Self-testing properties of Gisin's elegant Bell inequality

Ole Andersson,* Piotr Badziąg,† Ingemar Bengtsson,‡ and Irina Dumitru§
Fysikum, Stockholms Universitet, 106 91 Stockholm, Sweden

Adán Cabello‖
Departamento de Física Aplicada II, Universidad de Sevilla, 41012 Sevilla, Spain
(Received 26 July 2017; published 22 September 2017)

An experiment in which the Clauser-Horne-Shimony-Holt inequality is maximally violated is self-testing (i.e., it certifies in a device-independent way both the state and the measurements). We prove that an experiment maximally violating Gisin's elegant Bell inequality is not similarly self-testing. The reason can be traced back to the problem of distinguishing an operator from its complex conjugate. We provide a complete and explicit characterization of all scenarios in which the elegant Bell inequality is maximally violated. This enables us to see exactly how the problem plays out.

DOI: 10.1103/PhysRevA.96.032119

I. INTRODUCTION

Bell inequalities are correlation inequalities which are satisfied by any local realistic model but can be violated by quantum theory [1]. They thus allow us to test the former against the latter. They are also useful in practical applications like secure communication [2], reduction of communication complexity [3], and secure private randomness [4]. For such applications, the self-testing properties of some Bell inequalities play a major role, as they allow a maximal quantum violation to occur in an effectively unique way. In the current paper we investigate the self-testing properties implied by a maximal violation of the so-called elegant Bell inequality (EBI).

The EBI involves two parties, Alice and Bob, measuring three and four dichotomic observables, respectively. If the possible outcomes of these observables are taken to be -1 and $+1$, and we write E_{kl} for the expectation value of the product of the outcomes of Alice's kth observable and Bob's lth observable, the EBI reads

$$S \equiv E_{11} + E_{12} - E_{13} - E_{14} + E_{21} - E_{22} + E_{23} - E_{24} + E_{31} - E_{32} - E_{33} + E_{34} \leqslant 6. \quad (1)$$

The EBI does not define a facet of the classical correlation polytope and, therefore, it does not reflect the geometry of the latter. Rather, according to Gisin [5], its elegance resides in the way it is maximally violated by quantum theory. The maximum violation, proven to be $S = 4\sqrt{3}$ by Acín *et al.* [6], occurs when Alice and Bob use projective measurements whose eigenstates are maximally spread out on Bloch spheres, in a sense made precise below. In the particular case when they share a two-qubit state, Alice's measurement eigenstates form a complete set of three mutually unbiased bases (MUBs), while those of Bob are eight states that can be partitioned into two dual sets of SIC elements, see Fig. 1. SICs are also known as symmetric informationally complete positive operator-valued measures (SIC-POVMs). However, here the configuration arises from four projective measurements and not from two POVMs. Since MUBs (and SICs) are intriguing configurations of independent interest [7], we can ask the question: does maximum quantum violation of the EBI *require* the existence of three MUBs in dimension two, with no assumptions about the preparation and measurement devices being made?

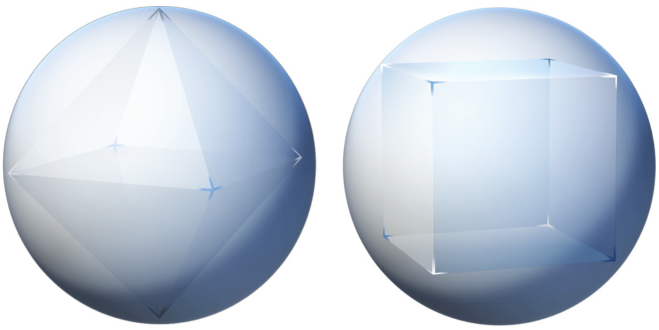
There is another motivation of more immediate practical relevance. Recently, Acín *et al.* [6] addressed the problem of how to use a two-qubit entangled state together with a local POVM measurement to certify the generation of two bits of device-independent private randomness. They provided two methods for such a certification. The simplest one was based on the EBI and was supported by numerical results. They suggested that an analytical proof of the correctness of the method should rely on a proof that a maximal violation of the EBI self-tests the maximally entangled state and the three Pauli measurements that give rise to the MUB.

In this paper we will prove that the EBI does *not* provide a self-test for the maximally entangled state and the three Pauli measurements, in the strict sense of Refs. [8,9]. It comes close to doing so though and we discuss the implications for the method suggested by Acín *et al.* in a separate paper [10]. In Sec. II of this paper we review the strict definition of self-testing. In Sec. III we discuss, following Refs. [6,11], maximal violation of the EBI. Section IV contains our main results on the self-testing properties of the EBI. To make the paper easier to read some of the detailed derivations are given in Sec. V. Finally, Sec. VI states our conclusions and the outlook.

II. SELF-TESTING EXPERIMENTS

The concept of *self-testing* was introduced by Mayers and Yao [12] as a test for a photon source which, if passed, guarantees that the source is adequate for the security of the BB84 protocol for quantum key distribution. Self-testing then received a stringent definition by the same authors in Ref. [13], a definition which was further polished by Magniez *et al.* [14] and McKague and Mosca [8,9]. In this paper we adopt the definition of self-testing used in these latter references.

*ole.andersson@fysik.su.se
†piotr.badziag@gmail.com
‡ingemar.bengtsson@fysik.su.se
§irina.dumitru@fysik.su.se
‖adan@us.es



(a) The octahedron in Alice's Bloch sphere. (b) The cube in Bob's Bloch sphere.

FIG. 1. Alice's and Bob's measurement eigenstates form two dual Platonic solids inscribed in Bloch spheres. Alice's eigenstates sit at the corners of an octahedron, Bob's eigenstates can be grouped into two dual sets of SIC vectors which sit at the corners of a cube. (a) The octahedron in Alice's Bloch sphere. (b) The cube in Bob's Bloch sphere.

The definition of being self-testing consists of a condensed description of how a *reference experiment* can be modified without affecting the statistics. Allowed modifications include local rotations, addition of ancillas, changes of the effect of observables outside the support of the state, and local embeddings of states and observables into greater or smaller Hilbert spaces [8,9]. Here we give the definition at a level of generality sufficient for our purposes. We thus consider a reference experiment involving two parties, Alice and Bob, performing m and n local dichotomic measurements $a_k = \{\Pi_\pm^{a_k}\}$ and $b_l = \{\Pi_\pm^{b_l}\}$, respectively, on a given bipartite state $|\phi\rangle$. (The subscript signs label the measurement outcomes.) We then say that the reference experiment is *self-testing* if for any other experiment in which Alice performs m local measurements $A_k = \{\Pi_\pm^{A_k}\}$ and Bob performs n local measurements $B_l = \{\Pi_\pm^{B_l}\}$ on a shared state $|\psi\rangle$, a complete agreement of the two experiments statistics, i.e., equality

$$\langle\phi|\Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi\rangle = \langle\psi|\Pi_\pm^{A_k}\Pi_\pm^{B_l}|\psi\rangle \tag{2}$$

for all k,l, implies the existence of a local unitary or, more precisely, a local isometric embedding

$$\begin{aligned}\Phi = \Phi_A\otimes\Phi_B : \mathcal{H}_A\otimes\mathcal{H}_B &\to (\mathcal{H}_A\otimes\mathcal{H}_a)\otimes(\mathcal{H}_B\otimes\mathcal{H}_b)\\ &= (\mathcal{H}_A\otimes\mathcal{H}_B)\otimes(\mathcal{H}_a\otimes\mathcal{H}_b)\end{aligned} \tag{3}$$

such that $\Phi(\Pi_\pm^{A_k}\Pi_\pm^{B_l}|\psi\rangle) = |\chi\rangle\otimes\Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi\rangle$, where $|\chi\rangle$ is some arbitrary but normalized "junk" vector in $\mathcal{H}_A\otimes\mathcal{H}_B$. (Here we use vocabulary introduced in Refs. [8,9].) Notice that the definition of self-testing captures, although in a rather abstract way, the physical intuition that the state generation includes a successful isolation of a "relevant part" of the total state. On this part, the measurements then act in a way stipulated by the reference experiment without entangling it with the rest of the state. We emphasize this by saying, for short, that the experiment is *effectively equivalent* to the reference experiment.

III. MAXIMAL VIOLATION OF THE EBI

The elegant Bell inequality can be violated in quantum theory. In fact, Acín *et al.* [6] have recently proven that the maximum quantum value that S can attain is $4\sqrt{3}$. The simplest setting when this happens, it turns out, is when Alice and Bob share two qubits in the maximally entangled state

$$|\phi_+\rangle = \tfrac{1}{\sqrt{2}}(|0_a0_b\rangle + |1_a1_b\rangle), \tag{4}$$

Alice's observables correspond to the three Pauli operators

$$a_1 = Z = \sigma_Z,\quad a_2 = X = \sigma_X,\quad a_3 = Y = \sigma_Y, \tag{5}$$

and Bob's observables correspond to

$$b_1 = \tfrac{1}{\sqrt{3}}(Z+X-Y),\quad b_3 = \tfrac{1}{\sqrt{3}}(-Z+X+Y), \tag{6a}$$

$$b_2 = \tfrac{1}{\sqrt{3}}(Z-X+Y),\quad b_4 = \tfrac{1}{\sqrt{3}}(-Z-X-Y). \tag{6b}$$

The elegance of the Bell inequality (1) is apparent [5] when we observe that the observables in Eqs. (5) and (6) give rise to two measurement structures which can be represented by two dual polyhedra in the Bloch ball: Alice's measurement eigenstates form a complete set of three MUBs, with each basis corresponding to a pair of opposite corners of an octahedron inscribed in the Bloch sphere, see Fig. 1(a). On the Bloch sphere, the eight eigenstates of Bob's projective measurements form the vertices of a dual cube, see Fig. 1(b). They can be grouped into two tetrahedra containing no adjacent corners. The vertices of such a tetrahedron can be regarded as the four vectors in a SIC, and we can arrange them such that one SIC is formed by the -1 outcome projectors and the other by the $+1$ outcome projectors. Below we will show that, in general, the EBI is maximally violated if and only if the state is a superposition of maximally entangled qubit states like the one in Eq. (4) and Alice's and Bob's observables split into direct sums of qubit MUB-SIC configurations similar to that just described.

To characterize all scenarios in which the EBI is maximally violated we consider a general one in which Alice measures three dichotomic observables A_1,A_2,A_3 and Bob measures four dichotomic observables B_1,B_2,B_3,B_4, all of which take the values -1 or $+1$, on a bipartite system in a state $|\psi\rangle$ such that $\langle\psi|\Sigma|\psi\rangle = 4\sqrt{3}$, where Σ is the *elegant Bell operator*:

$$\begin{aligned}\Sigma \equiv{}& A_1B_1 + A_1B_2 - A_1B_3 - A_1B_4 + A_2B_1 - A_2B_2\\ &+ A_2B_3 - A_2B_4 + A_3B_1 - A_3B_2 - A_3B_3 + A_3B_4.\end{aligned} \tag{7}$$

The first assertion, which, like all other assertions in this section, is proven in Sec. V, is that Alice's and Bob's observables preserve the supports, even the eigenspaces, of the respective marginal states: If $\lambda_1,\lambda_2,\dots,\lambda_m$ are the *different* Schmidt coefficients of $|\psi\rangle$, having multiplicities $d_1,d_2,\dots,d_m$, and $\mathcal{H}_A^i$ and $\mathcal{H}_B^i$ denote the d_i-dimensional eigenspaces of $\mathrm{tr}_B\,|\psi\rangle\langle\psi|$ and $\mathrm{tr}_A\,|\psi\rangle\langle\psi|$ corresponding to the eigenvalue λ_i^2, then Alice's observables send $\mathcal{H}_A^i$ into itself and Bob's observables send $\mathcal{H}_B^i$ into itself. As a consequence we can, without loss of generality, truncate Alice's and Bob's Hilbert spaces and restrict the observables to the support of the respective marginal state. We henceforth assume this has been done and we write A_k^i and B_l^i for the restriction of Alice's kth and Bob's lth observable to $\mathcal{H}_A^i$ and $\mathcal{H}_B^i$, respectively.

The second assertion is that Alice's observables anticommute: $\{A_k, A_l\} = 2\delta_{kl}$. (Since their eigenvalues equal -1 or $+1$, Alice's and Bob's observables are involutions, i.e., they square to the identity operator.) From this follows that $\mathcal{H}_A^i$ is even-dimensional, say $d_i = 2n_i$, and can be split into 2-dimensional and pairwise orthogonal subspaces, each left invariant by Alice's observables:

$$\mathcal{H}_A^i = \bigoplus_{p=1}^{n_i} \mathcal{H}_A^{ip}, \quad A_k^i = \bigoplus_{p=1}^{n_i} A_k^{ip}. \tag{8}$$

Furthermore, each subspace $\mathcal{H}_A^{ip}$ admits a basis $\{|0_A^{ip}\rangle, |1_A^{ip}\rangle\}$ with respect to which

$$A_1^{ip} = Z, \quad A_2^{ip} = X, \quad A_3^{ip} = \pm Y. \tag{9}$$

Notice the indefinite sign of A_3^{ip}; a similar sign indeterminacy was identified in [8], treating a related problem.

The third assertion is that every $\mathcal{H}_B^i$ can as well be decomposed into 2-dimensional orthogonal subspaces, each of which is left invariant by Bob's observables:

$$\mathcal{H}_B^i = \bigoplus_{p=1}^{n_i} \mathcal{H}_B^{ip}, \quad B_l^i = \bigoplus_{p=1}^{n_i} B_l^{ip}. \tag{10}$$

Moreover, $\mathcal{H}_B^{ip}$ admits a basis $\{|0_B^{ip}\rangle, |1_B^{ip}\rangle\}$ such that, as matrices with respect to $\{|0_A^{ip}\rangle, |1_A^{ip}\rangle\}$ and $\{|0_B^{ip}\rangle, |1_B^{ip}\rangle\}$,

$$B_1^{ip} = \tfrac{1}{\sqrt{3}}\left(A_1^{ip} + A_2^{ip} - A_3^{ip}\right) = \tfrac{1}{\sqrt{3}}(Z + X \mp Y), \tag{11a}$$

$$B_2^{ip} = \tfrac{1}{\sqrt{3}}\left(A_1^{ip} - A_2^{ip} + A_3^{ip}\right) = \tfrac{1}{\sqrt{3}}(Z - X \pm Y), \tag{11b}$$

$$B_3^{ip} = \tfrac{1}{\sqrt{3}}\left(-A_1^{ip} + A_2^{ip} + A_3^{ip}\right) = \tfrac{1}{\sqrt{3}}(-Z + X \pm Y), \tag{11c}$$

$$B_4^{ip} = \tfrac{1}{\sqrt{3}}\left(-A_1^{ip} - A_2^{ip} - A_3^{ip}\right) = \tfrac{1}{\sqrt{3}}(-Z - X \mp Y). \tag{11d}$$

The fourth and last assertion concerns the state. The bases $\{|0_A^{ip}\rangle, |1_A^{ip}\rangle\}$ and $\{|0_B^{ip}\rangle, |1_B^{ip}\rangle\}$ are eigenbases of Alice's and Bob's local states which will be constructed in such a way that the shared state obtains the representation

$$|\psi\rangle = \sum_{i=1}^{m}\sum_{p=1}^{n_i} \lambda_i \left(|0_A^{ip} 0_B^{ip}\rangle + |1_A^{ip} 1_B^{ip}\rangle\right) = \sqrt{2}\sum_{i=1}^{m}\sum_{p=1}^{n_i} \lambda_i |\phi_+^{ip}\rangle. \tag{12}$$

Notice that $|\phi_+^{ip}\rangle$ is the Einstein-Podolsky-Rosen singlet in the space $\mathcal{H}_A^{ip} \otimes \mathcal{H}_B^{ip}$, restricted to which Alice's and Bob's observables are given by Eqs. (9) and (11). For each i, we arrange that $A_3^{ip} = Y$ for $p \leqslant r_i$ and $A_3^{ip} = -Y$ for $p > r_i$, where $0 \leqslant r_i \leqslant n_i$. For any Schmidt coefficients λ_i and any r_i the EBI is maximally violated.

We end this section with some remarks about mixed states and general measurements violating the EBI maximally. If Alice and Bob share a mixed state which can be expanded as an incoherent sum of pure states, each of which individually maximally violates the EBI, then so does the mixed state. A straightforward convexity argument then shows that this is the only possibility for a mixed state violating the EBI maximally. One can also ask if the EBI can be maximally violated by nonprojective measurements. It turns out that this is not possible. More precisely, if Alice and Bob measure local dichotomic POVMs and the EBI is maximally violated, then the measurement operators preserve the supports of the local states, and when restricted to these supports the measurements are projective. A proof of this can be based on Naimark's dilation theorem (see, e.g., [15]) and the arguments in the second paragraph in Sec. V below.

IV. SELF-TESTING PROPERTIES OF THE EBI

By the previous section, Alice's observables split into an unknown number of 2-dimensional $\mathfrak{su}(2)$ representations and an unknown number of "transposed" $\mathfrak{su}(2)$ representations. The statistics, however, is independent of these numbers, since the statistics equals that of the experiment specified by Eqs. (4)–(6), from now on referred to as "the reference experiment." The reference experiment is therefore not self-testing, and neither is any other experiment in which only a maximal violation of the EBI is assumed. For if a local isometric embedding Φ exists, establishing an effective equivalence between the reference experiment and the generic experiment in Sec. III, then

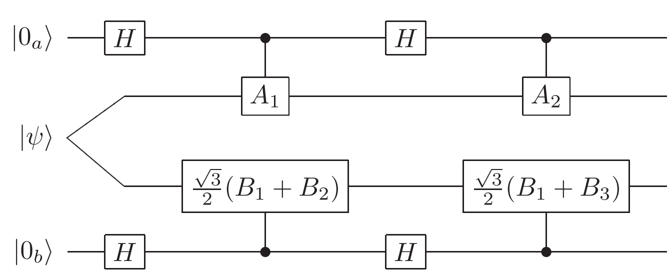
$$\langle\phi_+|a_2a_3(b_1+b_2)|\phi_+\rangle = \langle\Phi(A_2|\psi\rangle)|\Phi(A_3(B_1+B_2)|\psi\rangle)\rangle = \langle\psi|A_2A_3(B_1+B_2)|\psi\rangle. \tag{13}$$

But $\langle\phi_+|a_2a_3(b_1+b_2)|\phi_+\rangle = 2i/\sqrt{3}$ and

$$\langle\psi|A_2A_3(B_1+B_2)|\psi\rangle = \frac{2i}{\sqrt{3}}\sum_{i=1}^{m}\lambda_i^2(4r_i - 2n_i). \tag{14}$$

The results agree if and only if $r_i = n_i$ for all i. (Remember that $2n_i$ is the multiplicity of the Schmidt coefficient λ_i.) But, because the values of the differences $n_i - r_i$ are not determinable from the statistics of the experiment, this shows that a maximal violation of the EBI is not sufficient to conclude that the reference experiment is self-testing.

On the other hand, if we *require* that Eq. (13) *is* satisfied, in addition to a maximal violation of the EBI, the reference experiment *is* self-testing; an equivalence is provided by the local isometric embedding Φ given by the circuit



(Here H denotes the Hadamard gate and the control gates are triggered by the presence of $|1_a\rangle$ and $|1_b\rangle$.) McKague and Mosca used this isometric embedding to develop a generalized Mayers-Yao test, see [8], and McKague *et al.* [16] used it to show that the standard scenario in which the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality is maximally violated is robustly self-testing. Recently, a more universal form of this isometric embedding was used to prove that all pure bipartite entangled states can be self-tested [17].

Straightforward calculations show that

$$\Phi\big(\Pi_\pm^{A_k}\Pi_\pm^{B_l}|\phi_+^{ip}\rangle\big) = \big|0_A^{ip}0_B^{ip}\big\rangle \otimes \Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi_+\rangle, \tag{15}$$

where $\Pi_\pm^{A_k}$ and $\Pi_\pm^{B_l}$ are the projections onto the ± 1 eigenspaces of A_k and B_l, and $\Pi_\pm^{a_k}$ and $\Pi_\pm^{b_l}$ are the projections onto the ± 1 eigenspaces of the observables a_k and b_l in the reference experiment. Consequently,

$$\begin{aligned}\Phi\big(\Pi_\pm^{A_k}\Pi_\pm^{B_l}|\psi\rangle\big) &= \sqrt{2}\sum_{i=1}^{m}\sum_{p=1}^{n_i}\lambda_i\big|0_A^{ip}0_B^{ip}\big\rangle \otimes \Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi_+\rangle\\ &= |\chi\rangle \otimes \Pi_\pm^{a_k}\Pi_\pm^{b_l}|\phi_+\rangle.\end{aligned} \tag{16}$$

The last identity in Eq. (16) defines the junk vector $|\chi\rangle$. If Eq. (13) is *not* satisfied, the junk vector naturally splits into two parts, $|\chi\rangle = |\chi_1\rangle + |\chi_2\rangle$, defined by

$$|\chi_1\rangle = \sqrt{2}\sum_{i=1}^{m}\sum_{p=1}^{r_i}\lambda_i\big|0_A^{ip}0_B^{ip}\big\rangle, \tag{17}$$

$$|\chi_2\rangle = \sqrt{2}\sum_{i=1}^{m}\sum_{p=r_i+1}^{n_i}\lambda_i\big|0_A^{ip}0_B^{ip}\big\rangle. \tag{18}$$

Equation (16) is then no longer valid. Instead we have that

$$\Phi\big(\Pi_\pm^{A_1}\Pi_\pm^{B_l}|\psi\rangle\big) = |\chi_1\rangle\Pi_\pm^{a_1}\Pi_\pm^{b_l}|\phi_+\rangle + |\chi_2\rangle\Pi_\pm^{a_1}\Pi_\mp^{b_{5-l}}|\phi_+\rangle, \tag{19a}$$

$$\Phi\big(\Pi_\pm^{A_2}\Pi_\pm^{B_l}|\psi\rangle\big) = |\chi_1\rangle\Pi_\pm^{a_2}\Pi_\pm^{b_l}|\phi_+\rangle + |\chi_2\rangle\Pi_\pm^{a_2}\Pi_\mp^{b_{5-l}}|\phi_+\rangle, \tag{19b}$$

$$\Phi\big(\Pi_\pm^{A_3}\Pi_\pm^{B_l}|\psi\rangle\big) = |\chi_1\rangle\Pi_\pm^{a_3}\Pi_\pm^{b_l}|\phi_+\rangle + |\chi_2\rangle\Pi_\mp^{a_3}\Pi_\mp^{b_{5-l}}|\phi_+\rangle. \tag{19c}$$

Using these identities one can show that a measurement of Alice's third observable, or a measurement of any of Bob's observables, entangles the singlet part of the state with the junk part. But, interestingly, even though an adversary, Eve, having access only to the junk part, can detect a measurement of A_3 or any of the B_l, she cannot distinguish between the outcomes. This is so because, irrespective of the measurement outcome, all these measurements leave Eve's system in the same state.

V. DERIVATIONS

In this section we prove the assertions in Sec. III. Inspiration comes mainly from Acín *et al.*'s derivation of the least quantum bound for the EBI [6] and from Popescu and Rohrlich's characterization of the scenarios in which the CHSH Bell inequality is maximally violated [11].

First we prove that Alice's and Bob's observables preserve the supports of the marginal states. Thus let $|\psi\rangle$ be a state saturating the EBI and let $|\psi\rangle = \sum_{i=1}^m\sum_{p=1}^{d_i}\lambda_i|u_p^iv_p^i\rangle$ be a Schmidt decomposition, with i labeling the m different Schmidt coefficients and d_i being the multiplicity of λ_i. Define

$$D_1 = \tfrac{1}{\sqrt{3}}(A_1 + A_2 + A_3), \tag{20a}$$

$$D_2 = \tfrac{1}{\sqrt{3}}(A_1 - A_2 - A_3), \tag{20b}$$

$$D_3 = \tfrac{1}{\sqrt{3}}(-A_1 + A_2 - A_3), \tag{20c}$$

$$D_4 = \tfrac{1}{\sqrt{3}}(-A_1 - A_2 + A_3). \tag{20d}$$

Then $\sum_{l=1}^4(D_l - B_l)^2 = 8\mathbb{1} - 2\Sigma/\sqrt{3}$ and, hence,

$$\sum_{i=1}^{m}\sum_{p=1}^{d_i}\lambda_i D_l\big|u_p^iv_p^i\big\rangle = \sum_{i=1}^{m}\sum_{p=1}^{d_i}\lambda_i B_l\big|u_p^iv_p^i\big\rangle. \tag{21}$$

Multiplication of both sides by $\langle w,v_q^j|$, where $|w\rangle$ is any vector in $\mathcal{H}_A$ perpendicular to the support of $\mathrm{tr}_B\,|\psi\rangle\langle\psi|$, yields the identity $\lambda_j\langle w|D_l|u_q^j\rangle = 0$. Since the indices j and q are arbitrary and $\lambda_j > 0$, this proves that D_l preserves the support of $\mathrm{tr}_B\,|\psi\rangle\langle\psi|$. Then so does each A_k. A similar argument shows that the operators B_l preserve the support of the marginal state $\mathrm{tr}_A\,|\psi\rangle\langle\psi|$.

Next we prove that Alice's and Bob's observables preserve the eigenspaces of the marginal states. From Eq. (21) follows that for any two pairs of indices (i_1,p_1) and (i_2,p_2),

$$\lambda_{i_2}\big\langle u_{p_1}^{i_1}\big|D_l\big|u_{p_2}^{i_2}\big\rangle = \lambda_{i_1}\big\langle v_{p_2}^{i_2}\big|B_l\big|v_{p_1}^{i_1}\big\rangle. \tag{22}$$

This, in turn, implies that

$$\lambda_{i_1}^2\big\langle u_{p_1}^{i_1}\big|D_l\big|u_{p_2}^{i_2}\big\rangle = \lambda_{i_2}^2\big\langle u_{p_1}^{i_1}\big|D_l\big|u_{p_2}^{i_2}\big\rangle. \tag{23}$$

From Eq. (23) we can deduce that D_l and, hence, each A_k preserve the eigenspaces $\mathcal{H}_A^i$. By an identical argument also the operators B_l preserve the eigenspaces $\mathcal{H}_B^i$. We write A_k^i and D_l^i for the restrictions of A_k and D_l to $\mathcal{H}_A^i$, and B_l^i for the restriction of B_l to $\mathcal{H}_B^i$.

From Eq. (20) and the A_k being involutions follow that

$$\big(D_1^i\big)^2 = \mathbb{1} + \tfrac{1}{3}\big(\{A_1^i,A_2^i\} + \{A_1^i,A_3^i\} + \{A_2^i,A_3^i\}\big), \tag{24a}$$

$$\big(D_2^i\big)^2 = \mathbb{1} - \tfrac{1}{3}\big(\{A_1^i,A_2^i\} - \{A_1^i,A_3^i\} + \{A_2^i,A_3^i\}\big), \tag{24b}$$

$$\big(D_3^i\big)^2 = \mathbb{1} - \tfrac{1}{3}\big(\{A_1^i,A_2^i\} + \{A_1^i,A_3^i\} - \{A_2^i,A_3^i\}\big), \tag{24c}$$

$$\big(D_4^i\big)^2 = \mathbb{1} + \tfrac{1}{3}\big(\{A_1^i,A_2^i\} - \{A_1^i,A_3^i\} - \{A_2^i,A_3^i\}\big). \tag{24d}$$

Furthermore, from Eq. (22) and each B_l being an involution follows that D_l^i is an involution. But then, by Eq. (24),

$$\{A_1^i,A_2^i\} = \{A_1^i,A_3^i\} = \{A_2^i,A_3^i\} = 0. \tag{25}$$

Equation (25) implies that A_1^i, A_2^i, and $[A_1^i,A_2^i]/2i$ generate an $\mathfrak{su}(2)$ representation. We cannot, however, conclude that $A_3^i = [A_1^i,A_2^i]/2i$. Nevertheless, among the irreducible $\mathfrak{su}(2)$ representations only the 2-dimensional one satisfies Eq. (25). The space $\mathcal{H}_A^i$ must therefore be even-dimensional, say $d_i = 2n_i$, and be decomposable into an orthogonal direct sum of 2-dimensional subspaces, $\mathcal{H}_A^i = \bigoplus_{p=1}^{n_i}\mathcal{H}_A^{ip}$, each of which is left invariant by A_1^i and A_2^i; thus $A_1^i = \bigoplus_{p=1}^{n_i}A_1^{ip}$ and $A_2^i = \bigoplus_{p=1}^{n_i}A_2^{ip}$. Furthermore, since A_1^i and A_2^i are involutions, we can choose a provisional basis $\{|s_A^i\rangle\}_{s=1}^{d_i}$ in each $\mathcal{H}_A^i$ such that for every $1 \leqslant p \leqslant n_i$, $\{|(2p-1)_A^i\rangle,|(2p)_A^i\rangle\}$ is a basis in $\mathcal{H}_A^{ip}$ relative to which $A_1^{ip} = Z$ and $A_2^{ip} = X$.

It remains to prove that the decomposition of $\mathcal{H}_A^i$ can be chosen such that A_3^i also splits into a direct sum, $A_3^i = \bigoplus_{p=1}^{n_i}A_3^{ip}$, and that the basis in $\mathcal{H}_A^{ip}$ can be chosen such that $A_3^{ip} = \pm Y$. To this end, let $(A_3^i)_{p_2}^{p_1}$ be the 2×2 matrix which in the provisional basis describes how A_3^i connects $\mathcal{H}_A^{ip_1}$ to $\mathcal{H}_A^{ip_2}$. Then, by Eq. (25), and since A_3^i is Hermitian, $(A_3^i)_{p_2}^{p_1} = \omega_{p_2}^{p_1} Y$ for some real number $\omega_{p_2}^{p_1}$. Next introduce a tensor product structure in $\mathcal{H}_A^i$ by writing $|(2p-1)_A^i\rangle = |p\rangle \otimes |0\rangle$ and $|(2p)_A^i\rangle = |p\rangle \otimes |1\rangle$. Then $A_1^i = \mathbb{1} \otimes Z$, $A_2^i = \mathbb{1} \otimes X$, and $A_3^i = \Omega \otimes Y$, where Ω is the $n_i \times n_i$ matrix whose element on position (p_1,p_2) is $\omega_{p_2}^{p_1}$. Being Hermitian, Ω can be diagonalized, say $U^\dagger \Omega U = \mathrm{diag}(\omega_1,\omega_2,\ldots,\omega_{n_i})$. Then

$$(U^\dagger \otimes \mathbb{1}) A_1^i (U \otimes \mathbb{1}) = \mathbb{1} \otimes Z, \tag{26a}$$

$$(U^\dagger \otimes \mathbb{1}) A_2^i (U \otimes \mathbb{1}) = \mathbb{1} \otimes X, \tag{26b}$$

$$(U^\dagger \otimes \mathbb{1}) A_3^i (U \otimes \mathbb{1}) = \mathrm{diag}(\omega_1,\omega_2,\ldots,\omega_{n_i}) \otimes Y. \tag{26c}$$

Each diagonal element ω_p equals $+1$ or -1 because A_3^i is an involution. We choose U such that $\omega_p = +1$ for $p \leqslant r_i$ and $\omega_p = -1$ for $p > r_i$, where r_i is the number of positive diagonal elements. We then rotate the provisional basis by applying $U^\dagger \otimes \mathbb{1}$ to it and rotate the $\mathcal{H}_A^{ip}$ accordingly.

Next we consider Bob's observables. These are completely determined by Alice's observables. To see this, define

$$|s_B^i\rangle = \sum_{p=1}^{n_i} |v_p^i\rangle\langle s_A^i|u_p^i\rangle. \tag{27}$$

Then $\langle s_B^i|B_l^i|t_B^i\rangle = \langle t_A^i|D_l^i|s_A^i\rangle$ and, hence, by Eq. (20),

$$B_1^i = \tfrac{1}{\sqrt{3}}\left(A_1^i + A_2^i + A_3^i\right)^T, \tag{28a}$$

$$B_2^i = \tfrac{1}{\sqrt{3}}\left(A_1^i - A_2^i - A_3^i\right)^T, \tag{28b}$$

$$B_3^i = \tfrac{1}{\sqrt{3}}\left(-A_1^i + A_2^i - A_3^i\right)^T, \tag{28c}$$

$$B_4^i = \tfrac{1}{\sqrt{3}}\left(-A_1^i - A_2^i + A_3^i\right)^T. \tag{28d}$$

This proves Eqs. (11).

The assertion about the state is a straightforward consequence of the calculation

$$\begin{aligned}|\psi\rangle &= \sum_{i=1}^{m}\sum_{p=1}^{d_i} \lambda_i |u_p^i v_p^i\rangle \\ &= \sum_{i=1}^{m}\sum_{p=1}^{d_i}\sum_{s=1}^{d_i}\sum_{t=1}^{d_i} \lambda_i |s_A^i t_B^i\rangle\langle s_A^i|u_p^i\rangle\langle t_B^i|v_p^i\rangle \\ &= \sum_{i=1}^{m}\sum_{s=1}^{d_i}\sum_{t=1}^{d_i} \lambda_i |s_A^i t_B^i\rangle \delta_{st} \\ &= \sum_{i=1}^{m}\sum_{p=1}^{n_i} \lambda_i \left(|(2p-1)_A^i(2p-1)_B^i\rangle + |(2p)_A^i(2p)_B^i\rangle\right).\end{aligned} \tag{29}$$

If we define

$$|0_A^{ip}\rangle = |(2p-1)_A^i\rangle, \quad |1_A^{ip}\rangle = |(2p)_A^i\rangle, \tag{30}$$

$$|0_B^{ip}\rangle = |(2p-1)_B^i\rangle, \quad |1_B^{ip}\rangle = |(2p)_B^i\rangle, \tag{31}$$

then $|\psi\rangle$ takes the form in Eq. (12).

VI. CONCLUDING REMARKS

We have shown that maximal violation of the EBI by itself does not certify self-testability; additional requirements need to be met. The extra requirement that Eq. (13) should also be satisfied makes the experiment self-testing. That a maximal violation of the EBI does not lead to self-testability is because transposition of *some* of the components of Alice's observables does not affect the statistics but leads to an *inequivalent* experiment. Similar issues have been pointed out by other authors, see, e.g., Refs. [8,18], and it has been suggested that the definition of self-testing should be relaxed "to include this transposition equivalence" [19]. Then the results in this paper have to be taken into account since in such a relaxation we may be losing physically relevant information, as Eq. (14) shows. Alternative approaches to self-testing based on quantification of incompatibility of measurements have been proposed [18,20].

In addition, we have completely and explicitly characterized the scenarios in which the EBI is maximally violated. For a pair of qubits, maximal violation requires measurements corresponding to mutually unbiased bases on the Bloch sphere on one side and to measurements along the diagonals of a dual cube (inscribed in the Bloch sphere) on the other. The general case is a superposition of that for the pair of qubits.

In many applications, Bell inequalities are used to guarantee that quantum mechanical systems exhibit desired properties. The present paper provides information about the EBI which is potentially useful in any situation where a maximal violation of the EBI is used as such a resource. Examples include a construction for device-independent generation of private randomness proposed by Acín *et al.* [6]. We discuss this construction in a companion paper [10].

ACKNOWLEDGMENTS

We thank M. Nawareg and M. Smania for fruitful discussions, J. Kaniewski and Y.-C. Liang for useful comments on an earlier draft of the paper, and N. Gisin for encouraging remarks. We also thank P. Z. Andersson who produced Fig. 1. A.C. acknowledges support from Project No. FIS2014-60843-P, "Advanced Quantum Information" (MINECO, Spain), with FEDER funds, the FQXi Large Grant "The Observer Observed: A Bayesian Route to the Reconstruction of Quantum Theory," and the project "Photonic Quantum Information" (Knut and Alice Wallenberg Foundation, Sweden).

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

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, Bell's Inequalities and Quantum Communication Complexity, Phys. Rev. Lett. **92**, 127901 (2004).

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

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

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

[7] W. K. Wootters, Quantum measurements and finite geometry, Found. Phys. **36**, 112 (2006).

[8] M. McKague and M. Mosca, Generalized self-testing and the security of the 6-state protocol, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science, edited by W. van Dam, V. M. Kendon, and S. Severini (Springer, Berlin, 2010), Vol. 6519, p. 113.

[9] M. McKague, Quantum information processing with adversarial devices, Ph.D. thesis, University of Waterloo, 2010, arXiv:1006.2352.

[10] O. Andersson, P. Badziąg, I. Dumitru, and A. Cabello, Certification of two bits of randomness from one entangled bit using the elegant Bell inequality, arXiv:1707.00564.

[11] S. Popescu and D. Rohrlich, Which states violate Bell's inequality maximally?, Phys. Lett. A **169**, 411 (1992).

[12] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, in *Proceedings of the 39th IEEE Conference on Foundations of Computer Science, Palo Alto, CA, 1998*) (IEEE, New York, 1998).

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

[14] F. Magniez, D. Mayers, M. Mosca, and H. Olliver, Self-testing of quantum circuits, in *Proceedings of ICALP 2006*, Part I, Lecture Notes in Computer Science, edited by M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener (Springer, Berlin, 2006), Vol. 4051, p. 72.

[15] A. Holevo, in *Probabilistic and Statistical Aspects of Quantum Theory* (Scuola Normale Superiore Pisa, Pisa, Italy, 2011), p. 55.

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

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

[18] J. Kaniewski, Self-testing of binary observables based on commutation, Phys. Rev. A **95**, 062323 (2017).

[19] J. Kaniewski (private communication).

[20] S.-L. Chen, C. Budroni, Y.-C. Liang, and Y.-N. Chen, Natural Framework for Device-Independent Quantification of Quantum Steerability, Measurement Incompatibility, and Self-Testing, Phys. Rev. Lett. **116**, 240401 (2016).