Geometric structure of quantum correlators via semidefinite programming

Le Phuc Thinh,[1,*] Antonios Varvitsiotis,[2,†] and Yu Cai[1,‡]
[1]Centre for Quantum Technologies, National University of Singapore 117543, Singapore
[2]Department of Electrical & Computer Engineering, National University of Singapore 117583, Singapore

(Received 12 October 2018; published 10 May 2019)

Quantum information leverages correlations between spacelike separated parties in order to perform useful tasks such as secure communication and randomness certification. Nevertheless, not much is known about the intricate geometric features of the set quantum correlators. In this paper we study the structure of the set of quantum correlators using semidefinite programming, more precisely the boundary, extreme, and exposed points. We obtain quantum Bell inequalities characterizing a certain class of bipartite scenarios. In the case of two dichotomic measurements, extremal quantum correlators coincide with the correlators that uniquely determine the state and measurement operators, a property known as self-testing. We illustrate the usefulness of our theoretical findings with many examples and extensive computational work.

DOI: 10.1103/PhysRevA.99.052108

I. INTRODUCTION

Quantum theory distinguishes itself from classically conceived theories of physics in several ways, most notably in terms of the observed correlations between spacelike separated parties [1]. The existence of nonlocal quantum correlations predicted by Bell has been confirmed by numerous experiments [2–4], which have influenced deeply our understanding of the physical world, and have led to real-life applications in cryptography [5] and randomness certification [6] among others.

Despite the usefulness of nonlocal quantum distributions, the structure of the set of quantum distributions is not well understood. Most notably, there are many semidefinite programming hierarchies approximating the set of quantum correlations from the exterior, but these hierarchies only converge in the limit, e.g., see [7,8]. In fact, it was shown only recently in [9] that the set of (tensor product) quantum correlations is not closed.

From a practical perspective, to manipulate quantum information, one needs a robust method for identifying quantum systems. This motivates extensive work studying the relationship between objects in the theory, namely quantum states and measurements, and the theory's predictions, namely probabilities of experiments. This line of research is known as quantum tomography whose recent reincarnation is known as self-testing [10] and gate set tomography [11].

Here we study the geometric structure of the set of quantum correlators. As the quantum set is convex, its properties can be understood via various features of its convex geometry, i.e., its facial structure and its extreme points [12]. Such an approach of studying the quantum set within the framework of convex analysis was also employed in [13]. Our approach differs in that we use the rich duality theory of semidefinite programming as our main tool. The relevance of semidefinite programming for the study of quantum correlators was implicit in the work of Tsirelson [14], a connection that was pursued further in [7,8]. It essentially follows from [14] that the geometry of the set of quantum correlators is the projection of the geometry of the elliptope, a convex set of central interest in the field of combinatorial optimization [15].

Connections to semidefinite programming lead to several interesting results.

First, *exact and analytic* description of quantum correlations is extremely rare: the only known instance occurs in the case of two dichotomic measurements for Alice and Bob and is known as the Tsirelson-Landau-Masanes quantum Bell inequalities. We obtain analytic description for a more general scenario where Alice has two dichotomic measurements and Bob has an arbitrary number of dichotomic measurements (Theorem 1).

Second, we refine the above description of the boundary of quantum sets by deriving necessary and sufficient conditions for *extremality* (Theorem 2 and 3), and a sufficient condition for *exposedness* (Theorem 5). These characterizations take the form of semidefinite programming, i.e., efficiently solvable, which greatly facilitates the numerical study of specific quantum correlations.

Third, we show that these stronger geometric properties—extremality and exposedness—are not just theoretical curiosity but have significant impact on applications. Specifically, extremality and self-testing are equivalent in the case of two dichotomic measurements (Theorem 4). This means in particular that experimentalists are now allowed much more freedom in the class of correlations that, once observed, would uniquely determine the underlying quantum system. Further, exposedness of a correlation allows one to conclude the same property, but by using only the maximal quantum violation of a certain Bell inequality.

We start with a brief review of Bell nonlocality (Sec. II), followed by the precise definition of the set of quantum correlators, our main object of study. We then obtain characterization of this set via the positive semidefinite matrix

*cqtlept@nus.edu.sg
†avarvits@gmail.com
‡caiyu01@gmail.com

completion problem (Sec. III), which leads to an analytic description (Sec. IV). Further exploiting this connection, we study the convex geometry of quantum correlators, its extreme points (Sec. V A) and exposed points (Sec. V D), and present a connection between the geometric concept of extremality with the operational task of self-testing (Sec. V C). Algorithmic results and examples are interspersed in these sections whenever convenient. We conclude the paper with a high level overview of our results and pointers towards future research.

II. BELL NONLOCALITY

Bell experiment. The experimental and mathematical framework for studying behaviors between two spacelike separated parties is known as a bipartite Bell experiment. In this setting two parties, called Alice and Bob, perform independently and simultaneously local measurements on their corresponding subsystems and record the resulting outcomes. In this work, we restrict to Bell experiments where the parties can only perform *dichotomic* (i.e., two-outcome) measurements.

The event that the first party performed measurement x and got outcome a, whereas the second party performed measurement y and got outcome b is denoted by $(a, b|x, y)$. The next step is to consider physical theories that assign probabilities $p(a, b|x, y)$ to all possible events of a Bell experiment. The collection of all joint conditional probabilities $p(a, b|x, y)$ is called a *full behavior*.

Clearly, for any physical theory, behaviors satisfy nonnegativity and normalization conditions, i.e.,

$$p(a, b|x, y) \geqslant 0, \quad \forall a, b, x, y,$$
$$\sum_{a,b} p(a, b|x, y) = 1, \quad \forall x, y.$$

Furthermore, for reasonable physical theory, the behaviors that can be generated between spacelike separated parties have the property that each party's local marginal distribution does not depend on the other party's choice of measurement, i.e.,

$$\begin{aligned} \sum_b p(a, b|x, y) &= \sum_b p(a, b|x, y'), \quad \forall a, x, y \neq y', \\ \sum_a p(a, b|x, y) &= \sum_a p(a, b|x', y), \quad \forall b, y, x \neq x'. \end{aligned} \tag{1}$$

A full behavior that satisfies all the linear constraints given in (1) is called *no signaling*. Given a no-signaling behavior, we denote by $p_A(a|x)$ and $p_B(b|y)$ the local marginal distributions of Alice and Bob, respectively.

As we only consider dichotomic measurements, we can use an equivalent parametrization of a no-signaling behavior $p(a, b|x, y)$ in terms of average values. Explicitly, for outcome labels $a, b \in \{\pm 1\}$ we use the affine bijection

$$p(a, b|x, y) \mapsto (c_x, c_y, c_{xy}), \tag{2}$$

where

$$c_x = \sum_{a\in\{\pm1\}} a\, p_A(a|x), \quad c_y = \sum_{b\in\{\pm1\}} b\, p_B(b|y),$$
$$c_{xy} = \sum_{a,b\in\{\pm1\}} ab\, p(a, b|x, y).$$

The image of the set of full behaviors under the map (2) is called the set of *full correlators*, and its elements are denoted by (c_x, c_y, c_{xy}). Lastly, the coordinate projection of the set of full correlators on the coordinates c_{xy} is the *correlator space* and its elements are called *correlators*.

Local behaviors and correlators. A behavior $p(a, b|x, y)$ is called local deterministic if $p(a, b|x, y) = \delta_{a,f(x)}\delta_{b,g(y)}$, where δ is the Kronecker delta function and f, g are functions from the input set to the output set. Furthermore, a behavior $p(a, b|x, y)$ is called *local* if it can be written as a convex combination of local deterministic behaviors, i.e., $p(a, b|x, y) = \sum_i \mu_i p_i$, where $\mu \geqslant 0$, $\sum_i \mu_i = 1$, and each p_i is local deterministic.

Fixing outcome labels $a, b \in \{\pm 1\}$, the corresponding set of correlators is the convex hull of all $n \times m$ matrices $xy^\top$, where $x \in \{+1, -1\}^{n\times 1}$ and $y \in \{+1, -1\}^{m\times 1}$. This is known as the *cut polytope* of the complete bipartite graph $K_{n,m}$ (in ± 1 variables) and is of central importance in the field of combinatorial optimization [15].

Quantum behaviors and correlators. According to the (Hilbert space) axioms of quantum mechanics, a full behavior $p(a, b|x, y)$ is quantum, if there exist ρ, a quantum state acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and $\{M_a^x\}$ and $\{M_b^y\}$, local measurements acting on $\mathcal{H}_A$ and $\mathcal{H}_B$, i.e.,

$$\rho \succeq 0, \quad \mathrm{tr}(\rho) = 1,$$
$$M_a^x \succeq 0, \quad \sum_a M_a^x = 1,$$
$$M_b^y \succeq 0, \quad \sum_b M_b^y = 1,$$

such that $p(a, b|x, y) = \mathrm{tr}(M_a^x \otimes M_b^y \rho)$. Equivalently, a full correlator (c_x, c_y, c_{xy}) is quantum, if there exists a quantum state ρ acting on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and ± 1 observables $A_1, \ldots, A_n$, $B_1, \ldots, B_m$ acting on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, such that

$$\begin{aligned} c_x &= \mathrm{tr}((A_x \otimes I)\rho), \quad x \in [n], \\ c_y &= \mathrm{tr}((I \otimes B_y)\rho), \quad y \in [m], \\ c_{xy} &= \mathrm{tr}(\rho A_x \otimes B_y), \quad x \in [n], y \in [m]. \end{aligned} \tag{3}$$

The set of quantum correlators, denoted by $\mathrm{Cor}(n, m)$, is the set of all vectors c_{xy}, where $c_{xy} = \mathrm{tr}(\rho A_x \otimes B_y)$ for a quantum state ρ and ± 1 observables $A_1, \ldots, A_n$, $B_1, \ldots, B_m$. It is evident that the difference with full correlators lies in the lack of local marginals a_x, b_y. Note that the set of quantum correlators is a compact and convex subset of the cube $[-1, 1]^{nm}$. Throughout this work, we arrange the entries of a quantum correlator $c_{xy} \in \mathrm{Cor}(n, m)$ as an $n \times m$ matrix C, which we call a quantum correlation matrix. We use the vector and matrix representations interchangeably.

III. LINK TO SEMIDEFINITE PROGRAMMING

A semidefinite program (SDP) is a mathematical optimization problem, where the objective is to optimize a linear function over an affine slice of the cone of positive semidefinite matrices. A SDP in primal canonical form is given by

$$p^* = \sup_X \{\langle C, X\rangle : X \succeq 0,\ \langle A_i, X\rangle = b_i\ (i \in [\ell])\}, \tag{P}$$

where $\langle\cdot,\cdot\rangle$ denotes the trace inner product of matrices and the generalized inequality $X \succeq 0$ means that the matrix X is positive semidefinite, i.e., it has non-negative eigenvalues. SDPs are an important generalization of linear programming, which is obtained as a special case when all involved matrices are diagonal. SDPs have significant modeling power, powerful duality theory, and efficient algorithms for solving them.

The link between quantum correlators and SDPs originates in the seminal work of Tsirelson [14, Theorem 2.1] and later also in [8,16,17]. Specifically, Tsirelson showed that a matrix $C = (c_{xy}) \in [-1, 1]^{n\times m}$ is a quantum correlation matrix if and only if there exists a collection of real unit vectors $u_1, \dots, u_n, v_1, \dots, v_m$ such that

$$c_{xy} = \langle u_x, v_y\rangle, \quad \text{for all } x \in [n], y \in [m]. \tag{4}$$

We note that $\langle\cdot,\cdot\rangle$ denotes the canonical inner product of vectors. As a consequence of Tsirelson's theorem it follows that $C = (c_{xy}) \in [-1, 1]^{n\times m}$ is a quantum correlation matrix if and only if the following SDP is feasible:

$$\begin{aligned} \max_X \quad & 0, \\ \text{such that} \quad & X_{x,n+y} = c_{xy}, \ x \in [n], y \in [m], \\ & X_{ii} = 1, \ i \in [n+m], \\ & X \in \mathcal{S}^{n+m}_+. \end{aligned} \tag{5}$$

To establish this equivalence note that if $c_{xy} = \langle u_x, v_y\rangle, \forall x \in [n], y \in [m]$, where $\|u_x\| = \|v_y\| = 1$, the Gram matrix $\text{Gram}(u_1, \dots, u_n, v_1, \dots, v_m)$ is feasible for (5). Conversely, if $X \in \mathcal{S}^{n+m}_+$ is feasible for (5), by the spectral theorem for real symmetric matrices, there exist unit vectors $u_1, \dots, u_n, v_1, \dots, v_m$ such that $X = \text{Gram}(u_1, \dots, u_n, v_1, \dots, v_m)$. Clearly, this implies that $c_{xy} = \langle u_x, v_y\rangle, \ \forall x \in [n], y \in [m]$, and thus $C = (c_{xy})$ is a quantum correlation matrix.

Furthermore, a geometric interpretation of Tsirelson's theorem is that the set of $n \times m$ quantum correlation matrices $\text{Cor}(n, m)$ is the image of the set of $(n+m) \times (n+m)$ positive semidefinite matrices with diagonal entries equal to one, denoted by $\mathcal{E}_{n+m}$, under the projection

$$\Pi : \mathcal{S}^{n+m} \to \mathbb{R}^{n\times m}, \quad \begin{pmatrix} A & C \\ C^\top & B \end{pmatrix} \mapsto C, \tag{6}$$

i.e., we have that $\text{Cor}(n, m) = \Pi(\mathcal{E}_{n+m})$.

Any matrix in $\Pi^{-1}(C) \cap \mathcal{E}_{n+m}$ is called a *PSD completion* of C. Thus checking whether a matrix $C = (c_{xy}) \in [-1, 1]^{n\times m}$ is a quantum correlation matrix reduces to checking that the partially specified matrix $\begin{pmatrix} ? & C \\ C^\top & ? \end{pmatrix}$ can be completed to a full PSD matrix with diagonal entries equal to one. For example, the CHSH correlator $C = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is quantum, as the corresponding partial matrix

$$\left(\begin{array}{cc|cc} 1 & ? & 1/\sqrt{2} & 1/\sqrt{2} \\ ? & 1 & 1/\sqrt{2} & -1/\sqrt{2} \\ \hline 1/\sqrt{2} & 1/\sqrt{2} & 1 & ? \\ 1/\sqrt{2} & -1/\sqrt{2} & ? & 1 \end{array}\right) \tag{7}$$

admits a PSD completion, obtained by setting all the unspecified entries to zero.

The problem of completing a partially specified matrix into a full PSD matrix is an important instance of semidefinite programming, referred to as the *PSD matrix completion problem*; e.g., see [18] and references therein.

One of the most fruitful approaches for studying the PSD matrix completion problem has been the use of graph theory. Specifically, let $G = ([n], E)$ be a simple undirected graph, whose edges encode the positions of the known entries of the matrix. The *elliptope or coordinate shadow of a graph* G, denoted by $\mathcal{E}(G)$, is defined as the image of $\mathcal{E}_n$ under the coordinate projection

$$\Pi_G : \mathcal{S}^n \to \mathbb{R}^E, \quad A \mapsto (A_{ij})_{ij\in E}. \tag{8}$$

In other words, any vector $a \in \mathcal{E}(G) \subseteq \mathbb{R}^E$ corresponds to a G-partial matrix that admits a completion to a full PSD matrix with diagonal entries equal to one.

The properties and structure of the elliptope of a graph have been studied extensively; e.g., see [15,19–21]. By the definition of the elliptope of a graph, it is clear that

$$\text{Cor}(n, m) = \mathcal{E}(K_{n,m}),$$

where $K_{n,m}$ denotes the complete bipartite graph, where the bipartitions have n and m vertices, respectively. This link allows us to utilize properties concerning the structure of the elliptope of a graph $\mathcal{E}(G)$ in our study of the structure of the set of quantum correlators.

IV. ANALYTIC DESCRIPTION OF Cor(n, m)

A first property of $\mathcal{E}(G)$ of relevance to this work is that the elliptope of a graph $G = ([n], E)$ is a subset of a nonlinear transform of the *metric polytope*, denoted by $\text{Met}(G)$, which consists of all vectors $x = (x_e) \in \mathbb{R}^E$ satisfying

$$0 \leqslant x_e \leqslant 1, \quad \text{for all } e \in E, \tag{9}$$

$$\sum_{e\in F} x_e - \sum_{e\in C\setminus F} x_e \leqslant |F| - 1, \tag{10}$$

where C is any cycle in G and F is any odd cardinality subset of C. Recall that a cycle in a graph is a sequence of vertices starting and ending at the same vertex, where each two consecutive vertices in the sequence are adjacent to each other. We refer to the inequalities of type (9) and (10) as *box inequalities* and *cycle inequalities*, respectively.

The relation between $\mathcal{E}(G)$ and $\text{Met}(G)$ is completely understood; e.g., see [22, Theorem 4.7]. Specifically, it is known that, for any graph G, we have the inclusion $\mathcal{E}(G) \subseteq \cos(\pi(\text{Met}(G)))$. Furthermore, equality holds if and only if the graph G does not have the complete graph on four vertices, denoted by K_4, as a minor.

Two observations concerning this result are in order. First, note that the cosine function is applied componentwise, i.e., for a vector $x = (x_e) \in \mathbb{R}^E$ we define $\cos(x) \in \mathbb{R}^E$, where $\cos(x)_e = \cos x_e$. Second, a graph H is called a minor of a graph G, if H can be obtained from G through a series of edge deletions, edge contractions, and isolated node deletions.

Based on this and the fact that $\text{Cor}(n, m) = \mathcal{E}(K_{n,m})$, we now derive an analytic description for $\text{Cor}(n, m)$, whenever $\min\{n, m\} \leqslant 2$. Indeed, it is easy to check that the complete bipartite graph $K_{n,m}$ has the complete graph on four vertices K_4 as minor if and only if $\min\{n, m\} > 2$. Thus it follows that $\mathrm{Cor}(n, m) = \cos \pi(\mathrm{Met}(K_{n,m}))$ whenever $\min\{n, m\} \leqslant 2$. This gives the following.

Theorem 1. For $\min\{n, m\} \leqslant 2$, we have that $C = (c_{xy}) \in \mathrm{Cor}(n, m)$ if and only if the following linear system is feasible:

$$\begin{aligned} &0 \leqslant \theta_{xy} \leqslant \pi, \quad \forall x, y, \\ &0 \leqslant \theta_{1j} + \theta_{2i} + \theta_{2j} - \theta_{1i} \leqslant 2\pi, \\ &0 \leqslant \theta_{1i} + \theta_{2i} + \theta_{2j} - \theta_{1j} \leqslant 2\pi, \\ &0 \leqslant \theta_{1i} + \theta_{1j} + \theta_{2j} - \theta_{2i} \leqslant 2\pi, \\ &0 \leqslant \theta_{1i} + \theta_{1j} + \theta_{2i} - \theta_{2j} \leqslant 2\pi, \end{aligned} \tag{11}$$

where $3 \leqslant i < j \leqslant n + 2$ and $\theta_{xy} = \arccos(c_{xy})$.

As an example, in the case of $\mathrm{Cor}(2, 2)$, the resulting characterization is known as the Tsirelson-Landau-Masanes criterion, which has been rediscovered numerous times; e.g., see Refs. [14,16,23]. The description for $\mathrm{Cor}(2, n)$ when $n \geqslant 3$ is obtained here. The detailed argument leading to Theorem 1 is given in Appendix B.

The deceptively simple form of the inequalities in Theorem 1 may lead us to conjecture that the pairwise angle parametrization will be able to linearize the description of the set of quantum correlations. However, our preliminary investigation into scenario $\mathrm{Cor}(3, 3)$ showed otherwise: nonlinearity exists even in the pairwise angle parametrization (i.e., after taking the componentwise arccosine mapping). Hence an elegant parametrization for quantum correlators in general remains an open problem.

V. EXTREMAL AND EXPOSED CORRELATORS

In this section we use that $\mathrm{Cor}(n, m)$ is a projection of the elliptope $\mathcal{E}_{n+m}$, to study the convex geometry of $\mathrm{Cor}(n, m)$. We begin with its extreme points (or zero-dimensional faces) and continue with its exposed points.

A. Extremal correlators

A matrix $C \in \mathrm{Cor}(n, m)$ is an extreme point of $\mathrm{Cor}(n, m)$ if the equality $C = \lambda C_1 + (1 - \lambda)C_2$, where $\lambda \in (0, 1)$ and $C_1, C_2 \in \mathrm{Cor}(n, m)$, implies $C = C_1 = C_2$.

The set of extreme points of $\mathrm{Cor}(n, m)$, denoted by $\mathrm{ext}(\mathrm{Cor}(n, m))$, is important for the following reasons. First, since the set of quantum correlators is compact (i.e., closed and bounded) and convex, by the Krein-Milman theorem (e.g., see [24, Theorem 3.3]), $\mathrm{Cor}(n, m)$ is equal to the convex hull of its extreme points.

Secondly, Tsirelson showed that any quantum realization of an extremal correlator in $\mathrm{Cor}(n, m)$ corresponds to a complex representation of an appropriate Clifford algebra [14, Theorem 3.1]. As a consequence, depending on the parity of the rank of an extremal correlator C, it either has one or two "nonequivalent" (up to arbitrary unitaries) quantum representations. In modern language, Tsirelson's work specialized to the case of even-rank extremal correlators is a self-testing statement and a connection we pursue further Sec. V C.

In this section we derive an exact characterization for extremality in $\mathrm{Cor}(n, m)$, in terms of the PSD matrix completion problem. This fact essentially follows from the work of Tsirelson [14,25], and was also recently noted in [26, Theorem 3.3]. The main tool in the proof is a set of necessary conditions for extremality derived by Tsirelson, which we have collected in Theorem 8 in the Appendix.

Theorem 2. A correlator $C \in \mathrm{Cor}(n, m)$ is extremal if and only if C has a unique PSD completion $\hat{C} \in \mathcal{E}_{n+m}$, and furthermore,

$$\mathrm{rank}(\hat{C} \circ \hat{C}) = \binom{\mathrm{rank}(\hat{C}) + 1}{2}, \tag{12}$$

where $\circ$ denotes the Hadamard (componentwise) product of matrices.

Proof. The forward implication is a consequence of Theorem 8 (iii), combined with the following characterization of extreme points of the elliptope [27]:

$$E \in \mathrm{ext}(\mathcal{E}_n) \iff \mathrm{rank}(E \circ E) = \binom{\mathrm{rank}(E) + 1}{2}. \tag{13}$$

For the converse direction, by assumption we have that $\Pi^{-1}(C) \cap \mathcal{E}_{n+m} = \{\hat{C}\}$, where the map Π was defined in (6). Furthermore, the rank assumption on $\hat{C}$ combined with (13) implies that $\hat{C} \in \mathrm{ext}(\mathcal{E}_{n+m})$. Since $C \in \mathrm{ext}(\mathrm{Cor}(n, m))$ if and only if $\Pi^{-1}(C)$ is a face of $\mathcal{E}_{n+m}$, e.g., see [28, Lemma 2.4], we conclude that $C \in \mathrm{ext}(\mathrm{Cor}(n, m))$ as an extreme point is a face. ■

Illustrating the usefulness of Theorem 2, we now show the extremality of various quantum correlation matrices.

The only other technique available in the literature for showing extremality of a quantum correlator is via the notion of self-testing. Specifically, it was shown in [13, Proposition C.1] that a full correlator (c_x, c_y, c_{xy}), which is a self-test, is also necessarily an extreme point of the set of *full* correlators. It is easy to verify that this argument remains valid for correlators, i.e., if $C \in \mathrm{Cor}(n, m)$ is a self-test, it is also an extreme point of $\mathrm{Cor}(n, m)$.

Example 1. The CHSH correlator $C = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is well known to be a self-test (e.g., see [29, Theorem 4.1]), and thus it is an extreme point of $\mathrm{Cor}(2, 2)$. To recover this by Theorem 2, we first show that the matrix

$$\begin{pmatrix} 1 & a & 1/\sqrt{2} & 1/\sqrt{2} \\ a & 1 & 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} & 1 & b \\ 1/\sqrt{2} & -1/\sqrt{2} & b & 1 \end{pmatrix} \tag{14}$$

admits a unique PSD completion. Indeed, consider an arbitrary completion and let x_1, x_2, y_1, y_2 be the vectors in a Gram decomposition. Define

$$z_+ = \frac{x_1 + x_2}{\sqrt{2}}, \quad z_- = \frac{x_1 - x_2}{\sqrt{2}}.$$

Then clearly $\langle z_+, z_- \rangle = 0$. Furthermore, $\langle y_1, z_+ \rangle = 1$ and $\langle y_1, z_- \rangle = 0$. Since $\|y_1\| = 1$ it follows that

$$y_1 = \frac{z_+}{\|z_+\|}, \quad y_2 = \frac{z_-}{\|z_-\|}.$$

This implies that $b = \langle y_1, y_2\rangle = 0$. Similarly, we get that $a = 0$. Thus the unique PSD completion is

$$\hat{C} = \begin{pmatrix} 1 & 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1 & 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} & 1 & 0 \\ 1/\sqrt{2} & -1/\sqrt{2} & 0 & 1 \end{pmatrix}. \tag{15}$$

Lastly, as $\text{rank}(\hat{C}) = 2$ and $\text{rank}(\hat{C} \circ \hat{C}) = 3$, it follows by Theorem 2 that $C \in \text{ext}(\text{Cor}(2, 2))$.

Example 2. The Mayers-Yao correlator [10]

$$C = \begin{pmatrix} 1 & 0 & 1/\sqrt{2} \\ 0 & 1 & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} & 1 \end{pmatrix} \tag{16}$$

is a self-test (e.g., see [29, Theorem 4.2]), and thus it is an extreme point of Cor(3, 3). To recover this by Theorem 2 we first check that the corresponding matrix

$$\begin{pmatrix} 1 & a & b & 1 & 0 & 1/\sqrt{2} \\ a & 1 & c & 0 & 1 & 1/\sqrt{2} \\ b & c & 1 & 1/\sqrt{2} & 1/\sqrt{2} & 1 \\ 1 & 0 & 1/\sqrt{2} & 1 & d & e \\ 0 & 1 & 1/\sqrt{2} & d & 1 & f \\ 1/\sqrt{2} & 1/\sqrt{2} & 1 & e & f & 1 \end{pmatrix} \tag{17}$$

admits a unique PSD completion. To see this, consider an arbitrary PSD completion and let $x_1, x_2, x_3, y_1, y_2, y_3$ be a Gram decomposition. Since $\|x_1\| = \|y_1\| = 1$ and $\langle x_1, y_1\rangle = 1$, we have that $x_1 = y_1$. Similarly, we get that $x_2 = y_2$. These two conditions imply that

$$\begin{aligned} a &= \langle x_1, x_2\rangle = \langle x_1, y_2\rangle = 0, \\ b &= \langle x_1, x_3\rangle = \langle y_1, x_3\rangle = 1/\sqrt{2}, \\ c &= \langle x_2, x_3\rangle = \langle y_2, x_3\rangle = 1/\sqrt{2}, \\ d &= \langle y_1, y_2\rangle = \langle x_1, x_2\rangle = 0, \\ e &= \langle y_1, y_3\rangle = \langle x_1, x_3\rangle = 1/\sqrt{2}, \\ f &= \langle y_2, y_3\rangle = \langle x_2, x_3\rangle = 1/\sqrt{2}. \end{aligned} \tag{18}$$

Summarizing, the unique PSD completion of C is

$$\hat{C} = \begin{pmatrix} 1 & 0 & 1/\sqrt{2} & 1 & 0 & 1/\sqrt{2} \\ 0 & 1 & 1/\sqrt{2} & 0 & 1 & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} & 1 & 1/\sqrt{2} & 1/\sqrt{2} & 1 \\ 1 & 0 & 1/\sqrt{2} & 1 & 0 & 1/\sqrt{2} \\ 0 & 1 & 1/\sqrt{2} & 0 & 1 & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} & 1 & 1/\sqrt{2} & 1/\sqrt{2} & 1 \end{pmatrix}. \tag{19}$$

Lastly, since $\text{rank}(\hat{C}) = 2$ and $\text{rank}(\hat{C} \circ \hat{C}) = 3$ it follows by Theorem 2 that $C \in \text{ext}(\text{Cor}(2, 3))$.

Example 3. The quantum correlator

$$C = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -2 \end{pmatrix}$$

is a self-test [30] and thus an extreme point of Cor(2, 2). It can be easily checked that the corresponding partial matrix has a unique PSD completion given by

$$\hat{C} = \begin{pmatrix} 1 & -1/2 & 1/2 & 1/2 \\ -1/2 & 1 & 1/2 & -1 \\ 1/2 & 1/2 & 1 & -1/2 \\ 1/2 & -1 & -1/2 & 1 \end{pmatrix}.$$

As $\text{rank}(\hat{C}) = 2$ and $\text{rank}(\hat{C} \circ \hat{C}) = 3$, it follows that $C \in \text{ext}(\text{Cor}(2, 2))$.

Extreme points of Cor(2, 2). In this section we give an explicit characterization of the extreme points of Cor(2, 2), in terms of the angle parametrization from Theorem 1.

Theorem 3. For $C = (c_{xy}) \in \text{Cor}(2, 2)$ let $\theta_{xy} = \arccos(c_{xy}) \in [0, \pi]$ for all $x, y \in \{1, 2\}$.

(i) If $\text{rank}(C) = 1$, then C is extreme iff it is local deterministic, i.e., $C = uv^\top$, for $u, v \in \{+1, -1\}^2$.

(ii) If $\text{rank}(C) = 2$, then C is extreme iff it saturates exactly one of the inequalities

$$0 \leqslant \sum_{xy \neq x'y'} \theta_{xy} - \theta_{x'y'} \leqslant 2\pi$$

and at most one of the inequalities

$$0 \leqslant \theta_{xy} \leqslant \pi,$$

where $x, x', y, y' \in \{1, 2\}$.

The case $\text{rank}(C) = 1$ is straightforward so we mainly focus on the case $\text{rank}(C) = 2$. To prove extremality, we use the assumptions of the theorem to prove the existence of a unique completion that satisfies (12). Extremality then follows by Theorem 2.

For the converse direction, we translate the assumption of extremality, namely unique completability and the rank condition (12) to the level of the angle parameters θ_{xy}. As it turns out, these assumptions imply that the unspecified entries are uniquely determined in any completion. In turn, this shows that one cycle inequality and at most one box inequality are tight. The details are given in Appendix D.

B. Verifying extremality computationally

The examples given in the previous section illustrate the usefulness of the characterization of extremality given in Theorem 2. Nevertheless, it is not clear whether Theorem 2 leads to an algorithm for testing extremality, as *a priori* it is not immediately obvious how to systematically check whether the corresponding completion problem has a unique solution. We address this issue using the rich duality theory enjoyed by SDPs, summarized in Theorems 6 and 7 in Appendix A.

Back to the completion problem, given $C = (c_{xy}) \in \text{Cor}(n, m)$, its PSD completions coincide with the set of solutions of the SDP feasibility problem (5).

Next, we dualize the SDP (5). For this, we first write (5) in primal canonical form [recall (P)], i.e.,

$$\begin{aligned} \max_X \quad & 0 \\ \text{such that} \quad & \langle E_{x,n+y}, X\rangle = c_{xy},\ x \in [n], y \in [m], \\ & \langle E_{ii}, X\rangle = 1,\ i \in [n+m], \\ & X \in \mathcal{S}_+^{n+m}, \end{aligned} \tag{20}$$

where $E_{ij} = \frac{1}{2}(e_i e_j^\top + e_j e_i^\top)$ is the symmetric matrix with entry 1 at row i and column j and nonzero elsewhere, scaled by a factor of half.

The dual of the SDP (20) is given by

$$\inf_{\lambda, Z} \sum_{i=1}^{n+m} \lambda_i + \sum_{x=1}^{n} \sum_{y=1}^{m} \lambda_{xy} c_{xy}$$

$$\text{such that} \sum_{i=1}^{n+m} \lambda_i E_{ii} + \sum_{x=1}^{n} \sum_{y=1}^{m} \lambda_{xy} E_{x,n+y} = Z \in \mathcal{S}_+^{n+m}. \quad (21)$$

Note that the SDP (21) admits a positive definite feasible solution, e.g., obtained by setting $\lambda_{xy} = 0,\ \forall x, y$ and taking λ_i to be sufficiently large.

Furthermore, by weak duality for SDPs [cf. Theorem 6 (i)], we have that $0 = p^* \leqslant d^*$, i.e., $d^* > -\infty$. By strong duality for SDPs [cf. Theorem 6 (iv)], these two properties imply that the value of the dual SDP (21) is equal to zero, i.e., $d^* = 0$. Furthermore, $d^* = 0$ is clearly attained, e.g., take $\lambda_i = \lambda_{xy} = 0$. Lastly, as $C \in \text{Cor}(n, m)$ by assumption, the primal SDP (5) is also attained. Thus, to show that the SDP (5) has a unique solution, it suffices to exhibit a nondegenerate optimal solution for (21).

Specializing the definition of dual nondegeneracy for SDPs [see (A2) in Appendix A] to a dual feasible solution (λ, Z) for the SDP (21), this is equivalent to asking that $M = 0$ is the only solution of the system:

$$\begin{aligned} MZ &= 0, \\ M_{ii} &= 0, \quad 1 \leqslant i \leqslant m+n, \\ M_{ij} &= 0, \quad 1 \leqslant i \leqslant n,\ n+1 \leqslant j \leqslant n+m. \end{aligned} \quad (22)$$

An important observation is that (22) is a linear program in the entries of the symmetric matrix variable $M \in \mathcal{S}^{n+m}$, and thus it is efficiently solvable.

We are now ready to describe an algorithmic procedure for determining extremality of a given $C \in \text{Cor}(n, m)$, based on Theorem 2 and the notion of SDP nondegeneracy. For the convenience of the reader, the algorithm is summarized in a flow chart in Fig. 1.

Step 1. We solve the pair of primal-dual SDPs (20) and (21), to get X_{opt} and Z_{opt}, respectively.

Step 2. We check whether Z_{opt} is dual nondegenerate, i.e., we check whether $M = 0$ is the only solution to the linear programming problem (22) (where $Z = Z_{\text{opt}}$.)

Step 3a. If Z_{opt} is nondegenerate, then X_{opt} is the unique solution of the primal SDP (20) by Theorem 7. Lastly, we check whether

$$\text{rank}(X_{\text{opt}} \circ X_{\text{opt}}) = \binom{\text{rank}(X_{\text{opt}}) + 1}{2}.$$

If this holds then C is extreme, and if it fails, C is not extreme.

Step 3b. If Z_{opt} is degenerate and

$$\text{rank}(X_{\text{opt}}) + \text{rank}(Z_{\text{opt}}) = m + n, \quad (23)$$

we conclude that C is *not extreme*. Indeed, if C was extreme, by Theorem 2, X_{opt} would be the unique solution of the SDP (20). As $X_{\text{opt}}, Z_{\text{opt}}$ satisfy (23), by Theorem 7 (ii) the matrix Z_{opt} would be dual nondegenerate optimal solution, a contradiction.

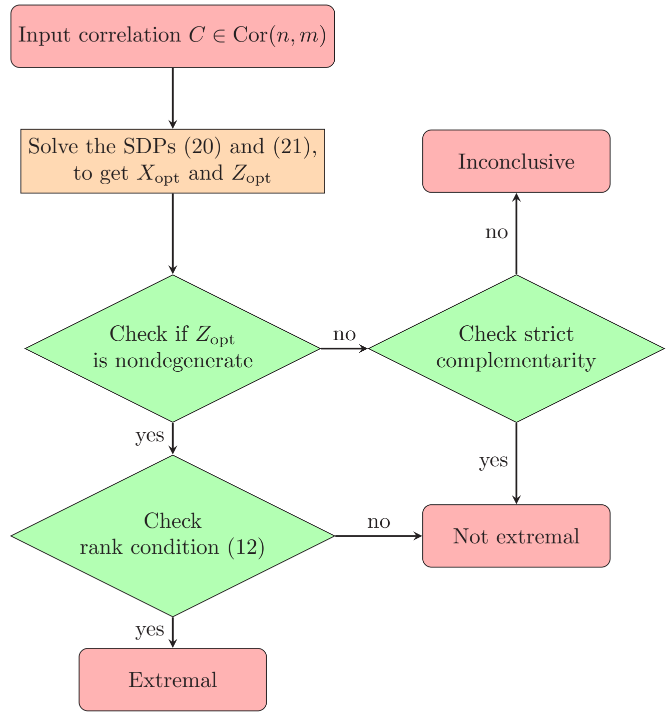

FIG. 1. Flow chart describing the algorithmic procedure for determining extremality in $\text{Cor}(n, m)$.

Step 3c. If Z_{opt} is degenerate and

$$\text{rank}(X_{\text{opt}}) + \text{rank}(Z_{\text{opt}}) < m + n, \quad (24)$$

our procedure is inconclusive.

Note that by weak duality for SDPs, we always have that $\text{rank}(X_{\text{opt}}) + \text{rank}(Z_{\text{opt}}) \leqslant m + n$. Thus condition (23) fails if and only if condition (24) holds.

We implemented this procedure on MATLAB® using the YALMIP package and Mosek as in [31]. Furthermore, we tested the performance of the procedure on randomly generated extremal points of Cor(2, 2). Specifically, with `randExtremeCorr22.m`, we generate a random point in extCor(2, 2) by randomly picking three angles, $\theta_1, \theta_2, \theta_3 \in (0, \pi)$, and setting $\phi = \theta_1 + \theta_2 + \theta_3$. If $\phi < \pi$ or $2\pi < \phi < 3\pi$, we set the fourth angle $\theta_4 = \phi$; otherwise, we discard this instance. Then, by Theorem 3, the corresponding correlator is extremal in Cor(2, 2). We applied our procedure, called `extremeCorr.m`, on 1000 extremal points generated by `randExtremeCorr22.m`. In all instances, our algorithm correctly detected that the generated points are indeed extreme.

C. Operational interpretation of extremality

It turns out that the geometric concept of extremality has a nice operational interpretation. We now explain the connection with the task of self-testing, which has been mentioned several times in the previous sections.

Self-testing, also referred to as device-independent characterization of the state and the measurements, or simply blind tomography, captures the idea that certain correlations between spacelike separated parties predicted by quantum theory determine the state and the measurement up to local isometries and other irrelevant degrees of freedom.

The term self-testing was introduced in the work by Mayers and Yao [10]. Nevertheless, the idea underlying self-testing was discovered earlier numerous times in the literature, for example, in the works of Tsirelson [14], Summers-Werner [32], and Popescu-Rohrlich [33]. The interested reader is referred to [29] for a general survey and [34,35] for more recent developments.

Self-testing can be formalized using the notion of *(pure) quantum realization* of a quantum correlator C. By this we mean an ensemble $(\mathcal{H}_A, \mathcal{H}_B, \psi, \{A_x\}_x, \{B_y\}_y)$ such that $c_{xy} = \psi^\dagger(A_x \otimes B_y)\psi$ for all $x \in [n], y \in [m]$, where ψ is a unit vector in $\mathcal{H}_A \otimes \mathcal{H}_B$, and the Hermitian operators A_x on $\mathcal{H}_A$, B_y on $\mathcal{H}_B$ all have eigenvalues in $[-1, 1]$.

Each quantum realization induces an entire orbit of realizations, obtained by applying local isometries. Concretely, given two isometries (i.e., $V^\dagger V = 1_{\mathcal{H}}$)

$$V_A : \mathcal{H}_A \to \mathcal{H}_{A'}, \quad V_B : \mathcal{H}_B \to \mathcal{H}_{B'},$$

then the ensemble

$$(\mathcal{H}_{A'}, \mathcal{H}_{B'}, (V_A \otimes V_B)\psi, \{V_A A_x V_A^\dagger\}_x, \{V_B B_y V_B^\dagger\}_y) \tag{25}$$

is another quantum realization of C. This subsumes adding subsystems because tensoring is an isometry.

We say that the correlation C self-tests the ensemble $(\mathcal{H}_A, \mathcal{H}_B, \psi, \{A_x\}_x, \{B_y\}_y)$ iff all other quantum realizations of C are of the form (25), i.e., for any other quantum realization $(\mathcal{H}_{A'}, \mathcal{H}_{B'}, \psi, \{A'_x\}_x, \{B'_y\}_y)$ there exist isometries $V_A : \mathcal{H}_A \otimes \mathcal{H}_{A''} \to \mathcal{H}_{A'}$ and $V_B : \mathcal{H}_B \otimes \mathcal{H}_{B''} \to \mathcal{H}_{B'}$ and a unit vector $\psi'' \in \mathcal{H}_{A''} \otimes \mathcal{H}_{B''}$, such that

$$\begin{aligned} \psi' &= (V_A \otimes V_B)(\psi \otimes \psi''), \\ A'_x &= V_A\big(A_x \otimes 1_{\mathcal{H}_{A''}}\big)V_A^\dagger, \\ B'_y &= V_B\big(B_y \otimes 1_{\mathcal{H}_{B''}}\big)V_B^\dagger. \end{aligned} \tag{26}$$

Furthermore, we say that C is a self-test if it self-tests some quantum realization $(\mathcal{H}_A, \mathcal{H}_B, \psi, \{A_x\}_x, \{B_y\}_y)$.

In the following theorem we give a geometric characterization of self-testing for the special case of $\mathrm{Cor}(2, 2)$.

Theorem 4. Let $C \in \mathrm{Cor}(2, 2)$ with $\mathrm{rank}(C) = 2$. The following are equivalent: (i) C is an extreme point of $\mathrm{Cor}(2, 2)$; (ii) C self-tests the singlet; (iii) C is a self-test.

Proof. In [30, Theorem 1] it is shown that a rank two correlator $C \in \mathrm{Cor}(2, 2)$ self-tests the singlet if and only if C saturates exactly one of the inequalities

$$-\pi \leqslant \sum_{xy \neq x'y'} \arcsin(c_{xy}) - \arcsin(c_{x'y'}) \leqslant \pi, \quad \forall x'y',$$

and at most one of the inequalities

$$-\pi/2 \leqslant \arcsin(c_{xy}) \leqslant \pi/2, \quad \forall x, y,$$

where $x, x' \in \{1, 2\}$, $y, y' \in \{3, 4\}$. Using that $\arccos(x) + \arcsin(x) = \frac{\pi}{2}$ and $\theta_{xy} = \arccos(c_{xy})$, the equivalence between (i) and (ii) follows from Theorem 3 (ii). Lastly, the equivalence between (ii) and (iii) is a special case of [14, Theorem 3.2]. ■

We remark that it is possible to give a direct proof of the relation between extremality and self-testing (without resorting to [30]) by resolving the mismatch between local isometries (used in the definition of self-testing) and global isometries (used in deriving the structure of realizations of extremal points).

D. Exposed correlators

An exposed face of $\mathrm{Cor}(n, m)$ is a subset $F \subseteq \mathrm{Cor}(n, m)$ for which there exists a matrix $A \in \mathbb{R}^{n\times m}$ such that $F = \mathrm{argmax}\{\langle A, X\rangle : X \in \mathrm{Cor}(n, m)\}$. A matrix $C \in \mathrm{Cor}(n, m)$ is an exposed point of $\mathrm{Cor}(n, m)$ if the singleton $\{C\}$ is an exposed face of $\mathrm{Cor}(n, m)$, i.e., there exists $A \in \mathbb{R}^{n\times m}$ such that

$$\{C\} = \mathrm{argmax}\{\langle A, X\rangle : X \in \mathrm{Cor}(n, m)\}.$$

Setting $b = \max\{\langle A, X\rangle : X \in \mathrm{Cor}(n, m)\}$, C is an exposed point of $\mathrm{Cor}(n, m)$ if the following two properties hold: *(i)* $\langle A, X\rangle \leqslant b$ for all $X \in \mathrm{Cor}(n, m)$ and *(ii)* $\langle A, X\rangle = b$ if and only if $X = C$. In this setting, we say that the hyperplane $\mathcal{H} = \{X \in \mathbb{R}^{n\times m} : \langle A, X\rangle = b\}$ exposes the point C.

The exposed points of a convex set are always extreme, but the converse is not always true. An example of such a point is the Hardy behavior [36], which is an extreme point of the set of full behaviors (as it is a self-test [37]), but was recently shown to be nonexposed [13]. In addition, combined with the relation to self-testing in $\mathrm{Cor}(2, 2)$, we get the interpretation that exposed points allow self-testing by means of a Bell inequality (the hyperplane $\mathcal{H}$ above).

In this section, we use again SDP duality theory to give a sufficient condition for a point $C \in \mathrm{Cor}(n, m)$ to be exposed. Our main tool is the following result.

Theorem 5. Let $C^* = (c^*_{xy})$ be an extreme point of $\mathrm{Cor}(n, m)$ and $Z^* = \sum_{i=1}^{n+m} \lambda^*_i E_{ii} + \sum_{x=1}^{n}\sum_{y=1}^{m} \lambda^*_{xy} E_{x,n+y}$ a dual optimal solution for (21).

(i) The hyperplane

$$\mathcal{H} = \left\{(c_{xy}) : -\sum_{x=1}^{n}\sum_{y=1}^{m} \lambda^*_{xy} c_{xy} = \sum_{i=1}^{n+m} \lambda^*_i\right\}, \tag{27}$$

supports the set $\mathrm{Cor}(n, m)$ at the point C^*, i.e.,

$$-\sum_{x=1}^{n}\sum_{y=1}^{m} \lambda^*_{xy} c_{xy} \leqslant \sum_{i=1}^{n+m} \lambda^*_i, \quad \forall C \in \mathrm{Cor}(n, m),$$

$$-\sum_{x=1}^{n}\sum_{y=1}^{m} \lambda^*_{xy} c^*_{xy} = \sum_{i=1}^{n+m} \lambda^*_i.$$

(ii) Furthermore, if the homogeneous linear system

$$MZ^* = 0, \quad M_{ii} = 0, \ 1 \leqslant i \leqslant n+m, \tag{28}$$

in the symmetric matrix variable $M \in \mathcal{S}^{n+m}$ has only the trivial solution $M = 0$, then the hyperplane $\mathcal{H}$ given in (27) exposes the point C^*.

Proof. Recall that the solution set of (20) coincides with the set of PSD completions of C^*. As C^* is extreme, by Theorem 2, it has a unique PSD completion $\hat{C}^* \in \mathcal{S}^{n+m}_+$, i.e., $\hat{C}^*$ is the unique solution of the SDP (20).

We have already seen that the values of (20) and (21) coincide, and both are attained. Consequently, as $\hat{C}^*$ and Z^*

are primal-dual optimal, we have $\langle \hat{C}^*, Z^* \rangle = 0$ [cf. Theorem 6 (iii)]. Expanding this we get

$$\sum_{i=1}^{n+m} \lambda_i^* + \sum_{x=1}^{n}\sum_{y=1}^{m} \lambda_{xy}^* c_{xy}^* = 0.$$

Lastly, consider an arbitrary $C \in \mathrm{Cor}(n, m)$ and let $\hat{C}$ be one of its PSD completions. As the PSD cone is self-dual we get that $\langle \hat{C}, Z_* \rangle \geqslant 0$, and expanding this gives

$$\sum_{i=1}^{n+m} \lambda_i^* + \sum_{x=1}^{n}\sum_{y=1}^{m} \lambda_{xy}^* c_{xy} \geqslant 0,$$

which shows that $\mathcal{H}$ supports $\mathrm{Cor}(n, m)$ at C^*. Equivalently, C^* is an optimal solution of the program:

$$\max \left\{ -\sum_{x=1}^{n}\sum_{y=1}^{m} \lambda_{xy}^* c_{xy} : C \in \mathrm{Cor}(n, m) \right\}. \tag{29}$$

Next, we further assume that the linear system (28) admits only the trivial solution. To show that the hyperplane $\mathcal{H}$ exposes C^*, it suffices to show that C^* is the unique optimal solution of (29). To do this, we first write (29) as an SDP in primal canonical form. Recalling that $\mathrm{Cor}(n, m) = \Pi(\mathcal{E}_{n+m})$, it immediately follows that (29) is equivalent to the SDP:

$$\begin{aligned} \max_X \quad & \langle \Lambda_b^*, X \rangle, \\ \text{such that} \quad & X_{ii} = 1,\ 1 \leqslant i \leqslant n+m, \\ & X \in \mathcal{S}_+^{n+m}, \end{aligned} \tag{30}$$

where $\Lambda_{xy}^* = -\lambda_{xy}^*$, $\forall x \in [n], y \in [m]$, and

$$\Lambda_b^* = \begin{pmatrix} 0_{n\times n} & \frac{\Lambda^*}{2} \\ \frac{\Lambda^{*\top}}{2} & 0_{m\times m} \end{pmatrix}.$$

The dual of (30) is given by

$$\begin{aligned} \min_{\lambda, Z} \ & \sum_{x=1}^{n} \lambda_x + \sum_{y=1}^{m} \mu_{n+y}, \\ \text{such that} \ & \sum_{x=1}^{n} \lambda_x E_{xx} + \sum_{y=1}^{m} \mu_y E_{n+y,n+y} - \Lambda_b^* = Z \in \mathcal{S}_+^{n+m}. \end{aligned} \tag{31}$$

As the primal (30) is strictly feasible and upper bounded, there exists no duality gap and the dual is attained; cf. Theorem 6 (iv). To show that C^* is exposed it remains to show that C^* is the unique optimal solution of (30). For this, by Theorem 7, it suffices to show that the dual SDP (31) has a nondegenerate optimal solution.

By the definitions of Z^* and Λ_b^* we have that $Z^* = \sum_{i=1}^{n+m} \lambda_i^* E_{ii} - \Lambda_b^*$, i.e., Z^* is dual feasible for (31). Furthermore, as $\langle \hat{C}^*, Z^* \rangle = 0$, and $\hat{C}^*, Z^*$ are primal-dual feasible for (30) and (31), respectively, they are primal-dual optimal. Lastly, the assumption (28) implies that Z^* is dual nondegenerate, and the proof is concluded. ■

We now illustrate the usefulness of Theorem 5 by two concrete examples, followed by a summary and the conclusions of our computational work.

Example 4. We prove that the hyperplane

$$c_{11} + c_{12} + c_{21} - c_{22} \leqslant 2\sqrt{2}$$

exposes the CHSH correlator. This means that observing a CHSH value of $2\sqrt{2}$ in an experiment self-tests a unique quantum realization. We have already seen that the matrix $\hat{C}$ given in (15) is the unique optimal solution for (20). As $\mathrm{rank}(\hat{C}) = 2$, the null space of $\hat{C}$ has dimension two, and a linear basis is given by

$$v_1 = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, -1, 0\right)^\top, \quad v_2 = \left(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}}, 0, -1\right)^\top.$$

Using these two vectors we define

$$Z^* = v_1 v_1^\top + v_2 v_2^\top = \begin{pmatrix} 1 & 0 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 1 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 1 & 0 \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 1 \end{pmatrix}.$$

Next, we show that Z^* is dual optimal for (21). Indeed, by construction Z^* is feasible for (21), and satisfies $\langle \hat{C}, Z^* \rangle = \langle \hat{C}, v_1 v_1^\top \rangle + \langle \hat{C}, v_2 v_2^\top \rangle = 0$. As $\hat{C}$ is optimal for (5), Theorem (6) (iii) implies that Z^* is dual optimal.

Having established that Z^* is dual optimal, Theorem 5 implies that the hyperplane $c_{11} + c_{12} + c_{21} - c_{22} \leqslant 2\sqrt{2}$ supports Cor(2, 2) at the CHSH correlator. Lastly, to prove that this hyperplane exposes the CHSH correlator, by Theorem 5 (ii), it suffices to show that the homogeneous linear system (28) only admits the trivial solution. A straightforward calculation reveals this is the case.

Example 5. We show that the hyperplane

$$\begin{aligned} &-12\sqrt{2}c_{14} + 4c_{15} - 4\sqrt{2}c_{16} + 4c_{24} - 12\sqrt{2}c_{25} - 4\sqrt{2}c_{26} \\ &-4\sqrt{2}c_{34} - 4\sqrt{2}c_{35} + 2(2 - 3\sqrt{2})c_{36} \leqslant 6(5\sqrt{2} + 2) \end{aligned} \tag{32}$$

exposes the Mayers-Yao correlator (16). This means that achieving the maximal quantum violation of the above Bell inequality self-tests a unique quantum realization. In Example 2, we showed that the SDP (20) has the unique solution

$$X^* = \begin{pmatrix} 1 & 0 & 1/\sqrt{2} & 1 & 0 & 1/\sqrt{2} \\ 0 & 1 & 1/\sqrt{2} & 0 & 1 & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} & 1 & 1/\sqrt{2} & 1/\sqrt{2} & 1 \\ 1 & 0 & 1/\sqrt{2} & 1 & 0 & 1/\sqrt{2} \\ 0 & 1 & 1/\sqrt{2} & 0 & 1 & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} & 1 & 1/\sqrt{2} & 1/\sqrt{2} & 1 \end{pmatrix}. \tag{33}$$

Note that $\mathrm{rank}(X^*) = 2$ and, in fact, its column space is spanned by the first two columns. Thus its null space has dimension four, and a basis is given by the vectors:

$$\begin{aligned} v_1 &= (-1, -1, -1, 1, 1, 1)^\top, \\ v_2 &= (-1, 1, 0, 1, -1, 0)^\top, \\ v_3 &= (1, 1, -\sqrt{2}, 1, 1, -\sqrt{2})^\top, \\ v_4 &= (1, 1, -1, -1, -1, 1)^\top. \end{aligned}$$

Using these vectors we define

$$Z^* = 2\sqrt{2}v_1v_1^\top + (3\sqrt{2}+1)v_2v_2^\top + v_3v_3^\top + \sqrt{2}v_4v_4^\top$$
$$= \begin{pmatrix} 2(3\sqrt{2}+1) & 0 & 0 & -6\sqrt{2} & 2 & -2\sqrt{2} \\ 0 & 2(3\sqrt{2}+1) & 0 & 2 & -6\sqrt{2} & -2\sqrt{2} \\ 0 & 0 & 3\sqrt{2}+2 & -2\sqrt{2} & -2\sqrt{2} & 2-3\sqrt{2} \\ -6\sqrt{2} & 2 & -2\sqrt{2} & 2(3\sqrt{2}+1) & 0 & 0 \\ 2 & -6\sqrt{2} & -2\sqrt{2} & 0 & 2(3\sqrt{2}+1) & 0 \\ -2\sqrt{2} & -2\sqrt{2} & 2-3\sqrt{2} & 0 & 0 & 3\sqrt{2}+2 \end{pmatrix}.$$

By construction, Z^* is positive semidefinite, feasible for (21), and satisfies $\langle X^*, Z^*\rangle = 0$. Consequently, by Theorem 6 (iii) we get that Z^* is dual optimal for (21) and thus, by Theorem 5 (i), we see that (32) is a valid hyperplane for $\mathrm{Cor}(3,3)$. It remains to show that the hyperplane (32) exposes the Mayers-Yao correlator. For this, by Theorem 5 (ii), it suffices to show that the linear system (28) only admits the trivial solution. An easy calculation shows that this is indeed the case.

Verifying exposedness computationally. Theorem 5 leads to an algorithm for checking whether a given extremal correlator C is exposed. This is summarized below.

Step 1. Solve the SDP (21) to find an optimal solution $Z^* = \sum_{i=1}^{n+m} \lambda_i^* E_{ii} + \sum_{x=1}^{n}\sum_{y=1}^{m} \lambda_{xy}^* E_{xy}$.

Step 2. Solve the SDP (31) to find an optimal solution Z. If Z is nondegenerate, then C is exposed. If Z is degenerate, the test is inconclusive.

We implemented this procedure, called `exposedCorr.m` [31], on 1000 randomly generated extremal correlators from $\mathrm{Cor}(2,2)$, generated by `randExtremeCorr22.m`. In all instances, our algorithm concluded that the corresponding correlators were also exposed. Our computations suggest that, for $\mathrm{Cor}(2,2)$, most extreme points are also exposed. This is not surprising because according to Straszewicz's theorem (see [38], Theorem 18.6), the set of exposed points are dense in the set of extremal points.

VI. CONCLUSIONS AND FUTURE WORK

In this paper we studied geometric features of the set of quantum correlators using semidefinite programming. Our starting point is that the set of quantum correlations can be seen as the projection of the feasible region of a semidefinite program, known as the elliptope. This connection leads to a characterization of its boundary, which generalizes the well-known Tsirelson-Landau-Masanes criterion (Theorem 1). Furthermore, based on this connection, we were able to translate results concerning the geometry of elliptopes to the set of quantum correlations. The first question we considered was to characterize its extreme points, or equivalently its zero-dimensional faces. We managed to give a complete characterization by making a link to the positive semidefinite matrix completion problem (Theorem 2).

Furthermore, for the simplest Bell scenario we determined an explicit characterization of its extreme points (Theorem 3). Next, we gave a sufficient condition for a correlator to be exposed (Theorem 5). Lastly, we show that, in the simplest Bell scenario, the geometric property of extremality coincides with the operational task of self-testing (Theorem 4).

Our investigations in this paper naturally lead to several future directions.

(1) Can one obtain further analytic characterizations for scenarios not captured by Theorem 1? Can one generalize to multipartite correlation scenarios?

(2) What is the facial structure of the set of quantum correlations?

(3) In the set of full quantum behaviors, is extremality still equivalent to self-testing? If not, is extremality equivalent to self-testing with global isometries?

The first two questions are evident; let us comment on the third one. Here self-testing with global isometries is a similar notion to self-testing, but with the "gauge" equivalence being relaxed to arbitrary global isometries (yet still preserving the observed behavior). In other words, the (equivalence) orbit of each realization is larger as we allow global isometries in addition to local isometries. Note that self-testing with global isometries implies the usual self-testing, but the converse does not hold in general. Now it turns out that Theorem 4 can be strengthened by adding the following equivalence: (iv) C is a self-testing with global isometries. ■

Thus extremality gives a stronger property than (usual) self-testing in this context. We leave the study of these concepts and their relationships as future work.

ACKNOWLEDGMENTS

We would like to thank J. Kaniewski, V. Scarani, and K. T. Goh for helpful discussions. L.P.T. is supported by the Singapore Ministry of Education Academic Research Fund Tier 3 (Grant No. MOE2012-T3-1-009), by the National Research Fund and the Ministry of Education, Singapore, under the Research Centres of Excellence programme. Y.C. is supported by the John Templeton Foundation Grant No. 60607 "Many-box locality as a physical principle." A.V. is supported by the NUS Young Investigator Award No. R-266-000-111-133 and by an NRF Fellowship (No. NRF-NRFF2018-01 and No. R-263-000-D02-281).

APPENDIX A: SEMIDEFINITE PROGRAMING

In this section we briefly collect all the tools from SDP duality theory that we use in this paper. For proofs of these facts and additional details, interested readers are referred to [39].

Theorem 6. Consider a pair of primal-dual SDPs:

$$p^* = \sup_X \{\langle C, X\rangle : X \succeq 0,\ \langle A_i, X\rangle = b_i\ (i \in [\ell])\}, \quad \text{(P)}$$

$$d^* = \inf_{y,Z} \left\{ \sum_{i=1}^{\ell} b_i y_i\ :\ \sum_{i=1}^{\ell} y_i A_i - C = Z \succeq 0 \right\}. \quad \text{(D)}$$

The following properties hold.

(i) (Weak duality) Let $X, (y, Z)$ be a pair of primal-dual feasible solutions for (P) and (D), respectively. Then, $\langle C, X\rangle \leqslant \sum_{i=1}^{\ell} b_i y_i$, i.e., $p^* \leqslant d^*$.

(ii) (Optimality condition) Let $X, (y, Z)$ be a pair of primal-dual feasible solutions for (P) and (D), respectively. If $\langle C, X\rangle = \sum_{i=1}^{\ell} b_i y_i$, then we have that $p^* = d^*$ and, furthermore, X and (y, Z) are primal-dual optimal solutions, respectively.

(iii) (Complementary slackness) Let $X, (y, Z)$ be a pair of primal-dual feasible solutions for (P) and (D), respectively. Under the assumption that $p^* = d^*$ we have that $X, (y, Z)$ are primal-dual optimal if and only if $\langle X, Z\rangle = 0$.

(iv) (Strong duality) Assume that $d^* > -\infty$ $(p^* < +\infty)$ and that (D) [(P)] is strictly feasible. Then $p^* = d^*$ and, furthermore, the primal (dual) optimal value is attained.

Given a pair of primal-dual SDPs (P) and (D), a primal feasible solution X is called *primal nondegenerate* if

$$\mathcal{T}_X + \text{span}\{A_1, \dots, A_\ell\}^\perp = \mathcal{S}^n \quad \text{(A1)}$$

and a dual feasible solution (y, Z) is *dual nondegenerate* if

$$\mathcal{T}_Z + \text{span}\{A_1, \dots, A_\ell\} = \mathcal{S}^n, \quad \text{(A2)}$$

where $\mathcal{T}_Z$ is the tangent space on the manifold of symmetric $n \times n$ matrices with rank equal to rank(Z), at the point Z, and the sum of two vectors spaces denotes the linear span of their union.

A concrete expression for the tangent space is

$$\mathcal{T}_Z^\perp = \{M \in \mathcal{S}^n : MZ = 0\}.$$

For example, see [40] or [41, Lemma 7.1.1].

The next result summarizes sufficient conditions for the unicity of optimal solutions to SDPs identified in [40], which we use extensively throughout this work.

Theorem 7. Consider a pair of primal-dual SDPs (P) and (D), where we assume that their optimal values are equal and that both are attained. We have the following.

(i) If (P) has a nondegenerate optimal solution, (D) has a unique optimal solution. Symmetrically, if (D) has a nondegenerate optimal solution, then (P) has a unique optimal solution.

(ii) Furthermore, let $X, (y, Z)$ be a pair of primal-dual optimal solutions that satisfy

$$\text{rank}(X) + \text{rank}(Z) = n,$$

a property known as strict complementarity. Then, if X is the unique optimal solution for (P), (y, Z) is dual nondegenerate. Symmetrically, if (y, Z) is the unique optimal for (D), X is primal nondegenerate.

APPENDIX B: NECESSARY CONDITIONS FOR EXTREMALITY

In this section we collect several useful properties of extreme points of Cor(n, m), identified in the seminal work of Tsirelson [14,25]. For a more modern proof of these facts the reader is referred to [42].

A family of vectors $u_1, \dots, u_n, v_1, \dots, v_m$ is called a C *system* of $C \in$ Cor(n, m) if they satisfy $\|u_x\| \leqslant 1$, $\|v_y\| \leqslant 1$, and $c_{xy} = \langle u_x, v_y\rangle$, $\forall x \in [n], y \in [m]$.

Theorem 8. For any $C \in$ ext(Cor(n, m)) we have the following.

(i) All C systems are necessarily unit vectors.

(ii) For any C system $\{u_1, \dots, u_n, v_1, \dots, v_m\}$ we have that span$(\{u_i\}_{i=1}^n) =$ span$(\{v_j\}_{j=1}^m)$.

(iii) C admits a unique PSD completion, i.e., there exists a *unique* matrix $\hat{C} \in \mathcal{E}_{n+m}$ with

$$\hat{C} = \begin{pmatrix} A & C \\ C^\top & B \end{pmatrix} \in \mathcal{E}_{n+m}.$$

Furthermore, we have that $\hat{C} \in$ ext$(\mathcal{E}_{n+m})$ and rank$(\hat{C}) =$ rank$(A) =$ rank$(B) =$ rank(C).

We note that the proof of Theorem 8 establishes the following chain of implications: (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii). To the best of our knowledge, it is not known whether any of these three conditions is equivalent to extremality.

APPENDIX C: PROOF OF THEOREM 1

Let $K_{2,n}$ be the complete bipartite graph, where the first bipartition has two vertices labeled $\{1, 2\}$ and the second bipartition has n vertices labeled $\{3, \dots, n+2\}$. As $K_{2,n}$ has no K_4 minor, by [22, Theorem 4.7] we have that Cor$(2, n) = \cos\pi($Met$(K_{2,n}))$. Setting $\theta_{xy} = \arccos(c_{xy})$, we get that $c = (c_{xy}) \in$ Cor$(2, n)$ if and only if there exists $a = (a_{xy}) \in$ Met$(K_{2,n})$ such that $c_{xy} = \cos(\pi a_{xy})$, i.e.,

$$\frac{\theta_{xy}}{\pi} \in \text{Met}(K_{2,n}).$$

The box constraints for Met$(K_{2,2})$ give

$$0 \leqslant \theta_{xy} \leqslant \pi, \quad \forall x, y.$$

We continue with the cycle inequalities of Met$(K_{2,n})$. Note that, for each $3 \leqslant i < j \leqslant n+2$, the graph $K_{2,n}$ contains one cycle of length four, namely $C = (1, i, j, 2)$. The cycle inequality for $F = \{1i\}$ gives

$$\theta_{1i} - \theta_{1j} - \theta_{2i} - \theta_{2j} \leqslant 0,$$

and the cycle inequality for $C \setminus F$ gives

$$\theta_{1j} + \theta_{2i} + \theta_{2j} - \theta_{1i} \leqslant 2\pi.$$

Summarizing, $c = (c_{xy}) \in$ Cor$(2, n)$ if and only if

$$\begin{aligned} &0 \leqslant \theta_{xy} \leqslant \pi, \quad \forall x, y, \\ &0 \leqslant \theta_{1j} + \theta_{2i} + \theta_{2j} - \theta_{1i} \leqslant 2\pi, \\ &0 \leqslant \theta_{1i} + \theta_{2i} + \theta_{2j} - \theta_{1j} \leqslant 2\pi, \\ &0 \leqslant \theta_{1i} + \theta_{1j} + \theta_{2j} - \theta_{2i} \leqslant 2\pi, \\ &0 \leqslant \theta_{1i} + \theta_{1j} + \theta_{2i} - \theta_{2j} \leqslant 2\pi, \end{aligned} \quad \text{(C1)}$$

where $3 \leqslant i < j \leqslant n+2$.

APPENDIX D: ALL THE EXTREME POINTS IN Cor(2, 2)

We present the proof of the complete characterization of extreme points in Cor(2, 2). In the main text, we employ the following labeling for the completion matrix:

$$\left(\begin{array}{cc|cc} 1 & ? & \cos\theta_{11} & \cos\theta_{12} \\ ? & 1 & \cos\theta_{21} & \cos\theta_{22} \\ \hline \cos\theta_{11} & \cos\theta_{21} & 1 & ? \\ \cos\theta_{12} & \cos\theta_{22} & ? & 1 \end{array}\right),$$

which derives from our notation of c_{xy} where $x \in [n]$ and $y \in [m]$ labels Alice's and Bob's measurements. However, we now switch to the following notation:

$$\left(\begin{array}{cc|cc} 1 & ? & \cos\theta_{13} & \cos\theta_{14} \\ ? & 1 & \cos\theta_{23} & \cos\theta_{24} \\ \hline \cos\theta_{13} & \cos\theta_{23} & 1 & ? \\ \cos\theta_{14} & \cos\theta_{24} & ? & 1 \end{array}\right),$$

which is derived from the natural position of elements within the completion matrix (e.g., $c_{13} = \cos\theta_{13}$ is the element at row 1 and column 3). We will be addressing the unspecified entries in a similar manner, so that the full completion matrix is notated as

$$\left(\begin{array}{cc|cc} 1 & \cos\theta_{12} & \cos\theta_{13} & \cos\theta_{14} \\ \cos\theta_{12} & 1 & \cos\theta_{23} & \cos\theta_{24} \\ \hline \cos\theta_{13} & \cos\theta_{23} & 1 & \cos\theta_{34} \\ \cos\theta_{14} & \cos\theta_{24} & \cos\theta_{34} & 1 \end{array}\right).$$

There is an evident correspondence between the notation in the main text and the notation here so that the upper 2×2 block still contains Alice and Bob's observable joint correlations.

Our strategy would be to use the conditions in Theorem 2 to understand which correlations are extreme in Cor(2, 2). This means understanding the conditions for unique completion to happen.

Lemma 9. Given $C = (c_{xy}) = (\cos\theta_{xy}) \in [-1, 1]^{2\times 2}$, define $m := \max\{|\theta_{31} - \theta_{41}|, |\theta_{32} - \theta_{42}|\}$ and

$$M := \min\{\theta_{31} + \theta_{41}, \theta_{32} + \theta_{42}, 2\pi - (\theta_{31} + \theta_{41}), 2\pi - (\theta_{32} + \theta_{42})\}.$$

Then C has a PSD completion if and only if one of the unspecified entries θ_{34} lies in the interval $[m, M]$.

The proof of this Lemma requires two basic results about the PSD completion problem. First, as any principal submatrix of a PSD matrix is also PSD, a necessary condition for $x \in \mathcal{E}(G)$ is that the restriction of x to any completely specified principal submatrix is PSD. In graph-theoretic language, if K is a clique in G, i.e., a fully connected subgraph of G, the restriction of x to K, denoted by x_K, should lie in $\mathcal{E}(K)$. The converse is the following.

Theorem 10. [20] Graph G is chordal (i.e., every circuit of length at least four in G has a chord) iff

$$\mathcal{E}(G) = \{x \in \mathbb{R}^E : x_K \in \mathcal{E}(K) \text{ for each clique } K \subseteq G\}.$$

Secondly, we will also need an explicit description of $\mathcal{E}(K_3)$, which has an elegant geometric interpretation (three vectors in Euclidean space).

Theorem 11. [43] Let $0 \leqslant \theta_1, \theta_2, \theta_3 \leqslant \pi$. Then, the matrix

$$C = \begin{pmatrix} 1 & \cos\theta_1 & \cos\theta_3 \\ \cos\theta_1 & 1 & \cos\theta_2 \\ \cos\theta_3 & \cos\theta_2 & 1 \end{pmatrix}$$

is positive semidefinite if and only if

$$\theta_1 \leqslant \theta_2 + \theta_3, \quad \theta_2 \leqslant \theta_1 + \theta_3, \\ \theta_3 \leqslant \theta_1 + \theta_2, \quad \theta_1 + \theta_2 + \theta_3 \leqslant 2\pi. \tag{D1}$$

Furthermore, C is singular if and only if one of the above inequalities holds with equality.

Proof of Lemma 9. Let $K_{2,2}$ be the graph with vertex set $\{1, 2, 3, 4\}$ and edges $\{(1, 3), (1, 4), (2, 3), (2, 4)\}$. By definition of the elliptope of a graph, $C \in \mathcal{E}(K_{2,2})$ if and only if there exists c_{34} such that $(C, c_{34}) \in \mathcal{E}(K_{2,2} \cup \{(3, 4)\})$. Nevertheless, the graph $K_{2,2} \cup \{3, 4\}$ is chordal, and thus by Theorem 10 we have that $C \in \mathcal{E}(K_{2,2})$ if and only if there exists $c_{34} \in [-1, 1]$ such that $(c_{13}, c_{14}, c_{34}) \in \mathcal{E}(K_3)$ and $(c_{23}, c_{24}, c_{34}) \in \mathcal{E}(K_3)$. Lastly, by Theorem 11, these two conditions are equivalent to the existence of $\theta_{34} \in [0, \pi]$ satisfying the following sixteen inequalities:

$$\theta_{13} \leqslant \theta_{14} + \theta_{34}, \quad \theta_{23} \leqslant \theta_{24} + \theta_{34}, \\ \theta_{14} \leqslant \theta_{13} + \theta_{34}, \quad \theta_{24} \leqslant \theta_{23} + \theta_{34}, \\ \theta_{34} \leqslant \theta_{13} + \theta_{14}, \quad \theta_{34} \leqslant \theta_{23} + \theta_{24}, \\ \theta_{13} + \theta_{14} + \theta_{34} \leqslant 2\pi, \quad \theta_{23} + \theta_{24} + \theta_{34} \leqslant 2\pi. \tag{D2}$$

Eliminating the unknown variable θ_{34} from the system (D2) we get $\theta_{34} \in [m, M]$. ■

Proof of Theorem 3. We split the proof into two parts based on the rank of the input correlation matrix written in the new notation we employed in this Appendix:

$$C = \begin{pmatrix} \cos\theta_{13} & \cos\theta_{14} \\ \cos\theta_{23} & \cos\theta_{24} \end{pmatrix}.$$

Rank-one case. Since this proof extends to arbitrary (n, m) and not just (2,2) we let $C \in \text{Cor}(n, m)$ with $\text{rank}(C) = 1$. We have to show that C is an extreme point if and only if $C = xy^\top$, for some vectors $x \in \{+1, -1\}^n$ and $y \in \{+1, -1\}^m$.

First, assume that $C = xy^\top$, where $x \in \{+1, -1\}^n$ and $y \in \{+1, -1\}^m$, and consider a convex combination

$$C = \sum_k \lambda_k C^k, \quad \text{where } \sum_k \lambda_k = 1,\ \lambda_k \geqslant 0, \tag{D3}$$

and the matrices C^k lie in $\text{Cor}(n, m)$, i.e., $C^k_{ij} = \langle u^k_i, v^k_j\rangle$, where $\|u^k_i\| = \|v^k_j\| = 1$. Note that

$$1 = |C_{ij}| = |x_i y_j| = \left|\sum_k \lambda_k C^k_{ij}\right| = \left|\sum_k \lambda_k \langle u^k_i, v^k_j\rangle\right| \\ \leqslant \sum_k \lambda_k \left|\langle u^k_i, v^k_j\rangle\right| \leqslant \sum_k \lambda_k = 1, \tag{D4}$$

and thus we have equality throughout. In particular, we get that $\sum_k \lambda_k |\langle u^k_i, v^k_j\rangle| = 1$, and as $|\langle u^k_i, v^k_j\rangle| \leqslant 1$, this implies that $|\langle u^k_i, v^k_j\rangle| = 1$, for all k, i, j. In other words, all matrices C^k have entries ± 1. Lastly, by (D3) we get that $C^k = xy^\top$ for all k, and thus C is extremal.

Conversely, let C be a rank-one extreme point of $\text{Cor}(n, m)$. In this setting, we have already mentioned that C admits a unique PSD completion $\hat{C} \in \mathcal{E}_{n+m}$ with $\hat{C} = \begin{pmatrix} A & C \\ C^\top & B \end{pmatrix} \in \mathcal{E}_{n+m}$ and, furthermore, $\hat{C} \in \text{ext}(\mathcal{E}_{n+m})$ and $\text{rank}(\hat{C}) = \text{rank}(A) = \text{rank}(B) = \text{rank}(C)$; e.g., see [42, Lemma 2.5]. By the assumptions we have that $\text{rank}(C) = 1$, and thus $\text{rank}(\hat{C}) = 1$, i.e.,

$$\hat{C} = \begin{pmatrix} x \\ y \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}^\top \in \mathcal{E}_{n+m}.$$

Since $\hat{C} \in \mathcal{E}_{n+m}$, it follows that $x_i^2 = y_i^2 = 1$. In turn, this shows that $C = xy^\top$, where $x \in \{+1, -1\}^n$ and $y \in \{+1, -1\}^m$.

Rank-two case. Let $C \in \text{Cor}(2, 2)$ with $\text{rank}(C) = 2$. We show that $C \in \text{extCor}(2, 2)$ if and only if it saturates exactly one of the cycle inequalities

$$0 \leqslant \sum_{xy \neq x'y'} \theta_{xy} - \theta_{x'y'} \leqslant 2\pi, \quad x, x' \in \{1, 2\},\ y, y' \in \{3, 4\},$$

and at most one of the box inequalities

$$0 \leqslant \theta_{xy} \leqslant \pi, \quad x \in \{1, 2\},\ y \in \{3, 4\}.$$

First, assuming that C saturates exactly one cycle inequality and at most one box inequality, we show that C is extremal. By Theorem 2, it suffices to show that C has a unique PSD completion $\hat{C}$, that furthermore satisfies the rank constraint between the correlation matrix C and its unique completion $\hat{C}$. For this, given an arbitrary PSD completion of the matrix C,

$$\left(\begin{array}{cc|cc} 1 & c_{12} & c_{13} & c_{14} \\ c_{12} & 1 & c_{23} & c_{24} \\ \hline c_{13} & c_{23} & 1 & c_{34} \\ c_{14} & c_{24} & c_{34} & 1 \end{array}\right), \tag{D5}$$

we show that c_{12} and c_{34} are uniquely determined. For concreteness, assume that the tight cycle inequality is

$$\theta_{13} + \theta_{23} + \theta_{24} - \theta_{14} = 0. \tag{D6}$$

This assumption is without loss of generality, as all cycle inequalities are equivalent up to permuting the parties and relabeling the outcomes. In the optimization community this is known as the "switching symmetry" of the cut polytope [15].

The fact that this equality leads to a unique completion should be evident by Lemma 9. However, let us be even more explicit and show that the unknown entries c_{12}, c_{34} are completely determined by this equation. Summing the two triangle inequalities

$$-\theta_{13} - \theta_{23} + \theta_{12} \leqslant 0, \quad -\theta_{24} - \theta_{12} + \theta_{14} \leqslant 0, \tag{D7}$$

we get that

$$\theta_{13} + \theta_{23} + \theta_{24} - \theta_{14} \geqslant 0, \tag{D8}$$

which combined with (D6) implies that

$$\theta_{12} = \theta_{13} + \theta_{23} = \theta_{14} - \theta_{24}. \tag{D9}$$

Indeed, if either of the triangle inequalities in (D7) were strict, then (D8) would also be a strict inequality, contradicting (D6). Similarly, using the two triangle inequalities

$$-\theta_{23} - \theta_{24} + \theta_{34} \leqslant 0, \quad -\theta_{34} - \theta_{13} + \theta_{14} \leqslant 0, \tag{D10}$$

we get that

$$\theta_{34} = \theta_{23} + \theta_{24} = \theta_{14} - \theta_{13}. \tag{D11}$$

Taking cosines in (D9) and (D11), we see that the two unspecified entries c_{12} and c_{34} in (D5) are uniquely determined. Specifically, we have

$$c_{12} = \cos(\theta_{12}) = c_{13}c_{23} - \sqrt{\left(1 - c_{13}^2\right)\left(1 - c_{23}^2\right)}, \tag{D12}$$

$$c_{34} = \cos(\theta_{34}) = c_{23}c_{24} - \sqrt{\left(1 - c_{23}^2\right)\left(1 - c_{24}^2\right)}, \tag{D13}$$

where we used that $\theta_{13}, \theta_{14}, \theta_{23}, \theta_{24} \in [0, \pi]$. Summarizing, C has a PSD unique completion, denoted by $\hat{C}$.

The last step of the proof is to show that

$$\text{rank}(\hat{C} \circ \hat{C}) = \binom{\text{rank}(\hat{C}) + 1}{2}.$$

For this, let $x_1, \ldots, x_4$ be a Gram decomposition of $\hat{C}$. By (D6), these four vectors span either a one-dimensional or a two-dimensional linear space. In particular, by projecting onto their linear span we may assume that they in fact lie in $\mathbb{R}^2$. Thus, for the rank of $\hat{C}$, there are two cases to consider: $\text{rank}(\hat{C}) \in \{1, 2\}$.

If $\text{rank}(\hat{C}) = 1$, since $\text{rank}(C) \leqslant \text{rank}(\hat{C})$ we have that $\text{rank}(C) = 1$, contradicting the assumption that $\text{rank}(C) = 2$. Thus we have that $\text{rank}(\hat{C}) = \text{rank}(C) = 2$. By Theorem 2, it remains to show that

$$\text{rank}(\hat{C} \circ \hat{C}) = \dim \text{span}(x_1x_1^\top, x_2x_2^\top, x_3x_3^\top, x_4x_4^\top) = 3.$$

Note that x_1 is not parallel to x_2, for otherwise the second row of C would be a multiple of the first one, contradicting the assumption $\text{rank}(C) = 2$. Similarly, x_3 is not parallel to x_4. Thus the sets $\{x_1, x_2\}$ and $\{x_3, x_4\}$ are the basis for $\mathbb{R}^2$. Furthermore, a simple calculation shows that

$$x_3 = \frac{\sin(\theta_{13})x_1 + \sin(\theta_{23})x_2}{\sin(\theta_{13} + \theta_{23})} \tag{D14}$$

and

$$x_4 = \frac{\sin(\theta_{14})x_1 + \sin(\theta_{24})x_2}{\sin(\theta_{14} + \theta_{24})}. \tag{D15}$$

For example, to see (D14), expand x_3 in the $\{x_1, x_2\}$ basis, i.e., $x_3 = \lambda x_1 + \mu x_2$. Taking inner products with x_1 and x_2, and eliminating μ in the resulting linear system, we get that $\lambda = [\cos(\theta_{13}) - \cos(\theta_{23})\cos(\theta_{12})]/\sin^2(\theta_{12})$. Lastly, substituting $\theta_{12} = \theta_{13} + \theta_{23}$, it follows that $\lambda = \sin(\theta_{13})/\sin(\theta_{13} + \theta_{23})$. Combining (D14) and (D15) we get

$$x_3x_3^\top = \frac{\sin^2(\theta_{13})x_1x_1^\top + \sin^2(\theta_{23})x_2x_2^\top + 2\sin(\theta_{13})\sin(\theta_{23})(x_1x_2^\top + x_2x_1^\top)}{\sin^2(\theta_{13} + \theta_{23})}, \tag{D16}$$

$$x_4x_4^\top = \frac{\sin^2(\theta_{14})x_1x_1^\top + \sin^2(\theta_{24})x_2x_2^\top + 2\sin(\theta_{14})\sin(\theta_{24})(x_1x_2^\top + x_2x_1^\top)}{\sin^2(\theta_{14} + \theta_{24})}. \tag{D17}$$

Next we show that

$$x_1x_2^\top + x_2x_1^\top \notin \text{span}(x_1x_1^\top, x_2x_2^\top). \tag{D18}$$

Without loss of generality, we may assume that $x_1 = (1,0)^\top$ because, for any unitary operator U, the vectors Ux_1, Ux_2, Ux_3, Ux_4 also define a Gram decomposition of $\hat{C}$. Furthermore, as $x_1 = (1,0)^\top$, we have that $x_2 = (\cos(\theta_{12}), \sin(\theta_{12}))^\top$ and, consequently,

$$x_1x_2^\top + x_2x_1^\top = \begin{pmatrix} 2\cos(\theta_{12}) & \sin(\theta_{12}) \\ \sin(\theta_{12}) & 0 \end{pmatrix},$$

$$x_1x_1^\top = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$x_2x_2^\top = \begin{pmatrix} \cos^2(\theta_{12}) & \cos(\theta_{12})\sin(\theta_{12}) \\ \cos(\theta_{12})\sin\theta_{12} & \sin^2(\theta_{12}) \end{pmatrix}.$$

As $\sin^2(\theta_{12}) \neq 0$ (since x_1 is not parallel to x_2) we see that (D18) holds.

Lastly, note that either $\sin(\theta_{13})\sin(\theta_{23}) \neq 0$ or $\sin(\theta_{14})\sin(\theta_{24}) \neq 0$. Indeed, if both are zero, we would have two tight box constraints, contradicting the hypothesis. Without loss of generality, say that $\sin(\theta_{13})\sin(\theta_{23}) \neq 0$. Because $x_1x_2^\top + x_2x_1^\top \notin \text{span}(x_1x_1^\top, x_2x_2^\top)$, it follows by (D16) that

$$x_3x_3^\top \notin \text{span}(x_1x_1^\top, x_2x_2^\top),$$

and thus $\dim \text{span}(x_1x_1^\top, x_2x_2^\top, x_3x_3^\top, x_4x_4^\top) \geqslant 3$. On the other hand, by (D16) and (D17) it follows that $\dim \text{span}(x_1x_1^\top, x_2x_2^\top, x_3x_3^\top, x_4x_4^\top) \leqslant 3$.

We now prove the converse direction of the theorem. Say that C is a rank two extreme point of Cor(2, 2). By Lemma [42, Lemma 2.5], C has a unique PSD completion $\hat{C}$, where $\text{rank}(\hat{C}) = \text{rank}(C) = 2$ and $\text{rank}(\hat{C} \circ \hat{C}) = 3$.

First, note that under the assumptions of the theorem there can be at most one tight box constraint. Indeed, having two (or more) tight box constraints implies that x_1, x_2, x_3, x_4 consists of two pairs of parallel vectors, which contradicts the fact that $\text{span}(x_1x_1^\top, x_2x_2^\top, x_3x_3^\top, x_4x_4^\top) = 3$. In turn, the fact that we have at most one tight box constraint implies that at most one cycle inequality can be tight. For concreteness, say that $\theta_{14} = \theta_{13} + \theta_{23} + \theta_{24}$ and $\theta_{13} = \theta_{14} + \theta_{23} + \theta_{24} - 2\pi$. Substituting the second equation into the first one we get that $\theta_{23} + \theta_{24} = \pi$, which when substituted back into the first equation gives that $\theta_{14} = \theta_{13} + \pi$. In turn, using that $\theta_{13}, \theta_{14} \in [0, \pi]$, this implies that $\theta_{14} = \pi, \theta_{13} = 0$, i.e., we have two tight box constraints, a contradiction. Thus it remains to exhibit one tight cycle inequality.

By assumption C is extreme and, thus, it admits a unique PSD completion, i.e., there exists a unique choice for c_{12} and c_{34} that makes the partial matrix (D5) PSD. In particular, there exists a unique choice for the value of $\theta_{34} = \arccos(c_{34})$. We are now ready to conclude the proof of our theorem.

We have already noted that, under the assumptions of the theorem, there exists a unique choice for the value of $\theta_{34} = \arccos(c_{34})$. Consequently, by Lemma 9, the interval $[m, M]$ should reduce to a single point, i.e., the two end points should coincide. This happens iff one expression from the lower bound m is equal to the upper bound M.

We consider two cases. First, if these two inequalities have disjoint support, we get a tight cycle inequality. For example, from the equality $\theta_{31} - \theta_{41} = \theta_{32} + \theta_{42}$ we get the tight cycle inequality $\theta_{31} = \theta_{41} + \theta_{32} + \theta_{42}$. Second, if the two inequalities have the same support, we get a tight box inequality. In turn, this gives a tight cycle inequality. For example, the equality $\theta_{32} - \theta_{42} = 2\pi - (\theta_{32} + \theta_{42})$ gives the tight box inequality $\theta_{32} = \pi$. As $\text{rank}(\hat{C}) = 2$, all size three minors of $\hat{C}$ are singular. In particular, the minor $\hat{C}[2, 3, 4]$ is singular and thus, by Theorem 11, one of the triangle inequalities for (2,3,4) is tight. Using that $\theta_{32} = \pi$, combined with the fact that we can have at most one box inequality, we get that $\theta_{34} + \theta_{24} = \pi$. Lastly, the minor $\hat{C}[1, 3, 4]$ is also singular and, again by Theorem 11, one of the triangle inequalities for (1,3,4) is tight. For example, if $\theta_{13} + \theta_{14} = \theta_{34}$, by eliminating θ_{34} we get that $\theta_{13} + \theta_{14} = \pi - \theta_{24}$, which is the tight cycle inequality $\theta_{13} + \theta_{14} + \theta_{24} = \theta_{32}$. ■

Let us conclude with a remark that the *rank-two case* can be proved with a purely algebraic argument, i.e., avoiding the use of Gram vectors, by using the fact that rank of a matrix M is the largest order of any nonzero minor in M. The advantage of this algebraic argument is to eliminate any kind of doubt caused by appeal to geometric intuitions.

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

[2] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. Å. Larsson, C. Abellán *et al.* , Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (2015).

[3] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán *et al.*, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature (London) **526**, 682 (2015).

[4] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman *et al.*, Strong Loophole-Free Test of Local Realism, Phys. Rev. Lett. **115**, 250402 (2015).

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

[6] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge, 2009.

[7] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner, The quantum moment problem and bounds on entangled multi-prover games, in *23rd Annual IEEE Conference on Computational Complexity* (IEEE, New York, 2008), pp. 199–210.

[8] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys. **10**, 073013 (2008).

[9] W. Slofstra, The set of quantum correlations is not closed, Forum Mathematics, Pi **7**, e1 (2019).
[10] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inform. Comput. **4**, 273 (2004).
[11] R. Blume-Kohout, J. K. Gamble, E. Nielsen, K. Rudinger, J. Mizrahi, K. Fortier, and P. Maunz, Demonstration of qubit operations below a rigorous fault tolerance threshold with gate set tomography, Nat. Commun. **8**, 14485 (2017).
[12] R. Webster, *Convexity* (Oxford University Press, Oxford, 1994).
[13] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani, Geometry of the set of quantum correlations, Phys. Rev. A **97**, 022104 (2018).
[14] B. S. Tsirelson, Quantum analogues of the Bell inequalities: The case of two spatially separated domains, J. Sov. Math. **36**, 557 (1987).
[15] M. Deza and M. Laurent, *Geometry of Cuts and Metrics* (Springer, New York, 2009), Vol. 15.
[16] L. J. Landau, Empirical two-point correlation functions, Found. Phys. **18**, 449 (1988).
[17] S. Wehner, Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities, Phys. Rev. A **73**, 022110 (2006).
[18] C. A. Floudas and P. M. Pardalos, *Encyclopedia of Optimization* (Springer Science & Business Media, New York, 2001), Vol. 1.
[19] D. Drusvyatskiy, G. Pataki, and H. Wolkowicz, Coordinate shadows of semidefinite and Euclidean distance matrices, SIAM J. Optim. **25**, 1160 (2015).
[20] R. Grone, C. Johnson, E. Sá, and H. Wolkowicz, Positive definite completions of partial Hermitian matrices, Linear Alg. Appl. **58**, 109 (1984).
[21] S.-I. Tanigawa, Singularity degree of the positive semidefinite matrix completion problem, SIAM J. Optim. **27**, 986 (2017).
[22] M. Laurent, The real positive semidefinite completion problem for series-parallel graphs, Linear Alg. Appl. **252**, 347 (1997).
[23] L. Masanes, Extremal quantum correlations for N parties with two dichotomic observables per site, arXiv:quant-ph/0512100.
[24] A. Barvinok, *A Course in Convexity* (American Mathematical Society, Providence, RI, 2002), Vol. 54.
[25] B. S. Tsirelson, Some results and problems on quantum Bell-type inequalities, Hadron. J. Suppl. **8**, 329 (1993).
[26] S. Gribling, D. de Laat, and M. Laurent, Matrices with high completely positive semidefinite rank, Linear Alg. Appl. **513**, 122 (2017).
[27] C.-K. Li and B.-S. Tam, A note on extreme correlation matrices, SIAM J. Matrix Anal. Appl. **15**, 903 (1994).
[28] M.-E. Nagy, M. Laurent, and A. Varvitsiotis, Forbidden minor characterizations for low-rank optimal solutions to semidefinite programs over the elliptope, J. Comb. Theory, Ser. B **108**, 40 (2014).
[29] V. Scarani, The device-independent outlook on quantum physics, Acta Phys. Slov. **62**, 347 (2012).
[30] Y. Wang, X. Wu, and V. Scarani, All the self-testings of the singlet for two binary measurements, New J. Phys. **18**, 025021 (2016).
[31] The code is available at https://arxiv.org/src/1809.10886/anc.
[32] S. J. Summers and R. Werner, Bell's inequalities and quantum field theory. I. General setting, J. Math. Phys. **28**, 2440 (1987).
[33] S. Popescu and D. Rohrlich, Which states violate Bell's inequality maximally? Phys. Lett. A **169**, 411 (1992).
[34] A. Coladangelo, K. T. Goh, and V. Scarani, All pure bipartite entangled states can be self-tested, Nat. Commun. **8**, 15485 (2017).
[35] J. Kaniewski, Self-testing of binary observables based on commutation, Phys. Rev. A **95**, 062323 (2017).
[36] L. Hardy, Quantum Mechanics, Local Realistic Theories, and Lorentz-Invariant Realistic Theories, Phys. Rev. Lett. **68**, 2981 (1992).
[37] R. Rabelo, Y. Z. Law, and V. Scarani, Device-Independent Bounds for Hardy's Experiment, Phys. Rev. Lett. **109**, 180401 (2012).
[38] R. T. Rockafellar, *Convex Analysis* (Princeton University Press, Princeton, NJ, 2015).
[39] E. De Klerk, Aspects of semidefinite programming, *Interior Point Algorithms and Selected Applications* (Kluwer Academic, Dordrecht, 2002).
[40] F. Alizadeh, J.-P. A. Haeberly, and M. L. Overton, Complementarity and nondegeneracy in semidefinite programming, Math. Program. **77**, 111 (1997).
[41] L. Lovász and K. Vesztergombi, Geometric representations of graphs, *Paul Erdös and his Mathematics* (Springer-Verlag, Berlin, Heidelberg, 1999), pp. 471–498.
[42] A. Prakash, J. Sikora, A. Varvitsiotis, and Z. Wei, Completely positive semidefinite rank, Math. Program., Ser. A **171**, 397 (2018).
[43] W. Barrett, C. R. Johnson, and P. Tarazaga, The real positive definite completion problem for a simple cycle, Linear Alg. Appl. **192**, 3 (1993).