# Device-Independent Certification of Genuinely Entangled Subspaces

Flavio Baccari,[1,*] Remigiusz Augusiak,[2,†] Ivan Šupić,[3] and Antonio Acín[4,5]
[1]Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, 85748 Garching, Germany
[2]Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland
[3]Département de Physique Appliquée, Université de Genève, 1211 Genève, Switzerland
[4]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
[5]ICREA–Institució Catalana de Recerca i Estudis Avancats, 08011 Barcelona, Spain

(Received 23 March 2020; accepted 7 December 2020; published 30 December 2020)

Self-testing is a procedure for characterizing quantum resources with the minimal level of trust. Up to now it has been used as a device-independent certification tool for particular quantum measurements, channels, and pure entangled states. In this work we introduce the concept of self-testing more general entanglement structures. More precisely, we present the first self-tests of an entangled subspace—the five-qubit code and the toric code. We show that all quantum states maximally violating a suitably chosen Bell inequality must belong to the corresponding code subspace, which remarkably includes also mixed states.

DOI: 10.1103/PhysRevLett.125.260507

*Introduction.*—Authentically quantum effects such as entanglement and measurement incompatibility play a key role in the development of various quantum information protocols. In this context, verifying that a device or an algorithm indeed uses quantum resources is a very important task. There are many frameworks for such kinds of verification, in a broad sense known as testing of quantum properties [1]. In a standard quantum property testing scenario a user, usually called verifier, aims to certify that their devices, commonly named provers, exploit some quantum resource.

The strongest form of verification is device independent [2–4] in which no assumptions are made on the devices; they are simply treated as black boxes. A device-independent certification performed by a completely classical verifier is also known as self-testing [5,6]. In such a scenario the only way to verify the "quantumness" of the provers is to interact with them, for example by asking them some questions by means of classical communication channels and receiving the answers through the same channels (see Fig. 1). Any information about the underlying physical system is then inferred by the verifier from the observed correlations between those answers.

In a self-testing scenario, a central concept is that of Bell nonlocality [7]. Observing nonlocal behaviors is essential to certify several interesting properties of quantum systems, such as the exact form of a quantum state [8–10], measurement [11,12], or a channel [13,14], all this up to certain well-understood equivalences. However, self-testing has so far been deemed as a procedure tailored to a single quantum state and it has been a highly nontrivial question if it can be used to certify less specific quantum properties.

Here, we address this problem and introduce the definition of self-testing of an entangled subspace. Although

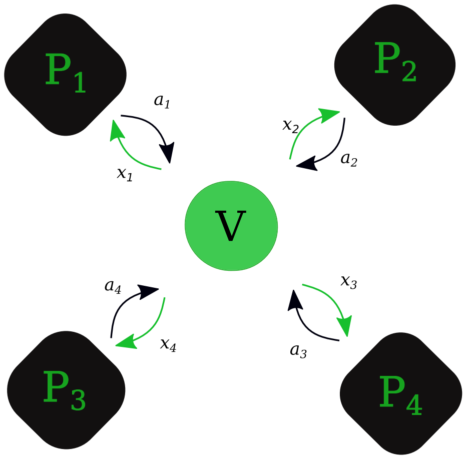

FIG. 1. A model of self testing. A classical verifier $V$ aims to certify a particular quantum property of the resource shared by noncommunicating provers $P_i$. The verifier sends different classical inputs $x_i$ to the provers and they respond with classical outputs $a_i$. If nonlocal, correlations between the outputs allow the verifier to make nontrivial conclusions about that quantum property.

Bell inequalities maximally violated by more than a single pure state are already known (e.g., Refs. [15,16]), we show for the first time that this kind of violation can be exploited to certify that a quantum state belongs to such a subspace. Hence, we present a relaxed definition of self-testing that is not able to distinguish between any mixture of the vectors belonging to the self-tested subspace. We present a first application of such a relaxed self-testing by constructing Bell inequalities whose maximal violation is attained by states belonging to some genuinely entangled subspaces, which are subspaces of multipartite Hilbert spaces consisting of only genuinely entangled states (see, e.g., [17]). As a paradigmatic example, we focus on those used in stabilizer error correcting codes [18], such as the five-qubit code [19,20] and the toric code [21], the latter allowing us to show that self-testing of subspaces is possible for systems composed of any number of particles. Interestingly, while still being based on the stabilizer formalism, our Bell inequalities are inequivalent to those presented in [22,23].

*Preliminaries.*—We begin with some preliminaries.

*The Bell scenario.*—Following the scenario depicted in Fig. 1, let us consider $N$ spatially separated provers $P_i$ sharing a quantum state $\rho_P$ that acts on some finite-dimensional Hilbert space $\mathcal{H}_P = \mathcal{H}_{P_1} \otimes \cdots \otimes \mathcal{H}_{P_N}$ and a verifier $V$ asking them questions $x_i$. Upon receiving the question $x_i$ the prover $P_i$ measures a quantum observable $A_{x_i}^{(i)}$ on their share of $\rho_P$ and returns $V$ the outcome of that measurement $a_i$. Here, we consider the simplest scenario in which all provers measure binary observables whose outcomes are labeled $a_i = \pm 1$. If this procedure is repeated sufficiently many times, the verifier can estimate the vector $\mathcal{P}$ of expectation values

$$\langle A_{x_{i_1}}^{(i_1)} \cdots A_{x_{i_k}}^{(i_k)} \rangle = \mathrm{Tr}[(A_{x_{i_1}}^{(i_1)} \otimes \cdots \otimes A_{x_{i_k}}^{(i_k)})\rho_P], \qquad (1)$$

with $i_1 < i_2 < \cdots < i_k$, $k = 1, \ldots, N$, and $i_j = 1, \ldots, N$. Below we refer to $\mathcal{P}$ as behavior or simply correlations.

The key ingredient making device-independent verification possible is that the correlations observed by the verifier exhibit quantum nonlocality [7]. The phenomenon of nonlocality consists of the existence of quantum correlations that cannot be reproduced by any local-realistic theory, or, phrasing alternatively, that violate Bell inequalities which bound the strength of correlations achievable in such theories. The most general form of a multipartite Bell inequality is

$$I_N \coloneqq \sum_{k=1}^{N} \sum_{\substack{1 \le i_1 < i_2 < \cdots < i_k \le N \\ x_{i_1}, \ldots, x_{i_N} = 0,1}} \alpha_{x_{i_1}, \ldots, x_{i_k}}^{i_1, \ldots, i_k} \langle A_{x_{i_1}}^{(i_1)} \cdots A_{x_{i_k}}^{(i_k)} \rangle \le \beta_c, \qquad (2)$$

where $\beta_c$ is the local bound, that is, the maximal value of $I_N$ over all local-realistic correlations.

*Genuinely entangled subspaces.*—Consider a bipartition of $N$ provers into two disjoint and nonempty groups $G$ and $G'$ and a pure multipartite state $|\psi\rangle \in \mathcal{H}_P$. We call it genuinely entangled if for any such bipartition $G|G'$ it cannot be written as a tensor product of pure states corresponding to $G$ and $G'$. We then call a subspace of $\mathcal{H}_P$ genuinely entangled if it consists of only genuinely multipartite entangled states (cf. Ref. [17]).

*Stabilizer codes.*—The $N$-fold tensor products of the Pauli operators $\{X, Z, Y, \mathbb{1}\}$ with the overall factor $\pm 1$ or $\pm i$ forms the Pauli group $\mathbb{P}_N$ under matrix multiplication. A stabilizer $\mathbb{S}_N$ is any Abelian subgroup of $\mathbb{P}_N$, and the stabilizer coding space $C_N$ consists of all vectors $|\psi\rangle$ such that $S_i|\psi\rangle = |\psi\rangle$ for any $S_i \in \mathbb{S}_N$. Hence, $C_N$ is the eigenspace of $\mathbb{S}_N$ corresponding to the eigenvalue $+1$. Its dimension depends on the number of independent generators $S_i$ of the stabilizer or, equivalently, the number of elements of $\mathbb{S}_N$: if $\mathbb{S}_N$ has $2^{N-k}$ elements for some $0 \le k < N$, then $\dim C_N = 2^k$. A stabilizer subspace of dimension $2^k$ might be used to encode $k$ logical qubits; the corresponding vectors belonging to $C_N$ are called quantum code words (for more details see Refs. [18,24,25]).

In the particular case of $|\mathbb{S}_N| = 2^N$, the subgroup stabilizes a unique state, known as the stabilizer state. Any stabilizer state is equivalent to a certain graph state under local unitary operations (see, e.g., Ref. [26]), and self-testing methods for graph states are already known [9,27]. Our aim here is to go beyond the $k = 1$ case and provide device-independent certification methods for higher-dimensional subspaces $C_N$. In order to exploit nonlocality as the resource for certification, a natural starting point are those stabilizers that generate genuinely entangled subspaces. In Supplemental Material A [28] we also provide a simple sufficient criterion to ascertain that a given stabilizer gives rise to a genuinely entangled subspace.

*Self-testing of entangled subspaces.*—Let us start off by providing the definition of self-testing of an entangled subspace. To this aim, let $\mathcal{H}_P$ be, as before, the prover's Hilbert space. Let then $\mathcal{H}_{P'}$ be a Hilbert space with dimension equal to that of the entangled subspace we want to self-test whereas $\mathcal{H}_{P''}$ some auxiliary Hilbert space such that $\dim \mathcal{H}_P = \dim \mathcal{H}_{P'} \dim \mathcal{H}_{P''}$. Notice that for the examples considered below $\mathcal{H}_{P'} = (\mathbb{C}^2)^{\otimes N}$.

Let then $|\phi\rangle_{PE}$ be a purification of the mixed state $\rho_P$ shared by the provers to a larger Hilbert space $\mathcal{H}_{PE} = \mathcal{H}_P \otimes \mathcal{H}_E$, where $\mathcal{H}_E$ represents all potential degrees of freedom which the provers do not have access to.

**Definition:** The behavior $\mathcal{P}$ self-tests the entangled subspace spanned by the set of entangled states $\{|\psi_i\rangle\}_{i=1}^{k}$ if for any pure state $|\phi\rangle_{PE} \in \mathcal{H}_{PE}$ compatible with $\mathcal{P}$ through (1) one can deduce that (i) every local Hilbert space has the form $\mathcal{H}_{P_i} = \mathcal{H}_{P'_i} \otimes \mathcal{H}_{P''_i}$; (ii) there exists a local unitary transformation $U_P = U_1 \otimes \cdots \otimes U_N$ acting on $\mathcal{H}_P$ such that

$$U_P \otimes \mathbb{1}_E(|\phi\rangle_{PE}) = \sum_i c_i |\psi_i\rangle_{P'} \otimes |\xi_i\rangle_{P''E}, \qquad (3)$$

for some normalized states $|\xi_i\rangle \in \mathcal{H}_{P''} \otimes \mathcal{H}_E$ and some nonnegative numbers $c_i \geq 0$ such that $\sum_i c_i^2 = 1$.

Note that, if the set $\{|\psi_i\rangle\}_{i=1}^k$ spans a genuinely entangled subspace, then the state on the right-hand side of Eq. (3) is genuinely multipartite entangled with respect to the partition $\mathcal{H}_{P_1}|\mathcal{H}_{P_2}|\cdots|\mathcal{H}_{P_N}$ [33]. This implies that the above self-testing statement can also be used as a certificate of genuine multipartite entanglement for the measured state. Note also that, analogously to the case of state self-testing, a subspace can be certified from the observed correlations $\mathcal{P}$ up to certain equivalences such as local unitary transformations or extra degrees of freedom described by $\mathcal{H}_{P''}$ and $\mathcal{H}_E$. Interestingly, here we identify an additional degree of freedom encoded in the scalars $c_i$. The freedom of varying the values of those scalars implies that self-testing of an entangled subspace can also be understood as self-testing of all mixed states supported on that subspace and giving rise to the correlations $\mathcal{P}$.

In what follows, we show how to prove a self-testing statement according to the above definition based solely on the fact that the observed behavior maximally violates a certain multipartite Bell inequality. As target subspaces we choose those used in quantum error correction. As quantum code words are highly entangled states, it is natural to expect them to display nonlocal correlations [34,35]. Notice that for our purposes it is not enough to simply observe nonlocal correlations, but it is crucial to prove that states belonging to the subspaces of interest maximally violate a Bell inequality and such an inequality has to be carefully tailored to the considered code space. A couple of methods based on the stabilizer formalism that does the job was recently put forward in Refs. [22,23]. Here, we provide an alternative construction, inspired by Ref. [27], that allows us to make a straightforward connection to the self-testing proof. Before moving to the presentation of the results, it is important to emphasize that, as many prior works on self-testing, we assume that the source produces identical and independently distributed copies of the state $\rho_P$.

*The five-qubit code.*—The five-qubit code is the smallest possible code that corrects single-qubit errors [19,20] on a logical qubit. It is also a stabilizer code, generated by the following four operators acting on $(\mathbb{C}^2)^{\otimes 5}$:

$$S_1 = X^{(1)}Z^{(2)}Z^{(3)}X^{(4)}, \qquad S_2 = X^{(2)}Z^{(3)}Z^{(4)}X^{(5)},$$
$$S_3 = X^{(1)}X^{(3)}Z^{(4)}Z^{(5)}, \qquad S_4 = Z^{(1)}X^{(2)}X^{(4)}Z^{(5)}, \qquad (4)$$

where $X^{(i)}, Z^{(i)}$ are the Pauli matrices acting on qubit $i$. One can check that the four operators above are independent and hence the code space, denoted $C_5$, is two dimensional, and, importantly, it is genuinely entangled (see Supplemental Material A [28] for a proof).

In order to prove a self-testing statement for this subspace, we introduce a Bell inequality that is maximally violated by any pure state from $C_5$. To do so we build the inequality directly from the generators (4). For the first party we assign $X^{(1)} \to (A_0^{(1)} + A_1^{(1)})/\sqrt{2}$ and $Z^{(1)} \to (A_0^{(1)} - A_1^{(1)})/\sqrt{2}$, while for the remaining parties we simply replace $X^{(i)} \to A_0^{(i)}$ and $Z^{(i)} \to A_1^{(i)}$, where $A_j^{(i)}$ are arbitrary binary observables (of unspecified but finite dimension) that are to be measured in a Bell experiment. Let then $\tilde{S}_i$ denote operators obtained from (4) by making the above substitutions.

Let us also define the following Bell inequality:

$$\begin{aligned} I_5 = {} & \langle (A_0^{(1)} + A_1^{(1)})A_1^{(2)}A_1^{(3)}A_0^{(4)}\rangle + \langle A_0^{(2)}A_1^{(3)}A_1^{(4)}A_0^{(5)}\rangle \\ & + \langle (A_0^{(1)} + A_1^{(1)})A_0^{(3)}A_1^{(4)}A_1^{(5)}\rangle \\ & + 2\langle (A_0^{(1)} - A_1^{(1)})A_0^{(2)}A_0^{(4)}A_1^{(5)}\rangle \leq 5, \qquad (5) \end{aligned}$$

whose local bound was directly computed by optimizing $I_5$ over deterministic strategies for which $A_{x_i}^{(i)} = \pm 1$. The above inequality is obtained by choosing a suitable linear combination of the expectation values of $\tilde{S}_i$, indeed it can be checked that $I_5 = \sqrt{2}(\langle \tilde{S}_1\rangle + \langle \tilde{S}_3\rangle) + \langle \tilde{S}_2\rangle + 2\sqrt{2}\langle \tilde{S}_4\rangle$.

The maximal quantum value of $I_5$ can also be straightforwardly determined and it amounts to $\beta_q = 4\sqrt{2} + 1$. To see that such value can be achieved by any state from $C_5$, let us notice that by making the following measurement choices

$$A_0^{(1)} = \frac{X + Z}{\sqrt{2}}, \qquad A_1^{(1)} = \frac{X - Z}{\sqrt{2}}, \qquad (6)$$

for the first party and $A_0^{(i)} = X$ and $A_1^{(i)} = Z$ $(i = 2, \ldots, 5)$ for the remaining ones, $I_5$ becomes the expectation value of the Bell operator: $\mathcal{B}_5' = \sqrt{2}(S_1 + S_2 + 2S_4) + S_3$. It follows that its maximal eigenvalue is $4\sqrt{2} + 1$ and it is precisely associated with the eigenspace stabilized by the four generators $S_i$ given in Eq. (4).

To prove that there does not exist a quantum state and observables giving rise to a higher violation of $I_5$ it is enough to show that the following decomposition

$$\begin{aligned} \beta_q \mathbb{1} - \mathcal{B}_5 = {} & \frac{1}{\sqrt{2}}(\mathbb{1} - \tilde{S}_1)^2 + \frac{1}{2}(\mathbb{1} - \tilde{S}_2)^2 \\ & + \frac{1}{\sqrt{2}}(\mathbb{1} - \tilde{S}_3)^2 + \sqrt{2}(\mathbb{1} - \tilde{S}_4)^2, \qquad (7) \end{aligned}$$

holds true, which implies that the eigenvalues of $\mathcal{B}_5$ do not exceed $\beta_q$ for any choice of local observables $A_{x_i}^{(i)}$.

The maximal violation of inequality (5) allows one to make the following self-testing statement.

**Fact 1:** Any behavior achieving the maximal quantum violation of $I_5$ self-tests the entangled subspace $C_5$.

*Proof.*—Here, we provide a sketch of the proof for illustrative purposes, deferring the details to Supplemental Material B [28]. Consider a state $|\phi\rangle_{PE} \in \mathcal{H}_{PE}$ and observables $A_{x_i}^{(i)}$ acting on $\mathcal{H}_{P_i}$ that maximally violate inequality (5). From the decomposition (7) one deduces that

$$(\tilde{S}_i \otimes \mathbb{1}_E)|\phi\rangle_{PE} = |\phi\rangle_{PE} \tag{8}$$

for $i = 1, \ldots, 4$, which can be used to prove the existence of local unitary operations $U_i$ acting on $\mathcal{H}_{P_i}$ such that $U\tilde{S}_i U^\dagger = S_i \otimes \mathbb{1}_{P''}$ for $i = 1, \ldots, 4$, where $U = U_1 \otimes \cdots \otimes U_5$ and the operators $S_i$ are given in Eq. (4). This allows us to rewrite Eq. (8) as $(S_i \otimes \mathbb{1}_{P''E})|\psi\rangle_{PE} = |\psi\rangle_{PE}$ with $|\psi\rangle_{PE} = (U \otimes \mathbb{1}_E)|\phi\rangle_{PE}$. As we show in Supplemental Material B [28], the most general state satisfying all these four conditions is exactly $c|\psi_1\rangle \otimes |\xi_1\rangle + \sqrt{1-c^2}|\psi_2\rangle \otimes |\xi_2\rangle$, where $0 \le c \le 1$, $|\psi_1\rangle$, and $|\psi_2\rangle$ are two orthogonal five-qubit states spanning $C_5$ whereas $|\xi_1\rangle$ and $|\xi_2\rangle$ are some auxiliary quantum states from $\mathcal{H}_{P''} \otimes \mathcal{H}_E$.

*The toric code.*—The toric code is a paradigmatic example of topological quantum error correction codes [21]. It allows one to store two logical qubits in four multiqubit pure states of arbitrarily large number of particles. The logical qubits can be associated with ground states of a 1/2-spin model on a torus, that is, a two-dimensional spin square lattice with periodic boundary conditions in which qubits are associated with the edges (see Fig. 2).

The toric code is also a stabilizer code with two types of stabilizing operators: the vertex and plaquette operators

$$S_v = \prod_{i\in v} X^{(i)}, \qquad S_p = \prod_{i\in p} Z^{(i)}. \tag{9}$$

For each of the generators $S_v$ and $S_p$, the product runs over operators acting on qubits sharing the same vertex $v$ or plaquette $p$, respectively (see Fig. 2). The above generators are not all independent, since they satisfy $\prod_v S_v = \prod_p S_p = \mathbb{1}$. By simple counting argument, it follows that the set of states stabilized by these operators spans a four-dimensional subspace, denoted $C_N^{\text{tor}}$, for any choice of the lattice size $L$.

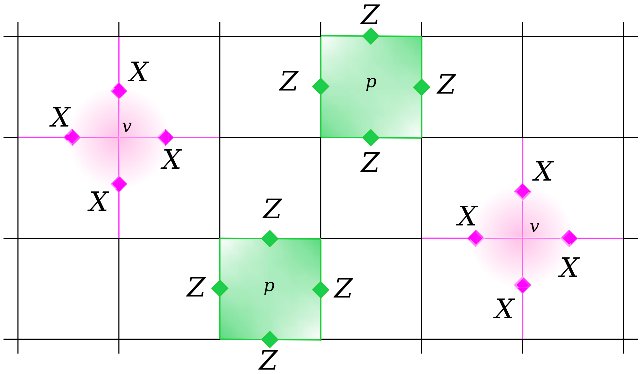

FIG. 2. The toric code. Each edge of the lattice represents a qubit. Stabilizing operators can be divided in two groups: those associated with each lattice vertex $v$ with $X$ acting on every qubit associated with an edge attached to the given vertex, or associated with each plaquette $p$ of the lattice with $Z$ acting on each qubit represented by an edge surrounding the plaquette.

The Bell inequality maximally violated by any mixed state supported in $C_N^{\text{tor}}$ can be derived in a manner analogous to the previous example. For an arbitrarily chosen edge $j$, we substitute the Pauli operators $X^{(j)}, Z^{(j)}$ acting on the corresponding qubit with the combinations $(A_0^{(j)} \pm A_1^{(j)})/\sqrt{2}$, while for the other qubits we simply have $X^{(i)}, Z^{(i)} \to A_0^{(i)}, A_1^{(i)}$ $(i \neq j)$. By applying this substitution to $S_v$ and $S_p$ we obtain operators $\tilde{S}_v$ and $\tilde{S}_p$ from which we obtain the following Bell inequality

$$I_N^{\text{tor}} \coloneqq \sum_v \langle \tilde{S}_v \rangle + \sum_p \langle \tilde{S}_p \rangle \le \beta_c^{\text{tor}}(N). \tag{10}$$

It is not difficult to realize that its classical bound $\beta_c^{\text{tor}}(N)$ amounts to $\beta_c^{\text{tor}}(N) = 2\sqrt{2} + |p| - 2 + |v| - 2 = N - 2\sqrt{2}(\sqrt{2}-1)$. Moreover, as proven in the Supplemental Material B [28], the quantum bound is $\beta_q^{\text{tor}}(N) = 4 + |p| + |v| - 4 = N > \beta_c^{\text{tor}}(N)$. It follows that any pure state from $C_N^{\text{tor}}$ achieves it, meaning that $C_N^{\text{tor}}$ is an entangled subspace; in fact, in Supplemental Material A [28] we prove it to be genuinely entangled. More importantly, as we prove in Supplemental Material B [28], the following self-testing statement can be made for it.

**Fact 1:** Any $N$-partite behavior $\mathcal{P}$ achieving the maximal quantum violation of $I_N^{\text{tor}}$ self-tests the entangled subspace $C_N^{\text{tor}}$.

*Noise robustness.*—In practice, finite sampling effects and experimental errors render the maximal violation of a Bell inequality impossible to reach. For this reason, it is important to be able to make certification statements when the violation is not maximal. In Supplemental Material C [28] we provide a framework allowing us to tackle this problem and use it to obtain a numerical indication of how robust our self-testing statement is for the five-qubit code. In particular, Fig. 3 shows how the numerically estimated subspace extractability, which we define to quantify how close is the self-tested subspace to the desired one, scales as a function of the observed Bell violation.

*Geometrical considerations.*—A Bell inequality is generally believed to be useful for state self-testing only if its maximal violation can be associated with a single quantum state and to a single point in the set of quantum correlations [16]. Remarkably, subspace self-testing allows one to make nontrivial statements for Bell inequalities maximally violated by more than one correlation point. As we show in Supplemental Material D [28], the subspace of quantum correlations maximally violating inequalities (5) and (10) is

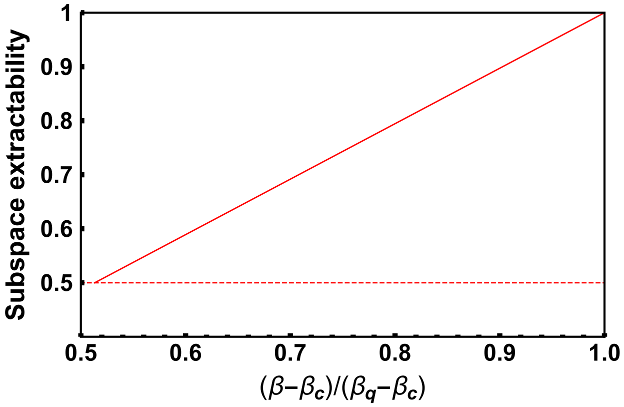

FIG. 3. Numerical estimation of the minimal subspace extractability for the target five-qubit Shor's code subspace as a function of the relative observed violation $(\beta-\beta_c)/(\beta_q-\beta_c)$ of the corresponding Bell inequality $I_5$.

spanned by two and three linearly independent correlation vectors, respectively. Our results on subspace self-testing can thus be seen as complementary to the weaker form of self-testing presented in [36]. While in [36] the multiple correlations points associated with the self-testing statement are achieved by varying the measurement operators on the same state, we instead obtain a similar phenomenon by performing the same measurements on different quantum states.

*Discussion.*—We introduce the notion of self-testing of entangled subspaces—a device-independent method of certification that an entangled state belongs to a certain subspace of dimension at least two. By exploiting the formalism of stabilizer error correction codes we present two examples of multipartite Bell inequalities whose maximal quantum violation serves the purpose, that is, enables self-testing of entangled subspaces. We also provide a framework to study the robustness of subspace self-testing when the experimental imperfections are taken into account and use it to investigate how robust is the self-testing statement for the five-qubit code. On a more fundamental level, our Bell inequalities can be used to identify flat structures in the boundary of the sets of quantum correlations.

Our work opens a plethora of possibilities for future research. By proposing a clear strategy to derive a Bell inequality and by being based on the broadly used stabilizer formalism, we believe that our self-testing technique has the potential to be generalized to other genuinely entangled stabilizer subspaces. From a broader point of view, it would be very interesting to understand which conditions a stabilizer subspace has to satisfy in order to be suitable for self-testing (see [37] for recent progress concerning this point). We also believe that the presented techniques are a promising tool to quantify the average fidelity of quantum codeword preparations, thus opening the way to the device-independent certification of quantum error correction codes. Characterizing in more detail the robustness properties of our self-testing methods would also be essential for that.

We acknowledge discussions with O. Makuta. F. B. acknowledges the support of the Spanish MINECO in the form of a Severo Ochoa Ph.D. fellowship during his time at ICFO and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation)—Project No. 414325145 in the framework of the Austrian Science Fund (FWF): SFB F71 during his time at MPQ. I. Š. acknowledges support from SNSF (Starting grant DIAQ). R. A. acknowledges the support from the Foundation for Polish Science through the First Team project (First TEAM/2017- 4/31) cofinanced by the European Union under the European Regional Development Fund. A. A. acknowledges support from the ERC AdG CERQUTE, the AXA Chair in Quantum Information Science, the Government of Spain (FIS2020-TRANQI and Severo Ochoa CEX2019-000910-S), Fundació Cellex, Fundació Mir-Puig, Generalitat de Catalunya (CERCA, AGAUR SGR 1381 and QuantumCAT).

[*]flavio.baccari@mpq.mpg.de
[†]augusiak@cft.edu.pl

[1] A. Montanaro and R. de Wolf, Theory Comput. Graduate Surv. **7**, 1 (2016).

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

[3] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning *et al.*, Nature (London) **464**, 1021 (2010).

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

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

[6] I. Šupić and J. Bowles, Quantum **4**, 337 (2020).

[7] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).

[8] A. Coladangelo, K. T. Goh, and V. Scarani, Nat. Commun. **8**, 15485 (2017).

[9] M. McKague, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science Vol. 6745, edited by D. Bacon, M. Martin-Delgado, and M. Roetteler (Springer, Berlin, Heidelberg, 2014), pp. 104–120.

[10] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, New J. Phys. **20**, 083041 (2018).

[11] J. Kaniewski, Phys. Rev. A **95**, 062323 (2017).

[12] S. Wagner, J.-D. Bancal, N. Sangouard, and P. Sekatski, Quantum **4**, 243 (2020).

[13] F. Magniez, D. Mayers, M. Mosca, and H. Ollivier, in *Automata, Languages and Programming*, edited by M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener (Springer Berlin Heidelberg, Berlin, Heidelberg, 2006), pp. 72–83.

[14] P. Sekatski, J.-D. Bancal, S. Wagner, and N. Sangouard, Phys. Rev. Lett. **121**, 180505 (2018).

[15] R. Augusiak and P. Horodecki, Phys. Rev. A **74**, 010305(R) (2006).

[16] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani, Phys. Rev. A **97**, 022104 (2018).

[17] M. Demianowicz and R. Augusiak, Phys. Rev. A **98**, 012313 (2018).

[18] D. E. Gottesman, Stabilizer codes and quantum error correction, Ph.D. Thesis, California Institute of Technology, 1997.

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

[20] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, Phys. Rev. Lett. **77**, 198 (1996).

[21] A. Y. Kitaev, Ann. Phys. (Amsterdam) **303**, 2 (2003).

[22] A. H. Shenoy and R. Srikanth, J. Phys. A **52**, 095302 (2019).

[23] M. Waegell and J. Dressel, npj Quantum Inf. **5**, 66 (2019).

[24] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[25] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[26] D.-M. Schlingemann, arXiv:quant-ph/0111080.

[27] F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín, Phys. Rev. Lett. **124**, 020402 (2020).

[28] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.125.260507 for a proof that the subspaces considered here contain only genuinely entangled states, proofs of Fact 1 and 2, an analysis of the robustness to noise of our self-testing statements and a detailed study of the geometrical structure of the faces maximally violating our inequalities, which includes Refs. [29–32].

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

[30] J. Kaniewski, Phys. Rev. Lett. **117**, 070402 (2016).

[31] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, Phys. Rev. A **80**, 062327 (2009).

[32] T. Coopmans, J. Kaniewski, and C. Schaffner, Phys. Rev. A **99**, 052123 (2019).

[33] Too see that, notice that upon performing a partial trace over the spaces $P''$ and $E$ and after a diagonalization, the resulting state $\rho_{P'} = \sum_i |\psi'_i\rangle\langle\psi'_i|$ is genuinely multipartite entangled, since it is fully supported on the subspace spanned by $\{|\psi_i\rangle\}_{i=1}^{k}$. It follows that the state $\rho_{P'P''}$ must also be genuinely multipartite entangled, since no GME state can be obtained after a partial trace of a non-GME one.

[34] D. P. DiVincenzo and A. Peres, Phys. Rev. A **55**, 4089 (1997).

[35] T. A. Walker, F. A. C. Polack, and S. L. Braunstein, Phys. Rev. Lett. **101**, 080501 (2008).

[36] J. Kaniewski, Phys. Rev. Research **2**, 033420 (2020).

[37] O. Makuta and R. Augusiak, arXiv:2012.01164.