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. The possible outcomes of these observables are taken to be three and four dichotomic observables, respectively. If 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
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 $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|0_A0_B\rangle + |1_A1_B\rangle)$, (4)

Alice’s observables correspond to the three Pauli operators

$$a_1 = Z = \sigma_Z, \quad a_2 = X = \sigma_X, \quad a_3 = Y = \sigma_Y,$$  (5)

and Bob’s observables correspond to

$$b_1 = \frac{1}{\sqrt{3}}(Z + X - Y), \quad b_2 = \frac{1}{\sqrt{3}}(Z - X + Y), \quad b_3 = \frac{1}{\sqrt{3}}(-Z - X - Y).$$  (6a)  (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. 1a. On the Bloch sphere, the eight eigenstates of Bob’s projective measurements form the vertices of a dual cube, see Fig. 1b. 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 $\Sigma$ is the elegant Bell operator:

$$\Sigma \equiv A_1 B_1 + A_1 B_2 - A_1 B_3 - A_1 B_4 + A_2 B_1 - A_2 B_2 + A_2 B_3 - A_2 B_4 + A_3 B_1 - A_3 B_2 - A_3 B_3 + A_3 B_4.$$  (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 $\lambda_1, \lambda_2, \ldots, \lambda_m$ are the different Schmidt coefficients of $|ψ⟩$, having multiplicities $d_1, d_2, \ldots, d_m$, and $\mathcal{H}_A$ and $\mathcal{H}_B$ denote the $d_i$-dimensional eigenspaces of $\text{tr}_B |ψ⟩⟨ψ|_B$ and $\text{tr}_A |ψ⟩⟨ψ|_A$ corresponding to the eigenvalue $\lambda_i^2$, then Alice’s observables send $\mathcal{H}_A$ into itself and Bob’s observables send $\mathcal{H}_B$ 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 $A_k^l$ and $B_l^i$ for the restriction of Alice’s $k$th and Bob’s $l$th observable to $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively.

The second assertion is that Alice’s observables anticommute: $\{A_k^l, A_l^k\} = 2\delta_{kl}$. (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 $\mathcal{H}_A$ is even-dimensional, say $d_A = 2n_1$, and can be split into 2-dimensional and pairwise orthogonal subspaces, each left invariant by Alice’s observables:

$$\mathcal{H}_A^p = \bigoplus_{p=1}^{n_1} \mathcal{H}_A^{ip}, \quad A_k^l = \bigoplus_{p=1}^{n_1} A_k^l|^p.$$

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

$$A_1^p = Z, \quad A_2^p = X, \quad A_3^p = \pm Y. \quad (9)$$

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

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

$$\mathcal{H}_B^p = \bigoplus_{p=1}^{n_1} \mathcal{H}_B^{ip}, \quad B_l^i = \bigoplus_{p=1}^{n_1} B_l^i|^p. \quad (10)$$

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

$$B_1^p = \frac{1}{\sqrt{2}}(A_1^p + A_2^p - A_3^p) = \frac{1}{\sqrt{2}}(Z + X \mp Y), \quad (11a)$$
$$B_2^p = \frac{1}{\sqrt{2}}(A_1^p - A_2^p + A_3^p) = \frac{1}{\sqrt{2}}(Z - X \pm Y), \quad (11b)$$
$$B_3^p = \frac{1}{\sqrt{2}}(-A_1^p + A_2^p + A_3^p) = \frac{1}{\sqrt{2}}(-Z + X \mp Y), \quad (11c)$$
$$B_4^p = \frac{1}{\sqrt{2}}(-A_1^p - A_2^p - A_3^p) = \frac{1}{\sqrt{2}}(-Z - X \pm Y). \quad (11d)$$

The fourth and last assertion concerns the state. The bases $\{|0_A^p⟩, |1_A^p⟩\}$ and $\{|0_B^p⟩, |1_B^p⟩\}$ 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

$$|ψ⟩ = \sum_{p=1}^{n_1} \lambda_p(|0_A^p0_B^p⟩ + |1_A^p1_B^p⟩) = \sqrt{2} \sum_{p=1}^{n_1} \lambda_p^p|φ^+_p⟩. \quad (12)$$

Notice that $|φ^+_p⟩$ is the Einstein-Podolsky-Rosen singlet in the space $\mathcal{H}_A^p \otimes \mathcal{H}_B^p$, restricted to which Alice’s and Bob’s observables are given by Eqs. (9) and (11). For each $i$, we arrange that $A_3^i = Y$ for $p \leq r_i$, and $A_3^i = -Y$ for $p > r_i$, where $0 \leq r_i \leq n_i$. For any Schmidt coefficients $\lambda_i$ 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 measures 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 $su(2)$ representations and an unknown number of ‘transposed’ $su(2)$ 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

$$⟨φ_+|a_2a_3(b_1 + b_2)|φ_+⟩ =$$

$$= ⟨Φ(A_2|ψ⟩)Φ(A_3(B_1 + B_2)|ψ⟩), \quad (13)$$

But $⟨φ_+|a_2a_3(b_1 + b_2)|φ_+⟩ = 2i/\sqrt{3}$ and

$$⟨ψ|A_2A_3(B_1 + B_2)|ψ⟩ = \frac{2i}{\sqrt{3}} \sum_{i=1}^{n_1} λ_i^2(4r_i - 2n_i). \quad (14)$$

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 $\Phi$ given by the circuit

\[
\begin{array}{c}
|0_a\rangle \\
|\psi\rangle \\
|0_b\rangle
\end{array}
\begin{array}{c}
H \\
\sqrt{\frac{3}{2}} (B_1 + B_2) \\
H
\end{array}
\begin{array}{c}
A_1 \\
\sqrt{\frac{3}{2}} (B_1 + B_3) \\
A_2
\end{array}
\]

(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 Merzky-Yao test, see [8], and McKague et al. [16] used it to show that the standard scenario in which the Clauser-Mosca used this isometric embedding to develop a generalization of Equation (16) is not valid. Instead we have that $|\chi\rangle$ is a Schmidt decomposition, with $i$ labeling the $m$ different Schmidt coefficients and $d_i$ being the multiplicity of $\lambda_i$. Define

\[
D_1 = \frac{1}{\sqrt{3}} (A_1 + A_2 + A_3), \\
D_2 = \frac{1}{\sqrt{3}} (A_1 - A_2 - A_3), \\
D_3 = \frac{1}{\sqrt{3}} (-A_1 + A_2 - A_3), \\
D_4 = \frac{1}{\sqrt{3}} (-A_1 - A_2 + A_3).
\]

Then $\sum_{i=1}^4 (D_i - B_i)^2 = 8 \lambda_1^2 - 2 \Sigma / \sqrt{3}$ and, hence,

\[
\sum_{i=1}^4 \lambda_i D_i |u_{i_{1}'} v_{i_{2}'}\rangle = \sum_{i=1}^4 \lambda_i B_i |u_{i'_{1}} v_{i'_{2}}\rangle.
\]

Multiplication of both sides by $|w, v_{q}^j\rangle$, where $|w\rangle$ is any vector in $H_A$ perpendicular to the support of $\text{tr}_B |\psi\rangle$, yields the identity $\lambda_j (\langle w | D_j | u_{i_{1}'} v_{i_{2}'}\rangle = 0$. Since the indices $j$ and $q$ are arbitrary and $\lambda_j > 0$, this proves that $D_j$ preserves the support of $\text{tr}_B |\psi\rangle$. Then so does each $A_k$. A similar argument shows that the operators $B_i$ preserve the support of the marginal state $\text{tr}_A |\psi\rangle$.

Next we prove that Alice’s and Bob’s observables preserve the eigenvalues of the marginal states. From Eq. (21) follows that for any two pairs of indices $(i_{1}, p_{1})$ and $(i_{2}, p_{2})$, one has

\[
\lambda_{i_{1}} (|u_{i_{1}} v_{i_{2}}\rangle |D_{i_{1}}| u_{i_{2}} v_{i_{2}}\rangle = \lambda_{i_{2}} (|u_{i_{1}} v_{i_{2}}\rangle |B_{i} | u_{i_{2}} v_{i_{2}}\rangle.
\]

This, in turn, implies that

\[
\lambda_{i_{1}}^2 (|u_{i_{1}} v_{i_{2}}\rangle |D_{i_{1}}| u_{i_{2}} v_{i_{2}}\rangle = \lambda_{i_{2}}^2 (|u_{i_{1}} v_{i_{2}}\rangle |B_{i} | u_{i_{2}} v_{i_{2}}\rangle.
\]

From Eq. (23) we can deduce that $D_j$ and, hence, each $A_k$ preserves the eigenvalues $H_{A_{j}}$. By an identical argument also the operators $B_i$ preserve the eigenvalues $H_{B_{i}}$. We write $A_k$ and $B_l$ for the restrictions of $A_k$ and $D_l$ to $H_{A_{j}}$, and $B_l$ for the restriction of $B_l$ to $H_{B_{i}}$.

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

\[
(D_{j_{1}})^2 = 1 + \frac{1}{3} \{A_{j_{1}}, A_{j_{2}}\} + \{A_{j_{1}}, A_{j_{3}}\} + \{A_{j_{2}}, A_{j_{3}}\}, \\
(D_{j_{2}})^2 = 1 - \frac{1}{3} \{A_{j_{1}}, A_{j_{2}}\} - \{A_{j_{1}}, A_{j_{3}}\} + \{A_{j_{2}}, A_{j_{3}}\}, \\
(D_{j_{3}})^2 = 1 - \frac{1}{3} \{A_{j_{1}}, A_{j_{2}}\} + \{A_{j_{1}}, A_{j_{3}}\} - \{A_{j_{2}}, A_{j_{3}}\}, \\
(D_{j_{4}})^2 = 1 + \frac{1}{3} \{A_{j_{1}}, A_{j_{2}}\} - \{A_{j_{1}}, A_{j_{3}}\} - \{A_{j_{2}}, A_{j_{3}}\}.
\]

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

\[
\{A_{j_{1}}, A_{j_{2}}\} = \{A_{j_{1}}, A_{j_{3}}\} = \{A_{j_{2}}, A_{j_{3}}\} = 0.
\]
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, $\mathcal{H}_A^i = \bigoplus_{n=1}^{n_i} \mathcal{H}_A^{ip}$, 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 $\{|s_A^i\rangle\}_{s=1}^{2n_i}$ in each $\mathcal{H}_A^i$ such that for every $1 \leq p \leq n_i$, $\{|(2p-1)\rangle_A^i, (2p)\rangle_A^i\}$ 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 $(A_3^{ip})_{p1}^2$ be the $2 \times 2$ matrix which in the provisional basis describes how $A_3^{ip}$ connects $\mathcal{H}_A^{ip}$ to $\mathcal{H}_A^{ip'}$. Then, by Eq. (25), and since $A_3^i$ is Hermitian, $(A_3^{ip})_{p2}^2 = \omega_2^p Y$ for some real number $\omega_2^p$. Next introduce a tensor product structure in $\mathcal{H}_A^i$ by writing $(2p-1)\rangle_A^i = |p\rangle \otimes |0\rangle$ and $(2p)\rangle_A^i = |p\rangle \otimes |1\rangle$. Then $A_1^i = \mathbb{1} \otimes Z$, $A_2^i = \mathbb{1} \otimes X$, and $A_3^i = \Omega \otimes Y$, where $\Omega$ is the $n_i \times n_i$ matrix whose element on position $(p_1, p_2)$ is $\omega_2^p$. Being Hermitian, $\Omega$ can be diagonalized, say $U^\dagger \Omega U = \text{diag}(\omega_1, \omega_2, \ldots, \omega_{n_i})$. Then

\begin{align}
(U^\dagger \otimes \mathbb{1}) A_1^i (U \otimes \mathbb{1}) &= \mathbb{1} \otimes Z, \\
(U^\dagger \otimes \mathbb{1}) A_2^i (U \otimes \mathbb{1}) &= \mathbb{1} \otimes X, \\
(U^\dagger \otimes \mathbb{1}) A_3^i (U \otimes \mathbb{1}) &= \text{diag}(\omega_1, \omega_2, \ldots, \omega_{n_i}) \otimes Y.
\end{align}

Each diagonal element $\omega_p$ equals $+1$ or $-1$ because $A_3^i$ is an involution. We choose $U$ such that $\omega_p = +1$ for $p \leq r_i$ 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

\begin{equation}
|s_B^i\rangle = \sum_{p=1}^{n_i} |v_p^i\rangle \langle s_A^i | u_p^i\rangle.
\end{equation}

Then $\langle s_B^i | B_1^i | s_B^i\rangle = \langle t_A^i | D_1^i | s_A^i\rangle$ and, hence, by Eq. (20),

\begin{align}
B_1^i &= \frac{1}{\sqrt{3}} (A_1^i + A_2^i + A_3^i)^T, \\
B_2^i &= \frac{1}{\sqrt{3}} (A_1^i - A_2^i - A_3^i)^T, \\
B_3^i &= \frac{1}{\sqrt{3}} (-A_1^i + A_2^i - A_3^i)^T, \\
B_4^i &= \frac{1}{\sqrt{3}} (-A_1^i - A_2^i + A_3^i)^T.
\end{align}

This proves Eq. (11).

The assertion about the state is a straightforward conse-}

quence of the calculation

\begin{equation}
|\psi\rangle = \sum_{i=1}^{m} \sum_{p=1}^{d_i} \lambda_i |u_p^i\rangle v_p^i\rangle
= \sum_{i=1}^{m} \sum_{p=1}^{d_i} \sum_{s=1}^{d_i} \lambda_i |s_A^i t_B^i\rangle \langle s_A^i | u_p^i\rangle (t_B^i | v_p^i\rangle
= \sum_{i=1}^{m} \sum_{s=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 \langle (2p-1)\rangle_A^i (2p-1)\rangle_B^i + |(2p)\rangle_A^i (2p)\rangle_B^i.
\end{equation}

If we define

\begin{equation}
|0_A^i\rangle = |(2p-1)\rangle_A^i, \quad |1_A^i\rangle = |(2p)\rangle_A^i,
|0_B^i\rangle = |(2p-1)\rangle_B^i, \quad |1_B^i\rangle = |(2p)\rangle_B^i,
\end{equation}

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 Acin et al. [6]. We discuss this construction in a companion paper [10].
ACKNOWLEDGMENTS

We thank Mohamed Nawareg and Massimiliano Smania for fruitful discussions, Jędrzej Kaniewski and Yeong-Cherng Liang for useful comments on an earlier draft of the paper, and Nicolas Gisin for encouraging remarks. We also thank Pär Z. Andersson who has produced Fig. 1. AC 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. Badzigić, I. Dumitru, and A. Cabello, Device-independent certification of two bits of randomness from one entangled bit and 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 Information & Computation 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, 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: Math. Theor. 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).