness of the form

$$\mathcal{W} = \sum_{ij} \omega_{ij} \pi_i \otimes \pi_j, \tag{19}$$

where the set $\{\pi_i\}$ consists of (at least) d^2 linearly independent quantum states. As in the qubit case, states $\{\pi_i\}$ can be prepared in a device independent manner by distant parties Charlie and Daisy, which now share with Alice and Bob, respectively, a tensor product of N maximally entangled pairs of qubits, where $N = \lceil \log d \rceil$. Specifically, by performing a parallel self-test of Lemma 1, one can certify tensor products of the Pauli measurements for Charlie and Daisy, which provide an informationally complete set of states $\{\pi_i\}$ for Alice and Bob (see Ref. [27]).

The same idea can also be utilized to certify the presence of entanglement in multipartite states of any dimension. Each party would share a suitable maximally entangled state with an auxiliary party, which is used to self-test the preparation of an informationally complete set of states. We stress however that this approach is not suitable to detect genuine multipartite entanglement. This is because the set of k-separable states is not closed under partial transposition on individual parties, so the imprecision in the sign of the self-tested $\pm\sigma_y$ measurement may lead to false positive results.

Noise robustness.—It is important to ask whether our protocol can be made robust to noise. Suppose that the violations of the Bell inequality [Eq. (3)] in step (ii) of the protocol differ from the maximum value. Since self-testing protocols are robust, the observed violation guarantees that the states and measurements must be close, though not exactly equal to the desired ones. In particular, suppose Eqs. (5)–(7) hold up to a small value θ in the ℓ_2 norm, i.e.,

$$\|U[\mathsf{X}^{\mathrm{C}}|\psi\rangle \otimes |00\rangle] - |\xi\rangle \otimes \sigma_{\mathrm{x}}^{\mathrm{C}'}|\Phi^{+}\rangle^{\mathrm{C}'\mathrm{A}'}\| \leq \theta, \qquad (20)$$

and similarly for Eqs. (6) and (7). In Ref. [27] we show that entanglement can still be certified if one changes the bound of Eq. (10) to read $\mathcal{I} \geq -\mathcal{O}(\theta)$. As a result, for nonmaximal violations, a fraction of entangled states close to the separable states is no longer detected.

Discussion.—A number of improvements to the self-testing part of our protocol would strengthen our results. For example, it may be possible to lower the requirement on the number of inputs or outputs by self-testing more efficient sets of informationally complete measurements in a high dimension (e.g., by using mutually unbiased bases or symmetric positive operator valued measures). Additionally, the overall noise robustness of the entanglement certification would benefit from improvements to the robustness of self-testing statements, which at the moment are typically weak. In principle, our technique can also be applied to convex sets of bipartite quantum states other than the separable set, provided that the set is closed under local unitaries and local transpositions. Furthermore, one may be able to apply our general method to other DI tasks such as quantum key distribution and randomness certification where MDI protocols already exist [37,38].

To conclude, our work opens new perspectives for entanglement certification by connecting different concepts such as self-testing and MDI protocols in a quantum network. For weakly entangled states where optimal Bell inequalities are not known, our method provides a general construction that is easily applicable to all states. Furthermore, it allows for DI entanglement certification of entangled states admitting a so-called local hidden variable model for which the standard approach fails. We hope that the present results motivate further studies on DI protocols that could be boosted by the use of quantum networks.

We are thankful for useful discussions with Paul Skrzypczyk, Nicolas Brunner, Marco Túlio Quintino, Flavien Hirsch, Thomas Vidick, Matteo Lostaglio, Michał Oszmaniec, and Alexia Salavrakos. This work was supported by the Ramón y Cajal fellowship, Spanish MINECO (QIBEQI FIS2016-80773-P and Severo Ochoa SEV-2015-0522), the AXA Chair in Quantum Information Science, Generalitat de Catalunya (CERCA Programme), Fundació Privada Cellex, and ERC CoG QITBOX. This work was funded by COST project CA16218 NANOCOHYBRI and Juan de la Cierva-formación.

[1] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).
[2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[3] D. Rosset, R. Ferretti-Schöbitz, J.-D. Bancal, N. Gisin, and Y.-C. Liang, Phys. Rev. A **86**, 062325 (2012).
[4] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[5] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[6] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010).
[7] O. Nieto-Silleras, S. Pironio, and J. Silman, New J. Phys. **16**, 013035 (2014).
[8] J. S. Bell, Physics **1**, 195 (1964).
[9] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[10] J. Barrett, Phys. Rev. A **65**, 042302 (2002).
[11] G. Tóth and A. Acín, Phys. Rev. A **74**, 030306(R) (2006).
[12] M. L. Almeida, S. Pironio, J. Barrett, G. Tóth, and A. Acín, Phys. Rev. Lett. **99**, 040403 (2007).
[13] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[14] R. Augusiak, M. Demianowicz, and A. Acín, J. Phys. A **47**, 424002 (2014).
[15] J. Bowles, F. Hirsch, M. T. Quintino, and N. Brunner, Phys. Rev. A **93**, 022121 (2016).
[16] D. Cavalcanti, L. Guerini, R. Rabelo, and P. Skrzypczyk, Phys. Rev. Lett. **117**, 190401 (2016).
[17] F. Hirsch, M. T. Quintino, T. Vértesi, M. F. Pusey, and N. Brunner, Phys. Rev. Lett. **117**, 190402 (2016).
[18] F. Hirsch, M. T. Quintino, T. Vértesi, M. Navascués, and N. Brunner, Quantum **1**, 3 (2017).
[19] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín, Phys. Rev. Lett. **119**, 190501 (2017).
[20] A. Sen(De), U. Sen, Č. Brukner, V. Bužek, and M. Żukowski, Phys. Rev. A **72**, 042310 (2005).
[21] D. Cavalcanti, M. L. Almeida, V. Scarani, and A. Acín, Nat. Commun. **2**, 184 (2011).
[22] D. Cavalcanti, R. Rabelo, and V. Scarani, Phys. Rev. Lett. **108**, 040402 (2012).
[23] F. Buscemi, Phys. Rev. Lett. **108**, 200401 (2012).
[24] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Phys. Rev. Lett. **110**, 060405 (2013).
[25] E. G. Cavalcanti, M. J. W. Hall, and H. M. Wiseman, Phys. Rev. A **87**, 032306 (2013).
[26] E. Verbanis, A. Martin, D. Rosset, C. C. W. Lim, R. T. Thew, and H. Zbinden, Phys. Rev. Lett. **116**, 190501 (2016).
[27] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín, Phys. Rev. A **97**, 042336 (2018).
[28] M. McKague and M. Mosca, Generalized self-testing and the security of the 6-state protocol, in *TQC 2010: Theory of Quantum Computation, Communication, and Cryptography,* edited by W. van Dam, V. M. Kendon, and S. Severini. Lecture Notes in Computer Science Vol. 6519 (Springer, Berlin, Heidelberg, 2011), pp. 113–130.
[29] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Phys. Rev. A **93**, 040102 (2016).
[30] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[31] S. Popescu and D. Rohrlich, Phys. Lett. A **169**, 411 (1992).
[32] S. L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).

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

[34] Note that McKague and Mosca [28] showed an equivalent result to Lemma 1 based on the Mayers-Yao self-test (see also Refs. [29,35]). In Ref. [27], we extend these results (see also Ref. [36]) by providing a generalization of Lemma 1 to a parallel self-test in arbitrary dimension as well as an analysis of the effect of imperfect statistics.

[35] O. Andersson, P. Badziąg, I. Dumitru and A. Cabello, Phys. Rev. A **97**, 012314 (2018).

[36] A. Coladangelo, A. Grilo, S. Jeffery, and T. Vidick, arXiv: 1708.07359.

[37] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

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