Quantum Correlations in the Minimal Scenario

Thinh P. Le[1], Chiara Meroni[2], Bernd Sturmfels[3,4], Reinhard F. Werner[5], and Timo Ziegler[5]

[1]Institute for Quantum Optics and Quantum Information Vienna, Boltzmanngasse 3 1090 Vienna, Austria

[2]Institute for Computational and Experimental Research in Mathematics, 121 South Main Street Providence RI 02903, USA

[3]Max Planck Institute for Mathematics in the Sciences Leipzig, Inselstrasse 22 04103 Leipzig, Germany

[4]Department of Mathematics, University of California, Berkeley, 970 Evans Hall #3840 Berkeley CA 94720-3840, USA

[5]Insitute für Theoretische Physik, Leibniz Universität Hannover, Appelstrasse 2 30167 Hannover, Germany

Dedicated to the memory of Boris Tsirelson

In the minimal scenario of quantum correlations, two parties can choose from two observables with two possible outcomes each. Probabilities are specified by four marginals and four correlations. The resulting four-dimensional convex body of correlations, denoted $\mathcal{Q}$, is fundamental for quantum information theory. We review and systematize what is known about $\mathcal{Q}$, and add many details, visualizations, and complete proofs. In particular, we provide a detailed description of the boundary, which consists of three-dimensional faces isomorphic to ellipropes and sextic algebraic manifolds of exposed extreme points. These patches are separated by cubic surfaces of non-exposed extreme points. We provide a trigonometric parametrization of all extreme points, along with their exposing Tsirelson inequalities and quantum models. All non-classical extreme points (exposed or not) are self-testing, i.e., realized by an essentially unique quantum model.

Two principles, which are specific to the minimal scenario, allow a quick and complete overview: The first is the pushout transformation, i.e., the application of the sine function to each coordinate. This transforms the classical correlation polytope exactly into the correlation body $\mathcal{Q}$, also identifying the boundary structures. The second principle, self-duality, is an isomorphism between $\mathcal{Q}$ and its polar dual, i.e., the set of affine inequalities satisfied by all quantum correlations ("Tsirelson inequalities"). The same isomorphism links the polytope of classical correlations contained in $\mathcal{Q}$ to the polytope of no-signalling correlations, which contains $\mathcal{Q}$.

We also discuss the sets of correlations achieved with fixed Hilbert space dimension, fixed state or fixed observables, and establish a new non-linear inequality for $\mathcal{Q}$ involving the determinant of the correlation matrix.
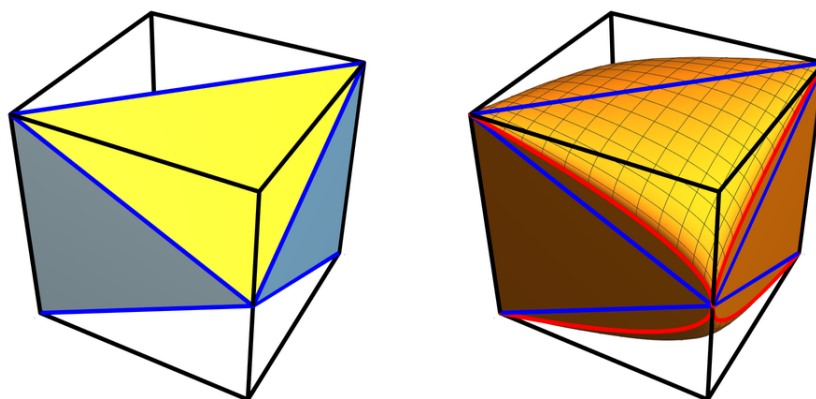
Thinh P. Le: Thinh.Le@oeaw.ac.at
Chiara Meroni: chiara_meroni@brown.edu
Bernd Sturmfels: bernd@mis.mpg.de
Reinhard F. Werner: reinhard.werner@itp.uni-hannover.de
Timo Ziegler: timo.ziegler@itp.uni-hannover.de

arXiv:2111.06270v3 [quant-ph] 9 Mar 2023

Contents

1 Introduction

The quantum correlation set is a fundamental object in quantum information theory. The key point is that some correlations predicted by quantum theory cannot be modeled within classical probability, more precisely under the constraints of "local realism". This far-reaching insight can be gained from just a single example, the singlet state of two quantum bits with a particular measurement setup. The correlations predicted by quantum theory were demonstrated experimentally [1] to high precision, and recently also while carefully closing some loopholes that persisted for decades [2, 3]. The non-classical nature is certified by the violation of the CHSH Bell inequality [4, 5], up to a maximum value of $2\sqrt{2}$ allowed by quantum theory. The correlation achieving $2\sqrt{2}$ also has the property of "self-testing", which means that its quantum realization is essentially unique. Just from the correlation measurement, one can infer not only the quantum state, but also the action of the measurement devices.

In this situation it is natural to ask: Where exactly lies the boundary between the classical and the quantum, between the quantum and the post-quantum correlations? What other correlations or quantum states exhibit the same features? In a correlation setting, N parties share some quantum state, so that each party can choose from M different measurements, each of which can have K different outcomes. So what exactly is the set of correlation data that can arise from either classical probability or quantum? This is a hard problem even for fairly small N, M, K, as seen on the open problems website [6, Problems 1,26,27,32,33,34]. The scenario mentioned in the first paragraph corresponds to $N = M = K = 2$, the smallest nontrivial scenario. Here, characterizations have been known since Tsirelson's seminal work [7], particularly in the "zero-marginals" case 222|0, defined by the property that each outcome by itself, without considering the results of other parties, is equidistributed. This is the scenario indicated by the adjective "minimal" in our title. We provide an overview of the literature below in Sect. 1.3. Known results are scattered. The connections between different characterizations are rarely given, the overall structure of the boundary is not analyzed, and no attempts at a full geometric understanding or visualization are made. Moreover, the self-duality of the body seems to have escaped notice of the wider community. All this will be provided in the present article, along with self-contained proofs of all assertions.

Our paper arose from a project of T.P.L. and R.F.W. aimed at a better understanding of self-testing. T.Z. joined as a Masters student. When we realized that even the 222-case was not clear in reasonable generality, we focused on that and could win the help of C.M. and B.S. from the mathematical side. The 222|0 case was to serve as the "well-understood example". Only that it was not understood at the desired level of detail. Furthermore, most of the available techniques for 222|0 do not apply to the full-marginal 222 case, from Tsirelson's correlation matrices to the cosine parametrization and the pushout principle to the semidefinite hierarchy. Doing justice to these techniques would have been a distraction in the full 222 context, so we decided to separate it, and organize the material into this 222|0 review with a geometric flavor. As work progressed, we realized that there was more in the works of Boris Tsirelson than we had recollections of. Tsirelson was writing at a time when the relevant community was very small (and included one of us, R.F.W., who should have remembered more). Back then long proofs of exotic material were hard to publish, which may be why he often chose to state his results without proof. But he was clearly a pioneer, coming more than a decade before the surge of interest with the rise of Quantum Information. Boris Tsirelson died last year, so we felt it was fitting to dedicate this paper to him, and include the proofs he left out. We like to think that he would have enjoyed our presentation.

This article is very much a two-communities paper. We ask experts from the quantum side to bear with us when we cover standard material, just as we ask patience from geometers when we explain basic notions. Aiming for completeness on a well-researched subject means that it is largely a review. But we hope that even those experienced with quantum correlations will find new connections, just as we have.

Our presentation is organized as follows: We first set the scene with a brief introduction to quantum correlations. This is followed by a mathematical discussion which states main results in a concise form. We then also give a brief summary of previous work. Sect. 2 offers a more extended description of the correlation body $\mathcal{Q}$, from basic visualization and overall properties to a detailed classification of boundary points. In Sect. 3 we focus on the dual body and its connection to $\mathcal{Q}$. These geometric and algebraic features are related back to quantum issues in Sect. 4. We also discuss constrained sets in which some of the quantum data are fixed, namely Hilbert space dimension (Sect. 4.5), state (Sect. 4.6), or the observables (Sect. 4.7). In these descriptive sections we give no proofs. Proofs are collected in Sect. 5. Every statement of a proposition or theorem begins with a clickable pointer such as ($\rightarrow$Sect. 5) to the
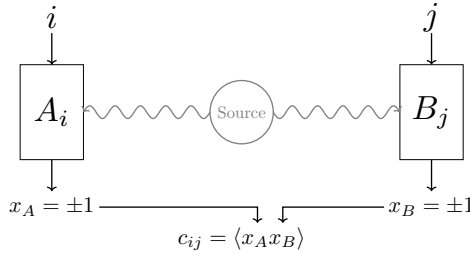
Figure 1: A correlation experiment: Alice chooses setting i and Bob chooses setting j. The outcomes of A_i and B_j are ± 1. One measures the correlation c_{ij} of these outcomes.

subsection containing the proof. An exception to this rule are statements that are clear from the context, and merely summarize a narrative just given. The proof section is organized in logical order, and should be readable from beginning to end without forward references. Naturally, this order differs from the narrative in Sect. 2-Sect. 4, and also from the theorems in Sect. 1.2.

1.1 Background from Physics: Quantum Correlations

In a correlation experiment, several parties carry out measurements on a shared quantum system. We consider $N = 2$ causally disconnected parties, conventionally called Alice and Bob. Each of them chooses from $M = 2$ possible measurements, labeled $i, j = 1, 2$, with $K = 2$ possible outcomes, labeled ± 1 (see Fig. 1). Thus there are four experiments, labeled by the pairs (i, j) of choices for Alice and Bob. The correlation $c_{ij} \in [-1, 1]$ is the probability of equal outcomes minus that of different outcomes. Equivalently, c_{ij} is the expectation of the product of the outcomes, when these are labeled as ± 1. The c_{ij} are not sufficient to reconstruct the full statistics. That would give an 8-dimensional convex body, whose coordinates are the marginals for single outcomes, plus one correlation for every pair (i, j). This count incorporates the no-signalling condition, namely that the marginals do not depend on the setting chosen at the other site. Restricting to the 4-tuples $c = (c_{11}, c_{12}, c_{21}, c_{22})$ corresponds to a *projection* of the 8-dimensional body. We can realize this projection geometrically by taking the equal weight mixture of the given model with one in which all outcomes are flipped to their negatives. This operation changes the sign of the marginals, but not of the correlations c_{ij}. Therefore, we can alternatively think of the 4-dimensional body as that *section* of the 8-dimensional body, in which the marginals are set equal to zero. This explains why we call our scenario in the 4-dimensional c-space the zero marginals case.

We are interested in the set $\mathcal{Q}$ of correlations $c = (c_{11}, c_{12}, c_{21}, c_{22})$ that are consistent with quantum theory. Quantum systems are described in some separable Hilbert space $\mathcal{H}$ over $\mathbb{C}$. The source is given by a positive Hermitian operator ρ acting on $\mathcal{H}$. It satisfies $\text{tr}(\rho) = 1$ and is called the *density operator*. The measurements are characterized by Hermitian operators A_1, A_2, B_1, B_2 on $\mathcal{H}$ that satisfy the hypotheses

$$[A_i, B_j] = 0 \quad \text{and} \quad -\mathbb{1} \leq A_i, B_j \leq \mathbb{1} \qquad \text{for } 1 \leq i, j \leq 2. \tag{1}$$

If $\mathcal{H} = \mathbb{C}^m$ then A_i and B_j are Hermitian $m \times m$ matrices and $\mathbb{1}$ is the identity matrix. Condition (1) says that A_i commutes with B_j and that the eigenvalues of all these matrices are in $[-1, 1]$. The commutation condition represents the hypothesis that the two parties are causally disconnected, i.e., all measurements by Alice can be executed jointly with those of Bob. In contrast, the commutators $[A_1, A_2]$ and $[B_1, B_2]$ are usually nonzero, i.e., the two measurement choices of each party individually are not commensurate.

We remark that in the quantum information community, the commuting condition is often made in the stronger form, namely that the separated labs of Alice and Bob are rendered by a Hilbert space tensor product $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, so that $A_i = A_i' \otimes \mathbb{1}_B$ and $B_j = \mathbb{1}_A \otimes B_j'$ with A_1', A_2' acting on $\mathcal{H}_A$, and B_1', B_2' acting on $\mathcal{H}_B$. In principle, this might lead to a smaller quantum correlation set than the one defined above. This is a hard problem in general, discussed as *Tsirelson's problem* at the end of this section. But, as we will also show below, in the minimal scenario there is no difference, so there is no possible harm in starting from the more inclusive condition (1).

The correlations are computed from the operators above by taking traces:

$$c_{ij} = \text{tr}(\rho A_i B_j) \qquad \text{for} \quad 1 \leq i, j \leq 2. \tag{2}$$

The *correlation body* $\mathcal{Q}$ consists of all points c in the cube $[-1,1]^4$ that admit such a representation.

There is an analogous set $\mathcal{C}$ in classical probability theory, where the A_i and B_j are ± 1-valued random variables, with joint probability distribution ρ. Writing angle brackets for expectations, the formula is

$$c_{ij} = \langle A_i B_j \rangle \qquad \text{for} \quad 1 \le i, j \le 2. \tag{3}$$

The classical set $\mathcal{C}$ consists of all points c in the cube $[-1,1]^4$ that admit such a representation.

We note that (3) is the special case of (2) when all A_i and B_j commute. All matrices can then be taken to be diagonal, and the diagonal entries of ρ form a probability distribution. (Analogous statements hold in infinite dimensional Hilbert spaces, where the A_i, B_j may have continuous spectra). Hence $\mathcal{C} \subset \mathcal{Q}$.

The whole point of our correlation body is that the reverse inclusion is false. A prominent example is

$$c = \tfrac{1}{\sqrt{2}}(1, 1, 1, -1) \in \mathcal{Q} \setminus \mathcal{C}. \tag{4}$$

It is easy to build a quantum representation, and this has been realized experimentally to very high precision. So the realizability of this c is a well-confirmed experimental fact. On the other hand, c cannot be classical, because the Clauser-Horne-Shimony-Holt version of John Bell's inequality holds for all $c \in \mathcal{C}$:

$$\text{CHSH}(c): \qquad \tfrac{1}{2}(c_{11} + c_{12} + c_{21} - c_{22}) \le 1. \tag{5}$$

The point c in (4) is not classical because the left hand side of (5) equals $\sqrt{2}$, and this exceeds 1. This is a remarkable result, the basis of an *experimentum crucis* ruling out a whole mode of describing Nature.

The experiments put quantum theory to a sharp test: The value $\sqrt{2}$ is an upper bound for all quantum correlations. If a value significantly larger than $\sqrt{2}$ had been found, then this would refute the quantum way of describing Nature, in just the same way as classical theories are excluded by a violation of Bell's CHSH inequality. This inequality and all linear inequalities bounding $\mathcal{Q}$ are called *Tsirelson inequalities*.

Tsirelson's bound has led to speculations about super-quantum correlations in families of theories ("generalized probabilistic theories"), and to the desire to view the quantum case in a larger context. The only constraint then would be that Alice choosing a measurement device makes no detectable difference for the probabilities of outcomes seen by Bob alone, i.e., without comparing outcomes with Alice. This is the *no signalling set* of correlations, denoted by $\mathcal{N}$. It satisfies $\mathcal{C} \subset \mathcal{Q} \subset \mathcal{N}$. Since in this paper we ignore marginals seen by only one partner, the remaining constraint is that c lies in the cube, so $\mathcal{N} = [-1,1]^4$.

A crucial property for quantum key distribution is that a maximal violation of the CHSH inequality can be achieved in an essentially unique way. Thus, by just verifying such correlations, without any knowledge about the construction of the devices, one can reconstruct ρ, A_i, B_j up to trivial enlargements. This property is called *self-testing*. It implies that any further system will be uncorrelated, so an eavesdropping third party could never learn anything about the data collected by Alice and Bob. We extend this property to all non-classical extreme points of $\mathcal{Q}$ in Thm. 19, and explain the cryptographic background in Sect. 4.2.

When the numbers N, M, K of parties, settings and outcomes are larger than $2, 2, 2$, computing optimal bounds for $\mathcal{Q}$ is a hard problem, and necessary and sufficient conditions describing $\mathcal{Q}$ are rare. Basically, one needs special algebraic properties to characterize the measurement operators, that are needed to show self-testing. In Tsirelson's work [7], Clifford algebra techniques allow statements about $NMK = 2M2$, and the C*-algebra generated by two projections allows at least a parametrization of the extreme points of $NMK = N22$ [8]. Thus, these cases can effectively be reduced to a finite dimensional Hilbert space. In general this is not possible: It is known [9] that restricting the dimension to be finite, in general, gives a set that is not closed, so some limiting correlations require infinite dimension.

Related is the problem of distinguishing the sets of correlations, in which the operators are just required to commute, as in (1), versus the more restrictive tensor product form described after that equation. In finite dimension the two are readily shown to be equivalent (see, e.g., [10]), which may have led Tsirelson to claim in [11] that the two were equivalent. The problem was first clearly noticed in the project [12] chararacterizing quantum correlations by semidefinite matrix hierarchies, where the commutation condition is easy to implement, but tensor products are more elusive. The authors of that study contacted Tsirelson, who ("to his crying shame" according to his own website) could not make work the argument that he had had in mind in [11]. This became *Tsirelson's problem*. This problem turned out to be equivalent to a celebrated conjecture in operator algebras [13, 14], and was finally solved 14 years later in the negative [15]. So we now know that in general there is a difference. From the detailed sharp characterizations of the minimal $\mathcal{Q}$ collected in this paper, including explicit finite dimensional tensor product models for all correlations, we see that the problem does not arise here. But such detailed knowledge is rare. This is one main motivation for the detailed geometric study that is to follow.

1.2 A View from Mathematics: Convex Algebraic Geometry

The theory of polytopes is a mature subject in mathematics [16]. Based on linear algebra, it leads to rich geometric objects classified by discrete combinatorial structures and a beautiful duality theory. In its guise as *linear programming*, i.e, optimization over a polytope with linear objective, it has found many applications. The natural next step in complexity is to go from linear algebra to *nonlinear algebra* [17]. If we replace convex sets and objectives described by linear inequalities with those described by polynomials, the basic geometric appeal and duality theory are still there. But we now enter into the world of algebraic geometry. Much richer ways of combining sets, partial descriptions and geometric constraints have to be considered. Examples play an important role in exploring these possibilities. Our study of quantum correlations serves as a showcase for nonlinear phenomena that occur in *convex algebraic geometry* [18, 19].

The correlation body $\mathcal{Q}$ is compact and convex. Compactness is not obvious but follows from Thm. 1. For convexity, let $c, \tilde{c} \in \mathcal{Q}$ have realizations (2) by matrices of size m and $\tilde{m}$. Any convex combination $\lambda c + (1-\lambda)\tilde{c}$ is realized by block matrices of size $m + \tilde{m}$, namely $\lambda \rho \oplus (1-\lambda)\tilde{\rho}$, $A_i \oplus \tilde{A}_i$ and $B_j \oplus \tilde{B}_j$. By contrast, if we were to fix m then compactness is easy to see but convexity generally fails. For instance, fixing $m = 1$, the image under (2) is the set of 2×2 matrices of rank ≤ 1 with each entry in $[-1, +1]$.

The body $\mathcal{Q}$ lies between two polytopes. First, $\mathcal{Q}$ is contained in the 4-cube $\mathcal{N} = [-1, 1]^4$, which has 16 vertices, 32 edges, 24 ridges and 8 facets. Second, $\mathcal{Q}$ contains the classical set $\mathcal{C}$, which is also a polytope. It has two equivalent descriptions, both of which are helpful for our project. On one hand, it is a *demicube*, which is defined to be the convex hull of the eight even vertices of $\mathcal{N}$, i.e., the vertices for which the product of the four ± 1-coordinates is $+1$. This describes the inclusion $\mathcal{C} \subset \mathcal{N}$. On the other hand, we can think of $\mathcal{C}$ as the *cross polytope* [16, Example 0.4], combinatorially dual to $\mathcal{N}$, whose extreme points lie on the Cartesian coordinate axes at unit distance from the origin. Hence $\mathcal{C}$ has 8 vertices, 24 edges, 32 ridges and 16 facets, the reversed sequence of that for $\mathcal{N}$. This census of the faces of $\mathcal{C}$ is of direct relevance for our description of the boundary of the convex body $\mathcal{Q}$, to be given in Prop. 7.

The correlation body $\mathcal{Q}$ is semialgebraic: It can be described by a Boolean combination of polynomial inequalities. Here a phenomenon arises that is unfamiliar from polytope theory. It is not sufficient to use a conjunction of polynomial inequalities. In other words, $\mathcal{Q}$ is not a basic semialgebraic set. Moreover, while both polynomials g and h in Thm. 1 (d) are needed, only h is determined by $\mathcal{Q}$, as the unique algebraic description of a part of the boundary, while there is some freedom of choice for g.

A main source of convex semialgebraic sets is the cone of positive semidefinite matrices. Quantum theory is entirely based on this cone. Its states, observables, and channels are all defined in terms of it. The intersection of the semidefinite matrix cone with an affine-linear space is called a *spectrahedron*. The set $\mathcal{Q}$ arises from a spectrahedron by projection, and it is thus in the class of *spectrahedral shadows* [20].

Each of the themes described in the previous paragraphs can be used to characterize the set $\mathcal{Q}$. This leads to six descriptions that look different at first glance. We summarize these in the following theorem.

Theorem 1 *($\rightarrow$Sect. 5.1) The following six items all describe the same subset $\mathcal{Q}$ in $\mathbb{R}^4$:*

(a) *The set of quantum correlations c, as defined in Sect. 1.1, i.e., the c_{ij} from (2) satisfying (1).*

(b) *The convex hull of the hypersurface $\left\{ (\cos\alpha, \cos\beta, \cos\gamma, \cos\delta) \in \mathbb{R}^4 \mid \alpha + \beta + \gamma + \delta \equiv 0 \mod 2\pi \right\}$.*

(c) *The image of the demicube $\mathcal{C}$ under the homeomorphism $\mathbf{sin}: \mathcal{N} \to \mathcal{N}$, $c \mapsto \sin\left(\frac{\pi}{2} c_{ij}\right)_{1 \leq i, j \leq 2}$.*

(d) *The semialgebraic set $\left\{ c \in \mathcal{N} \mid g(c) \geq 0 \text{ or } h(c) \geq 0 \right\}$, where*

$$g(c) = 2 - (c_{11}^2 + c_{12}^2 + c_{21}^2 + c_{22}^2) + 2c_{11}c_{12}c_{21}c_{22} \tag{6}$$
$$h(c) = 4(1 - c_{11}^2)(1 - c_{12}^2)(1 - c_{21}^2)(1 - c_{22}^2) - g(c)^2 . \tag{7}$$

(e) *The spectrahedral shadow consisting of all points $(c_{11}, c_{12}, c_{21}, c_{22}) \in \mathbb{R}^4$ such that the matrix*

$$C = \begin{pmatrix} 1 & u & c_{11} & c_{12} \\ u & 1 & c_{21} & c_{22} \\ c_{11} & c_{21} & 1 & v \\ c_{12} & c_{22} & v & 1 \end{pmatrix} \tag{8}$$

is positive semidefinite for some choice of $u, v \in \mathbb{R}$.

(f) The scalar products of pairs of unit vectors a_i, b_j in some Euclidean space: $c_{ij} = a_i \cdot b_j$ for $i, j = 1, 2$.

One way to describe a convex body is by the maxima of all linear functionals. This is the *support function*

$$\phi(f) = \sup\{f \cdot c \mid c \in \mathcal{Q}\}. \tag{9}$$

Here $f \in \mathbb{R}^4$ and "·" denotes the scalar product in $\mathbb{R}^4$. The following theorem gives an explicit formula.

Theorem 2 *(→Sect. 5.4) Consider the following expressions in four variables $f = (f_{11}, f_{12}, f_{21}, f_{22})$:*

$$k(f) = (f_{11}f_{22} - f_{12}f_{21})(f_{11}f_{12} - f_{21}f_{22})(f_{11}f_{21} - f_{12}f_{22}) \tag{10}$$

$$p(f) = f_{11}f_{12}f_{21}f_{22} \tag{11}$$

$$\phi_{\mathcal{C}}(f) = \max\{|f_{11}+f_{12}+f_{21}+f_{22}|, |f_{11}+f_{12}-f_{21}-f_{22}|, |f_{11}-f_{12}+f_{21}-f_{22}|, |f_{11}-f_{12}-f_{21}+f_{22}|\} \tag{12}$$

$$m(f) = \left(\min_{i,j}|f_{ij}|\right)\left(\sum_{i,j}|f_{ij}|^{-1}\right). \tag{13}$$

The support function of the correlation body $\mathcal{Q}$ equals

$$\phi(f) = \begin{cases} \sqrt{\frac{k(f)}{p(f)}} & \text{if } p(f) < 0 \text{ and } m(f) > 2, \\ \phi_{\mathcal{C}}(f) & \text{otherwise.} \end{cases} \tag{14}$$

The case distinction in (14) is between the "classical" case and the "quantum" case. Indeed, as the notation suggests, the piecewise linear expression $\phi_{\mathcal{C}}$ in (12) is the support function of the cross polytope $\mathcal{C}$. Hence $\phi_{\mathcal{C}}$ represents inequalities for classical correlations. On the other hand, in first case of (14), the maximizers are non-classical correlations, which share all essential properties with CHSH: For fixed f the maximizer is unique (see Prop. 17) and given by a unique quantum model (see Sect. 4).

Let $\mathcal{K}$ be a convex body that contains the origin in its interior. Then its dual or polar is a convex body $\mathcal{K}^\circ$ that represents the linear inequalities satisfied by $\mathcal{K}$. In symbols, we have $\mathcal{K}^\circ = \{f \mid f \cdot c \leq 1, \ c \in \mathcal{K}\}$. If $\mathcal{K}$ is a polytope then so is $\mathcal{K}^\circ$, and the face numbers of $\mathcal{K}^\circ$ are the reversal of the face numbers of $\mathcal{K}$.

Consider the sequence of inclusions $\mathcal{C} \subset \mathcal{Q} \subset \mathcal{N}$ we discussed above. Then we have $\mathcal{N}^\circ \subset \mathcal{Q}^\circ \subset \mathcal{C}^\circ$. Here $\mathcal{C}$ and $\mathcal{N}^\circ$ are cross polytopes, while $\mathcal{N}$ and $\mathcal{C}^\circ$ are 4-cubes. However, even stronger statements are true: $\mathcal{C}$ is affinely isomorphic to $\mathcal{N}^\circ$, and $\mathcal{N}$ is affinely isomorphic to $\mathcal{C}^\circ$. Moreover, these isomorphisms extend to the middle term in the inclusion $\mathcal{C} \subset \mathcal{Q} \subset \mathcal{N}$, i.e., the correlation body $\mathcal{Q}$ is *self-dual*:

Theorem 3 *(→Sect. 5.2) There is an orthogonal transformation H on $\mathbb{R}^4$ such that*

$$\mathcal{C}^\circ = \frac{1}{2}H\mathcal{N}, \quad \mathcal{N}^\circ = \frac{1}{2}H\mathcal{C} \quad \text{and} \quad \mathcal{Q}^\circ = \frac{1}{2}H\mathcal{Q}.$$

The proofs of the three theorems are presented in Sect. 5. While proving that they agree, we write $\mathcal{Q}_{(a)}, \mathcal{Q}_{(b)}, \mathcal{Q}_{(c)}, \mathcal{Q}_{(d)}, \mathcal{Q}_{(e)}, \mathcal{Q}_{(f)}$ for the six sets in Thm. 1. All objects and assertions are explained in detail in Sect. 2. along with lots of additional information. For instance, Prop. 7 describes the stratification of the boundary of $\mathcal{Q}$ into various patches. Readers might start with Fig. 2, Fig. 3, and Fig. 4.

1.3 Short review of previous work and preview of new results

The correlation body $\mathcal{Q}$ first came into focus in Tsirelson's work [21]. That paper gives no proofs, but some of them were supplied in [7]. This includes the characterization $\mathcal{Q}_{(a)} = \mathcal{Q}_{(f)}$ in the more general 2M2|0 case ([21, Thm. 1]=[7, Thm. 2.1]). Thereby the study of $\mathcal{Q}$, whose definition also allows infinite dimensional Hilbert spaces, is reduced to a finite dimensional problem. A semialgebraic description for the 222|0 case is given in [7, Thm. 2.2], along with an expression for the support function [7, Thm. 2.2]. This is our Thm. 2. Tsirelson calls these results 'elementary' consequences of (f), and does not provide a proof. He also thought about issues not covered in our review, like the full 222 case, multipartite scenarios ($N > 2$) [7, Sect. 5], and violations of CHSH inequalities by position and momentum ([7], see also [22]).

The spectrahedral shadow $\mathcal{Q}_{(e)}$ first appeared in Landau's work [23] as a relaxation of the correlation body. That the relaxation is tight follows from Tsirelson's theorem [21]. Landau also gave a nearly

semialgebraic characterization of $\mathcal{Q}$ (see (21) below), which only misses the semialgebraic standard form by containing a square root. He almost achieved the description (c).

The pushout (c) was found by Masanes [24], who stated that it identifies $\mathcal{C}$ and $\mathcal{Q}$. He also considered the cosine-parametrized manifold of correlations in (b). The pushout was used implicitly in [12, 25], in the form of a characterization of $\mathcal{Q}$ by linear inequalities applied to the inverse pushout. However, it was not pointed out that the linear inequalities just characterize $\mathcal{C}$. Of course, spectrahedral shadows are used as outer approximants to $\mathcal{Q}$ in the semidefinite hierarchies [26, 12]. This is an important technique for higher NMK, even though one gets the convex body exactly only in the minimal case.

We thought that self-duality (Thm. 3) was entirely our own idea, until we found it mentioned in [27, Sect.4] with only a private communication by Palazuelos and Villanueva (2011) as a reference. We could not trace a published proof.

The uniqueness of quantum models, now known as self-testing [28], was also studied by Tsirelson [7]. Independently, [29] obtained the self-testing property for the CHSH inequality. A covering of the set of extreme points $\partial_e \mathcal{Q}$, which results in the cosine parametrization (b) and its analog in the N22|0-case, were found in [8], see also [30]. The exact identification of the set of extreme points was found much later in [31, 25]. The minimal case is an important example in many applications such as quantum nonlocality [32, 33], self-testing [34], and quantum cryptography [35, 36].

Our contribution is, first, a systematic account with proofs of all these results. The condensation of all the existing characterizations of $\mathcal{Q}$ is Thm. 1. We give the first published proofs of support function (Thm. 2) and self-duality (Thm. 3). Our second contribution is the detailed geometric understanding of $\mathcal{Q}$, and particularly of its boundary. This includes visualizations wherever possible, the classification of types of boundary points, i.e., exposed and non-exposed extreme points, edges and 3-dimensional facets (Prop. 7) and the analysis of how these parts fit together in 4 dimensions (Fig. 8). Moreover, we provide semialgebraic descriptions of all boundary pieces, and analyze the symmetry group of $\mathcal{Q}$ (a bit larger than trivially expected). Third, we analyze the relation between $\mathcal{Q}$ and its polar dual $\mathcal{Q}^\circ$, i.e., the set of linear inequalities satisfied by $\mathcal{Q}$. By self-duality, this is affinely isomorphic to $\mathcal{Q}$, so much of the analysis can be taken over. But we also analyze how points on the boundary of $\mathcal{Q}$ map to their supporting hyperplanes in $\mathcal{Q}^\circ$ (Fig. 14). This is a part of the so-called normal cycle, which we studied in Sect. 3.4. Fourth, we consider the quantum models for all $c \in \mathcal{Q}$. This is again a traditional subject, going back at least to Bell, and to Tsirelson for the uniqueness question (see above). Our review is condensed into a theorem of equivalences (Thm. 19) including geometric conditions, and two kinds of cryptographic security. We also address correlation bodies under constraints such as bounded Hilbert space dimension, fixed state, or fixed observables. The last question suggested an apparently new and surprisingly simple non-linear inequality for $c \in \mathcal{Q}$, namely $|\det c| \leq 1$, with sharp condition for equality (Prop. 24).

2 Description of the Correlation Body

A convex body is a compact convex set with nonempty interior. The convex body $\mathcal{Q}$ has dimension four. Our aim is to describe it in every detail. Naturally, the geometric description will strain our 3-dimensional intuition. As always, the solution is to build the geometric intuitions (German "Anschauung", visualization) on analytic notions, such as sections, projections, affine submanifolds, extreme points, and faces, which have clear definitions, but also on low-dimensional instances on which intuitions can be grounded. In the case at hand, the dimension gap is not too large, and we will see that some three-dimensional sections faithfully display important features of the four-dimensional body. We will also point out where this becomes too misleading. One general cautionary remark is that extreme points of a section usually fail to be extremal in the higher-dimensional body.

This section is divided into subsections, which are organized by geometric features, from overall properties to the classification of boundary points and their explicit description, to the dual inequalities, and finally the quantum realizations. This is different from the logical ordering in a proof. A complete set of proofs will be given only later in Sect. 5, which is accordingly organized in logical progression.

2.1 Gallery

We visualize the 4-dimensional body $\mathcal{Q}$ by showing 3-dimensional sections. Some of these will be at the same time projections. For example, the zero marginal case arises from the full marginal case either by
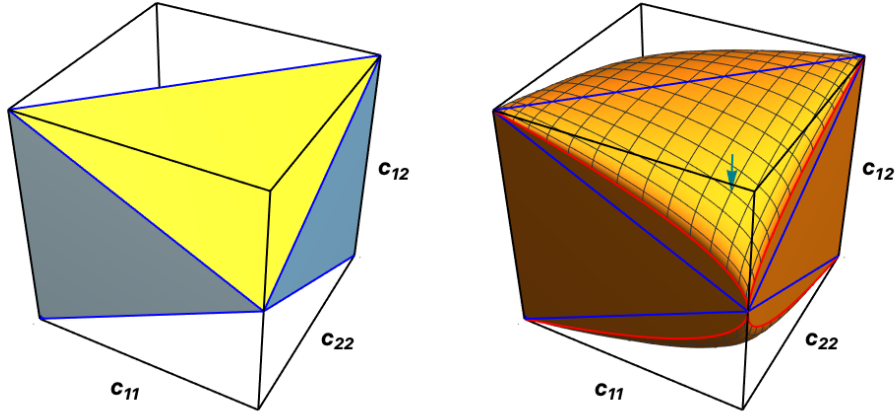
Figure 2: The Alice-Bob symmetric subsets of correlations ($c_{12} = c_{21}$), both a projection and a section of their 4-dimensional counterparts. Left: the polytopes: The cube $\mathcal{N}$ has black edges, and the octahedron $\mathcal{C}$ has blue edges, with two kinds of facets distinguished: CHSH-facets (yellow) defined by saturation of a CHSH-Bell inequality and "$\mathcal{N}$-facets" extending to facets of $\mathcal{N}$ (gray). Right: the correlation body $\mathcal{Q}$. Its boundary consists of a strictly convex surface of exposed extreme points, together with $\mathcal{N}$-faces extending those of $\mathcal{C}$, whose boundaries are outlined in red. The arrow points to the CHSH point $c = (1, 1, 1, -1)/\sqrt{2}$.
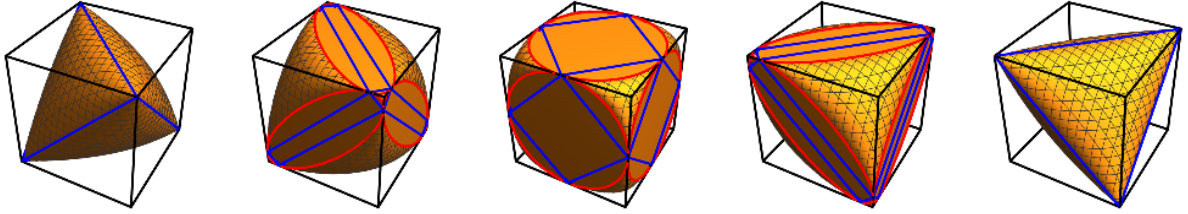

Figure 3: Parallel sections $c_{11} = t$ through the body $\mathcal{Q}$, for $t = -1, -0.8, 0, 0.8, 1$.

ignoring the marginals (a projection) or by taking the subset with zero marginals (a section by a linear subspace). Such sections/projections often arise by averaging over a symmetry group [37].

We begin in Fig. 2 with correlations that are symmetric under exchanging Alice and Bob, i.e., $c_{12} = c_{21}$. The corresponding projection is represented by $(c_{11}, c_{12}, c_{21}, c_{22}) \mapsto (c_{11}, c_{22}, (c_{12} + c_{21})/2)$. The corresponding sections of the polytopes $\mathcal{N}$ and $\mathcal{C}$ are a cube and an octahedron, respectively. The extreme points of the section of $\mathcal{C}$ are not all extremal in four dimensions: The point $(1, 1, 0)$, where two parabolas meet in Fig. 2, has $c_{12} = c_{21} = 0$. It is not extremal in $\mathcal{C}$. But it is the midpoint between the extreme points $(1, 1, -1, 1)$ and $(1, -1, 1, 1)$ of $\mathcal{C}$, which lie outside the section shown. The nonlinear boundary in Fig. 2 (right) is a quartic surface, obtained by setting $c_{12} = c_{21}$ in the sextic $h(c)$ and cancelling a factor $(c_{11} - c_{22})^2$. These geometric features have 4-dimensional counterparts, to be described later.

In Fig. 3 we show the sections parallel to the facets of the cube $\mathcal{N}$. These are obtained by fixing the value of one coordinate, say c_{11}, at a number t in the interval $[-1, 1]$. This family of pictures gives a full description of $\mathcal{Q}$. The corresponding projections are non-informative: They are equal to the full 3-cube. The special sections $c_{11} = \pm 1$ are facets of $\mathcal{Q}$. This 3-dimensional shape is known as the *elliptope*.

Other cutting directions, which can be expected to have an interesting symmetry are sections orthogonal to the main diagonals of $\mathcal{N}$. Like the vertices, they come in two kinds, either connecting two classical correlations or connecting two PR-boxes. In Fig. 4 we show, on the left, a cut very close to the hyperplane $c_{11} + c_{12} + c_{21} + c_{22} = 0$, which is orthogonal to the diagonal connecting the classical point $(1, 1, 1, 1)$ and its antipode. On the right in Fig. 4, we see the cut given by $c_{11} + c_{12} + c_{21} - c_{22} = 0$.
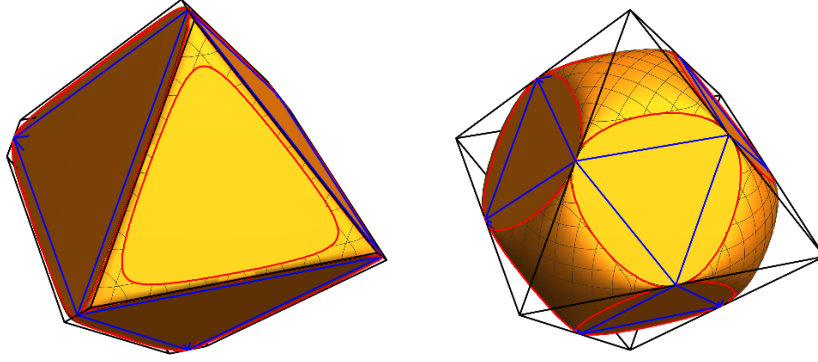
Figure 4: Sections through $\mathcal{Q}$ perpendicular to a long diagonal of the cube $\mathcal{N}$. There are two symmetry classes of diagonals: those connecting two classical correlations (left), and those connecting two PR-boxes (right). The cut on the right goes through the origin. On the left we would get the full octahedron. Our cut is thus slightly off-center.

2.2 Enclosing and enclosed polytopes

The cube $\mathcal{N}$ consists of the tuples $c = (c_{11}, c_{12}, c_{21}, c_{22})$ with $-1 \leq c_{ij} \leq 1$. It has $2^4 = 16$ vertices, namely the points in $\{-1, 1\}^4$. The classical distributions are the mixtures of uncorrelated c, i.e., $c_{ij} = a_i b_j$ for some $a_i, b_j \in [-1, 1]$. A classical correlation is extremal when $a_i, b_j = \pm 1$. Hence, the extreme points of $\mathcal{C}$ are also extreme points of $\mathcal{N}$, but which? This is decided by a sign: For a classical extreme point we have $c_{11} c_{12} c_{21} c_{22} = a_1^2 b_1^2 a_2^2 b_2^2 = +1$. So the classical extreme points of $\mathcal{C}$ are just the 8 even vertices of $\mathcal{N}$. The odd vertices are the so-called Popescu-Rohrlich (PR-)box correlations. They have neither classical nor quantum realizations: In (5) they satisfy CHSH$(c) = 2$, which clearly exceeds the quantum maximum.

The 16 facets of the demicube $\mathcal{C}$ come in two classes. These are distinguished by how they sit inside the cube $\mathcal{N}$. A facet in the first class extends to a facet of $\mathcal{N}$. It is the intersection of $\mathcal{C}$ with a hyperplane like $c_{11} = 1$. There are eight such facets, which we call $\mathcal{N}$-*facets* of $\mathcal{C}$. The more interesting kind is called a *CHSH-facet*, because it saturates a Clauser-Horne-Shimony-Holt inequality (5). There are eight such inequalities: Any odd number of minus signs can multiply the four correlations.

All of this can be seen also in the 3-dimensional cut along the hyperplane $c_{12} = c_{21}$ shown on the left in Fig. 2. The two polytopes are the intersection of $\mathcal{C}$ and $\mathcal{N}$ with this hyperplane. The CHSH-facets and the $\mathcal{N}$-facets are marked in different colors. Other slices of $\mathcal{C}$ (blue frame) and $\mathcal{N}$ (black frame) are shown in Figures 3 and 4. The cut through the origin, orthogonal to the long diagonal connecting classical vertices (approximately as in the left panel in Fig. 4) has the intersections with $\mathcal{N}$ and $\mathcal{C}$ equal to the same octahedron. Since $\mathcal{C} \subset \mathcal{Q} \subset \mathcal{N}$, this cut also makes our convex body $\mathcal{Q}$ look like a polytope.

Of course, in every cut we see the inclusions $\mathcal{C} \subset \mathcal{Q} \subset \mathcal{N}$. More precisely, the $\mathcal{N}$-facets of $\mathcal{C}$ extend to facets of $\mathcal{Q}$, which we also call $\mathcal{N}$-facets. This is typically a strict extension. The CHSH-facets are no longer faces of $\mathcal{Q}$. Instead, they become the basis of a bulging part of $\mathcal{Q}$, above which we find a single vertex of $\mathcal{N}$. In fact, this is a feature of any body between $\mathcal{C}$ and $\mathcal{N}$. We record this fact in the following proposition (also a corollary of [38]), which helps with keeping track of the parts of $\mathcal{Q}$.

Proposition 4 (→*Sect. 5.3.3*) *Every non-classical correlation $c \in \mathcal{N} \backslash \mathcal{C}$ violates exactly one of the eight CHSH-inequalities.*

A feature which will play a major role later, and is characteristic of the minimal case, is the *duality* between the polytopes $\mathcal{C}$ and $\mathcal{N}$. We saw this in Thm. 3, and it will be considered in detail in Sect. 3.

2.3 Pushout

The connection between the boundary structures of $\mathcal{Q}$ and $\mathcal{C}$ can be raised from a qualitative observation to a precise mathematical statement. There is a natural homeomorphism between the convex bodies. To this end, we define a transformation $\mathbf{sin} : \mathcal{N} \to \mathcal{N}$ of the cube, which we call the **pushout** operation:

$$\left(\mathbf{sin}\, c\right)_{ij} = \sin\!\left(\frac{\pi}{2} c_{ij}\right). \tag{15}$$

This is the coordinatewise application of a suitably scaled sine function. Since the sine maps the interval $[-\pi/2, \pi/2]$ bijectively and continuously onto $[-1, 1]$, we see that $\mathbf{sin}$ is bijective, continuous and has a continuous inverse. This is relevant because of the following astonishingly simple characterization of $\mathcal{Q}$.

Proposition 5 (→*Sect. 5.1.5*) $\mathcal{C}$ *is homeomorphic to* $\mathcal{Q}$ *under* $\mathbf{sin}$, *in particular* $\mathbf{sin}\,\mathcal{C} = \mathcal{Q}$.

The fact that $\mathbf{sin}\,\mathcal{C} = \mathcal{Q}$ was known to L. Masanes [24]. This fact was also often represented as $\mathbf{cos}(\pi\mathrm{MET}(K_{2,2}))$ in literature on matrix completion (see also Sect. 5.1.5). Here we strengthen the statement to a homeomorphism.

As a connection between convex bodies this is quite strange: The sine is neither convex nor concave on $[-\pi/2, \pi/2]$, so the $\mathbf{sin}$ transformation applied to a convex set normally does not give a convex set. Moreover, the $\mathbf{sin}$ function is transcendental but both sets have an algebraic description. So why does this work? What is the general principle? The pushout property is inherited by the sections in Fig. 2 and by the $\mathcal{N}$-facets because the hyperplanes $\{c_{12} = c_{21}\}$ and $\{c_{11} = -1\}$ are invariant under $\mathbf{sin}$. It also connects $\mathcal{C}$-sections and $\mathcal{Q}$-sections in Fig. 3 when the fixed c_{11}-coordinate is appropriately transformed. The closest we can come to a general principle is related to the fact that the pushout of the tetrahedron is the elliptope (see also [39]). This fact also underlines the cosine parametrization in Sect. 2.6. The threefolds of extreme points are parametrized by angles satisfying a linear constraint. A similar connection arises between two families of curves inside the 3-cube, on one hand Lissajous knots, i.e., cosine-parametrized closed rational curves, and, on the other, billiard knots, i.e., closed piecewise linear curves bouncing from the boundaries by specular reflection; see [40], [41, Fig. 3]. Another feature can be understood from the pushout characterization: At the edges of a polytope extending all the way to the boundary we get a rounded surface with continuous tangents. This is explained in Fig. 5.
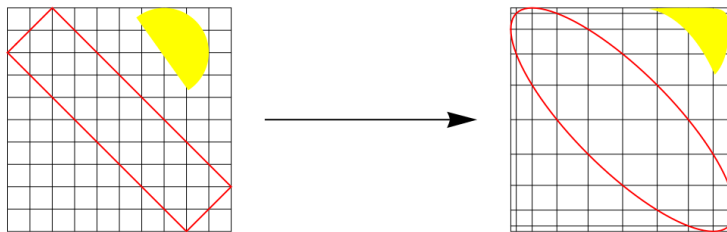

Figure 5: The 2-dimensional version of the pushout map in (15). The rectangle on the left gets mapped to the ellipse on the right. To verify this compare the scaled grid lines. The yellow semicircle shows that convexity is generally not preserved under the pushout map.

2.4 Symmetry

The symmetry group of the regular 4-cube $\mathcal{N} = [-1, 1]^4$ is the *hyperoctahedral group* B_4. This group has order $384 = 2^4 \times 4!$. All of these symmetries are given by rotations and reflections in $\mathbb{R}^4$. Each symmetry either preserves the parity of the vertices of $\mathcal{N}$, or it swaps the eight even vertices and the eight odd vertices. The symmetry group G of the demicube $\mathcal{C}$ is an index two subgroup of B_4, meaning $|B_4|/|G| = 2$. It consists of symmetries of $\mathcal{N}$ that preserve the parity. It follows from Prop. 5, and the fact that the pushout map commutes with coordinate permutations and sign changes, that $\mathcal{Q}$ has the same symmetry group G as $\mathcal{C}$.

Proposition 6 *The common symmetry group of* $\mathcal{Q}$ *and* $\mathcal{C}$ *has order* 192. *It is the semidirect product* $G = (\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_4$, *where* S_4 *is the symmetric group on four elements. The first factor swaps labels.*

It is noteworthy that this group is larger than one would expect from the definition of $\mathcal{Q}$. Indeed, some obvious symmetries arise from changing the conventions for describing the correlations: Which party is called Alice, which is Bob? Which outcome is $+1$ or -1, and which settings get the labels 1 or 2? Changing any of these conventions defines a transformation that clearly leaves each of the correlation sets invariant. The resulting group is visualized in Fig. 6, and acts on the tuples $(c_{11}, c_{12}, c_{21}, c_{22})$ by sign changes (first row) and permutations (second row) giving only 64 transformations. Not all sign changes can be obtained, only even ones, and the permutations cannot break pairs of diagonally opposing pairs

in the square form in which we arranged the c_{ij}. As the additional "non-trivial" transformation needed to generate the group given in Prop. 6, one can take the swap $(c_{11}, c_{12}, c_{21}, c_{22}) \mapsto (c_{12}, c_{11}, c_{21}, c_{22})$.
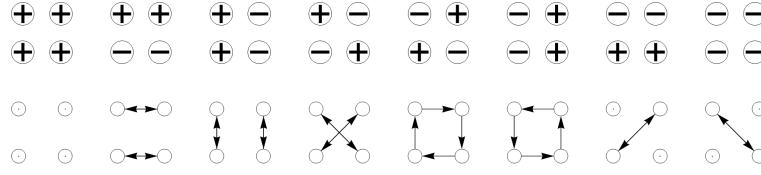

Figure 6: Symmetries that preserve the definition of quantum correlations. First row: sign patterns. Second row: the eight permutations arising from a swap of partners or relabeling. The symmetry group G of $\mathcal{Q}$, as described in Prop. 6, is larger: It allows *all* 24 permutations.

A group that played a key role in analyzing the classical polytope in the N22|0 case in [8] will also play a special role below for establishing self-duality. It is familiar to quantum physicists as a discrete version of phase spaces, describing a quantum or classical system in terms of "position" and "momentum", or "multiply" and "shift" operators, like σ_x and σ_z for qubits [42, 43]. To mathematicians it is familiar as the standard case of symplectic self-duality [44], where the position variables are given by a locally compact abelian group X, and the momenta by elements of the dual group $\widehat{X}$. The Hilbert space of the system is $\mathfrak{h} = L^2(X)$, on which X acts by transformation of the arguments, and $\widehat{X}$ by multiplication. This determines a projective representation of $X \times \widehat{X}$ on $\mathfrak{h}$ by the Weyl operators. The case of mechanics has $X = \mathbb{R}^f \cong \widehat{X}$, where f is called the number of degrees of freedom. For a single qubit, X is the two element group, and the Weyl operators are the Pauli matrices as above. For our problem we obtain the Klein four-group: a product of two copies of the two element group. The elements of this group are the indices of c_{ij}, with the convention that 1 is the identity and $2 \cdot 2 = 1$. Thus the correlation body is a subset of $\mathfrak{h}$. The 16 Weyl operators are the products of the first four elements of the each of the two lines in Fig. 6, the top row giving the momentum translations and the bottom row the position translations. A standard automorphism of this structure is the Fourier transform that takes functions on X to functions on $\widehat{X}$. This is not a symmetry of $\mathcal{Q}$, but, as we will see, takes $\mathcal{Q}$ to its dual convex body.

2.5 Boundary, faces, and extreme points

A *face* F of $\mathcal{Q}$ is a subset such that a convex decomposition of a point in F with non-zero weights must have all components in F. We use the term *facet* for faces of codimension 1. An *extreme point* of $\mathcal{Q}$ is a point c in $\mathcal{Q}$ such that $\{c\}$ is a face. A face is called *exposed* if it is the zero set of an affine-linear function which is non-negative on $\mathcal{Q}$. Since the pushout is a homeomorphism, it identifies the boundary of $\mathcal{Q}$ with the boundary of $\mathcal{C}$. The facets of the demicube $\mathcal{C}$ thus provide a partition of the boundary of the correlation body $\mathcal{Q}$. However, the image of a facet may now become curved, making interior points of the facet extremal in $\mathcal{Q}$. This happens exactly for the CHSH-facets of $\mathcal{C}$, as the following proposition shows. In the following we always list the interiors of faces because the boundaries already belong to another face. Here by "interior" we mean the relative interior, i.e., the interior in the affine span of the face.

Proposition 7 *(→Sect. 5.3.4) The convex body $\mathcal{Q}$ is the disjoint union of the following semialgebraic sets:*

(Qcx) 8 **classical exposed points** $c \in \partial_{\mathrm{e}} \mathcal{C}$.

(Qce) 24 **exposed edges**, *i.e., the interiors of line segments that connect pairs of classical exposed points.*

(Qnx) 32 *surfaces of* **non-exposed extreme points**.
Each is the pushout of a triangle in $\partial \mathcal{C}$, which is the intersection of an $\mathcal{N}$-facet and a CHSH-facet.

(Qqx) 8 *threefolds of* **exposed extreme points**.
Each threefold is the curved pushout of the interior of a CHSH-facet of $\mathcal{C}$, which is a tetrahedron.

(Qei) 8 **elliptopes**' *interiors, i.e., the interiors of the facets that arise from $\mathcal{N}$-facets of $\mathcal{C}$, as in Fig. 2.*

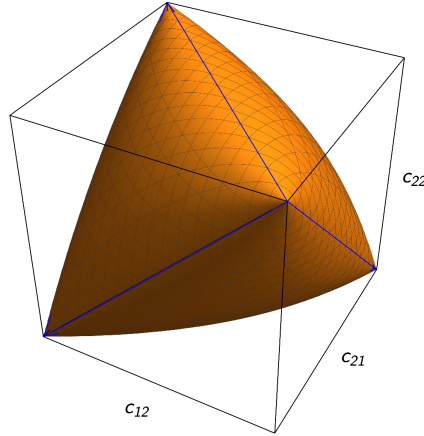*(Qin)* *The interior of $\mathcal{Q}$.*

Figure 7: Every 3-dimensional face of $\mathcal{Q}$ is an elliptope. Points of type ($\mathcal{Q}$cx) are vertices of the blue tetrahedron, ($\mathcal{Q}$ce) give blue edges, ($\mathcal{Q}$nx) is the orange surface. Extreme points of the elliptope are exposed in 3 dimensions, but not in 4. Type ($\mathcal{Q}$ei) comprise the interior.

The stratification of $\mathcal{Q}$ shown in Prop. 7 mirrors the stratification of the demicube $\mathcal{C}$ into relatively open faces. Indeed, the numbers seen in Prop. 7 count the faces of various dimension of $\mathcal{C}$. Namely, $\mathcal{C}$ has 8 vertices, 24 edges, 32 two-dimensional faces, etc. In short, the *f-vector* of $\mathcal{C}$ equals $(8, 24, 32, 8+8, 1)$.

The closures of sets of type ($\mathcal{Q}$) are said to be *of type* [$\mathcal{Q}$]. Types [$\mathcal{Q}$qx] and [$\mathcal{Q}$ei] suffice to cover the boundary. In the literature in convex algebraic geometry [45, 46], boundary strata (cf. Sect. 3.4 for a rough explanation) of codimension one are now called *patches*. Thus, our body $\mathcal{Q}$ has 16 patches, eight of type [$\mathcal{Q}$qx] and eight of type [$\mathcal{Q}$ei].

The difference between the types ($\mathcal{Q}$qx) and ($\mathcal{Q}$ei) will be important for what follows. It also relates to the two types of *maximal non-trivial faces* of $\mathcal{Q}$. The only two types are the singletons in ($\mathcal{Q}$qx), and the $\mathcal{N}$-facets [$\mathcal{Q}$ei]. These maximal faces are also exposed. Exposedness properties will be discussed later in their natural context: duality. An intuitive geometric understanding of the non-exposedness of type ($\mathcal{Q}$nx) can be gained from considering the pushout mechanism: This converts the junction between a CHSH-facet and an $\mathcal{N}$-facet of $\mathcal{C}$ to a junction with matching tangents. The prototype for this is shown in Fig. 5. The red ellipse is tangent to the boundary of the square at the four points of intersection. For ($\mathcal{Q}$nx)-points the same happens in higher dimension.

Since the ($\mathcal{Q}$qx) extreme points will be discussed in more detail, let us briefly describe the [$\mathcal{Q}$ei] facets. These elliptopes are visualized in Fig. 7, an enlarged version of the first panel in Fig. 3. Analytically, the elliptope, say the subset of correlations $c = (-1, x, y, z) \in \mathcal{Q}$, is described by the single inequality $1 - x^2 - y^2 - z^2 + 2xyz \geq 0$ in the cube; cf. [17, eqn (1.1)]. Since the pushout map restricts to $\mathcal{N}$-facets, it is the pushout of the $\mathcal{C}$-like tetrahedron that forms its skeleton. Indeed, the edges of $\mathcal{C}$ are marked by two of the c_{ij} being ± 1, and the other two equal up to a sign. This condition is invariant under pushout, so the edges of $\mathcal{C}$ are invariant as sets, but not pointwise fixed, and become exactly the [$\mathcal{Q}$ce]-edges of $\mathcal{Q}$.

How do all these pieces fit together? Once again this is readily answered by looking at the pushout identification of $\mathcal{Q}$ with $\mathcal{C}$. Consider the bicoloring of the facets of the cross polytope $\mathcal{C}$. The two colors distinguish CHSH and $\mathcal{N}$ types. Only tetrahedra of different types intersect in a surface, and each surface [$\mathcal{Q}$nx] is the intersection of a [$\mathcal{Q}$qx] and a [$\mathcal{Q}$ei]-set. The triangular surfaces ($\mathcal{Q}$nx) are thus faithfully portrayed in Fig. 7. The intersection of two [$\mathcal{Q}$qx]-surfaces is lower dimensional: If they are not disjoint opposites, they intersect in a straight edge [$\mathcal{Q}$ce].

In order to visualize the boundary structure we can use a *stereographic projection* from the origin. Each boundary point is first mapped to the line through the origin it generates, and then to the intersection of that line with a fixed reference hyperplane, to be identified with $\mathbb{R}^3$. This defines a rational map from the boundary of our convex body onto $\mathbb{R}^3$. It is 2-to-1, because it identifies points $\pm c$, but this hardly matters because this is a symmetry of $\mathcal{Q}$ and $\mathcal{C}$. If the reference hyperplane supports the body, then this will produce a local image of the boundary. Stereographic projection takes line segments to line segments, so the boundary of a polytope like $\mathcal{C}$ induces a subdivision of $\mathbb{R}^3$ into polyhedra. This is shown in the top row of Fig. 8, where the reference plane has been chosen as $\{c_{11} = 1\}$. Points with $c_{11} = 0$ are mapped to infinity, so facets containing such points are represented in two parts, connected via some infinite points,
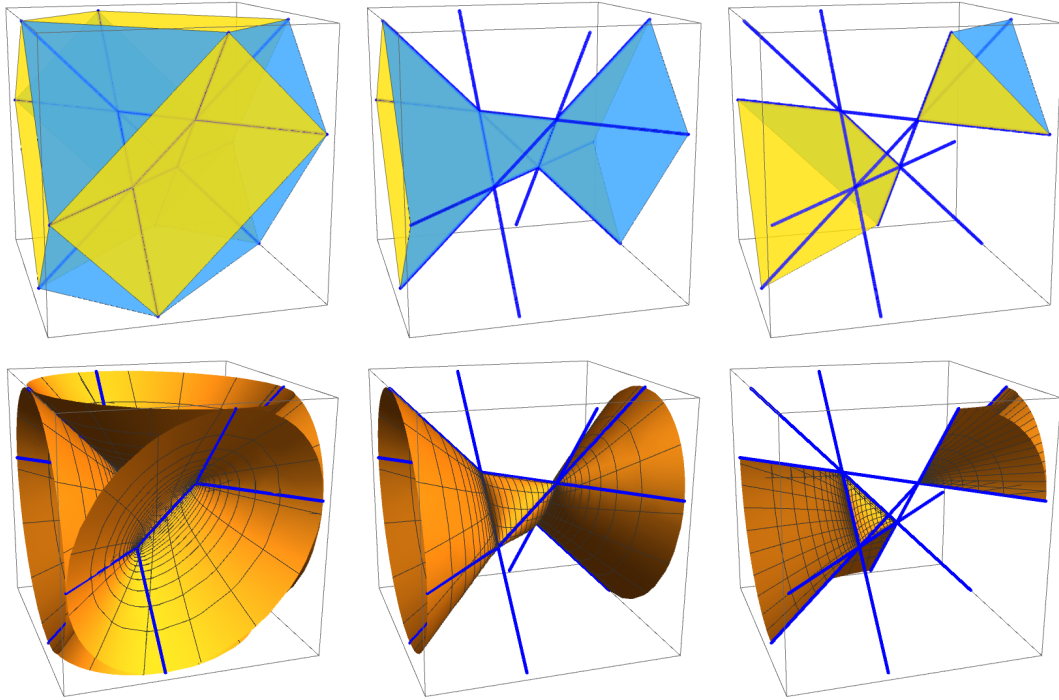
Figure 8: Stereographic projection of the boundaries of $\mathcal{C}$ (top row) and $\mathcal{Q}$ (bottom row). The common edges are shown as blue lines. The surfaces separate $\mathcal{N}$-facets from CHSH-facets. Their coloring for $\mathcal{C}$ corresponds to Fig. 2. For $\mathcal{Q}$ the surfaces are the boundary sets of type ($\mathcal{Q}$nx). Left panels: all boundaries. Center panels: The $\mathcal{N}$-face at the center, together with another $\mathcal{N}$-face. The latter is displayed in two pieces, connected via the plane at infinity. Right panels: a CHSH-face, resp. a ($\mathcal{Q}$qx) curved tetrahedron.

but forming a single polyhedron in projective geometry. This partitions $\mathbb{R}^3$ into 8 projective tetrahedra, all of which have the same four vertices. This reminds us that the "line segment between two given points" is intrinsically ambiguous in projective geometry. The term "projective polyhedron" is therefore often used for the whole tessellation, and not just for "connected region in projective space bounded by finitely many hyperplanes" as in this paragraph.

The resulting pictures are inside-out versions of *Schlegel diagrams* [16, Chapter 5], which represent 4-dimensional polytopes by stereographic projection from a point just outside a reference facet. When the projection point is close enough to that facet, the whole boundary is mapped to a polyhedral subdivision of the facet, thus avoiding infinite points and the identification of antipodes. The construction easily generalizes to other convex bodies. In this generalized setting convexity still guarantees that the ray from the projection point will cut the boundary in at most two points. But it may happen that one cannot arrange for one of these to be in the plane of the reference facet. Our body $\mathcal{Q}$ demonstrates this point. The only facets are $\mathcal{N}$ facets, and these are bounded by non-exposed extreme points, whose unique tangent plane is the plane of the reference facet. Therefore, no matter how close the projection point is chosen to the reference facet, the cone generated by the facet does not contain the whole body $\mathcal{Q}$. So the Schlegel map does not map $\partial\mathcal{Q}$ into the facet, and has non-trivial double images. Therefore we opted for the projection from the center, which is shown in the second row of Fig. 8.

Since the boundaries $\partial\mathcal{Q}$ and $\partial\mathcal{C}$ are identified via pushout, their stereographic projections are topologically equivalent partitions. Stereographic projection suggests another identification of $\partial\mathcal{C}$ and $\partial\mathcal{Q}$, namely by identifying points on the same ray through the origin. Such points are simply the same in Fig. 8, and that the stereographic projections of the boundaries are distinct shows the non-linearity of the pushout map. Indeed there are points c in a CHSH face, so that the multiple $\lambda c \in \partial\mathcal{Q}$ lies in an $\mathcal{N}$-face. Such c are readily found already in Fig. 2.

2.6 Curved tetrahedra

[Prop. 7](#) allows us to turn an affine parametrization of a CHSH-face into a trigonometric parametrization of a curved tetrahedron ($\mathcal{Q}$qx). For later purposes, we find cosines a bit more convenient than sines.

Proposition 8 (→*Sect. 5.1.4*) *The threefolds ($\mathcal{Q}$qx) of exposed extreme points on $\mathcal{Q}$ are parametrized by*

$$
\begin{aligned}
c = (c_{11}, c_{12}, c_{21}, c_{22}) &= (\cos\alpha, \cos\beta, \cos\gamma, \cos\delta) && \text{where} \\
\alpha + \beta + \gamma + \delta &= 0 \mod 2\pi && \text{and} \\
\Delta = \sin\alpha \cdot \sin\beta \cdot \sin\gamma \cdot \sin\delta &< 0.
\end{aligned}
\tag{16}
$$

The angle parameters can be taken as the triples (α, β, γ), with $\delta = -(\alpha + \beta + \gamma)$. In this 3-space, the sign of Δ marks a partition into two kinds of subsets: On the one hand, we have the curved tetrahedra with $\Delta < 0$ considered in [Prop. 8](#). A prototype which contains the CHSH-point $(\pi/4, \pi/4, \pi/4)$ is given by the conditions $\alpha, \beta, \gamma, \alpha + \beta + \gamma \in (0, \pi)$.

On the other hand, consider the angles with $\Delta > 0$. Adding multiples of π to any of α, β, γ (and hence implicitly to δ) corresponds to an even sign change on the c_{ij}, and hence a symmetry of $\mathcal{Q}$. Therefore, it suffices to consider the cube $(0, \pi)^3$. In this cube only $\sin\delta$ can be negative, so $\Delta > 0$ means $\alpha + \beta + \gamma \in (\pi, 2\pi)$. This is an octahedron, as shown in [Fig. 9](#). By taking cosines, these points end up in the interior of $\mathcal{Q}$.
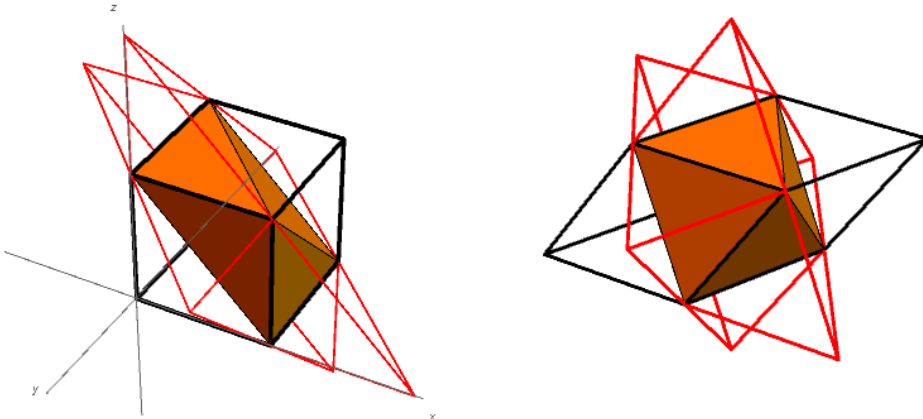
Figure 9: Left: the cube $(0, \pi)^3$ containing the octahedron given by $\alpha + \beta + \gamma \in (\pi, 2\pi)$, on which $\Delta > 0$. The (red and black) tetrahedra built on its faces have $\Delta < 0$, and are hence mapped to the curved tetrahedra ($\mathcal{Q}$qx) according to [Prop. 8](#). Right: an affine transformation of the left panel making the symmetry of permuting angles and the regularity of the tetrahedra and octahedra more evident.

Finally, note that the angle parameters (α, β, γ) with $\Delta = 0$ correspond to further boundary elements from [Prop. 7](#), as follows. The symmetries also help to reduce each of the classes in the following boundary version of the parametrization to a single case, which is readily checked.

Proposition 9 (→*Sect. 5.3.1*) *In the cosine parametrization of [Prop. 8](#), taking $\Delta = 0$ parametrizes further boundary strata of lower dimension. Specifically, we get points of type*

($\mathcal{Q}$cx) if and only if $\alpha, \beta, \gamma, \delta$ are all multiples of π,

($\mathcal{Q}$ce) if and only if exactly two of these angles are multiples of π, and

($\mathcal{Q}$nx) if and only if exactly one of these angles is a multiple of π.

2.7 Semialgebraic description

One possibility to decide quickly, for a given $c \in \mathbb{R}^4$, whether $c \in \mathcal{Q}$, is to apply the inverse pushout map, and to check whether the result lies in $\mathcal{C}$. This involves a transcendental function, and requires the checking of 16 linear inequalities. Here we consider an alternative, which only requires checking the positivity of two polynomials in c. In other words, we will describe our body $\mathcal{Q}$ as a semialgebraic set.

There is a standard method to obtain relevant polynomials from the parametrization given in Prop. 8. Namely, one represents each angle variable η by the point $(\cos\eta, \sin\eta)$ on the unit circle, i.e., one introduces new variables s_{ij} with $c_{ij}^2 + s_{ij}^2 = 1$, and expresses the constraint on the sum of angles by trigonometrically expanding. Then one eliminates the s_{ij}-variables. Computer algebra systems, such as Mathematica or Macaulay2 [47] handle such tasks routinely and, in this instance, in no time. The result is the identity $h(c) = 0$ with h the sextic polynomial in (19) below. But also the condition $\Delta < 0$ has to be transcribed, for which we use the following polynomial g, which on $(\mathcal{Q}\text{qx})$ satisfies $g(c) = \Delta$.

$$g(c) \;=\; 2 - (c_{11}^2 + c_{12}^2 + c_{21}^2 + c_{22}^2) + 2c_{11}c_{12}c_{21}c_{22}. \tag{17}$$

$$h(c) \;=\; 4(1 - c_{11}^2)(1 - c_{12}^2)(1 - c_{21}^2)(1 - c_{22}^2) - g(c)^2 \tag{18}$$

$$=\; 4(c_{11}c_{22} - c_{12}c_{21})(c_{11}c_{21} - c_{12}c_{22})(c_{11}c_{12} - c_{21}c_{22}) - \tag{19}$$
$$-(c_{11}+c_{12}-c_{21}-c_{22})(c_{11}-c_{12}+c_{21}-c_{22})(c_{11}-c_{12}-c_{21}+c_{22})(c_{11}+c_{12}+c_{21}+c_{22}).$$

We wrote two formulas for h, because (18) shows that h is invariant under the full symmetry group in Sect. 2.4, and (19) clarifies that the degree of h is six and not eight, as suggested by (18). Then we have:

Proposition 10 ($\rightarrow$Sect. 5.1.3) *A point c in the cube $\mathcal{N}$ lies in $\mathcal{Q}$ if and only if $h(c) \geq 0$ or $g(c) \geq 0$.*

While the polynomial h is an intrinsic feature of $\mathcal{Q}$, there is some freedom in the choice of g. Indeed, knowing a small piece of the boundary suffices to determine h. This is expressed by saying that h, together with the linear polynomials $1 \pm c_{ij}$ describe the *algebraic boundary* of $\mathcal{Q}$. At each boundary point of $\mathcal{Q}$ one of these polynomials vanishes. In algebraic geometry language [17, Chapter 2], the threefold $\{h(c) = 0\}$ is the *Zariski closure* of the curved tetrahedra in $(\mathcal{Q}\text{qx})$, or pieces thereof. This threefold has unbounded pieces outside the cube $\mathcal{N}$, but taking its convex hull after the intersection with $\mathcal{N}$ gives exactly $\mathcal{Q}$. This is visualized in Fig. 10 (left) which shows the surface $\{h(c) = 0\}$ in the 3-space $\{c_{12} - c_{21} = 0\}$. The unbounded pieces arise because the algebraic elimination process works just as well in the complex domain. So the circle $c^2 + s^2 = 1$, as a complex variety, also contains real points with imaginary s, corresponding to angles $\alpha = ir$ or $\alpha = \pi + ir$ with $r \in \mathbb{R}$, and hence $\cos\alpha = \pm\cosh r$ in Prop. 8.
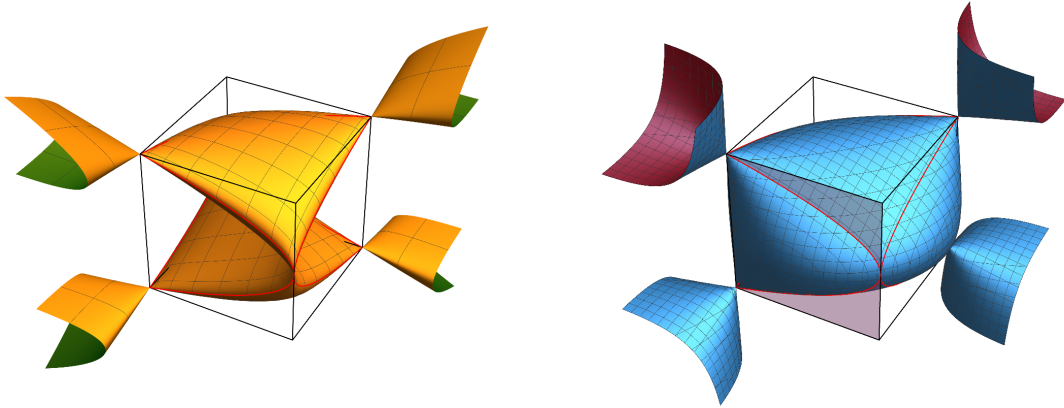
Figure 10: Inside the hyperplane $\{c_{12} = c_{21}\}$, we consider the two quartic surfaces $\{g = 0\}$ (right) and $\{(c_{11} - c_{22})^{-2}h = 0\}$ (left). The two surfaces intersect transversally in the red curves that are seen in the boundary of the cube.

What is the role of the second polynomial g? This polynomial is needed to make Prop. 10 true. Fig. 10 (left) shows the zero set of h, so h is negative on the outside of the yellow surface. This extends well into the cube, where $c \in \mathcal{Q}$, and even $c \in \mathcal{C}$, e.g., near the origin. Hence, "$c \in \mathcal{N}$ and $h(c) \geq 0$" would produce many false negatives. The disjunction with $g(c) \geq 0$ captures the convex hull of the threefold inside the cube $\mathcal{N}$. The surface defined by g in the hyperplane $\{c_{12} - c_{21} = 0\}$ is shown in Fig. 10 (right). Fig. 11 is a two-dimensional representation that shows the geometry of the relevant intersections.

We remark that more compact forms than the characterization by two polynomials can be given, if we allow the use of absolute values or roots. Such conditions can be converted to polynomial expressions.
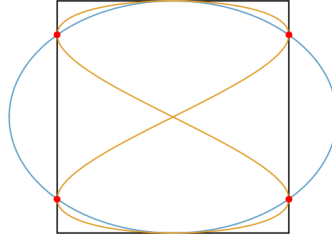
Figure 11: A slice that illustrates how the two surfaces in Fig. 10 intersect. The convex hull of the orange curve represents $\mathcal{Q}$. The disjunction $h(c) \geq 0$ *or* $g(c) \geq 0$ describes $\mathcal{Q}$. Note that $\mathcal{Q}$ is not a basic semialgebraic set, i.e., not a conjunction of polynomial inequalities.

However, they typically generate a case distinction, hence some overhead in the logical part of a semialgebraic description. For example, by taking a root in (18) and combining with Prop. 10, we can see that $c \in \mathcal{Q}$ is equivalent to $c \in \mathcal{N}$ together with the single inequality

$$g(c) \geq -2\sqrt{(1 - c_{11}^2)(1 - c_{12}^2)(1 - c_{21}^2)(1 - c_{22}^2)}. \tag{20}$$

The following reformulation, due to Landau [23], is not invariant under the full symmetry group of $\mathcal{Q}$:

$$\sqrt{(1 - c_{11}^2)(1 - c_{12}^2)} + \sqrt{(1 - c_{21}^2)(1 - c_{22}^2)} \geq |c_{11}c_{12} - c_{21}c_{22}|. \tag{21}$$

Note that these inequalities must be combined with the hypothesis $c \in \mathcal{N}$. This excludes unbounded solutions with a product of two negative factors under the square root.

2.8 Spectrahedral shadow

For any quantum correlations, given by a density operator ρ and observables A_1, A_2, B_1, B_2, and complex numbers $\xi_1, \ldots, \xi_4$, we consider the operator $X = \xi_1 A_1 + \xi_2 A_2 + \xi_3 B_1 + \xi_4 B_2$. Since $X^* X$ is positive semidefinite, we conclude that $\mathrm{tr}(\rho X^* X) = \sum_{\nu,\mu=1}^4 \overline{\xi_\nu} C_{\nu\mu} \xi_\mu \geq 0$, where we introduced the 4×4 matrix

$$C = (C_{\nu\mu}) = \begin{pmatrix} d_1 & u & c_{11} & c_{12} \\ \overline{u} & d_2 & c_{21} & c_{22} \\ c_{11} & c_{21} & d_3 & v \\ c_{12} & c_{22} & \overline{v} & d_4 \end{pmatrix}. \tag{22}$$

The entries other than c_{ij} are

$$u = \mathrm{tr}(\rho A_1 A_2), \qquad v = \mathrm{tr}(\rho B_1 B_2), \qquad \text{and} \quad d_1 = \mathrm{tr}(\rho A_1^2) \geq 0, \text{ etc.} \tag{23}$$

The positivity stated above is $C \geq 0$, our notation for C being positive semidefinite. The existence of u, v and d_i with $d_i^2 \leq 1$ making $C \geq 0$ is thus a necessary condition for $c \in \mathcal{Q}$. This is the bottom level of the semidefinite hierarchy [12] for quantum correlations. In the case at hand, the necessary condition is also sufficient, known since the time of Tsirelson [7]. We can further assume that u and v are real and that the diagonal entries are all 1.

Proposition 11 ($\rightarrow$*Sect. 5.1.1*) *A point c lies in the convex body $\mathcal{Q}$ if and only if there exist numbers $u, v \in \mathbb{R}$ such that $C \geq 0$ in (22) with $d_1 = d_2 = d_3 = d_4 = 1$.*

Hence, $\mathcal{Q}$ is characterized by a semidefinite matrix completion problem. This is essentially the completion problem for the 4-cycle, as discussed in [17, Example 12.16]. Our boundary polynomial $h(c)$ is obtained from the degree eight polynomial given there by setting the diagonal entries to be 1. The matrix inequality $C \geq 0$ defines a spectrahedron in $\mathbb{R}^6$, i.e., an intersection of the semidefinite matrix cone with an affine-linear space. Deleting the matrix entries u and v specifies a projection $\mathbb{R}^6 \to \mathbb{R}^4$. The correlation body $\mathcal{Q}$ is the image of the spectrahedron $\{C \geq 0\}$ under this projection. Thus, Prop. 11 furnishes an explicit realization of $\mathcal{Q}$ as a *spectrahedral shadow* [20].
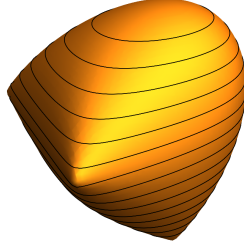
Figure 12: Nonuniqueness of matrix completion for a family of correlations $c = tc_{\text{CHSH}} + (1 - t)c_{\text{center}}$ with $c_{\text{center}} = (-1, 0, 0, 0)$ along the line segment from the center of an elliptope facet (top) to the CHSH-point (bottom). The horizontal cuts for fixed t (black meshes) represent the pairs (u, v) that make (22) positive semidefinite. These slices are 2-dimensional convex bodies that shrink to a point at both boundaries. The figure is a *quartic spectrahedron* [48].

A natural question to ask here is: How many completions can a correlation c have? Geometrically, this corresponds to studying the inverse images ("fibers") of the projection, that takes a $C \geq 0$ with unit diagonal to its upper right 2×2-submatrix $c \in \mathcal{Q}$. By definition, the set in the (u, v)-plane making $C \geq 0$ for given c is the intersection of an affine manifold with a positive definite cone: a spectrahedron. For example, Fig. 12 shows the union of these 2-dimensional fibers over a line that cuts through $\mathcal{Q}$. The following proposition establishes that the uniqueness of the completion problem (a one-point fiber) characterizes the boundary. Thus the rank of C can be seen as a property of $c \in \partial\mathcal{Q}$, and this turns out to distinguish different boundary elements.

Proposition 12 (→*Lem. 29* and *Sect. 5.3.1*)

(1) *The matrix completion problem has a unique solution (u, v) if and only if $c \in \partial\mathcal{Q}$.*

(2) *The resulting unique matrix C has rank 1 if c is of type (Qcx), it has rank 2 for types (Qce), (Qnx) and (Qqx), and it has rank 3 for type (Qei).*

(3) *The point c is in the interior (Qin) if and only if there is some completion with $\text{rank}\, C = 4$.*

We close with one remark regarding item (3). It is not true that *all* the completions C of a given interior point $c \in$ (Qin) have rank 4. For instance, the origin $c = 0 \in$(Qin) has among its completions the completion $C = \mathbb{1}$ of rank 4, but also the completion C with $u = v = 1$ of rank 2 (direct verification).

2.9 Volume

The volume of $\mathcal{Q}$ is a fundamental geometric invariant. It could be understood as the probability of quantum correlations in an ensemble, for which $c \in \mathcal{N}$ is distributed according to Lebesgue measure. This ensemble of generalized probabilistic theories has no operational meaning, so the volume has no direct physical relevance. However, the probabilistic interpretation suggests a way to compute it stochastically: The semialgebraic description gives us a fast way to decide whether $c \in \mathcal{Q}$, for points c in a random ensemble with each c_{ij} independent and equidistributed in $[-1, 1]$. A run of 10^6 samples led to

$$\frac{V(\mathcal{Q})}{V(\mathcal{N})} \approx 0.925898. \tag{24}$$

On account of $\sqrt{N}$-fluctuations, this can be expected to be accurate to within three digits.

On the other hand, we can compute the volume exactly, by integrating the pushout over $\mathcal{C}$. Since the pushout acts coordinatewise, the Jacobi matrix is diagonal and the functional determinant is readily determined. The resulting trigonometric integrals can be solved, giving the overall result

$$\frac{V(\mathcal{Q})}{V(\mathcal{N})} = \frac{3\pi^2}{2} \cdot \frac{1}{16} \approx 0.9252754126. \tag{25}$$

Similarly, the ratio $V(\mathcal{C})/V(\mathcal{N})$ can be estimated stochastically to be 0.666. Using the linear transformation $2H$ in (29), $V(\mathcal{C})$ is $\sqrt{\det((2H)^*(2H))} = 16$ times the volume of the 4-dimensional cross-polytope, defined as the convex hull of 8 points $(\pm 1, 0, 0, 0), (0, \pm 1, 0, 0), (0, 0, \pm 1, 0), (0, 0, 0, \pm 1)$ in $\mathbb{R}^4$. In general, the volume of the n-dimensional cross-polytope is $2^n/n!$, shown by induction from the observation that it equals 2^n times the volume of the standard n-simplex (the convex hull of the origin and standard basis of $\mathbb{R}^n$). Thus, $V(\mathcal{C}) = 2^5/3$ and we get exactly $V(\mathcal{C})/V(\mathcal{N}) = 2/3$ and

$$\frac{V(\mathcal{Q})}{V(\mathcal{C})} = \frac{3\pi^2}{2} \cdot \frac{3}{2^5} \quad \approx \quad 1.3879131189. \tag{26}$$

Our results agree with that of [49]. Also, these volumes give the probability ≈ 0.258609 on the task of sampling nonlocal quantum correlations $c \in \mathcal{Q} \setminus \mathcal{C}$, if one were to use the translationally invariant Lebegues measure to obtain a random point in $\mathcal{N}$. For this task, a better approach is clearly to change the measure to the unitarily invariant Haar measure, as studied in [50].

For the surface area, we get the volume of the $\mathcal{N}$-faces as the well-known elliptope volume $\pi^2/2$ [51]. For the volume of the curved tetrahedra (that is the one of the elliptope face, the pushout of the three dimensional tetrahedron) we did not find a closed expression. Testing the numerical value for being a simple fraction times a low power of π by continued fraction expansion also did not seem to give a simple expression. The ($\mathcal{Q}$nx) boundaries are directly expressed by the surface area of the elliptope. This area is known to be 5π, by a direct calculation found on `math.stackexchange.com`.

3 Description of the Dual Body

The polar $\mathcal{K}^\circ = \{f \mid f \cdot c \le 1,\ c \in \mathcal{K}\}$ of a convex body $\mathcal{K}$ provides the description of $\mathcal{K}$ by the affine inequalities it satisfies. Since $\mathcal{K}^{\circ\circ} = \mathcal{K}$, by [52, Thm. IV.1.5], this is a symmetric relation. We could ask all the questions we studied so far about the three bodies $\mathcal{C} \subset \mathcal{Q} \subset \mathcal{N}$ also about their polars. For the polars the inclusion is reversed, so $\mathcal{N}^\circ \subset \mathcal{Q}^\circ \subset \mathcal{C}^\circ$. The big surprise, which is a rather special feature of the minimal case, is that this dual chain of inclusions is essentially *the same* as the original chain. We will spell this out in detail. For now it just means the good news that much of the work is already done.

3.1 The duality transform

We first noticed the duality in the polytopes $\mathcal{C} \subset \mathcal{N}$ from the observation that their face counts by dimension (the f-vectors) are reversals of each other. Strengthening this to an isomorphism $\mathcal{C} \cong \mathcal{N}^\circ$ goes as follows. We start from the inequalities describing $\mathcal{N}$. These come from the 8 vertices of $\mathcal{N}^\circ$, which are

$$\pm (1, 0, 0, 0), \quad \pm(0, 1, 0, 0), \quad \pm(0, 0, 1, 0), \quad \pm(0, 0, 0, 1). \tag{27}$$

These have to be identified with the vertices of $\mathcal{C}$, i.e., the 8 even vertices of $\mathcal{N}$ itself. They are

$$\pm (1, 1, 1, 1), \quad \pm(1, -1, 1, -1), \quad \pm(1, 1, -1, -1), \quad \pm(1, -1, -1, 1). \tag{28}$$

The following transformation H maps the points in (27) to those in (28). So we get $\mathcal{C} = 2H\mathcal{N}^\circ$ with

$$H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{29}$$

Here we included the factor $1/2$ so that $H^2 = \mathbb{1}$. Since $H^* = H$, this matrix is then also unitary, i.e., a Hadamard matrix [53] (note different conventions for the normalization of such matrices though). Recall two basic properties of polar duality: $(s\mathcal{K})^\circ = \mathcal{K}^\circ/s$ for $s \ne 0$ and $(U\mathcal{K})^\circ = U\mathcal{K}^\circ$ for unitary U. This makes it easy to write down the consequences of $\mathcal{C} = 2H\mathcal{N}^\circ$ from dualization or multiplication with H:

$$\mathcal{N}^\circ = \tfrac{1}{2}H\mathcal{C} \qquad \text{and} \qquad \mathcal{C}^\circ = \tfrac{1}{2}H\mathcal{N}. \tag{30}$$

To visualize this duality, consider the left panel of Fig. 13. Since the section with the hyperplane $\{c_{12} = c_{21}\}$ is also a projection, and duality swaps projection and intersection operations, this 3-dimensional
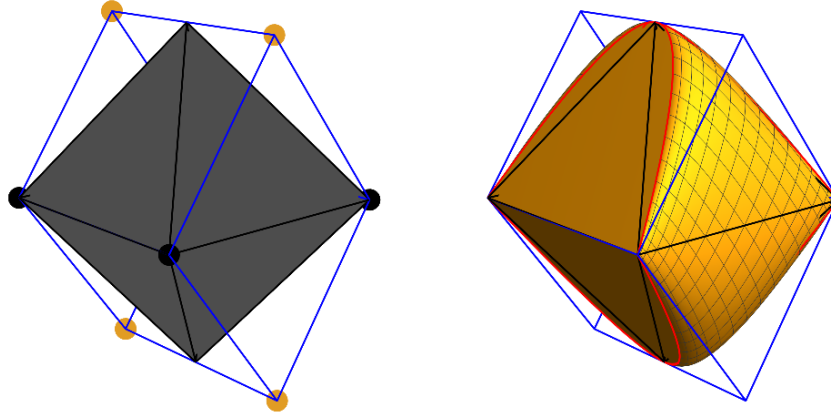
Figure 13: Polar duals for the Alice-Bob symmetric sections shown in Fig. 2. The marked vertices of $\mathcal{C}^\circ$ (blue cube frame) correspond to the facets of $\mathcal{C}$ in Fig. 2. The figure of $\mathcal{Q}^\circ$ (right panel) is an affine transformation of $\mathcal{Q}$ in Fig. 2. This expresses the self-duality.

picture faithfully represents the 4-dimensional polarity relations. The outer blue frame represents $\mathcal{C}^\circ$, the dual of the inner frame in Fig. 2 (Left). It is a cube whose vertices correspond to the facets of $\mathcal{C}$. They can thus correspond either to a CHSH-facet (marked in yellow) or to a $\mathcal{N}$-facet (marked in black). Overall, the figure looks like a rotation of its counterpart in Fig. 2. In 4 dimensions the required H is exactly an orthogonal reflection. In the 3-dimensional section it is still a submatrix of a rotation, and looks like a rotation because human 3D perception is highly capable of ignoring uneven affine stretching.

The right panel in Fig. 13 shows the pertinent section of the dual body $\mathcal{Q}^\circ$. We can draw it using the parametrized points f from Prop. 14. This mimics the right panel of Fig. 2, by the same transformation as the one used for the polytopes. Indeed, this is true exactly, also for the full 4-dimensional body:

Proposition 13 (→Sect. 5.2) $\mathcal{Q}^\circ = \frac{1}{2}H\mathcal{Q}$.

This is Thm. 3, but with the matrix H spelled out. The linear transformation H is far from unique. Indeed, if S_1, S_2 are matrices representing any of the symmetries from Sect. 2.4, then so are their transposes. Hence $H' = S_1 H S_2$, incidentally always again a Hadamard matrix, also maps the inclusion chain to its dual. Note that $S \mapsto S' = HSH^{-1}$ is an automorphism of the symmetry group which changes the semidirect product decomposition, so multiplication by an even number of signs can become a permutation and conversely. In fact, H is just the Fourier transform in the discrete phase space representation mentioned in Sect. 2.4, and in this picture it is the swap between position shifts and momentum shifts.

In the terminology of axiomatic quantum mechanics, this form of self-duality of a convex set is called "weak self-duality" [54], as opposed to stronger forms with a canonical isomorphism between the set and its dual, that is characteristic for Jordan algebra state spaces and in particular the quantum state space. Can one strengthen Prop. 13 in that direction? Indeed, we already have a canonical mapping taking each point c of a ($\mathcal{Q}$qx) patch to the unique maximizer f, via Prop. 8 and Prop. 14. By multiplying H with a symmetry of $\mathcal{Q}$ we can achieve that it takes the patch of c to the patch of f, but can we do it for all patches simultaneously? The answer is no: A map with that property would have to commute with all symmetries. Since our representation of the group G on $\mathbb{R}^4$ is irreducible, we would conclude that H is a multiple of the identity. Another context of interest are normed spaces: Since $-\mathcal{Q} = \mathcal{Q}$, our convex body $\mathcal{Q}$ is the unit ball of a norm in $\mathbb{R}^4$ and the dual normed space has unit ball $\mathcal{Q}^\circ$. So we have an example of a normed space that is isomorphic to its dual, a subject studied more generally, e.g., in [55].

After the completion of this work, we became aware of T. Fritz's results [27] which extend the duality of $\mathcal{C}$ and $\mathcal{N}$ to many parties and shows the impossibility of this duality for $M, K > 2$, i.e. scenarios with more than two measurements or two outcomes. There it was stated that the self-duality of $\mathcal{Q}$ was also known to C. Palazuelos and I. Villanueva (in a private communication), and that self-duality fails for the analogously defined three-partite body, but leaving the possibility for $N > 3$.

3.2 Parametrized extreme points of $\mathcal{Q}°$

The boundary patches ($\mathcal{Q}$qx) of exposed extreme points have a unique maximizing functional $f \in \mathcal{Q}°$. The parametrization by angles can be taken over directly.

Proposition 14 (→*Sect. 5.3.2*) *Let* $\alpha, \beta, \gamma, \delta$ *and* $c = (\cos \alpha, \cos \beta, \cos \gamma, \cos \delta)$ *satisfy the conditions of* *Prop. 8. Define*

$$f = (f_{11}, f_{12}, f_{21}, f_{22}) = \frac{1}{K} \left(\frac{1}{\sin \alpha}, \frac{1}{\sin \beta}, \frac{1}{\sin \gamma}, \frac{1}{\sin \delta} \right), \tag{31}$$

where $K = \cot \alpha + \cot \beta + \cot \gamma + \cot \delta$. *Then* $f \cdot c' \leq 1$ *for all* $c' \in \mathcal{Q}$ *with equality if and only if* $c' = c$. *Moreover, the vector* f *is uniquely determined by this property.*

Applying the duality transform to the point f in (31) gives again a point $2Hf \in \mathcal{Q}$ of type ($\mathcal{Q}$qx), which in turn can be parametrized by angles. The resulting map Φ from one tetrahedron of angles to another expresses the duality of boundary points.

For a concrete computation let T be the tetrahedron defined by $\alpha, \beta, \gamma, -\delta = \alpha + \beta + \gamma \in (0, \pi)$. Denote $\theta = (\alpha, \beta, \gamma, \delta)$ and write $c(\theta)$ and $f(\theta)$ for the images in Prop. 8 and Prop. 14. We obtain a self-map $\Phi : T \to T$ with the property

$$2H f(\theta) = c(\Phi(\theta)). \tag{32}$$

By definition, this map will commute with the permutations of vertices of T, which extend to symmetries of $\mathcal{Q}$. By self-duality it is also its own inverse. This map is visualized in Fig. 14.

By symmetry, these properties uniquely fix the map also for other ($\mathcal{Q}$qx)-patches. When doing this concretely, one has to observe that whereas the association of f with the unique maximizer c is a property of $\mathcal{Q}$, the concrete parametrization of the tetrahedra involves a convention, and depends on the choice of self-duality operator H. Therefore in solving (32) for $\Phi(\theta)$, on any of the tetrahedra in Fig. 9, one has to carefully pick the branches of the arccos function.
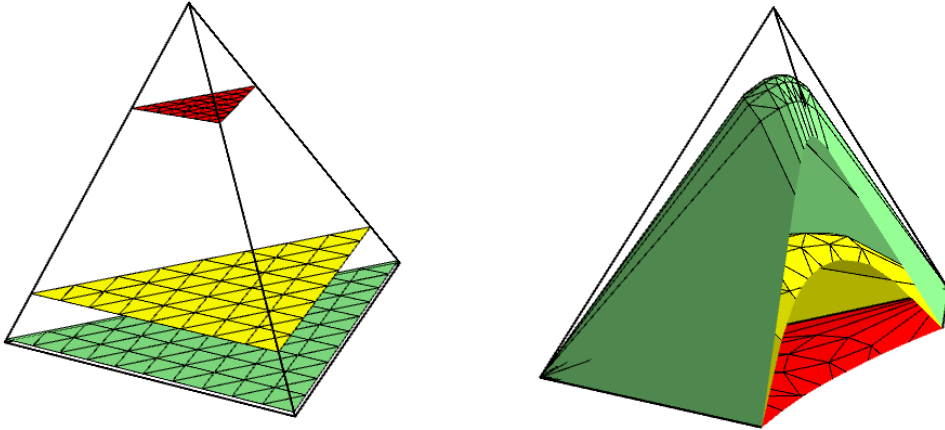
Figure 14: The map Φ from the tetrahedron T to itself: The triangular meshes on the left are mapped to the surfaces on the right. The figure on the right has been truncated so that the image surfaces can be seen. Since Φ commutes with vertex permutations, analogous surfaces can be drawn between any tetrahedron face and the opposing vertex. Since Φ^2 is the identity, the diagrams can also be read from right to left.

The map Φ is continuous and even analytic on the open tetrahedron. But it does not have a continuous extension to the closure of the tetrahedron. Indeed, a glance at (31) shows that when one of the angles in θ goes to zero, and the others to values not in $\{0, \pi\}$, the image $\Phi(\theta)$ approaches the opposite vertex. Hence the whole open part of the bottom face on the left goes to a single point. This is evident from Fig. 14 in the form that most of the triangles in the evenly spaced triangulation close to the base triangle end up close to the top vertex. Similarly, when θ approaches a point on the edge, the limit of $\Phi(\theta)$ depends on the direction from which the edge is approached.

3.3 Dualized descriptions

We can now apply the duality transform to each of the previous subsections to get analogues for $\mathcal{Q}^\circ$ of all the statements made about $\mathcal{Q}$. There is no simple analogue of the pushout. The cosine parametrization of the curved tetrahedra was already given an analogue in Prop. 14 (not via duality transform).

Consider the polynomials (17) and (19) of the semialgebraic description. Since $f = (f_{11}, f_{12}, f_{21}, f_{22}) \in \mathcal{Q}^\circ$ is equivalent to $2Hf \in \mathcal{Q}$, we need to consider these polynomials after substituting $c \mapsto 2Hf$. Note that such a substitution takes polynomials which are invariant under the symmetry group to polynomials with the same property. Moreover, by linearity of the substitution, homogeneous polynomials of some degree go to homogeneous polynomials of the same degree. This constrains the number of polynomials we need to consider. The invariant polynomials of degree two are proportional to $|c|^2 = c_{11}^2 + c_{12}^2 + c_{21}^2 + c_{22}^2$, and since H is orthogonal, this goes to itself under substitution. Among the quartics we need to consider the product $p(c) = c_{11}c_{12}c_{21}c_{22}$ that already appeared in Thm. 2. Under substitution it becomes

$$q(f) = p(2Hf) = (f_{11}+f_{12}+f_{21}+f_{22})(f_{11}-f_{12}+f_{21}-f_{22})(f_{11}+f_{12}-f_{21}-f_{22})(f_{11}-f_{12}-f_{21}+f_{22}). \quad (33)$$

This is the quartic part in (19). The sextic part of h is the polynomial k from Thm. 2. This is self-dual in the sense that $k(2Hf) = 64k(f)$. With these building blocks, the polynomials describing $\mathcal{Q}$ and $\mathcal{Q}^\circ$ are

$$
\begin{aligned}
h(c) &= 4k(c) - q(c), & h^\circ(f) &:= \tfrac{1}{256}\, h(2Hf) &= k(f) - p(f), \\
g(c) &= 2 - |c|^2 + 2p(c), & g^\circ(f) &:= \tfrac{1}{2}\, g(2Hf) &= 1 - 2|f|^2 + q(f).
\end{aligned}
\quad (34)
$$

We conclude that $f \in \mathcal{Q}^\circ$ if and only if $2Hf \in \mathcal{N}$ and ($g^\circ(f) \geq 0$ or $h^\circ(f) \geq 0$).

Describing $\mathcal{Q}^\circ$ as a spectrahedral shadow is done in general by the dual semidefinite hierarchy [26]. Indeed, the dual of a spectrahedral shadow is again of this form [18, Remark 5.43]. This holds because the operations of linear section and projection change roles under dualization, and the semidefinite cone is anyhow self-dual. In terms of matrix completion problems, where the primal matrix has unspecified entries (a subspace constraint), the dual matrix has zeros (resulting from the dual projection). In the case at hand, the unspecified entries u, v in C become zeros in the dual matrix, which we call F. The condition that the diagonal entries of C are 1 dualizes to constraint on the trace of F. This gives:

Proposition 15 ($\rightarrow$ *Sect. 5.2*) *A point $f = (f_{11}, f_{12}, f_{21}, f_{22})$ lies in the dual body $\mathcal{Q}^\circ$ if and only if there exist nonnegative real numbers p_1, p_2, p_3, p_4 with $\sum_{i=1}^4 p_i = 2$ such that*

$$
F = \begin{pmatrix}
p_1 & 0 & -f_{11} & -f_{12} \\
0 & p_2 & -f_{21} & -f_{22} \\
-f_{11} & -f_{21} & p_3 & 0 \\
-f_{12} & -f_{22} & 0 & p_4
\end{pmatrix} \geq 0. \quad (35)
$$

Moreover, there exists a completion satisfying the above constraints, and additionally $p_1 + p_2 = p_3 + p_4 = 1$. This condition is automatically satisfied for all boundary points.

Indeed, one checks that $\operatorname{tr} CF = 2 - 2f \cdot c$ holds for C from (22), so $\operatorname{tr} CF \geq 0$ is equivalent to $f \cdot c \leq 1$.

3.4 The normal cycle

The definition of the polar suggests to look at the *incidence relation* between points $c \in \mathcal{Q}$ and $f \in \mathcal{Q}^\circ$ for which the inequality $c \cdot f \leq 1$ is tight. For a fixed f, this naturally answers the question about what correlation maximizes this (Bell) inequality, and for a fixed c, the question which (Bell) inequality contain this as a maximizer. The resulting set is called the *normal cycle* [45, 46].

Given any convex body $\mathcal{K}$ in $\mathbb{R}^d$, which contains the origin in its interior, the normal cycle is defined as

$$\mathbf{N}(\mathcal{K}) = \left\{ (c, f) \in \partial\mathcal{K} \times \partial\mathcal{K}^\circ \mid c \cdot f = 1 \right\}. \quad (36)$$

This integrates $\mathcal{K}$ and $\mathcal{K}^\circ$ into a single structure, but it is useful far beyond this role. Importantly for our project, it gives a unified description of curved manifolds and polyhedral kinks, both of which are features of the correlation body $\mathcal{Q}$. It appears that this structure is not so well known in the quantum community. Therefore we begin with a brief description for an arbitrary $\mathcal{K}$ before specializing to $\mathcal{Q}$.

Fixing c to range over a subset $A \subset \partial\mathcal{K}$ leaves f to range over a closed face of $\mathcal{K}^\circ$. We denote by $A^\perp = \{f \in \mathcal{K}^\circ \mid \forall c \in A : c \cdot f = 1\}$ the set incident to A. We use the orthogonality symbol, and call $A^\perp$ the face orthogonal to A, although the relation is not given by the vanishing of a scalar product, unless we work in projective geometry, with homogenous coordinates and cones instead of convex sets (see [46]). The relation behaves in many ways like an orthogonality relation: Since $A \subset B$ implies $B^\perp \subset A^\perp$, and $A \subset B^\perp \Leftrightarrow B \subset A^\perp$, the map $A \mapsto (A^\perp)^\perp$ is a closure operation, taking A to the smallest face of the form $B^\perp$ containing it. This implies $A^{\perp\perp\perp} = A^\perp$. An *exposed face* is by definition a set of the form $\{x\}^\perp$.

Let us look at the two extreme cases of convex sets: First, we have strictly convex sets with smooth boundary whose only faces are exposed singletons $\{c\}$. Here, $\mathbf{N}(\mathcal{K})$ is the graph of a homeomorphic identification of $\partial\mathcal{K}$ with $\partial\mathcal{K}^\circ$. At each point we can introduce coordinates so that $\partial\mathcal{K}$ is the graph of a convex function. To second order it is given near c by a quadratic form, containing the curvature information. Dually, $\partial\mathcal{K}^\circ$ is given near f by the Legendre transform, hence the inverse quadratic form. Physicists are familiar with this reciprocity from the kinetic energy forms of Lagrange and Hamilton mechanics. In the limit, where curvature goes to zero in some directions, the dual curvature form diverges, corresponding to kinks of the dual manifold. Carrying this further, one gets to a situation where all curvature is concentrated on lower dimensional manifolds. This happens for polytopes.

For a polytope $\mathcal{K}$, the lattice of closed faces is neatly ordered by dimension, and $A \mapsto A^\perp$ is an order reversing bijection of face lattices. Although the normal cycle is far from being a convex set, given that $c \cdot f = 1$ is nonlinear, for every k-dimensional face F, the set $F \times F^\perp \subset \mathbf{N}(\mathcal{K})$ is a polytope of dimension $k + (d - k - 1) = d - 1$. Consider the 4-cube $\mathcal{N}$ and the demicube $\mathcal{C} = \mathcal{N}^\circ$. Their common normal cycle $\mathbf{N}(\mathcal{N}) = \mathbf{N}(\mathcal{C})$ consists of 80 strata, one for each of the $8 + 24 + 32 + 16$ pairs $(F, F^\perp)$, where $F \subset \partial\mathcal{C}$ and $F^\perp \subset \partial\mathcal{N}$ are faces. For instance, if $\dim(F) = 2$ then $\dim(F^\perp) = 1$ and $F \times F^\perp$ is a triangular prism.

Let us clarify the word *strata*. Consider an arbitrary semialgebraic set S. As a consequence of the Cylindrical Algebraic Decomposition (see, e.g., [56, Theorem 2.3.6]), the set S can be decomposed as a finite disjoint union of strata $S = \cup_{i=1}^N C_i$ with $\dim C_i = d_i$. Each stratum C_i is semialgebraically homeomorphic to $(0, 1)^{d_i}$. Moreover, the closure of C_i in S is given by the union of C_i with some other C_j such that $d_j < d_i$. Note that the decomposition of S into these strata is far from unique.

The power of the normal cycle lies in the uniform treatment covering the whole range of convex bodies from polytopes to smooth. Indeed, for any compact convex d-dimensional set $\mathcal{K}$ containing the origin in its interior, $\mathbf{N}(\mathcal{K})$ is always a $(d - 1)$-dimensional (Lipschitz Legendrian) submanifold of $\mathbb{R}^{2d}$ [57]. Moreover, the map $\mathcal{K} \mapsto \mathbf{N}(\mathcal{K})$ is continuous in the Hausdorff metric for sets. This makes the normal cycle a remarkably stable structure under approximations either by smooth manifolds or by polytopes.

The normal cycle plays the role of the normal bundle for more general geometric objects. It was defined by Federer [58] for sets of positive reach. These include convex bodies but also much crazier sets. It is an important tool from geometric measure theory, used for defining curvature measures [59, 60]. This is related to the classic result of Steiner, who noted that the volume of the smooth approximation to a body, which one gets as the union of all balls of small radius r centered on the body, is a polynomial in r, whose coefficients relate to curvature of different dimensionality. On the other hand, stable polyhedral approximations are needed in visualization, computer graphics and computational anatomy (see [61, 62, 63]). Recently, the normal cycle has also emerged as a key player in convex algebraic geometry [45, 46].

If a convex body $\mathcal{K} \subset \mathbb{R}^d$ is semialgebraic, then its normal cycle $\mathbf{N}(\mathcal{K})$ is semialgebraic as well, by [46, Theorem 1.7]. Moreover, $\mathbf{N}(\mathcal{K})$ admits a finite semialgebraic stratification whose top-dimensional strata are $(d - 1)$-dimensional. To recognize the nonlinear nature of the normal cycle, we also introduce the *algebraic normal cycle* $\overline{\mathbf{N}}(\mathcal{K})$. This is, by definition, the Zariski closure [64] of the normal cycle. It is a $(d - 1)$-dimensional subvariety [64] of the complex space $\mathbb{C}^{2d}$, modeled by conormal varieties as in [46, Section 2]. The radical ideal [64] of the algebraic normal cycle is the intersection of the prime ideals [64] associated to the various strata. If $\mathcal{K}$ is a polytope then each such prime ideal is generated by the linear polynomials in c that vanish on F, the linear polynomials in f that vanish on $F^\perp$, plus one bilinear polynomial $c \cdot f - 1$.

Our goal is to describe the normal cycle $\mathbf{N}(\mathcal{Q})$ of the correlation body $\mathcal{Q}$. We describe a stratification of $\mathbf{N}(\mathcal{Q})$ that mirrors the stratification of $\mathcal{Q}$ in Prop. 7. The symbol $(\mathcal{Q}nn,mm)$ will represent the set of points (c, f) in $\mathbf{N}(\mathcal{Q})$ such that $c \in (\mathcal{Q}nn)$ and $f \in (\mathcal{Q}mm)$, for the families from Prop. 7.

Proposition 16 *The normal cycle $\mathbf{N}(\mathcal{Q})$ is divided into $24 = 8 + 8 + 8$ strata of dimension 3 whose types are $(\mathcal{Q}qx,qx)$, $(\mathcal{Q}ei,cx)$, $(\mathcal{Q}cx,ei)$. These threefolds are separated by $88 = 32 + 32 + 24$ surfaces $(\mathcal{Q}nx,cx)$, $(\mathcal{Q}cx,nx)$, $(\mathcal{Q}ce,ce)$. The eight strata of type $(\mathcal{Q}qx,qx)$ belong to the same irreducible component of the*

algebraic normal cycle $\overline{\mathbf{N}(\mathcal{Q})}$, *so the radical ideal of* $\overline{\mathbf{N}(\mathcal{Q})}$ *is the intersection of* $17 = 1+8+8$ *prime ideals.*

All these features are made more explicit in Table 1. The labels refer to the strata of $\partial\mathcal{Q}$ (cf. Prop. 7).

c is a point of type	$(\mathcal{Q}\text{qx})$	$(\mathcal{Q}\text{cx})$	$(\mathcal{Q}\text{ei})$	$(\mathcal{Q}\text{ce})$	$(\mathcal{Q}\text{nx})$
$\{c\}^{\perp}$ is a set of type	$\{f\}, f \in(\mathcal{Q}\text{qx})$	$[\mathcal{Q}\text{ei}]$	$(\mathcal{Q}\text{cx})$	$[\mathcal{Q}\text{ce}]$	$(\mathcal{Q}\text{cx})$
$\{c\}^{\perp\perp}$ is a set of type	$\{c\}$	$\{c\}$	$[\mathcal{Q}\text{ei}]$	$[\mathcal{Q}\text{ce}]$	$[\mathcal{Q}\text{ei}]$
$\dim\{c\}^{\perp\perp}$	0	0	3	1	3
dim of face generated by c	0	0	3	1	0
$\dim\{c\}^{\perp}$	0	3	0	1	0
dim of manifold of such faces	3	0	0	0	2
sum of these dimensions	3	3	3	2	2
number of open strata in $\mathbf{N}(\mathcal{Q})$	8	8	8	24	32
irreducible components in $\overline{\mathbf{N}(\mathcal{Q})}$	1	8	8	0	0

Table 1: Classification of boundary points $c \in \partial\mathcal{Q}$, in the notation of Prop. 7, and what they correspond to in the normal cycle $\mathbf{N}(\mathcal{Q})$. The first three columns give the full-dimensional strata of $\mathbf{N}(\mathcal{Q})$. The last two columns are two of the three strata of dimension 2. The fact that the stratum $(\mathcal{Q}\text{cx,nx})$ does not appear here reflects the non-exposed nature of $(\mathcal{Q}\text{nx})$.

The extreme points $(\mathcal{Q}\text{qx})$ and their duals are both zero dimensional, hence maximally violate the typical counts for dual faces of polytopes. This is made up for by having a manifold of such points, so the local dimension of $\mathbf{N}(\mathcal{Q})$ is still $d - 1 = 3$. It is also clear, from the pushout transformation, that a tradeoff between manifold dimension and the dimensions of individual face pairs must be possible.

We now briefly discuss the strata $(\mathcal{Q}\text{ce})$ and $(\mathcal{Q}\text{nx})$ in the fourth and fifth column of Table 1. These are surfaces in the threefold $\mathbf{N}(\mathcal{Q})$. Points c on the surfaces $(\mathcal{Q}\text{nx})$ are supported only by the linear functional that supports the entire elliptope, which is $\{c\}^{\perp\perp}$. Hence there are 32 surfaces $(\mathcal{Q}\text{nx,cx})$ in $\mathbf{N}(\mathcal{Q})$. Dually, we also get 32 surfaces of type $(\mathcal{Q}\text{cx,nx})$. These do not appear in Table 1 because the faces of type $(\mathcal{Q}\text{nx})$ are not exposed and thus cannot be realized as $\{f\}^{\perp}$. This feature is highlighted by the jump in the dimension of $\{c\}^{\perp\perp}$ for $c \in(\mathcal{Q}\text{nx})$. All 64 surfaces arise as the intersection of the closure of $(\mathcal{Q}\text{qx,qx})$ with the closure of a stratum $(\mathcal{Q}\text{ei,cx})$ or $(\mathcal{Q}\text{cx,ei})$. Each intersection produces four such surfaces.

The exposed edges $(\mathcal{Q}\text{ce})$ of $\mathcal{Q}$ are supported by one-dimensional families of normal directions. These are the exposed edges $(\mathcal{Q}\text{ce})$ on $\mathcal{Q}^{\circ}$. We therefore have 24 squares of type $(\mathcal{Q}\text{ce,ce})$ in $\mathbf{N}(\mathcal{Q})$. Each square separates two 3-dimensional strata of type $(\mathcal{Q}\text{ei,cx})$ and $(\mathcal{Q}\text{cx,ei})$. In addition to the 64 curved triangles of type $(\mathcal{Q}\text{nx,cx})$ or $(\mathcal{Q}\text{cx,nx})$, this accounts for all 2-dimensional cells in our stratification of $\mathbf{N}(\mathcal{Q})$.

The 3-dimensional strata of $\mathbf{N}(\mathcal{Q})$ give the irreducible components of the algebraic normal cycle $\overline{\mathbf{N}(\mathcal{Q})}$. We begin with the most nonlinear stratum, denoted $(\mathcal{Q}\text{qx,qx})$. This stratum is characterized by Prop. 8 and Prop. 14. It is parametrized by angles $\alpha, \beta, \gamma, \delta$ that add up to 0 modulo 2π, and it consists of pairs (c, f) where c satisfies (16) and f satisfies (31). Its Zariski closure is an irreducible threefold in $\mathbb{C}^8$. Its prime ideal is generated by 17 polynomials. The first three of these 17 generators are familiar:

$$\ell = c_{11}f_{11} + c_{12}f_{12} + c_{21}f_{21} + c_{22}f_{22} - 1,$$
$$h = 4(c_{11}c_{22} - c_{12}c_{21})(c_{11}c_{21} - c_{12}c_{22})(c_{11}c_{12} - c_{21}c_{22})$$
$$\quad -(c_{11}+c_{12}-c_{21}-c_{22})(c_{11}-c_{12}+c_{21}-c_{22})(c_{11}-c_{12}-c_{21}+c_{22})(c_{11}+c_{12}+c_{21}+c_{22}),$$
$$h^{\circ} = f_{11}f_{12}f_{21}f_{22} - (f_{11}f_{22}-f_{12}f_{21})(f_{11}f_{21}-f_{12}f_{22})(f_{11}f_{12}-f_{21}f_{22}).$$

The remaining 14 generators of our prime ideal are the following polynomials:

$$c_{11}^2 f_{11}^2 - c_{22}^2 f_{22}^2 - f_{11}^2 + f_{22}^2,$$
$$c_{21} f_{11} f_{12} f_{21} + c_{22} f_{11} f_{12} f_{22} + c_{11} f_{11} f_{21} f_{22} + c_{12} f_{12} f_{21} f_{22},$$
$$c_{11}^2 f_{11} f_{12} - c_{21}^2 f_{21} f_{22} - c_{12} c_{21} f_{12} f_{22} + c_{11} c_{22} f_{12} f_{22} - f_{11} f_{12} + f_{21} f_{22},$$
$$c_{11}^2 f_{11} f_{21} - c_{12}^2 f_{12} f_{22} - c_{12} c_{21} f_{21} f_{22} + c_{11} c_{22} f_{21} f_{22} - f_{11} f_{21} + f_{12} f_{22},$$
$$c_{12}^2 f_{11} f_{12} - c_{21}^2 f_{21} f_{22} - c_{11} c_{21} f_{11} f_{22} + c_{12} c_{22} f_{11} f_{22} - f_{11} f_{12} + f_{21} f_{22},$$
$$c_{12}^2 f_{12} f_{21} - c_{11}^2 f_{11} f_{22} - c_{11} c_{21} f_{21} f_{22} + c_{12} c_{22} f_{21} f_{22} - f_{12} f_{21} + f_{11} f_{22},$$
$$c_{21}^2 f_{11} f_{21} - c_{12}^2 f_{12} f_{22} - c_{11} c_{12} f_{11} f_{22} + c_{21} c_{22} f_{11} f_{22} - f_{11} f_{21} + f_{12} f_{22},$$
$$c_{21}^2 f_{12} f_{21} - c_{11}^2 f_{11} f_{22} - c_{11} c_{12} f_{12} f_{22} + c_{21} c_{22} f_{12} f_{22} - f_{12} f_{21} + f_{11} f_{22},$$
$$(c_{11} c_{12}^2 + c_{11} c_{21}^2 + c_{11} c_{22}^2 - 2 c_{12} c_{21} c_{22}) f_{11} + c_{12}^3 f_{12} + c_{21}^3 f_{21} + c_{22}^3 f_{22} - 1,$$
$$c_{11} c_{12} f_{12} f_{21} - c_{21} c_{22} f_{12} f_{21} + c_{12} c_{21} f_{21} f_{22} - c_{11} c_{22} f_{21} f_{22} + c_{12}^2 f_{12} f_{22} - c_{22}^2 f_{12} f_{22},$$
$$c_{12} c_{21} f_{11} f_{21} - c_{11} c_{22} f_{11} f_{21} + c_{11} c_{21} f_{11} f_{22} - c_{12} c_{22} f_{11} f_{22} + c_{21}^2 f_{21} f_{22} - c_{22}^2 f_{21} f_{22},$$
$$c_{12} c_{21} f_{11} f_{12} - c_{11} c_{22} f_{11} f_{12} + c_{11} c_{12} f_{11} f_{22} - c_{21} c_{22} f_{11} f_{22} + c_{12}^2 f_{12} f_{22} - c_{22}^2 f_{12} f_{22},$$
$$(c_{12}^3 - c_{11}^2 c_{12} - c_{12} c_{21}^2 - c_{12} c_{22}^2 + 2 c_{11} c_{21} c_{22}) f_{12} - (c_{22}^3 - c_{11}^2 c_{22} - c_{12}^2 c_{22} - c_{21}^2 c_{22} + 2 c_{11} c_{12} c_{21}) f_{22},$$
$$(c_{21}^3 - c_{11}^2 c_{21} - c_{12}^2 c_{21} - c_{21} c_{22}^2 + 2 c_{11} c_{12} c_{22}) f_{21} - (c_{22}^3 - c_{11}^2 c_{22} - c_{12}^2 c_{22} - c_{21}^2 c_{22} + 2 c_{11} c_{12} c_{21}) f_{22}.$$

This list was generated by computer algebra as follows. We start from a list of polynomials that cuts out $\overline{\mathbf{N}(\mathcal{Q})}$ as a subset of $\mathbb{C}^8$. That list consists of ℓ, h, h° and the twelve 2×2 minors of the two matrices

$$\begin{pmatrix} c_{11} & c_{12} & c_{21} & c_{22} \\ \partial h^\circ / \partial f_{11} & \partial h^\circ / \partial f_{11} & \partial h^\circ / \partial f_{21} & \partial h^\circ / \partial f_{21} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} f_{11} & f_{12} & f_{21} & f_{22} \\ \partial h / \partial c_{11} & \partial h / \partial c_{11} & \partial h / \partial c_{21} & \partial h / \partial c_{21} \end{pmatrix}.$$

The respective rows are linearly dependent for any pair (c, f) of supporting linear functions. The resulting ideal has the desired prime ideal as its radical, by Hilbert's Nullstellensatz. We computed that radical.

We now describe the other components of the variety $\overline{\mathbf{N}(\mathcal{Q})}$. The eight strata $(\mathcal{Q}\text{ei,cx})$ consist of points (c, f) where one of the entries of f is ± 1 and the others are 0. This linear functional f exposes one of the elliptopes in $\partial \mathcal{Q}$. For example, consider $f = (1, 0, 0, 0)$. The prime ideal of this component is

$$\langle f_{11} - 1, f_{12}, f_{21}, f_{22}, c_{11} - 1 \rangle.$$

The corresponding stratum in the semialgebraic set $\mathbf{N}(\mathcal{Q})$ satisfies the additional cubic inequality

$$c_{12}^2 + c_{21}^2 + c_{22}^2 - 2 c_{12} c_{21} c_{22} \leq 1. \tag{37}$$

The boundary of the elliptope, seen inside $\mathbf{N}(\mathcal{Q})$, separates $(\mathcal{Q}\text{ei,cx})$ from the nonlinear stratum $(\mathcal{Q}\text{qx,qx})$.

By duality, there are also eight strata $(\mathcal{Q}\text{cx,ei})$ in the normal cycle $\mathbf{N}(\mathcal{Q})$. Now, the elliptopes appear in the f-coordinates and c is one of the 8 classical extreme points $(\mathcal{Q}\text{cx})$. These are obtained by exchanging the roles of f and c, using the linear transformation H. The ideal of one of the components $(\mathcal{Q}\text{cx,ei})$ is

$$\langle c_{11} - 1, c_{12} - 1, c_{21} - 1, c_{22} - 1, f_{11} + f_{12} + f_{21} + f_{22} - 1 \rangle.$$

The semialgebraic description of this stratum is obtained by setting $c = 2Hf$ in the cubic inequality (37).

3.5 Support function and gauge function

Two real valued functions are commonly used to describe a convex set $\mathcal{K}$. The first is the *gauge function* $\gamma_\mathcal{K}$ of the set [52]. It measures how far we have to go along a ray in some direction until we leave the set. The best known example is a norm as determined from its unit ball. The gauge function $\gamma_\mathcal{K}$ is the reciprocal of another well-known function in convex geometry: the *radial function* of the body.

The other standard measure is the maximum of a given linear functional over the given set. This is called the *support function* $\phi_\mathcal{K}$. In short, for any convex body $\mathcal{K}$ with 0 in its interior, we consider:

$$\gamma_\mathcal{K}(x) = \inf \{ \lambda \geq 0 \mid x \in \lambda \mathcal{K} \}, \tag{38}$$
$$\phi_\mathcal{K}(f) = \sup \{ f \cdot x \mid x \in \mathcal{K} \}. \tag{39}$$

Both functions are homogeneous of degree 1. From (38) we recover $\mathcal{K} = \{ x \mid \gamma_\mathcal{K}(x) \leq 1 \}$, and dually $\mathcal{K}^\circ = \{ f \mid \phi_\mathcal{K}(f) \leq 1 \}$. Hence, the support function of $\mathcal{K}$ is the gauge functional of $\mathcal{K}^\circ$. By self-duality, the two functions are closely related for $\mathcal{K} = \mathcal{Q}$. In the sequel we study $\phi = \phi_\mathcal{Q}$, and we drop the subscript.

Since the set $\mathcal{Q}$ has two markedly different kinds of boundary points, the support function requires a binary distinction concerning a functional f: *Will $\max_{c \in \mathcal{Q}} f \cdot c$ be attained at a classical point or at an exposed extreme point?* The answer is the same for all multiples of f, including $-f$, so we are really asking about the projective geometry of the boundary points of $\mathcal{Q}^\circ$, which is visualized for $\mathcal{Q}$ in Fig. 8. The separating surfaces are the images of the $[\mathcal{Q}nx]$ surfaces. Note that (after the identification of f with $-f$) there are four such surfaces. We can therefore not expect a simple algebraic relation to mark the distinction: Each of the elliptope boundaries has a Zariski completion with multiple additional irrelevant components overlapping the division Fig. 8, so some careful sifting of inequalities is needed.

Once we know the nature of the maximizer, however, the computation of ϕ is straightforward. In the first case, it is the maximum of an affine functional over the 8 vertices of $\mathcal{C}$. Namely, $\phi(f) = \phi_{\mathcal{C}}(f)$ with

$$
\begin{aligned}
\phi_{\mathcal{C}}(f) &= \max\{f \cdot c \mid c \in \partial_e \mathcal{C}\} \\
&= \max\{|f_{11}+f_{12}+f_{21}+f_{22}|, |f_{11}+f_{12}-f_{21}-f_{22}|, |f_{11}-f_{12}+f_{21}-f_{22}|, |f_{11}-f_{12}-f_{21}+f_{22}|\} \\
&= \|2Hf\|_\infty,
\end{aligned} \tag{40}
$$

In the second line, we grouped the maxima over a pair of antipodal classical extreme points by writing an absolute value. In the third line, $\|\cdot\|_\infty$ denotes the maximum norm on $\mathbb{R}^4$. This case applies exactly when the ray $\mathbb{R} f$ intersects the boundary of $\mathcal{Q}^\circ$ in an $\mathcal{N}$-facet.

The other possibility is that the ray intersects the boundary in a curved tetrahedron. In this case we think of ϕ as the gauge function of $\mathcal{Q}^\circ$. We need to determine the intersection point of the ray $\{\lambda f\}$ with $\partial \mathcal{Q}^\circ$. This point is in the zero set of h°. The equation $h^\circ(\lambda f) = 0$ in (34) is readily solved for λ, using the splitting of h° into homogeneous parts. We get $\lambda^6 k(f) - \lambda^4 p(f) = 0$, so in this case $\lambda = \phi(f)$ is

$$
\widetilde{\phi}(f) = \sqrt{\frac{k(f)}{p(f)}}. \tag{41}
$$

This function is homogeneous of degree 1, as required. The above heuristics is made precise in the following proposition, which extends Thm. 2:

Proposition 17 ($\rightarrow$*Sect. 5.4*) *For any $f \in \mathbb{R}^4 \setminus \{0\}$, the following conditions are equivalent:*

(1) *The ray $\{\lambda f\}$ intersects the boundary of $\mathcal{Q}^\circ$ in a point of type $(\mathcal{Q}qx)$.*

(2) *Some point $c \in \mathcal{Q}$ maximizing $f \cdot c$ is of type $(\mathcal{Q}qx)$.*

(3) *We have $p(f) < 0$ and*

$$
m(f) = \min_{i,j=1,2} |f_{ij}| \Big(\sum_{i,j=1,2} |f_{ij}|^{-1} \Big) > 2. \tag{42}
$$

(4) *We have $p(f) < 0$ and*

$$
\tilde{m}(f) = \Big(\frac{1}{f_{11}}+\frac{1}{f_{12}}+\frac{1}{f_{21}}+\frac{1}{f_{22}}\Big)\Big(\frac{1}{f_{11}}+\frac{1}{f_{12}}-\frac{1}{f_{21}}-\frac{1}{f_{22}}\Big)\Big(\frac{1}{f_{11}}-\frac{1}{f_{12}}+\frac{1}{f_{21}}-\frac{1}{f_{22}}\Big)\Big(\frac{1}{f_{11}}-\frac{1}{f_{12}}-\frac{1}{f_{21}}+\frac{1}{f_{22}}\Big) < 0.
$$

(5) *Perform a symmetry transformation (even number of sign changes) so that the maximum (40) of $f \cdot c$ over $\mathcal{C}$ is attained at the extreme point $c = (1,1,1,1)$, i.e., $\phi_{\mathcal{C}}(f) = f_{11}+f_{12}+f_{21}+f_{22}$. Then*

$$
f_{11}f_{12}f_{21} + f_{11}f_{12}f_{22} + f_{11}f_{21}f_{22} + f_{12}f_{21}f_{22} < 0. \tag{43}
$$

In this case the support function of $\mathcal{Q}$ is $\phi(f) = \widetilde{\phi}(f)$ from (41), otherwise $\phi(f) = \phi_{\mathcal{C}}(f)$ from (40).

In the domain described by Prop. 17, the maximizer of $\phi(f)$ is a unique exposed point $c^* \in \mathcal{Q}$. An explicit formula $f \mapsto c^*$ would correspond to solving for c given f in the system of 17 polynomials defining the stratum $(\mathcal{Q}qx,qx)$ in $\overline{\mathbf{N}(\mathcal{Q})}$. In terms of the angle parametrization of boundary pieces, it is essentially the self-dual counterpart of the map Φ sketched in Fig. 14.

We also numerically checked that our formula for the support function agrees with Tsirelson's formula [7]

$$
\phi_T(f) = \begin{cases} \sum_{ij} |f_{ij}| & \text{if } p(f) \geq 0 \\[2mm] \sum_{ij} |f_{ij}| - 2\min_{ij} |f_{ij}| & \text{if } p(f) < 0 \text{ and } m(f) \leq 2, \\[2mm] \sqrt{\Big(\sum_{ij} f_{ij}^2\Big) + |p(f)|\Big(\sum_{ij} f_{ij}^{-2}\Big)} & \text{if } p(f) < 0 \text{ and } m(f) \geq 2, \end{cases} \tag{44}
$$

but we were not able to reconstruct his proof.

4 Quantum Connections

We now return to Sect. 1.1, and we discuss what our geometric findings on $\mathcal{Q}$ mean for quantum theory. We begin by exhibiting explicit quantum models for the extremal points c of type ($\mathcal{Q}$qx). In Sect. 4.2 we examine what geometric features of some point $c \in \mathcal{Q}$ make it suitable for quantum key distribution. Actually, the extremal correlations have much stronger uniqueness properties, known as self-testing. We state these in Sect. 4.3. This is followed by a short reflection on the historical role of the elliptope case.

4.1 Quantum models

We introduced the convex body $\mathcal{Q}$ as the set of quantum correlations. We then mostly studied necessary conditions, i.e., consequences of the quantum form. But in order to show the sufficiency of any such condition, we must construct explicit quantum models. In this section we write out a parametrized family of quantum models, that realizes all points described in Prop. 8. That such a simple family already exhausts the extreme points of $\mathcal{Q}$ is, of course, a special feature of the minimal 222 case. In a sense which we will describe in Sect. 4.3, this family is actually *the only one* realizing the non-classical extreme points of $\mathcal{Q}$.

Using the notation introduced in Sect. 1.1, we set $m = 4$ and $\mathcal{H} = \mathbb{C}^4$. Algebraically, a quantum state is a positive semidefinite 4×4 matrix ρ with trace 1. For the density operator, we fix it as the rank one matrix with entries $\rho_{\alpha\beta} = \Psi_\alpha \overline{\Psi}_\beta$, defined by the unit vector

$$\Psi = \left(0 \,, \, \frac{1}{\sqrt{2}} \,, \, -\frac{1}{\sqrt{2}} \,, \, 0 \right)^T . \tag{45}$$

The measurements of the two parties are represented by the following real symmetric 4×4 matrices:

$$A_1 = \begin{pmatrix} \cos(\alpha) & 0 & \sin(\alpha) & 0 \\ 0 & \cos(\alpha) & 0 & \sin(\alpha) \\ \sin(\alpha) & 0 & -\cos(\alpha) & 0 \\ 0 & \sin(\alpha) & 0 & -\cos(\alpha) \end{pmatrix}, \quad A_2 = \begin{pmatrix} \cos(\gamma) & 0 & -\sin(\gamma) & 0 \\ 0 & \cos(\gamma) & 0 & -\sin(\gamma) \\ -\sin(\gamma) & 0 & -\cos(\gamma) & 0 \\ 0 & -\sin(\gamma) & 0 & -\cos(\gamma) \end{pmatrix},$$

$$B_1 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} -\cos(\alpha+\beta) & -\sin(\alpha+\beta) & 0 & 0 \\ -\sin(\alpha+\beta) & \cos(\alpha+\beta) & 0 & 0 \\ 0 & 0 & -\cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ 0 & 0 & -\sin(\alpha+\beta) & \cos(\alpha+\beta) \end{pmatrix}.$$

These matrices satisfy the hypotheses stated in (1). We now compute the four correlations c_{ij} in (2).

Lemma 18 *The point c with parameters $(\alpha, \beta, \gamma, \delta)$ in Prop. 8, even without the inequality constraint on Δ, satisfies $c_{ij} = \mathrm{tr}(\rho A_i B_j)$.*

This is a formal identity, for all $1 \le i, j \le 2$, and can be checked using computer algebra. However, this takes time and some careful typing, and is the approach of minimal insight. It is better to remember the physics, and to realize that this family is the "minimal" quantum model at the historical root of the subject. It arises naturally when Alice and Bob each see the polarization degree of freedom of a pair of photons, or the spin degree of freedom of a spin-1/2 particle, and their measurements are just polarization (or spin component) measurements. The only interesting quantity is then the angle between the orientations of the polarizers, and the correlation is just the cosine of this angle. In this form it was already used in John Bell's first paper [4], and in the work of CHSH [5]. The problem that needed to be solved for these authors was to adjust the angles in order to maximize the violation of the CHSH inequality. What we claim here is that the same physical setup suffices to realize the entire quantum correlation body $\mathcal{Q}$.

To see how this family is "minimal", note that when either Alice or Bob holds a classical system, for instance if the observables A_1 and A_2 commute, no entangled states are possible. This even characterizes classical systems [65]. Therefore only classical correlations can be constructed. Hence Alice's and Bob's subsystems need at least 2-dimensional Hilbert spaces. Since $[A_i, B_j] = 0$, these subsystems must be

combined in a tensor product, so $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$. Actually, we can take the A_i and B_j, as well as the density operator ρ, to be real rather than complex, so the Hilbert space is actually $\mathbb{R}^4$. Of course, for almost all of quantum physics, e.g., the Schrödinger equation, this would be an untenable restriction. As shown only recently, there are even correlation experiments of just the type considered here (only not minimal) that prove that "real quantum mechanics" is insufficient [66]. With the further simplification that $A_i^2 = B_j^2 = \mathbb{1}$, these matrices must be given on each side by reflections in planar geometry, a one parameter family. Explicitly, the reflections are

$$M(\tau) := \begin{pmatrix} \cos(\tau) & \sin(\tau) \\ \sin(\tau) & -\cos(\tau) \end{pmatrix} = \cos(\tau) \cdot \sigma_3 + \sin(\tau) \cdot \sigma_1 \quad \text{for } \tau \in [0, 2\pi]. \tag{46}$$

The matrices above are then $A_1 = M(\alpha) \otimes \mathbb{1}$, $A_2 = M(-\gamma) \otimes \mathbb{1}$, $B_1 = \mathbb{1} \otimes M(\pi)$, and $B_2 = \mathbb{1} \otimes M(\alpha+\beta+\pi)$.

The state ρ must be entangled. We choose a maximally entangled one, which is by definition pure on the whole system, $\rho = |\Psi\rangle\langle\Psi|$, and maximally mixed on the subsystems, i.e. for any matrix A we have

$$\langle\Psi|(A \otimes \mathbb{1})\Psi\rangle = \langle\Psi|(\mathbb{1} \otimes A)\Psi\rangle = \text{tr}(A)/2. \tag{47}$$

This would be too special for the full marginals case [67]. But here we can get away with it, and even fix the vector Ψ in (45) for the whole family. This is the unique vector (up to scaling) which is antisymmetric with respect to the exchange of the two tensor factors. For any matrix A, the vector $(A \otimes A)\Psi$ is again antisymmetric. Hence $(A \otimes A)\Psi = \varepsilon(A)\Psi$, for some homogeneous quadratic function ε, which is also multiplicative, i.e., equals the determinant. Inserting for A a one-parameter subgroup of SU(2), i.e., $A = \exp(itM)$ for traceless M, we find that $\varepsilon(A) = 1$ is constant. Hence, in first order in t, we have $(M \otimes \mathbb{1} + \mathbb{1} \otimes M)\Psi = 0$. Applying this to the matrices from (46) and combining with (47) we thus find

$$\begin{aligned} \text{tr}\big(\rho\, M(u) \otimes M(v)\big) &= \langle\Psi|M(u) \otimes M(v)\Psi\rangle = \langle\Psi|(M(u)M(v)) \otimes \mathbb{1}\Psi\rangle \\ &= \text{tr}\big(M(u)M(v)\big)/2 = -\cos(u-v). \end{aligned} \tag{48}$$

The last identity is seen by observing that $\text{tr}(AB^T)$ is the standard scalar product in matrix space, and using the addition theorem for the cosine, or, geometrically that the product of reflection across lines at an angle $u - v$ is the rotation by that angle. Inserting the choice of angles after (46) gives the result.

4.2 Geometric aspects of quantum key distribution

Quantum key distribution (QKD) is an important task in quantum information technology [68]. It furnishes the main practical reason for studying the body $\mathcal{Q}$. Here we discuss geometric features that are fundamental for that task. The goal of QKD is for two distant parties, Alice and Bob, to utilize quantum correlations for generating a key which is guaranteed to be secret from any eavesdropper, here called Eve. Eve is only assumed to be constrained by the laws of quantum mechanics, but otherwise enjoys every possible freedom. In particular, she is allowed to manipulate the correlated systems on which the scheme is based, the quantum channels by which they are transmitted, and even the measurement devices. She also gets a copy of the communications exchanged between Alice and Bob. However, she can only read these but not change them. One must also assume that once the data collection starts, Eve cannot reach into Alice's and Bob's lab and access their measurement settings or outcomes. Indeed, if Eve could do that, she would not even need to bother with the whole quantum setup, or she could play a trivial woman-in-the middle attack, and secrecy would be obviously impossible. So the rules of the game force her to gain at least some information from the quantum systems. According to the laws of quantum mechanics, this introduces a disturbance detectable by Alice and Bob. When they do detect such deviations from the expected statistics the key distribution has failed. Eve can always achieve that, but this is counted as a failure for her, because she will also not learn any secrets.

We want to show here that the minimal setup in this paper is already sufficient to support QKD. Moreover, the main security argument is based directly on the geometry of $\mathcal{Q}$. In undisturbed operation the setup leads to some correlations $c \in \mathcal{Q}$. Alice and Bob will use a random sample of their particles to verify this via the public classical channel, and will abort the process if they find significant deviations from c. We claim that QKD is possible whenever c is a *non-classical extreme point* (cf. [69])

Suppose Alice and Bob test their correlations and find them to be such a point $c \in \partial_e \mathcal{Q}$. What could Eve know about their measurement results? Let ε be a random variable that summarizes her findings.

The conditional correlation c_ε is the 2×2 matrix that pertains to those cases where Eve found ε. We have $c_\varepsilon \in \mathcal{Q}$ since Eve is constrained by quantum mechanics. Combining the data with the probabilities p_ε for observing ε, we get $c = \sum_\varepsilon p_\varepsilon c_\varepsilon$. But since c is extremal, all c_ε that appear with nonzero probability must be equal to c. That is the same as saying that ε is statistically independent of Alice's and Bob's information. So while Eve knows ε, she learns nothing about c.

Note, however, that the argument applies equally to classical extreme points. Only, in that case the extreme points are completely deterministic. In the case of deterministic agreement probabilities indeed factorize, say $c_{ij} = a_i b_j$. With $c_{ij} \in \{0, 1\}$ and $a_i, b_j \in [0, 1]$, this factorization would be $1 \cdot 1 = 1$ or $0 \cdot 0 = 0$. Of course, this is utterly useless for drawing a secret key. So what Alice and Bob use to generate the key are the non-trivial correlations that may be present in *non-classical* extreme points. Any non-classical correlation is fine for that purpose, since this may be further distilled into perfect agreement.

Note also that in case of non-classical extremal points, *any* pair (out of four) of measurement settings can be chosen to be the "key (generating) basis" due to the very definition of cryptographic security [69]. Weakening this to only the existence of one pair of measurement settings that is uncorrelated with Eve still supports a perfect QKD protocol. This necessitates moving to the full 8-dimensional body where a non-extremal point P has been shown to exhibit this phenomenon [70]. Intuitively, this means while the behaviour P admits a nontrivial convex decomposition $P = \sum p_\varepsilon P_\varepsilon$, Eve does not gain additional information in the key basis: $P_\varepsilon(a, b|\text{key}) = P(a, b|\text{key})$ for all a, b, ε; she only has an advantage in other pairs of settings where the outcomes are not used for making a pair of secret key.

The full analysis of QKD takes not only error correction into account, but also the overhead of statistically verifying that the given source is really described by c. This necessarily involves errors, and the experimental implementation will have additional errors of its own. The analysis, done carefully also for c sufficiently close to $\partial_e \mathcal{Q}$, results not in a blanket statement that Eve will know "nothing", but in a quantitative bound on how much she might know in the worst case. So, in addition to error correction (getting the keys to be really the same) one needs "privacy amplification", a process that had already been studied in purely classical settings [71] prior to the advent of QKD. The traditional information theoretic view focuses on rates in the asymptotic regime, i.e., for a large number of exchanged raw key bits. This systematically neglects the overhead of reliably estimating c. This can be considerable in real, and therefore finite, runs. A usable QKD security proof always has to include the finite key analysis, and all imperfections. This is far beyond the current paper, and we refer to [72, 73]. To connect with the literature, we emphasize that here we have described "device independent" QKD, for which the experimental entrance ticket is a "loophole free" Bell test, which has been achieved only recently [74, 2, 75]. Nevertheless, recent advances on the theoretical side [72, 36, 73] have resulted in proof-of-principle experiments such as [76, 77, 78] with varying degree of closeness to "loophole free". On the other hand, systems not realizing the ideal of device independence are already commercially available (see [79, Section 3.2]).

Coming back to the geometric features of $\mathcal{Q}$ relevant for QKD, we can first see some of the tradeoffs that enter the choice of $c \in \mathcal{Q}$. Choosing c of type ($\mathcal{Q}$nx) might seem advantageous, because then the outcomes of Alice and Bob agree for one of the settings, making the error correcting step superfluous. However, this comes at the price of moving closer to $\mathcal{C}$, so that relatively low noise may make privacy amplification harder. The traditional working point therefore has been the c from (5), maximally violating a CHSH inequality. As an exposed point this seems to simplify the tomography, because only one combination of correlations needs to be estimated. But this actually leaves unnecessary leeway in the tangent directions, which are only fixed to $\sqrt{\varepsilon}$, when the correlation is fixed to order ε. It is therefore better to use all the correlation data, rather than focusing on just one linear combination.

We further have to correct a simplification in the above argument for non-classical extreme points. It really applies only to the full statistics of Alice's and Bob's measurements including marginals, i.e., the 8-dimensional body of which $\mathcal{Q}$ is a projection. The key must be generated from the local measurement data, not just the combined outcomes entering a correlation. So it will be important to get extremality of $c \in \mathcal{Q}$ also when it is extended to 8 dimensions with zero marginals. This will be done in the following section, in particular in items (4),(5) of Thm. 19.

4.3 Uniqueness of quantum models

What can we deduce about the uniqueness of quantum realization of points in $\mathcal{Q}$? Prima facie there is no reason for any uniqueness. In Sect. 4 we made special choices to realize the extreme points *somehow*.

Why $m = 4$ in Lem. 18? Why not $m = 3$? What about $m = \infty$? That there is limited choice if we try to find realizations in minimal dimension says very little about the non-uniqueness if we allow more spacious Hilbert spaces. We begin by noting that there are some trivial ways in which uniqueness fails:

- *Unitary transformation*
  This refers to a change of basis in the Hilbert space $\mathcal{H}$. It makes the quantum model looks different but does not change the correlations c_{ij}. They are invariants of the action of the unitary group $U(m)$ on quintuples of matrices $(\rho, A_1, A_2, B_1, B_2)$ as in Sect. 1.1, with $\mathcal{H} = \mathbb{C}^m$. Two unitarily equivalent models, i.e., two quintuples in the same $U(m)$-orbit, are considered to be "the same".

- *Expansion*
  This means enlarging the Hilbert space $\mathcal{H}$ of the model by an additional summand $\mathcal{H}_0$ where the states act trivially. If we use the space $\mathcal{H} \oplus \mathcal{H}_0$, the state $\rho \oplus 0$ and the observables $A_i \oplus A_i^0$ and $B_j \oplus B_j^0$, with A_i^0 and B_j^0 arbitrary, provided (1) still holds, then the correlations do not change.

- *Adding multiplicity*
  This means enlarging $\mathcal{H}$ by an additional tensor factor where the measurement acts trivially. If we use $\mathcal{H} \otimes \mathcal{H}_\nu$ with $A_i \otimes \mathbb{1}$, $B_j \otimes \mathbb{1}$, and a state $\widetilde{\rho}$ whose partial trace over the second factor is ρ, then the correlation do not change. Writing the tensor product as a direct sum with respect to a basis of $\mathcal{H}_\nu$ makes this a direct sum of possibly correlated copies of the given model.

The best we can hope for is uniqueness of the quantum model for c up to these three operations. This is Condition (2) in Thm. 19 below. Condition (1) is the cryptographic security discussed in Sect. 4.2, i.e., anything an eavesdropper might know is statistically independent of c. Remarkably, the two conditions are equivalent. Moreover, cryptographic security is extended in (4) to all measurements made with observables in the algebra $\mathcal{A}$ generated by A_1, A_2, B_1, B_2. The central condition is (3), the uniqueness of a certain kind of model, defined by removing the redundancy of the operations of expansion and adding multiplicity. These *cyclic models* are defined by the property that $\rho = |\Psi\rangle\langle\Psi|$ is pure and Ψ is cyclic for the operators A_i, B_j, i.e., we get a dense subspace of $\mathcal{H}$ by acting with these operators repeatedly on Ψ.

Uniqueness results like Thm. 19 appear in the literature under the keyword *self-testing* [28, 34]. This indicates that the correlations can be used cryptographically without first verifying that the devices act as they should, or that the prepared state is as planned: Security is based directly on the observed correlations. Current definitions of self-testing [33, 28, 34, 25] implicitly use some of the equivalences below. Unlike these definitions and statements therein, our formulation below does not make purifying assumptions on the unknown models, i.e. "going to the church of the larger Hilbert space", nor require additional ancillas into which the ideal system is swapped.

Theorem 19 ($\rightarrow$ *Sect. 5.5) Fix a point $c \in \mathcal{Q}$. Let (ρ, A_i, B_j) be any quantum model in a Hilbert space $\mathcal{H}$ for the correlations c, and write $\mathcal{A}$ for the norm closed operator algebra generated by A_i, B_j. When applicable, denote by $(\hat{\rho}, \hat{A}_i, \hat{B}_j)$ the specific model for c given in Sect. 4.1. The following are equivalent:*

(1) *c is nonclassical and extremal in Q.*

(2) *There is a unique cyclic model for c. Explicitly, when $\rho = |\Psi\rangle\langle\Psi|$ is pure and cyclic for $\mathcal{A}$ (i.e., $\mathcal{A}|\Psi\rangle$ is dense in $\mathcal{H}$), then it is unitarily equivalent to the model specified for c in Sect. 4.1.*

(3) *The quantum model is unique up to unitary transformation, expansion and adding multiplicity. That is, by a unitary transformation any model can be brought into canonical form $\mathcal{H} = (\hat{\mathcal{H}} \otimes \mathcal{H}_\nu) \oplus \mathcal{H}_0$, $\rho = \hat{\rho} \otimes \rho_\nu \oplus 0$, $A_i = \hat{A}_i \otimes \mathbb{1}_\nu \oplus A_i^0$, and ditto for B_j.*

(4) *c has a unique extension to a quantum behavior p (necessarily extreme) in the 8-dimensional body including both correlations and marginals.*

(5) *c is cryptographically secure, i.e. its unique extension p is cryptographically secure (cf. [69]).*

(6) *c is algebraically secure, i.e. $\mathrm{tr}(\rho E X) = \mathrm{tr}(\rho E)\,\mathrm{tr}(\rho X)$ for $X \in \mathcal{A}$ and any E commuting with $\mathcal{A}$.*

We stress that these equivalences are claimed only for the minimal scenario assumed in this paper. For larger parameters NMK, the condition (1) may well be weaker than the others. This was noted by

Tsirelson who treated the 2M2|0 case and showed [7, Thm. 3.3] that for "odd rank" there are two inequivalent cyclic representations (but connected by transposition, a non-unitary operation). Recently, [80] gave another example thanks to the existence of inequivalent MUBs (this time even up to transposition). Parallel to Tsirelson's work, uniqueness was shown in [29, 81]. At the time, the authors were not aware of cryptographic applications, and R.F.W. (the second author of [29]) thought of this result as a fortuitous algebraic property of the CHSH expression, and unlikely to generalize. After an earlier attempt in [69], he only realized with the current work that the methods of [29] provide uniqueness for the largest scope possible within the 222 scenario.

In cryptography, one generally has only an approximation to c. Luckily, the uniqueness result holds robustly. As shown first in [81], one can find a nearby set of operators and a state realizing c precisely.

4.4 The role of the elliptope

Historically, the elliptope has played an important role for quantum correlations. John Bell's first inequality [4] concerned three measurement settings on each side, a 232 setting. The underlying quantum model was the singlet state ρ above, and the settings on the two sides pairwise equal, so that the outcomes where pairwise perfectly anticorrelated, hence opposite with probability one. Even without accepting Bell's conclusion that they are therefore "predetermined", or going into a discussion what that means, this simplifies the analysis to a discussion of just three possibilities. Although Bell does not include the picture, the quantum body is exactly the elliptope shown in Fig. 7, and the classical body is the embedded tetrahedron. Bell's original scenario and the elliptope continue to serve as a simplified example for explaining quantum correlations, from Mermin's classic article [82] to today [83].

However, perfect anticorrelation, while easily verified in the model, is much harder to get in the quantum experiments. It was the decisive advance due to Clauser, Horne, Shimony and Holt [5] to eliminate this experimentally doubtful assumption, and to identify the 222 case as the minimal setting.

Our analysis of the convex body $\mathcal{Q}$ shows that the elliptope still occurs in the 222 case, and that it suffices to assume (or experimentally verify) full correlation between only two of the observables. The geometric picture of Bell's analysis (he does not draw it, though) then holds. This is of interest in cryptography, since drawing key from the perfectly correlated settings eliminates the error correction step, albeit at the expense of the distance from the classical polytope, and hence harder noise requirements.

We close with the remark that the elliptope is iconic in many branches of the mathematical spectrum, notably in convex optimization, as the feasible region of a semidefinite program, and in Gaussian statistics, as the set of 3×3 correlation matrices. See the pointers surrounding [17, Figure 1.1] and [19, Figure 1].

4.5 Fixed Hilbert space dimension

The models above use a 4-dimensional Hilbert space. This is an option, that happens to be sufficient for getting the extreme points of $\mathcal{Q}$, but no assumption like this is made in the definition of $\mathcal{Q}$. As seen in Sect. 4.2, this is vital for QKD. However, one can ask how such an assumption would change $\mathcal{Q}$. For non-minimal settings, the question what inference about dimension can be drawn from an observed correlation has been studied extensively (see, e.g., [84, 85, 86]). So what can be said in the minimal setting? Here we just collect some basic observations, that can be skipped without loss for other sections.

Let us denote by $\mathcal{Q}_m$ the (warning: nonconvex!) set of quantum correlations that are obtainable by models as in Sect. 1.1 under the additional assumption $\dim \mathcal{H} = m$. We also write $\mathcal{C}_m \subset \mathcal{Q}_m$ for the corresponding set of classical correlations realized in a sample space of m points. Since we do not require $A_i^2 = B_j^2 = \mathbb{1}$, or tensor product separation, the set $\mathcal{Q}_m$ is increasing with m, and so is $\mathcal{C}_m$. Since building a model for a convex combination of correlations requires the direct sum of models, and this increases m, these sets are not in general convex. However, we know that extreme points of the full bodies can be realized in fixed dimensions, so $\partial_e \mathcal{C} \subset \mathcal{C}_1$ and $\partial_e \mathcal{Q} \subset \mathcal{Q}_4$. Thus Carathéodory's Theorem allows us to put a bound on the required m: Since in an n-dimensional convex body every point is the convex combination of at most $n + 1$ extreme points, and $n = 4$, we conclude that $\mathcal{C} \subset \mathcal{C}_5$ and $\mathcal{Q} \subset \mathcal{Q}_{20}$.

The Carathéodory bound is typically tight only for polytopes, where most points require $n + 1$ of the vertices for a convex representations. When there is a continuum of extreme points, that *Carathéodory number* is usually smaller. One extreme example for this are Euclidean balls of any dimension, in which every point is the convex combination of two antipodal boundary points. Another familiar example is the quantum state space with $\dim \mathcal{H} = m$, which has dimension $m^2 - 1$, although every density operator
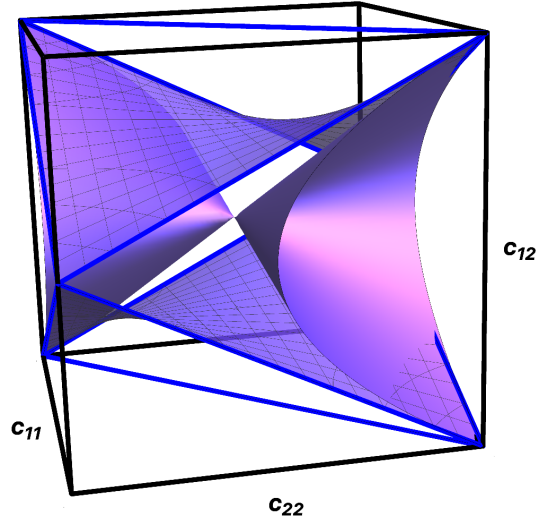
Figure 15: The set $\mathcal{C}_1 \equiv Q(\rho_A \otimes \rho_B) = \mathcal{N} \cap \{c : \det(c) = 0\}$ in the Alice-Bob symmetric plane. The black bounding cube is $\mathcal{N}$, and the edges of $\mathcal{C}$ are given as blue lines. The section of $\mathcal{C}_1$ with this plane is the (purple) double cone $c_{11}c_{22} = c_{12}^2$ emanating from the origin. The projection contains additional points bounded between the double cone and the (top and bottom) surfaces $2|c_{12}| - 1 = c_{11}c_{22}$.

has a spectral resolution into m pure states. Our body $\mathcal{Q}$ will be an intermediate case in this respect. The following result is also part of [7].

Proposition 20 (→*Sect. 5.6*) *Let $\mathcal{Q}_m$ be the set of quantum correlations obtainable from models with m-dimensional Hilbert space. Then $\mathcal{Q}_m \subset \mathcal{C} \neq \mathcal{Q}$ for $m \leq 3$, and $\mathcal{Q}_m = \mathcal{Q}$ for $m \geq 4$.*

The analogous set $\mathcal{C}_m$ for the cross polytope $\mathcal{C}$ is also interesting and worth further study. Obviously, $\mathcal{C}_1$ is the subset of rank 1 matrices $c \in \mathbb{R}^{2 \times 2}$, a condition which is invariant under the natural symmetry group of correlation bodies but *not* under the extended symmetry group discussed in Sect. 2.4.

In both cases an interesting variant of the problem is to look at the subset of models with $A_i^2 = B_j^2 = \mathbb{1}$ and/or a pure state ρ. Also it may be of interest to fix the observables, and consider the set of correlations resulting from varying ρ.

4.6 Fixed State

For many applications it is crucial that no assumption about the quantum state is made: the linear bounds given by $f \in \mathcal{Q}^\circ$ hold for *any* quantum state. In some applications, however, the state is well-known and the question is what correlations might be realized on that basis. The question really only makes sense, when the Alice-Bob split is also known, so we ask that $A_i \in \mathcal{A}$, $B_j \in \mathcal{B}$, where $\mathcal{A}$ and $\mathcal{B}$ are commuting operator algebras, typically even a tensor product split $\mathcal{A} = \mathcal{B}(\mathcal{H}_A) \otimes \mathbb{1}$ and $\mathcal{B} = \mathbb{1} \otimes \mathcal{B}(\mathcal{H}_B)$. We thus consider

$$\mathcal{Q}(\rho) := \{c_{ij} \in \mathbb{R}^4 : c_{ij} = \mathrm{tr}\rho A_i B_j, -\mathbb{1} \leq A_i, B_j \leq \mathbb{1}, A_i \in \mathcal{A}, B_j \in \mathcal{B}\}.$$

This is, in general, not a convex set. For example, when ρ is a product state, $c_{ij} = a_i b_j$ factorizes, and $\mathcal{Q}(\rho) = \mathcal{Q}_1 = \mathcal{C}_1$ in the sense of the previous section (see also Fig. 15). For entangled states close to that, the non-convexity will persist, even though there are some proper quantum correlations. A closed form or complete algebraic description of $\mathcal{Q}(\rho)$ can hardly be expected, so we just make a few remarks.

First, if we fix a a linear functional f, finding the maximal quantum value is a bilinear optimization problem. We can fix all observables except one, e.g. A_i, and isolate the linear functional by which it enters, i.e. find X_i such that $\sum_j f_{ij} \mathrm{tr}\rho(A \otimes B_j) = \mathrm{tr} X_i A$ or equivalently $X_i = \sum_j f_{ij} \mathrm{tr}_B(\rho \mathbb{1} \otimes B_j)$. Maximizing over A_i, is now the problem of finding the A with $-\mathbb{1} \leq A \leq \mathbb{1}$ for which $\mathrm{tr}(AX_i)$ is maximized. Clearly, that is $A_i = \mathrm{sign}(X_i)$ in the functional calculus of the hermitian operator X_i. The maximum is then the trace norm of X_i, which would seem to eliminate the A_i. However, it is better to just fix the optimal
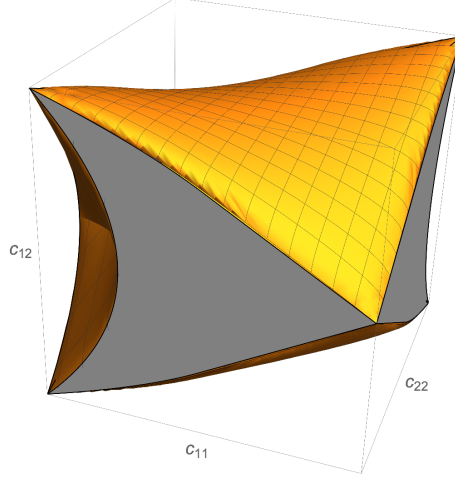
Figure 16: The projection of the set $\mathcal{Q}_{st}(1, 0.5)$ of Prop. 21 to the AB-symmetric plane. This is a 3-dimensional connected nonconvex semialgebraic set, the midpoint of a continuous family connecting $\mathcal{Q}_{st}(1,0) = \mathcal{C}_1$ from Fig. 15 with $\mathcal{Q}_{st}(1,1) = \mathcal{Q}$ from Fig. 2. The two-parameter family is homogeneous: $\mathcal{Q}_{st}(t\lambda_1, t\lambda_2) = t\mathcal{Q}_{st}(\lambda_1, \lambda_2)$, which for $t \leq 1/\sqrt{2} \approx .7$ is included in $\mathcal{C}$.

A_i, and optimize again with respect to the B_j in the next step, in a see-saw style. This works nicely in practice, and improves the target functional in every step. However, this iteration has no convergence guarantee.

The second remark is that we can give a "closed solution" in the case of a $2 \otimes 2$-dimensional Hilbert space, the minimal dimension where nonclassical correlations could manifest by Prop. 20. This generalizes a well-known formula by the Horodeckis [87] for the maximal CHSH-violation of a given two-qubit state to an arbitrary linear inequality. As in the case of the Horodecki formula, the result depends only on the two largest singular values of the matrix R described in the proposition.

Proposition 21 ($\rightarrow$*Sect. 5.7*) *Let ρ be a density operator on $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$, and let $\lambda_1 \geq \lambda_2 \geq 0$ be the two largest singular values of the 3×3-matrix with entries $R_{k\ell} = \mathrm{tr}[\rho\,(\sigma_k \otimes \sigma_\ell)]$ for Pauli matrices $\sigma_1, \sigma_2, \sigma_3$. Then the convex hull $\mathrm{co}\,\mathcal{Q}(\rho) = \mathrm{co}\big(\mathcal{Q}_{st}(\lambda_1, \lambda_2) \cup \mathcal{C}\big)$, where $\mathcal{Q}_{st}(\lambda_1, \lambda_2)$ is the set of correlations of the form*

$$c_{ij} = \lambda_1 \cos(\alpha_i) \cos(\beta_j) + \lambda_2 \sin(\alpha_i) \sin(\beta_j). \tag{49}$$

Moreover, we have $\mathcal{Q}(\rho) \subset \mathcal{C}$ if and only if $\lambda_1^2 + \lambda_2^2 \leq 1$.

The map of possibilities is shown in Fig. 17. The singular values for a vector with Schmidt spectrum $s_1 \geq s_2 \geq 0$, e.g., $\psi = s_1|{+}{+}\rangle + s_2|{-}{-}\rangle$ where $|{\pm}\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$ are $\lambda_1 = s_1^2 + s_2^2 = 1$ and $\lambda_2 = 2s_1 s_2$, which parametrizes the line segment PM. The fact that all these states (other than P) give correlations outside $\mathcal{C}$, and hence violate the CHSH inequality, is known as Gisin's Theorem [88].

4.7 Fixed Observables

Dually we can fix the operators A_i, B_j, so that the resulting compact convex semialgebraic set

$$\mathcal{Q}(A_i, B_j) := \{c_{ij} \in \mathbb{R}^4 \,:\, c_{ij} = \mathrm{tr}\rho A_i B_j, \rho \geq 0, \mathrm{tr}\rho = 1\} \tag{50}$$

is just an affine image of the quantum state space, a spectrahedron. Still an explicit description may be difficult. As in the case of a fixed state, the boundary in any single direction, i.e., the maximization of any affine functional f reduces to an eigenvalue problem, namely the largest eigenvalue of the operator $T(f) = \sum_{ij} f_{ij} A_i B_j$. Giving an algebraic solution might be harder because this corresponds to computing an algebraic formula for the largest root of a polynomial of high degree, depending on the dimension of the underlying Hilbert space.

The general case $-\mathbb{1} \leq A_i, B_j \leq \mathbb{1}$ can, in principle, be dealt with by a minimal dilation $U : \mathcal{H} \to \mathcal{K}$ so that $\mathcal{Q}(A_i, B_j)$ is the affine image of a specific isometric copy of the state space of $\mathcal{H}$ in $\mathcal{K}$. This is harder to work out, so we give a characterization only for the special case $A_i^2 = B_j^2 = \mathbb{1}$.
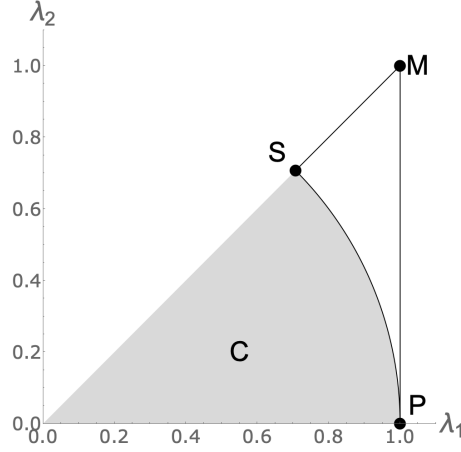
Figure 17: The map of singular value pairs (λ_1, λ_2) in Prop. 21. In the shaded region C, $\mathcal{Q}_{\mathrm{st}}(\lambda_1, \lambda_2) \subset \mathcal{C}$. The labelled points are: M: the maximally entangled case, P: a pure product state, all pure two-qubit states, parametrized for this purpose by their Schmidt spectra, lie on the segment PM. The diagonal gives scaled versions of $\mathcal{Q}$. At S the set just touches $\mathcal{C}$ from within.

Proposition 22 ($\rightarrow$*Sect. 5.8*) *Let A_i, B_j be hermitian operators on a finite dimensional Hilbert space with $[A_i, B_j] = 0$ and $A_i^2 = B_j^2 = \mathbb{1}$. Denote the spectrum of $(A_1 A_2 + A_2 A_1)/2$ by Σ_A, and define Σ_B analogously. Then*

$$\mathcal{Q}(A_i, B_j) = \mathrm{co}\{\mathcal{Q}_{\mathrm{obs}}(u, v) := S(u)\mathsf{O}(2)S(v)^\top \mid u \in \Sigma_A, \ v \in \Sigma_B\}, \qquad where \ S(u) = \begin{pmatrix} 1 & 0 \\ u & \sqrt{1 - u^2} \end{pmatrix},$$
(51)

and $\mathsf{O}(2)$ is the set of 2×2 orthogonal matrices, i.e. the circles of rotations and reflections about some axes.

There is a subtlety here when A_i, B_j are "genuinely infinite dimensional". Then the Prop. 22 holds, if we interpret the convex hull as the closed convex hull and $\mathcal{Q}(A_i, B_j)$ as the closure of the set of correlations attainable with arbitrary density operators. But for points in the continuous spectrum (not eigenvalues), certain boundary points will be unattainable by density operators in the given space. This is a straightforward consequence of the uniqueness theorem Thm. 19. When some self-testing correlation inequality f is attained, the maximum must be an eigenvector of the corresponding T_f. Such points can only be attained by singular states, i.e. positive normalized linear functionals not induced by density operators, because the continuous spectrum can be approximated by eigenvectors.

Since $\mathsf{O}(2)$ is the basic model for the fixed-observable correlation sets, we consider it in more detail.

Proposition 23 ($\rightarrow$*Sect. 5.8*)

(1) *The set $\mathcal{Q}_{\mathrm{obs}}(0,0) = \mathrm{co}\,\mathsf{O}(2)$ is the convex hull of two circles. The circles both have the origin as their center, and lie in orthogonal planes of $\mathbb{R}^4$.*

(2) *Both circles consist of extreme points, and any line connecting a pair of points from different circles is an exposed edge of $\mathcal{Q}_{\mathrm{obs}}(0,0)$. The union of these edges is the entire boundary.*

(3) *The necessary and sufficient semialgebraic condition for $c \in \mathcal{Q}_{\mathrm{obs}}(0,0)$ is that*

$$\ell(c) := 1 - (c_{11}^2 + c_{12}^2 + c_{21}^2 + c_{22}^2) + (\det c)^2 \geq 0 \qquad and \qquad -1 \leq \det c \leq 1. \tag{52}$$

Since the observables used by Alice and Bob for $\mathcal{Q}_{\mathrm{obs}}(0,0)$ are the same, the Alice-Bob swap symmetry leaves this set invariant, and so its intersection with the plane $\{c_{12} = c_{21}\}$ is at the same time the projection (see the double cone in Fig. 19). On the other hand, for general values of u and v this is not true, as shown in Fig. 18.

The above Proposition suggests that quantum points with $|\det c| = 1$ are self-testing.
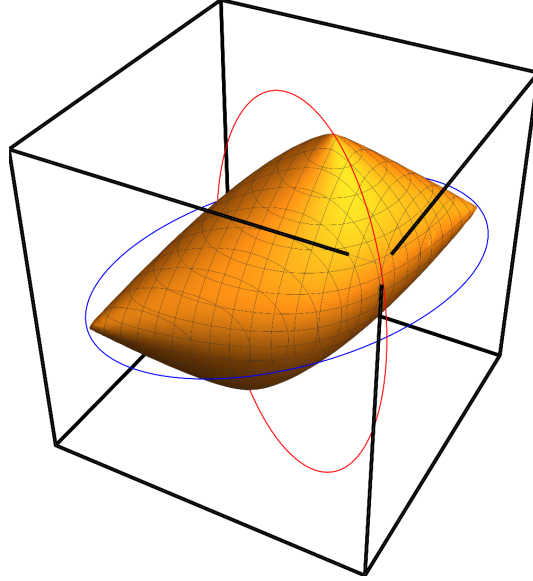
Figure 18: The fixed observable set $\mathcal{Q}_{\mathrm{obs}}(0.7, -0.9)$ of Prop. 22 in the Alice-Bob symmetric plane. The section with that plane is the orange body, while the projection is larger and is generated by the two circles shown. The red circle corresponds to maximal (positive) determinant, the blue one to minimal determinant.
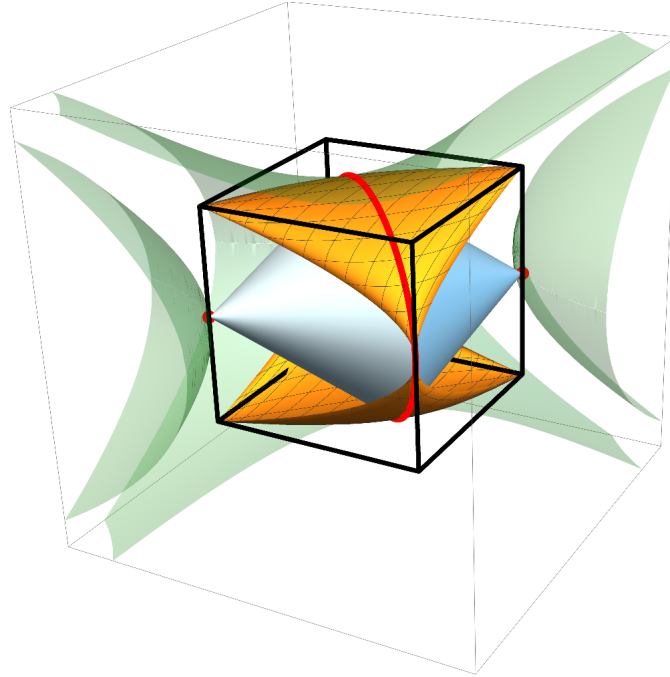
Figure 19: The determinant function in an Alice-Bob symmetric plane. Green: The two surfaces $\det c = -1$ (one-sheeted hyperboloid, cut open for visibility) and $\det c = +1$ (two-sheeted hyperboloid touching $\mathcal{N}$ only in two points). Orange: the boundary of $\mathcal{Q}$. The double cone inside $\mathcal{Q}$ is both a section and a projection of $\mathcal{Q}_{\mathrm{obs}}(0, 0)$. The intersection of all three sets, i.e., the case of equality in Prop. 24 is the red line, together with the two cone tips.

Proposition 24 *(→Sect. 5.8) For $c \in \mathcal{Q}$, $|\det c| \leq 1$ with equality if and only if c is an orthogonal matrix. In that case, in the unique cyclic quantum model for such correlations the identities $A_1 A_2 = -A_2 A_1$, and $B_1 B_2 = -B_2 B_1$ hold, i.e., up to unitary isomorphism all measurements operators A_i, B_j are Pauli matrices.*

5 Proofs

In this section we prove all theorems and propositions seen so far. Since many results in our paper have appeared previously in the literature, we could give many proofs by citation. However, we aim to make our text self-contained. Where the pedestrian argument, tailored to the case at hand, can be understood as an example of a more general theory, we provide this background as well. As a help for monitoring the logical flow we included some summaries of what has been shown up to some point. These are formatted like the definitions and propositions throughout the paper, and numbered consecutively with these.

There are, of course, many ways to organize the proofs. We now briefly describe our overall strategy and the structure of Sect. 5. We begin in Sect. 5.1 with the equivalences of Thm. 1, centered around the matrix completion problem. Self-duality (Thm. 3) follows in Sect. 5.2. On this path we already need some information about the boundary (e.g., in Sect. 5.1.4), which is extended to the detailed classification of boundary points in Sect. 5.3. The study of boundary points is perhaps a bit more detailed than necessary, since it uses a local criterion for excluding certain points from the extreme boundary of the convex hull of a variety. This technique might be helpful more generally. Sect. 5.4 contains the computation of the support function (Prop. 17), which proved to be more subtle than expected, even with a full understanding of the boundary. Finally the quantum properties, self-testing and all that, are established in Sect. 5.5.

5.1 Proof of Theorem 1

For the sake of this proof let us denote by $\mathcal{Q}_{(x)} \subset \mathbb{R}^4$ the set characterized by item (x) in Thm. 1. We have to show that these are all equal. The backbone of the proof is the chain

$$\mathcal{Q}_{(a)} \subset \mathcal{Q}_{(e)} = \mathcal{Q}_{(d)} = \mathcal{Q}_{(b)} \subset \mathcal{Q}_{(a)} \tag{53}$$

and separate arguments for $\mathcal{Q}_{(e)} = \mathcal{Q}_{(f)}$ and $\mathcal{Q}_{(b)} = \mathcal{Q}_{(c)}$. The main work will be getting the solution set $\mathcal{Q}_{(e)}$ of the matrix completion problem in great detail. The boundary information coming out of that, in particular for rank $C = 2$, will then be used to get the further equivalences and finally go back to $\mathcal{Q}_{(a)}$.

5.1.1 Making matrix completion real

The inclusion $\mathcal{Q}_{(a)} \subset \mathcal{Q}_{(e)}$ is an important step, because the definition of $\mathcal{Q}_{(a)}$ admits infinite Hilbert space dimension, while $\mathcal{Q}_{(e)}$ only allows finite dimension. This reduction step works for more parties, settings, and outcomes, as well, which is the whole point of the semidefinite hierarchies [26, 12]. But outside the minimal scenario the inclusion is strict.

We saw the inclusion $\mathcal{Q}_{(a)} \subset \mathcal{Q}_{(e)}$ at the beginning of Sect. 2.8. From the quantum model we naturally get a positive definite matrix with some unknown complex entries, and diagonal not equal to 1. These assumptions are part of the description of $\mathcal{Q}_{(e)}$, however. In order to prove $\mathcal{Q}_{(a)} \subset \mathcal{Q}_{(e)}$, we thus have to make sure that the additional assumptions do not make $\mathcal{Q}_{(e)}$ smaller. This is the content of Prop. 11.

Proof of Prop. 11

Consider a matrix $C \geq 0$ of the form (22) with diagonal entries $d_i \leq 1$, and let $C' = \Re e(C) = (C + \overline{C})/2$ be its entrywise real part. Then $C' \geq 0$ since the complex conjugate preserves positive semidefiniteness. Add to C' the matrix with diagonal entries $1 - d_i$ to get C''. Then $C'' \geq C' \geq 0$ is a matrix with the same off-diagonal c_{ij}, but in the standard form with u, v real and $d_i = 1$. ∎

5.1.2 Solving the real completion problem

In this and the following two sections, we proceed to actually solve the matrix completion problem defining $\mathcal{Q}_{(e)}$, i.e. decide which c permit real values u, v that make the following matrix positive semidefinite:

$$C = \begin{pmatrix} 1 & u & c_{11} & c_{12} \\ u & 1 & c_{21} & c_{22} \\ c_{11} & c_{21} & 1 & v \\ c_{12} & c_{22} & v & 1 \end{pmatrix}. \tag{54}$$

Equivalently, this is the decision problem for membership in the set $\{C | C \geq 0\}$, which is clearly the intersection of the cone of positive semidefinite with the hyperplane $\{M | \text{diag}(M) = (1, 1, 1, 1)\}$. The

solution uses Sylvester's criterion. We use the standard notation C_I for the principal submatrix selecting the rows and the columns specified by the indices in I, and $m_I = \det C_I$ for the corresponding principal minor. Sylvester's necessary and sufficient criterion for $C \geq 0$ is that $m_I \geq 0$ for all $2^n - 1$ index sets I, while for $C > 0$ is that $m_1, m_{12}, m_{123}, m_{1234} > 0$. The positivity of principal 2×2-minors gives $c_{ij}^2 \leq 1$ or equivalently $\mathcal{Q}_{(e)} \subset \mathcal{N}$ as a necessary condition. Consider next the principal 3×3-minors

$$C_{123} = \begin{pmatrix} 1 & u & c_{11} \\ u & 1 & c_{21} \\ c_{11} & c_{21} & 1 \end{pmatrix} \geq 0 \quad \text{and} \quad C_{124} = \begin{pmatrix} 1 & u & c_{12} \\ u & 1 & c_{22} \\ c_{12} & c_{22} & 1 \end{pmatrix} \geq 0. \tag{55}$$

These do not involve v, and they give a condition for u. We show that (55) is all we need to consider:

Lemma 25 *Suppose that, for some $u \in \mathbb{R}$, the matrices in (55) are positive semidefinite. Then one can find v such that in (54) we have $C \geq 0$, i.e., $c \in \mathcal{Q}_{(e)}$.*

Proof

We consider first the case of strict positivity, i.e., we are given $u \in \mathbb{R}$ satisfying (55) and additionally $C_{123} > 0$ and $C_{124} > 0$. This necessarily implies $|u| < 1$, by Sylvester's criterion. So far we have $m_1, m_{12}, m_{123} > 0$ so by Sylvester's criterion, we only need to find v such that $m_{1234} = \det C > 0$ in order to guarantee $C > 0$ for this v and the given u. Note that $\det C$ is a quadratic polynomial in v with a negative leading coefficient; therefore, if the desired v exists, the v maximizing this polynomial will do just as well. This is $v = (c_{11}c_{12} + c_{21}c_{22} - (c_{11}c_{22} + c_{12}c_{21})u)/(1 - u^2)$, and at that point we can compute the determinant and get

$$\max_{v \in \mathbb{R}} m_{1234} = (1 - u^2)^{-1} m_{123} m_{124} > 0. \tag{56}$$

This choice of v gives a completion $C > 0$ which is stronger than $C \geq 0$.

In general, we are only given $u \in \mathbb{R}$ satisfying (55). To reduce to the previous case, we consider a family $u(\lambda) \in \mathbb{R}$ satisfying $C_{123}(\lambda) > 0$ and $C_{124}(\lambda) > 0$, that depends on a parameter $0 < \lambda < 1$, constructed as follows: $C_{123}(\lambda) = \lambda C_{123} + (1 - \lambda)\mathbb{1}$, ditto for $C_{124}(\lambda)$, and with $u(\lambda) = \lambda u$. Applying our previous result, there exists $v(\lambda)$ making a completion $C(\lambda) > 0$. Observe that the $v(\lambda)$ that we took is then a continuous function of λ. Taking the limit $\lambda \to 1$, we have $u(\lambda) \to u$ by construction, $v(\lambda) \to v$ for some $v \in \mathbb{R}$ by continuity, and $C(\lambda) \to C \geq 0$. The principal submatrices 123 and 124 of C coincides with the given C_{123}, C_{124} we started with. Thus we found $v \in \mathbb{R}$ giving a completion $C \geq 0$ and the proof is complete. ∎

Alternatively, we could invoke a general result on semidefinite matrix completion [89, Theorem 7]: Consider the graph G whose edges represent the given entries of a partial matrix whose completion we seek. The obvious necessary conditions for completability are that for those subsets of vertices, where all matrix entries are specified (cliques of G), the corresponding submatrices are positive semidefinite. Then, if the graph is *chordal* (meaning any cycle of length ≥ 4 allows a shortcut), this condition is also sufficient. Moreover, this holds for both strict positive definiteness and semidefiniteness. In the case at hand, the graph given for $\mathcal{Q}_{(e)}$ is a 4-cycle shown in Fig. 20. Assuming the existence of u with $C_{123}, C_{124} \geq 0$ adds a diagonal, making the graph chordal. Hence no further condition needs to be considered.
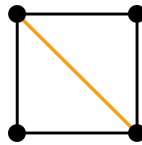
Figure 20: The black graph is the 4-cycle associated to $\mathcal{Q}_{(e)}$ with vertices 1, 3, 2, 4 starting from the upper-left corner. It is not chordal. On the other hand, adding the orange edge, which corresponds to assuming the existence of u satisfying (55), makes it chordal.

Lem. 25 eliminates v and leaves us with the nonnegativity of the following three principal minors:

$$\begin{array}{rccl} m_{12} &=& 1 - u^2 & (A) \\ m_{123} &=& 1 - c_{11}^2 - c_{21}^2 + 2c_{11}c_{21}u - u^2 & (B) \\ m_{124} &=& 1 - c_{12}^2 - c_{22}^2 + 2c_{12}c_{22}u - u^2 & (C) \end{array} \tag{57}$$

We have $c \in \mathcal{Q}_{(e)}$ if and only if these are simultaneously satisfied for the same u. By Helly's Theorem in $\mathbb{R}^1$ [90], the three positivity intervals have a common point if and only if they intersect pairwise. Hence we can consider pairwise intersections. The maximum of (B) is

$$\max_u m_{123} = (1 - c_{11}^2)(1 - c_{21}^2) = m_{13}m_{23} \geq 0, \tag{58}$$

attained at $u = c_{11}c_{21} \in [-1, 1]$, so its positivity interval intersects that of (A), and similarly for the pair (A, C). Hence only the pair (B, C) needs to be considered. We conclude:

Summary 26 *If $c \in \mathcal{N}$, then $c \in \mathcal{Q}_{(e)}$ if and only if (B) and (C) are both non-negative for some $u \in \mathbb{R}$.*

5.1.3 Joint positivity of two parabolas

We next examine the criterion in Sum. 26 independently of the specific context. We do the quantifier elimination carefully, because the structure of the solution explains the disjunction in Thm. 1 (d). Thus at the end of this section we will achieve the equality $\mathcal{Q}_{(e)} = \mathcal{Q}_{(d)}$.
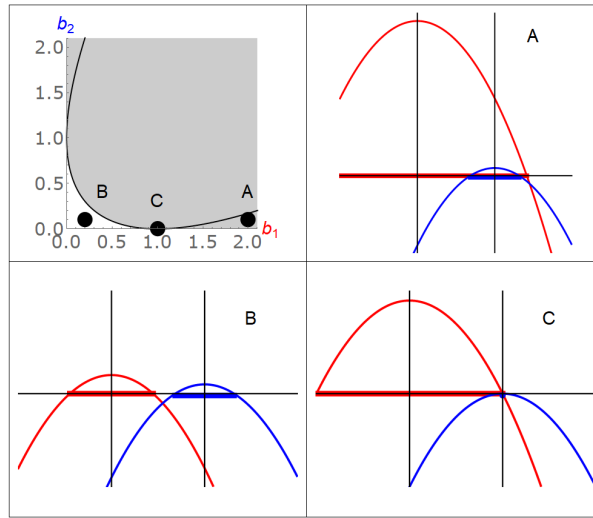

Figure 21: The configurations of two parabolas $f_i(x) = b_i - (x - a_i)^2$ with $a_1 = 0$ and $a_2 = 1$. Top Left: Parameter plane for (b_1, b_2). Shaded: region, where intersection of positivity ranges is nonempty. Points A,B,C: parameters for the other panels. Black Parabola: line at which the intersection of the parabolas lies on the x-axis.

The configurations of two parabolas in the following lemma are shown in Fig. 21. Both are given by quadratic polynomials $f(x) = b - (x - a)^2$ with the same negative quadratic term. The parameters are chosen so that $(x, y) = (a, b)$ is the location of the maximum. This function is positive in the interval $[a - \sqrt{b}, a + \sqrt{b}]$. The question is when for two such parabolas the positivity intervals overlap. It is clear that the problem is invariant under shifts (adding a constant to both a_1 and a_2), and $(a_1 - a_2)^2$ just sets a scale for the bs. Hence we could choose $a_1 = 0$ and $a_2 = 1$. Fig. 21 is drawn with this choice.

Lemma 27 *Given two quadratic polynomials $f_i(x) = b_i - (x - a_i)^2$, $i = 1, 2$, the following are equivalent:*

(1) There exists a point $u \in \mathbb{R}$ such that $f_1(u) \geq 0$ and $f_2(u) \geq 0$.
(2) $b_1 \geq 0 \wedge b_2 \geq 0 \wedge \left[b_1 + b_2 - (a_1 - a_2)^2 \geq 0 \vee 4b_1b_2 - (b_1 + b_2 - (a_1 - a_2)^2)^2 \geq 0 \right]$.

If one demands strict inequality then the following are also equivalent:

(1') There exists a point $u \in \mathbb{R}$ such that $f_1(u) > 0$ and $f_2(u) > 0$.
(2') $b_1 > 0 \wedge b_2 > 0 \wedge \left[b_1 + b_2 - (a_1 - a_2)^2 \geq 0 \vee 4b_1b_2 - (b_1 + b_2 - (a_1 - a_2)^2)^2 > 0 \right]$.

There is a very simple algebraic proof of this result which starts by solving $f_i(u) \geq 0$ for the domain of u that ensures positivity. Here we instead present a geometric proof based on Fig. 21. This proof

contains additional insights that allow verifying that $\mathcal{Q}$ is semialgebraic but not basic semialgebraic, and the semialgebraic description is not unique.

Proof
Clearly, both positivity ranges must be non-empty. Therefore, it is necessary that $b_1, b_2 \geq 0$. We can also trivially take care of the cases with $a_1 = a_2$, because then one positivity interval is contained in the other. The maximum of each parabola is clearly in the positivity interval. So if $b_1 \geq (a_1 - a_2)^2$ the maximum of the second parabola is in the positivity range of the first, and so there is a non-empty intersection. Symmetrically, this holds for $b_2 \geq (a_1 - a_2)^2$. This gives two closed rectangles in the (b_1, b_2)-plane with non-empty intersection.

Next consider the intersection of the two parabolas. Their unique intersection point is

$$\big(x_s, f_i(x_s)\big) \;=\; \left(\frac{a_1 + a_2}{2} - \frac{b_1 - b_2}{2(a_1 - a_2)}, \; \frac{4b_1 b_2 - \big(b_1 + b_2 - (a_1 - a_2)^2\big)^2}{4(a_1 - a_2)^2}\right). \tag{59}$$

Now suppose $f_i(x_s) \geq 0$. Then x_s is in the intersection of the positivity ranges. The corresponding region, defined by the positivity of the numerator of $f_i(x_s)$ in (59) is the closed parabola in the top left panel of Fig. 21. Hence we have non-zero intersection for the union of the two rectangles and the parabola in Fig. 21. This can be simplified as the union of just two regions, namely the parabola and the region $\{b_1 + b_2 \geq (a_1 - a_2)^2\}$, which contains the two rectangles plus a triangle, which is contained in the parabola.

To complete the proof of the first part, we need to show that, for any point outside this region, the positivity ranges have empty intersection. This complement is defined by the conditions $0 \leq b_i < (a_1 - a_2)^2$ and $f_i(x_s) < 0$. Now the first condition implies $|b_1 - b_2| < (a_1 - a_2)^2$. Hence the second term for x_s in (59) is bounded by $|a_1 - a_2|/2$, so x_s lies between a_1 and a_2. Therefore one of the maxima lies to the right of x_s and the other one lies on its left (as depicted in panel B of Fig. 21), and therefore the same holds for the positivity ranges of the parabolas. Since $f_i(x_s) < 0$ the ranges do not intersect. This completes the proof of the first part.

The primed statements characterize the interior of the parameter set, i.e., the region just described without the boundary points, for which $b_1 = 0$, or $b_2 = 0$ or $f_i(x_s) = 0$. ∎

We now apply Lem. 27 to the quadratic polynomials (B,C) in (57). The parameters are

$$\begin{aligned}
a_1 &= c_{11}c_{21}, & a_2 &= c_{12}c_{22}, \\
b_1 &= (1 - c_{11}^2)(1 - c_{21}^2), & b_2 &= (1 - c_{12}^2)(1 - c_{22}^2).
\end{aligned} \tag{60}$$

With this, the two polynomials in Lem. 27 (2) are g in (17) and h in (19). The combination of Sum. 26 and Lem. 27 now establishes the equivalence of (d) and (e) in Thm. 1. Furthermore, if $\pi : \mathbb{R}^6 \to \mathbb{R}^4$ denotes the projection $\pi(c, u, v) = c$, where we identify $\mathbb{R}^6$ with the real hermitian 4×4-matrices with unit diagonal, then $\mathrm{int}(\mathcal{Q}_{(e)}) = \mathrm{int}(\pi(\{C \geq 0\})) = \pi(\mathrm{int}(\{C \geq 0\})) = \pi(\{C > 0\})$. Thus, we have that the strict inequality result in Lem. 27 gives the characterization of the interior. We record this as follows:

Summary 28 $\mathcal{Q}_{(e)} = \mathcal{Q}_{(d)}$: *For $c \in \mathbb{R}^4$, we have $c \in \mathcal{Q}_{(e)}$ if and only if $c \in \mathcal{N}$ and $\big(g(c) \geq 0$ or $h(c) \geq 0\big)$. Furthermore, we have $c \in \mathrm{int}(\mathcal{Q}_{(e)})$ if and only if $c \in \mathrm{int}(\mathcal{N})$ and $\big(g(c) \geq 0$ or $h(c) > 0\big)$.*

5.1.4 Properties of the boundary and extreme points

Sum. 28 characterizes membership in the spectrahedral shadow $\mathcal{Q}_{(e)}$ and in its interior. We now come to its boundary which is the complement $\mathcal{Q}_{(e)} \setminus \mathrm{int}(\mathcal{Q}_{(e)})$, beginning with an extended version of the first statement in Prop. 12.

Lemma 29 *Given any point $c \in \mathcal{Q}_{(e)}$, the following three conditions are equivalent:*

(1) $c \in \partial\mathcal{Q}_{(e)}$.

(2) The matrix completion problem for c has a unique solution (u, v).

(3) Either $\big(c \in \partial\mathcal{N}$ and $g(c) \geq 0\big)$ or $\big(g(c) < 0$ and $\mathrm{rank}(C) \leq 2$ for every completion C of $c\big)$.

Proof

As before, let $\pi : \mathbb{R}^6 \to \mathbb{R}^4$ denote the projection $\pi(c, u, v) = c$, where we identify $\mathbb{R}^6$ with the real hermitian 4×4-matrices with unit diagonal.

not(1)⇒not(2)

Suppose that c is in the interior of $\mathcal{Q}_{(e)}$. Then we can write $c = \lambda 0 + (1 - \lambda)c''$ for some other $c'' \in \mathcal{Q}_{(e)}$ and $0 < \lambda \leq 1$. Then if $\pi(C'') = c''$, we get $C = \lambda \mathbb{1} + (1 - \lambda)C''$ with $\pi(C) = c$. This C has rank 4 since the eigenvalues is $\lambda + (1 - \lambda)\mathrm{eig}(C'')$, and a small ball $\mathcal{B}$ around C is still contained in the positive cone. Therefore the intersection $\pi^{-1}(c) \cap \mathcal{B}$ is a two-dimensional set, in the parameters (u, v), of matrix completions for c.

not(1)⇒not(3)

The first condition in (3) fails because $\mathrm{int}(\mathcal{Q}_{(e)}) \subset \mathrm{int}(\mathcal{N})$, and the second one fails because the preimage C just constructed has rank 4.

((1) and $c \in \partial\mathcal{N}$)⇒((2) and (3))

When c is in the boundary of the cube we must have $c_{ij} = \pm 1$ for some (i, j). Up to symmetry we may assume $c_{11} = -1$. Then from the form (57) of the principal minors we get that $m_{123}(u) = -(u + c_{21})^2$ and $m_{134}(v) = -(v + c_{12})^2$. These must be non-negative for any matrix completion, fixing $u = -c_{21}$ and $v = -c_{12}$. So (2) holds. Moreover, from (18) we see that $h(c) = -g(c)^2 \leq 0$. With $h(c) < 0$, Sum. 28 implies $g(c) \geq 0$, and with $h(c) = 0$ this is anyhow true. So the first alternative in (3) holds.

((1) and $c \notin \partial\mathcal{N}$)⇒((2) and (3))

By negation, the second sentence in Sum. 28 provides a characterization of $c \in \partial\mathcal{Q}_{(e)}$. Together with $c \notin \partial\mathcal{N}$ this implies ($g(c) < 0$ and $h(c) \leq 0$). On the other hand, $g(c) \geq 0$ or $h(c) \geq 0$ from $c \in \mathcal{Q}_{(e)}$. Together we have $h(c) = 0$. Hence the parabolas from Lem. 27 have a unique point of intersection at level 0. This point is given either by $u = a_1 - \sqrt{b_1} = a_2 + \sqrt{b_2}$, or $u = a_2 - \sqrt{b_2} = a_1 + \sqrt{b_1}$. Analogously there is also a unique v, and (2) holds. Moreover, these unique choices u, v make all third order principal minors $m_{123}, m_{124}, m_{234}, m_{134}$ vanish. This means $\mathrm{rank}(C) \leq 2$, and we obtain the second sentence of (3). ∎

The next lemma shows how the trigonometric functions arise in the parametrization of the boundaries.

Lemma 30

(1) If c is extremal in $\mathcal{Q}_{(e)}$ then it must have a unique matrix completion with $\mathrm{rank}\, C \leq 2$.

(2) It must then be of the form $c_{ij} = a_i \cdot b_j$ for unit vectors a_1, a_2, b_1, b_2 in the Euclidean space $\mathbb{R}^2$.

(3) This means that it can be written as $c_{ij} = \cos(\alpha_i - \beta_j)$ for some $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{R}$.

Proof

(1) Of course, extreme points are always part of the boundary, because any line segment through an extreme point necessarily contains some points outside the body. Hence the previous Lemma applies. So by part (3) of the previous Lemma they either have $\mathrm{rank}\, C \leq 2$ anyway, or else belong to a face of the cube $\mathcal{N}$. Up to symmetry this means $c_{22} = 1$. Then $C_{124} \geq 0$ forces $u = c_{12}$, so the extendability is just the elliptope condition $\det C_{123} = 1 - c_{11}^2 - c_{12}^2 - c_{21}^2 + 2c_{11}c_{12}c_{21} \geq 0$. Since c is furthermore extremal, it remains extremal in this face (direct verification). This implies c must belong to the boundary of the elliptope, namely this inequality must be tight, and so $\mathrm{rank}\, C_{123} \leq 2$. Since all 3×3 minors of C are zero, $\mathrm{rank}\, C \leq 2$.

(2) By the spectral theorem, every positive semidefinite $d \times d$ matrix can be written as a Gram matrix, i.e, $C_{\alpha\beta} = w_\alpha \cdot w_\beta$ for vectors $w_1, \ldots, w_d$ in some Euclidean space $\mathbb{R}^r$. Here $r = \mathrm{rank}\, C$ is the number of non-zero eigenvalues. In our case the diagonal matrix entries are 1, so these vectors are unit vectors. Moreover, the c_{ij} are themselves matrix elements of C, so we just need to rename the vectors according to whether the dimension belongs to Alice or to Bob, i.e., $a_1 = w_1$, $a_2 = w_2$, $b_1 = w_3$, and $b_2 = w_4$.

(3) Unit vectors in $\mathbb{R}^2$ lie on the unit circle, parameterized by angles. Scalar products between such vectors are the cosines of the enclosed angle. Setting $w_i = (\cos\alpha_i, \sin\alpha_i)$ for some $\alpha_i \in \mathbb{R}$, we thus have

$$C = \begin{pmatrix} 1 & \cos(\alpha_1 - \alpha_2) & \cos(\alpha_1 - \alpha_3) & \cos(\alpha_1 - \alpha_4) \\ \cos(\alpha_1 - \alpha_2) & 1 & \cos(\alpha_2 - \alpha_3) & \cos(\alpha_2 - \alpha_4) \\ \cos(\alpha_1 - \alpha_3) & \cos(\alpha_2 - \alpha_3) & 1 & \cos(\alpha_3 - \alpha_4) \\ \cos(\alpha_1 - \alpha_4) & \cos(\alpha_2 - \alpha_4) & \cos(\alpha_3 - \alpha_4) & 1 \end{pmatrix}. \tag{61}$$

Renaming according to the Alice/Bob distinction, i.e. $\alpha_3 = \beta_1$ and $\alpha_4 = \beta_2$, we obtain the claim. ∎

Part (2) of Lem. 30 says that $\partial_e \mathcal{Q}_{(e)} \subset \mathcal{Q}_{(f)}$, and part (3) that $\partial_e \mathcal{Q}_{(e)} \subset \mathcal{Q}_{(b)}$. Since $\mathcal{Q}_{(f)}$ is convex by a direct sum construction, and $\mathcal{Q}_{(b)}$ is anyhow defined to be convex, this also means that $\mathcal{Q}_{(e)} \subset \mathcal{Q}_{(f)}$ and $\mathcal{Q}_{(e)} \subset \mathcal{Q}_{(b)}$. The first of these inclusions can be inverted trivially, because we can just set $u = a_1 \cdot a_2$ and $v = b_1 \cdot b_2$ to get a matrix completion from the unit vectors a_i, b_j. To revert the second inclusion, we have to combine Sum. 28, the inclusion $\mathcal{Q}_{(a)} \subset \mathcal{Q}_{(e)}$ from Sect. 5.1.1, and the concrete quantum models from Sect. 4.1, which realize all cosine parametrized c, and thus show $\mathcal{Q}_{(b)} \subset \mathcal{Q}_{(a)}$. Altogether this gives

Summary 31 $\mathcal{Q}_{(e)} = \mathcal{Q}_{(f)}$, $\mathcal{Q}_{(e)} = \mathcal{Q}_{(d)}$, and $\mathcal{Q}_{(a)} \subset \mathcal{Q}_{(e)} \subset \mathcal{Q}_{(b)} \subset \mathcal{Q}_{(a)}$, i.e., all these sets are equal.

This leaves only one part of Thm. 1, namely the equality with $\mathcal{Q}_{(c)}$. This will be shown in Sect. 5.1.5. Also, we have established one part of Prop. 8, the cosine parametrization, in a slightly different parametrization. The parametrization used in Prop. 8 and Prop. 9 follows from the form (61) by setting

$$\alpha = \alpha_1 - \alpha_3, \quad \beta = \alpha_4 - \alpha_1, \quad \gamma = \alpha_3 - \alpha_2, \quad \delta = \alpha_2 - \alpha_4. \tag{62}$$

Note that the signs were chosen (not changing the respective cosine) such that $\alpha + \beta + \gamma + \delta = 0$. This constraint reflects the fact that only differences $\alpha_i - \alpha_j$ enter. What we have not shown yet, however, is the criterion $\Delta < 0$ for a tuple of angles to give an extreme point. This will be done in Sect. 5.3.2.

5.1.5 The pushout characterization

The continuous map $t \mapsto \sin(\pi t/2)$ takes the interval $[-1, 1]$ to itself, and it has a continuous inverse. By applying this map coordinate-wise, we conclude that the pushout map in (15) is a homeomorphism from the cube $\mathcal{N} = [-1, 1]^4$ to itself. Here we shall establish Prop. 5, which states that $\mathcal{Q} = \sin(\mathcal{C})$. Note that in the literature of matrix completion, this is often presented as $\mathcal{Q} = \cos(\pi \mathrm{MET}(K_{2,2}))$ which is obvious if one realizes that the metric polytope $\mathrm{MET}(K_{2,2})$ of the complete bipartite graph $K_{2,2}$ is isomorphic to the classical polytope $\mathcal{C}$. See [39] and references therein.

Our strategy is to show this for the boundaries, i.e., $\sin(\partial \mathcal{C}) = \partial \mathcal{Q}$. Suppose that we know this, then notice that $\sin$ maps connected components of $\mathcal{N} \setminus \partial \mathcal{C}$ to connected components of $\mathcal{N} \setminus \partial \mathcal{Q}$. Since 0 is in both the classical polytope and the quantum set, and $\sin(0) = 0$ we get that $\mathcal{C}$ is precisely mapped to $\mathcal{Q}$. Hence equality of the boundaries is sufficient.

We examine the boundary of the demicube $\mathcal{C}$ facet by facet. This task is greatly reduced by symmetry, given that $\sin$ commutes with all symmetry operations as explained in Sect. 2.4. Only one CHSH face and one $\mathcal{N}$-face need to be considered. Consider first the CHSH facet $\{(x, y, z, w) \in [-1, 1]^4 : x + y + z - w = 2\}$. The images of the points on this facet under the pushout map $\sin$ are

$$\sin(x, y, z, w) = \left(\sin\left(\frac{\pi}{2}x\right), \sin\left(\frac{\pi}{2}y\right), \sin\left(\frac{\pi}{2}z\right), \sin\left(\frac{\pi}{2}w\right) \right) = (\cos\alpha, \cos\beta, \cos\gamma, \cos\delta), \tag{63}$$

where $\alpha = \pi(1-x)/2$, $\beta = \pi(1-y)/2$, $\gamma = \pi(1-z)/2$, $\delta = \pi(w-1)/2$. This gives $\alpha + \beta + \gamma + \delta = \pi - (x + y + z - w)\pi/2 = 0$. Moreover, $x, y, z, w \in [-1, 1]$ implies $\alpha, \beta, \gamma \in [0, \pi]$ and $\delta \in [-\pi, 0]$. These inequalities imply $\Delta = \sin\alpha \sin\beta \sin\gamma \sin\delta \leq 0$. Hence we get exactly those parametrized patches ($\mathcal{Q}$qx) from Prop. 8, for which $\alpha, \beta, \gamma > 0 > \delta$. The other seven patches ($\mathcal{Q}$qx) are obtained by symmetry.

Next consider an $\mathcal{N}$-face of $\mathcal{C}$, say that defined by $w = 1$. The pushout map preserves this equation. We can now go through the same considerations as above, but in one dimension lower. The geometric statement is that the pushout of the tetrahedron equals the elliptope (see Fig. 7). This also follows from the fact that $\sin$ identifies their boundaries. We know this from the above discussion of the CHSH facets.

Together with Sum. 31 this completes the proof of Thm. 1.

5.2 Self-duality

Self-duality is a special feature of the pair $\mathcal{Q}, \mathcal{Q}^\circ$. It is *not* the kind of property that tends to hold for any sufficiently simple case. Indeed, in one dimension smaller, the elliptope $\mathcal{E}^3$ (see Fig. 7) is not self-dual: It has extreme points with a pointed normal cone, which translate to flat faces in $(\mathcal{E}^3)^\circ$. But $\mathcal{E}^3$ has no such faces, and hence is not self-dual. For an illustration of this phenomenon see [18, Figure 5.2].

With the boundary information obtained so far one could try to derive self-duality extreme point by extreme point. We take a more global approach based on the duality of the semidefinite matrices C and F, and their representations as Gram matrices. We begin with the characterization of the F matrices.

Proof of Prop. 15

The primal/dual characterization of spectrahedral shadows described briefly before the statement of Prop. 15 is a standard result, so we omit its proof and are left with the additional property $p_1 + p_2 = p_3 + p_4$ (necessarily $= 1$). We can take $p_1 + p_2$ and $p_3 + p_4$ both non-zero, since otherwise we have the trivial case $f = 0$, $F = \frac{1}{2}\mathbb{1}$. Indeed, if $p_1 + p_2 = 0$ then since $p_1, p_2 \geq 0$ it must be that $p_1 = p_2 = 0$. Now analyze the positivity of the 2×2 minor containing f_{11} to get $f_{11} = 0$ and likewise for all f_{ij}. (The reader might be tempted to conclude $F = 0_{2 \times 2} \oplus \mathbb{1}_{2 \times 2}$, but this will not achieve what we want.) Forgetting what we have just argued, given $f = 0$ there is clearly a completion $F = \frac{1}{2}\mathbb{1}$ that has the property $p_1 + p_2 = p_3 + p_4 = 1$.

Now observe that $F' = \Lambda F \Lambda$, where Λ is the diagonal matrix with diagonal $(\lambda, \lambda, \lambda^{-1}, \lambda^{-1})$ is also positive, and has the same off-diagonal block f_{ij}. The diagonal is changed to $(p'_1, p'_2, p'_3, p'_4) = (\lambda^2 p_1, \lambda^2 p_2, \lambda^{-2} p_3, \lambda^{-2} p_4)$. In order to satisfy the sum constraint we need $\lambda^2 = (p_3 + p_4)/(p_1 + p_2)$. Then $(F + F')/2$ is the desired extension with $p_1 + p_2 = p_3 + p_4$. This is different from F, if $\lambda^2 \neq 1$.

Finally, using a similar argument, we show that if the point f has a completion F for which the condition $p_1 + p_2 = p_3 + p_4 = 1$ does not hold, then f is not extreme. Using the diagonal matrix with $(\lambda_A, \lambda_A, \lambda_B, \lambda_B)$, and assuming, without loss that $x = p_1 + p_2 - 1 > 0$, the normalization condition becomes $\lambda_A^2(1 + x) + \lambda_B^2(1 - x) = 2$. Then choosing both terms equal to 1 maximizes $\lambda_A \lambda_B = (1 - x^2)^{-1/2} > 1$. We conclude that $f'_{ij} = \lambda_A \lambda_B f_{ij}$ is again in $\mathcal{Q}^\circ$, so f is not a boundary point. ∎

We now consider matrices C and F as Gram matrices of suitable vectors in a real Euclidean space. That is, we choose a_1, a_2, b_1, b_2 from the characterization (f) in Thm. 1, and similarly four vectors x_1, x_2, y_1, y_2 whose scalar products give F, and $-f_{ij} = x_i \cdot y_j$. The conditions for these vectors for C to be of the form (54) and F to be of the form (35) with $p_1 + p_2 = 1$ are

$$\|a_1\| = \|a_2\| = 1 \qquad \text{and} \qquad x_1 \perp x_2, \quad \|x_1\|^2 + \|x_2\|^2 = 1, \tag{64}$$

and analogous conditions for b_j and y_j. The sets of vectors can be mapped to each other by

$$a_1 = x_1 + x_2, \quad a_2 = x_1 - x_2 \quad \text{and} \qquad x_1 = (a_1 + a_2)/2, \quad x_2 = (a_1 - a_2)/2. \tag{65}$$

With the analogous relations for the b_j and y_j we get a bijective correspondence between the allowed vectors. Expressing the relation by the 2×2-Hadamard matrix $H_2 = 2^{-1/2} \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix} \right)$ and inserting the relations into $c_{ij} = a_i \cdot b_j$ this correspondence relates the 4-vector $c = (c_{11}, c_{12}, c_{21}, c_{22})$ to the corresponding $f \in \mathbb{R}^4$ by $H = H_2 \otimes H_2$, i.e., (29). This proves the duality theorems Prop. 13 and Thm. 3.

5.3 Further boundary properties

The pushout characterization makes the disjoint union structure of Prop. 7 obvious, but we need to verify various geometric properties of strata mentioned in that proposition.

5.3.1 Classification of boundary points by rank

We now show the rank statements in Prop. 12, and the parametrization of boundary points in Prop. 9. Rather than treating these separately, we prove them together, following the classification of boundary points in Prop. 7. We organize these items firstly by the options given in Lem. 29, and secondly by rank C, where C is a matrix completion for c. Again, let us recall the projection $\pi : \mathbb{R}^6 \to \mathbb{R}^4$ used in the proof of Lem. 29.

($\mathcal{Q}$in) $\Leftrightarrow$ rank C may be 4.
If C has rank 4, then so have the points in some open ball $\mathcal{B} \ni C$. Since the projection is an open map,

$\pi(\mathcal{B})$ is open. Hence $c = \pi(C) \in \pi(\mathcal{B}) \subset \mathcal{Q}$ is in the interior. For the converse note that, for any pair of interior points c, c', we can write c as a convex combination in which c' has positive weight. Hence if c' has a full rank completion, so does c, i.e., every interior point. (An explicit version of this, with $c' = 0$, $C' = \mathbb{1}$, was used in the beginning of the proof of Lem. 29.)

From here to the end of this proof, c will be in the boundary, and so c has a unique completion C by Lem. 29. In the twofold case distinction of Lem. 29 (3) we now begin with the first case, $c \in \partial\mathcal{N}$, so that for at least one pair (i,j) we have $|c_{ij}| = 1$. Up to symmetry we can take $c_{11} = 1$. Then the vector $(1, 0, -1, 0)$ is in the kernel of C, and, consequently rows/columns 1 and 3 of C are proportional, and rank $C \leq 3$.

$(\mathcal{Q}\mathbf{ei}) \Leftrightarrow c \in \partial\mathcal{Q}$ and rank $C = 3$.
Consider the submatrix C_{124} of C obtained by deleting the redundant 3rd row/column, that is the second matrix in (55) with $u = c_{21}$. Its semidefiniteness means that (c_{12}, c_{21}, c_{22}) is in the closed elliptope. It has full rank, i.e., rank $C = \text{rank } C_{124} = 3$, precisely if c is in the interior of this elliptope. Note that the second case of Lem. 29 (3) contributes no further cases with rank 3, so that the implication "$\Leftarrow$" holds in all cases.

From now on we have rank $C \leq 2$, and so by Lem. 30 (3), the matrix C lies in the cosine-parametrized family written out in (61). We consider instead differences of angles as variables $(\alpha, \beta, \gamma, \delta)$, as in Prop. 8 and Prop. 9. Since $(c_{11}, c_{12}, c_{21}, c_{22}) = (\cos\alpha, \cos\beta, \cos\gamma, \cos\delta)$, the condition $c_{ij} = \pm 1$ defining a facet of $\mathcal{N}$ just correponds to the corresponding angle being a multiple of π.

$(\mathcal{Q}\mathbf{nx}) \Leftrightarrow c \in \partial\mathcal{Q}$, rank $C = 2$, and for exactly one pair (i,j) we have $|c_{ij}| = 1$.
$(\mathcal{Q}\mathbf{ce}) \Leftrightarrow c \in \partial\mathcal{Q}$, rank $C = 2$, and for exactly two pairs (i,j) we have $|c_{ij}| = 1$.
We are still in the closed elliptope (Fig. 7). The boundary is singled out either by the reduced rank, or equivalently the cosine parametrization with one angle a multiple of π. The generic boundary points are exposed in 3 dimensions, but (as we will see in Sect. 5.3.4) not in 4 dimensions. (This is a general feature of exposedness: it depends on the ambient convex set and space.) If c in Fig. 7 lies in a facet of the 3-cube, i.e., one more angle becomes a multiple of π, we get a point on an edge of $\mathcal{Q}$. This proves the two equivalences above.

$(\mathcal{Q}\mathbf{cx}) \Leftrightarrow c \in \partial\mathcal{Q}$ and rank $C = 1$
Of course, we may set even more $|c_{ij}| = 1$. When three angles are multiples of π, so must be the fourth, since they add up to zero. This is also geometrically obvious from Fig. 7: The only points of $\mathcal{Q}$ that lie on an edge of the 3-cube are endpoints. So in this case we have a classical extreme point. It is easy to see that this implies rank 1: Up to symmetry this is the case $c_{ij} = 1$ for all $i, j = 1, 2$, which clearly has the rank 1 matrix $C_{ij} \equiv 1$ as a completion. For the converse, note that rank $C = 1$ and $C \geq 0$ imply $C_{ij} = x_i x_j$ for some vector x, and $c_{ij} = x_i x_{j+2}$. If we now insist on the special form of C from Prop. 11, i.e., unit diagonal, we must have an extreme point just from the rank condition. However, with $|x_i| < 1$, we get even many interior rank 1 points. Therefore, in the above equivalence $c \in \partial\mathcal{Q}$ needs to be imposed as well.

$(\mathcal{Q}\mathbf{qx}) \Leftrightarrow c \in \partial\mathcal{Q} \cap (\text{int}\,\mathcal{N}) \Leftrightarrow \Delta < 0$ in Prop. 8
Finally, we come to the other branch of Lem. 29 (3). From the semialgebraic description of $\mathcal{Q}$ in Prop. 10 this type consists of the points $c \in \mathcal{N}$ with $h(c) = 0$ and $g(c) < 0$. But for the cosine parametrized correlations with $\delta = -(\alpha + \beta + \gamma)$ we get the identity

$$g(\cos\alpha, \cos\beta, \cos\gamma, \cos\delta) = 2\Delta. \tag{66}$$

This completes the proofs of Prop. 12 and Prop. 9.

5.3.2 Exposing functionals: first order analysis

Proof of Prop. 14
Since c is a boundary point, we have $c \cdot f = \max\{c \cdot f' | f' \in \mathcal{Q}^\circ\} = 1$ for some $f \in \mathcal{Q}^\circ$. Indeed, if the maximum over the compact set $\mathcal{Q}^\circ$ were $M < 1$, we would have $c/M \in \mathcal{Q}^{\circ\circ} = \mathcal{Q}$, and c would be in the interior. We fix some such f. Thus $c' \cdot f$ has a global maximum at $c' = c$, and therefore a local maximum on the surface $c_{ij} = \cos\theta_{ij}$ with $\sum_{ij}\theta_{ij} = 0$ where the θ_{ij} are the given angles.

We analyze this extremum problem by introducing a Lagrange multiplier λ. The critical equations are

$$0 = d\Big(\sum_{ij} f_{ij}\cos(\theta_{ij}) + \lambda\theta_{ij}\Big) = \sum_{ij}\big(-f_{ij}\sin(\theta_{ij}) + \lambda\big)\,d\theta_{ij}. \tag{67}$$

Because $\Delta < 0$, all $\sin(\theta_{ij}) \neq 0$, and $f_{ij} = \lambda/\sin(\theta_{ij})$. The multiplier is determined from $c \cdot f = 1$ to be $\lambda^{-1} = \sum_{ij}\cot\theta_{ij} \equiv K$. Hence a maximizing f is unique, and given by the formula. ∎

This proof utilizes our knowledge from other sources that such c are extremal. When computing the convex hull of a parametrized surface (as in [45]) this is the tricky part. We can compute the tangent hyperplane at every point of such a surface, but is the local extremum a global maximum? It is then natural to look first at the local criterion and to rule out saddle points. That is, by looking at the parametrization in second order Taylor approximation, we can determine whether the surface is locally on one side of the tangent plane. If not, the point can be omitted from the list of potential extreme points. We carried this out for the case at hand, and found that *all* points with $\Delta > 0$ are saddles.

When a variety is not given by a parametrization, but by implicit equations, the first order analysis is just the definition of the dual variety. From the self-duality of the convex body we thus conclude that $\{h = 0\}$ is a self-dual variety. For the study of $\mathcal{Q}$ this is not only modified by intersecting with the cube, but also by eliminating the branch of the variety in the interior of $\mathcal{Q}$. Under dualization these operations are connected, i.e., the duals of the normalized tangents of interior points end up outside the dual body.

5.3.3 Unique CHSH violation

It is clear that each curved tetrahedron, being the pushout of a CHSH-face, violates exactly that CHSH inequality. That this is true for all non-classical correlations is an elementary fact that we have not used otherwise. Its self-dual version has likewise nothing to do with $\mathcal{Q}$, but only with the enclosing polytopes $\mathcal{C}$ and $\mathcal{N}$. It states that for any non-trivial Bell inequality, i.e., for any affine inequality valid for all classical correlations ($f \in \mathcal{C}^\circ$), which is not true by virtue of positivity constraints alone ($f \notin \mathcal{N}^\circ$) there is a unique non-local box ($c \in \partial_e\mathcal{N}$) making this evident ($c \cdot f > 1$).

Proof of Prop. 4

The 8 CHSH inequalities are $\pm c_{11} \pm c_{12} \pm c_{21} \pm c_{22} \leq 2$, where the product of the signs is -1. Given two distinct inequalities of this sort, the signs cannot be equal in all four places (then the inequalities would be the same), and also not in three places (because this would imply equality on the fourth place). Adding two violated inequalities ($\cdots > 2$) thus gives $\pm 2c_{ij} \pm 2c_{kl} > 4$, which contradicts the inequality $|c_{ij}| \leq 1$ following from non-signalling. Hence at most one such inequality is violated for $c \in \mathcal{N}$. On the other hand, for $c \notin \mathcal{C}$ at least one is violated. ∎

5.3.4 Face orthogonality

We now consider the normal cycle and the orthogonality relations of faces. Some claims about exposedness are already made in Prop. 7. These and the entries in Table 1 will now be treated in detail. As in Sect. 5.3, statements are grouped by boundary types. For points $\{c\}$ of each type we must identify the functionals $f \in \mathcal{Q}^\circ$ attaining the maximal value 1 at c, i.e., the face $\{c\}^\perp$. Note that the orthogonal face operation

$$S^\perp = \{f \in \mathcal{Q}^\circ | \forall c \in S \subset \mathcal{Q},\ c \cdot f = 1\} \tag{68}$$

also depends on the whole convex body in which this is taken (here: $\mathcal{Q}$). We will write $S^{\perp c}$ and $S^{\perp\mathcal{N}}$ when we take orthogonal complements with regards to $\mathcal{C}$ and $\mathcal{N}$ respectively. Obviously, the operation is monotone in the sense that for $S \subset \mathcal{C}$ we have $S^{\perp\mathcal{N}} \subset S^\perp \subset S^{\perp c}$.

$(\mathcal{Q}\text{cx})^\perp = [\mathcal{Q}\text{ei}] = (\mathcal{Q}\text{ei})\cup(\mathcal{Q}\text{nx})\cup(\mathcal{Q}\text{ce})\cup(\mathcal{Q}\text{cx})$:
Consider a classical extreme point in $(\mathcal{Q}\text{cx})$; without loss of generality $c = (1, 1, 1, 1)$. Then $\{c\}^\perp \subset \{c\}^{\perp c}$, i.e., $\{c\}^\perp$ is a face contained in a facet of the cube $\mathcal{C}^\circ$. This was our definition of an $\mathcal{N}$-face. Since these characterizations are taken over by self-duality, let us look at $2Hf$ for $f \in \{c\}^\perp$. The first component $(2Hf)_{11}$ is just $c \cdot f = 1$; the others (with maybe a sign added) are the scalar products of f with all the other classical points, which need to be ≤ 1 for $f \in \mathcal{Q}^\circ$. Hence $2Hf$ is indeed in the standard cube, with $(2Hf)_1 = 1$. The condition $2Hf \in \mathcal{Q}$ singles out an elliptope satisfying the third order inequality,

which in terms of f is the elementary symmetric polynomial appearing in (43), albeit with the opposite inequality. Note that $\{c\}^\perp$ is thus the closed elliptope $[\mathcal{Q}\text{ei}]$, which also contains boundary points of type $(\mathcal{Q}\text{cx}),(\mathcal{Q}\text{ce}),(\mathcal{Q}\text{nx})$. Computing their complements, as we will do presently, will give faces including c.

$(\mathcal{Q}\text{ei})^\perp = (\mathcal{Q}\text{cx})$:
Starting from an interior elliptope point c, self-duality gives us essentially the dual of the previous paragraph. More explicitly, set $c = (1, x, y, z)$ with $1 - x^2 - y^2 - z^2 + 2xyz \geq 0$, and $x^2, y^2, z^2 < 1$, to avoid edges and classical extreme points. For an interior point, the equality $c \cdot f = 1$ clearly extends from c to the face generated by this. Hence f must be $(1, 0, 0, 0)$, and $2Hf = (1, 1, 1, 1)$ is the classical extreme point considered in the previous paragraph.

$(\mathcal{Q}\text{nx})^\perp = (\mathcal{Q}\text{cx})$:
More care is needed for elliptope boundary points, because, in principle, this could allow more freedom for f. We will use the local extremality in the sense of Sect. 5.3.2, with angles $\theta_{11} = 0$, and $\sin(\theta_{ij}) \neq 0$ for the other $(i, j) \neq (1, 1)$. Then the equation $f_{ij}\sin(\theta_{ij}) = \lambda$ implies $\lambda = 0 \cdot f_{11} = 0$; since the other sines are $\neq 0$, then once again the only possibility is $f = (1, 0, 0, 0)$. This shows that the $(\mathcal{Q}\text{nx})$-points are indeed non-exposed extreme points as claimed in Prop. 7.

$(\mathcal{Q}\text{ce})^\perp = [\mathcal{Q}\text{ce}] = (\mathcal{Q}\text{ce}) \cup (\mathcal{Q}\text{cx})$:
Now consider a point c on an edge, but not an endpoint. This forces exactly two angles, say $\theta_{11} = \theta_{12}$, to be zero (cf. Prop. 9) and by the same reasoning used in the previous paragraph, $\lambda = 0$, and $f_{21} = f_{22} = 0$. However, f_{11} and f_{12} remain unconstrained and merely have to add up to 1. Remarkable here is that we get a drop of expected dimension from $\mathcal{C}$, where the complement of and edge is a 2-dimensional face:

$$\{(1, 1, 0, 0)\}^{\perp c} = \left\{ ((1+x)/2, (1-x)/2, y/2, -y/2) \mid |x| + |y| \leq 1 \right\}. \tag{69}$$

Geometrically, 3-dimensional faces of $\mathcal{C}$ containing this edge meet at an angle, whereas the corresponding elliptopes are tangent. This difference is explicitly seen comparing the rows of Fig. 8.

$(\mathcal{Q}\text{qx})^\perp = (\mathcal{Q}\text{qx})$:
Here points go to points, as discussed in detail in Sect. 5.3.2.

Table 1 also gives the manifold dimensions of each boundary type. We only have one continuous family of type $(\mathcal{Q}\text{qx})$, of dimension 3. All other types occur only in discrete instances, i.e., with dimension zero.

5.4 Support function

As described in Sect. 3.5, we seek the criteria for a ray to hit the boundary of $\mathcal{Q}^\circ$ either in an exposed extreme point or in an $\mathcal{N}$-face. The relevant geometry is shown in Fig. 8. A point in these diagrams represents a ray, and the separating surfaces precisely mark the distinction we need to study here. The problem becomes almost trivial, however, if we already know by which face the ray leaves the surrounding cube: Then we just have to check whether the boundary point is inside or outside the elliptope, for which we have a convenient third order criterion. The following proof is based on the case distinction by cube faces. But since these are all connected by symmetries, it boils down to just considering one case.

Proof of Prop. 17
    (1)⇔(2): We use the normal cycle: The set of pairs $(c, f) \in \mathbf{N}(\mathcal{Q})$ such that both c and f are uniquely determined when the other is fixed is just the stratum $(\mathcal{Q}\text{qx},\text{qx})$. Hence, if f is of type $(\mathcal{Q}\text{qx})$, so is c.
    Reduction by symmetry:
Applying a symmetry to f, i.e., a permutation of the components or an even number of sign changes, clearly does not change the validity of (1), (2), (3), or (4), while (5) respects the symmetry by requiring the necessary transformation to be made first. Hence it suffices prove for f in a standard form achievable by symmetry transformation. Since all extreme points of $\mathcal{C}$ are connected by symmetry we can assume, as required in (5) that a maximizer for $c \cdot f$ in $\partial_e\mathcal{C}$ is $c = (1, 1, 1, 1)$. Now suppose that two or more coordinates $f_{ij} < 0$. Then, by applying an even sign change to c we could increase $c \cdot f$. So our assumption actually rules out more than one negative sign. By the same argument, if there is a negative sign, this must be on an f_{ij} which minimizes $|f_{ij}|$. By a permutation we may assume that this element is f_{22}.
    We can quickly handle the case that all $f_{ij} \geq 0$. In that case, $\max\{c \cdot f | c \in \mathcal{C}\} = \sum_{ij} f_{ij} = \sum_{ij} |f_{ij}| = \max\{c \cdot f | c \in \mathcal{N}\}$. So the maximum over $\mathcal{Q}$ is attained at a classical point, $p(f) \geq 0$ and the product in

(43) cannot be < 0, so all conditions evaluate to false. So we may assume that there is just one negative sign and sort the remaining f_{ij}. That is, from now on we take

$$f_{11} \geq f_{12} \geq f_{21} \geq |f_{22}| > 0 > f_{22}. \tag{70}$$

$(1) \Leftrightarrow (5)$: We use the same classification of boundary points for $\mathcal{Q}$ and $\mathcal{Q}^\circ$ via duality transform. So (1) means that $c = 2Hf$ is a multiple of a $(\mathcal{Q}qx)$ point. We know that the component with the largest absolute value is the first, $c_{11} = \sum_{ij} f_{ij}$. Thus the point where the ray $\mathbb{R}c$ intersects the boundary of $\mathcal{N}$ is $(1, c_{12}/c_{11}, c_{21}/c_{11}, c_{22}/c_{11}) = (1, x, y, z)$. This is in an $\mathcal{N}$-facet of $\mathcal{Q}$ if and only if $1 - x^2 - y^2 - z^2 + 2xyz \geq 0$. Otherwise, this intersection is already outside of $\mathcal{Q}$, and hence the ray intersects $\partial \mathcal{Q}$ at a $(\mathcal{Q}qx)$ point. So the necessary and sufficient condition for (1) is that the cubic is < 0. Multiplying by c_{11}^3, which we know to be positive, and rearranging the resulting homogeneous polynomial in the f_{ij}, gives condition (5).

$(5) \Leftrightarrow (3)$: Under the above symmetry reduction we have

$$m(f) \;=\; (-f_{22})\Big(\frac{1}{f_{11}} + \frac{1}{f_{12}} + \frac{1}{f_{21}} - \frac{1}{f_{22}}\Big) \;=\; 1 - \frac{f_{22}}{f_{11}} - \frac{f_{22}}{f_{12}} - \frac{f_{22}}{f_{21}}. \tag{71}$$

Subtracting 1 from both sides of the inequality $m(f) > 2$, and multiplying by $f_{11}f_{12}f_{21}$, gives (5).

$(4) \Leftrightarrow (5)$: The first factor in $\tilde{m}(f)$ is the polynomial in (43), divided by $p(f)$. So while $p(f) < 0$, the positivity of this factor is equivalent to (4). We complete the proof by showing that under the symmetry reduction (70) the other three factors are always, respectively, positive, negative and positive. Indeed, in the second factor the f_{11} and f_{22}-terms together are positive, and so are the f_{12} and f_{21}-terms. Similarly, in the third factor we group the f_{11}, f_{12} and the f_{21}, f_{22}-terms (both negative), and use the same grouping in the forth factor, giving two positive terms. ∎

It is interesting to see what a purely algebraic approach as in [18, Section 5.3] would say about the situation. First of all, the support function asks us to compute a maximum of a linear functional over a variety. Evaluating just the first order conditions, we get an expression for the maximum for each patch of $\partial \mathcal{Q}$. For the curved $(\mathcal{Q}qx)$ patches this will be just $\tilde{\phi}$. So we get little progress over the simple story told in Sect. 3.5. In many well-known problems of duality, we can simply take the maximum of the different branches of the algebraic function. For example when computing the Legendre transform $(\mathcal{L}F)(p) := \sup_x \{p \cdot x - F(x)\}$ of a non-convex function like $F(x) = x^4 - x^2$ one gets a multi-valued function defined by eliminating x from the cubic $p = dF(x)$. This algebraic version of the Legendre transform is easily corrected by taking the supremum from the convex definition just given as a maximum over the branches. One might therefore guess (and we tried that out in an early stage of this work) that our support function is simply the maximum of the two branches $\tilde{\phi}$ and $\phi_{\mathcal{C}}$. Suffice it to say that this fails, and one easily finds points where $\tilde{\phi}(f) > \phi_{\mathcal{C}}(f) = \phi(f)$. To get this to work, one must ensure that the associated maximizers are contained in the quantum set.

5.5 Quantum representations of extreme points

We now prove Thm. 19. A central role will be played by the uniqueness of a cyclic model. Recall that *every* state of a C*-algebra has a unique cyclic model known as the GNS (Gelfand-Naimark-Segal) representation. What makes uniqueness of a cyclic model non-trivial for correlations $c \in \mathcal{Q}$ is that the algebra itself is not known from expectation values: We can usually not infer the multiplication rules for the A_i, B_j from just these expectations, nor the expectation of, say, $A_1 B_2^2$. If the cyclic model is unique up to unitary isomorphism, as condition (2) of Thm. 19 asserts, then all algebraic relations are fixed.

According to Thm. 19 uniqueness fails for the *classical* extreme points, so these provide a key example. The correlations are $c_{ij} = a_i b_j$ with $a_i, b_j = \pm 1$. These numbers constitute a model with one dimensional Hilbert space, which is obviously cyclic. The models related by $a_i' = -a_i$ and $b_j' = -b_j$ clearly give the same c, but the unitary operator connecting the model Hilbert spaces cannot take a_1 to a_1', so these are not unitarily equivalent. More generally, any classical correlation $c \in \mathcal{C}$ allows a model with $a_1 = +\mathbb{1}$, and another with $a_1 = -\mathbb{1}$. So no classical correlation can have property (2).

Any $c \in \mathcal{Q}$ has *some* cyclic model: By definition of $\mathcal{Q}$, it has a model. The state induced on the algebra $\mathcal{A}$ generated by all A_i, B_j in that model then has a GNS-representation, which is cyclic. Moreover, it has a *finite dimensional* cyclic representation. Indeed, by Carathéodory's Theorem we can represent c as a

46

finite convex combination of extreme points. Since we have provided finite dimensional models for each of these, we can combine them into a single cyclic model by the direct sum construction

$$\mathcal{H} = \bigoplus_k \mathcal{H}_k \text{ with } A_i = \bigoplus_k A_i^{(k)}, \ B_j = \bigoplus_k B_j^{(k)}, \text{ and } \Psi = \bigoplus_k \sqrt{p_k} \Psi^{(k)}, \tag{72}$$

where p_k is the convex weight of the kth contributing extreme point. This could fail to be cyclic, for example, if two of the extreme points used were actually (needlessly) the same. In that case one can take the cyclic subspace generated from Ψ instead. In any case, from Carathéodory's bound we can get by with 5 terms, so the overall dimension can be chosen to be ≤ 20.

The direct sum construction can be reversed: If P_k are orthogonal projections in the Hilbert space of some cyclic model commuting with all A_i, B_j, then setting $\mathcal{H}_k = P_k \mathcal{H}$, $p_k = \langle \Psi | P_k \Psi \rangle$, $\Psi^{(k)} = \sqrt{p_k} P_k \Psi$, and $A_i^{(k)}, B_j^{(k)}$ the restrictions of A_i, B_j to $\mathcal{H}_k$ we have just written the given model in the form (72).

Proof of Thm. 19
(1)$\Rightarrow$(2):
Let c be a non-classical extreme point, and let Ψ be the cyclic vector of some quantum model. By Prop. 12, there is a unique matrix completion C with $-1 < u, v < 1$ and rank 2. The real part of the Gram matrix of the four vectors $\chi_1, \ldots, \chi_4 = A_1\Psi, A_2\Psi, B_1\Psi, B_2\Psi$ is such a completion, so it must equal C. Thus $\Re e\langle A_1\Psi | A_2\Psi \rangle = u$, but it is not immediately obvious that this scalar product has to be real.

Since $\operatorname{rank} C = 2$ we have two linearly independent *real* vectors ξ in the kernel of C. Any such vector satisfies $\sum_{ij} \xi_i \langle \chi_i | \chi_j \rangle \xi_j + \sum_{ij} \xi_i \overline{\langle \chi_i | \chi_j \rangle} \xi_j = 0$. Since both terms are positive, they must vanish separately, and $\sum_j \xi_j \chi_j = 0$. Thus the linear relations between the χ_i are given by real coefficients. Since the 1, 2 and 3, 4 submatrices of C are both nonsingular (as a consequence of $-1 < u, v < 1$), either (χ_1, χ_2) or (χ_3, χ_4) can serve as a basis for the kernel of C, and the two are related by a non-singular real 2×2-matrix γ, so

$$B_j \Psi = \sum_i \gamma_{ji} A_i \Psi. \tag{73}$$

In particular, $c_{ij} = \langle A_i\Psi | B_j\Psi \rangle = \sum_k \langle A_i\Psi | A_k\Psi \rangle \gamma_{jk}$. Since the matrices c and γ are real, so is the scalar $\langle A_1\Psi | A_2\Psi \rangle = u$. Thus, there was no need after all to take the real part in the first paragraph of this proof.

It follows from (73) that non-commutative polynomials in A_1, A_2 acting on Ψ already span the whole space. By cyclicity of Ψ this is true for polynomials involving also the B_j. Now we can successively get rid of the factors B_j in any polynomial acting on Ψ: In any monomial consider the rightmost factor B_j, so we have an expression of the form

$$M B_j M_A \Psi = M\, M_A B_j \Psi = \sum_i \gamma_{ji}\, M\, M_A A_i \Psi, \tag{74}$$

where M is a monomial involving factors A_i, B_k and M_A is a monomial containing only factors A_i. In the evaluation we used that B_j commutes with all A_i, hence with M_A, and (73). By downwards induction on the number of B_j-factors we get that the vectors $M_A \Psi$ span the space. Symmetrically the same is true for polynomials in B. Next suppose that $f(A_1, A_2, \mathbb{1})\Psi = 0$ for some non-commutative polynomial. Then even the operator equation $f(A_1, A_2, \mathbb{1}) = 0$ holds, because we can multiply with any polynomial in B, commute through and use the cyclicity just established.

The first application is to $f = \mathbb{1} - A_1^2$, which is positive, and has zero expectation $\langle \Psi | f\Psi \rangle$ because $C_{11} = 1$. This implies $f\Psi = 0$, and hence $f = 0$. We conclude that $A_1^2 = A_2^2 = B_1^2 = B_2^2 = \mathbb{1}$. Similarly,

$$\begin{aligned}
\Psi &= B_j^2 \Psi = B_j \sum_i \gamma_{ji} A_i \Psi = \sum_i \gamma_{ji} A_i B_j \Psi = \left(\sum_i \gamma_{ji} A_i \right)^2 \Psi \\
&= (\gamma_{j1}^2 + \gamma_{j2}^2)\Psi + \gamma_{j1}\gamma_{j2}(A_1 A_2 + A_2 A_1)\Psi.
\end{aligned} \tag{75}$$

If $\gamma_{j1}\gamma_{j2} \neq 0$ then $(A_1 A_2 + A_2 A_1)\Psi$ is a multiple of Ψ, and so $(A_1 A_2 + A_2 A_1)$ is a multiple of the identity, and from C_{12} this multiple is $2u$. This conclusion does not depend on j, so it is valid whenever $\gamma_{j1}\gamma_{j2} \neq 0$ holds either for $j = 1$ or for $j = 2$. Now if $\gamma_{j1}\gamma_{j2} = 0$, one of the coefficients is zero, and by (73) $B_j\Psi$ is proportional to some $A_i\Psi$. By taking the norm, the factor (the non-zero γ_{ji}) is ± 1 and $c_{ij} = \pm 1$. That

is, the correlation is on an $\mathcal{N}$-facet. But this cannot hold for the other $B_{j'}$ at the same time except for a classical c. Hence in either case

$$(A_1 A_2 + A_2 A_1) = 2u\mathbb{1}. \tag{76}$$

Using this identity and $A_i^2 = \mathbb{1}$, every word in A_1 and A_2 simplifies to a linear combination of $\mathbb{1}, A_1, A_2$, and $A_1 A_2$. Hence the *-algebra $\mathcal{P}_2$ generated by A_1 and A_2 is at most four dimensional. It is non-commutative, because $A_1 A_2 = A_2 A_1$ would imply $4u^2\mathbb{1} = (A_1 A_2 + A_2 A_1)^2 = 4\mathbb{1}$, hence $|u| = 1$. Therefore $\mathcal{P}_2$ is isomorphic to $\mathrm{Mat}_2(\mathbb{C})$, the smallest noncommutative finite dimensional C*-algebra of 2×2-matrices with complex entries.

Next, we claim that the state induced by the vector Ψ on our algebra $\mathcal{P}_2$ has the form

$$M \mapsto \langle\Psi|M\Psi\rangle =: \tau(M) = \tfrac{1}{2}\mathrm{tr}M \tag{77}$$

when M is a polynomial in the A_i. Note that the normalized trace is uniquely characterized among states on the 2×2-matrices by the algebraic "tracial property" $\tau(AB) = \tau(BA)$. Indeed, setting $A = |e_i\rangle\langle e_1|$ and $B = |e_1\rangle\langle e_j|$ in the equation gives $\tau(|e_i\rangle\langle e_j|) = \delta_{ij}/2$. Therefore, we only have to establish the tracial property for the given state. Now, using (73),

$$0 = \langle\Psi|MB_j\Psi\rangle - \langle B_j\Psi|M\Psi\rangle = \sum_i \gamma_{ji}\langle\Psi|(MA_i - A_iM)\Psi\rangle. \tag{78}$$

Since γ is non-singular, we conclude $\langle\Psi|(A_iM - MA_i)\Psi\rangle = 0$. By induction on the degree of an arbitrary other polynomial M' in the A_i, we have the tracial property $\langle\Psi|(M'M - MM')\Psi\rangle = 0$, proving (77). We note that $M'M - MM' = 0$ is false in general for any two polynomials (e.g. (76)), but is true under expectation value as we have shown.

Since $A_j^2 = \mathbb{1}$ and $A_j^* = A_j$, we must either have $A_j = \pm 1$, which would entail classical correlation, or else $\mathrm{tr}A_j = 0$. The trace of (76) gives $\mathrm{tr}A_1 A_2 = u$ and so we have evaluated $\langle\Psi|M\Psi\rangle$ on all polynomials in A_i. By the reduction process used above we can also compute the expectations involving polynomials in both A_i and B_j. Hence by the GNS construction [91] the cyclic model is unique. Moreover, it is equivalent to the model in Sect. 4.1 via a unique unitary isomorphism that maps the linearly independent (since $|u| < 1$) vectors $\Psi, A_1\Psi, A_2\Psi, A_1 A_2\Psi$ to the corresponding vectors of the standard model (then also cyclic). This finishes the proof. We remark that the family of standard models was defined for points other than those in (1) may very well be cyclic but not unique for these points.

(2)⇒(1):
Assume c has a unique cyclic model. Any property that holds in some cyclic model must be true for this unique one. For example, the unique model must be finite dimensional. Similarly, dilation theory tells us that $A_1^2 = \mathbb{1}$. To this end, we first decompose the algebra into irreducible summands. In each summand the algebras generated by A_1, A_2 and B_1, B_2 must themselves be irreducible, so full matrix algebras. Hence the algebras are combined in a tensor product, and are represented on a Hilbert space tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$. We can write $A_1 = V^*\widehat{A}_1 V \otimes \mathbb{1}_B$, where $V : \mathcal{H}_A \to \widehat{\mathcal{H}}_A$ is isometric, and $\widehat{A}_1^2 = \mathbb{1}$. This construction preserves the commutativity of A_i and B_j, and mapping the cyclic vector by $V \otimes \mathbb{1}_B$ to the larger space we get a model with $A_1^2 = \mathbb{1}$. Restricting to the cyclic subspace preserves this property. Hence the unique cyclic model must also satisfy it, and similarly for the other operators.

Now suppose there is a factor $\lambda > 1$ such that $\lambda c \in \mathcal{Q}$. Then using a cyclic model for λc and scaling down the A_i by a factor $1/\lambda$ we get a cyclic model with $A_1^2 \neq \mathbb{1}$. Hence c does not have a unique model. It follows that c must be on the boundary of $\mathcal{Q}$.

Consider now the boundary classification of Prop. 7. The classical types ($\mathcal{Q}$cx) and ($\mathcal{Q}$ce) anyhow fail to have unique models, as mentioned in the second paragraph of Sect. 5.5). So in order to show that c is of type ($\mathcal{Q}$nx) or ($\mathcal{Q}$qx), a non-classical extreme point, we only need to exclude points in an elliptope interior (type ($\mathcal{Q}$ei)). Let us assume without loss that $c_{11} = 1$. Consider the one parameter family of correlations $(1, \lambda c_{12}, c_{21}, \lambda c_{22})$ with λ increasing from 1. This will intersect the elliptope boundary for some $\lambda > 1$. Starting from a model at that point, and scaling $B_2 \mapsto B_2/\lambda$ we can obtain a model with $\|B_2\| < 1$. As argued before, this contradicts the uniqueness of the cyclic model.

(3)⇒(2):
Consider a cyclic model of the type described in (2). In $\rho = |\Psi\rangle\langle\Psi|$ the state vector must be of the form $\Psi = \Psi \otimes \Psi_\nu \oplus 0$. The cyclic subspace contains only vectors of the form $(X\Psi) \otimes \Psi_\nu \oplus 0$, so $\mathcal{H}_0 = \{0\}$ and $\mathcal{H}_\nu = \mathbb{C}\Psi_\nu \cong \mathbb{C}$, and this tensor factor can be omitted.

(2)⇒(3):
Given a model $\mathcal{H}$ for c, let us denote by $\mathcal{A}$ the norm closed algebra generated by the A_i, B_j, by $\mathcal{A}'$ its commutant, i.e., the algebra of operators commuting with every element of $\mathcal{A}$. By $\mathcal{K}_\rho$, we denote the vector space of $\phi \in \mathcal{H}$ such that $|\phi\rangle\langle\phi| \leq \lambda\rho$ for some factor λ. The closure of $\mathcal{K}_\rho$ is called the support of ρ. (In finite dimension, $\mathcal{K}_\rho$ is closed and also equal to the range of ρ, but in infinite dimension $\overline{\mathcal{K}_\rho}$ may be strictly larger than $\mathcal{K}_\rho$.) Then we define $\mathcal{H}_0$ as the subspace orthogonal to all vectors of the form $XY\phi$ with $X \in \mathcal{A}$, $Y \in \mathcal{A}'$, and $\phi \in \mathcal{K}_\rho$. Since this $\mathcal{H}_0$ is an invariant subspace for all $X \in \mathcal{A}$, every $X \in \mathcal{A}$ splits into a direct sum of a component on $\mathcal{H}_0$, about which we can say nothing at all, and a rest, which we will need to characterize. So we may assume $\mathcal{H}_0 = \{0\}$ in the sequel.

For any unit vector of the form $\Psi_1 = Y\phi$ with $Y \in \mathcal{A}'$ and $\phi \in \mathcal{K}_\rho$ consider the cyclic representation subrepresentation of $\mathcal{A}$ on $\mathcal{A}\Psi_1$. Then for positive $X \in \mathcal{A}$ we get

$$
\begin{aligned}
\langle\Psi_1|X\Psi_1\rangle &= \langle\phi|Y^*\sqrt{X}^2 Y\phi\rangle = \langle\phi|\sqrt{X}Y^*Y\sqrt{X}\phi\rangle \\
&\leq \|Y\|^2\langle\phi|\sqrt{X}\,\sqrt{X}\phi\rangle = \|Y\|^2\,\mathrm{tr}(|\phi\rangle\langle\phi|X) \leq \lambda\|Y\|^2\,\mathrm{tr}\rho X.
\end{aligned}
$$

Thus as a functional on $\mathcal{A}$ the state defined by Ψ_1 is dominated by a multiple of ρ, hence is a convex component of ρ. Since we have already established from (2) that c is extremal, Ψ_1 defines again a cyclic model for c, and is hence unitarily isomorphic to the standard model for c. In particular, all algebraic identities of that model hold on $\mathcal{A}Y\phi$, and since such vectors span dense subspace, they hold on all of $\mathcal{H}$.

There is now a polynomial G in the generators A_i, B_j that in the standard model is equal to the one-dimensional projection onto the state vector. When $\hat{X} \in \mathcal{B}(\hat{\mathcal{H}})$ and $X \in \mathcal{A}$ are given by the same polynomial in the generators, we therefore have $GXG = \langle\hat{\Psi}|\hat{X}\hat{\Psi}\rangle G$. Moreover, all vectors $Y\phi$ from the previous paragraph are in $G\mathcal{H}$. We can therefore define $\mathcal{H}_\nu = G\mathcal{H}$, and get a unitary operator $U : \hat{\mathcal{H}}\otimes\mathcal{H}_\nu \to \mathcal{H}$ defined by $U(\hat{X}\hat{\Psi}\otimes\Phi_\nu) = X\Phi_\nu$. Since ρ has support in $G\mathcal{H}$ we have $U^*\rho U = |\hat{\Psi}\rangle\langle\hat{\Psi}|\otimes\rho_\nu$ for some state $\rho_\nu \in \mathcal{B}(\mathcal{H}_\nu)$, as claimed in the standard form (3).

(3)⇒(6):
From the explicit form of the model it is clear that any operator E commuting with $\mathcal{A}$ is of the form $E = \mathbb{1} \otimes E_1 \oplus E_0$. Hence $\mathrm{tr}(\rho E X) = \mathrm{tr}(\rho_\nu E_1)\langle\hat{\Psi}|X\hat{\Psi}\rangle = \mathrm{tr}(\rho E)\,\mathrm{tr}(\rho X)$.

(6)⇒(5):
This is trivial, because the factorization is no longer demanded for all $X \in \mathcal{A}$, but only for those X actually measured in the experiment (including the marginals!).

(5)⇒(4):
Since the marginals are now included, their expectations, which define p must also be those of the unique model, i.e., zero.

(4)⇒(1):
First we eliminate the classical extreme points as they do not have unique extensions p, as explained in the beginning of this Section. If c is not extremal, i.e., on an edge, in an elliptope interior or the interior of $\mathcal{Q}$, then $c = \lambda c' + (1-\lambda)c''$ for some $\lambda > 0$ and c' classical. So we get distinct extensions by fixing the extension of c'' but changing that of c'. ∎

5.6 Dependence on Hilbert space dimension

We now return to Sect. 4.5, and we prove the remaining statement on the Hilbert space dimension. We remark that $\mathcal{Q}_m = \mathcal{Q}$ for $m \geq 4$ is already proved in Tsirelson's original paper [7]. Here we provide a different geometric proof.

Proof of Prop. 20
(1) Let $c \in \mathcal{Q}_m$ be a quantum correlation in an m-dimensional Hilbert space. Then the algebra $\mathcal{A}$ generated by A_i, B_j can be decomposed into irreducible components, represented on orthogonal subspaces $\mathcal{H}_\alpha$. c is then a convex combination of correlations realized in $\mathcal{H}_\alpha$ with weights equal to the expectation of the projection onto this subspace. When $m \leq 3$, we also have $\dim\mathcal{H}_\alpha \leq 3$, so it suffices to consider the case of a single summand, i.e., $\mathcal{A}$ acting irreducibly.

Consider now the subalgebra $\mathcal{A}_A$ generated only by the A_i. An element in the center of $\mathcal{A}_A$, i.e., one that commutes with A_1 and A_2, also commutes with the B_j, and is therefore in the center of $\mathcal{A}$. By

irreducibility it has to be a multiple of $\mathbb{1}$. Therefore, $\mathcal{A}_A$ is a finite dimensional C*-algebra with trivial center, and has to be isomorphic to a full matrix algebra, say the $n \times n$ matrices. Similarly, we get a matrix dimension n' for the algebra generated by the B_j. Since the two sets of operators commute, and even generate commutants of each other, $\dim \mathcal{H}_\alpha = nn'$. Hence, by assumption, $nn' \leq m \leq 3$, so either $n = 1$ or $n' = 1$.

Taking the first case without loss, $A_i = a_i\mathbb{1}$ and the contribution from this summand is $c_{ij} = \mathrm{tr}_\alpha(\rho A_i B_j) = a_i\mathrm{tr}_\alpha(\rho B_j)$, which is a product, hence classical.

We note that this argument also applies in any quantum model with $[A_1, A_2] = 0$ ([65]), and hence if $A_i = a_i\mathbb{1}$ for some i: Then every irreducible component gives a product correlation, and the resulting convex combination is still classical.

(2) By monotonicity, we only need to show that $\mathcal{Q} \subset \mathcal{Q}_4$. We already know that many boundary points are in $\mathcal{Q}_4$, since we built explicit 4-dimensional models in Sect. 4.1. In particular, $[\mathcal{Q}\mathrm{qx}] \subset \mathcal{Q}_4$. Here $[\mathcal{Q}\mathrm{qx}]$ is the closure of the exposed extreme points ($\mathcal{Q}\mathrm{qx}$), and by the discussion after Prop. 7 covers all boundary elements except the elliptope interiors.

Some points in the interior of $\mathcal{Q}$ can now be obtained by simple scaling: When A_i, B_j, ρ is a model for c, and $0 \leq \lambda \leq 1$, then $A_i' = \lambda A_i$, $B_j' = B_j$, $\rho' = \rho$ is a model for λc with the same dimension. Turning this around, we can consider, for any $c \in \mathcal{Q}$ with $c \neq 0$, the unique point $\bar{c} = tc$, which is the intersection of the ray $\{tc|t \geq 0\}$ with $\partial\mathcal{Q}$ (possible because $\mathcal{Q}$ is a compact convex set with origin in the interior). Then if $\bar{c} \in [\mathcal{Q}\mathrm{qx}]$, we have $c \in \mathcal{Q}_4$.

This leaves points, for which $\bar{c}$ is in an elliptope interior. By the argument just used, we only need to show that elliptope interiors themselves are in $\mathcal{Q}_4$, and by symmetry we may choose the elliptope in the $\mathcal{N}$-facet $c_{11} = 1$. To this end, we consider a modified rescaling, namely $A_1' = A_1$, $B_1' = B_1$, $A_2' = \lambda A_2$, and $B_2' = \lambda B_2$, and $\rho' = \rho$. This also leaves the dimension unchanged, and realizes the correlation $c'(\lambda) = (1, \lambda c_{12}, \lambda c_{21}, \lambda^2 c_{22})$. Clearly, with $\lambda = 0$ we get the center of the elliptope. For all other points c we find a suitable boundary point by inverse scaling: For $\lambda > 1$ the curve $c'(\lambda)$ is unbounded, and so eventually crosses the elliptope boundary. So we can use the model for that boundary point and scale with $1/\lambda$. ∎

5.7 Fixed state

Proof of Prop. 21

Suppose one of the A_i, B_j has a proper convex decomposition into extreme points of the allowed set, where "proper" means that several distinct points each appear with positive weight. This would make any correlation c obtained with these operators a convex combination of others. Suppose this c is an extreme point of $\mathrm{co}\,\mathcal{Q}(\rho)$. Then the convex combination of correlations cannot be proper, i.e., all the correlations appearing with a positive weight must be equal. So either all A_i, B_j are extremal in the first place, or the extreme points in their convex decomposition also represent c. In either case, the extreme points of $\mathrm{co}\,\mathcal{Q}(\rho)$ can be realized by operators such that each A_i and B_j is extremal. This means that $A_i^2 = B_j^2 = \mathbb{1}$, because if A with $-\mathbb{1} \leq A \leq \mathbb{1}$ has any eigenvalues *other than* ± 1, it can be convexly decomposed in this set into two operators with the same eigenvectors, but with eigenvalues ± 1.

In two dimensions there are just two eigenvalues ± 1 which are either the same or distinct. This gives the union structure in the statement of the proposition to be proved. When they are the same, we have $A_i = \pm \mathbb{1}$. Then by part (1) of the proof in Sect. 5.6 the resulting correlation is classical. Moreover, all extremal classical correlations can be generated with $A_i, B_j = \pm\mathbb{1}$. When none of A_i, B_j are $\pm\mathbb{1}$, we obtain correlations that belong to a set denoted $\mathcal{Q}_{\mathrm{st}}$. By definition, $\mathcal{Q}_{\mathrm{st}}$ is the set of all correlations obtained with *extremal* A_i, B_j, none of which is $\pm\mathbb{1}$. In total, $\mathrm{co}\,\mathcal{Q}(\rho)$ is the convex hull of $\mathcal{C}$ joined with $\mathcal{Q}_{\mathrm{st}}$. It is worth noting, however, that extreme points of $\mathrm{co}\,\mathcal{Q}_{\mathrm{st}}$ might not be extremal in $\mathrm{co}\,\mathcal{Q}(\rho)$, because for some ρ, e.g., ρ close to the maximally mixed state, this set may be small, and even $\mathcal{Q}_{\mathrm{st}} \subset \mathcal{C}$. In this case $\mathcal{Q}(\rho) \subset \mathcal{C}$, and the given state can only ever produce classical correlations (see below).

Our next step is to determine $\mathcal{Q}_{\mathrm{st}}$. Hermitian 2×2-matrices A with eigenvalues ± 1 can be expanded in Pauli matrices $\sigma_1, \sigma_2, \sigma_3$ as $A = \sum_{k=1}^3 a_k\sigma_k =: \vec{a} \cdot \vec{\sigma}$, where $\vec{a} \in \mathbb{R}^3$ is a Euclidean unit vector. That is, we have now to choose 4 unit vectors $\vec{a}_1, \vec{a}_2, \vec{b}_1, \vec{b}_2$. This parametrization gives

$$c_{ij} = \mathrm{tr}\rho A_i \otimes B_j = \vec{a}_i \cdot R\vec{b}_j, \tag{79}$$

where R is the matrix of Pauli expectations given in the proposition. Suppose now that R is replaced by URV with orthogonal matrices $U, V \in \text{Mat}_3(\mathbb{R})$. This corresponds to a change of the state (by a local unitaries), but since we can use U and V to change the vectors $\vec{a}_i, \vec{b}_j$, the *set* of correlations remains the same. Now the singular value decomposition allows us to choose URV diagonal, where, by definition the diagonal elements of this matrix are the singular values $\lambda_1, \lambda_2, \lambda_3$ of the original R. The set of the resulting correlations is now $\mathcal{Q}_{\text{st}} = \mathcal{Q}_{\text{st}}(\lambda_1, \lambda_2, \lambda_3) = \{c \in \mathbb{R}^4 | c_{ij} = \vec{a}_i \cdot \text{Diag}(\lambda_1, \lambda_2, \lambda_3)\vec{b}_j, \text{ unit vectors } \vec{a}_i, \vec{b}_j \in \mathbb{R}^3\}$ with $D := \text{Diag}(\lambda_1, \lambda_2, \lambda_3)$ the diagonal matrix with these elements along the diagonal.

Moreover, the choice $\vec{a}_i, \vec{b}_j \in \mathbb{R}^3$ can be decomposed into first choosing two-dimensional subspaces W_A, W_B and then choosing $\vec{a}_i \in W_A, \vec{b}_j \in W_B$, resulting in $\mathcal{Q}_{\text{st}}$ the union of sets of correlations with fixed W_A, W_B. What does each of these set look like? It clearly has the same form as above but with D projected to two-dimensions via orthogonal projections P_A onto W_A and P_B onto W_B, that is

$$\mathcal{Q}_{\text{st}}(W_A, W_B) = \{c \in \mathbb{R}^4 | c_{ij} = \vec{a}_i \cdot P_A D P_B \vec{b}_j, \text{ unit vectors } \vec{a}_i, \vec{b}_j \in \mathbb{R}^2\}. \tag{80}$$

Then everything said in the previous paragraph applies with the only change that the 3×3-matrix R is replaced by a 2×2-matrix $P_A D P_B$, so there are only two singular values denoted λ_1, λ_2 (abuse of notation, these are generally distinct from the original singular values of R in three-dimension). Denote the resulting set of correlations by $\mathcal{Q}_{\text{st}}(\lambda_1, \lambda_2)$. Since unit vectors in two dimensions are of the form $\vec{a}_i = (\cos(\alpha_i), \sin(\alpha_i))$, and R is now the diagonal matrix with entries (λ_1, λ_2), this set is exactly the one described in the proposition.

It remains to compute the convex hull. Observe that there is a monotonicity relation when taking convex hull: if $\lambda_1 \leq \mu_1$ and $\lambda_2 \leq \mu_2$ then $\text{co}\, \mathcal{Q}_{\text{st}}(\lambda_1, \lambda_2) \subset \text{co}\, \mathcal{Q}_{\text{st}}(\mu_1, \mu_2)$. Indeed, it suffices to consider the case $\lambda_1 \leq \mu_1$. Starting from any model $c_{ij} = \mu_1 \cos(\alpha_i) \cos(\beta_j) + \mu_2 \sin(\alpha_i) \sin(\beta_j)$ with the larger μ_1, we take the convex combination

$$p\left(\mu_1 \cos(\alpha_i) \cos(\beta_j) + \mu_2 \sin(\alpha_i) \sin(\beta_j)\right) + (1 - p)\left(\mu_1 \cos(\pi - \alpha_i) \cos(\beta_j) + \mu_2 \sin(\pi - \alpha_i) \sin(\beta_j)\right)$$

to get $c'_{ij} = \mu_1(p - (1-p)) \cos(\alpha_i) \cos(\beta_j) + \mu_2 \sin(\alpha_i) \sin(\beta_j)$. That is, precisely to the corresponding correlation with $\mu'_1 = (2p - 1)\mu_1$, which can thus be made equal to any $\lambda_1 \leq \mu_1$.

Therefore, in the union over all W_A, W_B we can ignore all subspace pairs for which the singular values λ'_1, λ'_2 of the projected $P_A D P_B$-matrix are dominated by those of another one. We claim there is one pair of subspaces with largest pair of projected singular values: $W_A = W_B$ is a/the eigenspace (nonunique if D is degenerate) of the top two eigenvalues λ_1, λ_2 of D or equivalently of R. This follows by the observation that the squares of the non-zero singular values of any matrix M are the non-zero eigenvalues of M^*M. When $M = P_A D P_B$, the squares of its two singular values are the eigenvalues of $P_B D^* P_A D P_B$. Now $D^* P_A D$ is positive semidefinite rank 2 matrix, so we can apply the Rayleigh-Ritz variational principle [92, Theorem XIII.3]: The eigenvalues of $P_B D^* P_A D P_B$ are largest, when P_B is just the projection onto the eigenspace associated with the two largest eigenvalues of $D^* P_A D$, or equivalently of $P_A D D^* P_A$ (since the eigenvalues of X^*X and XX^* are the same). The same Rayleigh-Ritz argument can be applied again to maximize the two eigenvalue by picking P_A as the projection to the eigenspace of two largest eigenvalues of DD^*. To summarize, when we take the $\lambda_1 \geq \lambda_2 \geq \lambda_3$ to be the singular values of R, we have

$$\text{co}\, \mathcal{Q}_{\text{st}}(\lambda_1, \lambda_2, \lambda_3) = \text{co}\, \mathcal{Q}_{\text{st}}(\lambda_1, \lambda_2). \tag{81}$$

This concludes the proof of the main statement of Prop. 21.

Finally, we have to check when $\mathcal{Q}(\rho)$ becomes classical. This happens iff all CHSH inequalities are satisfied, also in $\mathcal{Q}_{\text{st}}(\lambda_1, \lambda_2)$. By symmetry and from (5) we have

$$\text{CHSH}(c) = \frac{1}{2}\left(\vec{a}_1 \cdot R(\vec{b}_1 + \vec{b}_2) + \vec{a}_2 \cdot R(\vec{b}_1 - \vec{b}_2)\right), \tag{82}$$

which is clearly maximized with respect to the unit vectors $\vec{a}_i$ as $\frac{1}{2}\left(\|R(\vec{b}_1 + \vec{b}_2)\| + \|R(\vec{b}_1 - \vec{b}_2)\|\right)$. Since the $\vec{b}_1 \pm \vec{b}_2$ are orthogonal vectors, we can write $\vec{b}_1 \pm \vec{b}_2 = \lambda_\pm \vec{e}_\pm$, where $\vec{e}_+$ and $\vec{e}_-$ are orthogonal unit vectors and $\lambda_+^2 + \lambda_-^2 = \|\vec{b}_1 + \vec{b}_2\|^2 + \|\vec{b}_1 - \vec{b}_2\|^2 = 4$. Thus by Cauchy-Schwarz inequality

$$\max \text{CHSH}(c) = \frac{1}{2}\left(\lambda_+\|R\vec{e}_+\| + \lambda_-\|R\vec{e}_-\|\right) \leq \left(\|R\vec{e}_+\|^2 + \|R\vec{e}_-\|^2\right)^{\frac{1}{2}}. \tag{83}$$

The choice of orthogonal unit vectors $\vec{e}_\pm$ maximizing this expression is the eigenvectors of R^*R for its to largest eigenvectors, which are λ_1^2 and λ_2^2. ∎

5.8 Fixed observables

Proof of Prop. 22

By Jordan's Lemma [30] or C*-algebra of two projections [93], any choice of operators A_1, A_2 and B_1, B_2 is a representation this algebra and so it decomposes into irreducibles. We first show that $\mathcal{Q}(A_i, B_j) = \mathrm{co}\{\mathcal{Q}_{\mathrm{obs}}(u,v) \mid u \in \Sigma_A, v \in \Sigma_B\}$ for some correlation sets $\mathcal{Q}_{\mathrm{obs}}(u,v)$ to be defined later. Indeed, let Π_i denote the central projection onto the ith irreducible summand, then restricted to this summand the operator $A_1 A_2 + A_2 A_1 = 2u\mathbb{1}$ for some $u \in \Sigma_A$ because it commutes with all generators. This can be used to drastically simplify polynomials in A_1, A_2, so that they generate the algebra of 2×2-matrices, except at the endpoints $u = \pm 1$, where they form a commutative subalgebra. That is, up to isomorphism we can take $A_1 = \sigma_1$, and $A_2 = \cos\alpha\,\sigma_1 + \sin\alpha\,\sigma_3$, so that $u = \cos\alpha$. The same holds for Bob with central parameter v, and the operators are combined as $A_i \otimes B_j$. Whenever $\lambda_i = \mathrm{tr}(\rho\Pi_i) \neq 0$, we can define the state $\rho_i = \lambda_i^{-1}\Pi_i\rho\Pi_i$, and the corresponding correlation $c^i \in \mathcal{Q}_{\mathrm{obs}}(u,v)$, the affine image of the state space of $\mathbb{C}^2 \otimes \mathbb{C}^2$ under $\rho \mapsto \mathrm{tr}(\rho A_i(u) \otimes B_j(v))$. Thus, $c \in \mathcal{Q}(A_i, B_j)$ implies that it is a convex hull of points in $\mathcal{Q}_{\mathrm{obs}}(u,v)$. The converse is also true.

The sets $\mathcal{Q}_{\mathrm{obs}}(u,v)$ are affinely isomorphic to each other except when $u,v = \pm 1$. To see this, observe that $A_i(u) = \sum_{i'} S(u)_{ii'} A_{i'}(0)$, likewise for $B_j(v)$, and consequently $c(u,v) = S(u)c(0,0)S(v)^\top$ where both $c(u,v) \in \mathbb{R}^4$ and $c(0,0) \in \mathbb{R}^4$ are formed with the same density operator ρ, namely $c_{ij}(u,v) = \mathrm{tr}\rho A_i(u) \otimes B_j(v)$. This gives $\mathcal{Q}_{\mathrm{obs}}(u,v) = S(u)\mathcal{Q}_{\mathrm{obs}}(0,0)S(v)^\top$, which is sufficient for the purpose of this Proposition. Note, in addition, that $\mathcal{Q}_{\mathrm{obs}}(u,v)$ are all non-isometrically isomorphic to $\mathcal{Q}_{\mathrm{obs}}(0,0)$ since $S(u)$ are invertible whenever $-1 < u < 1$.

It remains to show that $\partial_e \mathcal{Q}_{\mathrm{obs}}(0,0) = \mathsf{O}(2)$. Since all $A_i(0) \otimes B_j(0)$ commute with $U = \sigma_2 \otimes \sigma_2$, we can assume without loss that ρ commutes with U. Moreover, extreme points must come from pure states $\rho = |\psi\rangle\langle\psi|$, which by the argument in Sect. 5.1.1 we can choose as given by a real vector ψ. Together these imply $\psi_+ = (\cos t, \sin t, \sin t, -\cos t)/\sqrt{2}$ or $\psi_- = (\cos t, \sin t, -\sin t, \cos t)/\sqrt{2}$, which gives two families of extreme points

$$\begin{pmatrix} -\cos 2t & \sin 2t \\ \sin 2t & \cos 2t \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} \cos 2t & -\sin 2t \\ \sin 2t & \cos 2t \end{pmatrix}, \tag{84}$$

belonging to two orthogonal subspaces of $\mathbb{R}^4$. These are exactly all the 2×2 orthogonal matrices: the reflections and rotations. ∎

Proof of Prop. 23

The general element of $\mathcal{Q}_{\mathrm{obs}}(0,0)$ can be written as

$$c = \lambda \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} + \mu \begin{pmatrix} \cos\beta & \sin\beta \\ \sin\beta & -\cos\beta \end{pmatrix}, \tag{85}$$

where $\lambda, \mu \geq 0$, and $\lambda + \mu < 1$. The two extremal circles are, by definition, the points with $\{\lambda, \mu\} = \{0, 1\}$. This covers convex combinations form different circles, when $\lambda + \mu = 1$. If some contributions to a convex combination come from the same circle, this just reduces the corresponding coefficient. From this description it is clear that all points with $\lambda + \mu < 1$ belong to the interior of the body. The respective planes are given by $c_{11} - c_{22} = c_{12} + c_{21} = 0$, and $c_{11} + c_{22} = c_{12} - c_{21} = 0$, respectively. They are clearly Euclidean orthogonal. The body is symmetric under rotations in any of these planes, so all connecting edges are symmetry equivalent, and one can also check directly that they are all exposed. Note that the image of a cylinder that three-dimensional geometric intuition maybe suggests as the convex hull of two circles is entirely misleading here: The interiors of the circles are not faces but in the interior of the body.

To get the semialgebraic description, note that, with $s = \sum_{ij} c_{ij}^2$,

$$\begin{aligned} 4\lambda^2 &= (c_{11} + c_{22})^2 + (c_{12} - c_{21})^2 = s + 2\det c \\ 4\mu^2 &= (c_{11} - c_{22})^2 + (c_{12} + c_{21})^2 = s - 2\det c. \end{aligned} \tag{86}$$

So in order to get a polynomial condition for the c_{ij} we need to express the necessary and sufficient condition $\lambda + \mu \leq 1$ in terms of λ^2 and μ^2. By successive squaring we get first $2\lambda\mu \leq (1 - \lambda^2 - \mu^2)$, and then $0 \leq (1 - 2\lambda^2 - 2\mu^2 + (\lambda^2 - \mu^2)^2)$. Using $s = 2(\lambda^2 + \mu^2)$ and $\det c = (\lambda^2 - \mu^2)$ gives the
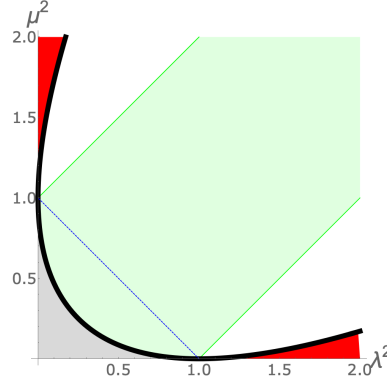
Figure 22: The condition $\lambda + \mu \leq 1$ is expressed in terms of λ^2 and μ^2 as the gray shaded region near the origin. The bounding parabola extends further, so the inequality which it expresses needs to be supplemented by further conditions to exclude the red shaded areas. We choose the intersection with the green strip, which amounts to a condition on $\det c$. But other choices, e.g., the triangle bounded by the dashed blue line would also work. The latter would express that $\mathcal{Q}_{\mathrm{obs}}(0,0)$ is contained in a ball of radius $\sqrt{2}$.

inequality for ℓ given in the proposition. On the boundary $\lambda + \mu = 1$ these inequalities are equalities. So this polynomial is clearly the algebraic description of the boundary. However, the second squaring step is not reversible, so we get some unwanted elements in the Zariski closure. As for $\mathcal{Q}$, where we had to augment the boundary polynomial h by an additional (non-unique) polynomial inequality $g \geq 0$, there are different ways of achieving this. Fig. 22 is the map for this purpose. We see that we can either supplement the polynomial inequality $\lambda^2 + \mu^2 \leq 1$, meaning $s \leq 2$, or by the determinant inequality given in the proposition. $\blacksquare$

Proof of Prop. 24

We have shown in Prop. 24 that on $\mathcal{Q}_{\mathrm{obs}}(0,0)$ the determinant inequality holds, and by Prop. 22 and the observation that $\det S(u) \leq 1$, the same holds for all components $\mathcal{Q}(A_i, B_j)$ with different singleton spectra Σ_A, Σ_B. This would finish the argument if $\det$ were a convex function. However, it clearly is not.

We therefore take a more global approach using the detailed knowledge compiled in the paper. First of all, it suffices to show the determinant inequality on the boundary $\partial \mathcal{Q}$, because the determinant is homogenous and every point $c \in \mathcal{Q}$ can be written as $c = \lambda c'$ with $\lambda \leq 1$ and $c' \in \partial \mathcal{Q}$. This shows that also the cases of equality can only lie on the boundary. For the curved tetrahedra we can use the cosine parametrization Prop. 8. The determinant is easily evaluated and simplifies to

$$\det c = -\sin(\alpha + \beta)\sin(\alpha + \gamma) \in [-1, 1]. \tag{87}$$

On an $\mathcal{N}$-facet, say $\{c_{11} = 1\}$, the determinant is an affine function of c_{22}. Hence its maximum will be attained on the bounding elliptope, where the previous argument applies.

For the case of equality it suffices to find points in the parametrized surface with $\det c = -1$, since the sign can be reversed by a symmetry transformation. From (87) we find, up to an overall sign for all angles and modulo 2π that $\alpha + \beta = \pi/2 = \alpha + \gamma$. So we get $\beta = \gamma$, making c Alice-Bob symmetric. Moreover, the fourth angle is $\delta = -(\alpha + \beta + \gamma) = -\alpha - 2(\pi/2 - \alpha) = \alpha - \pi$, so that $c_{22} = -c_{11}$. This singles out the circle of reflection matrices, shown in red in Fig. 19. $\blacksquare$

6 Outlook

6.1 What more of $\mathcal{Q}$?

There are some geometric aspects of $\mathcal{Q}$ we did not discuss, although they might be natural and interesting.

- *Robustness of self-testing*
  In the practice of quantum key distribution, the correlation c is determined by statistical evaluation.

The assumption that c is an extremal point is never exactly verifiable. Therefore, one needs explicit bounds of the sort: When c is known up to accuracy ε (confidence intervals), then the eavesdropper cannot know more than δ about the bits used for key generation. Various definitions of "accuracy" and "know more" can be given. In any case, the concrete bound δ as a function of ε will depend also on the local geometry of $\mathcal{Q}$, particularly the curvature. Giving more details here would have turned this into a paper on key distribution. Generally speaking, self-testing is a robust phenomenon: Near-extremal correlations allow the conclusion that the observables involved can be deformed (norm-)slightly so that they turn into the minimal two-qubit example [81].

- *Integral curvatures*
  As mentioned in Sect. 3.4, the Steiner volume polynomial contains information about curvature integrals of the boundary. In Sect. 2.9 we merely determined the volume, but no further coefficients.

- *Weakly self-dual geometry*
  The Hadamard matrix defines an indefinite pseudo-Euclidean metric on $\mathbb{R}^4$, for which $\mathcal{Q}$ is self-dual. Some natural questions come with this structure, but it is unclear whether it sheds any light on $\mathcal{Q}$.

- *Constrained Hilbert space dimension*
  The basics were discussed in Sect. 4.5, but a full characterization is still lacking.

6.2 How does this generalize?

Many of the techniques described above were originally drafted to address more general situations. Let us briefly indicate their natural levels of generality.

- *The full 222 case, and the C*-algebra generated by two projections*
  In the minimal 222 case, without the zero marginals condition, the quantum body $\mathcal{Q}$ is a convex body in $\mathbb{R}^8$. The semidefinite matrix completion point of view is not directly effective for breaking this down to a finite dimensional problem. As has been noted also by Masanes [30] (actually more generally for the N22 case) this can be achieved by the representation theory of the universal C*-algebra generated by two projections [93]. This provides a description of the extreme points parametrized by the product of spheres $\mathbb{S}^1 \times \mathbb{S}^1 \times \mathbb{S}^3$, analogous to Prop. 8. A `Macaulay2` computation reveals that this variety has degree 40 and its prime ideal is generated by 28 polynomials whose degrees are $5, 6, 7$ and 8. This may be a starting point for the analysis of the 222 case.

- *Higher universal correlation bodies*
  It is clear that the analog of $\mathcal{Q}$ can be defined for larger N, M, or K, or any specification of parties settings and outcomes. However, the construction is notoriously non-constructive; see [94].

- *Semidefinite hierarchies*
  We used this extensively, and got a complete characterization of the minimal $\mathcal{Q}$ out of it, just using the bottom level (as explained in Sect. 2.8) of the hierarchy. In fact, this characterizes the minimal case within the full 222 scenario with marginals: If the bottom-level semidefinite relaxation of the full 222 case is tight, i.e., $c \in (\mathcal{Q}\text{qx})$, self-testing Thm. 19 (2) implies zero marginals, so we must be in the 222|0 case. For larger N, M, or K, a gap can be expected to exist and become rapidly larger. Hierarchies are still the key tool for getting upper bounds, but tightness is too much to ask. It should also be noted that in spite of the proven convergence of the hierarchy it is computationally unfeasible to really push this to high levels. It is unclear (to us) for which other cases a tight bound at some higher but finite hierarchy level holds.

- *Parametrized extreme points*
  Although this is perhaps best understood via the two-projections theory, another parametrization of the extreme points (not explicitly using this theory) in the N22 case was given in [8].

- *Duality*
  The duality in Thm. 3 clearly depends on minimality: The duality of $\mathcal{N}$ and $\mathcal{C}$ requires at least the dimensions of these sets to coincide, which fails for $MK > 4$.

- *Correlation matrices and Clifford algebras*
  All the above extensions drop the 0-marginal condition or increase N. We stress that Tsirelson's technique of correlation matrices is an extension in another direction, i.e., to 2M2|0, with general M.

- *Algebra*
  Algebraic methods are expected to apply once a reduction to finite dimension has been achieved by other means. We found them directly useful in the full 222 case (work in progress), but there are clearly also applications to N22 and 2M2 cases. However, the complexity of algebraic characterizations can be expected to increase very rapidly. Even worse are the case distinctions and inequalities of a *semi*-algebraic description. We can understand this from the classical case, the characterization of $\mathcal{C}$. Here the algebra is linear, but the inequality part, i.e., the determination of all Bell inequalities, is a family of convex hull problems, which is known to grow badly [95]. So no general results can be expected, but as in the classical case [6, Problem 1] one can look for trails into the wilderness, e.g., infinite families of models defined by special properties or symmetries.

- *Algebraic statistics*
  Consider the ± 1-valued random variables A_1, A_2, B_1, B_2 satisfying (1). Their statistical model is the graphical model whose graph G is the 4-cycle with edges $A_1 - B_1$, $B_1 - A_2$, $A_2 - B_2$, $B_2 - A_1$. This is [96, Example 4] up to relabelling. The sufficient statistics of this model are obtained by applying the linear map $A(G)$ in [96, Example 4]. The image of this map is our classical polytope $\mathcal{C}$. In particular this map is a bijection between the model and $\mathcal{C}$ and inverting it is called *maximum likelihood estimation* (MLE). We can recover also $\mathcal{N}$ from this construction, and more in general such polytopes can be defined for any toric model. For an undirected graphical model G we have that $\mathcal{C} = \mathcal{N}$ if and only if the graph is decomposable; the four-cycle model is the smallest non-decomposable model so we can deduce also from this argument that the inclusion is strict. It would be particularly interesting to examine the general 222 case through the lens of algebraic statistics.

Acknowledgements

References

[1] Alain Aspect, Philippe Grangier, and Gérard Roger. "Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities". Phys. Rev. Lett. **49**, 91–94 (1982).

[2] B. Hensen, R. Hanson, et al. "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". Nature **526**, 682 EP – (2015). arXiv:1508.05949.

[3] N. Sangouard, J.-D. Bancal, N. Gisin, W. Rosenfeld, P. Sekatski, M. Weber, and H. Weinfurter. "Loophole-free Bell test with one atom and less than one photon on average". Phys. Rev. A **84**, 052122 (2011). arXiv:1108.1027.

[4] J. S. Bell. "On the Einstein Podolsky Rosen paradox". Physics **1**, 195–200 (1964).

[5] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. "Proposed experiment to test local hidden-variable theories". Phys. Rev. Lett. **23**, 880–884 (1969).

[6] R. F. Werner et al. "Open quantum problems". url: `https://oqp.iqoqi.oeaw.ac.at/`.

[7] Boris S. Tsirelson. "Quantum analogues of the Bell inequalities. the case of two spatially separated domains". J. Soviet Math. **36**, 557–570 (1987).

[8] R. F. Werner and M. M. Wolf. "All multipartite Bell-correlation inequalities for two dichotomic observables per site". Phys. Rev. A **64**, 032112 (2001). arXiv:quant-ph/0102024.

[9] William Slofstra. "The set of quantum correlations is not closed". Forum of Mathematics, Pi **7**, e1 (2019). arXiv:1703.08618.

[10] Volkher B. Scholz and R. F. Werner. "Tsirelson's problem" (2008). arXiv:0812.4305.

[11] Boris S Tsirelson. "Some results and problems on quantum Bell-type inequalities". Hadronic Journal Supplement **8**, 329–345 (1993). url: `https://www.tau.ac.il/~tsirel/download/hadron.html`.

[12] Miguel Navascues, Stefano Pironio, and Antonio Acín. "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations". New J. Phys. **10**, 073013 (2008). arXiv:0803.4290.

[13] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner. "Connes' embedding problem and Tsirelson's problem". J. Math. Phys. **52**, 012102 (2011). arXiv:1008.1142.

[14] Tobias Fritz. "Tsirelson's problem and Kirchberg's conjecture". Rev. Math. Phys. **24**, 1250012 (2012). arXiv:1008.1168.

[15] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. "MIP*=RE" (2020). arXiv:2001.04383.

[16] Günther M. Ziegler. "Lectures on polytopes". Springer. Berlin (1995).

[17] Mateusz Michałek and Bernd Sturmfels. "Invitation to nonlinear algebra". Volume 211 of Graduate Studies in Mathematics. AMS. (2021).

[18] Grigoriy Blekherman, Pablo Parrilo, and Rekha Thomas. "Semidefinite optimization and convex algebraic geometry". MOS-SIAM Series on Optimization 13. SIAM. Philadelphia (2012).

[19] Bernd Sturmfels and Caroline Uhler. "Multivariate Gaussians, semidefinite matrix completion, and convex algebraic geometry". Ann. Inst. Statist. Math. **62**, 603–638 (2010). arXiv:0906.3529.

[20] Claus Scheiderer. "Spectrahedral shadows". SIAM J. Appl. Algebra Geometry **2**, 26–44 (2018). arXiv:1612.07048.

[21] B. S. Cirel'son. "Quantum generalizations of Bell's inequality". Lett. Math. Phys. **4**, 93–100 (1980).

[22] Jukka Kiukas and Reinhard F. Werner. "Maximal violation of Bell inequalities by position measurements". J. Math. Phys. **51**, 072105 (2010). arXiv:0912.3740.

[23] Lawrence J. Landau. "Empirical two-point correlation functions". Found. Phys. **18**, 449–460 (1988).

[24] L Masanes. "Necessary and sufficient condition for quantum-generated correlations" (2003) arXiv:quant-ph/0309137.

[25] Yukun Wang, Xingyao Wu, and Valerio Scarani. "All the self-testings of the singlet for two binary measurements". New J. Phys. **18**, 025021 (2016). arXiv:1511.04886.

[26] Andrew C Doherty, Yeong-Cherng Liang, Ben Toner, and Stephanie Wehner. "The quantum moment problem and bounds on entangled multi-prover games". In 23rd Annual IEEE Conference on Computational Complexity. Pages 199–210. IEEE (2008). arXiv:0803.4373.

[27] Tobias Fritz. "Polyhedral duality in Bell scenarios with two binary observables". J. Math. Phys. **53**, 072202 (2012). arXiv:1202.0141.

[28] Dominic Mayers and Andrew Yao. "Self testing quantum apparatus". Quantum Info. Comput. **4**, 273–286 (2004). arXiv:quant-ph/0307205.

[29] Stephen J. Summers and Reinhard F. Werner. "Maximal violation of Bell's inequalities is generic in quantum field theory". Commun. Math. Phys. **110**, 247–259 (1987).

[30] L Masanes. "Extremal quantum correlations for n parties with two dichotomic observables per site" (2005) arXiv:quant-ph/0512100.

[31] Le Phuc Thinh, Antonios Varvitsiotis, and Yu Cai. "Geometric structure of quantum correlators via semidefinite programming". Phys. Rev. A **99**, 052108 (2019). arXiv:1809.10886.

[32] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. "Bell nonlocality". Rev. Mod. Phys. **86**, 419–478 (2014). arXiv:1303.2849.

[33] Koon Tong Goh, Jędrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani. "Geometry of the set of quantum correlations". Phys. Rev. A **97**, 022104 (2018). arXiv:1710.05892.

[34] Ivan Šupić and Joseph Bowles. "Self-testing of quantum systems: a review". Quantum **4**, 337 (2020). arXiv:1904.10042.

[35] Rene Schwonnek, Koon Tong Goh, Ignatius W. Primaatmaja, Ernest Y. Z. Tan, Ramona Wolf, Valerio Scarani, and Charles C. W. Lim. "Device-independent quantum key distribution with random key basis". Nat. Commun. **12**, 2880 (2020). arXiv:2005.02691.

[36] Ernest Y. Z. Tan, René Schwonnek, Koon Tong Goh, Ignatius William Primaatmaja, and Charles C. W. Lim. "Computing secure key rates for quantum key distribution with untrusted devices". npj Quantum Inf. **7**, 158 (2021). arXiv:1908.11372.

[37] K. G. H. Vollbrecht and R. F. Werner. "Entanglement measures under symmetry". Phys. Rev. A **64**, 062307 (2001). arXiv:quant-ph/0010095.

[38] Peter Bierhorst. "Geometric decompositions of Bell polytopes with practical applications". J. Phys. A **49**, 215301 (2016). arXiv:1511.04127.

[39] Monique Laurent. "The real positive semidefinite completion problem for series-parallel graphs". Linear Algebra and its Applications **252**, 347–366 (1997).

[40] Vaughan F. R. Jones and J. H. Przytycki. "Lissajous knots and billiard knots". Banach Cent. Pub. **42**, 145–163 (1998).

[41] Kaie Kubjas, Pablo A Parrilo, and Bernd Sturmfels. "How to flatten a soccer ball". In Aldo Conca, Joseph Gubeladze, and Tim Römer, editors, Homological and Computational Methods in Commutative Algebra. Volume 20 of INdAM Ser., pages 141–162. Springer (2017).

[42] Kathleen S. Gibbons, Matthew J. Hoffman, and William K. Wootters. "Discrete phase space based on finite fields". Phys. Rev. A **70**, 062101 (2004). arXiv:quant-ph/0401155.

[43] Reinhard F. Werner. "Uncertainty relations for general phase spaces". Frontiers of Physics **11**, 1–10 (2016). arXiv:arxiv:1601.03843.

[44] Amritanshu Prasad, Ilya Shapiro, and M.K. Vemuri. "Locally compact abelian groups with symplectic self-duality". Adv. Math. **225**, 2429–2454 (2010). arXiv:0906.4397.

[45] Daniel Ciripoi, Nidhi Kaihnsa, Andreas Löhne, and Bernd Sturmfels. "Computing convex hulls of trajectories". Rev. Un. Mat. Argentina **60**, 637–662 (2019). arXiv:1810.03547.

[46] Daniel Plaumann, Rainer Sinn, and Jannik Lennart Wesner. "Families of faces and the normal cycle of a convex semi-algebraic set". Beitr. Algebra Geom. (2022). arXiv:2104.13306.

[47] Daniel R. Grayson and Michael E. Stillman. "Macaulay2, a software system for research in algebraic geometry". Available at http://www.math.uiuc.edu/Macaulay2/.

[48] John Ottem, Kristian Ranestad, Bernd Sturmfels, and Cynthia Vinzant. "Quartic spectrahedra". Mathematical Programming, Ser. B **151**, 585–612 (2015). arXiv:1311.3675.

[49] Adán Cabello. "How much larger quantum correlations are than classical ones". Phys. Rev. A **72**, 012113 (2005). arXiv:quant-ph/0409192.

---

[50] C. E. González-Guillén, C. H. Jiménez, C. Palazuelos, and I. Villanueva. "Sampling quantum nonlocal correlations with high probability". Commun. Math. Phys. **344**, 141–154 (2016). arXiv:1412.4010.

[51] C. R. Johnson and G. Nævdal. "The probability that a (partial) matrix is positive semidefinite". In I. Gohberg, R. Mennicken, and C. Tretter, editors, Recent Progress in Operator Theory. Pages 171–182. Basel (1998). Birkhäuser Basel.

[52] H. H Schaefer and M. P Wolff. "Topological vector spaces". Springer. (1999).

[53] Wojciech Tadej and Karol Życzkowski. "A concise guide to complex Hadamard matrices". Open Systems & Information Dynamics **13**, 133–177 (2006). arXiv:quant-ph/0512154.

[54] H. Barnum, C.P. Gaebler, and A. Wilce. "Ensemble steering, weak self-duality, and the structure of probabilistic theories". Found. Phys **43**, 1411–1427 (2013). arXiv:0912.5532.

[55] Nikos Yannakakis. "Stampacchia's property, self-duality and orthogonality relations". Set-Valued and Variational Analysis **19**, 555–567 (2011). arXiv:1008.4958.

[56] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. "Real algebraic geometry". Volume 36 of A Series of Modern Surveys in Mathematics. Springer Berlin, Heidelberg. (2013).

[57] Joseph H. G. Fu. "Algebraic integral geometry". Pages 47–112. Springer Basel. Basel (2014). arXiv:1103.6256.

[58] Herbert Federer. "Curvature measures". Trans. Amer. Math. Soc. **93**, 418–491 (1959).

[59] Peter Wintgen. "Normal cycle and integral curvature for polyhedra in Riemannian manifolds". In Gy. Soos and J. Szenthe, editors, Differential Geometry. Volume 21. North-Holland, Amsterdam (1982).

[60] Martina Zähle. "Integral and current representation of Federer's curvature measures". Arch. Math. **46**, 557–567 (1986).

[61] David Cohen-Steiner and Jean-Marie Morvan. "Restricted Delaunay triangulations and normal cycle". In SCG '03: Proceedings of the nineteenth annual symposium on Computational geometry. Pages 312–321. (2003).

[62] Pierre Roussillon and Joan Alexis Glaunès. "Surface matching using normal cycles". In Frank Nielsen and Frédéric Barbaresco, editors, Geometric Science of Information. Pages 73–80. Cham (2017). Springer International Publishing.

[63] Kehua Su, Na Lei, Wei Chen, Li Cui, Hang Si, Shikui Chen, and Xianfeng Gu. "Curvature adaptive surface remeshing by sampling normal cycle". Computer-Aided Design **111**, 1–12 (2019).

[64] David A. Cox, John Little, and Donal O'Shea. "Ideals, varieties, and algorithms". Undergraduate Texts in Mathematics. Springer Cham. (2015). Fourth edition.

[65] Guido A. Raggio. "A remark on Bell's inequality and decomposable normal states". Lett. Math. Phys. **15**, 27–29 (1988).

[66] Marc-Olivier Renou, David Trillo, Mirjam Weilenmann, Thinh P. Le, Armin Tavakoli, Nicolas Gisin, Antonio Acín, and Miguel Navascués. "Quantum theory based on real numbers can be experimentally falsified". Nature **600**, 625–629 (2021). arXiv:2101.10873.

[67] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. "All pure bipartite entangled states can be self-tested". Nature Commun. **8**, 15485 (2017). arXiv:1611.08062.

[68] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". Theoret. Comp. Sci. **560**, 7–11 (2014). arXiv:2003.06557.

[69] T. Franz, F. Furrer, and R. F. Werner. "Extremal quantum correlations and cryptographic security". Phys. Rev. Lett. **106**, 250502 (2011). arXiv:1010.1131.

[70] Jędrzej Kaniewski. "Weak form of self-testing". Phys. Rev. Research **2**, 033420 (2020). arXiv:1910.00706.

[71] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. "Generalized privacy amplification". IEEE Transactions on Information Theory **41**, 1915–1923 (1995).

[72] Pavel Sekatski, Jean-Daniel Bancal, Xavier Valcarce, Ernest Y.-Z. Tan, Renato Renner, and Nicolas Sangouard. "Device-independent quantum key distribution from generalized CHSH inequalities". Quantum **5**, 444 (2021). arXiv:2009.01784.

[73] Ernest Y.-Z. Tan, Pavel Sekatski, Jean-Daniel Bancal, René Schwonnek, Renato Renner, Nicolas Sangouard, and Charles C.-W. Lim. "Improved DIQKD protocols with finite-size analysis". Quantum **6**, 880 (2022). arXiv:2012.08714.

[74] Marissa Giustina et al. "Significant-loophole-free test of Bell's theorem with entangled photons". Phys. Rev. Lett. **115**, 250401 (2015). arXiv:1511.03190.

[75] Lynden K. Shalm et al. "Strong loophole-free test of local realism". Phys. Rev. Lett. **115**, 250402 (2015). arXiv:1511.03189.

Accepted in ⟨ʒuantum 2023-02-28, click title to verify. Published under CC-BY 4.0.

58

[76] D. P Nadlinger, J.-D. Bancal, and et al. "Experimental quantum key distribution certified by Bell's theorem". Nature **607**, 682–686 (2022). arXiv:2109.14600.

[77] Wei Zhang, Harald Weinfurter, et al. "A device-independent quantum key distribution system for distant users". Nature **607**, 687–691 (2022). arXiv:2110.00575.

[78] Feihu Xu, Yu-Zhe Zhang, Qiang Zhang, and Jian-Wei Pan. "Device-independent quantum key distribution with random postselection". Phys. Rev. Lett. **128**, 110506 (2022). arXiv:2110.02701.

[79] Wikipedia authors. "Quantum key distribution". url: `https://en.wikipedia.org/wiki/Quantum_key_distribution`. (accessed: 25-October-2021).

[80] Armin Tavakoli, Máté Farkas, Denis Rosset, Jean-Daniel Bancal, and Jedrzej Kaniewski. "Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments". Science Advances **7**, eabc3847 (2021). arXiv:1912.03225.

[81] Stephen J. Summers and Reinhard F. Werner. "Maximal violation of Bell's inequalities for algebras of observables in tangent spacetime regions". Ann. Inst. H. Poincaré. **49**, 215–243 (1988).

[82] N. David Mermin. "Is the moon there when nobody looks? Reality and the quantum theory". Physics Today **38**, 38–47 (1985).

[83] Michael Janas, Michael E. Cuffaro, and Michel Janssen. "Putting probabilities first. How Hilbert space generates and constrains them" (2019) arXiv:1910.10688.

[84] Nicolas Brunner, Stefano Pironio, Antonio Acín, Nicolas Gisin, André Allan Méthot, and Valerio Scarani. "Testing the dimension of Hilbert spaces". Phys. Rev. Lett. **100**, 210503 (2008). arXiv:0802.0760.

[85] Yu Cai, Jean-Daniel Bancal, Jacquiline Romero, and Valerio Scarani. "A new device-independent dimension witness and its experimental implementation". J. Phys. A **49**, 305301 (2016). arXiv:1606.01602.

[86] Wan Cong, Yu Cai, Jean-Daniel Bancal, and Valerio Scarani. "Witnessing irreducible dimension". Phys. Rev. Lett. **119**, 080401 (2017). arXiv:1611.01258.

[87] R. Horodecki, P. Horodecki, and M. Horodecki. "Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition". Phys. Lett. A **200**, 340–344 (1995).

[88] N. Gisin. "Bell's inequality holds for all non-product states". Physics Letters A **154**, 201–202 (1991).

[89] R. Grone, C.R. Johnson, E.M. Sá, and H. Wolkowicz. "Positive definite completions of partial Hermitian matrices". Lin. Alg. Appl. **58**, 109–124 (1984).

[90] Alexander Barvinok. "A course in convexity". Graduate Studies in Mathematics 54. AMS. Providence (2002).

[91] J. Dixmier. "C*-algebras". North-Holland mathematical library. North-Holland. (1982).

[92] M. Reed and B. Simon. "Methods of modern mathematical physics IV: Analysis of operators". Elsevier Science. (1978).

[93] Iain Raeburn and Allan M. Sinclair. "The C*-algebra generated by two projections.". Math. Scand. **65**, 278–290 (1989).

[94] Roy Araiza, Travis Russell, and Mark Tomforde. "A universal representation for quantum commuting correlations". Ann. Henri Poinc. **23**, 4489–4520 (2022). arXiv:2102.05827.

[95] I. Pitowsky. "Quantum probability – quantum logic". Volume 321 of Lect.Notes Phys. Springer. (1989).

[96] Dan Geiger, Christopher Meek, Bernd Sturmfels, et al. "On the toric algebra of graphical models". Ann. Statist. **34**, 1463–1492 (2006). arXiv:math/0608054.

Authors' addresses:

Thinh P. Le, IQOQI Vienna   `Thinh.Le@oeaw.ac.at`
Chiara Meroni, ICERM Providence   `chiara_meroni@brown.edu`
Bernd Sturmfels, MPI-MiS Leipzig and UC Berkeley   `bernd@mis.mpg.de`
Reinhard F. Werner, Leibniz Universität Hannover   `reinhard.werner@itp.uni-hannover.de`
Timo Ziegler, Leibniz Universität Hannover   `timo.ziegler@itp.uni-hannover.de`