Device-independent certification of 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 Fotòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
5 ICREA - Institució Catalana de Recerca i Estudis Avancats, 08011 Barcelona, Spain

Self-testing is a procedure for characterising 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.

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 kind 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 (DI) [2–4] in which no assumptions are made on the devices; they are simply treated as black-boxes. A DI 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 behaviours 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 genuinely entangled subspaces, which are subspaces of multipartite Hilbert spaces consisting of only genuinely entangled pure states (see, e.g., [15]). Although Bell inequalities maximally violated by more than a single pure state are already known (e.g. Refs. [16, 17]), 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 representative entangled subspaces, namely those used in stabilizer error correcting codes [18]. In particular, we focus on paradigmatic examples 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].

Preliminaries. We begin with some preliminaries.

1 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. Here we

![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 P1. 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.](image-url)
consider the simplest scenario in which all provers measure binary observables whose outcomes are labelled $a_i = \pm 1$. If this procedure is repeated sufficiently many times, the verifier can estimate the collection $\mathcal{P}$ of expectation values

$$
\langle A_{x_1}^{(i_1)} \cdots A_{x_k}^{(i_k)} \rangle = \text{Tr} \left[ \left( A_{x_1}^{(i_1)} \otimes \cdots \otimes A_{x_k}^{(i_k)} \right) \rho^P \right]
$$

(1)

with $i_1 < i_2 < \ldots < i_k$, $k = 1, \ldots, N$ and $i_j = 1, \ldots, N$. Below we refer to $\mathcal{P}$ as to behaviour 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. Recall the most general form of a multipartite Bell inequality to be

$$
I_N := \sum_{k=1}^{N} \sum_{x_{i_1}, \ldots, x_{i_k} = 0, 1} \alpha_{i_1, \ldots, i_k} \langle A_{x_1}^{(i_1)} \cdots A_{x_k}^{(i_k)} \rangle \leq \beta_c,
$$

(2)

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

(2) 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 entangled states (cf. Ref. [15]).

(3) Stabilizer codes. The $N$-fold tensor products of the Pauli operators $\{X, Z, Y, 1\}$ with the overall factor $\pm 1$ or $\pm i$ forms the Pauli group $\mathbb{P}_N$ under matrix multiplication. A stabilizer $S_N$ 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 $S_i \in S_N$. Hence, $C_N$ is the eigenspace of $S_N$ 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 $S_N$: if $S_N$ has $2^N-k$ elements for some $0 \leq k < N$, 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, 23, 24]).

In the particular case of $|S_N| = 2^N$, 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. [25]), and self-testing methods for graph states are already known [9, 26]. Our aim here is to go beyond the $k = 1$ case and provide device-independent certification methods for higher-dimensional subspaces $C_N$. Still, in order to exploit nonlocality as the resource for certification we restrict our attention to those stabilizers that generate genuinely entangled subspaces. In Appendix B 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 $\mathcal{H}_P^\prime$ be a Hilbert space with dimension equal to that of the entangled subspace we want to self-test whereas $\mathcal{H}_P^{\prime\prime}$ some auxiliary Hilbert space such that $\dim \mathcal{H}_P = \dim \mathcal{H}_P^\prime \dim \mathcal{H}_P^{\prime\prime}$. Notice that for the examples considered below $\mathcal{H}_P^\prime = (\mathbb{C}^2)^{\otimes N}$.

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 provers do not have access to.

Definition. The behaviour $\mathcal{P}$ 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 $\mathcal{H}_P = \mathcal{H}_P^\prime \otimes \mathcal{H}_P^{\prime\prime}$; ii) there exists a local unitary transformation $U_P = U_1 \otimes \cdots \otimes U_N$ acting on $\mathcal{H}_P$ such that

$$
(U_P \otimes \mathbb{I}_E)|\phi\rangle_{PE} = \sum_i p_i |\psi_i\rangle_{P^\prime} \otimes |\xi_i\rangle_{P^{\prime\prime},E}
$$

(3)

for some normalised states $|\xi_i\rangle \in \mathcal{H}_E$ and some positive numbers $p_i \geq 0$ such that $\sum_i p_i^2 = 1$.

Notice that, analogously to self-testing of quantum states, self-testing of subspaces, being based on drawing conclusions only from the observed correlations $\mathcal{P}$, can be done only up to certain equivalences such as local unitary transformations or extra degrees of freedom described by $\mathcal{H}_P^\prime$ and $\mathcal{H}_E$. Interestingly, here we identify an additional degree of freedom encoded in the scalars $p_i$. 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 will show how to prove a self-testing statement according to the above definition based solely on the fact that the observed behaviour 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 [27, 28]. 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 method based on the stabilizer formalism that does the job was recently put forward in Ref. [22]. Here we provide an alternative construction, inspired by Ref. [26], that allows us to make a straightforward connection to the self-testing proof.

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 \((\mathbb{C}^2)^{\otimes 5}\):

\[
S_1 = X^{(1)}Z^{(2)}Z^{(3)}X^{(4)}, \quad S_2 = X^{(2)}Z^{(3)}Z^{(4)}X^{(5)},
\]
\[
S_3 = X^{(1)}X^{(3)}Z^{(4)}Z^{(5)}, \quad S_4 = Z^{(1)}X^{(2)}X^{(4)}Z^{(5)},
\]

(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 multipartite entangled (see Appendix B 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 \(X^{(i)} \rightarrow A_0^{(i)} + A_1^{(i)}\) and \(Z^{(i)} \rightarrow A_0^{(i)}\), where \(A_0^{(i)}\) are arbitrary binary observables (of unspecified but finite dimension) that are to be measured in a Bell experiment. Let then \(S_i\) denote operators obtained from (4) by making the above substitutions.

By considering a suitably chosen linear combination of the expectation values of \(S_i\), we obtain the following Bell inequality

\[
I_5 = \langle (A_0^{(1)} + A_1^{(1)})A_1^{(2)}A_1^{(3)}A_0^{(4)} \rangle + \langle A_0^{(2)}A_1^{(3)}A_1^{(4)}A_0^{(5)} \rangle
+ \langle (A_0^{(4)} + A_1^{(4)})A_0^{(3)}A_1^{(1)}A_0^{(5)} \rangle
+ 2\langle (A_0^{(1)} - A_1^{(1)})A_0^{(2)}A_1^{(4)}A_0^{(5)} \rangle \leq 5
\]

(5)

whose local bound was directly computed by optimizing \(I_5\) over deterministic strategies for which \(A_1^{(i)} = \pm 1\).

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

\[
A_0^{(1)} = \frac{X + Z}{\sqrt{2}}, \quad A_1^{(1)} = \frac{X - Z}{\sqrt{2}},
\]

(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 leads to the following Bell operator: \(B_5 = \sqrt{2}(S_1 + S_2 + 2S_4) + S_3\). It follows that its maximal eigenvalue is \(4\sqrt{2} + 1\) and it is precisely associated to 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

\[
\beta_q \mathbb{I} - B_5 = \frac{1}{\sqrt{2}} (\mathbb{I} - S_1)^2 + \frac{1}{2} (\mathbb{I} - S_2)^2
+ \frac{1}{\sqrt{2}} (\mathbb{I} - S_3)^2 + \sqrt{2} (\mathbb{I} - S_4)^2,
\]

(7)

holds true, which implies that the eigenvalues of \(B_5\) do not exceed \(\beta_q\) for any choice of local observables \(A_1^{(i)}\) and quantum state \(\rho^j\).

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

**Fact 1.** Any behaviour achieving the maximal quantum violation of \(I_5\) self-tests the entangled subspace \(C_5\) in the sense of our definition.

**Proof.** Here we provide a sketch of the proof for illustrative purposes, deferring the details to Appendix A. Imagine that a state \(|\phi\rangle_{PE} \in \mathcal{H}_{PE}\) and observables \(A_0^{(i)}\) acting on \(\mathcal{H}_{PE}\) maximally violate our inequality (5). From the decomposition (7) one deduces that

\[
(\tilde{S}_i \otimes \mathbb{I}_E) |\phi\rangle_{PE} = |\phi\rangle_{PE}
\]

(8)

for \(i = 1, \ldots, 4\), which can be used to prove the existence of local unitary operations \(U_i\) acting on \(\mathcal{H}_{Pe}\) such that \(U_i \tilde{S}_i U_i^\dagger = S_i \otimes \mathbb{I}_pe\) for \(i = 1, \ldots, 4\), where \(U = U_4 \otimes \cdots \otimes U_5\) and the operators \(S_i\) are given in Eq. (4). This allows us to rewrite (8) as \((S_i \otimes \mathbb{I}_{pE}) |\psi\rangle_{PE} = |\psi\rangle_{PE}\) with \(|\psi\rangle_{PE} = (U \otimes \mathbb{I}_E) |\phi\rangle_{PE}\). As we show in Appendix A, the most general state satisfying all these four conditions is exactly \(|\psi\rangle_1 \otimes |\xi_1\rangle + \sqrt{1 - p^2} |\psi_2\rangle \otimes |\xi_2\rangle\), where \(0 \leq p \leq 1\), \(|\psi_1\rangle\) 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 \(\mathcal{H}_{PE}\). \(\square\)

**The toric code.—** The toric code is a paradigmatic example of the class of topological quantum error correction codes [21]. It allows one to store two logical qubits in four multi-qubit pure states of arbitrarily large number of particles. The logical qubits can be associated to 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 to the edges (see Fig. 2).

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

\[
S_v = \prod_{i \in v} X^{(i)}, \quad S_p = \prod_{i \in p} Z^{(i)}.
\]

(9)

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

The Bell inequality maximally violated by any mixed state supported in \(C_{tor}^N\) can be derived in a manner analogous to the one described in 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 \(X^{(i)}, Z^{(i)} \rightarrow A_0^{(i)}, A_1^{(i)} (i \neq j)\). By applying this substitution to \(S_v\) and \(S_p\) we obtain operators \(S_v\) and \(S_p\) from
The toric code. Each edge of the lattice represents a qubit. Stabilizing operators can be divided in two groups: those associated to each lattice vertex $v$ with $X$ acting on every qubit associated to an edge attached to the given vertex, or associated to each plaquette $p$ of the lattice with $Z$ acting on each qubit represented by an edge surrounding the plaquette.

which we obtain the following Bell inequality

$$I_N^{\text{tor}} := \sum_v \langle \tilde{S}_v \rangle + \sum_p \langle \tilde{S}_p \rangle \leq \beta_c^{\text{tor}}(N).$$

(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 we prove it in the Appendix A 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 Appendix B we prove it to be genuinely entangled. More importantly, as we prove in Appendix A, the following self-testing statement can be made for it.

**Fact 2.** Any $N$-partite behaviour $\mathcal{P}$ achieving the maximal quantum violation of $I_N^{\text{tor}}$ self-tests the entangled subspace $C_N^{\text{tor}}$.

**Geometrical considerations.** A Bell inequality is generally believed to be useful for state self-testing only if its maximal violation can be associated to a single quantum state and to a single point in the set of quantum correlations [17]. Remarkably, it turns out that subspace self-testing allows to make non-trivial self-testing statements about Bell inequalities maximally violated by more than one correlation point (hence by all the non-extremal points in between them).

We show that this is the case by using the example of the five-qubit code, while leaving the more general case of the toric code for the Appendix. First, we identify two orthogonal states $|\psi_{1,2}\rangle$ in the stabilized subspace $C_5$ as those associated to the eigenvalues $-1, +1$ for the operator $S_5 = Z^{(1)}Z^{(2)}Z^{(3)}Z^{(4)}Z^{(5)}$. This can be done because $S_5$ commutes with all the generators (4) and it is independent from them. To see that the behaviours $\mathcal{P}_1, \mathcal{P}_2$ obtained by performing the local measurements in (6) on these two states are different, we apply to $S_5$ the map between Pauli matrices and observables that we use to derive the Bell inequalities (5) and (10). By using the fact that $|\psi_{1,2}\rangle$ are eigenstates of that operators, one derives that the corresponding behaviours lead to expectation values satisfying

$$\langle \tilde{S}_5 \rangle_{\mathcal{P}_i} = \frac{1}{\sqrt{2}} \left( (A_0^{(1)} - A_1^{(1)})A_1^{(2)}A_1^{(3)}A_1^{(4)}A_1^{(5)}) \right)_{\mathcal{P}_i} = (-1)^i,$$

which can only be fulfilled if the two correlators involved take different values for $\mathcal{P}_1$ and $\mathcal{P}_2$.

Our results on subspace self-testing can thus be seen as complementary to the weaker form of self-testing presented in [29]. While in [29] the multiple correlations points associated to the self-testing statement are achieved by varying the measurement operators, we obtain a similar phenomenon by changing the quantum state instead.

**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. Exploiting then the stabilizer formalism in the multiqubit Hilbert spaces we present two examples of multipartite Bell inequalities whose maximal quantum violation serves the purpose, that is, enables self-testing of entangled subspaces according to our definition. These are the two-dimensional subspaces corresponding to the five-qubit code as well as the four-dimensional subspace corresponding to the toric code, both well-known in the context of quantum error correction. On a more fundamental level, our Bell inequalities identify face structures in the set of quantum correlations of nonzero dimension, showing at the same time that self-testing methods are not limited to extremal points in the quantum set, but can also be attributed to higher-dimensional flat objects in its boundary such as faces (see also Ref. [29]); in particular, here we show that in the simplest multipartite Bell scenario, the quantum set has a face of dimension three for any number of parties (see Appendix C).

Our work opens a plethora of possibilities for future research. For instance, it is interesting to understand whether our self-testing techniques can be generalized to other stabilizer error correcting codes (see [30] for a recent progress on this point); in particular, it is unclear whether our approach applies to subspaces which are not genuinely entangled such as for instance the one corresponding to the Shor code. On the level of quantum correlations it is interesting to understand what is the maximal dimension of the face structure that can be identified with the aid of Bell inequalities obtained within our approach. We also leave for future research a potential applicability of self-testing of the error correcting codes in quantum computing protocols. Let us finally notice that our work should be understood as a proof of principle, and therefore the question of robustness of our self-testing statements is deferred to future considerations.

**Acknowledgements.**— The majority of this work was carried out while F.B. was at ICFO. He acknowledges the support of Spanish MINECO in the form of a Severo Ochoa PhD fellowship. I.S. acknowledges support from SNSF (Starting
I Šupić, A Coladangelo, R Augusiak, and A Acín. Self-testing graph states. In D. Bacon, Thomas A. Walker, Fiona A. C. Polack, and Samuel L. Braunstein, editors, Automata, Languages and Programming, pages 72–83, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

Pavel Sekatski, Jean-Daniel Bancal, Sebastian Wagner, and Nicolas Sangouard. Certifying the building blocks of quantum computers from Bell’s theorem. Phys. Rev. Lett., 121:180505, Nov 2018. doi:10.1103/PhysRevLett.121.180505.

Maciej Demianowicz and Remigiusz Augusiak. From unextendible product bases to genuinely entangled subspaces. Phys. Rev. A, 98:012313, Jul 2018. doi:10.1103/PhysRevA.98.012313.

Remigiusz Augusiak and Paweł Horodecki. Bound entanglement maximally violating bell inequalities: Quantum entanglement is not fully equivalent to cryptographic security. Phys. Rev. A, 74:010305, Jul 2006. doi:10.1103/PhysRevA.74.010305.

Koon Tong Goh, Jędrzej Kaniewski, Elie Wolfe, Tamás Véresdi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. Geometry of the set of quantum correlations. Phys. Rev. A, 97:022104, Feb 2018. URL: https://link.aps.org/doi/10.1103/PhysRevA.97.022104, doi:10.1103/PhysRevA.97.022104.

Daniel Eric Gottesman. Stabilizer Codes and Quantum Error Correction. PhD thesis, California Institute of Technology, 1997. doi:10.7907/rrz7-drt7.

Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. Phys. Rev. A, 54:3824–3851, Nov 1996. doi:10.1103/PhysRevA.54.3824.

Raymond Laflamme, Cesar Miquel, Juan Pablo Paz, and Wojciech Hubert Zurek. Perfect quantum error correcting code. Phys. Rev. Lett., 77:198–201, Jul 1996. doi:10.1103/PhysRevLett.77.198.

A.Yu. Kitaev. Fault-tolerant quantum computation by anyons. Annals of Physics, 303(1):2–30, 2003. doi:https://doi.org/10.1016/S0003-4916(02)00018-0.

Akshata H Sheny and R Srikanth. Maximally nonlocal subspaces. Journal of Physics A: Mathematical and Theoretical, 52(9):095302, Feb 2019. doi:10.1088/1751-8121/ab0046.

A. M. Steane. Error correcting codes in quantum theory. Phys. Rev. Lett., 77:793–797, Jul 1996. doi:10.1103/PhysRevLett.77.793.

Peter W. Shor. Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A, 52:R2493–R2496, Oct 1995. doi:10.1103/PhysRevA.52.R2493.

D Schlingemann. Stabilizer codes can be realized as graph codes, 2001. arXiv:quant-ph/0111080. arXiv:quant-ph/0111080.

F. Baccari, R. Augusiak, I. Šupić, J. Tura, and A. Acín. Scalable Bell inequalities for qubit graph states and robust self-testing. Phys. Rev. Lett., 124:020402, Jan 2020. doi:10.1103/PhysRevLett.124.020402.

David P. DiVincenzo and Asher Peres. Quantum code words contradict local realism. Phys. Rev. A, 55:4089–4092, Jun 1997. doi:10.1103/PhysRevA.55.4089.

Thomas A. Walker, Fiona A. C. Polack, and Samuel L. Braunstein. Error correcting Bell inequalities. Phys. Rev. Lett., 101:080501, Aug 2008. doi:10.1103/PhysRevLett.101.080501.
APPENDIX A: PROOFS OF SELF-TESTING STATEMENTS

Here we provide full proofs of the self-testing statements for the subspaces considered in the main text. For completeness we first recall a very useful fact, proven already in Refs. [31, 32] that will be used in our proofs.

Lemma 1. [31, 32] Consider two hermitian operators $\tilde{X}$ and $\tilde{Z}$ acting on a Hilbert space $\mathcal{H}$ of dimension $D < \infty$ and satisfying the idempotency property $\tilde{X}^2 = \tilde{Z}^2 = I$ as well as the anticommutation relation $\{\tilde{X}, \tilde{Z}\} = 0$. Then, $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^d$ for some $d$ such that $D = 2d$, and there exist a local unitary operator $U$ for which

$$U\tilde{X}U^\dagger = X \otimes I_d, \quad U\tilde{Z}U^\dagger = Z \otimes I_d,$$  

(12)

where $X$ and $Z$ are the $2 \times 2$ Pauli matrices introduced before and $I_d$ is a $d \times d$ identity acting on the auxiliary Hilbert space.

This above lemma provides a way to characterize the measurement observables from their commutation properties. If the state to be self-tested can be tomographically retrieved by using two Pauli measurements, proving Lemma 1 basically reduces self-testing to the quantum state tomography.

Proof. First of all, the fact that $\tilde{X}$ and $\tilde{Z}$ square to identity and are hermitian implies that their eigenvalues are $\pm 1$. This means that they are also unitary and allows one to rewrite the anticommutation relation $\{\tilde{X}, \tilde{Z}\} = 0$ as

$$\tilde{X}\tilde{Z}\tilde{X} = -\tilde{Z},$$  

(13)

or as

$$\tilde{Z}\tilde{X}\tilde{Z} = -\tilde{X}.$$  

(14)

As both $\tilde{X}$ and $\tilde{Z}$ are unitary and hermitian, these identities imply that the eigenspaces of both these operators corresponding to the eigenvalues $\pm 1$ have equal dimensions. This has two consequences. The first one is that the Hilbert space they both act on is $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^d$ with finite $d$ such that $D = 2d$. The second one is that there exists a unitary $U : \mathcal{H} \rightarrow \mathcal{H}$ which brings the eigenvectors $|e_i^+\rangle$ of $\tilde{Z}$ to the product form

$$U|e_i^+\rangle = |0\rangle|g_i\rangle,$$  

(15)

$$U|e_i^-\rangle = |1\rangle|g_i\rangle,$$  

(16)

with $|g_i\rangle$ being some orthogonal basis in $\mathbb{C}^d$, which means that

$$U\tilde{Z}U^\dagger = Z \otimes I_d.$$  

(17)

To obtain (12) for the $\tilde{X}$ operator it is enough to notice that Eq. (13) implies that $\tilde{X}$ exchanges the eigenvectors of $\tilde{Z}$ corresponding to different eigenvalues, that is,

$$|e_i^-\rangle = \tilde{X}|e_i^+\rangle.$$  

Thus, in the product basis (15), $\tilde{X}$ is of the form

$$U\tilde{X}U^\dagger = X \otimes I_d,$$  

(18)

which completes the proof.

Self-testing the five-qubit code subspace

In this section we provide a detailed proof of self-testing of the $C_5$ subspace stabilized by the operators (4). To this aim let us assume that a state $|\phi\rangle \in \mathcal{H}_{PE}$ and observables $A_i^{(i)}$ acting on $\mathcal{H}_P$ violate maximally our inequality (5). Then, making the following substitutions

$$\tilde{X}^{(1)} = \frac{1}{\sqrt{2}} \left[ A_0^{(1)} + A_1^{(1)} \right], \quad \tilde{Z}^{(1)} = \frac{1}{\sqrt{2}} \left[ A_0^{(1)} - A_1^{(1)} \right],$$  

(19)

and $\tilde{X}^{(i)} = A_0^{(i)}$ and $\tilde{Z}^{(i)} = A_1^{(i)}$ for $i = 2, \ldots, 5$, the operators $\tilde{S}_i$ introduced already in the main body of our work can be stated as

$$\tilde{S}_1 = \tilde{X}^{(1)}\tilde{Z}^{(2)}\tilde{Z}^{(3)}\tilde{X}^{(4)}, \quad \tilde{S}_2 = \tilde{X}^{(2)}\tilde{Z}^{(3)}\tilde{Z}^{(4)}\tilde{X}^{(5)},$$  

$$\tilde{S}_3 = \tilde{X}^{(1)}\tilde{X}^{(2)}\tilde{Z}^{(3)}\tilde{Z}^{(4)}\tilde{Z}^{(5)}, \quad \tilde{S}_4 = \tilde{Z}^{(1)}\tilde{X}^{(2)}\tilde{Z}^{(4)}\tilde{Z}^{(5)}.$$  

(20)

From the sum-of-squares decomposition (7) we deduce that they satisfy the following conditions

$$\tilde{S}_i |\phi\rangle = |\phi\rangle,$$  

(21)

where to simplify the notation, here and below we omit the identity acting on $\mathcal{H}_E$.

Let us now prove, using relations (21), that for any $i$, the operators $\tilde{X}^{(i)}$ and $\tilde{Z}^{(i)}$ satisfy the conditions of Lemma 1 on the support of $\rho_1$ with the latter being the reduced density matrix of $|\phi\rangle$ corresponding to the Hilbert space $\mathcal{H}_P$. First, it is direct to see that, by the very construction, $\tilde{X}^{(1)}$ and $\tilde{Z}^{(1)}$ satisfy the anticommutation relation

$$\{\tilde{X}^{(1)}, \tilde{Z}^{(1)}\} = 0.$$  

(22)

To prove that they also square to identity on the support of $\rho_1$ we use the condition (21) for $i = 1$ and $i = 4$, obtaining

$$\tilde{S}_1^2 |\phi\rangle = \tilde{S}_4^2 |\phi\rangle = |\phi\rangle,$$  

(23)

which due to the fact that $[\tilde{X}^{(i)}]^2 = [\tilde{Z}^{(i)}]^2 = I$ for $i = 2, \ldots, 4$ immediately imply that $[\tilde{X}^{(1)}]^2$ and $[\tilde{Z}^{(1)}]^2$ are $I$ on the support of $\rho_1$. 

[29] Jędrzej Kaniewski. A weak form of self-testing, 2019. arXiv:1910.00706v1. arXiv:1910.00706.
[30] Ovidiusz Makuta and Remigiusz Augusiak. Self-testing stabilizer subspaces of maximal dimension, 2020. to be published.
[31] Sandu Popescu and Daniel Rohrlich. Which states violate Bell’s inequality maximally? Physics Letters A, 169(6):411–414, 1992.
[32] Jędrzej Kaniewski. Analytic and nearly optimal self-testing bounds for the Clauser-Horne-Shimony-Holt and Mermin inequalities. Phys. Rev. Lett., 117:070402, Aug 2016. doi: 10.1103/PhysRevLett.117.070402.
Let us now prove the anticommutation relations for the remaining operators $\hat{X}^{(i)}$ and $\hat{Z}^{(i)} \ (i = 2, \ldots, 5);$ notice that, by definition, they already satisfy $[\hat{X}^{(i)}]^2 = [\hat{Z}^{(i)}]^2 = 1.$ To this end, we rewrite the conditions (21) for $i = 1, 4$ as
\[
\hat{X}^{(2)} \phi = \hat{Z}^{(1)} \hat{X}^{(4)} \hat{Z}^{(5)} \phi, \quad \hat{Z}^{(2)} \phi = \hat{X}^{(1)} \hat{Z}^{(3)} \hat{X}^{(4)} \phi, \tag{24}
\]
which leads us to
\[
\{ \hat{X}^{(2)}, \hat{Z}^{(2)} \} |\phi\rangle = \{ \hat{X}^{(1)}, \hat{Z}^{(1)} \} \hat{Z}^{(3)} \hat{Z}^{(5)} |\phi\rangle = 0, \tag{25}
\]
where the last equality is a consequence of Eq. (22). In a similar way one can exploit the operator relations stemming from Eq. (21) to obtain anticommutation relations for the remaining three sites. Indeed, we can combine the conditions (21) for $\hat{S}_3$ and $\hat{S}_4$ to get
\[
\{ \hat{X}^{(4)}, \hat{Z}^{(4)} \} |\phi\rangle = \{ \hat{X}^{(1)}, \hat{Z}^{(1)} \} \hat{X}^{(2)} \hat{X}^{(3)} |\phi\rangle = 0, \tag{26}
\]
and combine $\hat{S}_2$ and $\hat{S}_4$ to obtain
\[
\{ \hat{X}^{(5)}, \hat{Z}^{(5)} \} |\phi\rangle = \{ \hat{X}^{(1)}, \hat{Z}^{(1)} \} \hat{Z}^{(2)} \hat{Z}^{(3)} |\phi\rangle = 0. \tag{27}
\]
Finally, we combine the conditions arising from $\hat{S}_2$ and $\hat{S}_3$ to show
\[
\{ \hat{X}^{(3)}, \hat{Z}^{(3)} \} |\phi\rangle = \{ \hat{X}^{(5)}, \hat{Z}^{(5)} \} \hat{Z}^{(1)} \hat{Z}^{(2)} |\phi\rangle = 0. \tag{28}
\]
Given the above anticommutation relations for operators acting on all sites, we can now make use of Lemma 1 which allows us to exploit the local unitary operations $U_i : \mathcal{H}_{P'} \rightarrow \mathcal{H}_{P'}$ that map the operators $\hat{Z}^{(i)}, \hat{X}^{(i)}$ to the qubit Pauli matrices in the sense that
\[
U_i \hat{Z}^{(i)} U_i^\dagger = Z^{(i)} \otimes 1_{P''}, \quad U_i \hat{X}^{(i)} U_i^\dagger = X^{(i)} \otimes 1_{P''}, \tag{29}
\]
with $i = 1, \ldots, 5.$ If we define $|\psi\rangle = (U \otimes 1_E) |\phi\rangle,$ where $U = U_1 \otimes \ldots \otimes U_5,$ it follows from the conditions (21) and the transformations (29), that
\[
S_i \otimes 1_{P''} |\psi\rangle = |\psi\rangle \quad (i = 1, \ldots, 4), \tag{30}
\]
where $S_i$ are the qubit stabilizing operators defined in (4).

Let us finally prove that the most general form of a state $|\psi\rangle \in (\mathbb{C}^2)^\otimes 5 \otimes \mathcal{H}_{P''} \otimes \mathcal{H}_{P''}$ compatible with the conditions (30) is
\[
|\psi\rangle = p |\psi_1\rangle \otimes |\xi_1\rangle + \sqrt{1 - p^2} |\psi_2\rangle \otimes |\xi_2\rangle, \tag{31}
\]
where $|\psi_1\rangle$ are two orthonormal states spanning $C_5$, $|\xi_1\rangle \in \mathcal{H}_{P''}$ are some auxiliary states and $p \in [0, 1].$

To this aim, we consider the Schmidt decomposition of $|\psi\rangle$ with respect to the tensor product of the five-qubit Hilbert space $(\mathbb{C}^2)^\otimes 5$ and $\mathcal{H}_{P''} \otimes \mathcal{H}_{P''},$
\[
|\psi\rangle = \sum_j \lambda_j |\eta_j\rangle |\varphi_j\rangle, \tag{32}
\]
where $|\eta_j\rangle \in (\mathbb{C}^2)^\otimes 5$ as well as $|\varphi_j\rangle \in \mathcal{H}_{P''} \otimes \mathcal{H}_{P''}$ are some orthogonal vectors in the corresponding Hilbert spaces. By plugging Eq. (32) into Eq. (30) we arrive at
\[
\sum_j \lambda_j (S_i |\eta_j\rangle) |\varphi_j\rangle = \sum_j \lambda_j |\eta_j\rangle |\varphi_j\rangle, \tag{33}
\]
which after projecting onto $|\varphi_j\rangle$ gives $S_i |\eta_j\rangle = |\eta_j\rangle$ for every $i = 1, 2, 3, 4.$ This means that each vector $|\eta_j\rangle$ belongs to the subspace $C_5$ and therefore it might be written as $|\eta_j\rangle = \alpha_j |\psi_1\rangle + \beta_j |\psi_2\rangle$ for some $\alpha_j$ and $\beta_j$ such that $|\alpha_j|^2 + |\beta_j|^2 = 1.$ Substituting this last form into Eq. (32), directly leads to
\[
|\psi\rangle = |\psi_1\rangle |\xi_1\rangle + |\psi_2\rangle |\xi_2\rangle \tag{34}
\]
with some in general unnormalized vectors $|\xi_i\rangle \in \mathcal{H}_{P''} \otimes \mathcal{H}_{P''}.$ Clearly, this can be rewritten as
\[
|\psi\rangle = p |\psi_1\rangle |\xi_1\rangle + \sqrt{1 - p^2} |\psi_2\rangle |\xi_2\rangle, \tag{35}
\]
where $p \in [0, 1]$ and $|\xi_i\rangle$ are now normalized. This completes the proof.

Self-testing the genuinely entangled subspace corresponding to the toric code

Let us begin by writing explicitly the Bell inequality maximally violated by any state belonging to $C_N^{tor}$ Recall to this end that every qubit $i$ is contained in two plaquettes and is connected to two vertices, which we identify as $p_{1}^{(i)}, p_{2}^{(i)}$ and $v_1^{(i)}, v_2^{(i)}$ respectively. Now, our Bell inequality reads
\[
I_N^{tor} := \langle B_N^{tor} \rangle = \sum_v \langle \hat{S}_v \rangle + \sum_p \langle \hat{S}_p \rangle \leq \beta_{N}^{tor} (N), \tag{36}
\]
where the classical bound reads
\[
\beta_{N}^{tor} (N) = N - 2\sqrt{2}(\sqrt{2} - 1), \tag{37}
\]
whereas the Bell operator is given by
\[
B_N^{tor} = \frac{1}{\sqrt{2}} \sum_{k=1,2} (A_0^{(j)} + A_1^{(j)}) \prod_{i \in v_1^{(i)}} A_0^{(j)} \prod_{i \in v_2^{(i)}} A_1^{(j)} \prod_{i \in \tilde{v}_1^{(i)} \setminus v_1^{(i)}} A_0^{(j)} \prod_{i \in \tilde{v}_2^{(i)} \setminus v_2^{(i)}} A_1^{(j)} + \sum_{v \neq v_1^{(i)} \cup v_2^{(i)}} \prod_{i \in v} A_0^{(j)} + \sum_{p \neq p_{1}^{(i)} \cup p_{2}^{(i)}} \prod_{i \in p} A_1^{(j)}, \tag{38}
\]
where qubit $j$ is the chosen qubit for which our Bell expression contains combinations of observables.

The maximal quantum violation of this inequality amounts to
\[
\beta_{N}^{tor} (N) = 4 + |p| + |v| - 4 = |p| + |v| = N \tag{39}
\]
In short, we refer to a qubit associated to a vertical (horizontal) edge as a vertical (horizontal) qubit. To label qubits, we choose a reference vertical qubit $j$ and start counting forward by moving to the next vertical qubit on the right. By proceeding in this way, we label qubits from $j + 1$ to $j + L - 1$. After that, we move to the horizontal qubit on the top-right side of qubit $j$ and label it $j + L$, proceeding then forward with the next horizontal qubit to the right, until arriving at the qubit to the left of $j + L$. It then follows that the vertical qubit on top of $j$ would be labelled as $j + 2L$. Similarly, we can label plaquettes and vertex stabilizing operators depending on where are located with respect to a given qubit, as shown in the Figure for the case of qubit $j$. An analogous procedure can be done to label operators with respect to a horizontal qubit.

For instance, we could refer to $S^{(j)}_{v_{j}}$ as $S^{(j+L)}_{v_{j}}$, or to $S^{(j)}_{v_{j}}$ as $S^{(j+L)}_{v_{j}}$.

and can be achieved by the following measurements

$$A^{(j)}_{0} = \frac{X + Z}{\sqrt{2}}, \quad A^{(j)}_{1} = \frac{X - Z}{\sqrt{2}},$$

for the party $j$, and

$$A^{(i)}_{0} = X, \quad A^{(i)}_{1} = Z \quad (41)$$

for the remaining parties $i \neq j$, and any state belonging to $C^{tor}_{N}$. It follows that (38) is violated for any $N$.

To prove that (39) is indeed the maximal quantum value of $B^{tor}_{N}$ one checks that the following sum-of-squares decomposition holds true

$$\beta^{tor}_{N} (N) \mathbb{I} - B^{tor}_{N} = \frac{1}{\sqrt{2}} \sum_{k=1,2} \left( \mathbb{I} - \frac{A^{(j)}_{0} + A^{(j)}_{1}}{\sqrt{2}} \prod_{i \in v^{(j)}_{x}, i \neq j} A^{(i)}_{0} \right)^{2} + \frac{1}{\sqrt{2}} \sum_{k=1,2} \left( \mathbb{I} - \frac{A^{(j)}_{0} - A^{(j)}_{1}}{\sqrt{2}} \prod_{i \in p^{(j)}_{y}, i \neq j} A^{(i)}_{1} \right)^{2}$$

$$+ \sum_{v \neq v^{(j)}_{x}, v^{(j)}_{y}} \left( \mathbb{I} - \prod_{i \in v} A^{(i)}_{0} \right)^{2} + \sum_{v \neq v^{(j)}_{x}, v^{(j)}_{y}} \left( \mathbb{I} - \prod_{i \in p} A^{(i)}_{1} \right)^{2} \quad (42)$$

Let us now move on to proving Fact 2. To this end, let us assume that an $N$-partite state $|\phi \rangle$ and observables $A^{(i)}_{x_{i}}$ $(x_{i} = 0, 1)$ maximally violate our Bell inequality, that is

$$\langle \phi | B^{tor}_{N} | \phi \rangle = \beta^{tor}_{N} (N) \quad (43)$$

with $B^{tor}_{N}$ given in Eq. (38).
Let us now introduce the operators
\[
\tilde{X}^{(j)} = \frac{A_0^{(j)} + A_1^{(j)}}{\sqrt{2}}, \quad \tilde{Z}^{(j)} = \frac{A_0^{(j)} - A_1^{(j)}}{\sqrt{2}},
\]
for the chosen party \( j \), and \( \tilde{X}^{(i)}, \tilde{Z}^{(i)} = A_0^{(i)}, A_1^{(i)} \) for all \( i \neq j \). We now make use of the condition resulting from the sum-of-squares decomposition (42) to prove that for any \( i \), the operators \( \tilde{X}^{(i)}, \tilde{Z}^{(i)} \) anticommute and square to identity on the support of \( \rho \), with the latter being the reduced density matrix of \( |\phi\rangle \). Indeed, from Eqs. (42) and (43) one infers that
\[
\hat{S}_v |\phi\rangle = \hat{S}_p |\phi\rangle = |\phi\rangle \quad \forall p, v.
\]
To do so, it is convenient to associate to each qubit in the lattice the subset of operators (63) that act non-trivially on it. That is, those that contain \( X \) or \( Z \) on this site. It is easy to see that for a two-dimensional lattice of any size there are precisely two vertex and two plaquette operators acting non-trivially on each qubit. For later convenience, let us then introduce a notation for these four non-trivial generators: if the qubit \( j \) corresponds to a horizontal edge, we identify the corresponding generators as
\[
\left\{ S_v^{(j)}, S_v^{(j)} \right\} \quad \forall v.
\]
where the arrows in the notation refer to where the vertex (plaquette) is located with respect to the qubit. Similarly, if the qubit \( j \) corresponds to a vertical edge, we denote the corresponding four stabilizing operators as
\[
\left\{ S_p^{(j)}, S_p^{(j)} \right\} \quad \forall p.
\]
Notice that, given two neighbouring qubits (i.e., qubits associated to edges connected to the same vertex), some of the elements in the two subsets in (46) and (47) are common (see Fig. 3 for an example). Let us now focus on the qubit \( j \) and consider a vertex and a plaquette operator that act non-trivially on it. With loss of generality, we can take them to be \( S_v^{(j)} \) and \( S_p^{(j)} \). From the stabilizing conditions (45) for \( S_v^{(j)} \) and \( S_p^{(j)} \) as well as the fact that, by the very construction, the operators \( \tilde{X}^{(j)} \) and \( \tilde{Z}^{(j)} \) with \( j \neq i \) square to identity, we obtain
\[
\left( \tilde{X}^{(j)} \right)^2 |\phi\rangle = \left( \tilde{Z}^{(j)} \right)^2 |\phi\rangle = |\phi\rangle.
\]
This directly implies that, as anticipated, both \( \tilde{X}^{(j)} \) and \( \tilde{Z}^{(j)} \) square to identity on the support of \( \rho_j \). Then, by virtue of Eq. (44), one directly sees that
\[
\{ \tilde{X}^{(j)}, \tilde{Z}^{(j)} \} = 0.
\]
Let us now move to the remaining pairs of operators \( \tilde{X}^{(i)} \) and \( \tilde{Z}^{(i)} \) with \( i \neq j \) and prove that they anticommute too; recall that by definition they square to identity. We will proceed in a recursive way. First, let us assume that \( j \) is associated to a vertical edge and consider one of the neighbours of \( j \), denoted \( j + L \) (cfr. Fig. 3). To prove the anticommutation relation for the operators acting on this qubit we assume, without any loss of generality that the plaquette and vertex operators shared between party \( j \) and \( j + L \) are exactly \( \tilde{S}_v^{(j)} \) and \( \tilde{S}_p^{(j)} \). By making use of the corresponding stabilizing conditions (45) and the fact that all the local operators square to identity on the support of the state, we obtain the following equations
\[
\tilde{X}^{(j)} \tilde{X}^{(j+L)} |\phi\rangle = \tilde{X}^{(j)} \tilde{X}^{(j+2L)} |\phi\rangle,
\tilde{Z}^{(j)} \tilde{Z}^{(j+L)} |\phi\rangle = \tilde{Z}^{(j)} \tilde{Z}^{(j+1)} \tilde{Z}^{(j-L)} |\phi\rangle.
\]
which lead us to
\[
\{ \tilde{X}^{(j)}, \tilde{Z}^{(j)} \} = 0
\]
for any \( i \).

Having the anticommutation relations for all the parties, we make use of Lemma 1 which implies the existence of a unitary operations \( \hat{U}_j \) acting on \( \mathcal{H}_{\rho_j} \) such that
\[
\hat{U}_j \hat{X}_j \hat{U}_j^\dagger = X^{(j)} \otimes 1_{p''}, \quad \hat{U}_j \hat{Z}_j \hat{U}_j^\dagger = Z^{(j)} \otimes 1_{p''}
\]
for any \( j \). Now, denoting \( |\psi\rangle = U \otimes 1_E |\phi\rangle \), we see that \( |\psi\rangle \) satisfies the following stabilizing conditions
\[
S_v \otimes 1_{p''} |\psi\rangle = |\psi\rangle \quad \forall v, \quad S_p \otimes 1_{p''} |\psi\rangle = |\psi\rangle \quad \forall p,
\]
where \( S_v \) and \( S_p \) are the stabilizing operators given in Eq. (9). Using the same method as in the case of the five-qubit code one can show that
\[
|\psi\rangle = \sum_{i=1}^4 p_i |\psi_i\rangle \otimes |\xi_i\rangle,
\]
where \( p_i \) are nonnegative numbers such that \( p_1^2 + p_2^2 + p_3^2 + p_4^2 = 1 \), \( |\psi_i\rangle \) are \( N \)-qubit vectors spanning \( C^\text{tor} \) and \( |\xi_i\rangle \in \mathcal{H}_{p''} \) are some auxiliary states. This completes the proof.

**APPENDIX B: PROVING THAT SUBSPACES \( C_5 \) AND \( C^\text{tor}_N \) ARE GENUINELY ENTANGLED**

Here we prove that the subspaces corresponding to the five-qubit code \( C_5 \) and the toric code \( C^\text{tor}_N \) are genuinely entangled, that is, contain only multipartite genuinely entangled states.
We begin by providing a simple sufficient criterion for a subspace generated by a stabilizer \( S \) to be genuinely entangled. To this end, assume that \( S \) is generated by a set of \( k \) stabilizing operators \( \{ S_i \}_{i=1}^k \). Consider then a bipartition of \( N \) parties into two disjoint and nonempty groups \( G \) and \( G' \) such that \( |G| + |G'| = N \), and denote by \( G \) the set of all such bipartitions. Given a bipartition \( G|G' \), every stabilizing operator \( S_i \) can be written as

\[
S_i = S_i^G \otimes S_i^{G'}
\]

with \( i = 1, \ldots, k \), where each \( S_i^G \) and \( S_i^{G'} \) acts on the Hilbert space associated to the group \( G \) (\( G' \)). Notice that due to the fact that for any pair \( i \neq j \), the operators \( S_i \) and \( S_j \) commute, either

\[
[S_i^G, S_j^G] = 0 \quad \text{and} \quad [S_i^{G'}, S_j^{G'}] = 0,
\]

or

\[
[S_i^G, S_j^{G'}] = 0 \quad \text{and} \quad [S_i^{G'}, S_j^G] = 0.
\]

Let us now formulate our criterion.

**Fact 3.** Consider a stabilizer \( S \) generated by a set of stabilizing operators \( S_i \) (\( i = 1, \ldots, k \)). If for any bipartition of \( N \) parties into two disjoint and nonempty subsets \( G \) and \( G' \) there exist \( i \neq j \) such that \( \{ S_i^G, S_j^{G'} \} = 0 \), then the subspace \( S_N \) stabilized by \( S_i \) is genuinely multipartite entangled.

**Proof.** Let us begin by assuming that the subspace \( S_N \) is not genuinely entangled, which means that it contains a pure state \( |\psi\rangle \) such that

\[
|\psi\rangle = |\psi_G\rangle \otimes |\psi_{G'}\rangle
\]

for some bipartition \( G|G' \). From the fact that \( S_i |\psi\rangle = |\psi\rangle \) we infer that with respect to this bipartition

\[
S_i^G |\psi_G\rangle = e^{i \varphi_i} |\psi_G\rangle
\]

for some \( \varphi_i \in \mathbb{R} \) (analogous identities hold true for the \( G' \) group). This contradicts the fact that there exist \( i \neq j \) such that

\[
\{ S_i^G, S_j^{G'} \} |\psi_G\rangle = 0,
\]

which completes the proof. \( \square \)

Notice that, as \( S_i \) mutually commute, the anticommutation relation in Fact 3 might also be formulated for \( G' \).

**Subspace \( C_N \)**

Let us now illustrate the power of our criterion by applying it to the subspace \( C_N \) corresponding to the five-qubit code. Recall that the corresponding stabilizing operators are given by

\[
S_1 = X^{(1)}Z^{(2)}Z^{(3)}X^{(4)}, \quad S_2 = X^{(2)}Z^{(3)}Z^{(4)}X^{(5)},
S_3 = X^{(1)}X^{(3)}Z^{(4)}Z^{(5)}, \quad S_4 = Z^{(1)}X^{(2)}X^{(4)}Z^{(5)}.
\]

In the five-partite case the relevant bipartitions can be divided into two possibilities: one party versus the rest (five such bipartitions) and two parties versus three (ten such cases).

In the first case one notices that for any bipartition \( G|G' \) with a single-element set \( G = \{ i \} \) there always exists a pair of the stabilizing operators such that \( S_i^G = X^{(k)} \) and \( S_j^{G'} = Z^{(k)} \) and the condition (58) is satisfied.

Let us then consider the second case. By direct check one realizes that for any bipartition \( G|G' \) with \( G = \{ i, j \} \) such that \( i < j \) there exists a stabilizing operator \( S_m \) for which \( S_m^G = X^{(i)}Z^{(j)} \) (\( i < j \)) and another stabilizing operator \( S_n \) (\( m \neq n \)) such that \( S_n^G = X^{(j)} \) or \( S_n^G = Z^{(i)} \) or \( S_n^G = X^{(i)}X^{(j)} \), or finally \( S_n^G = Z^{(i)}z^{(j)} \).

**Subspace \( C_N \)**

Here we show, employing Fact 3, that the four-dimensional subspaces identified by the toric code consist of only genuinely entangled states. To this aim, it is enough to find, for any bipartition \( G|G' \), two stabilizing operators that anticommute when restricted to \( G \) or \( G' \). Recall that the stabilizer associated to the toric code is generated by the following operators

\[
S_v = \prod_{i \in v} X^{(i)}, \quad S_p = \prod_{i \in p} Z^{(i)}.
\]

where one defines a different \( S_v \) for any vertex and \( S_p \) for any plaquette in the lattice. In the following we will provide a constructive proof that such a set of stabilizing operators satisfies the assumptions of Fact 3 for a lattice of any size. Before doing that, however, let us analyse some basic properties of this stabilizer. Notice that plaquette and vertex operators are composed of products of different Pauli matrices (\( Z \) and \( X \) respectively) that, if taken independently, anticommute with each other. However, the products in (63) are chosen carefully in order to define stabilizing operators that mutually commute. This happens because for any pair of plaquette and vertex operators, the subsets of qubits on which they act non-trivially are either disjoint or they overlap on exactly two particles. In particular, the latter is exactly the case of a plaquette and a vertex generator acting non-trivially on the same pair of neighbouring qubits. For example, as shown in Figure 3, if \( j \) is a vertical edge qubit, \( S^{(j)}_{v,1} \) and \( S^{(j)}_{p,2} \) would be two mutually commuting operators composed of a pair of anticommuting Pauli matrices acting on \( j \) and its neighbour \( j + L \). Notice that here we are adopting the notation introduced in Appendix B to denote stabilizing operators acting non-trivially on a given qubit.

We are now ready to go back to proving that the toric code meets the assumptions of Fact 3, i.e., given any bipartition \( G|G' \), one can find two stabilizing operators that anticommute when restricted to the subset \( G \). Thanks to the analysis of the commuting properties of the generators (63) conducted above, it is now clear how to find two such operators. Namely, it suffices to find a pair of neighbouring qubits \( i \) and \( j \), belonging
to a different subset of the bipartition, i.e., \( i \in G \) and \( j \in G' \) or vice versa. Then, the two anticommuting operators will be the plaquette and vertex operator acting non-trivially on both the qubits restricted to, for example, the subset containing \( i \). Indeed, since \( j \) does not belong to the same subset, it follows that the non-trivial support of the two restricted generators now overlaps only on qubit \( i \), where the two operators act with the Pauli matrix \( X \) and \( Z \) respectively.

Therefore, proving that the subspace stabilized by the toric code is GME for any number of particles reduces to showing that such a pair of anticommuting operators can be found for any nontrivial bipartition \( G|G' \) with \( G, G' \neq \emptyset \).

To see that this is indeed the case it is enough to realize that for any bipartition \( G|G' \) there exist a vertex operator \( S_v \) which is divided between \( G \) and \( G' \) in the sense that at least one of the qubits \( S_v \) acts on belongs to \( G \) and at least one to \( G' \). To prove this last statement, assume that such a vertex does not exist. Then, pick a vertex whose all qubits belong to, say \( G \); recall that by assumption \( G \) is empty. Then all vertices connected to the chosen vertex by a qubit must also belong to \( G \); recall that we assumed that there is no vertex divided between the two sets \( G \) and \( G' \). Taking into account that all vertices in lattice are connected, following the above reasoning it is not difficult to realize that in fact all vertices must belong to \( G \), meaning that \( G' \) is empty. This, however, contradicts the assumption that the bipartition \( G|G' \) is nontrivial.

Consider then a vertex \( v \) which is divided between \( G \) and \( G' \). We consider two possibilities: either one qubit associated to \( v \) belongs to \( G \) or two. The third case of three qubits belonging to \( G \) is equivalent to the first one because we can always consider \( G' \) instead of \( G \). In the first case, we consider one of the two plaquette operators \( S_p \) which act nontrivially on the qubit belonging to \( G \). Then, it clearly follows that \( S_v \) and \( S_p \) anticommute when restricted to \( G \). The second case is slightly more involved: one has to identity a plaquette operator \( S_p \) which acts nontrivially on only one of the \( G \) qubits connected to the vertex \( v \). In such a case, one can indeed show that \( S_p^v \) and \( S_p^G \) satisfy the anticommutation relation. Let us show that one can always find such a plaquette operator, by considering the two possible subcases of the two \( G \) qubits connected to the vertex \( v \) being: (i) both horizontal or vertical qubits, or (ii) a horizontal and a vertical qubit each. For (i), we can label the two qubits without loss of generality as \( j \) and \( j + 2L \). Then, by adopting the notation introduced above, a valid choice for the required plaquette operator is either \( S_{p,v}^{(j)} \) or \( S_{p,v}^{(j)} \) (see Fig. 3). Similarly, in the subcase (ii), we can take the two qubits to be \( j \) and \( j + L \), so that the desired plaquette operator becomes \( S_{p,v}^{(j)} \). This ends the proof.

**APPENDIX C: GEOMETRICAL STRUCTURE OF THE SET OF POINTS MAXIMALLY VIOLATING \( I_N^{tor} \)**

Here we show that the correlations maximally violating the Bell inequality (5) span a four-dimensional affine space in the boundary of the set of quantum correlations, for the the case of any lattice size \( L \).

To this aim, we follow a similar reasoning as for the five-qubit code case presented in the main text and we introduce the following operators

\[
Z_{\text{hot}} = \prod_{i=0}^{L-1} Z^{(j+i)} \tag{64}
\]

and

\[
Z_{\text{vert}} = \prod_{i=1}^{L-1} Z^{(j+2i)} . \tag{65}
\]

They consist of a product of \( Z \) operators acting respectively on an horizontal and vertical loop around the torus, containing a reference qubit \( j \). It is direct to see that they mutually commute and that they commute with any plaquette \( S_p \) and vertex \( S_v \) operator. Moreover, they are independent of the stabilizer \( S_{tor}^{\text{vert}} \). Hence, we can use them to define an orthonormal basis for the two-qubit subspace of the toric code. More precisely, such a basis can be chosen to be the collection of four states \( \{ |\psi_{ab}\rangle \}_{a,b=\pm 1} \) on \( C_{tor}^2 \), defined as the eigenstates of \( Z_{\text{hot}} \) (\( Z_{\text{vert}} \)) with eigenvalue \( a \) (\( b \)).

By performing the measurements leading to the maximal violation of (10) on each of those states, one obtains the corresponding correlation points \( P_{\text{ab}} \). To show that, for \( a, b = \pm 1 \), these four points are represented by linearly independent vectors, it is enough to make use of the fact that the related states \( |\psi_{ab}\rangle \) are eigenvectors of the two additional operators \( Z_{\text{hot}} \) and \( Z_{\text{vert}} \). In particular, let us assume that the reference qubit \( j \) is the one where the substitution \( X^{(j)}, Z^{(j)} \rightarrow (A_0^{(j)} \pm A_1^{(j)})/\sqrt{2} \) has been made. Then if follows that the corresponding correlation points must satisfy

\[
\langle \hat{Z}_{\text{hot}} \rangle_{P_{ab}} = \frac{1}{\sqrt{2}} \langle (A_0^{(j)} - A_1^{(j)}) \prod_{i=1}^{L-1} A_1^{(j+i)} \rangle_{P_{ab}} = a \tag{66}
\]

and

\[
\langle \hat{Z}_{\text{vert}} \rangle_{P_{ab}} = \frac{1}{\sqrt{2}} \langle (A_0^{(j)} - A_1^{(j)}) \prod_{i=1}^{L-1} A_1^{(j+2i)} \rangle_{P_{ab}} = b \tag{67}
\]

showing that the four correlation points must differ at least on these expectation values. Let us notice that one can follow the same reasoning for any other pair of vertical and horizontal loop operators, leading to similar conditions for other \( L \)-body expectation values arising from the \( P_{ab} \)’s.