New Journal of Physics
The open-access journal for physics

A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations

Miguel Navascués[1,2,4], **Stefano Pironio**[2] **and Antonio Acín**[2,3]
[1] Institute for Mathematical Sciences, Imperial College London, SW7 2PG, UK
[2] ICFO-Institut de Ciencies Fotoniques, 08860 Castelldefels (Barcelona), Spain
[3] ICREA-Institució Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain
E-mail: m.navascues@imperial.ac.uk, Stefano.Pironio@icfo.es and Antonio.Acin@icfo.es

New Journal of Physics **10** (2008) 073013 (29pp)
Received 15 February 2008
Published 8 July 2008
Online at http://www.njp.org/
doi:10.1088/1367-2630/10/7/073013

Abstract. We are interested in the problem of characterizing the correlations that arise when performing local measurements on separate quantum systems. In a previous work (Navascués *et al* 2007 *Phys. Rev. Lett.* **98** 010401), we introduced an infinite hierarchy of conditions necessarily satisfied by any set of quantum correlations. Each of these conditions could be tested using semidefinite programming. We present here new results concerning this hierarchy. We prove in particular that it is complete, in the sense that any set of correlations satisfying every condition in the hierarchy has a quantum representation in terms of commuting measurements. Although our tests are conceived to rule out non-quantum correlations, and can in principle certify that a set of correlations is quantum only in the asymptotic limit where all tests are satisfied, we show that in some cases it is possible to conclude that a given set of correlations is quantum after performing only a finite number of tests. We provide a criterion to detect when such a situation arises, and we explain how to reconstruct the quantum states and measurement operators reproducing the given correlations. Finally, we present several applications of our approach. We use it in particular to bound the quantum violation of various Bell inequalities.

[4] Author to whom any correspondence should be addressed.

Contents

1. Introduction

The main goal of quantum information science (QIS) is to understand the possibilities and limitations of the quantum formalism for information processing and communication. Research in QIS is concerned on one hand with the design of new protocols exploiting the transmission and manipulation of information encoded in quantum states (see for instance [1]). On the other hand, it seeks to identify the constraints on information processing imposed by the quantum formalism. For instance, various information tasks, such as unconditionally secure bit commitment, have been shown to be impossible in a quantum world [2].

A standard scenario in QIS, and which serves as a primitive for more complex protocols, consists of two distant, non-communicating parties, conventionally called Alice and Bob, who share a quantum system in a joint state ρ. Each party makes a measurement on his share of the state and obtains a classical outcome. On a phenomenological level, we may describe the situation by saying that the two parties have access to a black box (see figure 1). When Alice inputs a measurement X into the box, she gets as output a measurement outcome

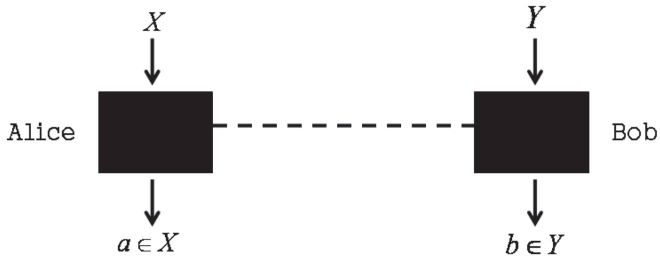

Figure 1. Local measurements on a system shared by two observers viewed as a black-box process. Alice chooses a measurement input X and obtains a measurement output $a \in X$. Similarly, Bob chooses an input Y and receives an output $b \in Y$. The behavior of the system is characterized by the joint probabilities $P(a, b)$.

$a \in X$; similarly, when Bob inputs a measurement Y, he receives an output $b \in Y$. The behavior of the box is completely characterized by the joint detection probabilities $P(a, b)$. From now on, we simply call a *behavior* the set $P = \{P(a, b)\}$ of all such probabilities.

Though in the above scenario the parties are separated and perform local measurements, their outcomes a and b may be non-trivially correlated, in particular if the initial quantum state ρ is entangled. These correlated data can be exploited for different tasks, such as communication complexity [3] or key distribution [4]. From the perspective of QIS, it is thus meaningful to characterize which outcome correlations can or cannot be produced by two non-communicating quantum observers. The main problem with which we are concerned in this paper is thus the following: given a behavior P, do there exist a quantum state ρ and local measurements X and Y reproducing the outcome probabilities described by P? Note that we do not impose here any constraints on the dimension of the system shared by Alice and Bob, as we are interested in the most general set of correlations that can be obtained with quantum resources.

The special case of classical observers is relatively well understood. The correlations obtained in this scenario coincide with the ones that can be achieved with shared randomness, or using another terminology, with those that are described by local-hidden variable models [5]. For a given number of possible measurement inputs and outputs, the set of local classical correlations forms a convex polytope whose vertices correspond to all the possible deterministic assignments of outputs to inputs. It thus follows that linear programming can be used to decide if a given behavior is reproducible by two local classical observers [6, 7]. The facets of the classical polytope, which form the boundary of the classical region, correspond to the well-known Bell inequalities [8].

Our understanding of the general case of quantum observers, with which we are concerned here, is more rudimentary. The difficulty lies in the fact that we do not have a practical characterization of the set of quantum behaviors and that this set cannot be described by a finite number of extreme points (see figure 2) [9].

Apart from the QIS motivation, the problem of characterizing the set of quantum behaviors is also of relevance from a fundamental perspective. Indeed, while quantum mechanics has been so far confirmed by plenty of experiments, we cannot exclude that someday it will be disproved. If some experimental data were inconsistent with the quantum model that we have for the experiment, would that however necessarily imply the breakdown of the whole

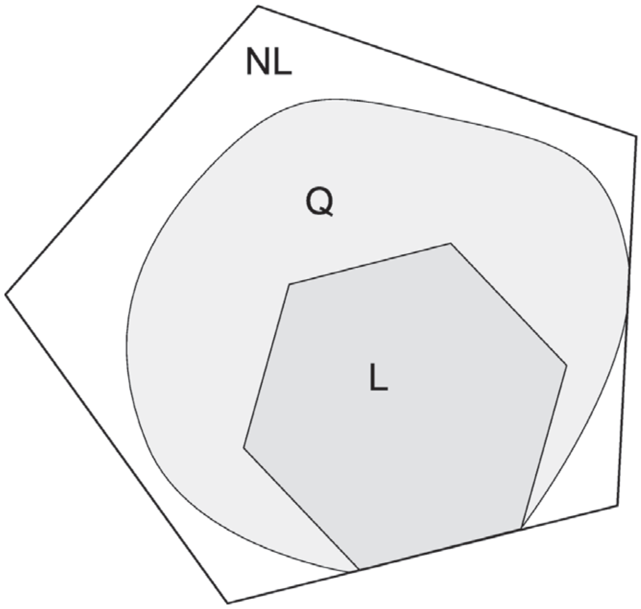

Figure 2. Schematic representations of the space of joint distributions $P(a, b)$ (for fixed and finite number of possible inputs and outputs). L denotes the set of correlations that admit a local model; it is a polytope and membership in L can be decided using linear programming [6, 7]. NL is the global set that contains all (in particular non-local) correlations; it is again a polytope. The region accessible to quantum mechanics is Q. The quantum set is not a polytope, i.e. it does not have a finite number of extreme points. As represented in the figure, Q contains L and is a proper subset of NL. See [9] or [10] for more details.

quantum formalism? How could one exclude that there is no other quantum model explaining the observed data? The problem then is to establish experimentally testable conditions that can rule out the whole quantum structure, in a similar fashion as Bell's inequalities do for the locally causal model. In this context, one is again confronted with the problem of characterizing the constraints on correlations imposed by the quantum formalism.

One of the first researchers to study the characterization of quantum correlations was Tsirelson in 1980 [11]. Tsirelson got several important results for the case of measurements with binary outcomes [9]; most notably he derived the maximal quantum violation of the Clauser–Horne–Shimony–Holt (CHSH) inequality [12]. More recently, the problem has attracted the interest of several researchers working in QIS [13]. Among the latest contributions, we point out the work of Wehner [14], who showed that part of Tsirelson's findings could be implemented using a relatively new numerical tool called semidefinite programing (SDP). A short introduction to this technique is given in appendix A, more details can be found in [15]. Apart from Wehner's paper, there are several other papers using SDP techniques to bound the set of quantum correlations [16, 17]. Most of these results deal with the case of two-outcome measurements.

In a recent work [18], we introduced a hierarchy of SDP tests to check if a given behavior admits a quantum representation; this hierarchy is similar in spirit to some existing SDP hierarchies for the characterization of the set of separable states [19, 20]. Compared to previous constructions, our method is completely general as it can be applied to any number of parties, measurements and outcomes, and is independent of the dimension of the quantum systems. In this work, we explore further the approach introduced in [18].

The basic idea behind our method is presented in section 3. Instead of directly searching for a quantum state and measurement operators reproducing a given behavior—a computationally highly difficult task, if not impossible if the dimension of the system is unbounded—we consider instead a family of weaker conditions. Each of our conditions amounts to verify the existence of a positive semidefinite matrix whose structure depends on the general algebraic properties satisfied by quantum states and measurement operators. If one of our conditions is not satisfied, we can immediately conclude that the given behavior is not quantum. In section 4, we show that our family of tests can be organized as an infinite hierarchy of increasingly stronger conditions. We prove that in the asymptotic limit, our hierarchy is complete in the sense that any behavior that satisfies all the conditions in the hierarchy necessarily has a quantum representation in terms of commuting measurements. We show further that in some cases it is possible to conclude that a behavior is quantum after a *finite* number of steps only. We provide a criterion to detect when such a situation arises, and we explain how to reconstruct in this case explicit quantum states and measurement operators reproducing the given behavior. Based on these latter results, we then show how a slight modification of our tests allow us to reduce the problem of deciding if a behavior has a quantum representation with quantum systems of finite dimension d to a rank minimization problem. Unfortunately, and contrary to SDP, there are no efficient algorithms to solve rank-minimization problems. In section 5, we present several applications of our method. We use it in particular to put upper bounds on the quantum violation of various Bell inequalities. We conclude with a discussion and some open questions in section 6.

2. Definitions

2.1. Measurement scenario

We consider measurement scenarios as illustrated in figure 1. We assume that outputs corresponding to different inputs are labeled in a distinct way. Each output, say a of Alice, is thus uniquely associated to a single input $X(a)$. We denote by A the set of all outputs of Alice and by B the set of all outputs of Bob. The inputs of Alice may be viewed as disjoint subsets of A, and those of Bob as disjoints subsets of B. A measurement scenario is thus specified by a quadruple $(A, B, \mathcal{X}, \mathcal{Y})$, where $\mathcal{X}$ and $\mathcal{Y}$ are partitions of A and B, respectively.

The measurement scenarios that we consider in this paper always involve a *finite* number of inputs and outputs, i.e. A and B are finite sets. A behavior P thus consists of a finite set of $|A| \times |B|$ joint probabilities: $P = \{P(a, b) : a \in A, b \in B\}$. For instance, in the case where Alice and Bob have each a choice between s different inputs that each yield one out of d outputs, a behavior consists of $s^2 \times d^2$ joint probabilities. Except when otherwise mentioned, we assume in the remaining of the paper that a measurement scenario $(A, B, \mathcal{X}, \mathcal{Y})$ and a behavior P have been specified. Our aim is to determine if P represents a possible quantum process.

2.2. Quantum behaviors

Definition 1. *The behavior P is a quantum behavior if there exists a pure state $|\psi\rangle$ in a Hilbert space $\mathcal{H}$, a set of measurement operators $\{E_a : a \in A\}$ for Alice, and a set of measurement* *operators* $\{E_b : b \in B\}$ *for Bob, such that for all* $a \in A$ *and* $b \in B$

$$P(a,b) = \langle\psi|E_a E_b|\psi\rangle\,, \tag{1}$$

with the measurement operators E *satisfying*

1. $E_a^\dagger = E_a$ *and* $E_b^\dagger = E_b$ *(hermiticity),*
2. $E_a E_{\bar{a}} = \delta_{a\bar{a}} E_a$ *if* $X(a) = X(a')$ *and* $E_b E_{\bar{b}} = \delta_{b\bar{b}} E_b$ *if* $Y(b) = Y(b')$ *(orthogonality),*
3. $\sum_{a\in X} E_a = \mathbb{1}$ *and* $\sum_{b\in Y} E_b = \mathbb{1}$ *(completeness),*
4. $[E_a, E_b] = 0$ *(commutativity).*

The set of all quantum behaviors will be denoted by Q.

The first three properties are necessary to ensure that the operators E_a and E_b are projectors and define proper measurements. The fourth property simply expresses the fact that Alice and Bob perform separated measurements on the global state $|\psi\rangle$.

Note that more generally we could have defined a quantum behavior in terms of a mixed state ρ rather than a pure one and in terms of general measurements, also known as positive operator valued measures (POVM) [1], rather than projective ones. But remark also that in our definition we put no restrictions at all on the dimension of the Hilbert space. Since any general measurement on a given Hilbert space can be viewed as a projective measurement on a larger Hilbert space, and any mixed state ρ can be viewed as a subsystem of a larger system in a pure state $|\psi\rangle$ [1], the above definition turns out to be completely general.

Property 3 implies that the marginal probabilities $P(a) = \sum_{b\in Y} P(a,b)$ and $P(b) = \sum_{a\in X} P(a,b)$ are well defined and independent of what is measured on the other side (i.e. P satisfies the no-signaling constraints). This also implies that in the above definition there is some redundancy in the specification of the operators $\{E_a : a \in A\}$ of Alice since any one of them can be written as the identity minus the other ones. To simplify further the definition above, select an output $a_X \in X$ for each input X and introduce the reduced output sets $\tilde{X} = \{a : a \in X, a \neq a_X\}$ and $\tilde{A} = \cup_X \tilde{X}$. Introduce analogous sets $\tilde{Y}$ and $\tilde{B}$ for Bob. The following definition is then equivalent to definition 1.

Definition 2. *The behavior* P *is a quantum behavior if there exists a pure (normalized) state* $|\psi\rangle$ *in a Hilbert space* $\mathcal{H}$*, a set of measurement operators* $\{E_a : a \in \tilde{A}\}$ *for Alice, and a set of measurement operators* $\{E_b : b \in \tilde{B}\}$ *for Bob such that for all* $a \in \tilde{A}$ *and* $b \in \tilde{B}$

$$\begin{aligned} P(a) &= \langle\psi|E_a|\psi\rangle, \\ P(b) &= \langle\psi|E_b|\psi\rangle, \\ P(a,b) &= \langle\psi|E_a E_b|\psi\rangle, \end{aligned} \tag{2}$$

with the measurement operators satisfying

1. $E_a^\dagger = E_a$ *and* $E_b^\dagger = E_b$ *(hermiticity),*
2. $E_a E_{\bar{a}} = \delta_{a\bar{a}} E_a$ *if* $X(a) = X(a')$ *and* $E_b E_{\bar{b}} = \delta_{b\bar{b}} E_b$ *if* $Y(b) = Y(b')$ *(orthogonality),*
3. $[E_a, E_b] = 0$ *(commutativity).*

It is clear that any behavior satisfying definition 1 also satisfies definition 2. The converse statement is also true. Indeed given sets of operators $\{E_a : a \in \tilde{A}\}$ and $\{E_b : b \in \tilde{B}\}$ satisfying definition 2, define the missing operators E_{a_X} and E_{b_Y} through $E_{a_X} = \mathbb{1} - \sum_{a\in\tilde{X}} E_a$ and $E_{b_Y} = \mathbb{1} - \sum_{b\in\tilde{Y}} E_b$. It is then easy to see that the now-complete sets $\{E_a : a \in A\}$ and $\{E_b : b \in B\}$ satisfy definition 1.

Before concluding this subsection, note that when dealing with finite dimensional Hilbert spaces, one tends to associate a tensor product structure to separated measurements. This leads to another set Q' of quantum behaviors, possibly equivalent to Q, and defined as follows.

Definition 3. *The behavior P belongs to the set of quantum behaviors Q' if there exists a pure state $|\psi\rangle$ in a composite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, a set of measurement operators $\{E_a : a \in A\}$ for Alice, and a set of measurement operators $\{E_b : b \in B\}$ for Bob, such that for all $a \in A$ and $b \in B$*

$$P(a, b) = \langle\psi|E_a \otimes E_b|\psi\rangle, \tag{3}$$

with the measurement operators E satisfying

1. *$E_a^\dagger = E_a$ and $E_b^\dagger = E_b$ (hermiticity),*
2. *$E_a E_{\bar{a}} = \delta_{a\bar{a}} E_a$ if $X(a) = X(a')$ and $E_b E_{\bar{b}} = \delta_{b\bar{b}} E_b$ if $Y(b) = Y(b')$ (orthogonality),*
3. *$\sum_{a\in X} E_a = \mathbb{1}_A$ and $\sum_{b\in Y} E_b = \mathbb{1}_B$ (completeness).*

Clearly, $Q' \subseteq Q$. However, it is an open question whether these two sets are equal. In the special case of finite dimensional Hilbert spaces, they turn out to be identical [21]. In this work, we adopt definition 1, or equivalently definition 2, partly because it is much better tailored to the structure of our construction. We will come back to the commutation versus tensor product issue in section 6.1.

2.3. Sets of operators and sequences

In this section, we introduce a few other definitions that will be needed later on.

Let $\mathcal{E}$ denote the set of projectors appearing in definition 1, i.e. $\varepsilon = \{E_a : a \in A\} \cup \{E_b : b \in B\}$, and $\tilde{\mathcal{E}}$ denote the set of projectors of definition 2 plus the identity, i.e. $\tilde{\mathcal{E}} = \mathbb{1} \cup \{E_a : a \in \tilde{A}\} \cup \{E_b : b \in \tilde{B}\}$.

Let $\mathcal{O} = \{O_1, \ldots, O_n\}$ be a set of n operators, where each O_i is a linear combination of products of projectors in $\tilde{\mathcal{E}}$. Thus $\mathcal{O}$ is a finite subset of the algebra generated by $\tilde{\mathcal{E}}$. Note that we can equally well define the set $\mathcal{O}$ in terms of $\mathcal{E}$, since $\mathcal{E}$ and $\tilde{\mathcal{E}}$ are equivalent up to linear combinations. Define $\mathcal{F}(\mathcal{O})$ as the set of all independent equalities of the form

$$\sum_{ij} (F_k)_{ij} \langle\psi|O_i^\dagger O_j|\psi\rangle = g_k(P), \quad k = 1, \ldots, m, \tag{4}$$

which are satisfied by the operators O_i, where the coefficients $g_k(P)$ are linear functions of the probabilities $P(a, b)$:

$$g_k(P) = (g_k)_0 + \sum_{a,b} (g_k)_{ab} P(a, b) \tag{5}$$

and where $|\psi\rangle$ is the state appearing in definition 2. These equations are the ones that formally follow from the definition of the O_is, the relation (2), and properties 1–3 of definition 2. Each set of operators $\mathcal{O}$ define such a collection of equations. As an example of equation of the form (4), suppose that the set $\mathcal{O}$ contains the operators $\{O_k\}_{k=1}^d = \{E_b E_a S : a \in X\}$, where S is some arbitrary operator in the algebra generated by $\mathcal{E}$, and also contains the operator $O_{d+1} = E_b S$. Then $\sum_{k=1}^d O_k^\dagger O_k = \sum_{a\in X}(E_b E_a S)^\dagger E_b E_a S = \sum_{a\in X} S^\dagger E_a E_b E_b E_a S = \sum_{a\in X} S^\dagger E_b E_a E_b S = S^\dagger E_b E_b S = O_{d+1}^\dagger O_{d+1}$, and thus $\sum_{k=1}^d \langle\psi|O_k^\dagger O_k|\psi\rangle - \langle\psi|O_{d+1}^\dagger O_{d+1}|\psi\rangle = 0$.

Let *a sequence* S be a product of projectors in $\tilde{\mathcal{E}}$. Examples of sequences are E_a and $E_a E_{a'} E_b$. Note that some sequences may correspond to the null operator, for instance, $E_a E_a' = 0$ if $a \neq a'$, and $X(a) = X(a')$; in the following, when we speak of a sequence, we always mean a non-null sequence. The *length* $|S|$ of a sequence is the minimum number of projectors needed to generate it. For instance $|E_a E_b E_a| = |E_a E_a E_b| = |E_a E_b| = 2$. By convention, the length of the identity operator is $|\mathbb{1}| = 0$. We define $\mathcal{S}_n$ to be the set of sequences of length smaller than or equal to n (excluding null sequences). Thus

$$
\begin{aligned}
\mathcal{S}_0 &= \{\mathbb{1}\},\\
\mathcal{S}_1 &= \mathcal{S}_0 \cup \{E_a : a \in \tilde{A}\} \cup \{E_b : b \in \tilde{B}\},\\
\mathcal{S}_2 &= \mathcal{S}_0 \cup \mathcal{S}_1 \cup \{E_a E_{a'} : a, a' \in \tilde{A}\} \cup \{E_b E_{b'} : b, b' \in \tilde{B}\} \cup \{E_a E_b : a \in \tilde{A}, b \in \tilde{B}\},\\
\mathcal{S}_3 &= \ldots .
\end{aligned}
$$

It is clear that $\mathcal{S}_1 \subseteq \mathcal{S}_2 \subseteq \ldots$, and that any operator $O_i \in \mathcal{O}$ can be written as a linear combination of operators in $\mathcal{S}_n$ for n sufficiently large.

3. Basic idea of our method

The following proposition associates to each set of operators $\mathcal{O}$ satisfying equations (4) a condition that restricts the possible correlations that can arise between two quantum observers.

Proposition 4. *Let $\mathcal{O}$ be a set of operators and $\mathcal{F}(\mathcal{O})$ the set of equations of the form (4) satisfied by operators in $\mathcal{O}$. Then, a necessary condition for a behavior P to be quantum is that there exists a complex Hermitian $n \times n$ positive semidefinite matrix $\Gamma \succeq 0$ whose entries Γ_{ij} satisfy*

$$\sum_{ij} (F_k)_{ij}\Gamma_{ij} = g_k(P), \quad k = 1, \ldots, m. \tag{6}$$

Moreover, if the coefficients F_k and g_k in (4) are real, we can take Γ to be real as well.

Proof. If P is quantum, there exist a state $|\psi\rangle$ and projectors E_a and E_b as in definition 2, and therefore there also exist operators O_i satisfying the relations (4). Then simply define the entries of the matrix Γ through

$$\Gamma_{ij} = \langle\psi|O_i^\dagger O_j|\psi\rangle. \tag{7}$$

Clearly, Γ satisfies (6). Moreover, it is positive semidefinite since for all $v \in \mathbb{C}^n$

$$v^\dagger \Gamma v = \sum_{ij} v_i^* \Gamma_{ij} v_j = \sum_{ij} v_i^* \langle\psi|O_i^\dagger O_j|\psi\rangle v_j = \langle\psi|V^\dagger V|\psi\rangle \geqslant 0, \tag{8}$$

where $V = \sum_j v_j O_j$.

If the coefficients F_k and g_k in (1) are real, redefine Γ as $(\Gamma + \Gamma^*)/2$. Then Γ still is positive semidefinite and satisfies (6). □

Any $n \times n$ positive semidefinite matrix Γ satisfying the linear constraints (6) will be called a *certificate* associated to $\mathcal{O}$. As an illustration, we now give two examples of application of proposition 4.

Example 1. Consider a measurement scenario where Alice has a choice between two measurements, $X = 1$ or 2, to perform on her subsystem, and where both measurements yield binary outcomes with values $\pm X$. Likewise, Bob has a choice between two measurements, $Y = 3$ or 4, with outcomes $\pm Y$.

The single-party measurement averages $C_X = P(+X) - P(-X)$ and $C_Y = P(+Y) - P(-Y)$ together with the two-party correlation functions $C_{XY} = P(+X, +Y) + P(-X, -Y) - P(+X, -Y) - P(-X, +Y)$ fully determine the response of the joint system of Alice and Bob. The observed data are thus characterized by the eight numbers $\{C_1, C_2, C_3, C_4, C_{12}, C_{13}, C_{23}, C_{24}\}$ which are equivalent to the knowledge of the entire set of probabilities $P(\pm X, \pm Y)$.

Criterion 5. *If the data observed by Alice and Bob represent the response of a quantum system, there exists a real symmetric* 5×5 *positive semidefinite matrix* $\Gamma \succeq 0$ *of the form*

$$\Gamma = \begin{pmatrix} 1 & C_1 & C_2 & C_3 & C_4 \\ & 1 & u & C_{13} & C_{14} \\ & & 1 & C_{23} & C_{24} \\ & & & 1 & v \\ & & & & 1 \end{pmatrix}, \tag{9}$$

where u *and* v *are unspecified entries.* (*We have only given the upper triangular part of* Γ *since it is symmetric.*)

Proof. If the data observed by Alice and Bob represent the response of a quantum system, there exist a state $|\psi\rangle$, two projectors $E_{\pm X}$ associated to each of the two measurements $X = 1, 2$ of Alice and two projectors $E_{\pm Y}$ associated to each of the two measurements $Y = 3, 4$ of Bob. Let $\mathcal{O} = \{\sigma_0, \sigma_1, \ldots, \sigma_4\}$, where $\sigma_0 = \mathbb{1}$ is the identity operator and $\sigma_i = E_{+i} - E_{-i}$ $(i = 1, \ldots, 4)$. It is easily verified from equations (1) and properties 1–4 that these operators satisfy the equalities

$$\langle\psi|\sigma_i^\dagger \sigma_i|\psi\rangle = 1 \quad i = 0, \ldots, 4, \tag{10}$$

$$\langle\psi|\sigma_0^\dagger \sigma_i|\psi\rangle = C_i \quad i = 1, \ldots, 4, \tag{11}$$

$$\langle\psi|\sigma_i^\dagger \sigma_j|\psi\rangle = C_{ij} \quad i = 1, 2; \quad j = 3, 4, \tag{12}$$

which are the counterparts of equations (4). It immediately follows that the associated 5×5 matrix $\Gamma_{ij} = \langle\psi|\sigma_i^\dagger \sigma_j|\psi\rangle$ has the form (9). It can be taken real if we further redefine Γ as $(\Gamma + \Gamma^*)/2$. □

Example 2. Consider the case where Alice and Bob have a choice between s different measurements that each yield one out of d possible outcomes. The s measurements of Alice are labeled $X = 1, \ldots, s$ and her $m = s \times d$ possible outcomes are labeled $a = 1, \ldots, m$, where outcomes in the range $1 + (k-1)\,d, \ldots, kd$ belong to the measurement $X = k$. Analogously, the s measurements of Bob are labeled $Y = s+1, \ldots, 2s$ and his $m = s \times d$ outcomes are

$b = m+1, \ldots, 2m$, where again outcomes in the range $1+(k-1)d, \ldots, kd$ belong to the measurement $Y = k$. This measurement scenario is characterized by the m^2 joint probabilities $P(a, b)$. □

Criterion 6. *If the set of m^2 probabilities $P(a, b)$ admits a quantum representation, there exists a $2m \times 2m$ real symmetric positive semidefinite matrix $\Gamma \succeq 0$ of the form*

$$\Gamma = \begin{pmatrix} Q & P \\ P^T & R \end{pmatrix}, \tag{13}$$

where the submatrix P is the $m \times m$ table of probabilities with entries $P_{ab} = P(a, b)$, and where the submatrices Q and R satisfy

$$Q_{aa'} = \delta_{aa'} P(a), \qquad \text{if } X(a) = X(a'), \tag{14}$$

$$R_{bb'} = \delta_{bb'} P(b), \qquad \text{if } Y(b) = Y(b'). \tag{15}$$

Proof. If the measurement scenario is a quantum measurement scenario, there exist a quantum state $|\psi\rangle$, m projectors E_a for Alice, and m projectors E_b for Bob satisfying the properties of definition 1. Consider the set $\mathcal{O} = \mathcal{E} = \{E_1, \ldots, E_m, E_{m+1}, \ldots, E_{2m}\}$ consisting of the m operators of Alice and the m ones of Bob. They satisfy the equalities

$$\begin{aligned} \langle\psi|E_a E_b|\psi\rangle &= P(a, b), \\ \langle\psi|E_a E_a'|\psi\rangle &= \delta_{aa'} P(a), \qquad \text{if } X(a) = X(a'), \\ \langle\psi|E_b E_b'|\psi\rangle &= \delta_{bb'} P(b), \qquad \text{if } Y(b) = Y(b'), \end{aligned} \tag{16}$$

as implied by equations (1) and property 2. It immediately follows that the certificate Γ associated to $\mathcal{O}$ has the form (13). □

Note that the matrix (13) can be thought of as a table of probabilities, where Γ_{ij} is the probability to obtain the two outcomes $i, j \in \{1, \ldots, 2m\}$. The only entries of this matrix which are not specified are the entries $\Gamma_{aa'} = Q_{aa'}$ associated to different measurements of Alice, $X(a) \neq X(a')$, and the entries $\Gamma_{bb'} = R_{bb'}$ associated to different measurements of Bob, $Y(b) \neq Y(b')$. This is coherent with our interpretation of Γ since in a quantum scenario these entries correspond to non-commuting measurements performed on the same subsystem and are thus not jointly observable. Nonetheless, if the correlations $P(a, b)$ have a quantum origin it is possible to assign a numerical value to these undetermined entries, namely $\langle\psi|E_a E_{a'}|\psi\rangle$ and $\langle\psi|E_b E_{b'}|\psi\rangle$[5], such that the overall matrix (13) is positive semidefinite.

3.1. Testing the existence of a certificate with SDP

Checking the existence of a certificate Γ, such as the ones given in examples 1 and 2, can be cast as a SDP. Indeed, it amounts to solving the following problem

$$\begin{aligned} \text{maximize} \quad & \lambda, \\ \text{subject to} \quad & \operatorname{tr}\left(F_k^T \Gamma\right) = g_k(P), \quad k = 1, \ldots, m, \\ & \Gamma - \lambda \mathbb{1} \succeq 0, \end{aligned} \tag{17}$$

[5] Or the real part of these expressions, if we take Γ real.

which after some elementary manipulations can be put in the form (A.1). A positive solution $\lambda \geqslant 0$ to the above problem implies that there exists a positive semidefinite matrix $\Gamma \succeq \lambda I \succeq 0$ compatible with the linear constraints (6). A strictly negative solution $\lambda < 0$ means that any matrix Γ compatible with (6) is necessarily negative definite and thus that the given behavior P does not represent the outcome of a quantum experiment.

As mentioned in appendix A, there exist many available programs to solve problems of the type (17). Such programs solve these problems both in their primal and dual forms. The dual of (17) is

$$\begin{aligned} \text{minimize} \quad & \sum_k y_k g_k(P), \\ \text{subject to} \quad & F(y) = \sum_k y_k F_k^T \succeq 0, \\ & \sum_k y_k \mathrm{tr}(F_k^T) = 1. \end{aligned} \tag{18}$$

If a program returns a negative solution for the primal for a given behavior P^*, it also yields a dual feasible point y such that $\sum_k y_k g_k(P^*) < 0$. This dual feasible point provides a proof that the given behavior P^* is not quantum; it can be interpreted as a *quantum Bell inequality* violated by P^* in the sense that $\sum_k y_k g_k(P) \geqslant 0$ is a linear inequality satisfied by all quantum probabilities. Indeed, the coefficients $g_k(P)$ defined in (5) depend linearly on the probabilities $P(a, b)$, and thus the expression $\sum y_k g_k(P)$ is a linear expression in the probabilities $P(a, b)$. Moreover, from the second line of (18), we deduce that for all behaviors P having a positive certificate $\Gamma \succeq 0$, in particular, for all quantum behaviors, this linear expression is positive: $\sum_k y_k g_k(P) = \sum_k y_k \mathrm{tr}(F_k^T \Gamma) = \mathrm{tr}(F(y)\Gamma) \geqslant 0$ since $\Gamma \succeq 0$. The behavior P^*, however, violates this inequality, $\sum_k y_k g_k(P^*) < 0$, which demonstrates that it does not belong to Q.

3.2. Equivalence between certificates

Each set $\mathcal{O}$ of operators that we can write down yields a different condition satisfied by quantum theory. However, not all conditions built in this way are independent, as the following lemma shows.

Lemma 7. *Let $\mathcal{O}$ and $\mathcal{O}'$ be two sets of operators such that every operator in $\mathcal{O}'$ is a linear combination of operators in $\mathcal{O}$. Then, the existence of a certificate Γ associated to $\mathcal{O}$ (for a given P) implies the existence of a certificate Γ' associated to $\mathcal{O}'$.*

Proof. By hypothesis, every operator $O_i' \in \mathcal{O}'$ can be written as $O_i' = \sum_k C_{ik} O_k$, where $O_k \in \mathcal{O}$. Define then $\Gamma_{ij}' \equiv \sum_{kl} C_{ki}^* \Gamma_{kl} C_{lj}$. It is clear that Γ' satisfies the equalities (6) associated to $\mathcal{O}'$, given that Γ satisfies the ones associated to $\mathcal{O}$. We also have that $\Gamma' = C^\dagger \Gamma C \succeq 0$, and thus Γ' is a certificate associated to $\mathcal{O}'$. □

The criterion of example 2 for $s = 2$ and $d = 2$, for instance, is equivalent to the one of example 1, because the set of eight operators $\{E_{+1}, E_{-1}, E_{+2}, E_{-2}, E_{+3}, E_{-3}, E_{+4}, E_{-4}\}$ is linearly equivalent to the set of five operators $\{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$.

In numerical implementations, we have of course always interest to use a criterion based on a set $\mathcal{O}$ of linearly independent operators so as to minimize the size of the matrices involved.

Note also that to check systematically all the conditions that follow from our approach, it is sufficient to check the ones associated with the sets $\mathcal{S}_n$ defined in section 2.3 since they generate by linear combinations all other possible operators. This point is made more precise in the next section.

4. A hierarchy of necessary conditions

Motivated by the above lemma, define a *certificate of order* n, denoted Γ^n, as a certificate associated to the set of operators $\mathcal{S}_n$. A certificate of order n is thus a $|\mathcal{S}_n| \times |\mathcal{S}_n|$ matrix and to index its row and columns we will use symbols that are in direct correspondence with the elements of $\mathcal{S}_n$. Sequence operators S, E_a, $E_a S$, and $\mathbb{1}$ will be associated with row or column indices, s, a, as, and 1, respectively. We define the length $|s|$ of an index s to be the length $|S|$ of the corresponding sequence S. A certificate Γ^n is thus a matrix with entries $\{\Gamma^n_{s,t} : |s|, |t| \leqslant n\}$, which according to the proof of proposition 4 may be interpreted as $\Gamma^n_{s,t} = \langle\psi|S^\dagger T|\psi\rangle$ if P is a quantum behavior.

From proposition 4 and the definition of the set $\mathcal{S}_n$, we deduce that Γ^n is a real positive semidefinite matrix that satisfies the linear equalities

$$\Gamma^n_{1,1} = 1\,, \quad \Gamma^n_{1,a} = P(a)\,, \quad \Gamma^n_{1,b} = P(b)\,, \quad \Gamma^n_{a,b} = P(a,b), \tag{19}$$

for all $a \in \tilde{A}$ and $b \in \tilde{B}$, and

$$\Gamma^n_{s,t} = \Gamma^n_{u,v}, \quad \text{if } S^\dagger T = U^\dagger V, \qquad \left(\Gamma^n_{s,t} = 0, \quad \text{if } S^\dagger T = 0\right), \tag{20}$$

for all $|s|, |t|, |u|, |v| \leqslant n$. Here the relations $S^\dagger T = U^\dagger V$ (or $S^\dagger T = 0$) are the ones that follow from properties 1–3 of definition 2. For instance, $\Gamma^n_{ab,a} = \Gamma^n_{1,ab}$, and $\Gamma^n_{ab,a'} = 0$ if $X(a) = X(a')$.

As we mentioned earlier, $\mathcal{S}_1 \subseteq \mathcal{S}_2 \subseteq \cdots \subseteq \mathcal{S}_n \subseteq \ldots$, and thus the family of certificates $\Gamma^1, \Gamma^2, \ldots, \Gamma^n, \ldots$, represents a hierarchy of conditions satisfied by quantum probabilities, where each condition in the hierarchy is stronger than the previous ones. Moreover, since in the limit $n \to \infty$ the linear span of $\mathcal{S}_n$ coincides with the entire algebra of operators generated by $\tilde{\mathcal{E}}$, this hierarchy embraces, according to lemma 7, all the conditions that can be built from our approach. The strategy that we propose to verify the quantum origin of a given behavior P is thus the following. Check first if there exists a certificate Γ^1 of order 1 associated to P. If there is no such certificate, we can conclude that the behavior P is not quantum, otherwise check the existence of a certificate Γ^2 of order 2. Repeat the procedure with certificates of increasing order as long as the behavior P satisfies the previous tests.

A geometrical interpretation of our hierarchy is given in figure 3, where Q^n denotes the set of all behaviors P for which there exists a certificate of order n.

4.1. Sufficiency of the hierarchy

We now show that our hierarchy is complete in the sense that $\lim_{n\to\infty} Q^n = Q$ or in other words that any non-quantum behavior P necessarily fails one of our conditions at some step in the hierarchy.

Theorem 8. *Let P be a behavior such that there exists a certificate Γ^n of order n for all $n \geqslant 1$. Then P belongs to Q.*

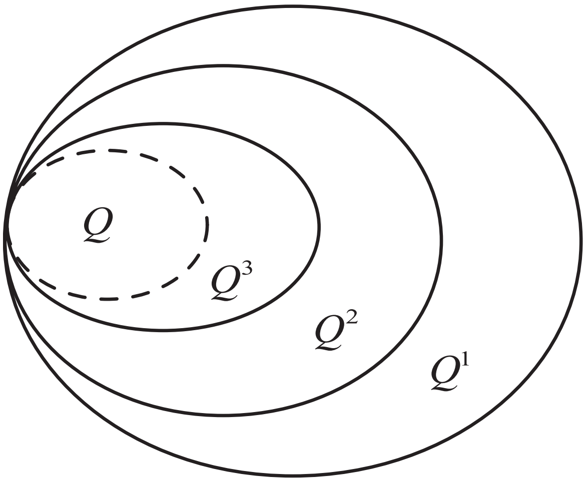

Figure 3. Geometrical interpretation of our hierarchy. Q is the set of quantum behaviors. Q^n denotes the set of all behaviors for which there exists a certificate of order n. Testing the existence of a certificate of order n amounts to determine if a given behavior P belongs to Q^n. Certificates of higher order provide a more accurate approximation of the quantum set Q, but are more demanding from a computational point of view.

Proof. The proof proceeds in two steps. We first show that the sequence of certificates Γ^n admits a proper limit $\lim_{n\to\infty}\Gamma^n \to \Gamma^\infty$. We then construct from the matrix Γ^∞ a quantum state and quantum operators acting on a (possibly infinite-dimensional) Hilbert space $\mathcal{H}$ that reproduce the behavior P.

Note first, as shown in appendix B, that all the entries $\{\Gamma^n_{s,t} : |s|, |t| \leqslant n\}$ of the matrices Γ^n are bounded by 1, i.e. $|\Gamma^n_{s,t}| \leqslant 1$. Now, complete each matrix Γ^n with zeros to make it an infinite matrix $\hat{\Gamma}^n$ with entries $\{\hat{\Gamma}^n_{s,t} : |s|, |t| = 0, 1, \ldots\}$; we can then view the matrices $\hat{\Gamma}^n$ as infinite vectors in l_∞ (the normed space of all bounded sequences $u = (u_1, u_2, \ldots)$, with norm given by $\|u\|_\infty = \sup_i |u_i|$). As the sequence $\{\hat{\Gamma}^n : n = 1, 2, \ldots\}$ belongs to the unit ball of l_∞, it admits, by the Banach–Alaoglu theorem, a subsequence $\{n_i\}$ that converges in the weak-$*$ topology to a limit $\hat{\Gamma}^{n_i} \to \Gamma^\infty$ when $i \to \infty$ [22]. This implies in particular pointwise convergence, i.e.

$$\lim_{i\to\infty} \hat{\Gamma}^{n_i}_{s,t} \to \Gamma^\infty_{s,t}, \tag{21}$$

for all s, t. From the pointwise convergence, we deduce that Γ^∞ satisfies equations (19) and (20) for all s, t, u and v. Moreover, let $\hat{\Gamma}^n_N$ denote the submatrix of $\hat{\Gamma}^n$ corresponding to the entries $\{\hat{\Gamma}^n_{s,t} : |s|, |t| \leqslant N\}$. Since $\hat{\Gamma}^n_N \succeq 0$ for all n and N, (21) implies that $\Gamma^\infty_N \succeq 0$ for all $N = 1, 2, \ldots$.

In the remainder of the proof, we construct from the matrix Γ^∞ a state $|\phi\rangle$ and operators $\{\hat{E}_a : a \in \tilde{A}\}$ and $\{\hat{E}_b : b \in \tilde{B}\}$ satisfying the properties of definition 2.

The fact that $\Gamma^\infty_N \succeq 0$ for all N implies that there exists an infinite family of vectors $\{|v_s\rangle : |s| = 0, 1, 2, \ldots\}$ whose scalar products reproduce the entries of Γ^∞, i.e.

$$\Gamma^\infty_{s,t} = \langle v_s | v_t \rangle \tag{22}$$

for any s, t of length $|s|, |t| = 0, 1, 2 \ldots$. One way to establish this fact is through a sequential Cholesky decomposition of the matrices Γ^∞_N [23].

We now take as our Hilbert space $\mathcal{H}$ the vector space spanned by the vectors $|v_s\rangle$ and define, for all $a \in \tilde{A}$, projectors $\hat{E}_a$ as follows

$$\hat{E}_a = \text{proj}\left(\text{span}\left\{|v_{as}\rangle : |as| = 1, 2, \ldots\right\}\right) \tag{23}$$

where $\text{proj}(V)$ is the projector on the subspace V. Since $(E_a S)^\dagger E_{a'} T = \delta_{a,a'} S^\dagger E_a T$ when $X(a) = X(a')$, it follows from (20) and (22) that $\langle v_{as}|v_{a't}\rangle = \delta_{a,a'}\langle v_s|v_{at}\rangle$, which in turn implies that

$$\hat{E}_a|v_{a's}\rangle = \delta_{aa'}|v_{as}\rangle, \quad \text{if } X(a) = X(a'). \tag{24}$$

An immediate consequence of this is that

$$\hat{E}_a\hat{E}_{a'} = \delta_{aa'}\hat{E}_a, \quad \text{if } X(a) = X(a'), \tag{25}$$

i.e. that the operators $\{\hat{E}_a : a \in \tilde{X}\}$ form an orthogonal set of projectors. They thus satisfy properties 1 and 2 of definition 2.

Let us now examine the action of $\hat{E}_a$ over an arbitrary vector $|v_s\rangle$. We find that

$$\begin{aligned}\hat{E}_a|v_s\rangle &= \hat{E}_a|v_{as}\rangle + \hat{E}_a\left(|v_s\rangle - |v_{as}\rangle\right)\\ &= |v_{as}\rangle + \hat{E}_a\left(|v_s\rangle - |v_{as}\rangle\right)\\ &= |v_{as}\rangle.\end{aligned} \tag{26}$$

The last identity follows from the fact that $\langle v_{at}|v_s\rangle - \langle v_{at}|v_{as}\rangle = 0$ which can be deduced from (20), (22), and the relation $(E_a T)^\dagger S - (E_a T)^\dagger E_a S = 0$. Property (26) implies in particular that

$$\hat{E}_a|v_1\rangle = |v_a\rangle. \tag{27}$$

By repeating the above construction, we can build operators $\{\hat{E}_b : b \in \tilde{B}\}$ for Bob that satisfy properties analogous to (25)–(27). From (26), (27) and the corresponding relations for Bob, we deduce by induction that

$$\hat{S}|v_1\rangle = |v_s\rangle \tag{28}$$

for any sequence $\hat{S}$ of length $|\hat{S}| = 0, 1, 2, \ldots$ of the projectors $\{\hat{E}_a : a \in \tilde{A}\}$ and $\{\hat{E}_b : b \in \tilde{B}\}$. Combining equations (22) and (28), we find that

$$\Gamma^\infty_{s,t} = \langle\phi|\hat{S}^\dagger\hat{T}|\phi\rangle, \tag{29}$$

where we have defined $|\phi\rangle = |v_1\rangle$. Note that $|\phi\rangle$ is a normalized vector since $\langle\phi|\phi\rangle = \Gamma^\infty_{1,1} = 1$. Equations (29) together with (19) imply that the state $|\phi\rangle$ and the operators $\hat{E}_a$ and $\hat{E}_b$ satisfy equations (2).

It now remains to verify property 3, i.e. that $[\hat{E}_a, \hat{E}_b] = 0$. From the relation $(E_a S)^\dagger E_b T - (E_b S)^\dagger E_a T = 0$, the properties (20) satisfied by Γ^∞ and (29), we deduce that

$$\langle\phi|\hat{S}^\dagger[\hat{E}_a, \hat{E}_b]\hat{T}|\phi\rangle = 0 \tag{30}$$

for any sequences $\hat{S}$, $\hat{T}$ of length $|\hat{S}|, |\hat{T}| = 0, 1, 2, \ldots$ As the vectors $\hat{S}|\phi\rangle$ and $\hat{T}|\phi\rangle$ span the support of the operators $\hat{E}_a$ and $\hat{E}_b$, equation (30) implies that the commutator $[\hat{E}_a, \hat{E}_b]$ is equal to zero. □

Corollary 9. *Q is a closed set.*

Proof. From theorem 8, we know that $Q = \bigcap_{i=1}^{\infty} Q^i$. As each of the sets Q^i is closed, its infinite intersection must be a closed set as well. □

4.2. Stopping criteria and extraction of quantum state and measurements

Our hierarchy of conditions characterizes the quantum set Q in an asymptotic limit. Testing only a finite number of our conditions may at most allow us to conclude that a given behavior *does not belong* to Q (more precisely, testing the conditions up to the nth step in the hierarchy allows us to detect all behaviors that do not belong to Q^n). We now show that in certain cases, it is possible to conclude at a finite order n in the hierarchy that a given behavior P *does belong* to Q. In this case, we can also recover from the certificate Γ^n the quantum state $|\psi\rangle$ and the measurements E_a and E_b reproducing the behavior P.

Let Γ^n be a certificate of order n associated to the behavior P. For any given pair of inputs X and Y, consider the set of indices $\mathcal{S}_{XY} = \{s : |s| \leqslant N-1\} \cup \{s = abs' : a \in \tilde{X}, b \in \tilde{Y}, |s| \leqslant N\}$, and define $\Gamma^n_{X,Y}$ as the submatrix of Γ^n with entries $\{\Gamma^n_{s,t} : s, t \in \mathcal{S}_{X,Y}\}$. If

$$\text{rank}(\Gamma^n_{X,Y}) = \text{rank}(\Gamma^n), \tag{31}$$

for all X, Y, then we will say that the certificate Γ^n has a *rank loop*.

Theorem 10. *A behavior P has a quantum representation of finite dimension d if and only if P admits, for some finite N, a certificate Γ^N of order N with a* rank *loop, and* $\text{rank}(\Gamma^N) \leqslant d$.

Here, by a representation of dimension d, we mean that there exist a quantum state $|\Psi\rangle \in \mathcal{H}$ and a set of operators $\{E_a, E_b \in B(\mathcal{H})\}$ satisfying the conditions of definition 2 for some Hilbert space $\mathcal{H}$ of finite dimension $\dim(\mathcal{H}) = d$. We denote by Q_d the set of all behaviors having a d-dimensional quantum representation.

Proof. We first prove that if P has a finite dimensional representation, there exists a certificate of order n with a rank loop. As $P \in Q_d$, there exist a state $|\phi\rangle \in \mathcal{H}$ and projective measurements $E_\mu \in B(\mathcal{H})$, as in definition 2, for some Hilbert space of $\dim(\mathcal{H}) = d$. The matrix Γ^n with entries $\Gamma^n_{s,t} = \langle\phi|S^\dagger T|\phi\rangle$ for all $S, T \in \mathcal{S}_n$ is clearly a certificate of order n associated to P. Because $\mathcal{S}_n \subseteq \mathcal{S}_{n+1}$, Γ^n is a submatrix of Γ^{n+1} for any n, and thus $\text{rank}(\Gamma^n) \leqslant \text{rank}(\Gamma^{n+1})$. On the other hand, the space generated by the vectors $S|\phi\rangle$, S being an arbitrary sequence, has a dimension less or equal than $\dim(\mathcal{H}) = d$ and therefore $\text{rank}(\Gamma^n) \leqslant d$ for all n. These two conditions imply that there exists an N such that $\text{rank}(\Gamma^N) = \text{rank}(\Gamma^{N+1}) \leq d$. It follows that $\text{rank}(\Gamma^{N+1}_{X,Y}) = \text{rank}(\Gamma^{N+1})$, for all X, Y, and thus that Γ^{N+1} has a rank loop[6].

Let us now prove the converse statement. Suppose thus that P admits a certificate Γ^N with a rank loop and satisfying $\text{rank}(\Gamma^N) = d$. Similarly to section 4.1, we can perform a Cholesky decomposition of Γ^N to write $\Gamma^N_{st} = \langle v_s|v_t\rangle$ for some finite set of vectors $\{|v_s\rangle : |s| \leqslant N\}$, whose span is a vector space of dimension at most d. Again as in section 4.1 we can then define a set of operators $\hat{A} = \{\hat{E}_a : a \in \tilde{A}\}$ as

$$\hat{E}_a = \text{proj}\left(\text{span}\{|v_{as}\rangle : |as| \leqslant N\}\right). \tag{32}$$

It is easy to see that these projector operators satisfy (25), and using the same arguments as in section 4.1, one can see that they also fulfill

$$\hat{E}_a|v_s\rangle = |v_{as}\rangle, \tag{33}$$

[6] What we have proven is that P has a, in general, *complex* rank looped certificate. To see that P also has a *real* rank looped certificate, note that, for any set n, $\text{Re}(\Gamma^n)$ is also a valid certificate for P. On the other hand, $\text{rank}(\text{Re}(\Gamma^n)) \leqslant 2 \cdot \dim(\mathcal{H})$, so the previous arguments can be applied to $\text{Re}(\Gamma^n)$.

for $|as| \leqslant N$. In an analogous way, we build operators $\hat{B} = \{\hat{E}_b \,:\, b \in \tilde{B}\}$ for Bob with the same properties. It is then immediate that $\langle v_1|\hat{S}^\dagger \hat{T}|v_1\rangle = \Gamma^N_{st}$, for sequences $|\hat{S}|, |\hat{T}| \leqslant N$. In particular, $\langle v_1|\hat{E}_a \hat{E}_b|v_1\rangle = P(a,b)$. The operators in $\hat{A}$ and $\hat{B}$ thus satisfy equation (2) and conditions 1 and 2 of definition 2. It remains to show that they also satisfy condition 3, i.e. commutativity.

Take any quadruple a, b, X, Y such that $a \in \tilde{X}$, $b \in \tilde{Y}$, and consider the set of indices $\mathcal{S}_{XY}$ defined above theorem 10. Then, for any pair of indices $s, t \in \mathcal{S}_{XY}$,

$$\langle v_s|\hat{E}_a \hat{E}_b - \hat{E}_b \hat{E}_a|v_t\rangle = \Gamma^N_{as,bt} - \Gamma^N_{bs,at} = 0\,. \tag{34}$$

The first equality in (34) follows from the fact that $|as|, |at|, |bs|, |bt| \leqslant N$. To see that $|as| \leqslant N$, for instance, note that from the definition of $\mathcal{S}_{XY}$, either $|s| \leqslant N-1$ (and then $|as| \leqslant N$), or $s = a'b's'$ with $a' \in \tilde{X}, b' \in \tilde{Y}$ and $|s| \leqslant N$ (and then since $a \in \tilde{X}$, $|as| = |aa'b's'| = |\delta_{a,a'}a'b's'| \leqslant N$). The second equality in (34) comes from the constraints imposed on the certificate Γ^N by the operator identity $S^\dagger E_a E_b T - S^\dagger E_b E_a T = 0$. On the other hand, condition (31) implies that

$$\mathrm{span}(\{|v_s\rangle \,:\, |s| \leqslant N\}) = \mathrm{span}(\{|v_s\rangle \,:\, S \in \mathcal{S}_{XY}\}). \tag{35}$$

Since the first set of vectors spans the support of the operators $\hat{E}_a$, $\hat{E}_b$, relation (34) implies that $\hat{E}_a$, $\hat{E}_b$ commute. As this holds for any quadruple a, b, X, Y, it follows that $P \in Q_d$. □

Corollary 11. *Let P be a behavior corresponding to a bipartite system where Alice's (Bob's) measurements have d_A (d_B) possible outcomes and such that each of the probabilities satisfies $P(a,b) > 0$. Let Γ^2 be a certificate of order 2 compatible with this behavior. Then,* $\mathrm{rank}(\Gamma^2) = d_A d_B$ *implies that $P \in Q_d$, with $d = d_A d_B$.*

Proof. If $P(a,b) > 0, \forall a \in A, \forall b \in B$, then, for any pair of measurements X, Y, the $d_A d_B$ vectors $\{|v_s\rangle : s = \mathbb{1}, E_a, E_b, E_a E_b : a \in \tilde{X}, b \in \tilde{Y}\}$ can be shown to be linearly independent. This, together with the fact that the rank of the whole matrix is equal to $d_A d_B$, implies that Γ^2 has a rank loop. □

The above theorem says that if our SDP outputs a certificate Γ with a rank loop, we know that P belongs to Q_d, with $d = \mathrm{rank}(\Gamma)$. Moreover, from the proof of theorem 10 it is not difficult to see that we can even reconstruct the state $|\psi\rangle$ and measurements E_a and E_b that yield this finite-dimensional representation.

Given a behavior P admitting a quantum representation of dimension d, there may be, however, different certificates of order n compatible with P, including some without rank loops. We have no guarantee that our SDP will output a certificate that has a rank loop, and thus in general we cannot guarantee that our hierarchy of SDP tests will stop after a finite number of iterations.

In view of this, it would be useful to incorporate some rank minimization techniques in the implementation of our hierarchy. That is, when checking the existence of certificates of order n, we would like as well to minimize the rank of the corresponding matrices. Indeed, let $\hat{\Gamma}^n$ be the certificate of order n for P with minimum rank, and consider the series $\hat{\Gamma}^1, \hat{\Gamma}^2, \hat{\Gamma}^3, \ldots$. If $\mathrm{rank}(\hat{\Gamma}^{n+1}) \neq \mathrm{rank}(\hat{\Gamma}^n)$, then $\mathrm{rank}(\hat{\Gamma}^{n+1}) \geqslant \mathrm{rank}(\hat{\Gamma}^n) + 1$. This, together with the fact that $\mathrm{rank}(\hat{\Gamma}^n) \leqslant d$ for all n, implies that there exists some $N \leqslant d$ such that $\mathrm{rank}(\hat{\Gamma}^{N+1}) = \mathrm{rank}(\hat{\Gamma}^N)$. On the other hand, for all X, Y

$$\mathrm{rank}(\hat{\Gamma}^N) \leqslant \mathrm{rank}(\hat{\Gamma}^{N+1}_{X,Y}) \leqslant \mathrm{rank}(\hat{\Gamma}^{N+1}), \tag{36}$$

and so $\mathrm{rank}(\hat{\Gamma}^{N+1}) = \mathrm{rank}(\hat{\Gamma}^{N+1}_{X,Y})$, i.e. $\hat{\Gamma}^{N+1}$ has a rank loop.

Unfortunately, there are no known efficient methods to solve rank minimization of positive semidefinite matrices with linear constraints. There are, however, heuristics [24] that typically arrive at the optimal solution in just a few iterations.

5. Applications

In this section, we present several applications of our method. We first derive simple analytic conditions that are satisfied by all quantum probabilities involving two measurements with two possible outcomes. We then show how to apply our method to establish upper bounds on the quantum violation of Bell inequalities.

From a general perspective, the hierarchy of necessary conditions that we have introduced represents a systematic way of getting better and better approximations to the set of quantum correlations. Moreover, these approximations are nicely characterized in terms of semidefinite constraints. Our method can thus be useful in any kind of optimization problem over this set. This is particularly true when we want to optimize the violation of Bell inequalities since they are linear functions of the behaviors and thus the entire optimization problem can be cast as a SDP.

Although the applications that we present here are restricted to a bipartite scenario, our method can also be applied to a multipartite scenario, e.g. see [25].

5.1. Analytic conditions for quantum behaviors with two inputs and two outputs

Consider the measurement scenario described in example 1 of section 3, involving two measurements with two possible outcomes for each observer. As we showed, a necessary condition for a behavior to be quantum in this scenario is the existence of a positive semidefinite matrix of the form (9). This condition corresponds to the first one in our hierarchy and thus characterize the set of behaviors Q^1. In the following, we provide an analytic characterization of this set. The conditions that we obtain can be interpreted as the quantum analogues of Bell inequalities.

We make use of the following two lemmas:

Lemma 12. (Schur's lemma) [23] *Let M be a matrix such that*

$$M = \begin{pmatrix} P & Q \\ Q^T & R \end{pmatrix} \succeq 0, \tag{37}$$

with $P \succ 0$. Then, $M \succeq 0$ if and only if $R - Q^T P^{-1} Q \succeq 0$.

Lemma 13. *Let $M_{z,t}$ be a real symmetric matrix of the form*

$$M_{z,t} = \begin{pmatrix} 1 & z & x_1 & x_2 \\ & 1 & x_3 & x_4 \\ & & 1 & t \\ & & & 1 \end{pmatrix}, \tag{38}$$

with $|x_i| \leqslant 1$, $i = 1, 2, 3, 4$. Let $f(x_1, x_2, x_3, x_4) = \arcsin(x_1) + \arcsin(x_2) + \arcsin(x_3) - \arcsin(x_4)$. Then, there exists a pair of values (z, t) such that $M_{z,t} \succeq 0$ if and only if

$$|f(x_1, x_2, x_3, x_4)| \leqslant \pi \tag{39}$$

for all possible permutations of x_1, x_2, x_3, x_4.

Proof. See appendix E. □

Now, apply Schur's lemma to matrix (9), taking the upper block to be $P = 1 \succ 0$. It then follows that the positivity of (9) is equivalent to the positivity of the matrix Γ given by

$$\Gamma' = \begin{pmatrix} 1-C_1^2 & u-C_1C_2 & C_{13}-C_1C_3 & C_{14}-C_1C_4 \\ & 1-C_2^2 & C_{23}-C_2C_3 & C_{24}-C_2C_4 \\ & & 1-C_3^2 & v-C_3C_4 \\ & & & 1-C_4^2. \end{pmatrix}. \tag{40}$$

Note that we can restrict our analysis to the case where all the elements in the diagonal are strictly positive. Indeed, if a diagonal element is equal to zero, the corresponding measurement, say by Alice, is deterministic, i.e. it always returns the same outcome. Then, Alice is left with one effective measurement (at most) and there always exists a classical, hence a quantum, model for this type of scenario. Suppose thus that all the diagonal elements of Γ' are different from zero. Multiplying Γ' on both sides by the diagonal matrix $M_{ii} = (1 - C_i^2)^{-1/2}$ $(i = 1, \ldots, 4)$, we obtain a matrix of the same form as the one of lemma 13. Applying this lemma, we conclude, together with the previous observation, that a necessary and sufficient condition for a behavior to belong to Q^1 is either that there exist an i such that $C_i^2 = 1$ or that

$$\left| \sum_{i,j} \arcsin\left(\frac{C_{ij} - C_iC_j}{\sqrt{(1-C_i^2)(1-C_j^2)}} \right) - 2\arcsin\left(\frac{C_{kl} - C_kC_l}{\sqrt{(1-C_k^2)(1-C_l^2)}} \right) \right| \leqslant \pi, \tag{41}$$

for all $k = 1, 2$ and $l = 3, 4$. This condition is of course only a necessary condition for quantum behaviors.

Note that a weaker necessary condition for a behavior to be quantum follows from the positivity of

$$\Gamma = \begin{pmatrix} 1 & u & C_{13} & C_{14} \\ & 1 & C_{23} & C_{24} \\ & & 1 & v \\ & & & 1 \end{pmatrix}, \tag{42}$$

which is simply a submatrix of (9). A direct application of lemma 13 implies that a behavior is quantum if $|\sum_{ij} \arcsin(C_{ij}) - 2\arcsin(C_{kl})| \leqslant \pi$ for all $k = 1, 2$, $l = 3, 4$. This condition, which, as we said, is weaker than (41), had previously been obtained in [9, 26, 27].

5.2. *Quantum violation of Bell inequalities*

Bell inequalities are constraints satisfied by all behaviors that originate from classical non-communicating observers. As mentioned in section 1, for a finite number of measurements and outcomes, the set of behaviors achievable using classically correlated instructions (shared randomness) defines a polytope, that is, a convex set with a finite number of extreme points (see also figure 2). It can then alternatively be completely characterized by a finite number of facets, which correspond to the well-known Bell inequalities [5]. A given behavior P thus admits a local classical model if and only if it satisfies all the Bell inequalities. In the space of behaviors, a Bell inequality can be viewed as a hyperplane that separates the space in two regions. A generic Bell inequality can thus be written as

$$I(P) = \sum_{a,b} c_{ab} P(a, b) \leqslant I_{\mathrm{C}}, \tag{43}$$

where c_{ab} are the real coefficients defining the inequality and I_C is the maximal value achievable by local classical points (and in particular which is attained by the extreme points lying on the facet defined by the Bell inequality).

Since the work of Bell [8], we know that some quantum behaviors are incompatible with a local classical description, that is, that they violate a Bell inequality. This fact is often referred to as quantum non-locality. In spite of many years of work on quantum non-locality, there are no methods able to provide the maximal quantum violation of a general Bell inequality, or just non-trivial upper bounds to it[7]. An important exception already mentioned in section 1 is the (tight) bound derived by Tsirelson on the maximal violation of the CHSH inequality.

Since our hierarchy of necessary conditions provides better and better approximations to the set of quantum correlations, it can be used to derive better and better upper bounds to the quantum violation of a Bell inequality. Actually, our proof of completeness guarantees the convergence to the maximal quantum value that we denote by I_Q. That is, by maximizing the value $I(P)$ of a Bell inequality over the behaviors $P(a,b) \in Q^n$ admitting a certificate of order n, one gets an upper bound I_n to I_Q. Clearly, we have that $I_1 \geqslant I_2 \cdots \geqslant I_n \geqslant \cdots \geqslant I_Q$ and $\lim_{n\to\infty} I_n \to I_Q$. Even while we are only able to prove convergence to the quantum value in the asymptotic limit, the quantum value or a very good upper-bound to it can often already be obtained for a small relaxation order n, as we show in the following.

The fact that Bell inequalities are linear functions of the joint probabilities $P(a,b)$ signifies that we can cast the computation of these upper bounds as SDP. Indeed, note that for any certificate Γ^n, we can write the value $I(P)$ of a Bell inequality as $I(P) = \mathrm{tr}(\beta_n \Gamma^n)$, where β_n is a matrix whose elements are all zero but the entries corresponding to $\Gamma^n_{a,b}$. For instance, in the case $n = 1$ one has (see (13)),

$$\beta_1 = \frac{1}{2}\begin{pmatrix} 0 & C \\ C^T & 0 \end{pmatrix}, \tag{44}$$

where C is the matrix whose elements are the coefficients c_{ab} in (43) defining the Bell inequality. Therefore the calculation of I_n amounts to solve the following SDP

$$\begin{aligned} &\text{maximize} && \mathrm{tr}(\beta_n \Gamma^n) \\ &\text{subject to} && \mathrm{tr}\left(F_k^T \Gamma^n\right) = g_k(P), \quad k = 1, \ldots, m \\ &&& \Gamma^n \succeq 0. \end{aligned} \tag{45}$$

In the remainder of this subsection, we illustrate this approach by applying it to several Bell inequalities.

But before presenting these results, let us make two technical remarks. First, note that in the above optimization problems, we can in general consider certificates that are intermediate between, say, a certificate of order 1 and a certificate of order 2. Such a certificate would be associated to a set of sequences of operators $\mathcal{S}$ satisfying $\mathcal{S}_1 \subset \mathcal{S} \subset \mathcal{S}_2$. For instance, we could consider the set $\mathcal{S}_{1+AB} = \mathcal{S}_1 \cup \{E_a E_b, :\ a \in \tilde{A}, b \in \tilde{B}\}$ consisting of $\mathcal{S}_1$ together with all products of one operator of Alice and one for Bob (while $\mathcal{S}_2$ also contains product of two operators of Alice and product of two operators of Bob). The corresponding bound I_{1+AB} would then satisfy $I_1 \leqslant I_{1+AB} \leqslant I_2$. In some cases this bound might already be useful while requiring less computational resources than I_2. In the following, we will therefore also consider such bounds

[7] Lower bounds to the maximal quantum violation can easily be obtained by searching specific states and measurements that violate the inequality.

Table 1. Upper bounds on the violation of the CGLMP inequality derived from our construction. The local bound is equal to 2. The upper bound I_{1+AB} is already equal, up to numerical precision, to the lower bounds given in [29]. We also provide the size of the certificates in each case. Note that the rank loop conditions defined in section 4.2 are not applicable to certificates of order 1.

	I_1			I_{1+AB}		
d	Value	Matrix size	Rank loop	Value	Matrix size	Rank loop
2	2.8284	5	N/A	2.8284	9	Yes
3	3.1547	9	N/A	2.9149	25	Yes
4	3.2126	13	N/A	2.9727	49	Yes
5	3.2997	17	N/A	3.0157	81	Yes
6	3.3378	21	N/A	3.0497	121	Yes
7	3.3843	25	N/A	3.0776	169	Yes
8	3.4115	29	N/A	3.1013	225	Yes

based on intermediate certificates. The notation that we use is obvious, for instance $I_{1+AB+AA'B}$ is the bound associated with the set of sequence operators $\mathcal{S}_{1+AB+AA'B} = \mathcal{S}_1 \cup \{E_a E_b\} \cup \{E_a E'_a E_b\}$. Note that the rank loop conditions derived in section 4.2 generalize to the case of intermediate certificates, see appendix C.

The second technical remark is that, as shown in appendix D, the probabilities $P(a, b) = \Gamma^n_{a,b}$ corresponding to a certificate Γ^n are guaranteed to be positive only for certificates of order $n \geqslant 2$ (or more generally for certificates associated with set of operators $\mathcal{S} \supseteq \mathcal{S}_{1+AB}$). Thus, when we maximize, as in (45), a Bell inequality over all behaviors for which there exists a certificate Γ^1 of order 1, it may so happen that the bound I_1 that we obtain correspond to a solution with negative probabilities. By explicitly adding to the SDP (45), the constraints $\Gamma^1_{a,b} \geqslant 0$ that probabilities must be positive[8], we thus strengthen the upper bound I_1. In the remainder of this section, when we mention an upper bound obtained from a certificate of order 1, we always refer to this strengthened version.

We start by analyzing the Collins–Gisin–Linden–Massar–Popescu (CGLMP) family of Bell inequalities introduced in [28]. These inequalities are defined in a bipartite scenario where the two observers can each make two measurements of d outcomes. We refer the reader to the original reference for the detailed description of these inequalities. The inequality corresponding to the case $d = 2$ is the CHSH inequality. The best-known lower bounds on the quantum violation of these inequalities for $d \leqslant 8$ are those given in [29]. The upper-bounds that we obtained using our method are given in table 1. Note first that in the case $d = 2$ (CHSH) the first certificate already provides the actual quantum value, which is equal to the Tsirelson bound. For d larger than 2, the quantum value is recovered at the successive step corresponding to the certificate Γ^{1+AB}. This can be seen by noting that the upper-bounds I_{1+AB} are equal to the lower bounds given in [29]. Alternatively, one reaches the same conclusion by noting that the stopping criteria based on rank loops presented in section 4.2 are satisfied. Thus, Γ^{1+AB}, and therefore Γ^2, is already enough to get the maximal quantum violation of CGLMP inequalities (at least until $d = 8$) and certificates Γ^n with $n > 2$ are redundant.

[8] Adding such constraints leaves the optimization problem in a SDP form.

Table 2. Upper bounds derived from our construction on the violation of the inequality introduced in [30, 31]. The local bound is equal to 0. The upper bound $I_{1+AB+AA'B}$ is already equal, up to numerical precision, to the lower bound obtained numerically for qutrits. We also provide the size of the certificates in each case.

Upper bound	Value	Matrix size	Rank loop
I_1	0.3333	7	N/A
I_{1+AB}	0.2653	16	No
$I_{1+AB+AA'B}$	0.2532	22	Yes

We have also considered other, perhaps less standard, Bell inequalities, like the one presented in [30] (see also [31]) for the case in which Alice performs two measurements, one of two outcomes and one of three outcomes, while Bob performs three two-outcome measurements. The results are summarized in table 2. One can also get numerical lower bounds for the maximal quantum violation for fixed dimension. In the case of qutrits, the derived quantum violation is equal to 0.2532 [30, 31]. This is precisely the same value obtained when checking the last certificate of table 2. This certificate then, or equivalently Γ^3, already provides a tight bound on the maximal quantum violation. The same conclusion follows again by studying the rank of the matrices appearing in these certificates.

Finally, we also applied our techniques to the Froissard inequality, also referred to as I_{3322} inequality, given in [32, 33]. Again, we refer the interested reader to these references for the explicit form of the inequality. The best-known quantum violation of this inequality is equal to 0.25 in the case of qubit systems, while the classical value is equal to zero. By applying our hierarchy of conditions to this inequality, one gets the upper bounds given in table 3. Note that the values derived for Γ^2 and Γ^3 are quite close and that no rank loop is observed[9]. It is remarkable that none of our upper bounds coincides with the best-known lower bounds on the quantum violation, although they are very close to it. This may be because in the case of this inequality our hierarchy approaches more slowly the quantum solution, assuming it to be equal to 0.25. However, one cannot exclude that the maximal quantum violation of this inequality is obtained for systems of dimension larger than two. Indeed, the existence of this type of inequalities has recently been proven in [31, 34, 35]. Thus, a quantum violation close to 0.2509 is perhaps attainable beyond qubits.

6. Discussion and open questions

Characterizing the correlations attainable by quantum means is a fundamental problem in QIS and, more generally, in quantum mechanics. To our knowledge, our construction represents the only available tool to tackle this problem with full generality: it applies to any number of parties, measurements and outcomes. Moreover, the first steps in our hierarchy are easily computable since they correspond to SDPs of reasonable size. Our construction provides a systematic way of getting better and better approximations to the set of quantum correlations and can be applied, for instance, to identify correlations that do not admit a quantum representation, or to estimate the maximum quantum violation of Bell inequalities.

[9] Rank loops should be considered in a cautious way. Indeed it is sometimes difficult to numerically distinguish a zero from a small eigenvalue.

Table 3. Upper bounds on the violation of the I_{3322} inequality derived from our construction. The local bound is equal to 0. Interestingly, none of our tests coincides with the best-known lower bound on the quantum violation, obtained for qubit systems. We also provide the size of the certificates in each case.

Upper bounds	Value	Matrix size	Rank loop
I_1	0.3333	7	N/A
I_{1+AB}	0.2515	16	No
I_2	0.25091	28	No
I_3	0.25089	88	No

In this work, after having presented in detail the hierarchy of necessary conditions already introduced in [18], we have (i) proved the completeness of the hierarchy, (ii) introduced a criterion based on rank loops that can guarantee at a finite order in the hierarchy that a set of joint probabilities is quantum, and we have shown in this case how to reconstruct the quantum state and measurements reproducing these probabilities, (iii) presented several examples illustrating the usefulness of the method. Although our results are described in the bipartite case, they can easily be extended to the multipartite scenario. To conclude this work, we would like to go back to the commutation versus tensor product issue briefly mentioned in section 2.2, discuss the computational complexity of our approach, and then present several open questions related to the set of quantum correlations achievable with finite dimensional Hilbert spaces.

We mention that it is possible to generalize the hierarchy presented in this work and our proof of convergence to other polynomial optimization problems with non-commutative variables [36]. A similar generalization was also recently introduced in [37] to put upper-bounds on the entangled value of quantum multi-player games. We also mention that an alternative proof of convergence of our hierarchy is possible using a result of Helton and McCullough [38], as noted in [37, 39].

6.1. Commutation versus tensor product

There are two possible ways to impose that Alice and Bob perform measurements on separated systems: through the condition that their measurement operators commute, or through a tensor product splitting of the whole Hilbert space. The two sets of quantum correlations Q and Q' associated with each possibility are defined in section 2.2. Clearly, measurements that have a product form commute with each other, and thus $Q' \subseteq Q$. In the special case of finite-dimensional systems, one can in fact show that both definitions are equivalent, i.e. $Q = Q'$ [21, 40] (see also [41]). For infinite-dimensional systems whether they are equivalent or not is, at the moment of writing, an open question [21]. It is not even known if Q' is dense in Q. (Note that the statement in [9] that the two sets are equivalent is actually unproven [40].)

One can debate which definition should be regarded as the proper one. Arguments in favor of the tensor product structure are presented in [21]. Here, we have chosen commutativity as this choice is consistent with the ethos adopted in this work. Indeed, our main objective is to characterize the set of correlations compatible with the general structure of quantum theory, but imposing as few additional constraints as possible: we impose no restrictions on states, measurements, or even on the Hilbert space dimension. In this spirit, it should then be pointed out that there exist in quantum field theories algebras of local (in the sense of commuting) observables that cannot be split in a tensor product structure[10], yet in which it is possible to investigate the correlations that can arise between two separated observers, and in particular to study the amount by which Bell inequalities are violated [42]. By investigating the structure of the set Q defined through commutativity, we are sure to include also these examples and thus to deal with the most general correlations compatible with the quantum theory.

Of course, making the above distinction is only meaningful if Q and Q' happen to be distinct. But note that actually most of the results of this work are independent of the definition chosen. As $Q' \subseteq Q$, all the necessary conditions satisfied by points in Q, in particular all the ones constituting the hierarchy, are also valid for Q'. The stopping criteria presented in section 4.2 are associated with correlations achievable with finite-dimensional spaces, for which we know that $Q = Q'$, and thus also apply to both cases. The unique distinction arises when we consider the asymptotic behavior of our hierarchy: as our proof of convergence to Q explicitly use infinite-dimensional systems, the hierarchy will also converge to Q' only if $Q = Q'$ in the most general setting. But for all practical applications of our method where only a finite number of steps of the hierarchy are involved, in particular for all numerical applications, one choice of definition or the other does not make any difference. For instance, all the results presented in section 5 apply equally well to both cases.

Note that it is not surprising that the limit of the hierarchy tends to Q rather than Q', as the space separation between Alice and Bob's measurements appears in the hierarchy only in the form of constraints associated to the commutativity of these local observables. For example, since $E_a E_b E_{a'} = E_a E_{a'} E_b$, we impose that $\Gamma^n_{aba'} = \Gamma^n_{aa'b}$ for all n. If we insist that the hierarchy should tend to Q' rather than Q, it will probably be necessary to add new constraints associated to the tensor product structure. These constraints will have to reflect the (at the moment unproven) differences, at the level of operator algebra, between the commutation and tensor product case.

6.2. Complexity of the hierarchy

The computational complexity of our tests scales badly with the order n of the relaxation. For instance, in a measurement scenario with s inputs and d outputs, it is not difficult to see that the size of a certificate of order n is roughly $(ds)^n$. The algorithms used to solve the SDPs associated with such certificates have a running time that is polynomial in the size of the matrix defining the SDP. Thus, using SDP to decide if a certificate of order n exists requires a time exponential in n.

Note, however, that the numerical results presented in section 5.2 suggest that it might be sufficient, at least for some families of measurement scenarios, to consider relaxations only up to a bounded value n to characterize, or obtain an already good approximation, of the quantum set. Indeed, in the examples that we considered, when maximizing the violation of Bell inequalities we hit the quantum value, or obtained a very good upper-bound on it, already at the second or third step in the hierarchy. The suggestion that a finite number of steps of

[10] This result does not directly imply that $Q \neq Q'$ since it could happen that all the correlations obtained by performing commuting measurements on states belonging to these spaces can also be realized in spaces with a tensor product structure.

the hierarchy might already characterize, or approximate well, the quantum region turns out to be true in some particular case. For instance, for measurement scenarios with two outputs, a result of Tsirelson [11] implies that deciding if a set of correlators (i.e. a quantity such as the C_{ij} defined in example 1 of section 3) is quantum can exactly be decided through SDP, as noted by Wehner [14]. The SDP considered by Wehner is a weaker version of the first step of our hierarchy. In [43], the authors show how for a certain family of measurement scenarios, corresponding to *unique games*, the quantum set can be well approximated through SDP. The SDPs considered in [43] correspond again to the first step of our hierarchy[11].

If all these results suggest that our construction might indeed provide an efficient characterization of the quantum set for some particular quantum scenarios, we do not expect this to be true in full generality, as it has recently been shown, at least in the tripartite case, that calculating the maximal quantum violation of a Bell inequality is an NP-hard problem [44].

6.3. Finite dimensional quantum systems

In this work, we were mainly interested in characterizing the set of quantum behaviors without any bound on the dimension of the Hilbert space. We now present several open questions linked to the finite-dimensional case.

- Consider all possible quantum behaviors of d outcomes where the number of measurements is arbitrary. Gill recently asked whether these correlations are attainable by measuring d-dimensional quantum systems[12]. The answer to this question is no, as shown in [34] for the case of three observers and in [31, 35] for bipartite systems. Actually, no finite dimension is sufficient to generate the whole set of quantum correlations of d outcomes for three parties, while the same result seems very plausible in the bipartite case [31, 35]. Consider however a scenario where the number of measurements is also finite. Are now all quantum correlations (exactly) attainable by measuring a finite dimensional quantum system?
- Consider a measurement scenario with a finite number of inputs and outputs. It is easy to see that in the tensor product scenario discussed in section 6.1, a quantum behavior can be approximated arbitrarily well using finite-dimensional Hilbert spaces (see for instance [37]). Does the same result hold in the commutative case? If yes, then combining this result with the fact that $Q' = Q$ for finite-dimensional systems, would imply that Q' is dense in Q, and thus that our hierarchy converges to the quantum set Q' defined through the tensor product structure.
- What is the structure of the set of quantum behaviors corresponding to a Hilbert space of fixed dimension d? Very little is known in this case, we even do not known if the corresponding quantum set is convex.
- In relation with the above question, it would be interesting to understand how to incorporate in our hierarchy a bound on the Hilbert space dimension. It is in principle always possible to decide if a behavior can be represented with a Hilbert space of given dimension through SDP [31] using known techniques of polynomial optimization [45, 46]. The corresponding SDPs, however, are very demanding from a computational point of view, much more

[11] With the additional constraint, when maximizing the violation of Bell inequality, that the probabilities must be positive, as mentioned in section 5.2.
[12] See the open problem 26.a at http://www.imaph.tu-bs.de/qi/problems/problems.html.

than the one obtained from our construction where we do not bound the dimension. Can one modify our construction to design more efficient methods to approximate the set of correlations corresponding to d-dimensional quantum systems?

As suggested by the results of section 4.2, a possibility would be to incorporate a bound on the rank of our certificates. There are, however, to our knowledge no efficient methods to solve SDPs with rank constraints. Is there any efficient way to relax these rank constraints to obtain good approximations to the set of quantum correlations with finite dimension?

Acknowledgments

We thank B Tsirelson and R Werner for useful discussions and correspondence on the commutation versus tensor product question, and T Ito and B Toner for pointing out to us the possibility of an alternate proof of convergence of our hierarchy through the results of Helton and McCullough. We acknowledge financial support from the EU project QAP (IST-FET FP6-015848), from the Spanish MEC, under FIS2004-05639, Consolider-Ingenio QOIT projects, and a 'Juan de la Cierva' grant, and from the Generalitat de Catalunya.

Appendix A. Basics of SDP

SDP [15] is a subfield of convex optimization concerned with the following optimization problem, known as the *primal problem*

$$\begin{aligned} &\text{maximize} && \mathrm{tr}(GZ), \\ &\text{subject to} && \mathrm{tr} F_i Z = c_i, \quad i = 1, \ldots, p, \\ &&& Z \succeq 0. \end{aligned} \tag{A.1}$$

The problem variable is the $n \times n$ matrix Z and the problem parameters are the $n \times n$ matrices G, F_i and the scalars c_i. A matrix Z is said to be *primal feasible* if it satisfies the conditions expressed in (A.1).

For each primal problem there is an associated *dual problem*, which is a minimization problem of the form

$$\begin{aligned} &\text{minimize,} && c^T x, \\ &\text{subject to} && F(x) = \sum_{i=1}^{p} x_i F_i - G \succeq 0, \end{aligned} \tag{A.2}$$

where the variable is the vector x with p components x_i. The dual problem is also a SDP, i.e. it can be put in the same form as (A.1). A vector x is said to be *dual feasible* when $F(x) \geqslant 0$.

The key property of the dual program is that it yields bounds on the optimal value of the primal program. To see this, take a dual feasible point x and a primal feasible point Z. Then $c^T x - \mathrm{tr}(GZ) = \sum_{i=1}^{p} \mathrm{tr}(ZF_i)x_i - \mathrm{tr}(GZ) = \mathrm{tr}(ZF(x)) \geqslant 0$. This proves that the optimal primal value p^* and the optimal dual value d^* satisfy $d^* \leqslant p^*$. In fact, it usually happens that $d^* = p^*$. A sufficient condition for this to hold is that there exists a strict feasible point of the primal problem [15], that is, that there exists a matrix $Z \succ 0$ that is primal feasible. Such a situation appears in the SDP problem (17), as for any matrix Γ satisfying the corresponding linear constraints, we can always take λ small enough so that $\Gamma - \lambda \mathbb{1} \succ 0$.

There exist many available numerical packages to solve SDPs, for instance for Matlab, the toolboxes SeDuMi [47] and YALMIP [48]. Such algorithms usually solve both the primal and the dual at the same time and thus yield bounds on the accuracy of the obtained solution.

Appendix B. Certificates have bounded entries

Proposition 21. *Let Γ^n be a certificate of order n for a behavior P. Then, $|\Gamma^n_{st}| \leqslant 1$, for all sequences S, T. That is, the set of all certificates of order n for P is bounded.*

Proof. Because $\Gamma^n \succeq 0$, it just suffices to prove that all diagonal elements are smaller or equal than 1. Consider thus any 2×2 submatrix of Γ^n:

$$\begin{pmatrix} \Gamma^n_{ss} & \Gamma^n_{st} \\ \Gamma^n_{ts} & \Gamma^n_{tt} \end{pmatrix}. \tag{B.1}$$

This submatrix must be positive semidefinite or, equivalently, its coefficients have to satisfy $\Gamma^n_{ss}, \Gamma^n_{tt} \geqslant 0$ and $\Gamma^n_{ss} \cdot \Gamma^n_{tt} \geqslant \Gamma^n_{st} \cdot \Gamma^n_{ts}$. Now, take $T = E_a S$. From the operator relation $S^\dagger T = T^\dagger S = T^\dagger T$, it follows that $\Gamma^n_{st} = \Gamma^n_{ts} = \Gamma^n_{tt}$. This, together with the positivity conditions, implies that

$$\Gamma^n_{tt} \leqslant \Gamma^n_{ss}, \quad \text{for } T = E_a S, \quad \forall |S| \leqslant n, \quad a \in \tilde{A}. \tag{B.2}$$

In particular,

$$\Gamma^n_{aa} \leqslant \Gamma^n_{11} = 1, \quad \text{for all } a. \tag{B.3}$$

And, obviously, the same relations hold replacing as by bs. By induction, it is straightforward that $\Gamma^n_{ss} \leqslant 1, \forall S$, and, therefore, $|\Gamma^n_{st}| \leqslant 1, \forall S, T$. □

Appendix C. Rank loop conditions for intermediate certificates

We state here some results about rank loop conditions similar to the ones introduced in section 4.2 and which hold for 'intermediate certificates' such as those that we used in section 5.2 to maximize the violation of Bell inequalities.

Let us first define more precisely the certificates that we are considering here. Given a pair of measurements X, Y, denote by $\mathcal{S}_{n+XY}$ the set of sequences $\mathcal{S}_n \cup \{S \in \mathcal{S}_{n+1} : S = E_a E_b S', a \in \tilde{X}, b \in \tilde{Y}\}$, i.e. $\mathcal{S}_{n+XY}$ is the set that contains all sequences of length n together with all the sequences of length $n+1$ that are of the form $E_a E_b S'$ for some $a \in \tilde{X}, b \in \tilde{Y}$. It is thus intermediate between the set of sequences of length n and $n+1$, as $\mathcal{S}_n \subseteq \mathcal{S}_{n+XY} \subseteq \mathcal{S}_{n+1}$. Given a vector n of positive integers n_{XY}, define $\mathcal{S}_{n+AB}$ as the union of all sets $\mathcal{S}_{n_{xy}+XY}$. By abuse of notation, when n is an integer we interpret it as the vector $(n, n, \ldots, n)$. With the notation that we have just defined, we have for instance that $\mathcal{S}_{1+AB} = \{\mathbb{1}, E_a, E_b, E_a E_b : a, b \in \tilde{A}, \tilde{B}\}$, which is one of the set of sequences that we used in the numerical applications presented in section 5.2.

Given an arbitrary certificate Γ associated to a set of operators $\mathcal{S}$ and a vector n of positive integers such that $\mathcal{S}_{n+XY} \subseteq \mathcal{S}$, denote by Γ_{n+XY} the submatrix of Γ corresponding to the set of sequences $\mathcal{S}_{n+XY}$. Define similarly Γ_{n+AB}. If there exists a vector N such that

$$\operatorname{rank}(\Gamma_{N_{\mathrm{xy}}+XY}) = \operatorname{rank}(\Gamma_{N+AB}), \tag{C.1}$$

for all X, Y, then we will say that the certificate Γ has a rank loop. (Note that this definition is weaker than the one given in section 4.2.)

Theorem 15. *A behavior P has a quantum representation of finite dimension d if and only if P admits, for some N, a certificate Γ with a* rank *loop, and* $\mathrm{rank}(\Gamma_{N+AB}) \leqslant d$.

Corollary 16. *Let P be a behavior corresponding to a bipartite system where Alice's (Bob's) measurements have d_A (d_B) possible outcomes and such that each of the probabilities satisfies $P(a, b) > 0$, for all $a \in A, b \in B$. Let Γ be a certificate compatible with this behavior associated to the set of operators $\mathcal{S}$, with $\mathcal{S}_{1+AB} \subseteq \mathcal{S}$. Then,* $\mathrm{rank}(\Gamma) = d_A d_B$ *implies that P has a quantum representation of dimension $d_A d_B$.*

The proofs of theorem 15 and corollary 16 follow along the same lines as the proofs of theorem 10 and corollary 11.

Appendix D. Certificates and non-negativity of probabilities

Let $\mathcal{S}_{1+AB} = \{\mathbb{1}, E_a, E_b, E_a E_b : a, b \in \tilde{A}, \tilde{B}\}$ be the set of all sequences of length less than 1, together with all product operators consisting of one operator of Alice and one of Bob. The proposition here below states that the existence of a certificate Γ corresponding to a set of operators that contains $\mathcal{S}_{1+AB}$ as a subset, thus in particular the existence of a certificate of order n with $n \geqslant 2$, implies that the elements $P(a, b)$ of the behavior associated to Γ are proper probabilities, i.e. they are non-negative numbers.

Before showing this, however, let us remind some notation introduced in section 2.2. We defined a behavior as a set of joint probabilities $P = \{P(a, b) : a \in A, b \in B\}$ and implicitly assumed that they satisfy the no-signaling constraints $P(a) = \sum_{b \in Y} P(a, b)$ and $P(b) = \sum_{a \in X} P(a, b)$. To remove the redundancy associated with these constraints, we introduced the reduced outcome sets $\tilde{A}$ and $\tilde{B}$ so that P can be alternatively represented as $P = \{P(a), P(b), P(a, b) : a \in \tilde{A}, b \in \tilde{B}\}$. Having reminded this definition, it is now easy to see that the sets of operators $\mathcal{S}_{1+AB} = \{\mathbb{1}, E_a, E_b, E_a E_b : a, b \in \tilde{A}, \tilde{B}\}$ and $\mathcal{S}_{AB} = \{E_a E_b : a \in A, b \in B\}$ are linearly equivalent.

Proposition 17. *Consider a measurement scenario $(A, B, \mathcal{X}, \mathcal{Y})$, and let $P = \{P(a, b) : a \in A, b \in B\}$ be a set of real numbers. If there exists a certificate Γ for P corresponding to a set $\mathcal{S}$ such that $\mathcal{S}_{1+AB} \subseteq \mathcal{S}$, then the numbers $P(a, b)$ represent proper probabilities, i.e., $P(a, b) \geqslant 0$, for all a and b.*

Proof. Let P admit a certificate as in proposition 17. Then, according to lemma 7, P also admits a certificate associated to the set $\mathcal{S}_{1+AB}$, and thus also a certificate Γ' associated to the set $S_{AB} = \{E_a E_b : a \in A, b \in B\}$. Since $\Gamma' \succeq 0$, its diagonal elements $\Gamma'_{ab,ab} = P(a, b)$ must be non-negative. □

Appendix E. Proof of lemma 13

Proof. Suppose that there exists a pair of values (z, t), with $|t| < 1$, such that

$$M_{z,t} = \begin{pmatrix} P & Q \\ Q^T & R \end{pmatrix} \succeq 0, \tag{E.1}$$

with $P = \begin{pmatrix} 1 & z \\ z & 1 \end{pmatrix}$, $Q = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$, $R = \begin{pmatrix} 1 & t \\ t & 1 \end{pmatrix}$. Because $|t| < 1$ implies $R \succ 0$, lemma 12 in section 5 states that the positivity of $M_{z,t}$ is equivalent to the condition $D \equiv P - Q^T Q^{-1} Q \succeq 0$.

Now, D is a 2×2 matrix with non diagonal free entries and so its positive semidefiniteness is equivalent to demanding that $D_{11}, D_{22} \geqslant 0$. Therefore, we can get rid of the variable z. Taking into account that $t^2 - 1 < 0$, we have that both conditions are equivalent to

$$\alpha_1 \leqslant y \leqslant \alpha_2, \quad \beta_1 \leqslant y \leqslant \beta_2, \tag{E.2}$$

for $\alpha_{1,2} = x_1 x_2 \mp \sqrt{x_1^2 x_2^2 - x_2^2 - x_1^2 + 1}$ and $\beta_{1,2} = x_3 x_4 \mp \sqrt{x_3^2 x_4^2 - x_3^2 - x_4^2 + 1}$.

It can be verified that $|\alpha_{1,2}|, |\beta_{1,2}| \leqslant 1$. A solution $\max(\alpha_1, \beta_1) \leqslant t \leqslant \min(\alpha_2, \beta_2)$ can be found if and only if

$$\alpha_1 \leqslant \beta_2, \quad \beta_1 \leqslant \alpha_2, \tag{E.3}$$

and the requirement that $|t| < 1$ translates into $\max(\alpha_1, \beta_1), \min(\alpha_2, \beta_2)$ are not both equal to ± 1.

Now, it can be proved that condition (E.3) holds for *any* matrix $M_{z,t}$ for which there exists a pair of values z, t that makes it positive semidefinite. To see this, notice that, for $M_{z,t}$ to be positive semidefinite it is necessary that $|t| \leqslant 1$. So, if such a couple of values exist, for any $\epsilon > 0$ the matrix $\frac{1}{\sqrt{1+\epsilon}}(M_{z,t} + \epsilon \mathbb{1})\frac{1}{\sqrt{1+\epsilon}}$ is of the form (38) and there exists a pair of values $(z' = z'/(1+\epsilon), t' = t/(1+\epsilon))$, with $|t'| < 1$ that make it positive semidefinite. Therefore, the vector $(x_i/(1+\epsilon)$ has to satisfy (E.3). Because this holds for any $\epsilon > 0$, by continuity, also the vector (x_i) will satisfy (E.3).

Next we will prove that any vector satisfying (E.3) corresponds to a matrix of the type M for which there exists a couple of values (z, t) that make it positive semidefinite. Suppose, thus, that (E.3) holds. Two situations can arise: either $\max(\alpha_1, \beta_1) = \min(\alpha_2, \beta_2) = \pm 1$ or not. In the second case, we know that we can find a pair of values (z, t) such that $M_{z,t} \succeq 0$, whereas in the first case it can be shown that $x_1 = x_2 = x$; $x_3 = x_4 = x'$. But a positive semidefinite M matrix for this case is given by the formula $M = D \cdot (M^* + \mathrm{diag}(\frac{1}{x^2} - 1, (\frac{1}{x'})^2 - 1, 0, 0)) \cdot D$, where $D = \mathrm{diag}(x, x', 1, 1)$ and $M^* \succeq 0$ is a 4×4 matrix whose entries are all ones. Therefore, condition (E.3) is necessary and sufficient to guarantee the existence of a pair of values (z, t) such that $M_{z,t} \succeq 0$. Making the change of variables $x_i \to \sin(\phi_i)$ in (E.3) leaves us with (36). □

References

[1] Nielsen M and Chuang I 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)

[2] Lo H-K and Chau H F 1997 *Phys. Rev. Lett.* **78** 3410
Mayers D 1997 *Phys. Rev. Lett.* **78** 3414

[3] Brassard G 2001 *Preprint* quant-ph/0101005

[4] Acin A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501

[5] Werner R F and Wolf M M 2001 *Quantum Inform. Comput.* **1** 1

[6] Kaszlikowski D, Gnaciński P, Zukowski M, Miklaszewski W and Zeilinger A 2000 *Phys. Rev. Lett.* **85** 4418

[7] Massar S, Pironio S, Roland J and Gisin B 2002 *Phys. Rev.* A **66** 052112

[8] Bell J S 1964 *Physics* **1** 195

[9] Tsirelson B 1993 *Had. J. Suppl.* **8** 329

[10] Barrett J, Linden N, Massar S, Pironio S, Popescu S and Roberts D 2005 *Phys. Rev.* A **71** 022101

[11] Cirelson B S 1980 *Lett. Math. Phys.* **4** 83

[12] Clauser J F, Horne M A, Shimony A and Holt R A 1969 *Phys. Rev. Lett.* **23** 880

[13] Masanes L 2005 *Preprint* quant-ph/0512100v1
Cabello A 2004 *Phys. Rev. Lett.* **92** 060403
Filipp S and Svozil K 2004 *Phys. Rev. Lett.* **93** 130407
Burhman H and Massar S 2004 *Preprint* quant-ph/0409066
[14] Wehner S 2005 *Preprint* quant-ph/0510076
[15] Vandenberghe L and Boyd S 1996 *SIAM Rev.* **38** 49
[16] Avis D, Imai H and Ito T 2006 *Preprint* quant-ph/0605148
[17] Liang Y C and Doherty A C 2006 *Preprint* quant-ph/0608128
[18] Navascués M, Pironio S and Acín A 2007 *Phys. Rev. Lett.* **98** 010401
[19] Doherty A C, Parrilo P A and Spedalieri F M 2004 *Phys. Rev.* A **69** 022308
[20] Eisert J, Hyllus P, Guehne O and Curty M 2004 *Phys. Rev.* A **70** 062317
[21] See the open problem 33 at http://www.imaph.tu-bs.de/qi/problems/problems.html.
[22] Reed M and Simon B 1980 *Functional Analysis* (New York: Academic)
[23] Horn R A and Johnson C 1999 *Matrix Analysis* (Cambridge: Cambridge University Press)
[24] Fazel M 2002 *PhD Thesis* Stanford University
[25] Toner B and Verstraete F 2006 *Preprint* quant-ph/0611001
[26] Landau L J 1988 *Found. Phys.* **18** 449
[27] Masanes L 2005 *Preprint* quant-ph/0512100v1
[28] Collins D, Gisin N, Linden N, Massar S and Popescu S 2002 *Phys. Rev. Lett.* **88** 040404
[29] Acín A, Durt T, Gisin N and Latorre J I 2002 *Phys. Rev.* A **65** 052325
[30] Pironio S All CHSH polytopes, in preparation
[31] Brunner N, Pironio S, Acín A, Gisin N, Methot A A and Scarani V 2008 *Phys. Rev. Lett.* **100** 210503
[32] Froissard M 1981 *Nuovo Cimento* B **64** 241
[33] Collins D and Gisin N 2004 *J. Phys. A: Math. Gen.* **37** 1175
[34] Perez-Garcia D, Wolf M M, Palazuelos C, Villanueva I and Junge M 2007 *Preprint* quant-ph/0702189v2
[35] Vertesi T and Pal K F 2007 *Preprint* 0712.4225
[36] Navascues M, Pironio S and Acin A Convergent relaxations for polynomial optimization with non-commutative variables, in preparation
[37] Ito T, Kobayashi H and Matsumoto K Quantum multi-prover interactive proofs and decidability, in preparation
[38] Helton J W and McCullough S A 2004 *Trans. Am. Math. Soc.* **356** 3721
[39] Doherty A C, Liang Y, Toner B and Wehner S in preparation
[40] Tsirelson B 2007 private communication
[41] Murray F J and von Neumann J 1936 *Ann. Math.* **37** 116
[42] Summers S J and Werner R 1988 *Ann. Inst. H. Poincaré* A **49** 215
[43] Kempe J, Regev O and Toner B 2007 *Preprint* 0710.0655
[44] Kempe K M B T J, Kobayashi H and Vidick T 2007 *Preprint* 0704.2903
[45] Lasserre J B 2001 *SIAM J. Optim.* **11** 796
[46] Henrion D and Lassserre J B 2006 *IEEE Trans. Aut. Contr.* **51** 192
[47] Sturm J *SeDuMi, a MATLAB Toolbox for Optimization Over Symmetric Cones* Online at http://sedumi.mcmaster.ca
[48] Löfberg J *Yalmip: A Toolbox for Modeling and Optimization in MATLAB* Online at http://control.ee.ethz.ch/∼joloef/yalmip.php