The Quantum Moment Problem and Bounds on Entangled Multi-Prover Games

Andrew C. Doherty
School of Physical Sciences
The University of Queensland
Queensland 4072, Australia

Yeong-Cherng Liang
School of Physical Sciences
The University of Queensland
Queensland 4072, Australia

Ben Toner
Centrum voor Wiskunde en Informatica
Kruislaan 413
1098 SJ Amsterdam, The Netherlands

Stephanie Wehner
Institute for Quantum Information
California Institute of Technology
Pasadena, CA 91125, USA

Abstract

We study the quantum moment problem: Given a conditional probability distribution together with some polynomial constraints, does there exist a quantum state $\rho$ and a collection of measurement operators such that (i) the probability of obtaining a particular outcome when a particular measurement is performed on $\rho$ is specified by the conditional probability distribution, and (ii) the measurement operators satisfy the constraints. For example, the constraints might specify that some measurement operators must commute.

We show that if an instance of the quantum moment problem is unsatisfiable, then there exists a certificate of a particular form proving this. Our proof is based on a recent result in algebraic geometry, the noncommutative Positivstellensatz of Helton and McCullough [Trans. Amer. Math. Soc., 356(9):3721, 2004].

A special case of the quantum moment problem is to compute the value of one-round multi-prover games with entangled provers. The strategy of the verifier is fixed. He randomly chooses two questions according to some fixed probability distribution and sends one question to each prover. Alice and Bob then each return an answer to the verifier. The verifier decides whether to accept these answers on the basis of some predefined rules of the game that specify whether the given answers are winning answers for the questions sent. To win the game, Alice and Bob may agree on any strategy beforehand, but they may no longer communicate once the game has started. The maximum probability with which Alice and Bob can cause the verifier to accept is known as the value of the game. A simple example is the well-known CHSH game [11, 12]. In this case, the questions and answers are bits. The verifier chooses questions $s \in \{0, 1\}$ and $t \in \{0, 1\}$ uniformly at random and sends $s$ to Alice and $t$ to Bob. In order to win the game, Alice and Bob must reply with bits $a, b \in \{0, 1\}$ such that $s \land t = a \oplus b$, i.e., the logical AND of $s$ and $t$ should be equal to the XOR of $a$ and $b$. It is straightforward to verify that the CHSH game has value $3/4$.

Interactive proof systems have received considerable attention since their introduction by Babai [1] and Goldwasser, Micali and Rackoff [17] in 1985. Of special interest to us are proof systems with multiple provers [2, 4, 7, 14, 15, 27], as introduced by Ben-Or, Goldwasser, Kilian and Widgerson [4], which can be described in terms of multi-prover games between a verifier, and two or more provers. While the provers are computationally unbounded, the verifier is limited to probabilistic polynomial time. Both the provers and the verifier have access to a common input string $x$. The goal of the provers is to convince the verifier that $x$ belongs to a pre-specified language $L$. The verifier’s aim, on the other hand, is to determine whether the provers’

two-prover cooperative game of incomplete information is played by a verifier against two provers, Alice and Bob. The strategy of the verifier is fixed. He randomly chooses two questions according to some fixed probability distribution and sends one question to each prover. Alice and Bob then each return an answer to the verifier. The verifier decides whether to accept these answers on the basis of some predefined rules of the game that specify whether the given answers are winning answers for the questions sent. To win the game, Alice and Bob may agree on any strategy beforehand, but they may no longer communicate once the game has started. The maximum probability with which Alice and Bob can cause the verifier to accept is known as the value of the game. A simple example is the well-known CHSH game [11, 12]. In this case, the questions and answers are bits. The verifier chooses questions $s \in \{0, 1\}$ and $t \in \{0, 1\}$ uniformly at random and sends $s$ to Alice and $t$ to Bob. In order to win the game, Alice and Bob must reply with bits $a, b \in \{0, 1\}$ such that $s \land t = a \oplus b$, i.e., the logical AND of $s$ and $t$ should be equal to the XOR of $a$ and $b$. It is straightforward to verify that the CHSH game has value $3/4$.

Interactive proof systems have received considerable attention since their introduction by Babai [1] and Goldwasser, Micali and Rackoff [17] in 1985. Of special interest to us are proof systems with multiple provers [2, 4, 7, 14, 15, 27], as introduced by Ben-Or, Goldwasser, Kilian and Widgerson [4], which can be described in terms of multi-prover games between a verifier, and two or more provers. While the provers are computationally unbounded, the verifier is limited to probabilistic polynomial time. Both the provers and the verifier have access to a common input string $x$. The goal of the provers is to convince the verifier that $x$ belongs to a pre-specified language $L$. The verifier’s aim, on the other hand, is to determine whether the provers’

1 Introduction

The study of multi-prover games has led to many exciting results in classical complexity theory. A one-round
claim is indeed valid. In each round, the verifier sends a \( \text{poly}(|x|) \) size query to the provers, who return a polynomial size answer. At the end of the protocol, the verifier either accepts, meaning that he concludes \( x \in L \), or rejects, based on the messages exchanged and on his own private randomness. A language \( L \) has a multi-prover interactive proof system if there is a protocol such that, if \( x \in L \), there exist answers the provers can give which will cause the verifier to accept with high probability, but, if \( x \not\in L \), then there is no strategy for the provers that will cause the verifier to accept, except with small probability. Fixing \( x \) and \( L \) leads to a particular game. Let MIP denote the class of languages having a multi-prover interactive proof system. It has been shown that classical two-prover interactive proof systems are just as powerful as proof systems involving more than two provers. In fact, Babai, Fortnow and Lund [2], and Feige and Lovász [15] have shown that a language is in NEXP if and only if it has a two-prover one-round proof system, i.e., MIP = NEXP.

1.1 Games with entanglement

In this paper, we study multi-prover games in a quantum setting. In particular, we allow Alice and Bob to share an entangled quantum state as part of their strategy. After receiving their questions, the provers may perform any local measurement on their part of the entangled state, and decide on an answer based on the outcome of their measurement. All communication between the verifier and the provers remains classical. The entangled value of a game is the maximum probability with which Alice and Bob can win using entanglement. It turns out that sharing entanglement can increase the probability that the provers can cause the verifier to accept, an effect known as quantum nonlocality [3]. For example, if the provers share a maximally entangled state of two qubits they can win the CHSH game (cause the verifier to accept) with probability \( p_{\text{CHSH}} \approx 85% > 3/4 \).

We write MIP\(^*\) for the set of languages that have interactive proofs with entangled provers. Very little is known about MIP\(^*\). Most importantly, prior to this work it was not known whether there exists an algorithm of any complexity for deciding membership in MIP\(^*\), except for extremely restricted classes of games. In particular, if we restrict to games where Alice and Bob each answer a single bit \( a, b \in \{0, 1\} \), and the verifier only looks at the XOR of these two bits, then the (entangled) value of the game can be computed in time polynomial in the number of questions [9, 12]. Let \( \oplus \text{MIP}[2] \) denote the restricted class where the verifier’s output is a function of the XOR of two binary answers. Then \( \oplus \text{MIP}[2] \subseteq \text{EXP} \) [12], while it is known that the classical class \( \oplus \text{MIP} = \text{NEXP} \), for certain completeness and soundness parameters [19], i.e., XOR proof systems are significantly weakened if the provers are allowed to share entanglement. In fact, such a proof system can even be simulated using just a single quantum prover, i.e., \( \oplus \text{MIP}^* \subseteq \text{QIP}(2) \subseteq \text{EXP} \) [40, 25].

Unfortunately, very little is known for more general games when we allow shared entanglement between the provers, for example, when Alice and Bob give longer answers, or when there are more than two provers. Kempe et al. have shown that it is NP-hard to approximate the entangled value of a three-prover game with exponential precision [23]. For two-prover unique games (where for each pair of questions and each answer of one prover there is exactly one winning answer for the other prover), it is known that we can approximate the entangled value to within a constant in polynomial time [24]. Masanes [30] has shown how to compute the value of multi-prover games where the questions to, and the answers from each prover are bits. But even for very small games with a limited number of questions, the entangled value is typically unknown.

Assuming that the provers share quantum entanglement is a reasonable model because it captures the properties of a multi-prover game that a verifier can enforce physically: while the verifier can enforce the condition that the provers cannot communicate by ensuring that they are spacelike-separated, he has no way to ensure that provers in a quantum universe do not share entanglement. Multi-prover games with entangled provers are also known as nonlocal games with entanglement. Here, we are concerned with the following question: Can we compute the entangled value of nonlocal games with multiple provers? And, can we decide membership of MIP\(^*\)?

1.2 Results

Quantum moment problem. To reach our goal, we first introduce the quantum moment problem, a generalization of our problem. Informally, the quantum moment problems asks whether, given a conditional probability distribution and some polynomial constraints on observables, we can find a quantum state and quantum measurements that satisfy the constraints and provide us with the required probabilities. We may use the constraints to impose certain restrictions on the form of our quantum measurements. For example, we may wish to demand that two measurement operators act independently on two separate subsystems. Determining whether there is an entangled strategy for a multi-prover game that achieves a certain winning probability is a special case of the quantum moment problem.

Other special cases of the quantum moment problem include the classical marginal problem [37], which asks whether, given certain marginal distributions, we can find a joint distribution that has the desired marginals. Our problem is also closely related to the quantum marginal problem in which the aim is to find a density matrix for a multipartite
quantum system that is consistent with a specified set of reduced density matrices for specific subsystems. This problem is QMA-complete and has attracted a lot of interest recently [29]. A special case is \(N\)-representability, an important problem with a long history in quantum chemistry [26].

One key difference between our quantum moment problem and the quantum marginal problem is that in the latter case the dimension of the quantum state, and its various subsystems, is specified. In the quantum moment problem the aim is to find a state satisfying the given constraints in a quantum system of any, possibly infinite, dimension. Finally, it may also be possible to treat games with quantum verifier within the framework of the quantum moment problem.

**Refuting unsatisfiable instances.** We describe a general way of proving that an instance of a quantum moment problem is unsatisfiable. The proof follows from a recent result of Helton and McCullough [20], a Positivstellensatz for polynomials in noncommuting variables. The choice of polynomials will define a particular instance of the quantum moment problem, where the variables correspond to measurement operators. In Helton and McCullough’s result the noncommuting variables are required to satisfy certain polynomial equality and inequality constraints but can be evaluated in any quantum system, even an infinite-dimensional one. Informally, the Positivstellensatz states that any such polynomial that is positive can be written as a sum of squares, a form that makes it obvious that the polynomial is positive. By positive we mean that, whenever the constraints are satisfied, the polynomial is positive semidefinite, i.e. it has a positive expectation value for all quantum states of any quantum system. Such a representation as a sum of squares acts as a certificate for the unsatisfiability of an instance of a quantum moment problem. Certificates of this kind have often been used in the theoretical physics literature to place very general bounds on quantum moments (see for example [16]). Helton and McCullough’s result shows that such certificates are all that is ever required to demonstrate that an instance of the quantum moment problem is unsatisfiable.

**Tensor products and commutation.** In order to apply the Positivstellensatz to obtain bounds on the entangled values of two-prover games, we need to incorporate a constraint in the corresponding quantum moment problem that ensures Alice and Bob’s measurements act on different subsystems \(\mathcal{H}_A\) and \(\mathcal{H}_B\). When Alice and Bob’s quantum systems are finite-dimensional, this means that one demands that the Hilbert space \(\mathcal{H}\) describing the joint system should decompose as \(\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B\). Alice and Bob’s measurements should be of the form \(A_s \otimes B_t\) with \(A_s \in \mathcal{H}_A\) and \(B_t \in \mathcal{H}_B\) for all questions \(s\) and \(t\). Unfortunately, we can only apply the Positivstellensatz when the constraints are polynomials in \(A_s\) and \(B_t\). Thus we need an additional trick to impose an explicit tensor product structure. To get around this problem, we demand that for all \(s\) and \(t\) we have \([A_s, B_t] = 0\), i.e., that all measurement operators of Alice commute with all those of Bob. If the Hilbert space is finite-dimensional, then imposing the commutativity constraints is actually equivalent to demanding a tensor product structure. This result is well-known in the mathematical physics literature [39]. In the full version of this paper [13], we provide a simple version of this argument accessible from a computer science perspective, which directly applies to our analysis of multi-prover games.

From a physics point of view, however, the usual requirement on observables that can be measured in space-like separated regions is that they should commute, not that they should have a tensor product factorization. Indeed, this commutativity requirement on local observables is regarded by many as an axiom that should be satisfied by any reasonable quantum mechanical theory of nature [18]. Unfortunately, when the algebra of observables cannot be represented on a finite-dimensional Hilbert space, it is an open question whether this commutativity property implies the existence of a tensor product factorization. Our results will provide bounds on the values of multi-prover games that are valid for all quantum systems whenever the observables of different players commute. We will refer to the maximum probability of winning a game \(G\) with (possibly) infinite-dimensional observables satisfying commutativity constraints as the field-theoretic value \(\omega^f(G)\) of the game. It is an open question whether this is the same as the usual entangled value of the game. In analogy with MIP\(^*\), which was defined with a tensor product structure in mind, we also define the class MIP\(^f\), where the tensor products are replaced by the commutativity requirement. The class MIP\(^f\) seems more appropriate to our main motivation of studying the power of multi-prover games where the provers are only limited by what can be achieved physically.

**A hierarchy of semidefinite programs.** The Positivstellensatz leads to certificates that indicate when a particular quantum moment problem is unsatisfiable. But how can we find such certificates? If we place a bound on the size of the certificate, then the problem of determining whether there exists a certificate of that size can be formulated as a semidefinite program (SDP) [5]. In particular, searching for certificates of increasing size yields a hierarchy of SDPs. The resulting hierarchy is very similar to the one presented in a groundbreaking paper of Navascués, Pironio and Acín [33], which partly motivated this work.

In many applications, including multi-prover games, we are not only interested in whether a specific instance of the moment problem is satisfiable, but also in finding the best possible bound on some linear combination of moments.
Once again fixing the size of the certificates of infeasibility straightforwardly leads to a hierarchy of SDPs that provide progressively tighter bounds. For a multi-prover game \( G \), it was previously not known whether the solutions to this hierarchy of SDPs converged to the entangled value of the game, denoted \( \omega^*(G) \). Here we almost show this. What we actually show is that the hierarchy converges to the field-theoretic value \( \omega_f(G) \). Fix some probability \( p \). Then Positivstellensatz only yields a certificate that there is no entangled strategy that wins with probability \( p \) if there is also no such strategy even with infinite-dimensional measurement operators. If the measurement operators are infinite-dimensional, then the commutativity constraints do not necessarily imply the existence of a tensor product structure.

**Languages in MIP\(^f\) are recursive** Since the hierarchy converges, we can compute the value of an entangled game and hence obtain an algorithm for deciding membership of MIP\(^f\) (and of MIP*\(^\omega\), under the assumption that the optimal value is achieved with finite-dimensional operators). This implies that languages in these classes are recursive.

**Example: A new Tsirelson inequality** Finally, we demonstrate the power of our technique by providing a simple, algorithmically constructed, certificate bounding the quantum value of a tripartite Bell inequality of Ito, Kobayashi, Preda, Sun, and Yao [22].

### 1.3 Open Questions

Are there games \( G \) such that \( \omega^*(G) \) is strictly less than \( \omega_f(G) \)? Can it really help the provers to have infinite-dimensional systems when the number of questions and answers in the game are finite? One way to establish that there is no advantage to having infinite-dimensional systems would be to ‘round’ the SDP hierarchy directly to a quantum strategy with finite entanglement, bypassing the (nonconstructive) Positivstellensatz altogether. For XOR-games, the first level of our hierarchy is tight and it is well-known how a solution of the SDP can be transformed into a quantum strategy via Tsirelson’s construction [8, 9, 10]. However, there exist nonlocal games for which the first level of the hierarchy does not provide us with the optimal value of the game, but merely gives us an upper bound. This fact alone shows that for general games, we cannot find such a nice embedding of vectors into observables as can be done for XOR-games. However, something similar may still be possible for other restricted classes of games.

We also do not establish anything about the rate of convergence of the SDP hierarchy. In some numerical experiments with small games, the low levels of the SDP hierarchy do yield optimal solutions. Establishing this in general would provide an upper bound on MIP*. We have made partial progress on this question by proving convergence for a particular hierarchy of SDPs.

### 1.4 Related work

In [33], Navascués, Pironio, and Acín (NPA) defined a closely related semidefinite programming hierarchy. Subsequently, and independently of us, NPA have proved that their semidefinite programming hierarchy converges to the field-theoretic value of the game [31]. Our paper and theirs are complementary: While our work emphasizes the connection with Positivstellensatz of Helton and McCullough, NPA prove convergence directly. Their proof does have one advantage: when their hierarchy converges to the field-theoretic value of the game at a finite level, NPA obtain a bound on the dimension of the state required to play optimally. NPA have also extended their new technique for proving convergence to general polynomial optimization problems in noncommutative variables [32].

Finally, our techniques have been extended by Ito, Kobayashi, and Matsumoto to the case of games with quantum messages between the verifier and provers [21].

### 1.5 Outline

In Section 2, we provide an introduction to nonlocal games including all necessary definitions. Section 3 then defines the quantum moment problem, and Section 4 introduces our main tools. In particular, Section 4.1 provides an explanation of why we obtain a tensor product structure from commutation relations, and in Section 4.2, we show that if a quantum moment problem is unsatisfiable, we can find certificates of this fact using the Positivstellensatz. We then use these tools in our SDP hierarchy in Section 5 and conclude in Section 5.2 with some explicit examples.

### 2 Preliminaries

#### 2.1 Notation

We assume general familiarity with the quantum model [36]. In the following, we use \( A^\dagger \) to denote the conjugate transpose of a matrix \( A \). A matrix is Hermitian if and only if \( A^\dagger = A \). We write \( A \geq 0 \) to indicate that \( A \) is positive semidefinite, i.e., it is Hermitian and has no negative eigenvalues. We also use \( A = 0 \) to express that \( A \) is the all-zero matrix and \( A \neq 0 \) to indicate that \( A \) has at least one non-zero entry. The \((i,j)\)-entry of \( A \) will be denoted by \( [A]_{i,j} \). For two matrices \( A \) and \( B \) we write their commutator as \( [A,B] = AB - BA \). We use \( \mathcal{H} \) to denote a Hilbert space and \( \mathcal{H}_k \) the Hilbert space belonging to subsystem \( k \). \( \mathbb{I}_k \) is the identity on system \( k \), and
\( \mathbb{B}(\mathcal{H}) \) denotes the set of all bounded operators on the Hilbert space \( \mathcal{H} \). Unless stated otherwise, we take all systems to be finite-dimensional. We will also employ the shorthand \( \mathbb{B}(\mathcal{H})^n := \mathbb{B}(\mathcal{H}) \times \cdots \times \mathbb{B}(\mathcal{H}) \) for the \( n \)-fold Cartesian product of \( \mathbb{B}(\mathcal{H}) \), and let \( [n] := \{ 1, \ldots, n \} \). Furthermore, we will use \( |S| \) and \( |L| \) to denote the number of elements of a set \( S \) and list \( L \) respectively.

For the purpose of subsequent discussion, we now note that a Hermitian polynomial \( p(X) \) in noncommutative variables \( X = (X_1, \ldots, X_k) \) is a sum of squares (SOS) if there exist polynomials \( r_j(X) \) of appropriate dimension such that \( p(X) = \sum_{j} r_j^2(X) \). It is important to note that if \( p(X) \) is an SOS, it is also a positive semidefinite matrix, i.e., \( p(X) \geq 0 \).

### 2.2 Games

As an example application of the quantum moment problem, we will consider cooperative games among \( n \) parties. For simplicity, we first describe the setting for only two parties, henceforth called Alice and Bob. A generalization is straightforward. Let \( S, T, A \) and \( B \) be finite sets, and \( \pi \) a probability distribution on \( S \times T \). Let \( V \) be a predicate on \( S \times T \times A \times B \). Let \( G = G(V, \pi) \) be the following two-person cooperative game: a pair of questions \( (s, t) \in S \times T \) is chosen at random according to the probability distribution \( \pi \). Then \( s \) is sent to Alice, and \( t \) to Bob. Upon receiving \( s \), Alice has to reply with an answer \( a \in A \). Likewise, Bob has to reply to question \( t \) with an answer \( b \in B \). Alice and Bob win if \( V(s, t, a, b) = 1 \) and lose otherwise. Alice and Bob may agree on any kind of strategy beforehand, but they are no longer allowed to communicate once they have received questions \( s \) and \( t \). The value \( \omega(G) \) of a game \( G \) is the maximum probability that Alice and Bob win the game. In what follows, we will write \( V(a, b|s, t) \) instead of \( V(s, t, a, b) \) to emphasize the fact that \( a \) and \( b \) are the answers for the given questions \( s \) and \( t \).

Here, we are particularly interested in nonlocal games where Alice and Bob are allowed to share an entangled state \( |\psi\rangle \) to help them win the game. Let \( \mathcal{H}_A \) and \( \mathcal{H}_B \) denote the Hilbert spaces of Alice and Bob respectively. The state \( |\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \) is part of the quantum strategy that Alice and Bob can agree on beforehand. This means that for each game, Alice and Bob can choose a specific \( |\psi\rangle \) to maximize their chance of success. In addition, Alice and Bob can agree on quantum measurements, where we may without loss of generality assume that these are projective measurements [12].

1By Neumark’s theorem, any generalized measurements described by positive-operator-valued measure can be implemented as projective measurements in some higher dimensional Hilbert space. See, for example, pp. 285 of [36].

tive measurement described by \( \{ A_a^s : a \in A \} \) on \( \mathcal{H}_A \). For each \( t \in T \), Bob has a projective measurement described by \( \{ B_t^b : b \in B \} \) on \( \mathcal{H}_B \). For questions \( (s, t) \in S \times T \), Alice performs the measurement corresponding to \( s \) on her part of \( |\psi\rangle \) which gives her outcome \( a \). Likewise, Bob performs the measurement corresponding to \( t \) on his part of \( |\psi\rangle \) with outcome \( b \). Both send their outcomes back to the verifier. The probability that Alice and Bob answer \( (a, b) \in A \times B \) is then given by

\[
\langle \psi | A_a^s \otimes B_t^b | \psi \rangle.
\]

**Definition 2.1.** The entangled value of a two-prover game with classical verifier \( G = G(\pi, V) \) is given by:

\[
\omega^e(G) = \lim_{d \to \infty} \max_{|\psi\rangle \in \mathcal{C}^d} \max_{\|\psi\| = 1} \sum_{a, b, s, t} \pi(s, t) \times V(a, b|s, t) \langle \psi | A_a^s \otimes B_t^b | \psi \rangle,
\]

where \( A_a^s \in \mathbb{B}(\mathcal{H}_A) \) and \( B_t^b \in \mathbb{B}(\mathcal{H}_B) \) for some Hilbert space \( \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \), satisfying \( A_a^s, B_t^b \geq 0, \sum_a A_a^s = \mathbb{1}_A, \sum_b B_t^b = \mathbb{1}_B \) for all \( s \in S \) and \( t \in T \).

We also define:

**Definition 2.2.** The field-theoretic value of a two-prover game with classical verifier \( G = G(\pi, V) \) is given by:

\[
\omega^f(G) = \sup_{A_a^s, B_t^b} \left\| \sum_{a, b, s, t} \pi(s, t) V(a, b|s, t) A_a^s B_t^b \right\|,
\]

where \( \| O \| \) is the operator norm of \( O \), \( A_a^s \in \mathbb{B}(\mathcal{H}_A) \) and \( B_t^b \in \mathbb{B}(\mathcal{H}_B) \) for some Hilbert space \( \mathcal{H} \), satisfying \( A_a^s, B_t^b \geq 0, \sum_a A_a^s = \mathbb{1}_A, \sum_b B_t^b = \mathbb{1}_B \) for all \( s \in S, t \in T \), \( a \in A \), and \( b \in B \).

**Lemma 2.3.** Let \( G = G(\pi, V) \) be a two-prover game with classical verifier. Then \( \omega^e(G) \leq \omega^f(G) \).

**Proof.** Let \( \varepsilon > 0 \). Choose \( d \) sufficiently large so that there is a normalized state \( |\psi\rangle \) and operators \( A_a^s, B_t^b \) defining a strategy with winning probability at least \( \omega^f(G) - \varepsilon \). Let \( A_a^s = A_a^s \otimes \mathbb{1}_B \) and \( B_t^b = \mathbb{1}_A \otimes B_t^b \). Then \( A_a^s \) and \( B_t^b \) are positive semidefinite operators on \( \mathbb{C}^{d^2} \) satisfying all the conditions in Definition 2.2. Finally,

\[
\omega^f(G) = \sup_{A_a^s, B_t^b} \left\| \sum_{a, b, s, t} \pi(s, t) V(a, b|s, t) A_a^s B_t^b \right\| \geq \left\| \sum_{a, b, s, t} \pi(s, t) V(a, b|s, t) A_a^s B_t^b \right\| \geq \langle \psi | \sum_{a, b, s, t} \pi(s, t) V(a, b|s, t) A_a^s B_t^b | \psi \rangle \geq \omega^e(G) - \varepsilon.
\]

Since \( \varepsilon \) was arbitrary, the result follows. \( \square \)
In our examples, we will sometimes use the term Bell inequality [3] to refer to a particular nonlocal game. This is an equivalent formulation, where we only consider terms of the form \(|\psi|A_s^aB_t^b|\psi\rangle\). The value of the game can then be obtained by averaging. In inequalities where Alice and Bob have, respectively, two measurement outcomes for each possible choice of measurement setting (i.e., \(A = B = \{0, 1\}\)), their measurements can be described by observables of the form \(A_s = A_0^a - A_1^a\) and \(B_t = B_0^b - B_1^b\) respectively. In this case, we state inequalities in the form of the observables \(A_s\) and \(B_t\) where we will use the shorthand \(\langle A_sB_t \rangle = \langle |\psi|A_sB_t|\psi\rangle\).

When considering games among \(N\) players \(P_1, \ldots, P_N\), let \(S_1, \ldots, S_N\) and \(A_1, \ldots, A_N\) be finite sets corresponding to the possible questions and answers respectively. Let \(\pi\) be a probability distribution on \(S_1 \times \ldots \times S_N\), and let \(V\) be a predicate on \(A_1 \times \ldots \times A_N \times S_1 \times \ldots \times S_N\). Then \(G = G(V, \pi)\) is the following \(N\)-player cooperative game: A set of questions \((s_1, \ldots, s_N) \in S_1 \times \ldots \times S_N\) is chosen at random according to the probability distribution \(\pi\). Player \(P_j\) receives question \(s_j\), and then responds with an answer \(a_j \in A_j\). The players win if and only if 

\[
V(a_1, \ldots, a_N|s_1, \ldots, s_N) = 1
\]

Let \(|\psi\rangle\) denote the players’ choice of state, and let \(X_j := \{X_j^{a_j} | a_j \in A_j\}\) denote the positive-operator-valued measure(ment) (POVM) of player \(P_j\) for question \(s_j \in S_j\), i.e., \(\sum_{a_j} X_j^{a_j} = 1\) and \(X_j^{a_j} \geq 0\) for all \(a_j\). The value of the game can now be written as

\[
\omega^*(G) = \lim_{d \to \infty} \max_{|\psi\rangle} \max_{||\psi|| = 1} \sum_{s_1, \ldots, s_N} \pi(s_1, \ldots, s_N) \cdot \\
\sum_{a_1, \ldots, a_N} V(a_1, \ldots, a_N|s_1, \ldots, s_N) \cdot \\
\langle \psi| X_j^{a_j} \otimes \cdots \otimes X_j^{a_j} |\psi\rangle,
\]

where the maximization is taken over all legitimate POVMs \(X_j\) for all \(j \in [N]\). Similarly, we can now write the field-theoretic value of the game as

\[
\omega^f(G) = \sup_{X_1, \ldots, X_N} \left\| \sum_{s_1, \ldots, s_N} \pi(s_1, \ldots, s_N) \cdot \\
\sum_{a_1, a_N} V(a_1, \ldots, a_N|s_1, \ldots, s_N) X_j^{a_j} \cdots X_j^{a_j} \right\|
\]

where we now have \(\sum_{a_j} X_j^{a_j} = 1\) for all \(a_j\), and \([X_j^{a_j}, X_j^{a_j'}] = 0\) for all \(j \neq j'\).

### 2.3 Interactive proof systems

Interactive proof systems can be phrased in terms of games. For completeness, we here provide a definition of MIP. We refer to the introduction and the previous section for an explanation of the significance of enforcing locality with commutation relations rather than a tensor product structure.

**Definition 2.4.** For \(0 \leq s < c \leq 1\), let \(\text{MIP}^c_{s}^{k}[k]\) denote the class of all languages \(L\) recognized by a \(k\)-prover interactive proof system with entanglement such that:

- The interaction between the verifier and the provers is limited to one round of classical communication. The verifier chooses \(k\) questions from a finite set of possible questions, according to a fixed probability distribution known to the provers, and sends one question to each prover. Afterwards, the provers may perform any measurement that has tensor product form on a shared state \(|\psi\rangle\) that they have chosen ahead of time. Each prover returns an answer to the verifier, whose decision function is known to the provers.

- If \(x \in L\) then there exists a strategy for the provers for which the probability that the verifier accepts is at least \(c\) (the completeness parameter).

- If \(x \notin L\) then, whatever strategy the \(k\) provers follow, the probability that the verifier accepts is at most \(s\) (the soundness parameter).

**Definition 2.5.** For \(0 \leq s < c \leq 1\), let \(\text{MIP}^f_{s}^{c,k}[k]\) denote the class corresponding to a modified version of the previous definition: here we merely ask that the measurements operators between the different players commute.

### 3 The quantum moment problem

#### 3.1 General form

Let us first state the quantum moment problem in its most general form, before explaining its connection to nonlocal games. Intuitively, the quantum moment problem asks whether, given a certain probability distribution, is it possible to find quantum measurements and a state that provide us with such a distribution.

**Definition 3.1 (Quantum moment problem).** Given a list of numbers \(M = \{m_i | m_i \in [0, 1]\}\), a set of polynomial equations \(\mathcal{R} = \{r = 0 \mid r : \mathbb{B}(\mathcal{H})^{\times|\mathcal{M}|} \to \mathbb{B}(\mathcal{H})\}\), and polynomial inequalities \(\mathcal{S} = \{s \geq 0 \mid s : \mathbb{B}(\mathcal{H})^{\times|\mathcal{M}|} \to \mathbb{B}(\mathcal{H})\}\), does there exist said Hilbert space \(\mathcal{H}\), operators \(M_i \in \mathbb{B}(\mathcal{H})\) and a state \(\rho \in \mathbb{B}(\mathcal{H})\) such that

1. For all \(m_i \in \mathcal{M}\), \(\text{Tr}(M_i \rho) = m_i\).
2. For all \(r \in \mathcal{R}, r(M_1, \ldots, M_{|\mathcal{M}|}) = 0\).
3. For all \(s \in \mathcal{S}, s(M_1, \ldots, M_{|\mathcal{M}|}) \geq 0\).
3.2 Nonlocal games

In this paper, we are particularly interested in the special case of the quantum moment problem where we consider measurements on many space-like separated systems as in the setting of nonlocal games. Consider two systems, Alice $\mathcal{H}_A$ and Bob $\mathcal{H}_B$. On each system, $\mathcal{H}_A$ and $\mathcal{H}_B$, we can perform one of a finite set of possible measurements, $S$ and $T$, each of which has the same finite set of outcomes, $A$ and $B$, respectively. Let $m^{A\bar{B}}(ab|st)$ denote the joint probability of obtaining outcomes $a$ and $b$ given measurement settings $s$ and $t$. Our question is whether there is a joint state $\rho$ and measurement operators $A_s^a$ on $\mathcal{H}_A$ and $B_t^b$ on $\mathcal{H}_B$ that give rise to these probabilities. First of all, how can we express the fact that we want our measurement operators to act on the individual systems $\mathcal{H}_A$ and $\mathcal{H}_B$ alone? We will later use this constraint instead of the one in Eq. (3). Finally, we want to know if there exist operators of the form $[A_s^a, B_t^b] = 0$. Our question is whether there is a joint state $\rho$ and measurement operators $A_s^a$ on $\mathcal{H}_A$ and $B_t^b$ on $\mathcal{H}_B$ that give rise to these probabilities. First of all, how can we express the fact that we want our measurement operators to act on the individual systems $\mathcal{H}_A$ and $\mathcal{H}_B$ alone? We will later use this constraint instead of the one in Eq. (3).

Furthermore, we need to impose additional polynomial constraints to ensure that our operators are valid measurements. For all $s \in S$ and $t \in T$, we insist that

$$\sum_{a \in A} A_s^a - I = 0 \quad \text{and} \quad \sum_{b \in B} B_t^b - I = 0,$$

and

$$A_s^a \geq 0 \quad \text{and} \quad B_t^b \geq 0. \quad (3)$$

Recall that we may restrict ourselves to considering projective measurements. We may thus add the equality constraints

$$(A_s^a)^2 = A_s^a \quad \text{and} \quad (B_t^b)^2 = B_t^b,$$

which automatically imply that $A_s^a, B_t^b \geq 0$. For simplicity, we will later use this constraint instead of the one in Eq. (3).

Finally, we want to know if there exist operators of the above form such that

$$\nu = \left\| \sum_{a,b,s,t} \pi(s,t) V(a,b|s,t) A_s^a B_t^b \right\|$$

for some success probability $\nu$. Semidefinite programming will allow us to turn this question of existence into an optimization problem.

4 Tools

We need two key tools for our analysis. The first one allows us to deal with the fact that we want measurements to have tensor product form. Our second tool is an extension of the non-commutative Positivstellensatz of Helton and McCullough to the field of complex numbers, from which we will derive a converging hierarchy of semidefinite programs.

4.1 Tensor product structure from commutation relations

We first show that imposing commutativity constraints does indeed give us the tensor product structure required for our analysis of nonlocal games. It is well-known that the following statement holds within the framework of quantum mechanics — an algebra of type-I [39] (a simple version of this argument accessible from a computer science perspective can be found in the long version [13]).

**Lemma 4.1.** Let $\mathcal{H}$ be a finite-dimensional Hilbert space, and let $\{X_{s,j}^a \in \mathbb{B}(\mathcal{H}) \mid \forall j \in [N] \text{ and for all } s_j \in S_j, a_j \in A_j \}$. Then the following two statements are equivalent:

1. For all $j, j' \in [N], j \neq j'$, and all $s_j \in S_j, s_{j'} \in S_{j'}$, $a_j \in A_j$ and $a_{j'} \in A_{j'}$ it holds that $[X_{s_j}^{a_j}, X_{s_{j'}}^{a_{j'}}] = 0$.
2. There exist Hilbert spaces $\mathcal{H}_1, \ldots, \mathcal{H}_N$ such that $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ and for all $j \in [N], \text{ all } s_j \in S_j, a_j \in A_j \text{ we have } X_{s_j}^{a_j} \in \mathbb{B}(\mathcal{H}_j)$.

4.2 Positivstellensatz

Our second tool, the Positivstellensatz (in combination with semidefinite programming) will allow us to find certificates for the fact that a quantum moment problem is infeasible. For simplicity, we here describe the Positivstellensatz from the perspective of nonlocal games. An extension to the general quantum moment problem is straightforward. Our results follow almost directly from Helton and McCullough’s work and our proof closely follows that in [20]. We provide a complete proof of the Positivstellensatz in the long version of this paper [13] for three reasons: (i) the proof is more straightforward in our concrete setting, (ii) Helton and McCullough’s theorem is formulated for symmetric operators over the field $\mathbb{R}$, and we need to work with Hermitian operators over the field $\mathbb{C}$, and (iii) so we can highlight the nonconstructive steps in the proof. We first define:

**Definition 4.2 (Convex Cone $C_P$).** Let $P$ be a collection of Hermitian polynomials in (noncommutative) variables $\{X_{s,j}^a\}$. The convex cone $C_P$ generated by $P$ consists of polynomials of the form

$$q = \sum_{i=1}^M r_i^1 r_i + \sum_{i=1}^N \sum_{j=1}^L s_{ij}^1 p_i s_{ij}, \quad (4)$$
where \( p_i \in \mathcal{P}, M, N \) and \( L \) are finite, and \( r_i, s_{ij} \) are arbitrary polynomials.

In the following, we will call Eq. (4) a weighted sum of squares (WSOS) representation of \( q \).

The purpose of the set \( \mathcal{P} \) is to keep track of the constraints on the measurement operators. Note that when considering the measurement operators for nonlocal games, it is sufficient to restrict to measurement operators that are positive semidefinite. The Positivstellensatz as such does not only hold for Hermitian variables, but allows us to use any noncommuting matrix variables. In the following, we will always take our measurement operators to be of the form \( X^a_s = (X^a_s)\dagger X^a_s \). Clearly, \( X^a_s \) is itself a Hermitian polynomial in the variable \( X^a_s \). For clarity of notation, we will omit this explicit expansion in the future. This expansion will not increase the size of the SDP.

We can now write our constraints in terms of the following sets of Hermitian polynomials. We use the short hand notation \( O_{-j} := X^{a_1}_1 \ldots X^{a_{j-1}}_j X^{a_{j+1}}_{j+1} \ldots X^{a_N}_N \) to refer to a product of measurement operators where we exclude player \( j \). First, we want measurements on different subsystems to commute. In the multi-party case, this gives us the set of polynomials

\[
Q_1 = \{ s[X^a_{s_j}, O_{-j}] \mid \forall s_j \in S_j, a_j \in A_j \text{ and } \forall O_{-j} \}.
\]

Second, we want our operators to form valid measurements.

\[
Q_2 = \bigcup_{j, s_j} \{ \mathbb{1} - \sum_{a_j} X^a_{s_j} \}.
\]

Finally, by Neumark’s theorem [36], we may take our measurement operators to be projectors, this gives

\[
Q_3 = \bigcup_{j, s_j, a_j} \{ (X^a_{s_j})^2 - X^a_{s_j} \}.
\]

It’s not hard to see that these constraints actually give us orthogonality of the projectors. For clarity, however, we may also include the following sets of polynomials

\[
Q_4 = \{ s[X^a_{s_j}, X^b_{s_j}'] \mid \forall s_j \in S_j \text{ and } \forall a_j \neq a_j' \},
\]

\[
Q_5 = \{ X^a_{s_j} X^{a_j'}_{s_j} + X^{a_j'}_{s_j} X^a_{s_j} \mid \forall s_j \in S_j \text{ and } \forall a_j \neq a_j' \},
\]

which explicitly demand that projectors corresponding to the same \( s_j \) are orthogonal.

Let \( \mathcal{Q} = Q_1 \cup Q_2 \cup Q_3 \cup Q_4 \cup Q_5 \) and let \( \mathcal{P} = \mathcal{Q} \cup (-\mathcal{Q}) \). Note that all polynomials in \( \mathcal{P} \) are Hermitian. It is clear if the measurement operators satisfy the constraints, then the term \( \sum_{s_{ij}} s_{ij} p_{ij} \) vanishes for arbitrary polynomials \( s_{ij} \) since all the polynomials \( p_{ij} \in \mathcal{P} \) vanish. We are now ready to state the Positivstellensatz.

**Theorem 4.3 (Positivstellensatz).** Let \( G = G(\pi, V) \) be an \( N \)-prover game and let \( \mathcal{P} \) be the cone generated by the set \( \mathcal{P} \) defined above. Set

\[
q_\nu = \nu \mathbb{1} - \sum_{s_1, \ldots, s_N} \pi(s_1, \ldots, s_N) \sum_{a_1, \ldots, a_N} V(a_1, \ldots, a_N|s_1, \ldots, s_N) X^{a_1}_{s_1} \ldots X^{a_N}_{s_N}. \tag{5}
\]

If \( q_\nu > 0 \) whenever the constraints \( \mathcal{P} \) are satisfied, then \( q_\nu \in \mathcal{C}_\mathcal{P} \), i.e.,

\[
\nu \mathbb{1} - \sum_{s_1, \ldots, s_N} \pi(s_1, \ldots, s_N) \sum_{a_1, \ldots, a_N} V(a_1, \ldots, a_N|s_1, \ldots, s_N) X^{a_1}_{s_1} \ldots X^{a_N}_{s_N}
= \sum_i r_i^\dagger r_i + \sum_{i, j} s_{ij}^\dagger p_i s_{ij},
\]

for some \( p_i \in \mathcal{P}, \) and some polynomials \( r_i, s_{ij} \).

### 5 Finding upper bounds

We now show how to approximate the field-theoretic value of a nonlocal game using semidefinite programming. We construct a converging hierarchy of SDPs, where each level in this hierarchy gives us a better upper bound on the value of the game. To this end we will use the Positivstellensatz of Theorem 4.3 in combination with the beautiful approach of Parrilo [34, 35].

Recall from Definition 2.2 for the field-theoretic value of the two-player game that if for some real number \( \nu \) we have

\[
q_\nu = \nu \mathbb{1} - \sum_{a, b, s, t} \pi(s, t) V(a, b|s, t) A^a_s B^b_t \geq 0, \tag{7}
\]

whenever the operators \( \{ A^a_s \} \) and \( \{ B^b_t \} \) form a valid set of measurements, then \( \nu \) is an upper bound for the optimum value of the game, that is \( \nu \geq \omega_f(G) \). In the multiplayer case we also have \( \nu \geq \omega_f(G) \) if \( q_\nu \), as defined in equation (5), is positive whenever the measurements are valid. However, this condition seems difficult to check so we take a different approach. Suppose that \( q_\nu \) is a WSOS (6), so that

\[
q_\nu = \sum_{i=1}^M r_i^\dagger r_i + \sum_{i=1}^N \sum_{j=1}^L s_{ij}^\dagger p_i s_{ij}, \tag{8}
\]

for some polynomials \( r_i \) and \( s_{ij} \) in the variables \( \{ A^a_s \} \) and \( \{ B^b_t \} \). Notice that whenever the operators \( \{ A^a_s \} \) and \( \{ B^b_t \} \) form a valid set of measurements the polynomials \( p_i \) vanish since they are in \( \mathcal{P} \). So by inspection of (8) we may conclude \( q_\nu \geq 0 \) for these values of \( \{ A^a_s \} \) and \( \{ B^b_t \} \) and hence \( \nu \geq \omega_f(G) \). Intuitively, the WSOS representation of
Consider the problem given above for \( q_\nu \) as in Eq. (9). Notice that all of the constraint polynomials \( p_i \) defined in Section 4.2 have total degree less than or equal to 2 so we require that each \( r_i \) is of total degree \( n \) and each \( s_{ij} \) is of total degree at most \( n - 1 \). The lowest level of the hierarchy has \( n = 1 \) and corresponds to applying the method of Lagrange multipliers to finding the entangled value of the game. In the following, we use the term level \( n \) to refer to a level of the hierarchy where the total degree of \( q_\nu \) is \( 2n \). For a game \( G \), denote the solution to the SDP at level \( n \) as \( \omega_n^{\text{sdp}}(G) \). It should be clear that if \( q_\nu \) has a WSOS decomposition of degree \( 2n \), it must also have a WSOS decomposition with higher degree. As such, the optimum derived from the hierarchy of SDPs must obey the following inequalities:

\[
\omega_1^{\text{sdp}}(G) \geq \omega_2^{\text{sdp}}(G) \geq \cdots \geq \omega_n^{\text{sdp}}(G). \tag{10}
\]

**Theorem 5.1.** The solutions to the SDP hierarchy converge to \( \omega^f(G) \), i.e., \( \lim_{n \to \infty} \omega_n^{\text{sdp}} = \omega^f(G) \).

**Proof.** That \( \omega_n^{\text{sdp}}(G) \geq \omega^f(G) \) for all \( n \) follows from our discussion above. To find lower bounds on \( \omega_n^{\text{sdp}}(G) \), we use the Positivstellensatz given by Theorem 4.3. Fix \( \varepsilon > 0 \) and let \( \nu = \omega^f(G) + \varepsilon \) with \( q_\nu \) defined as in Eq. (5). By Theorem 4.3, \( q_\nu \) has a representation as a WSOS, Eq. (9). Let \( 2D \) be the maximum degree of the polynomials \( r_i \) and \( s_{ij} \) that occur in the WSOS decomposition. Then, if we consider a level \( D \) SDP relaxation, we must necessarily arrive at an optimum such that \( \omega_D^{\text{sdp}}(G) \leq \omega^f(G) + \varepsilon \). So for any \( \varepsilon > 0 \) there is a \( D \) such that \( \omega_D^{\text{sdp}}(G) \leq \omega^f(G) + \varepsilon \). Moreover, from Eq. (10) we have \( \omega_n^{\text{sdp}}(G) \leq \omega^f(G) + \varepsilon \) whenever \( n \geq D \) and so \( \omega_n^{\text{sdp}}(G) \) converges to \( \omega^f(G) \). \( \square \)

There are many connections of this semidefinite programming hierarchy to other methods that can be used to bound the quantum values of games. In particular, it can be shown that the dual semidefinite programs to this hierarchy are equivalent to the moment matrix methods of NPA [33], thus showing that the hierarchy of semidefinite programs discussed in that work converges to the entangled value of the game. Our example of the CHSH inequality below demonstrates this connection explicitly. In relation to this, it is worth noting that the duality between the two approaches (sum of squares and moment matrix) arises also in the case of commutative variables where the moment matrix methods of Laserre [28] are dual to the SDPs discussed by Parrilo [35].

### 5.2 Examples

**The CHSH inequality.** We will now look at the simplest nonlocal game that is derived from a Bell inequality known as the CHSH inequality [11]. In particular, we will illustrate
how our tools allow us to prove [8] that
\[ S_{\text{CHSH}} = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle \leq 2\sqrt{2}, \]
where \( A_1, A_2 \) and \( B_1, B_2 \) are observables with eigenvalues \( \pm 1 \) corresponding to Alice and Bob’s measurement settings respectively. First of all, note that since we are only interested in expectation values of the form \( \langle A_1 B_2 \rangle \), and not the probabilities of individual measurement outcomes, we may simplify our problem. We only need to demand that \( [A_j, B_k] = 0 \) for all \( j, k \in \{1, 2\} \) and also polynomials
\[
p_j^{(A)} := \mathbb{1} - (A_j)^2, \quad p_j^{(B)} := \mathbb{1} - (B_j)^2, \quad j = 1, 2,
\]
which guarantee that the observables do indeed have eigenvalues \( \pm 1 \). The Bell operator for the CHSH inequality is given by [6]
\[ B_{\text{CHSH}} = A_1 B_1 + A_1 B_2 + A_2 B_1 - A_2 B_2. \]
Hence, to find the optimum value our goal is to
\[
\begin{align*}
\text{minimize} & \quad \nu \\
\text{subject to} & \quad q_\nu = \nu \mathbb{1} - B_{\text{CHSH}} \in C_P.
\end{align*}
\]
The numerical package SOSTOOLS [38] gives a frontend to SDP solvers and explains how to apply these techniques in the case of commutative variables. Similar methods can be applied here. However, for our simple example, it is not hard to see how this problem can be recast in a language that may be more familiar.

Since \( B_{\text{CHSH}} \) is a noncommutative polynomial of degree 2, the lowest level relaxation consists of looking for a WSOS decomposition for \( q_\nu \) that is of degree 2. To this end, we shall consider a vector of monomials of degree 1, namely, \( z = (A_1, A_2, B_1, B_2)^T \). Our goal is to find a \( 4 \times 4 \) positive matrix \( \Gamma \) such that \( z^\dagger \Gamma z \) is the first term of the WSOS decomposition (8) and so \( q_\nu = z^\dagger \Gamma z \) whenever the constraints are satisfied.

Evidently, since we want \( z^\dagger \Gamma z \) to be a Hermitian polynomial, and we want our commutation constraints to hold, so we may without loss of generality take \( \Gamma \) to be real and symmetric. Note that this already takes care of the commutation constraints. Moreover, since all remaining constraints are quadratic, when looking for a WSOS decomposition for \( q_\nu \), it suffices to consider \( s_{ij} \) in Eq. (9) as multiples of \( \mathbb{1} \). Let \( \gamma_{ij} = [\Gamma]_{ij} \), then a small calculation shows that this amounts to requiring
\[
\nu = \gamma_{11} + \gamma_{22} + \gamma_{33} + \gamma_{44}
\]
and that \( \Gamma \) should be of the form
\[
\Gamma = \frac{1}{2} \begin{pmatrix}
2\gamma_{11} & 0 & -1 & -1 \\
0 & 2\gamma_{22} & -1 & 1 \\
-1 & -1 & 2\gamma_{33} & 0 \\
-1 & 1 & 0 & 2\gamma_{44}
\end{pmatrix}.
\]
With these constraints the proposed WSOS is
\[
q_\nu = z^\dagger \Gamma z + \sum_{j=1}^2 \gamma_{jj} p_j^{(A)} + \sum_{j=3}^4 \gamma_{jj} p_j^{(B)}.
\]
Now if we can find a \( \Gamma \geq 0 \) that is of this form, then whenever the polynomials given above vanish, \( q_\nu = z^\dagger \Gamma z \) is an SOS. To see this, note that in this case, we may write \( \Gamma = U^\dagger DU \), where \( U \) is unitary and \( D = \text{diag}(d_i) \) only consists of nonnegative diagonal entries. Then we can write \( q_\nu \) as \( \sum_i d_i (U z)_i^\dagger (U z)_i \), which is clearly an SOS. Conversely, note that if \( q_\nu = \sum_{j=1}^2 \gamma_{jj} p_j^{(A)} - \sum_{j=3}^4 \gamma_{jj} p_j^{(B)} \) is an SOS, we can find such a matrix \( \Gamma \). Hence, we can rephrase our optimization problem as the SDP
\[
\begin{align*}
\text{minimize} & \quad \text{Tr}(\Gamma) \\
\text{subject to} & \quad \Gamma \geq 0.
\end{align*}
\]
This is, in fact, exactly the dual of the SDP corresponding to the first level of the SDP hierarchy given by NPA [33], and the dual of the SDP for the special case of XOR games [41]. Solving this SDP, one obtains \( \gamma_{11} = \gamma_{22} = \gamma_{33} = \gamma_{44} = 1/\sqrt{2} \), which gives \( 2\sqrt{2} \) as an optimum. From here and Eq. (11), it is possible to write down a WSOS decomposition for \( \nu = 2\sqrt{2} \) as
\[
q_{2\sqrt{2}} = 2\sqrt{2} \mathbb{1} - B_{\text{CHSH}} = \frac{1}{2\sqrt{2}}(h_1^2 h_1 + h_2^2 h_2) + \frac{1}{\sqrt{2}} \sum_{j=1}^2 p_j^{(A)} + \frac{1}{\sqrt{2}} \sum_{j=3}^4 p_j^{(B)},
\]
with \( h_1 = A_1 + A_2 - \sqrt{2} B_1 \) and \( h_2 = A_1 - A_2 - \sqrt{2} B_2 \). This immediately implies that whenever the constraints are satisfied, \( q_{2\sqrt{2}} \geq 0 \) and hence \( B_{\text{CHSH}} \leq 2\sqrt{2} \mathbb{1} \). It is well known that for the CHSH inequality, this bound can be achieved [8].

A tripartite Bell inequality Finally, we examine a tripartite Bell inequality [22]. Alice, Bob and Charlie can each perform one of three possible measurements, each of which has two possible outcomes. As before, we express each measurement as an observable with eigenvalues \( \pm 1 \). For simplicity, let \( A_1, A_2, A_3, B_1, B_2, B_3 \) and \( C_1, C_2, C_3 \) correspond to the observables of Alice, Bob and Charlie respectively. The inequality states that for any shared state \( \rho \) we have
\[
S_{\text{IKPSY}} = (B_{\text{IKPSY}})^\dagger \rho (B_{\text{IKPSY}}) \leq 3\sqrt{3},
\]
where the Bell operator \( B_{\text{IKPSY}} \) is
\[
B_{\text{IKPSY}} = A_1 B_2 C_3 + A_2 B_3 C_1 + A_3 B_1 C_2 - A_1 B_3 C_2 - A_2 B_1 C_3 - A_3 B_2 C_1.
\]
a noncommutative polynomial of degree 3.

The constraints are analogous to the CHSH case. Among them are $p_j^{(A)} := I - (A_j)^2$, $p_j^{(B)} := I - (B_j)^2$, and $p_j^{(C)} := I - (C_j)^2$, for $j = 1, 2, 3$.

We consider the SDP relaxation

$$
\begin{aligned}
\text{minimize} & \quad \nu, \\
\text{subject to} & \quad q_\nu = \nu I - B_{\text{IKPSY}} \in C_P,
\end{aligned}
$$

where $q_\nu$ is a polynomial of degree at most 6. As before, we implicitly enforce the commutativity constraints, $[A_i, B_j] = 0$, $[A_i, C_k] = 0$, and $[B_j, C_k] = 0$ for all $i, j, k \in \{1, 2, 3\}$. With this assumption, it turns out that it suffices to consider the 25-element vector $z$ defined in Fig. 1. Since the constraint polynomials are quadratic, when looking for a WOS decomposition for $q_\nu$, we need to consider $s_{ij}$ in Eq. (9) as an arbitrary polynomial of $A_i, B_j$ and $C_k$ with degree at most 2. Proceeding in a way analogous to what was done for the CHSH inequality and solving the resulting SDP, one obtains the $25 \times 25$ positive semidefinite matrix $\Gamma = \Gamma_{7 \times 7} \bigoplus_{i=1}^{6} \Gamma_{3 \times 3}$, where $\Gamma_{7 \times 7}$ and $\Gamma_{3 \times 3}$ are defined in Fig. 1. It is simple to check that $\Gamma_{7 \times 7}$ and $\Gamma_{3 \times 3}$ are positive semidefinite.

From some simple calculations, it then follows that whenever the constraints $A_i^2 = B_j^2 = C_k^2 = I$ are satisfied, we have

$$
z^\dagger \Gamma z = 3\sqrt{3} I - B_{\text{IKPSY}}.
$$

An explicit sum of squares decomposition may be extracted from this data. For example, a simple calculation shows that $6\sqrt{3} z^\dagger \Gamma z$ is equal to

$$
h_0 + \sum_{j=1}^{2} (h_{+j} h_{+j} + h_{-j} h_{-j}) + \frac{1}{2} \sum_{j,k=1,2,3} h_{j,k}^\dagger h_{j,k},
$$

where

$$
h_0 = 3\sqrt{3} I - B_{\text{IKPSY}},
$$

$$
h_{+j} = A_1 B_2 C_3 + e^{i(2\pi j/3)} A_2 B_3 C_1 + e^{i(4\pi j/3)} A_3 B_1 C_2,
$$

$$
h_{-j} = A_1 B_3 C_2 + e^{i(2\pi j/3)} A_2 B_1 C_3 + e^{i(4\pi j/3)} A_3 B_2 C_1,
$$

$$
h_{j,k} = A_j B_k C_k + A_j B_k C_{j,k} + A_k B_j C_j \quad j \neq k.
$$

We refer the reader to [13] for further details.

6 Acknowledgements

We thank Stefano Pironio and Tsuyoshi Ito for interesting discussions and for sharing drafts of their papers [31, 21]. AD and YCL are supported by the Australian Research Council. BT is supported by the EU FP6-FET Integrated Project QAP CT-015848, NWO VICI project 639-023-302, and the Dutch BSIK/BRICKS project. SW is supported by NSF grant PHY-0456720.

References


