Monogamy of non-local quantum correlations

BY BEN TONER 1,2, *

1 Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
2 Institute for Quantum Information, California Institute of Technology, Pasadena, CA 91125, USA

We describe a new technique for obtaining Tsirelson bounds, which are upper bounds on the quantum value of a Bell inequality. Since quantum correlations do not allow signalling, we obtain a Tsirelson bound by maximizing over all no-signalling probability distributions. This maximization can be cast as a linear programme. In a setting where three parties, A, B and C, share an entangled quantum state of arbitrary dimension, we (i) bound the trade-off between AB’s and AC’s violation of the Clauser–Horne–Shimony–Holt inequality and (ii) demonstrate that forcing B and C to be classically correlated prevents A and B from violating certain Bell inequalities, relevant for interactive proof systems and cryptography.

Keywords: quantum; non-locality; Bell inequality; interactive proof systems

1. Introduction

One of the remarkable properties of quantum entanglement is that it is monogamous: if Alice (A), Bob (B) and Charlie (C) each have a qubit, and A and B are maximally entangled, then C’s qubit must be completely uncorrelated with either A’s or B’s. This property is inherently non-classical: if A, B and C have bits instead of qubits, and A’s bit is always the same as B’s bit, then there is no restriction on how A’s bit is correlated with C’s bit. In this work, we consider the correlations that result from making local measurements on a multipartite quantum system. Some such quantum correlations violate Bell (1964) inequalities. We show how these correlations, termed non-local, can also be monogamous.

Consider, for example, the well-known Clauser–Horne–Shimony–Holt (CHSH) inequality (Clauser et al. 1969). Two parties, A and B, share a quantum state $\rho$, and each chooses one of two observables to measure on their component of the state. Define the CHSH operator

\[ B_{\text{CHSH}} = A_1 \otimes (B_1 + B_2) + A_2 \otimes (B_1 - B_2), \]

where $A_1$ and $A_2$ ($B_1$ and $B_2$) are A’s (B’s) observables and are Hermitian operators with spectrum in $[-1, +1]$. Then the CHSH inequality states that $|\langle B_{\text{CHSH}} \rangle_{\text{LHV}}| \leq 2$, for all local hidden variable (LHV) models. There are, however, entangled states, e.g. the singlet state of two qubits $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, such that

* Address for correspondence: Centrum voor Wiskunde en Informatica Kruislaan 413, 1098 SJ Amsterdam, The Netherlands (bentoner@bentoner.com).
Thus the correlations arising from measuring this state cannot be described by any LHV model. In fact, it is true that $|\text{tr}(\mathcal{B}_{\text{CHSH}}\rho)| \leq 2\sqrt{2}$ for all observables $A_1$, $A_2$, $B_1$ and $B_2$, and all states $\rho$. Such a bound on the maximum entangled value of a Bell inequality is termed a Tsirelson bound (Cirel’son 1980). Although we do not yet know how to calculate the best such bound for an arbitrary Bell inequality, a number of ad hoc techniques have been developed (Cirel’son 1980; Tsirelson 1987; Buhrman & Massar 2004; Cleve et al. 2004; Masanes 2005; Navascués et al. 2007, 2008; Doherty et al. 2008).

In this paper, we introduce a new technique for obtaining Tsirelson bounds. Since local measurements on spatially separated components of a multipartite quantum system can be carried out simultaneously, such measurements cannot be used to send a signal from one party to another. The outcomes of local measurements on an entangled quantum state are therefore described by a no-signalling probability distribution. Maximization over all no-signalling probability distributions can be cast as a linear programme, and so we obtain an upper bound by solving this linear programme. This gives an efficient algorithm for obtaining Tsirelson bounds.

We use this new technique to study the monogamy of quantum and no-signalling correlations. Suppose that three parties, A, B and C, share an entangled quantum state of arbitrary dimension. We start by bounding the trade-off between AB’s and AC’s violation of the CHSH inequality. Thus, we prove an analogue for quantum correlations of the famous theorem of Coffman et al. (2000), which describes the trade-off between how entangled A is with B, and how entangled A is with C.

In our second application, we illustrate a way to prevent A and B from violating a Bell inequality, even if they can share an arbitrary entangled state. We do this by introducing an extra party C, and forcing one of the parties, say B, to be classically correlated with C. For the odd-cycle Bell inequality of Cleve et al. (2004), we prove that the presence of C prevents A and B from violating the Bell inequality at all. Finding methods to prevent entangled parties from violating Bell inequalities is important because it allows us to extend results about the computational hardness of computing the classical value of a Bell inequality to the quantum domain. Indeed, subsequent to the work described in this paper, Kempe et al. (in press) have used the same idea (but entirely different proof techniques) to show that it is NP-hard to calculate, or even to approximate to exponential precision, the entangled value of a three-player Bell inequality.

Our second result also has a cryptographic interpretation. Suppose that A and B are trying to share a secret key, and that C is eavesdropping on them. If A and B observe correlations that would cause them to win the two-player odd-cycle game with a probability greater than $1 - 1/2n$, then this limits how correlated C can be with B. Barrett et al. (2005) have presented a key distribution protocol along these lines, which is provably secure against no-signalling eavesdroppers (see also Acín et al. 2006).

The rest of this paper is structured as follows. After defining our framework in §2, we describe the linear programme in §3. We then present our applications: in §4, we study the monogamy of the CHSH inequality, while in §5 we study the odd-cycle Bell inequality.
2. Framework

(a) Non-local games

We cast our results in the language of non-local games, also known as cooperative games of incomplete information (see Cleve et al. 2004). Let \( V : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to [0, 1] \) be a function and let \( \pi \) be a probability distribution on \( \mathbb{Z}_2^m \). Then, \( V \) and \( \pi \) define an \( m \)-player non-local game \( G(V, \pi) \) as follows: a referee chooses a set of questions \((q_1, q_2, \ldots, q_m) \in \mathbb{Z}_2^m\) randomly, according to \( \pi \), and sends question \( q_i \) to player \( i \). Each player must answer with a bit \( a_i \). The players are not permitted to communicate after receiving the questions, but they may agree on a strategy before receiving them. They win with probability \( V(a_1, a_2, \ldots, a_m | q_1, q_2, \ldots, q_m) \) (where the ‘|’ in \( V(\cdot | \cdot) \) separates answers from questions). The classical value of a game \( G(V, \pi) \), denoted \( \omega_c(G) \), is the maximum probability with which the players can win, assuming they use purely classical strategies. The quantum value, denoted \( \omega_q(G) \), is the supremum of the winning probabilities obtained using strategies where the players are allowed to share an entangled quantum state. The no-signalling value, denoted \( \omega_{ns}(G) \), is the maximum winning probability, assuming the players are allowed (black box) access to any no-signalling probability distribution. It is clear that \( \omega_c(G) \leq \omega_q(G) \leq \omega_{ns}(G) \).

(b) The CHSH game

We describe how to interpret the CHSH inequality within this framework. The CHSH game \( G_{\text{CHSH}} \) is defined by setting \( m = n = 2 \), letting \( \pi \) be the uniform distribution on \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) and letting \( V(a_1, a_2 | q_1, q_2) = [a_1 \oplus a_2 = q_1 \land q_2] \), where \( a_1 \oplus a_2 \) is the exclusive-or of bits \( a_1 \) and \( a_2 \), and \( q_1 \land q_2 \) is the and of bits \( q_1 \) and \( q_2 \), and \([\phi] = 1 \) if \( \phi \) is true and \( 0 \) otherwise. Then, the winning probability of a particular strategy is \( 1/2 + \langle B_{\text{CHSH}} \rangle / 8 \), where \( B_{\text{CHSH}} \) is the CHSH operator of equation (1.1) and \( \langle \cdot \rangle \) is the appropriate expectation value for the strategy, classical, quantum or no-signalling. It follows that \( \omega_c(G_{\text{CHSH}}) = 3/4, \omega_q(G_{\text{CHSH}}) = 1/2 + 1/(2\sqrt{2}) \approx 0.85 \) and \( \omega_{ns}(G_{\text{CHSH}}) = 1 \).

(c) Classical correlation restricts Bell inequality violation

Consider a two-player game \( G(V, \pi) \) that is played by A and B\(_0\). Here, we review the work of Masanes et al. (2006), who show how forcing B\(_0\) to be classically correlated with additional players B\(_1\), B\(_2\), ..., B\(_N\) restricts the advantage that A and B\(_0\) can gain by sharing entanglement.

For \( N \geq 1 \), define the \( N \)th extension of a two-player game \( G(V, \pi) \) to be the \((N+2)\)-player game \( G_N(V_N, \pi_N) \), with \( \pi_N \) defined by choosing \((q_1, q_2)\) according to \( \pi \) and setting \( q_2 = q_3 = q_4 = \cdots = q_{N+2} \), and

\[
V_N(\{a_i\}|\{q_i\}) = V(a_1, a_2 | q_1, q_2) \times [a_2 = a_3 = a_4 = \cdots = a_{N+2}]. \tag{2.1}
\]

We also set \( G_0 = G \). The idea is that we send B\(_0\)'s question to the other B\(_i\) and the players win if (i) the answers A and B\(_0\) satisfy the winning condition of \( G(V, \pi) \) and (ii) all the B\(_i\) agree.

**Theorem 2.1 (Result 1 of Masanes et al. (2006)).** Let \( G(V, \pi) \) be a two-player game. Then, the values of its extensions satisfy
(i) \(\omega_c(G_N) = \omega_c(G)\) for all \(N\) and
(ii) \(\omega_{\text{ns}}(G_N)\) is a non-increasing sequence in \(N\), with \(\omega_{\text{ns}}(G_{n-1}) = \omega_c(G)\), where \(n\) is the number of possible questions for \(B_0\) in \(G\).

Terhal et al. (2003), building on the work of Werner (1989), earlier proved a similar result for \(\omega_q(G_N)\).

3. Tsirelson bounds by linear programming

An \(m\)-party no-signalling probability distribution is a set of probabilities

\[
p(\{a_i\}_{i=1}^m | \{q_i\}_{i=1}^m),
\]

subject to
(i) Positivity. For all \(\{a_i\}\) and all \(\{q_i\}\), \(p(\{a_i\}|\{q_i\}) \geq 0\),
(ii) Normalization. For all \(\{q_i\}\), \(\sum_{\{a_i\}} p(\{a_i\}|\{q_i\}) = 1\), and
(iii) No-signalling. For each subset \(S \subset \mathbb{Z}_m\) of the \(m\) parties, the marginal probability distribution on \(\mathbb{Z}_m - S\) must be independent of the inputs of the parties in \(S\). In particular, \(\sum_{\{a_i; i \in S\}} p(\{a_i\}|\{q_i\})\) must be independent of \(\{q_i; i \in S\}\) for all \(\{a_i; i \notin S\}\) and for all \(\{q_i; i \notin S\}\).

The no-signalling value of \(G\) is given by

\[
\omega_{\text{ns}}(G) = \max_p \sum_{\{a_i, q_i\}} \pi(\{q_i\}) \mathcal{V}(\{a_i\}|\{q_i\}) p(\{a_i\}|\{q_i\}),
\]

where the maximization is performed over all conditional probability distributions \(p = p(\{a_i\}_{i=1}^m | \{q_i\}_{i=1}^m)\), subject to the three sets of linear constraints enumerated above. We observe that \(\omega_{\text{ns}}(G)\) is the solution to a linear programme in variables \(p(\{a_i\}|\{q_i\})\). Solving this programme for \(\omega_{\text{ns}}(G)\) gives an upper bound on \(\omega_q(G)\). Moreover, even if we cannot solve the linear programme, we can obtain an upper bound on \(\omega_{\text{ns}}(G)\) by constructing a solution to the dual programme (see Boyd & Vandenberghe (2004) for an introduction to convex optimization).

Note that for the CHSH game, the no-signalling value \(\omega_{\text{ns}}(G_{\text{CHSH}}) = 1\) (Popescu & Rohrlich 1994), so the linear-programming technique provides only a trivial bound on \(\omega_q(G_{\text{CHSH}})\).

4. An analogue of the Coffman–Kundu–Wootters theorem for non-local quantum correlations

Suppose three parties, A, B and C, each have a qubit. There is a well-known theorem of Coffman et al. (2000) that describes the trade-off between how entangled A is with B and how entangled A is with C. It states that \(C_{AB}^2 + C_{AC}^2 \leq 4 \det \rho_A\), where \(C_{AB}\) is the concurrence between A and B; \(C_{AC}\) is the concurrence between A and C; and \(\rho_A\) is the reduced density matrix of A.

To derive a similar expression for correlations, we consider a generalization of the CHSH game to three players, suggested by Michael Nielsen (see also Scarani & Gisin 2001). In the new game, \(G'_{\text{CHSH}}\), the referee sends bits chosen uniformly at random to each of the three players, and with probability 1/2 checks if
\[ a_1 \oplus a_2 = q_1 \land q_2 \text{ and with probability } 1/2 \text{ checks if } a_1 \oplus a_3 = q_1 \land q_3. \]

Formally, \( \pi \) is uniform on \( \mathbb{Z}_2^3 \) and

\[
V(a_1, a_2, a_3|q_1, q_2, q_3) = \frac{1}{2}[a_1 \oplus a_2 = q_1 \land q_2] + \frac{1}{2}[a_1 \oplus a_3 = q_1 \land q_3]. \tag{4.1}
\]

Then, the winning probability of a particular strategy is

\[
\frac{1}{2} + \frac{1}{16} \langle B^{AB}_{\text{CHSH}} \rangle + \frac{1}{16} \langle B^{AC}_{\text{CHSH}} \rangle, \tag{4.2}
\]

where the superscripts denote on which parties the CHSH operator acts. It is easy to see that \( \omega_c(G'_{\text{CHSH}}) = 3/4 \) (a strategy where everyone always answers 0 achieves this, and this strategy is the best possible, by the CHSH inequality applied to AB and BC separately). It turns out that \( \omega_{\text{ns}}(G'_{\text{CHSH}}) = 3/4 \) too, as is easily verified using linear-programming software, which implies the following theorem.

**Theorem 4.1.** Suppose three parties, A, B and C, share any quantum state \( \rho \) (of arbitrary dimension) and each chooses to measure one of two observables. Then,

\[
|\text{tr}(B^{AB}_{\text{CHSH}})\rangle + |\text{tr}(B^{AC}_{\text{CHSH}})\rangle \leq 4. \tag{4.3}
\]

Theorem 4.1 establishes a trade-off between AB’s and AC’s violation of the CHSH inequality. In particular, CHSH correlations are monogamous: if AB violates the CHSH inequality, then AC cannot, as has already been shown for no-signalling correlations by Masanes et al. (2006). Note that if AB and AC each share an EPR pair, there are measurements such that either \( \text{tr}(B^{AB}_{\text{CHSH}}) \) or \( \text{tr}(B^{AC}_{\text{CHSH}}) \) is \( 2\sqrt{2} \), which at first appears to contradict theorem 4.1. It does not: in theorem 4.1, we insist that A’s observables are the same in \( \text{tr}(B^{AB}_{\text{CHSH}}) \) and \( \text{tr}(B^{AC}_{\text{CHSH}}) \). This is in the same spirit as the requirement of Coffman–Kundu–Wootters that B and C are entangled with the same qubit of A. In the following corollary we generalize this result.

**Corollary 4.2.** Suppose that \( N+2 \) parties \( A, B_0, B_1, \ldots, B_N \) share a quantum state and each chooses to measure one of two observables. Then, A violates the CHSH inequality with at most one of the \( B_i \).

**Proof.** Suppose A violates the CHSH inequality with both \( B_j \) and \( B_k \), then \( j \neq k \). Trace out the rest of the \( B_i \)’s. We obtain a contradiction with theorem 4.1.

For no-signalling probability distributions, we also have a converse of theorem 4.1: for any pair \( (\langle B^{AB}_{\text{CHSH}} \rangle, \langle B^{AC}_{\text{CHSH}} \rangle) \) consistent with inequality (4.3), there is a no-signalling probability distribution with these expectation values. This is because we can write \( (\langle B^{AB}_{\text{CHSH}} \rangle, \langle B^{AC}_{\text{CHSH}} \rangle) \) as a convex combination of \((4, 0),(0, 4)\) and \((0, 0)\), each of which is achieved by a no-signalling probability distribution. Thus, inequality (4.3) establishes precisely which values of \( (\langle B^{AB}_{\text{CHSH}} \rangle, \langle B^{AC}_{\text{CHSH}} \rangle) \) are allowed. For quantum theory, Toner & Verstraete (2006) have subsequently shown that the allowed region is described by \( \langle B^{AB}_{\text{CHSH}} \rangle^2 + \langle B^{AC}_{\text{CHSH}} \rangle^2 \leq 8. \)
5. The odd-cycle game

Our second example illustrates how violation of a Bell inequality can preclude classical correlation with another party. We start with a two-player game based on an interactive proof for graph colourability. Imagine that the two players, A and B, are trying to convince the referee that an odd cycle of length $n$ is two-colourable (which it is not, as $n$ is odd). The referee sends them each the name of a vertex, such that the two vertices are either the same or adjacent. A and B each send one of two colours back to the referee. The referee requires that, when the vertices are the same, the two colours should agree and, when the vertices are adjacent, the colours should differ. Formally, we define a two-player game $G_{OC}$ as follows: let $n \geq 3$ be an odd integer, let $\pi$ be uniform over the set $\{(q_1, q_2) \in \mathbb{Z}_n \times \mathbb{Z}_n : q_1 = q_2 \text{ or } q_1 + 1 \equiv q_2 \pmod{n}\}$ and let $V$ be defined by $V(a_1, a_2 | q, q) = [a_1 = a_2], \quad V(a_1, a_2 | q, q + 1) = [a_1 \neq a_2].$ It is established by Braunstein & Caves (1990) and Cleve et al. (2004) that $\omega_c(G_{OC}) = 1 - 1/2n$ and $\omega_q(G_{OC}) = \cos^2(\pi/4n)$.

Now consider the first extension of this game, which we denote $G'_{OC}$. Formally, $G'_{OC}$ is defined by using the same distribution as $G_{OC}$ on $(q_1, q_2)$, and setting $q_2 = q_3$. The function $V$ is defined by

\begin{align}
V(a_1, a_2, a_3 | q, q, q) &= [a_1 = a_2 = a_3], \\
V(a_1, a_2, a_3 | q, q + 1, q + 1) &= [a_1 \neq a_2 = a_2].
\end{align}

Theorem 2.1 implies that $\omega_c(G'_{OC}) = \omega_q(G_{OC}) = 1 - 1/2n$. We show that sharing entanglement (or indeed no-signalling correlations) gives no advantage for $G'_{OC}$.

**Theorem 5.1.** For the first extension of the odd-cycle game,

\begin{equation}
\omega_c(G'_{OC}) = \omega_q(G'_{OC}) = \omega_{ns}(G'_{OC}) = 1 - \frac{1}{2n}.
\end{equation}

This result is remarkable because it establishes that adding just one additional player is sufficient to prevent A and B from gaining advantage by sharing entanglement, rather than the $n-1$ additional players required in theorem 2.1. In the context of interactive proof systems, we can interpret the fact that $\omega_q(G_{OC}) > \omega_c(G_{OC})$ in the two-player game as saying that sharing entanglement allows the provers to cheat, because it increases the probability with which they are able to convince the referee that the odd cycle is two-colourable. Theorem 5.1 shows that we can counter this by adding an extra prover, and forcing B to be classically correlated with this prover. This placed no extra burden on classical provers, because an optimal classical strategy is deterministic, but it prevents quantum provers from gaining any advantage by sharing entanglement.

Recently, Raz (in press) studied how the classical value of the odd-cycle game behaves under parallel repetition. A parallel repetition of an $m$-player game $G(V, \pi)$ is, roughly speaking, a game where the $m$-players try to win $k>1$ instances of the game simultaneously. More formally, for each $j=1, \ldots, k$, the referee samples questions $(q_{i,j}, \ldots, q_{m,j})$ according to $\pi$. (Questions with different values of $j$ are independent.) The referee then sends questions $q_{i,1}, \ldots, q_{i,k}$ to player $i$. Player $i$ is expected to return $k$ answers, labelled $a_{i,1}, \ldots, a_{i,k}$. The
players win if for all $j=1, \ldots, k$ it is true that $V(a_{1,j}, \ldots, a_{m,j}|q_{1,j}, \ldots, q_{m,j}) = 1$. We write $G^k$ for the $k$-fold parallel repetition of a game $G$. It is immediately clear that

$$\omega(G^k) \geq \omega(G)^k,$$

(5.4)

because the players can just play each instance of the game independently, using an optimal strategy for each instance.

Specializing now to the odd-cycle game, for the quantum value, the inequality in equation (5.4) is actually tight: Cleve et al. (2007) have proved that

$$\omega_q(G^k_{OC}) = \omega_q(G_{OC})^k,$$

(5.5)

a result known as a strong parallel repetition theorem. What is surprising is that equation (5.4) is not tight for the classical value: Raz (in press) has shown that equation (5.4) can be improved to

$$\omega_c(G^k_{OC}) \geq 1 - \frac{1}{n} O(\sqrt{k}),$$

(5.6)

whereas equation (5.4) gives only $\omega_c(G^k_{OC}) \geq (1 - 1/2n)^k$. (We note that equation (5.6) is itself almost tight, up to logarithmic factors; Feige et al. 2007.) This is a counterexample to strong parallel repetition in the classical case.

Theorem 5.1 gives rise to a similar counterexample for the quantum (and no-signalling) values of three-player games. Consider the first extension of the odd-cycle game, $G'_{OC}$. Observe that

$$\omega_{ns}(G'^k_{OC}) \geq \omega_q(G'^k_{OC}) \geq \omega_c(G'^k_{OC}) = \omega_c(G^k_{OC}) \geq 1 - \frac{1}{n} O(\sqrt{k}),$$

(5.7)

where the first two inequalities are obvious, the equality follows from theorem 2.1(i), and the second inequality is equation (5.6). Comparing this to $\omega_q(G'_{OC}) = 1 - 1/2n$, as established in theorem 5.1, we observe that $G'_{OC}$ is a counterexample to strong parallel repetition in the quantum case. The same remarks apply in the no-signalling case.

Proof of theorem 5.1. Throughout this proof, the addition of elements in $\mathbb{Z}_n$ is understood to be taken modulo $n$. There are a number of symmetries we can use to simplify the problem. Without changing the probability of winning:

(i) all parties can flip the binary value of their outputs, and/or
(ii) all parties can add an integer to their inputs, and/or
(iii) B and C can exchange roles.

For a given no-signalling strategy, let $p(a, b, c|i, j, k)$ be the probability that $(A, B, C)$ answer $(a, b, c)$ when asked $(i, j, k)$. Then, we can take $p(a, b, c|i, j, k)$ to be symmetric under these three symmetries. In particular, symmetry (i) implies we can restrict attention to $a=0$ and symmetry (ii) to $i=0$. Therefore, let $r(b, c|j, k) = p(0, b, c|0, j, k)$. We shall use symmetry (iii) to give extra constraints, rather than to reduce the number of parameters.
We rewrite the primary linear programme in these variables, labelling the constraints to facilitate writing down the dual programme. Our goal is to maximize

\[ \omega_{ns}(G'_{0C}) = \frac{1}{2} \max_r [r(0,0|0,0) + r(1,1|1,1)], \] (5.8)

subject to

— (normalization) \( n(j,k), \)

\[ \sum_{b,c} r(b,c|j,k) = 1, \] (5.9)

for \( 0 \leq j, k < n, \)

— (symmetry) \( s(b,c|j,k), \)

\[ r(b,c|j,k) = r(c,b|k,j), \] (5.10)

for \( b, c \in \{0,1\}, 0 \leq j,k < n; \) note that, when \( b = c \) and \( j = k, \) this constraint is trivial,

— (no-signalling conditions, A to BC) \( y(d|j,k), \)

\[ r(0,d|j,j+k) + r(1,1-d|j,j+k) = r(0,d|0,k) + r(1,1-d|0,k), \] (5.11)

for \( d \in \{0,1\}, 1 \leq j < n, 0 \leq k < n, \)

— (no-signalling conditions, B to AC) \( z(d|j,k), \)

\[ r(0,d|j,k) + r(1,d|j,k) = r(0,d|0,k) + r(1,d|0,k), \] (5.12)

for \( d \in \{0,1\}, 1 \leq j < n, 0 \leq k < n. \)

We omit the no-signalling conditions in the other directions (BC to A and AC to B), which do not further constrain the solution.

Each constraint in the primary linear programme corresponds to a variable in the dual, as labelled above. The objective of the dual programme is to minimize

\[ \frac{1}{2n} \sum_{j,k} n(j,k), \] (5.13)

subject to the constraints \( \mu(0,0|0,0), \mu(1,1|1,1) \geq n, \mu(b,c|j,k) \geq 0, \) for all \( b, c \in \{0,1\}, 0 \leq j, k < n, \) where

\[ \mu(b,c|j,k) = n(j,k) + s(b,c|j,k) - s(c,b|k,j) \]

\[ + [j = 0] \sum_{j' = 1}^{n-1} \left( y\left( \frac{1-2bc}{2}, j', k \right) + z(c|j', k) \right) \]

\[ - [j \neq 0] \left( y\left( \frac{1-2bc}{2}, j, k-j \right) + z(c|j,k) \right). \] (5.14)

We now give an explicit solution to the dual. This solution was constructed by numerically solving the linear programme for small \( n, \) iteratively converting the inequality constraints into a consistent set of equality conditions by generalizing from the small \( n \) solutions, and then inverting these constraints to yield the solution. While we used numerical methods to obtain the solution, we emphasize that the final solution can be checked analytically, without any need for numerical
computation. The non-zero variables are

\[ n(0, 0) = 2n - 1, \] (5.15)

\[ s(0, 1|0, 0) = 3n/2, \] (5.16)

\[ s(0, 1|1, 0) = -n + 1, \] (5.17)

\[ s(0, 0|0, 1) = -n + 1, \] (5.18)

\[ s(0, 1|1, 1) = -n/2, \] (5.19)

\[ s(0, 0|j, j + 1) = (-1)^j, \quad \text{for } j = 1, 2, \ldots, n - 1, \] (5.20)

\[ s(0, 1|j, j + 1) = -(-1)^j, \quad \text{for } j = 1, 2, \ldots, n - 1, \] (5.21)

\[ y(0|1, 0) = -2n + 3, \] (5.22)

\[ y(0|1, k) = -n + k + 5/2 + (-1)^k/2, \quad \text{for } k = 1, 2, \ldots, n - 1, \] (5.23)

\[ y(1|1, 0) = 3 - 3n/2, \] (5.24)

\[ y(1|1, 1) = -n + 4, \] (5.25)

\[ y(1|j, 1) = -(-1)^j, \quad \text{for } j = 2, 3, \ldots, n - 1, \] (5.26)

\[ y(1|1, k) = -n + k + 5/2 + (-1)^k/2, \quad \text{for } k = 2, 3, \ldots, n - 2, \] (5.27)

\[ y(1|1, n - 1) = -n + 3, \] (5.28)

\[ y(1|j, n - 1) = 1 - (-1)^j, \quad \text{for } j = 2, 3, \ldots, n - 1, \] (5.29)

\[ z(0|1, 0) = n - 3, \] (5.30)

\[ z(0|1, 1) = 2n - 3, \] (5.31)

\[ z(0|1, 2) = n - 4, \] (5.32)

\[ z(0|j, j - 1) = -1, \quad \text{for } j = 2, 3, \ldots, n - 1, \] (5.33)
Substituting into equation (5.13), we find that
\[ u_m \]

\[ \rho_{z|j, j + 1} = (-1)^j, \quad \text{for } j = 2, 3, \ldots, n - 1, \]  
\[ \rho_{z|1, k} = n - k - 3/2 + (-1)^k/2, \quad \text{for } k = 3, 4, \ldots, n - 1, \]  
\[ \rho_{z|1, j - 1} = -1 + (-1)^j, \quad \text{for } j = 1, 2, \ldots, n - 1, \]  
\[ \rho_{z|1, k} = n - k - 3/2 + (-1)^k/2, \quad \text{for } k = 1, 2, \ldots, n - 1. \]  

All other variables are zero.

For this solution, it is tedious but straightforward to establish the following:
\[ \mu(0, 0|0, 0) = \mu(1, 1|1, 1) = n, \mu(0, 1|0, 0) = 2n, \mu(1, 0|0, 1) = 2n - 2, \mu(0, 0|j, j - 1) = 1 + (-1)^j \text{ for } j = 1, 2, \ldots, n - 1; \mu(1, 1|k + 1, k) = 1 + (-1)^k \text{ for } k = 1, 2, \ldots, n - 1; \text{and } \mu(b, c|j, k) = 0, \text{ otherwise.} \]  
Thus, our solution satisfies the constraints. Substituting into equation (5.13), we find that \( \omega_{ns}(G'_OC) \leq 1 - 1/2n \), which proves theorem 5.1.

I thank Richard Cleve, John Preskill, Graeme Smith, Frank Verstraete and John Watrous for their useful suggestions, and Michael Nielsen for suggesting theorem 4.1. This work was supported in part by the NSF under grant no. PHY-456720, the ARO under grant no. W911NF-05-1-0294, the EU FP6-FET Integrated Project QAP CT-015848, NWO VICI project 639-023-302 and the Dutch BSIK/BRICKS project.

References

Acín, A., Gisin, N. & Masanes, L. 2006 From Bell’s theorem to secure quantum key distribution. Phys. Rev. Lett. 97, 120 405. (doi:10.1103/PhysRevLett.97.120405)

Barrett, J., Hardy, L. & Kent, A. 2005 No signaling and quantum key distribution. Phys. Rev. Lett. 95, 010 503. (doi:10.1103/PhysRevLett.95.010503)

Bell, J. S. 1964 On the Einstein–Podolsky–Rosen paradox. Physics 1, 195–200.

Boyd, S. & Vandenberghe, L. 2004 Convex optimization. Cambridge, UK: Cambridge University Press. (http://www.stanford.edu/~boyd/cvxbook/)

Braunstein, S. & Caves, C. 1990 Wringing out better Bell inequalities. Ann. Phys. (NY) 202, 22–56. (doi:10.1016/0003-4916(90)90339-P)

Bvhrman, H. & Massar, S. 2004 Causality and Cirel’son bounds. (http://arXiv.org/abs/quant-ph/0409066)

Cirel’son, B. S. 1980 Quantum generalizations of Bell’s inequality. Lett. Math. Phys. 4, 93–100. (doi:10.1007/BF00417500)

Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. 1969 Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. 23, 880–884. (doi:10.1103/PhysRevLett.23.880)

Cleve, R., Høyer, P., Toner, B. & Watrous, J. 2004 Consequences and limits of nonlocal strategies. In Proc. 19th IEEE Conf. on Computational Complexity (CCC 2004), pp. 236–249. (http://arXiv.org/abs/quant-ph/0404076)

Cleve, R., Složstra, W., Unger, F. & Upadhyay, S. 2007 Perfect parallel repetition theorem for quantum XOR proof systems. In Proc. 22nd IEEE Conf. on Computational Complexity (CCC 2007), pp. 109–114.

Coffman, V., Kundu, J. & Wootters, W. K. 2000 Distributed entanglement. Phys. Rev. A 61, 052 306. (doi:10.1103/PhysRevA.61.052306)
Doherty, A. C., Liang, Y.-C., Toner, B. & Wehner, S. 2008 The quantum moment problem and bounds on entangled multi-prover games. In Proc. 23rd IEEE Conf. on Computational Complexity (CCC 2004). (http://arXiv.org/abs/0803.4373)

Feige, U., Kindler, G. & O’Donnell, R. 2007 Understanding parallel repetition requires understanding foams. In Proc. 22nd IEEE Conf. on Computational Complexity (CCC 2007), pp. 179–192.

Kempe, J., Kobayashi, H., Matsumoto, K., Toner, B. & Vidick, T. In press. Entangled games are hard to approximate. In Proc. 49th IEEE Symp. on Foundations of Computer Science (FOCS 2008). (http://arXiv.org/abs/0704.2903)

Masanes, L. 2005 Extremal quantum correlations for N parties with two dichotomic observables per site. See http://arXiv.org/abs/quant-ph/0512100.

Masanes, L., Acín, A. & Gisin, N. 2006 General properties of nonsignaling theories. Phys. Rev. A 73, 012 112. (doi:10.1103/PhysRevA.73.012112)

Navascués, M., Pironio, S. & Acín, A. 2007 Bounding the set of quantum correlations. Phys. Rev. Lett. 98, 010 401. (doi:10.1103/PhysRevLett.98.010401)

Navascués, M., Pironio, S. & Acín, A. 2008 A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. New J. Phys. 10, 073 013. (http://arXiv.org/abs/0803.4290)

Popescu, S. & Rohrlich, D. 1994 Nonlocality as an axiom. Found. Phys. 24, 379. (doi:10.1007/BF02058098)

Raz, R. In press. A counterexample to strong parallel repetition. In Proc. 49th IEEE Symp. on Foundations of Computer Science (FOCS 2008). ECCC report TR08-018.

Scarani, V. & Gisin, N. 2001 Quantum communication between n partners and Bell’s inequalities. Phys. Rev. Lett. 87, 117 901. (doi:10.1103/PhysRevLett.87.117901)

Terhal, B. M., Doherty, A. C. & Schwab, D. 2003 Symmetric extensions of quantum states and local hidden variable theories. Phys. Rev. Lett. 90, 157 903. (doi:10.1103/PhysRevLett.90.157903)

Toner, B. F. & Verstraete, F. 2006 Monogamy of Bell correlations and Tsirelson’s bound. (http://arXiv.org/abs/quant-ph/0611001)

Tsirelson, B. S. 1987 Quantum analogues of the Bell inequalities. The case of two spatially separated domains. J. Sov. Math. 36, 557–570. (doi:10.1007/BF01663472)

Werner, R. F. 1989 An application of Bell’s inequalities to a quantum state extension problem. Lett. Math. Phys. 17, 359–363. (doi:10.1007/BF00399761)