Constructing multipartite Bell inequalities from stabilizers

Qi Zhao [1,2,*] and You Zhou [3,4,†]

[1] *QICI Quantum Information and Computation Initiative, Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*
[2] *Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, Maryland 20742, USA*
[3] *Key Laboratory for Information Science of Electromagnetic Waves (Ministry of Education), Fudan University, Shanghai 200433, China*
[4] *Department of Physics, Harvard University, Cambridge, Massachusetts 02138, USA*

(Received 20 March 2022; accepted 2 December 2022; published 26 December 2022)

Bell inequality with a self-testing property has played an important role in quantum information processing with both fundamental and practical significance. However, it is generally challenging to find Bell inequalities used for self-testing multipartite states, and actually, there are not many known candidates. In this work we propose a systematic framework to construct Bell inequalities from stabilizers which are maximally violated by general stabilizer states, with two observables for each local party. We show that the constructed Bell inequalities can self-test any stabilizer state if and only if these stabilizers can uniquely determine the state in a device-dependent manner. This bridges the gap between device-independent and device-dependent verification methods. Our framework can provide plenty of Bell inequalities for self-testing N-party stabilizer states. Among them, we give two families of Bell inequalities with different advantages: (1) a family of Bell inequalities with a constant ratio of quantum and classical bounds using $2N$ correlations, and (2) *single pair* inequalities improving on all previous robustness self-testing bounds using $N+1$ correlations, which are both efficient and robust for realizations in multipartite systems.

DOI: 10.1103/PhysRevResearch.4.043215

I. INTRODUCTION

Bell inequalities, as a test for quantum correlations, can distinguish quantum physics from its classical counterpart [1,2]. They not only play a fundamental role in quantum physics, but also can be utilized in many practical quantum information processing tasks, such as the quantum key distribution [3–6], quantum randomness generation [7–12], blind quantum computing [13,14], and quantum resource detection [15–17].

One of the most striking applications of Bell nonlocality is the simultaneous verification of quantum states and measurements, based on the maximal violation of Bell inequalities [3,18]. The verification only relies on the input and output statistics without the trust of the realization of devices, which is different from traditional quantum tomography and other device-dependent methods [19,20]. This phenomenon is usually referred to as self-testing. When the violation of Bell inequality is only close to its maximal quantum value, one can also estimate the fidelity between the underlying state and the target state, which is referred to as robust self-testing. Tremendous efforts have been made to self-test various types of quantum states [21–26] and improve robust self-testing performance, which is helpful in the realistic implementation [18,27,28].

Even though Bell inequality and self-testing are of fundamental and practical significance, it is generally challenging and not clear to propose Bell inequalities used for self-testing, especially for multipartite states, due to the exponential increase of the dimension of total Hilbert space. Some interesting and inspiring attempts have been made focusing on high-dimensional maximally entangled states [24] and graph states [25,26,29–31]. However, all the previous works either proposed Bell inequalities without exploring their applicability in self-testing or only show that a certain family of proposed Bell inequalities is valid for self-testing. The candidates for the Bell inequality of general stabilizer states which can be used for self-testing are still limited.

Meanwhile, device-dependent multipartite entanglement witnesses [32–34] and state verification methods [35,36] have been extensively studied with the development of large-scale entanglement preparations [37–39]. Many efforts have been made aiming at graph states or general stabilizer states, which are important resources in quantum information processing tasks, e.g., measurement-based quantum computing [40,41], quantum routing, and quantum networks [42–44]. The entanglement witness and the state verification of stabilizer states can be greatly simplified by utilizing the property of stabilizers [35,45–51]. Focusing on the device-independent scenario,

*zhaoq@cs.hku.hk
†you_zhou@fudan.edu.cn

it is thus an interesting open problem to ask whether the same properties can be applied for constructing Bell inequalities.

In this work, inspired by Ref. [25], which constructs the Bell inequalities from the generators, we propose a systematical framework for constructing Bell inequalities with two local observables from stabilizers. We show that the necessary and sufficient condition to realize the self-testing is that a set of stabilizers used in the construction can uniquely determine the state device dependently, which closes the gap between the device-dependent and -independent verifications. Taking advantage of the framework, we provide more choices of Bell inequalities with self-testing. As applications, two families of Bell inequalities are proposed showing different advantages. For any stabilizer state, we construct Bell inequalities with constant ratio of quantum and classical bounds with a linear number of correlations. To further enable the robust self-testing, we take examples of quantum multipartite states up to 6 qubits, including Greenberger-Horne-Zeilinger (GHZ) states and cluster states, and give the fidelity lower bound according to the Bell inequality violation. In particular, also with a linear number of correlations, we construct a type of Bell inequality, referred to as a *single pair* inequality, showing the best-known robust self-testing bound, which outperforms Mermin inequality [28,52] and Bell inequalities proposed in [25]. As a side result, our Bell inequalities can also serve as a device-independent entanglement witness, which provides more alternatives for the entanglement detection in the device-independent scenario.

II. GRAPH STATES AND THE STABILIZER FORMALISM

Stabilizer states [53,54] can be transformed to graph states via local unitary operations [55]. Thus in the following we discuss graph states without loss of generality. A graph state can be defined based on a graph $\mathcal{G} = (V, E)$, with vertices set $V = \{1, 2, \dots, N\}$ and edges set $E \subset [V]^2$. Two vertices i, j are adjacent if there is an edge (i, j) connecting them, and the adjacent set of vertex i is denoted as n_i. Let the qubits take the role of the vertices and the edges represent the controlled-Z operations. Then a graph state can be written as

$$|\psi_{\mathcal{G}}\rangle = \prod_{(i,j)\in E} \mathrm{CZ}^{\{i,j\}}|+\rangle^{\otimes N}, \tag{1}$$

where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ is the eigenstate of the Pauli X matrix and $\mathrm{CZ}^{\{i,j\}}$ is the controlled-Z gate, $\mathrm{CZ}^{\{i,j\}} = |0\rangle_i\langle 0| \otimes \mathbb{I}_j + |1\rangle_i\langle 1| \otimes Z_j$. Hereafter X_i, Y_i, Z_i denote the Pauli operators of the qubit i. Graph states can be uniquely determined by N generators,

$$G_i = X_i \bigotimes_{j\in n_i} Z_j, \tag{2}$$

which commute with each other and satisfy $G_i|\psi_{\mathcal{G}}\rangle = |\psi_{\mathcal{G}}\rangle$, $\forall i$, that is, the unique eigenstate with eigenvalue 1 for all the N generators. As a result, a graph state can also be written as a product of projectors of the generating operators:

$$|\psi_{\mathcal{G}}\rangle\langle\psi_{\mathcal{G}}| = \prod_{i=1}^{N} \frac{G_i + \mathbb{I}}{2}. \tag{3}$$

All the stabilizing operators can be generated by the multiplication of these generators,

$$S = \prod_i G_i, \tag{4}$$

which satisfies $S|\psi_{\mathcal{G}}\rangle = |\psi_{\mathcal{G}}\rangle$. For simplicity, we use the phrase "stabilizers" to represent the stabilizing operators hereafter. The property of stabilizers can be utilized to verify the graph states and construct the entanglement witness efficiently [45,49].

III. CONSTRUCTING BELL INEQUALITIES FROM PAIRABLE STABILIZERS

For an N-party graph state $\psi_{\mathcal{G}}$ from graph $\mathcal{G}$, we label each party with registers $1, 2 \dots, N$. We refer to the graph as K-colorable if one can label the graph with K different colors, requiring that there is no pair of adjacent vertices of the same color. According to this definition, we can divide all the N vertices into K disjoint subsets $C_{k=1,2,\cdots,K}$ such that there is no edge inside each C_k. The smallest K is referred to as the chromatic number of $\mathcal{G}$.

In this work we mainly explore the efficient Bell inequalities with two local observables for each party. We transform Pauli operators X and Z in the stabilizers to the observables in Bell inequalities according to certain rules. For a graph state, its generators only involve I, X, and Z operators, whereas the multiplication of generators from different color subsets can introduce Y operators in the stabilizers. Thus we only focus on the stabilizers S which are generated by the generators from the same color subset C_k:

$$S = \prod_{i\in C_k} G_i. \tag{5}$$

These stabilizers can be represented by the tensor product of Pauli operators, $S = \bigotimes_i M_i$, where $M_i \in \{X, Z, \mathbb{I}\}$. For simplicity, we define a sequence $(s_1, \dots, s_N)$ to express a stabilizer S with $s_i = 1$ when $M_i = X$, $s_i = -1$ when $M_i = Z$, and $s_i = 0$ when $M_i = \mathbb{I}$. Before showing the construction of Bell inequalities, let us first define a relationship between two stabilizers.

Definition 1. Two stabilizers $S^1 = \bigotimes_i M_i^1$, $S^2 = \bigotimes_i M_i^2$ are called *pairable* if there exists at least one position i such that local operators are anticommutative, that is, $\exists\, i$, $M_i^1 = Z, M_i^2 = X$ or $M_i^1 = X, M_i^2 = Z$ $(s_i^1 s_i^2 = -1)$.

Note that *pairable* stabilizers could have more than one anticommutative position. Thus this definition is different with anticommutative stabilizers. Hereafter, we use the subscript i to represent ith party and use superscript to represent different stabilizers. Here we choose one pair of *pairable* stabilizers S^1 and S^2, and one anticommutative position T. For position $i = T$, we replace the Pauli operators X_i and Z_i in the stabilizers S^1 and S^2 by observables $A_i + B_i$ and $A_i - B_i$, respectively. As for all the other positions $i \neq T$, we replace X_i and Z_i by A_i and B_i, respectively. Consequently, the Bell inequality based on *pairable* stabilizers S^1 and S^2 is shown as follows.

Lemma 1.

$$\mathcal{B}_{1,2} = \sum_{j=1,2} \left\langle \left(A_i + s_i^j B_i\right)_{i=T} \prod_{i\neq T} P_i\left(s_i^j\right) \right\rangle \leqslant \beta_c, \tag{6}$$

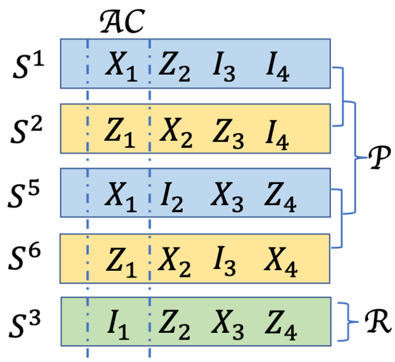

FIG. 1. An example of $\mathcal{P}, \mathcal{R}$ with a suitable $\mathcal{AC}$ for the four-party cluster state. For a given $\mathcal{ST} = \{1, 2, 3, 5, 6\}$ where $S^1 = G_1 = X_1Z_2$, $S^2 = G_2 = Z_1X_2Z_3$, $S^3 = G_3 = Z_2X_3Z_4$, $S^5 = G_1G_3$, $S^6 = G_2G_4$, we can assign $\mathcal{P} = \{(1, 2), (5, 6)\}$, $\mathcal{R} = \{3\}$ with $\mathcal{AC} = \{1\}$. We can also assign $\mathcal{P} = \{(2, 3), (2, 5)\}$, $\mathcal{R} = \{1, 6\}$ with $\mathcal{AC} = \{3\}$.

where $P_i(0) = \mathbb{I}, P_i(1) = A_i, P_i(-1) = B_i, A_i, B_i$ are all binary observables. The classical bound for this Bell inequality is $\beta_c = 2$ and the quantum bound (the maximal quantum value) $\beta_Q = 2\sqrt{2}$, which can be reached by the graph state $\psi_{\mathcal{G}}$.

The quantum bound is achieved by taking $A_i = \frac{X+Z}{\sqrt{2}}, B_i = \frac{X-Z}{\sqrt{2}}$ when $i = T$, and $A_i = X, B_i = Z$ when $i \neq T$. Here the choice of the measurement settings is the same with Ref. [25] and Clauser-Horne-Shimony-Holt (CHSH) inequality [56]. Intuitively, we can choose a lot of *pairable* stabilizers to construct Bell inequalities. We first choose a subset of the stabilizer set as $\mathcal{ST} \subset \mathcal{S}$. According to the *pairable* property, we define some *pairable* stabilizers in $\mathcal{ST}$ as

$$\mathcal{P} = \{(l, k)|S^l, S^k \in \mathcal{ST} \text{ are pairable}, \ l < k\}. \tag{7}$$

Note that for different pairs, they can share the same stabilizer, for example, we allow $(1, 2), (1, 3) \in \mathcal{P}$. Besides the *pairable* stabilizers, we also define the set of all the other nonpairable stabilizers in $\mathcal{ST}$ as $\mathcal{R}$. Moreover, to be more general, we define a vertex subset $\mathcal{AC} \subset V$ to replace the Pauli operators X and Z on these positions with $A - B$ and $A + B$, such as $\mathcal{AC} = \{T\}$ in $\mathcal{B}_{1,2}$.

For given $\mathcal{ST}, \mathcal{P}, \mathcal{R}$, we require that the set $\mathcal{AC}$ satisfies

(1) For every pair of *pairable* stabilizers, S^l and S^k, $\{l, k\} \in \mathcal{P}$, there exists only one position $T_{l,k} \in \mathcal{AC}$ such that the measurement setting of stabilizers, S^l and S^k in this position, are anticommutative. For other positions $i \in \mathcal{AC}\{T_{l,k}\}$, the measurement settings in S^l and S^k are all $\mathbb{I}$, $s_i^l = s_i^k = 0$.

(2) For every stabilizer $S^r (r \in \mathcal{R})$, the measurements in any position $i \in \mathcal{AC}$ are $\mathbb{I}$, $s_i^r = 0$.

These requirements are used to guarantee a large ratio of quantum and classical bounds in the constructed Bell inequalities. Luckily, one can always find an $\mathcal{AC}$ for the chosen stabilizer set $\mathcal{ST}$, satisfying these requirements by the following lemma.

Lemma 2. For any given stabilizer set $\mathcal{ST}$ containing *pairable* stabilizers, one can always assign the stabilizers of $\mathcal{ST}$ into the paring set $\mathcal{P}$ and the remaining subset $\mathcal{R}$, and then find a suitable $\mathcal{AC}$ satisfying two requirements listed above.

Thus it is generally feasible to construct Bell inequalities from a stabilizer set $\mathcal{ST}$. In order to make this construction clearer, we show an example of a 4-qubit cluster state in Fig. 1.

There are also other constructions for this given stabilizer set $\mathcal{ST}$; here we only give two constructions as examples.

For $\mathcal{P}$, $\mathcal{R}$ with a suitable $\mathcal{AC}$ satisfying the above two requirements, we construct the Bell inequalities for general graph states as follows:

Theorem 1.

$$\sum_{(l,k)\in\mathcal{P}} \mathcal{B}_{l,k} + \sum_{r\in\mathcal{R}} \mathcal{B}_r \leqslant \beta_c = 2|\mathcal{P}| + |\mathcal{R}|,$$

$$\mathcal{B}_{l,k} = \sum_{j=l,k} \left\langle \prod_{i\in\mathcal{AC}} \left(A_i + s_i^j B_i\right) \prod_{i\notin\mathcal{AC}} P_i\left(s_i^j\right) \right\rangle, \tag{8}$$

$$\mathcal{B}_r = \left\langle \prod_{i\notin\mathcal{AC}} P_i(s_i^r) \right\rangle,$$

where $P_i(s_i^j)$ are defined in Lemma 1, and $|\mathcal{P}|$ and $|\mathcal{R}|$ denote the number of elements in sets $\mathcal{P}$ and $\mathcal{R}$, respectively. The quantum bound $\beta_Q = 2\sqrt{2}|\mathcal{P}| + |\mathcal{R}|$ and the corresponding graph state $\psi_{\mathcal{G}}$ can reach this maximal quantum value.

Note that novel CHSH-like multipartite Bell inequalities proposed in [25] can be seen as special cases of Theorem 1 by choosing all the stabilizers being generators in Eq. (2), that is, $\mathcal{ST} = \{S^i|S^i = G_i, i \in \{1, \dots, N\}\}$, where G_i is the generator associated with the ith vertex. In particular, assuming the first vertex is the one with the largest number of neighbors, $|n_1| = \max_i |n_i|$, the generators in $\mathcal{ST}$ are assigned into $\mathcal{P} = \{(1, j)|j \in n_1\}$, $\mathcal{R} = \{r|r \neq n_1 \cup 1\}$ with $\mathcal{AC} = \{1\}$.

Sufficient and necessary condition for self-testing. Besides ruling out the classical hidden variable model, Bell inequalities further provide us a method to verify quantum states in a device-independent manner. Though the graph state $\psi_{\mathcal{G}}$ can reach the maximal quantum value of all Bell inequalities constructed from its stabilizers in Theorem 1, not all these Bell inequalities can verify $\psi_{\mathcal{G}}$ uniquely. Here in this section, based on the constructed Bell inequalities, we explore the sufficient and necessary condition for the self-testing of graph states.

Definition 2. Suppose that the Bell inequality $\mathcal{B}_{\mathcal{G}}$, constructed from the stabilizers of $\psi_{\mathcal{G}}$, is maximally violated by a state ψ and corresponding local observables A_i, B_i. If up to local isometries, all states ψ and the corresponding local observables which maximally violate the Bell inequalities $\mathcal{B}_{\mathcal{G}}$ are equivalent to the graph state $\psi_{\mathcal{G}}$, and $\frac{X_i+Z_i}{\sqrt{2}}$, $\frac{X_i-Z_i}{\sqrt{2}}$ when $i \in \mathcal{AC}$; X_i, Z_i when $i \notin \mathcal{AC}$, we say this Bell inequality $\mathcal{B}_{\mathcal{G}}$ can self-test graph state $\psi_{\mathcal{G}}$.

In the conventional device-dependent verification of graph states, we have the following fact about determining the graph state $\psi_{\mathcal{G}}$ with the trust of measurement devices.

Fact 1. [53,54] For the device-dependent verification, a set of stabilizer measurements can uniquely determine the state $\psi_{\mathcal{G}}$, if and only if it contains N independent stabilizers. A set of stabilizers is independent if they cannot generate each other by multiplication and note that any other stabilizers can be generated by N independent stabilizers.

Theorem 2. The family of Bell inequalities proposed in Theorem 1 can self-test the graph state $\psi_{\mathcal{G}}$, if and only if the stabilizers in $\mathcal{ST}$ together can determine the graph state $\psi_{\mathcal{G}}$.

Via this theorem, we make a close connection between the device-independent and -dependent verifications. If the stabilizers can determine the graph state under the trust of measurement devices, then one can always transform these stabilizers to Bell inequalities and apply it to verify the state without trusting the devices under our framework. Thus any witnesses and state verification methods based on stabilizers could inspire the construction of Bell inequalities.

IV. APPLICATIONS

Utilizing the above framework, we propose various families of Bell inequalities, which show the advantages in different aspects. Note that in this section we only explore Bell inequalities with the self-testing property.

A. Constant ratio of quantum and classical bounds β_Q/β_C

At first, we prefer to select Bell inequalities with a large ratio of quantum and classical bounds β_Q/β_C, which is beneficial for the experimental violation under practical setups and can lead to good performance in cryptography tasks [5]. From Theorem 1, it is clear that the maximal β_Q/β_C is $\sqrt{2}$ when $\mathcal{R}=\varnothing$ in our construction. Utilizing the properly designed multiplications of generators from the graph state, we can construct self-testing Bell inequalities with the maximal ratio for any graph state.

Corollary 1. For any N-party graph state $\psi_{\mathcal{G}}$, based on our framework one can construct Bell inequalities using $2N$ correlations to reach the maximal $\beta_Q/\beta_C=\sqrt{2}$ with a self-testing property at the same time.

The proof and detailed constructions are shown in Appendix C. In Ref. [25], only an asymptotic case (infinity large N) and some special states, for example, a GHZ state, can reach this ratio $\beta_Q/\beta_C=\sqrt{2}$. Due to flexible choices of stabilizers, instead of only using generators, our framework provides Bell inequalities with generally larger β_Q/β_C than the constructions in [25], also using a linear number of correlations, which are efficient and scalable for practical demonstrations in multipartite systems.

B. Improved robust self-testing bounds

In the robust self-testing, one would like to lower bound the state fidelity to the target graph state $\psi_{\mathcal{G}}$ (under local isometries), only on account of the Bell inequality value which deviates from the maximal quantum value. We give a formal definition of robust self-testing as follows.

Definition 3. Bell inequality $\mathcal{B}_{\mathcal{G}}$ and a Bell value β self-test the graph state $\psi_{\mathcal{G}}$ with fidelity f if for any underlying state ρ achieves the Bell value β and satisfies that

$$F(\Lambda(\rho),\quad \psi_{\mathcal{G}})\geqslant f, \tag{9}$$

where Λ is a local isometry.

Here we expect that Bell inequalities can show good performance in the robust self-testing task. Benefiting from the flexibility of our construction, one can have many choices of Bell inequalities at hand. We give constructions of some typical examples, 3-qubit and 4-qubit GHZ states, and 4-qubit one-dimensional (1D) cluster states in Tables I, II, and III, respectively, with different $\mathcal{AC},\mathcal{P},\mathcal{R}$ and β_Q/β_C. Based on the method in [25,28], in Fig. 2, we numerically show their performance in robust self-testing and also compare with the Mermin inequality, which is widely used for self-testing GHZ states [28,52].

In principle, the robustness analysis can be extended to more qubits, and one can explore more possible Bell inequalities via our framework. The limitation to the extension is due to the difficulty of numerical optimization for large-qubit-number cases. Here we also show some examples of 5-qubit and 6-qubit graph states in Fig. 3. The results are shown in Fig. 4, and Tables IV and VIII.

From Fig. 2 one can find that larger β_Q/β_C value does not necessarily lead to a better performance in the robust self-testing, which is characterized by the slope of the curves. The reason behind this phenomenon may be that the method of estimating fidelity is not tight or optimal. In our examples, we find that the best robust self-testing Bell inequality share the same property, that is, they are constructed from only one *pairable* stabilizers, i.e., $|\mathcal{P}|=1$, and other stabilizers all in $\mathcal{R}$. (See Bell inequality 1 in Table I, Bell inequalities 1 and 2 in Table II, Bell inequality 1 in Table III.) We name them as *single pair* Bell inequalities,

$$\mathcal{B}_{1,2}+\sum_{r\in\mathcal{R}}\mathcal{B}_r\leqslant 2+|\mathcal{R}|. \tag{10}$$

TABLE I. Three-qubit GHZ (cluster) state with with generators $G_1=X_1Z_2, G_2=Z_1X_2Z_3$, and $G_3=Z_2X_3$. And we choose stabilizers as $S^1=G_1$, $S^2=G_2$, $S^3=G_3$, and $S^4=G_1G_3$. According to our framework, actually we can construct totally 12 Bell inequalities with self-testing. Here we only take a few of them as examples. Our constructions are shown in bold.

GHZ_3	$\mathcal{AC}$	$\mathcal{P}$	$\mathcal{R}$	β_Q/β_C
1	{1}	{(1, 2)}	{3}	$(2\sqrt{2}+1)/3$
2	{1}	{(1, 2), (2, 4)}	{3}	$(4\sqrt{2}+1)/5$
3	{1}	{(1, 2), (2, 4)}	$\varnothing$	$\sqrt{2}$
4 [25]	{2}	{(1, 2), (2, 3)}	$\varnothing$	$\sqrt{2}$

TABLE II. Four-qubit GHZ state with generators $G_1=X_1Z_2Z_3Z_4$, $G_2=Z_1X_2$, $G_3=Z_1X_3$, and $G_4=Z_1X_4$. And we choose stabilizers as $S^1=G_1$, $S^2=G_2$, $S^3=G_3$, $S^4=G_4$, $S^5=G_2G_3$, and $S^6=G_2G_4$. Our constructions are shown in bold.

GHZ_4	$\mathcal{AC}$	$\mathcal{P}$	$\mathcal{R}$	β_Q/β_C
1	{1}	{(1, 2)}	{5, 6}	$(\sqrt{2}+1)/2$
2	{2}	{(1, 2)}	{3, 4}	$(\sqrt{2}+1)/2$
3	{1}	{(1, 2), (1, 3)}	{6}	$(4\sqrt{2}+1)/5$
4 [25]	{1}	{(1, 2), (1, 3), (1, 4)}	$\varnothing$	$\sqrt{2}$

TABLE III. Four-qubit 1D cluster state with generators $G_1=X_1Z_2, G_2=Z_1X_2Z_3, G_3=Z_2X_3Z_4, G_4=Z_3X_4$. We choose stabilizers as $S^1=G_1$, $S^2=G_2$, $S^3=G_3$, $S^4=G_4$, $S^5=G_1G_3$, $S^6=G_2G_4$. Our constructions are shown in bold.

$Cluster_4$	$\mathcal{AC}$	$\mathcal{P}$	$\mathcal{R}$	β_Q/β_C
1	{1}	{(1, 2)}	{3, 4}	$(\sqrt{2}+1)/2$
2 [25]	{2}	{(1, 2), (2, 3)}	{4}	$(4\sqrt{2}+1)/5$
3	{1}	{(1, 2), (5, 6)}	$\varnothing$	$\sqrt{2}$
4	{2}	{(1, 2), (3, 6)}	$\varnothing$	$\sqrt{2}$

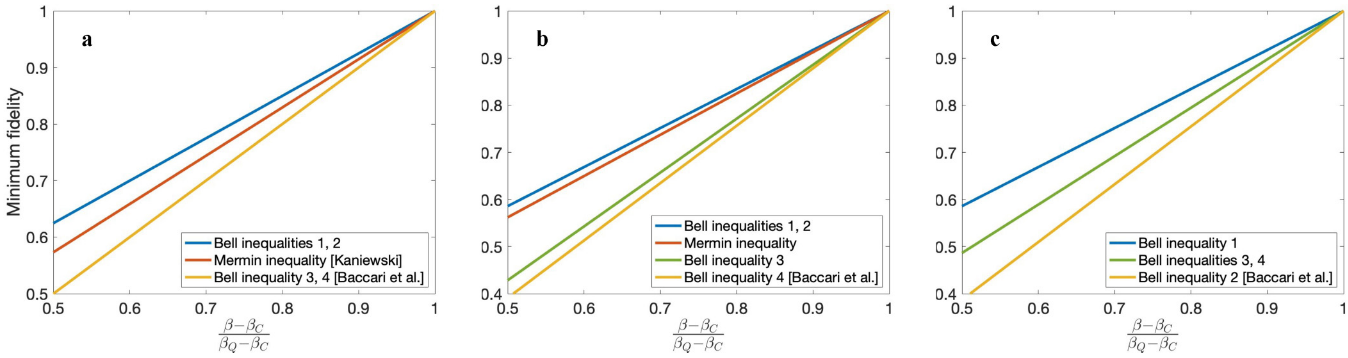

FIG. 2. Numerical estimation of the lower bound of fidelity to the target graph state vs normalized Bell inequality value $\frac{\beta-\beta_C}{\beta_Q-\beta_C}$: (a) 3-qubit GHZ state, (b) 4-qubit GHZ state, and (c) 4-qubit cluster state. We compare different constructions of Bell inequalities from our framework with previous results. The best candidates for robust self-testing are *single pair* inequalities, which are the blue curves in the figure, where it shows the best-known robustness self-testing performance, surpassing Mermin inequality in [28] and Bell inequalities proposed in [25], which are shown in the red curve and yellow curve, respectively.

From these examples and the realizable lower bounds of the fidelity, one can see that our constructed *single pair* Bell inequalities provide the best-known robust self-testing bound, improving the previous self-test bound in [25,28]. Note that compared to Mermin inequality with 2^N correlations, *single pair* Bell inequalities only contain $N+1$ correlations, which is more efficient and scalable for large-scale system verification. This shows the potentiality of our framework.

C. Device-independent entanglement witness

As a side result of the robust self-testing bound, one can also construct a device-independent genuine entanglement witness by applying the linear self-testing fidelity bound $F \geqslant a\frac{\beta-\beta_C}{\beta_Q-\beta_C}+b$ with slope a and intercept b.

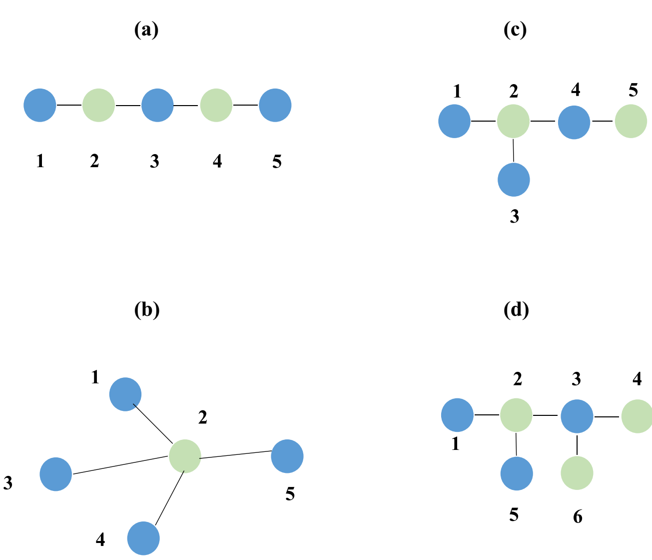

FIG. 3. Different 5-qubit and 6-qubit graph states: (a) 5-qubit cluster state, (b) 5-qubit GHZ state, (c) 5-qubit graph state $\mathcal{G}_5$, and (d) 6-qubit graph state $\mathcal{G}_6$.

Corollary 2.

$$\sum_{(l,k)\in\mathcal{P}} \mathcal{B}_{l,k} + \sum_{r\in\mathcal{R}} \mathcal{B}_r \overset{\text{bi-sep.}}{\leqslant} \beta_{\frac{1}{2}},$$

$$\beta_{\frac{1}{2}} = \frac{(0.5-b)(\beta_Q-\beta_C)}{a} + \beta_C, \tag{11}$$

where $\mathcal{B}_i$ and $\mathcal{B}_r$ are Bell correlations shown in Theorem 1, $\beta_{\frac{1}{2}}$ is the threshold Bell value. The violation of this inequality implies the existence of genuine entanglement.

This corollary is due to the fact that the underlying state possesses genuine entanglement when fidelity with a certain graph state exceeds $\frac{1}{2}$ [45,49]. The Bell value $\beta_{\frac{1}{2}}$ corresponds to a fidelity lower bound $\frac{1}{2}$. Thus any Bell value greater than $\beta_{\frac{1}{2}}$ implies the existence of genuine entanglement.

In the following we give genuine entanglement bounds $\beta_{\frac{1}{2}}$ and the detailed construction for *single pair* inequality with the best-known robustness bound. The device-independent genuine entanglement witness of three-party, four-party GHZ and four-party cluster are shown, respectively, in Eq. (12). Note that here the bound $\beta_{\frac{1}{2}}$ are from numerical results, not the accurate theoretical bound. Any violation of these inequalities implies the existence of genuine entanglement, and a similar method can also be used to detect more detailed entanglement structures in a device-independent manner:

$$\begin{aligned}
&\langle (A_1+B_1)B_2\rangle + \langle (A_1-B_1)A_2B_3\rangle \\
&\quad + \langle B_2A_3\rangle \overset{\text{bi-sep.}}{\leqslant} 3.2766, \\
&\langle (A_1+B_1)B_2B_3B_4\rangle + \langle (A_1-B_1)A_2\rangle \\
&\quad + \langle A_2A_3\rangle + \langle A_2A_4\rangle \overset{\text{bi-sep.}}{\leqslant} \tfrac{3}{2}+2\sqrt{2}, \\
&\langle (A_1+B_1)B_2\rangle + \langle (A_1-B_1)A_2B_3\rangle + \langle B_2A_3B_4\rangle \\
&\quad + \langle B_3A_4\rangle \overset{\text{bi-sep.}}{\leqslant} \tfrac{3}{2}+2\sqrt{2}.
\end{aligned} \tag{12}$$

V. DISCUSSION

In summary, we propose a systematical framework to construct Bell inequalities directly from stabilizers and further

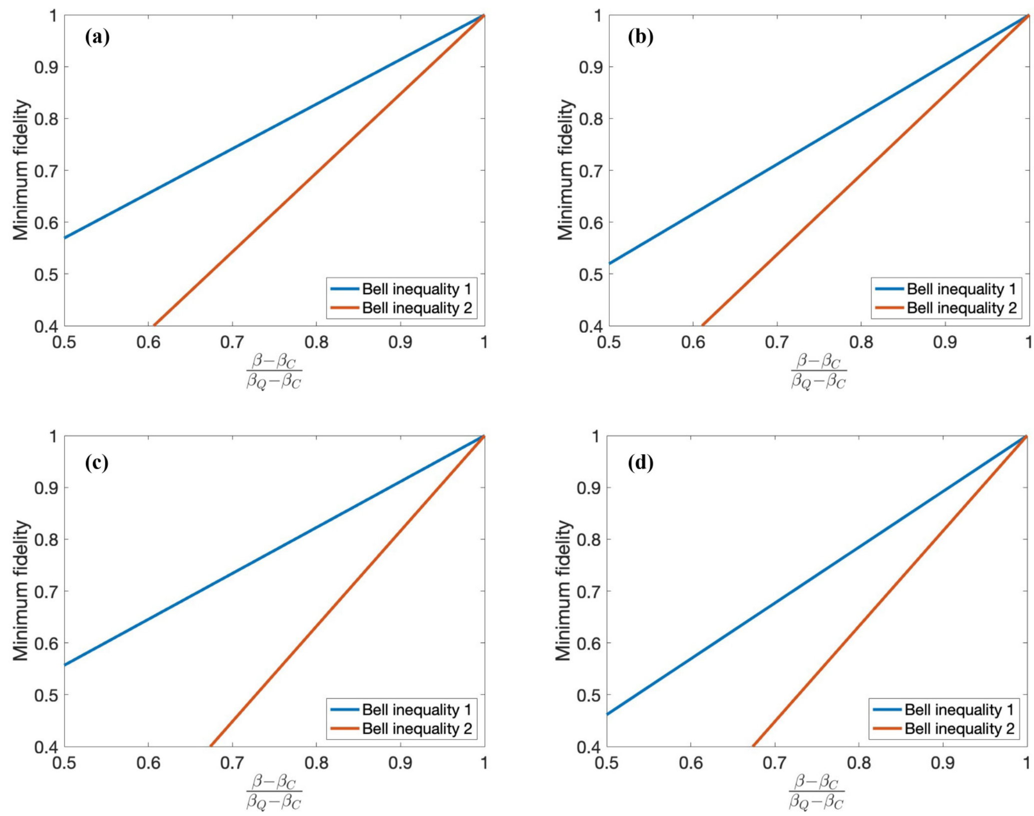

FIG. 4. Numerical estimation of the lower bound of fidelity to the target graph state vs normalized Bell inequality value $\frac{\beta-\beta_C}{\beta_Q-\beta_C}$: (a) 5-qubit GHZ state, (b) 5-qubit cluster state, (c) 5-qubit graph state $\mathcal{G}_5$, and (d) 6-qubit graph state $\mathcal{G}_6$. The best candidates for robust self-testing are *single pair* inequalities, which are the blue curves in the figure. Bell inequalities 1 and Bell inequalities 2 are shown in Table IV.

provide a one-to-one map from the device-dependent verification to the self-testing one. The framework can provide us with a large number of Bell inequalities to select for different application scenarios, for instance, a *single pair* Bell inequality for robust self-testing. Even though the fidelity lower bounds for robust self-testing are obtained by numerics, these results are also instructive for obtaining a (tight) analytical bound for general graph states in the future [28]. One may also find other interesting inequalities with other advantages. Our proposed Bell inequalities have been applied to self-test multiparticle graph states [57,58]. Similar to the entanglement witness, a modification of coefficients between different Bell expressions may be beneficial for improving the ratio of quantum and classical bounds and the robust self-testing performance [48,49,59].

TABLE IV. Five- and six-qubit graph states in Fig. 3; Bell inequalities constructed with generators. $\{i\}$ denotes the generator G_i associated to the ith qubit.

Cluster$_4$	$\mathcal{AC}$	$\mathcal{P}$	$\mathcal{R}$	β_Q/β_C
1	{1}	{(1, 2)}	{3, 4, 5}	$(2\sqrt{2}+3)/5$
2	{2}	{(1, 2), (2, 3)}	{4,5}	$(4\sqrt{2}+2)/6$
GHZ$_5$	$\mathcal{AC}$	$\mathcal{P}$	$\mathcal{R}$	β_Q/β_C
1	{1}	{(1, 2)}	{3, 4, 5}	$(2\sqrt{2}+3)/5$
2	{2}	{(1, 2), (2, 3), (2, 4), (2, 5)}	∅	$\sqrt{2}$
$\mathcal{G}_5$	$\mathcal{AC}$	$\mathcal{P}$	$\mathcal{R}$	β_Q/β_C
1	{1}	{(1, 2)}	{3, 4, 5}	$(2\sqrt{2}+3)/5$
2	{2}	{(1, 2), (2, 3), (2, 4)}	{5}	$(6\sqrt{2}+1)/7$
$\mathcal{G}_6$	$\mathcal{AC}$	$\mathcal{P}$	$\mathcal{R}$	β_Q/β_C
1	{1}	{(1, 2)}	{3, 4, 5, 6}	$(2\sqrt{2}+4)/6$
2	{2}	{(1, 2), (2, 3), (2, 5)}	{4, 6}	$(6\sqrt{2}+2)/8$

Via the proposed framework, we close the gap between device-independent and -dependent witness and verification, and borrow the experience from device-dependent study. This connection can inspire more complicated Bell inequality constructions, for instance, ones with more than two local measurements, applying Y operators in stabilizers. It would also be interesting to extend the method to hypergraph states, nonstabilizer states, high-dimensional entangled states, and entangled subspaces [60–64], or explore a weak form of self-testing which verifies the state without a full self-testing of measurements [65,66].

Under the context of entanglement detection, like the entanglement witnesses shown above, one can also obtain device-independent entanglement (structure) witnesses [16,48,49,67], and we leave these problems to future work.

ACKNOWLEDGMENTS

Q.Z. acknowledges support from the Department of Defense through the Hartree Postdoctoral Fellowship at QuICS and the HKU Seed Fund for New Staff. Y.Z. acknowledges support from National Natural Science Foundation of China Grant No. 12205048, startup funding from Fudan University, the Templeton Religion Trust under Grant No. TRT 0159, and the ARO under Contract No. W911NF1910302.

APPENDIX A: PROOF FOR CONSTRUCTED BELL INEQUALITIES

1. Proof for Lemma 1

For any *pairable* stabilizers S^1 and S^2, we choose one of its anticommutative position, e.g., T, such that $s_T^1 s_T^2 = -1$. It is not hard to see that the classical value of $\mathcal{B}_{1,2}$ cannot be greater than $\langle A_T + B_T\rangle + \langle A_T - B_T\rangle \leqslant 2$. Then we prove the quantum bound by expressing the difference as

$$2\sqrt{2} - \mathcal{B}_{1,2} = \left\langle \frac{1}{\sqrt{2}}\left[\mathbb{I} - \left(\frac{A_T + B_T}{\sqrt{2}}\right)\prod_{i\neq T} P_k(s_i^1)\right]^2 + \frac{1}{\sqrt{2}}\left[\mathbb{I} - \left(\frac{A_T - B_T}{\sqrt{2}}\right)\prod_{i\neq T} P_k(s_i^2)\right]^2\right\rangle \geqslant 0. \tag{A1}$$

The quantum bound is reached by choosing $A_T = \frac{X+Z}{\sqrt{2}}, B_T = \frac{X-Z}{\sqrt{2}}$ and $A_i = X, B_i = Z$ for $i \neq T$ with the underlying state as the graph state $\psi_{\mathcal{G}}$.

2. Proof for Lemma 2

We choose one pair of *pairable* stabilizers S^1 and S^2, and choose one anticommutative position, denoted as T. We divide all the stabilizers belonging to $\mathcal{ST}$ into three subsets according to the measurement setting on the Tth position:

$$\begin{aligned}\mathcal{P}_+ &= \{S|s_T = 1, S\in\mathcal{ST}\},\\ \mathcal{P}_- &= \{S|s_T = -1, S\in\mathcal{ST}\},\\ \mathcal{P}_0 &= \{S|s_T = 0, S\in\mathcal{ST}\}.\end{aligned} \tag{A2}$$

Any stabilizers $S^l \in \mathcal{P}_+$ and $S^k \in \mathcal{P}_-$ are *pairable*. If $|\mathcal{P}_+| \neq |\mathcal{P}_-|$, we can reuse the stabilizers. In this way all the stabilizers in $\mathcal{P}_+ \cup \mathcal{P}_-$ can be assigned into paring set $\mathcal{P}$ and also let $\mathcal{P}_0 = \mathcal{R}$ and $\mathcal{AC} = T$. Then the above construction satisfies two listed requirements.

3. Proof for Theorem 1

First the classical bound can be obtained by multiple uses of the result in Lemma 1, that is, $\sum_{(l,k)\in\mathcal{P}}(\mathcal{B}_l + \mathcal{B}_k) \leqslant 2|\mathcal{P}|$, and the fact $\sum_{r\in\mathcal{R}}\mathcal{B}_r \leqslant |\mathcal{R}|$. Then we prove the quantum bound by showing that

$$2\sqrt{2}|\mathcal{P}| + |\mathcal{R}| - \sum_{(l,k)\in\mathcal{P}}(\mathcal{B}_l + \mathcal{B}_k) - \sum_{r\in\mathcal{R}}\mathcal{B}_r \geqslant 0. \tag{A3}$$

Note that here in each $\mathcal{B}_l$, $\mathcal{B}_k$, and $\mathcal{B}_r$ all the observables A and B are not fixed measurement settings but arbitrary dichotomic observables. Similar to the proof of Lemma 1, this inequality can be transformed into a sum of the following squares:

$$\begin{aligned} 2\sqrt{2} - \mathcal{B}_l - \mathcal{B}_k &= \left\langle \frac{1}{\sqrt{2}}\left[\mathbb{I} - \prod_{i\in\mathcal{AC}}(A_i + s_i^l B_i)\prod_{i\notin\mathcal{AC}} P_i(s_i^l)\right]^2 \right.\\ &\quad \left. + \frac{1}{\sqrt{2}}\left[\mathbb{I} - \prod_{i\in\mathcal{AC}}(A_i + s_i^k B_i)\prod_{i\notin\mathcal{AC}} P_i(s_i^k)\right]^2\right\rangle \geqslant 0, \end{aligned} \tag{A4}$$

$$1 - \mathcal{B}_r = \left\langle \frac{1}{2}\left[\mathbb{I} - \prod_{i\notin\mathcal{AC}} P_k(s_i^j)\right]^2\right\rangle \geqslant 0. \tag{A5}$$

The quantum bound is reached by choosing $A_i = \frac{X+Z}{\sqrt{2}}, B_i = \frac{X-Z}{\sqrt{2}}$ when $i \in \mathcal{AC}$; $A_i = X, A_i = Z$ when $i \notin \mathcal{AC}$ where the underlying state is the graph state $\psi_{\mathcal{G}}$.

APPENDIX B: PROOF FOR SELF-TESTING OF THEOREM 2

First we prove the "if " part. The proof of this part is similar to Refs. [18,25]. We assume the underlying state is ψ and observables are O_i for the ith party and prove that for all correlations in Bell inequality there exists an isometry $\Phi = \bigotimes_{i=1}^N \Phi_i$ with local isometries Φ_i,

$$\Phi\left[\prod_i O_i(s_i^j)|\psi\rangle\right] = \prod_i P_i(s_i^j)(|\psi_{\mathcal{G}}\rangle \otimes |extra\rangle), \tag{B1}$$

where for $i \in \mathcal{AC}, P_i(0) = \mathbb{I}, P_i(1) = \frac{X+Z}{\sqrt{2}}; P_i(-1) = \frac{X-Z}{\sqrt{2}}$, for $i \notin \mathcal{AC}, P_i(0) = \mathbb{I}, P_i(1) = X, P_i(-1) = Z$.

Without loss of generality, in the following we assume $\mathcal{AC} = \{1\}$ and the case where $\mathcal{AC}$ contains more than one position can be proved similarly. Denote

$$\begin{aligned}\tilde{X}_1 &= \frac{1}{c\sqrt{2}}[O_1(1) + O_1(-1)],\\ \tilde{Z}_1 &= \frac{1}{c'\sqrt{2}}[O_1(1) - O_1(-1)].\end{aligned} \tag{B2}$$

Here we also change zero eigenvalues of $O_1(1) \pm O_1(-1)$ to 1, and c, c' are normalized parameters such that $|\tilde{X}_1| = |\tilde{Z}_1| = 1$. Please refer to Refs. [25,68] for more details of this construction. For $i \neq 1$, we denote $\tilde{X}_i = O_i(1)$ and $\tilde{Z}_i = O_i(-1)$, which are the actual implemented observables.

A key step of the proof is to show that for each position i, when acting on the underlying state ψ, $\tilde{X}_i$ and $\tilde{Z}_i$ are anticommutative, i.e.,

$$(\tilde{X}_i\tilde{Z}_i + \tilde{Z}_i\tilde{X}_i)|\psi\rangle = 0, \quad i = 1, 2\ldots, N. \tag{B3}$$

When the Bell inequality reaches the maximal value, the inequalities in Eqs. (A4) and (A5) in the proof of Theorem 1 should be saturated when acting on the state ψ. As a result, according to each square in the equations, we have

$$\begin{aligned}\tilde{X}_1|\psi\rangle &= \prod_{i\neq 1} O_i(s_i^l)|\psi\rangle,\\ \tilde{Z}_1|\psi\rangle &= \prod_{i\neq 1} O_i(s_i^k)|\psi\rangle,\\ |\psi\rangle &= \prod_{i\neq 1} O_i(s_i^r)|\psi\rangle,\end{aligned} \tag{B4}$$

where $(l,k)\in\mathcal{P}$ and $r\in\mathcal{R}$. For the position $i=1$, the anticommutative relationship can be obtained directly from Eq. (B2):

$$(\tilde{X}_1\tilde{Z}_1+\tilde{Z}_1\tilde{X}_1)|\psi\rangle=0. \tag{B5}$$

Since the stabilizers in $\mathcal{ST}=\mathcal{P}\cup\mathcal{R}$ can determine the graph state $\psi_{\mathcal{G}}$, $\mathcal{ST}$ at least contains N independent stabilizers. For all generators in Eq. (2), there always exist a series of stabilizers $S^{i_1},\dots,S^{i_m}$ from $\mathcal{ST}$ satisfying

$$G_i=\prod_{j=1}^{m}S^{i_j}, \tag{B6}$$

with $m\leqslant N$. By multiple uses of Eq. (B4) and plugging into Eq. (B6), we have

$$\tilde{X}_i|\psi\rangle=\prod_{j\in n_i}\tilde{Z}_j|\psi\rangle \tag{B7}$$

for all $1\leqslant i\leqslant N$. Thus for $j\in n_1$, by utilizing the relations of vertex 1 and j in Eq. (B7), we have

$$(\tilde{Z}_j\tilde{X}_j+\tilde{X}_j\tilde{Z}_j)|\psi\rangle=(\tilde{Z}_1\tilde{X}_1+\tilde{X}_1\tilde{Z}_1)\prod_{i\in\mathcal{C}(1,j)}Z_i|\psi\rangle, \tag{B8}$$

where $\mathcal{C}(1,j)=[n_1\cup n_j]\setminus[\{1,j\}\cup(n_1\cap n_j)]$ denotes the set of all the vertices which are neighbors of either 1 or j but are not 1 or j themselves. Starting from position 1, we can obtain the anticommutative relationship for the positions $j\in n_1$:

$$(\tilde{X}_j\tilde{Z}_j+\tilde{Z}_j\tilde{X}_j)|\psi\rangle=0,\quad j\in n_1. \tag{B9}$$

Then in the same way we can obtain the anticommutative relationship for the operators whose corresponding vertex is the neighbor of the vertices in $n(1)$. Because the graph is connected, we can iterate the above procedure and get the anticommutative relationship for all parties. The construction of the isometry Φ is exactly the same with that in [25], and we do not repeat it here.

Secondly, we prove the "only if" part. Here we tackle the situation that one constructs the Bell inequality via Theorem 1, i.e., using some stabilizers with the CHSH trick, but the stabilizer set involved there is not complete, i.e., the elements in the set cannot generate all the stabilizers. Then we prove that one cannot self-test the underlying state, by constructing a mixed state to make a contradiction.

Suppose the stabilizer set $\mathcal{ST}$ involved in Theorem 1 cannot determine the graph state. That is, it can at most contain $N-1$ independent stabilizers denoted by $S^1,S^2,\dots,S^{N-1}$, and we can always find one generator denoted by $S^N=G_N$ that cannot be expressed by the product of stabilizers in $\mathcal{ST}$. Consequently, we construct a state

$$\rho=\frac{1}{2}\prod_{i=1}^{N-1}\frac{S^i+\mathbb{I}}{2}, \tag{B10}$$

which is the maximally mixed state in the two-dimensional subspace, determined by $S^1,S^2,\dots,S^{N-1}$ all taking the eigenvalue 1. As a result, ρ has exactly the same value with $\psi_{\mathcal{G}}=\prod_{i=1}^{N}\frac{S^i+\mathbb{I}}{2}$ for Bell inequalities constructed from $\mathcal{ST}$.

Note that ρ is actually the mixture of $\psi_{\mathcal{G}}$ and another state:

$$\rho=\frac{(\mathbb{I}+G_N)/2+(\mathbb{I}-G_N)/2}{2}\prod_{i=1}^{N-1}\frac{S^i+\mathbb{I}}{2}=\frac{1}{2}(\psi_{\mathcal{G}}+\psi_{\mathcal{G}}'). \tag{B11}$$

Here the state $\psi_{\mathcal{G}}'$ is determined by $S_1,S_2,\dots,S_{N-1}$, all taking the eigenvalue 1 and G_N taking -1:

$$\psi_{\mathcal{G}}'=\frac{(\mathbb{I}-G_N)}{2}\prod_{i=1}^{N-1}\frac{S_i+\mathbb{I}}{2}. \tag{B12}$$

Since $\{S_i\}_1^N$ is complete, one can uniquely determine whether $G_i|\psi_{\mathcal{G}}'\rangle=|\psi_{\mathcal{G}}'\rangle$ or $-|\psi_{\mathcal{G}}'\rangle$ by multiplying the results of them, and we denote the vertex subset $\mathcal{D}=\{i:G_i|\psi_{\mathcal{G}}'\rangle=-|\psi_{\mathcal{G}}'\rangle\}$. As a result, $\psi_{\mathcal{G}}'$ can also be transformed from $\psi_{\mathcal{G}}$ by local unitary:

$$|\psi_{\mathcal{G}}'\rangle=\prod_{i\in\mathcal{D}}Z_i|\psi_{\mathcal{G}}\rangle. \tag{B13}$$

In the following we show that ρ cannot be transformed to $\psi_{\mathcal{G}}$ by local isometries, which contradicts the self-testing claim. Let us focus on any single qubit, say the first qubit, and take it as the subsystem B and the remaining qubits as A. The quantum conditional entropy on A of the state $\psi_{\mathcal{G}}$ is

$$S(A|B)_{\psi_{\mathcal{G}}}=S(AB)_{\psi_{\mathcal{G}}}-S(B)_{\psi_{\mathcal{G}}}=-1, \tag{B14}$$

where we use the fact that $\psi_{\mathcal{G}}$ is pure and the entanglement entropy of the first qubit is 1 [55]. On the other hand, the quantum conditional entropy of the state ρ shows

$$S(A|B)_\rho=S(AB)_\rho-S(B)_\rho=1-S(B)_\rho\geqslant 0, \tag{B15}$$

where we apply the fact that ρ is a maximally mixed state in the subspace, and the entropy of B is upper bounded by the qubit number 1.

It is known that $S(A|B)$ quantifies how many qubits need to be sent from A (Alice) to B (Bob) to reconstruct ρ_{AB} at Bob's side in the quantum state merging task [69]. A negative value indicates that one does not need to send qubits but can also *gain* $-S(A|B)$ maximally entangled pairs. Considering the two states given before, suppose one can transform ρ to $\psi_{\mathcal{G}}$ with local isometries, and we show this contradicts the quantum state merging efficiency. First, transform ρ to $\psi_{\mathcal{G}}$ with local isometries, and then one can finish the quantum state merging of $\psi_{\mathcal{G}}$ without any qubit sending but get one entangled pair. Finally, one can transform $\psi_{\mathcal{G}}$ back to ρ using local operations according to Eq. (B13) with 1/2 probability, which contradicts $S(A|B)_\rho\geqslant 0$.

APPENDIX C: PROOF FOR APPLICATIONS

1. Proof for Corollary 1

We divide the N vertices of the graph with chromatic number K into K disjointed subset C_k. According to Lemma 3 below, one can always find a vertex, without loss of generality, denoted as the vertex 1 belonging to the first color subset, $1\in C_1$ satisfying that from every other color subset C_k $(k\neq 1)$ there always exists at least one vertex $v_k\in C_k$ such that vertex 1 and v_k are neighbors, i.e., $v_k\in n_1$. We construct K disjoint stabilizer sets as follows:

$$\begin{aligned}\mathcal{P}_1 &= \{G_1, G_1G_j \mid j \in C_1 \setminus \{1\}\},\\ \mathcal{P}_k &= \{G_i, G_iG_j \mid i \in C_k \cap n_1, j \in C_k \setminus n_1\},\\ &k = 2, 3 \ldots, K,\end{aligned} \tag{C1}$$

where G_i denotes the generator of the ith vertex. Here $\mathcal{P}_1$ contains G_1 and the multiplications of G_1 with the other generators from the first color set C_1. For $2 \leqslant k \leqslant K$, $\mathcal{P}_k$ contains the generators of the neighbors of vertex 1, and the multiplications of these generators with the other generators from the same color set C_k. For simplicity of construction, we only consider the multiplication of G_j with one of the generators from n_1, say G_k.

It is not hard to check that any pair of $S^i \in \mathcal{P}_1, S^j \in \mathcal{P}_k$ is *pairable*. In particular, they are anticommutative at the first position $i = 1$. We denote the stabilizers in $\mathcal{P}_1$ as $S^1, \ldots S^{|C_1|}$ and other stabilizers in $\mathcal{P}_2, \ldots, \mathcal{P}_K$ as $S^{|C_1|+1}, \ldots S^N$. We choose $\mathcal{AC} = \{1\}$, and when $2|C_1| \leqslant N$ we construct the corresponding Bell inequality by reusing stabilizer S^1 as follows:

$$(N - 2|C_1| + 1)\mathcal{B}_1 + \sum_{j=2}^{N} \mathcal{B}_j \leqslant \beta_C = 2(N - |C_1|), \tag{C2}$$

where $\mathcal{B}_j = \langle (A_1 + s_1^j B_1) \prod_{i \neq 1} P_i(s_i^j) \rangle$. When $2|C_1| > N$, we reuse the stabilizer S^N and construct the Bell inequality:

$$(2|C_1| - N + 1)\mathcal{B}_N + \sum_{j=1}^{N-1} \mathcal{B}_j \leqslant \beta_C = 2|C_1|. \tag{C3}$$

These two Bell inequalities both have $2N$ correlations, and the maximal quantum values are $\beta_Q = 2\sqrt{2}(N - |C_1|)$, $\beta_Q = 2\sqrt{2}|C_1|$, respectively. As a result, the ratio $\beta_Q/\beta_C = \sqrt{2}$ for both cases.

The stabilizers we used are $\mathcal{ST} = \bigcup_{k=1,2\ldots,K} \mathcal{P}_k$ containing N independent stabilizers. Via Theorem 2, we prove that the above inequality can self-test the graph state $\psi_{\mathcal{G}}$.

Lemma 3. For any graph $\mathcal{G} = (V, E)$ whose chromatic number is K with disjoint color sets $C_1, \ldots, C_K$, $V = \bigcup_{k=1}^{K} C_k$, there always exists a vertex, for example, $1 \in C_1$ satisfying that from every other color subset, we could find at least one vertex $v_k \in C_k$ $k = 2, \ldots, K$ such that vertex 1 and v_k are neighbors, $v_k \in n_1$.

Proof. We prove this Lemma by contradiction. Assuming that we could not find the vertex satisfying the requirement, we denote the vertex with the maximal different color neighbors as vertex 1. Thus there exists a color set, for example, C_K, with no vertex from it is neighbor to vertex 1. Then we pick one vertex from C_K, denoted as vertex v_K, where we can always find a color set C_q ($q \neq K$) such that every vertex in C_q is not neighbor to v_K; otherwise it is contradictive to the assumption that vertex 1 has the maximal different color neighbors. Then we can color this vertex v_K with color q. Repeat this procedure for the vertices in color set C_K, and we find that this graph can be colored with $K - 1$ color, which causes a contradiction. ■

TABLE V. Numerical fidelity bound for the 3-qubit GHZ (cluster) state.

3-qubit GHZ (cluster)	s	μ
1 & 2	0.906	–2.4686
3 & 4	0.6036	–2.4145
Mermin [28,52]	$\frac{2+\sqrt{2}}{8}$	$-\frac{1}{\sqrt{2}}$

2. Robust self-testing of graph states

In this section we give a detailed explanation about numerical robustness results of self-testing shown in Fig. 2. One could also refer to Refs. [25,28] for the details of the proof. We would like to lower bound the fidelity between the measured state ρ and the target graph state ψ_G (under local isometry), with the knowledge of the Bell inequality value. To this end, mathematically equivalently, one can adopt a local extraction channel and the maximal fidelity shows

$$F = \max_{\Lambda=\Lambda_1\otimes\Lambda_2\cdots\Lambda_N} \langle \psi_G | \Lambda(\rho) | \psi_G \rangle, \tag{C4}$$

where Λ_i is the local channel on the ith party. Alternatively, the fidelity can be written as follows:

$$\mathrm{Tr}[\rho \Lambda_1^\dagger \otimes \Lambda_2^\dagger \cdots \Lambda_N^\dagger (|\psi_G\rangle\langle\psi_G|)], \tag{C5}$$

where $\Lambda_i^\dagger$ is the dual channel of Λ_i. Note that here the dual of the extraction map acts on the graph state, and we denote the state after this dual channel as $K = \Lambda_1^\dagger \otimes \Lambda_2^\dagger \cdots \Lambda_N^\dagger(|\psi_G\rangle\langle\psi_G|)$.

To find a reliable lower bound of the fidelity from the Bell inequality value, one can choose appropriate parameters s and μ such that the following inequality on operators always holds:

$$K \geqslant s\mathcal{B} + \mu\mathbb{I}, \tag{C6}$$

where $\mathcal{B}$ is the Bell inequality to self-test the state. In this way the fidelity is bounded as $F \geqslant s\beta + \mu$, with $\beta = \mathrm{Tr}(\rho\mathcal{B})$ the Bell inequality value.

Since the measurement of $\mathcal{B}$ is restricted to the dichotomic scenario, on account of the Jordan Lemma, one can reduce the state to the N-qubit space, and the possible measurements can be parameterized by the angles $\theta_i \in [0, \pi/2]$ as

$$\begin{aligned}A_i &= \cos\theta_i X_i + \sin\theta_i Z_i,\\ B_i &= \cos\theta_i X_i - \sin\theta_i Z_i,\end{aligned} \tag{C7}$$

for $i \in T$, the rotated set, and for other qubits

$$\begin{aligned}A_i &= \cos\theta_i H_i + \sin\theta_i V_i,\\ B_i &= \cos\theta_i H_i - \sin\theta_i V_i,\end{aligned} \tag{C8}$$

TABLE VI. Numerical fidelity bound for the 4-qubit GHZ state.

4-qubit GHZ	s	μ
1 & 2	1	$-1 - 2\sqrt{2}$
3	0.69	–3.5931
4	0.49	–3.1578
Mermin	0.219	–0.752

TABLE VII. Numerical fidelity bound for the 4-qubit cluster state.

4-qubit cluster	s	μ
1	1	$-1-2\sqrt{2}$
2	0.7400	–3.9262
3 & 4	0.6200	–2.5071

where $H_i(V_i) = (X_i \pm Z_i)/\sqrt{2}$. Consider a specific extraction channel in Ref. [28],

$$\Lambda_i(\rho) = \frac{1+g(\theta_i)}{2}\rho + \frac{1-g(\theta_i)}{2}\Gamma_i(\theta_i)(\rho)\Gamma_i(\theta_i), \quad \text{(C9)}$$

where $g(\theta_i) = (1+\sqrt{2})(\sin\theta_i + \cos\theta_i + 1)$, and $\Gamma_i(\theta_i)$ is the operator on the ith qubit: for $i \in T$, $\Gamma_i(\theta_i) = X_i(Z_i)$ as $\theta_i < (\geqslant)\pi/4$; for $i \notin T$, $\Gamma_i(\theta_i) = H_i(V_i)$ as $\theta_i < (\geqslant)\pi/4$. Now the Bell inequality $\mathcal{B}$ and the operator K are both parameterized with θ_i, and the inequality in Eq. (C6) shows

$$K(\theta_1, \theta_2, \dots, \theta_N) \geqslant s\mathcal{B}(\theta_1, \theta_2, \dots, \theta_N) + \mu\mathbb{I}, \quad \text{(C10)}$$

where we should find an optimal s and μ for all possible $\theta_1, \theta_2, \dots, \theta_N$. However, in practice we cannot go through all $\vec{\theta}$. Thus, in our numerics we only consider a finite set of $\vec{\theta} =$ with $\theta_i = 2\pi\frac{j}{h}(j = 0, \dots, h)$ and give an approximate lower bound.

TABLE VIII. Numerical fidelity bound for the 5- and 6-qubit graph states.

5-qubit cluster	s	μ
1	1.16	–5.7610
2	0.93	–6.1209
5-qubit GHZ	s	μ
1	1.04	–5.0616
2	0.46	–4.2043
5-qubit $\mathcal{G}_5$	s	μ
1	1.07	–5.2364
2	0.74	–6.0191
6-qubit $\mathcal{G}_6$	s	μ
1	1.3	–7.877
2	0.74	–6.7591

In Figs. 2 and 4, all the robustness results are obtained from the above inequality numerically. To be specific, given a fixed s, we find the minima of the minimal eigenvalue of $K(\vec{\theta}) - s\mathcal{B}(\vec{\theta})$ for all $\vec{\theta}$. A slower slope indicates a better bound. Thus, to find the optimal linear bound, we let the relation $s\beta_Q + \mu = 1$ hold, that is, the fidelity approaches 1 for the maximal quantum value, and find the minimum s. We list all the numerically obtained s and μ in Tables V, VI, VII and VIII.

[1] J. S. Bell, *On the Einstein-Podolsky-Rosen Paradox. Physics 1, 195–200 (1964)*, Speakable and Unspeakable in Quantum Mechanics (Cambridge University Press, Cambridge, England, 1987).

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

[3] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, in *Proceedings of the IEEE 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)* (IEEE, New York, 1998), pp. 503–509.

[4] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (2014).

[5] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14 (ACM Press, New York, 2014), pp. 417–426.

[6] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nat. Commun. **9**, 459 (2018).

[7] R. Colbeck, Ph.D. thesis, Trinity College, University of Cambridge, 2006.

[8] 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, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[9] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quantum Inf. **2**, 16021 (2016).

[10] A. Acín and L. Masanes, Certified randomness in quantum physics, Nature (London) **540**, 213 (2016).

[11] Y. Liu, Z. Qi, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan *et al.*, Device-independent quantum random-number generation, Nature (London) **562**, 548 (2018).

[12] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam *et al.*, Experimentally generated randomness certified by the impossibility of superluminal signals, Nature (London) **556**, 223 (2018).

[13] B. W. Reichardt, F. Unger, and U. Vazirani, Classical command of quantum systems, Nature (London) **496**, 456 (2013).

[14] H.-L. Huang, Q. Zhao, X. Ma, C. Liu, Z.-E. Su, X.-L. Wang, L. Li, N.-L. Liu, B. C. Sanders, C.-Y. Lu, and J.-W. Pan, Experimental Blind Quantum Computing for a Classical Client, Phys. Rev. Lett. **119**, 050503 (2017).

[15] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Device-Independent Entanglement Quantification and Related Applications, Phys. Rev. Lett. **111**, 030501 (2013).

[16] Y.-C. Liang, D. Rosset, J.-D. Bancal, G. Pütz, T. J. Barnea, and N. Gisin, Family of Bell-like Inequalities as Device-Independent Witnesses for Entanglement Depth, Phys. Rev. Lett. **114**, 190401 (2015).

[17] F. Baccari, D. Cavalcanti, P. Wittek, and A. Acín, Efficient Device-Independent Entanglement Detection for Multipartite Systems, Phys. Rev. X **7**, 021042 (2017).

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

[19] K. Vogel and H. Risken, Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase, Phys. Rev. A **40**, 2847 (1989).
[20] M. Paris and J. Rehacek, *Quantum State Estimation*, Lecture Notes in Physics Vol. 649 (Springer, Berlin, 2004).
[21] X. Wu, Y. Cai, T. H. Yang, H. N. Le, J.-D. Bancal, and V. Scarani, Robust self-testing of the three-qubit w state, Phys. Rev. A **90**, 042339 (2014).
[22] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, Device-independent parallel self-testing of two singlets, Phys. Rev. A **93**, 062121 (2016).
[23] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. **8**, 15485 (2017).
[24] A. Salavrakos, R. Augusiak, J. Tura, P. Wittek, A. Acín, and S. Pironio, Bell Inequalities Tailored to Maximally Entangled States, Phys. Rev. Lett. **119**, 040402 (2017).
[25] 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 (2020).
[26] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, Self-testing multipartite entangled states through projections onto two systems, New J. Phys. **20**, 083041 (2018).
[27] C. A. Miller and Y. Shi, Optimal robust self-testing by binary nonlocal XOR games, in *Proceedings of the 8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*, edited by S. Severini and F. Brandao, Leibniz International Proceedings in Informatics (LIPIcs) Vol. 22 (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2013), pp. 254–262.
[28] J. Kaniewski, Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities, Phys. Rev. Lett. **117**, 070402 (2016).
[29] V. Scarani, A. Acín, E. Schenck, and M. Aspelmeyer, Nonlocality of cluster states of qubits, Phys. Rev. A **71**, 042325 (2005).
[30] O. Gühne, G. Tóth, P. Hyllus, and H. J. Briegel, Bell Inequalities for Graph States, Phys. Rev. Lett. **95**, 120405 (2005).
[31] O. Gühne and A. Cabello, Generalized Ardehali-Bell inequalities for graph states, Phys. Rev. A **77**, 032108 (2008).
[32] B. M. Terhal, A family of indecomposable positive linear maps based on entangled quantum states, Linear Algebra Appl. **323**, 61 (2001).
[33] O. Guhne and G. Toth, Entanglement detection, Phys. Rep. **474**, 1 (2009).
[34] N. Friis, G. Vitagliano, M. Malik, and M. Huber, Entanglement certification from theory to experiment, Nat. Rev. Phys. **1**, 72 (2019).
[35] S. Pallister, N. Linden, and A. Montanaro, Optimal Verification of Entangled States with Local Measurements, Phys. Rev. Lett. **120**, 170502 (2018).
[36] H. Zhu and M. Hayashi, Efficient Verification of Pure Quantum States in the Adversarial Scenario, Phys. Rev. Lett. **123**, 260504 (2019).
[37] X.-L. Wang, Y.-H. Luo, H.-L. Huang, M.-C. Chen, Z.-E. Su, C. Liu, C. Chen, W. Li, Y.-Q. Fang, X. Jiang, J. Zhang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, 18-Qubit Entanglement with Six Photons' Three Degrees of Freedom, Phys. Rev. Lett. **120**, 260502 (2018).
[38] N. Friis, O. Marty, C. Maier, C. Hempel, M. Holzäpfel, P. Jurcevic, M. B. Plenio, M. Huber, C. Roos, R. Blatt, and B. Lanyon, Observation of Entangled States of a Fully Controlled 20-Qubit System, Phys. Rev. X **8**, 021012 (2018).
[39] M. Gong, M.-C. Chen, Y. Zheng, S. Wang, C. Zha, H. Deng, Z. Yan, H. Rong, Y. Wu, S. Li, F. Chen, Y. Zhao, F. Liang, J. Lin, Y. Xu, C. Guo, L. Sun, A. D. Castellano, H. Wang, C. Peng *et al.*, Genuine 12-Qubit Entanglement on a Superconducting Quantum Processor, Phys. Rev. Lett. **122**, 110501 (2019).
[40] R. Raussendorf and H. J. Briegel, A One-Way Quantum Computer, Phys. Rev. Lett. **86**, 5188 (2001).
[41] R. Raussendorf, D. E. Browne, and H. J. Briegel, Measurement-based quantum computation on cluster states, Phys. Rev. A **68**, 022312 (2003).
[42] H. J. Kimble, The quantum internet, Nature (London) **453**, 1023 EP (2008).
[43] S. Perseguers, G. J. Lapeyre Jr., D. Cavalcanti, M. Lewenstein, and A. Acín, Distribution of entanglement in large-scale quantum networks, Rep. Prog. Phys. **76**, 096001 (2013).
[44] M. Caleffi, Optimal routing for quantum networks, IEEE Access **5**, 22299 (2017).
[45] G. Tóth and O. Gühne, Detecting Genuine Multipartite Entanglement with Two Local Measurements, Phys. Rev. Lett. **94**, 060501 (2005).
[46] M. Hayashi and T. Morimae, Verifiable Measurement-Only Blind Quantum Computing with Stabilizer Testing, Phys. Rev. Lett. **115**, 220502 (2015).
[47] K. Fujii and M. Hayashi, Verifiable fault tolerance in measurement-based quantum computation, Phys. Rev. A **96**, 030301(R) (2017).
[48] H. Lu, Q. Zhao, Z.-D. Li, X.-F. Yin, X. Yuan, J.-C. Hung, L.-K. Chen, L. Li, N.-L. Liu, C.-Z. Peng, Y.-C. Liang, X. Ma, Y.-A. Chen, and J.-W. Pan, Entanglement Structure: Entanglement Partitioning in Multipartite Systems and Its Experimental Detection Using Optimizable Witnesses, Phys. Rev. X **8**, 021072 (2018).
[49] Y. Zhou, Q. Zhao, X. Yuan, and X. Ma, Detecting multipartite entanglement structure with minimal resources, npj Quantum Inf. **5**, 83 (2019).
[50] Y. Zhou, Entanglement detection under coherent noise: Greenberger-Horne-Zeilinger-like states, Phys. Rev. A **101**, 012301 (2020).
[51] P. Zeng, Y. Zhou, and Z. Liu, Quantum gate verification and its application in property testing, Phys. Rev. Res. **2**, 023306 (2020).
[52] N. D. Mermin, Extreme Quantum Entanglement in a Superposition of Macroscopically Distinct States, Phys. Rev. Lett. **65**, 1838 (1990).
[53] D. Gottesman, Stabilizer codes and quantum error correction, arXiv:quant-ph/9705052.
[54] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, 10th ed. (Cambridge University Press, New York, NY, USA, 2011).
[55] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel, Entanglement in graph states and its applications, in *Proceedings of the International School of Physics "Enrico Fermi"*, edited by G. Casati, D. L. Shepelyansky, P. Zoller, and G. Benenti (IOS Press, 2006), Vol. 162, pp. 115–218.

[56] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).
[57] D. Wu, Q. Zhao, X.-M. Gu, H.-S. Zhong, Y. Zhou, L.-C. Peng, J. Qin, Y.-H. Luo, K. Chen, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Robust Self-Testing of Multiparticle Entanglement, Phys. Rev. Lett. **127**, 230503 (2021).
[58] D. Wu, Q. Zhao, C. Wang, L. Huang, Y.-F. Jiang, B. Bai, Y. Zhou, X.-M. Gu, F.-M. Liu, Y.-Q. Mao, Q.-C. Sun, M.-C. Chen, J. Zhang, C.-Z. Peng, X.-B. Zhu, Q. Zhang, C.-Y. Lu, and J.-W. Pan, Closing the Locality and Detection Loopholes in Multiparticle Entanglement Self-Testing, Phys. Rev. Lett. **128**, 250401 (2022).
[59] Q. Zhao, G. Wang, X. Yuan, and X. Ma, Efficient and robust detection of multipartite Greenberger-Horne-Zeilinger-like states, Phys. Rev. A **99**, 052349 (2019).
[60] M. Rossi, M. Huber, D. BruB, and C. Macchiavello, Quantum hypergraph states, New J. Phys. **15**, 113022 (2013).
[61] T. Kraft, C. Ritz, N. Brunner, M. Huber, and O. Gühne, Characterizing Genuine Multilevel Entanglement, Phys. Rev. Lett. **120**, 060502 (2018).
[62] J. Bavaresco, N. Herrera Valencia, C. KlMei ckl, M. Pivoluska, P. Erker, N. Friis, M. Malik, and M. Huber, Measurements in two bases are sufficient for certifying high-dimensional entanglement, Nat. Phys. **14**, 1032 (2018).
[63] Y. Zhou, C. Guo, and X. Ma, Decomposition of a symmetric multipartite observable, Phys. Rev. A **99**, 052324 (2019).
[64] F. Baccari, R. Augusiak, I. Šupić, and A. Acín, Device-Independent Certification of Genuinely Entangled Subspaces, Phys. Rev. Lett. **125**, 260507 (2020).
[65] J. Kaniewski, A weak form of self-testing, Phys. Rev. Res. **2**, 033420 (2020).
[66] A. Tavakoli, M. Farkas, D. Rosset, J.-D. Bancal, and J. Kaniewski, Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments: Bell inequalities, device-independent certification and applications, Sci. Adv. **7**, eabc3847 (2021).
[67] P.-S. Lin, J.-C. Hung, C.-H. Chen, and Y.-C. Liang, Exploring Bell inequalities for the device-independent certification of multipartite entanglement depth, Phys. Rev. A **99**, 062338 (2019).
[68] C. Bamps and S. Pironio, Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing, Phys. Rev. A **91**, 052111 (2015).
[69] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).