computational complexity

PERFECT PARALLEL REPETITION THEOREM FOR QUANTUM XOR PROOF SYSTEMS

RICHARD CLEVE, WILLIAM SLOFSTRA, FALK UNGER,
AND SARVAGYA UPADHYAY

Abstract. We consider a class of two-prover interactive proof systems where each prover returns a single bit to the verifier and the verifier's verdict is a function of the XOR of the two bits received. We show that, when the provers are allowed to coordinate their behavior using a shared entangled quantum state, a perfect parallel repetition theorem holds in the following sense. The prover's optimal success probability for simultaneously playing a collection of XOR proof systems is exactly the product of the individual optimal success probabilities. This property is remarkable in view of the fact that, in the classical case (where the provers can only utilize classical information), it does not hold. The theorem is proved by analyzing parities of XOR proof systems using semidefinite programming techniques, which we then relate to parallel repetitions of XOR games via Fourier analysis.

Keywords. Quantum computing, interactive proof systems, parallel repetition.

Subject classification. 81P68, 68Q10.

1. Introduction and summary of results

The theory of interactive proof systems has played an important role in the development of computational complexity and cryptography. Also, the impact of quantum information on the theory of interactive proof systems has been shown to have interesting consequences [18, 23]. In [5] a variant of the model of interactive proof system was introduced where there are two provers who have unlimited computational power subject to the condition that they cannot communicate between themselves once the execution of the protocol starts. This model is sufficiently powerful to characterize NEXP [1].

Our present focus is on *XOR interactive proof systems*, which are based on *XOR games*. For a predicate $f : S \times T \to \{0, 1\}$ and a probability distribution π on $S \times T$, define the XOR game $G = (f, \pi)$ operationally as follows.

- The Verifier selects a pair of questions $(s, t) \in S \times T$ according to distribution π.

- The Verifier sends one question to each prover: s to prover Alice and t to prover Bob (who are forbidden from communicating with each other once the game starts).

- Each prover sends a bit back to the Verifier: a from Alice and b from Bob.

- The Verifier accepts if and only if $a \oplus b = f(s, t)$.

A definition that is essentially equivalent to this[1] appears in [8]. In the classical version, the provers have unlimited computing power, but are restricted to possessing classical information; in the quantum version, the provers may possess qubits whose joint state is entangled. In both versions, the communication between the provers and the verifier is classical.

An *XOR interactive proof system* (with soundness probability s and completeness probability $c > s$) for a language L associates an XOR game with every input string x, such that:

- S_x and T_x consist of strings of length polynomial in $|x|$, π_x can be sampled in time polynomial in $|x|$, and f_x can be computed in time polynomial in $|x|$.

- If $x \in L$ then the maximum acceptance probability over prover's strategies is at least c.

- If $x \notin L$ then the maximum acceptance probability over prover's strategies is at most s.

In [8] it is pointed out that results in [4, 16] imply that, in the case of classical provers, these proof systems have sufficient expressive power to recognize every language in NEXP (with soundness probability $s = 11/16 + \epsilon$ and completeness probability $c = 12/16 - \epsilon$, for arbitrarily small $\epsilon > 0$). Thus, although these proof systems appear restrictive, they can recognize any language that an unrestricted multi-prover interactive proof system can. Moreover, in [9, 25] it is shown that any language recognized by a quantum XOR proof system is in

---

[1]Except that *degeneracies* are allowed, where for some (s, t) pairs, the Verifier is allowed to accept or reject independently of the value of $a \oplus b$. All results quoted here apply to nondegenerate games.

EXP. Thus, assuming EXP $\neq$ NEXP, quantum entanglement strictly weakens the expressive power of XOR proof systems.

Returning to XOR games, quantum physicists have, in a sense, been studying them since the 1960s, when John Bell introduced his celebrated results that are now known as Bell inequality violations [3]. An example is the *CHSH* game, named after the authors of [7]. In this game, $S = T = \{0, 1\}$, π is the unform distribution on $S \times T$, and $f(s, t) = s \wedge t$. It is well known that, for the *CHSH* game, the best possible classical strategy succeeds with probability $3/4$, whereas the best possible quantum strategy succeeds with higher probability of $(1 + 1/\sqrt{2})/2 \approx 0.85$ [7, 21].

Following [8], for an XOR game G, define its *classical value* $\omega_c(G)$ as the maximum possible success probability achievable by a classical strategy. Similarly, define its *quantum value* $\omega_q(G)$ as the maximum possible success probability achievable by a quantum strategy.

1.1. Taking the sum of XOR games. For any two XOR games $G_1 = (f_1, \pi_1)$ and $G_2 = (f_2, \pi_2)$, define their *sum (modulo 2)* as the XOR game

$$(1.1) \qquad\qquad G_1 \oplus G_2 = (f_1 \oplus f_2, \pi_1 \times \pi_2) \,.$$

In this game, the verifier begins by choosing questions $((s_1, t_1), (s_2, t_2)) \in (S_1 \times T_1) \times (S_2 \times T_2)$ according to the product distribution $\pi_1 \times \pi_2$, sending (s_1, s_2) to Alice and (t_1, t_2) to Bob. Alice and Bob then win if and only if their respective outputs, a and b, satisfy $a \oplus b = f_1(s_1, t_1) \oplus f_2(s_2, t_2)$.

A simple way for Alice and Bob (who may or may not share entanglement) to play $G_1 \oplus G_2$ is to optimally play G_1 and G_2 separately, producing outputs a_1, b_1 for G_1 and a_2, b_2 for G_2, and then to output $a = a_1 \oplus a_2$ and $b = b_1 \oplus b_2$ respectively. It is straightforward to calculate that the above method for playing $G_1 \oplus G_2$ succeeds with probability

$$(1.2) \qquad\qquad \omega(G_1)\omega(G_2) + \big(1 - \omega(G_1)\big)\big(1 - \omega(G_2)\big) \,.$$

Is this the optimal way to play $G_1 \oplus G_2$?

The answer is *no* for *classical* strategies. To see why this is so, note that, using this approach for the XOR game *CHSH* $\oplus$ *CHSH*, produces a success probability of $5/8$. A better strategy is for Alice to output $a = s_1 \wedge s_2$ and Bob to output $b = t_1 \wedge t_2$. It is straightforward to verify that this latter strategy succeeds with probability $3/4$.

Our first result is that the answer is *yes* for *quantum* strategies.

THEOREM 1.3 (Additivity). *For any two XOR games G_1 and G_2 an optimal quantum strategy for playing $G_1 \oplus G_2$ is for Alice and Bob to optimally play G_1 and G_2 separately, producing outputs a_1, b_1 for G_1 and a_2, b_2 for G_2, and then to output $a = a_1 \oplus a_2$ and $b = b_1 \oplus b_2$.*

The proof of Theorem 1.3 uses a known characterization of quantum strategies for individual XOR games as semidefinite programs. Section 2 contains the proof.

1.2. Parallel repetition of XOR games. For any sequence of XOR games $G_1 = (f_1, \pi_1)$, ..., $G_n = (f_n, \pi_n)$, define their *conjunction*, denoted by $\wedge_{j=1}^n G_j$, as follows. The verifier chooses questions $((s_1, t_1), \ldots, (s_n, t_n)) \in (S_1 \times T_1) \times \cdots \times (S_n \times T_n)$ according to the product distribution $\pi_1 \times \cdots \times \pi_n$, and sends $(s_1, \ldots, s_n)$ to Alice and $(t_1, \ldots, t_n)$ to Bob. Alice and Bob output bits $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, respectively, and win if and only if their outputs simultaneously satisfy these n conditions: $a_1 \oplus b_1 = f_1(s_1, t_1), \ldots, a_n \oplus b_n = f_n(s_n, t_n)$. (Note that $\wedge_{j=1}^n G_j$ is not itself an XOR game for $n > 1$.)

One way for Alice and Bob to play $\wedge_{j=1}^n G_j$ is to independently play each game optimally. This succeeds with probability $\prod_{j=1}^n \omega(G_j)$. Is this the optimal way to play $\wedge_{j=1}^n G_j$?

The answer is *no* for classical strategies. It is shown in [2] that[2] $\omega_c(CHSH \wedge CHSH) = 10/16 > 9/16 = \omega_c(CHSH)\omega_c(CHSH)$.

Our second result is that the answer is *yes* for quantum strategies.

THEOREM 1.4 (Parallel repetition). *For any XOR games $G_1, \ldots, G_n$, we have that $\omega_q(\wedge_{j=1}^n G_j) = \prod_{j=1}^n \omega_q(G_j)$.*

This is a quantum version of Raz's parallel repetition theorem [20] for the restricted class of XOR games. We call it a *perfect* parallel repetition theorem because the probabilities are multiplicative in the exact sense (as opposed to an asymptotic sense, as in [20]). The proof of Theorem 1.4 is based on Theorem 1.3 combined with Fourier analysis techniques for boolean functions. Section 3 contains the proof.

1.3. Comparison with other work. There is no known parallel repetition theorem along the lines of [20] for quantum games (where the players share entanglement). As far as we know, our results represent the first progress in

---

[2]After posing this question about $\omega_c(CHSH \wedge CHSH)$, the answer was first shown to us by S. Aaronson, who independently discovered the classical protocol and then found the prior result in [2].

this direction. Recently, Holenstein [17] gave a simplified proof of the parallel repetition theorem that applies to classical and no-signalling strategies. Neither of these cases capture quantum strategies for XOR games (for example, every XOR game has value 1 in the no-signaling model).

For games other than XOR games, the question of parallel repetition remains open. Watrous [24] has shown that, there is a binary game (that is not an XOR game) for which $\omega_q(G) = \omega_q(G \wedge G) = 2/3$, as in the classical case. For completeness, this is shown in Appendix A. This implies that a perfect parallel repetition property does not automatically apply to quantum games.

For a broad class of games, Feige and Lovász [13] define quantities that are relaxations – and hence upper bounds – of their classical values, and show that one of these quantities satisfies a parallel repetition property analogous to Theorem 1.4. For any XOR game G, the Feige–Lovász relaxations of its classical value are equal to the quantum value of G. Although this was also noted previously [11, 12], for completeness, an explicit proof of this is shown in Appendix B. It is important to note that, *for general games*, the relationship between their quantum values and the Feige–Lovász relaxations of their classical values are not understood. As far as we know, neither quantity bounds the other for general games. However, using the fact that they are equivalent for XOR games combined with our Theorem 1.4, we deduce (in Appendix B) that, whenever $G_1, \ldots, G_n$ are XOR games, the quantum value of $\wedge_{j=1}^n G_j$ coincides with its associated Feige–Lovász relaxations. (Note that this does not reduce our Theorem 1.4 to the results in [13], since we invoke Theorem 1.4 to deduce that the quantum value and the Feige–Lovász relaxations are the same for $\wedge_{j=1}^n G_j$.)

2. Proof of the additivity theorem

In this section we prove Theorem 1.3, which is stated in Section 1.1.

It is convenient to define the quantum *bias* of an XOR game as $\varepsilon_q(G) = 2\omega_q(G) - 1$. Then, due to (1.2), to prove Theorem 1.3, it suffices to show that $\varepsilon_q(G_1 \oplus G_2) = \varepsilon_q(G_1)\varepsilon_q(G_2)$.

Since Alice and Bob can independently play games G_1 and G_2 optimally and then take the parity of their outputs as their outputs for $G_1 \oplus G_2$, we immediately have the following.

PROPOSITION 2.1. *For two XOR games G_1 and G_2, $\varepsilon_q(G_1 \oplus G_2) \geq \varepsilon_q(G_1)\varepsilon_q(G_2)$.*

The nontrivial part of the proof is the reverse inequality.

A quantum strategy for an XOR game consists of a bipartite quantum state $|\psi\rangle$ shared by Alice and Bob, a set of observables X_s ($s \in S$) corresponding to Alice's part of the quantum state, and a set of observables Y_t ($t \in T$) corresponding to Bob's part of the state. The bias achieved by this strategy is given by

$$\sum_{s,t} \pi(s,t)(-1)^{f(s,t)} \langle\psi|X_s \otimes Y_t|\psi\rangle \ .$$

We make use of a vector characterization of XOR games due to [22] (also pointed out in [8]), which is a consequence of the following.

THEOREM 2.2 ([8, 22]). *Let S and T be finite sets, and let $|\psi\rangle$ be a pure quantum state with support on a bipartite Hilbert space $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$ such that $dim(\mathcal{A}) = dim(\mathcal{B}) = n$. For each $s \in S$ and $t \in T$, let X_s and Y_t be observables on $\mathcal{A}$ and $\mathcal{B}$ with eigenvalues ± 1 respectively. Then there exists real unit vectors x_s and y_t in $\mathbb{R}^{2n^2}$ such that*

$$\langle\psi|X_s \otimes Y_t|\psi\rangle = x_s \cdot y_t \,,$$

for all $s \in S$ and $t \in T$.

Conversely, suppose that S and T are finite sets, and x_s and y_t are unit vectors in $\mathbb{R}^N$ for each $s \in S$ and $t \in T$. Let $\mathcal{A}$ and $\mathcal{B}$ be Hilbert space of dimension $2^{\lceil N/2 \rceil}$, $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$ and $|\psi\rangle$ be a maximally entangled state on $\mathcal{H}$. Then there exists observables X_s and Y_t with eigenvalues ± 1, on $\mathcal{A}$ and $\mathcal{B}$ respectively, such that

$$\langle\psi|X_s \otimes Y_t|\psi\rangle = x_s \cdot y_t \,,$$

for all $s \in S$ and $t \in T$.

Using Theorem 2.2, we can characterize Alice and Bob's quantum strategies by a choice of unit vectors $\{x_s\}_{s \in S}$ and $\{y_t\}_{t \in T}$. Using this characterization, the bias becomes

$$(2.3) \qquad \varepsilon_q(G) = \max_{\{x_s\},\{y_t\}} \sum_{s,t} \pi(s,t)(-1)^{f(s,t)} \, x_s \cdot y_t \,.$$

The *cost matrix* for the XOR game G is defined as the matrix A with entries $A_{s,t} = \pi(s,t)(-1)^{f(s,t)}$.

Note that any matrix A, with the provision that the absolute values of the entries sum to 1, is the cost matrix of an XOR game. If G_1 and G_2 are XOR games with cost matrices A_1 and A_2 respectively, then the cost matrix

of $G_1 \oplus G_2$ is $A_1 \otimes A_2$. Also, for $0 \leq \lambda \leq 1$, define the convex combination $\lambda G_1 + (1 - \lambda)G_2$ to be the XOR game with cost matrix

$$\begin{pmatrix} 0 & \lambda A_1 \\ (1 - \lambda)A_2 & 0 \end{pmatrix}.$$

This convex combination can be interpreted as the game where, with probability λ, game G_1 is played and, with probability $1 - \lambda$, game G_2 is played (and Alice and Bob are informed about which game is occurring). Also, for a game G with cost matrix A, define G^T to be the game with cost matrix A^T. In other words, Alice and Bob switch places to play G^T. The next proposition summarizes some simple facts.

PROPOSITION 2.4.

(i) $\varepsilon_q(G_1 \oplus G_2) = \varepsilon_q(G_2 \oplus G_1)$ and $\varepsilon_q(G) = \varepsilon_q(G^T)$.

(ii) For all $0 \leq \lambda \leq 1$,

$$\varepsilon_q\big(\lambda G_1 + (1 - \lambda)\,G_2\big) = \lambda\varepsilon_q(G_1) + (1 - \lambda)\,\varepsilon_q(G_2)$$

and

$$G_1 \oplus \big(\lambda G_2 + (1 - \lambda)G_3\big) = \lambda(G_1 \oplus G_2) + (1 - \lambda)(G_1 \oplus G_3).$$

The bias of a quantum XOR game may be stated as a semidefinite programming problem (SDP). We refer to Boyd and Vandenberghe [6] for a detailed introduction to semidefinite programming. For cost matrix A, the bias is equivalent to the objective value of problem

(2.5) $\max \ \mathrm{Tr}\left(A^T U_1^T U_2\right) : \mathrm{diag}\left(U_1^T U_1\right) = \mathrm{diag}\left(U_2^T U_2\right) = \bar{e}\,,$

where $\{x_s\}$ and $\{y_t\}$ appear as the columns of U_1 and U_2 respectively. Here $\mathrm{diag}(M)$ denotes the column vector of diagonal entries of the matrix M, and $\bar{e}$ is the column vector $(1, \ldots, 1)^T$. We begin by considering the game $\frac{1}{2}G + \frac{1}{2}G^T$, whose cost matrix

$$B = \begin{pmatrix} 0 & \frac{1}{2}A \\ \frac{1}{2}A^T & 0 \end{pmatrix}$$

has useful structural properties, one of them being that it is symmetric. Proposition 2.4 implies that $\varepsilon_q(\frac{1}{2}G + \frac{1}{2}G^T) = \varepsilon_q(G)$. This enables us to express the value of game G in terms of the SDP (P_B) defined by

$$\max \ \mathrm{Tr}(BX) \quad : \quad \mathrm{diag}(X) = \bar{e}, \quad X \succeq 0\,.$$

The notation $X \succeq Y$ means that the matrix $X - Y$ lies in the cone of positive semidefinite matrices. That (P_B) is equivalent to problem (2.5) follows from the fact that a semidefinite matrix X can be written as $(U_1, U_2)^T (U_1, U_2)$ for some matrices U_1 and U_2.

To show that an optimal solution for (P_B) exists, we can examine the Lagrange–Slater dual of (P_B). The dual, denoted by (D_B), is defined as

$$\min \ (x, y)\bar{e} \quad : \quad \Delta(x, y) \succeq B \, ,$$

where $\Delta(x, y)$ denotes the diagonal matrix with entries given by the (row) vectors x, y. Both (P_B) and (D_B) have Slater points – that is, feasible points in the interior of the semidefinite cone. Explicitly, the identity matrix is a Slater point for (P_B), and $\bar{e}$ is a Slater point for (D_B). Therefore, by the strong duality theorem, the optimal values of (P_B) and (D_B) are the same and both problems have optimal solutions attaining this value.

The next lemma establishes the upper bound for the game $(\frac{1}{2}G_1 + \frac{1}{2}G_1^T) \oplus (\frac{1}{2}G_2 + \frac{1}{2}G_2^T)$ (which we will show afterwards has the same bias as $G_1 \oplus G_2$).

LEMMA 2.6. *If G_1 and G_2 are XOR games, then*

$$\varepsilon_q \left(\left(\frac{1}{2}G_1 + \frac{1}{2}G_1^T \right) \oplus \left(\frac{1}{2}G_2 + \frac{1}{2}G_2^T \right) \right) \leq \varepsilon_q(G_1)\varepsilon_q(G_2) \, .$$

PROOF.   Let G_1 and G_2 be two games with cost matrices A_1 and A_2, respectively, and let

$$(2.7) \qquad B_1 = \begin{pmatrix} 0 & \frac{1}{2}A_1 \\ \frac{1}{2}A_1^T & 0 \end{pmatrix} \quad \text{and} \quad B_2 = \begin{pmatrix} 0 & \frac{1}{2}A_2 \\ \frac{1}{2}A_2^T & 0 \end{pmatrix} .$$

Let (x_1, y_1) and (x_2, y_2) be optimal solutions to (D_{B_1}) and (D_{B_2}), respectively, which implies $\Delta(x_i, y_i) - B_i \succeq 0$ and $\varepsilon_q(G_i) = (x_i, y_i)\bar{e}$, for $i = 1, 2$. It suffices to show that $(x_1, y_1) \otimes (x_2, y_2)$ is a solution to $(D_{B_1 \otimes B_2})$, since $B_1 \otimes B_2$ is the cost matrix of $(\frac{1}{2}G_1 + \frac{1}{2}G_1^T) \oplus (\frac{1}{2}G_2 + \frac{1}{2}G_2^T)$. Note that, for *arbitrary* B_1 and B_2, $\Delta(x_1, y_1) \succeq B_1$ and $\Delta(x_2, y_2) \succeq B_2$ does *not* imply that $\Delta(x_1, y_1) \otimes \Delta(x_2, y_2) \succeq B_1 \otimes B_2$ (a simple counterexample is when $\Delta(x_1, y_1) = \Delta(x_2, y_2) = 0$ and $B_1 = B_2 = -I$). We make use of the structure of B_1 and B_2 arising from (2.7). For each i, $\Delta(x_i, y_i) - B_i \succeq 0$ implies that, for all (row) vectors u, v,

$$0 \leq \begin{pmatrix} u & v \end{pmatrix} \begin{pmatrix} \Delta(x_i) & -\frac{1}{2}A_i \\ -\frac{1}{2}A_i^T & \Delta(y_i) \end{pmatrix} \begin{pmatrix} u^T \\ v^T \end{pmatrix}$$

$$= \begin{pmatrix} u & -v \end{pmatrix} \begin{pmatrix} \Delta(x_i) & +\frac{1}{2}A_i \\ +\frac{1}{2}A_i^T & \Delta(y_i) \end{pmatrix} \begin{pmatrix} u^T \\ -v^T \end{pmatrix} ,$$

which in turn implies that $\Delta\,(x_i, y_i) + B_i \succeq 0$ also holds. Therefore,

$$\big(\Delta(x_1, y_1) - B_1\big) \otimes \big(\Delta(x_2, y_2) + B_2\big) \succeq 0 \quad \text{and}$$
$$\big(\Delta(x_1, y_1) + B_1\big) \otimes \big(\Delta(x_2, y_2) - B_2\big) \succeq 0\,,$$

which, by averaging, yields

$$\Delta(x_1, y_1) \otimes \Delta(x_2, y_2) - B_1 \otimes B_2 \succeq 0\,.$$

Therefore, $(x_1, y_1) \otimes (x_2, y_2)$ is a feasible point in the dual $(\mathrm{D}_{B_1 \otimes B_2})$, which obtains the objective value $\varepsilon_q(G_1)\varepsilon_q(G_2)$, which implies the lemma. $\square$

Now we may complete the proof of Theorem 1.3. Using Proposition 2.1 for line (2.8), Lemma 2.6 for line (2.9) and Proposition 2.4 and some easy algebra for the rest we can derive the following

$\varepsilon_q\,(G_1 \oplus G_2)$
(2.8)
$\quad \geq \varepsilon_q\,(G_1)\,\varepsilon_q\,(G_2)$
(2.9)

$$\geq \varepsilon_q \left(\left(\frac{1}{2}G_1 + \frac{1}{2}G_1^T \right) \oplus \left(\frac{1}{2}G_2 + \frac{1}{2}G_2^T \right) \right)$$

$$= \varepsilon_q \left(\frac{1}{4}(G_1 \oplus G_2) + \frac{1}{4}(G_1 \oplus G_2^T) + \frac{1}{4}(G_1^T \oplus G_2) + \frac{1}{4}(G_1^T \oplus G_2^T) \right)$$

$$= \varepsilon_q \left(\frac{1}{2} \left[\frac{1}{2}(G_1 \oplus G_2) + \frac{1}{2}(G_1 \oplus G_2^T) \right] + \frac{1}{2} \left[\frac{1}{2}(G_1 \oplus G_2) + \frac{1}{2}(G_1 \oplus G_2^T) \right]^T \right)$$

$$= \frac{1}{2}\varepsilon_q\,(G_1 \oplus G_2) + \frac{1}{2}\varepsilon_q\,\big(G_1 \oplus G_2^T\big)\,.$$

Therefore $\varepsilon_q(G_1 \oplus G_2) \geq \varepsilon_q(G_1 \oplus G_2^T)$. By symmetry, $\varepsilon_q(G_1 \oplus G_2^T) \geq \varepsilon_q(G_1 \oplus G_2)$, as well, which means that all of the above inequalities must be equalities. This completes the proof of Theorem 1.3.

3. Parallel repetition theorem

In this section we prove Theorem 1.4, which is stated in Section 1.2.
    We begin with the following simple probabilistic lemma.

LEMMA 3.1. *For any sequence of binary random variables $X_1, X_2, \ldots, X_n$,*

$$\frac{1}{2^n} \sum_{M \subseteq [n]} \mathrm{E}\big[(-1)^{\oplus_{j \in M} X_j}\big] = \Pr[X_1 \ldots X_n = 0 \ldots 0].$$

PROOF.   By the linearity of expectation,

$$\frac{1}{2^n} \sum_{M \subseteq [n]} \mathrm{E}\left[(-1)^{\oplus_{j \in M} X_j}\right] = \mathrm{E}\left[\frac{1}{2^n} \sum_{M \subseteq [n]} (-1)^{\oplus_{j \in M} X_j}\right]$$

$$= \mathrm{E}\left[\ \prod_{j=1}^{n} \left(\frac{1 + (-1)^{X_j}}{2}\right)\ \right]$$

$$= \Pr\left[X_1 \ldots X_n = 0 \ldots 0\right],$$

where the last equality follows from the fact that

$$\prod_{j=1}^{n} \big(1 + (-1)^{X_j}\big) \neq 0$$

only if $X_1 \ldots X_n = 0 \ldots 0$. $\square$

We introduce the following terminology. For any strategy $\mathcal{S}$ (classical or quantum) for any game G, define $\omega(\mathcal{S}, G)$ as the success probability of strategy $\mathcal{S}$ on game G. Similarly, define the corresponding bias as $\varepsilon(\mathcal{S}, G) = 2\omega(\mathcal{S}, G) - 1$.

Now let $\mathcal{S}$ be any protocol for the game $\wedge_{j=1}^{n} G_j$. For each $M \subseteq [n]$, define the protocol $\mathcal{S}_M$ (for the game $\oplus_{j \in M} G_j$) as follows.

1. Run protocol $\mathcal{S}$, yielding $a_1, \ldots, a_n$ for Alice and $b_1, \ldots, b_n$ for Bob.

2. Alice outputs $\oplus_{j \in M} a_j$ and Bob outputs $\oplus_{j \in M} b_j$.

LEMMA 3.2.
$$\frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon(\mathcal{S}_M, \oplus_{j \in M} G_j) = \omega(\mathcal{S}, \wedge_{j=1}^{n} G_j).$$

PROOF.   For all $j \in [n]$, define $X_j = a_j \oplus b_j \oplus f_j(s_j, t_j)$. Then, for all $M \subseteq [n]$, we have $\mathrm{E}[(-1)^{\oplus_{j \in M} X_j}] = \varepsilon(\mathcal{S}_M, \oplus_{j \in M} G_j)$, and $\Pr[X_1 \ldots X_n = 0 \ldots 0] = \omega(\mathcal{S}, \wedge_{j=1}^{n} G_j)$. The result now follows from Lemma 3.1. $\square$

COROLLARY 3.3.

(3.4) $$\omega_c(\wedge_{j=1}^n G_j) \le \frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_c(\oplus_{j \in M} G_j)$$

and

(3.5) $$\omega_q(\wedge_{j=1}^n G_j) \le \frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_q(\oplus_{j \in M} G_j) \,.$$

Now, to complete the proof of Theorem 1.4, using Theorem 1.3, we have

$$\frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_q(\oplus_{j \in M} G_j) = \frac{1}{2^n} \sum_{M \subseteq [n]} \prod_{j \in M} \varepsilon_q(G_j)$$

$$= \prod_{j=1}^n \left(\frac{1 + \varepsilon_q(G_j)}{2} \right)$$

(3.6) $$= \prod_{j=1}^n \omega_q(G_j) \,.$$

Combining this with (3.5), we deduce $\omega_q(\wedge_{j=1}^n G_j) = \prod_{j=1}^n \omega_q(G_j)$, which completes the proof of Theorem 1.4.

Comments.   Although (3.5) is used to prove a tight upper bound on $\omega_q(\wedge_{j=1}^n G_j)$, (3.4) cannot be used to obtain a tight upper bound on $\omega_c(\wedge_{j=1}^n G_j)$ for general XOR games. This is because $\varepsilon_c(CHSH) = \varepsilon_c(CHSH \oplus CHSH) = 1/2$ and it can be shown that $\varepsilon_c(CHSH \oplus CHSH \oplus CHSH) = 5/16$. Therefore, for $G_1 = G_2 = G_3 = CHSH$, the right side of (3.4) is $\frac{1}{8} \sum_{M \subseteq [3]} \varepsilon_c(\oplus_{j \in M} G_j) = 34.5/64$, whereas $\omega_c(\wedge_{j=1}^3 G_j)$ must be expressible as an integer divided by 64 (in fact[3], $\omega_c(\wedge_{j=1}^3 G_j) = 31/64$).

Acknowledgements

---

[3]This was independently calculated by S. Aaronson and B. Toner, by searching over a finite number of deterministic classical strategies.

References

[1] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[2] J. Barrett, D. Collins, L. Hardy, A. Kent, and S. Popescu. Quantum nonlocality, Bell inequalities and the memory loophole. *Physical Review A* 66:042111, 2002.

[3] J. Bell. On the Einstein–Podolsky–Rosen paradox. *Physics*, 1(3):195–200, 1964.

[4] M. Bellare, O. Goldreich, and M. Sudan. Free bits, PCPs, and non-approximability – towards tight results. *SIAM Journal on Computing*, 27(3):804–915, 1998.

[5] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, p. 113–131, 1988.

[6] S. Boyd and L. Vandenberghe. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.

[7] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[8] R. Cleve, P. Høyer, B. Toner, J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th IEEE Conference on Computational Complexity*, p. 236–249, 2004.

[9] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. Presentation given at *19th IEEE Conference on Computational Complexity*, June 2004.

[10] U. Feige. On the success probability of two provers in one-round proof systems. In *Proceedings of the Sixth Annual Conference on Structure in Complexity Theory*, p. 116–123, 1991.

[11] U. Feige and M. Goemans. Approximating the value of two prover proof systems, with applications to MAX 2SAT and MAX DICUT. In *Proceedings of the Third Israel Symposium on Theory of Computing and Systems*, p. 182–189, 1995.

[12] U. Feige, G. Kindler, and R. O'Donnell. Understanding parallel repetition requires understanding foams. In *Proceedings of the 21st IEEE Conference on Computational Complexity*, p. 179–192, 2007.

[13] U. Feige and L. Lovász. Two-prover one-round proof systems: Their power and their problems. In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, p. 733–744, 1992.

[14] L. Fortnow. Complexity theoretic aspects of interactive proof systems. PhD thesis, Massachusetts Institute of Technology, May 1989. Technical Report MIT/LCS/TR-447.

[15] L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. *Theoretical Computer Science*, 134:545–557, 1994.

[16] J. Håstad. Some optimal inapproximability results. *Journal of the ACM*, 48(4):798–859, 2001.

[17] T. Holenstein. Parallel repetition: Simplifications and the no-signaling case. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, p. 411–419, 2007.

[18] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, p. 608–617, 2000.

[19] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003.

[20] R. Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[21] B. S. (Tsirelson) Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[22] B. S. (Tsirelson) Tsirel'son. Quantum analogues of the Bell inequalities: The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36:557–570, 1987.

[23] J. Watrous. PSPACE has constant-round quantum interactive proof systems. in *Proceedings of the Fortieth Annual Symposium on Foundations of Computer Science*, p. 112–119, 1999.

[24] J. Watrous. Personal communication, 2004.

[25] S. Wehner. Entanglement in interactive proof systems with binary answers. In *Proceedings of STACS 2006*, p. 162–171, 2006.

A. Perfect parallel repetition fails for non-XOR binary games

In this appendix, we give the unpublished proof due to Watrous [24] that there is a binary game G (that is not an XOR game) for which $\omega_q(G) = \omega_q(G \wedge G) = 2/3$. The game used was originally proposed by Fortnow, Feige and Lovász [13, 14], who showed that $\omega_c(G) = \omega_c(G \wedge G) = 2/3$.

The game has binary questions ($S = T = \{0, 1\}$) and binary answers ($A = B = \{0, 1\}$). The operation of the game is as follows. The Verifier selects a pair of questions (s, t) uniformly from $\{(0, 0), (0, 1), (1, 0)\}$ and sends s and t to Alice and Bob, respectively. Then the Verifier accepts the answers, a from Alice and b from Bob, if and only if $s \vee a \neq t \vee b$.

Consider a quantum strategy for this game, where $|\phi\rangle$ is the shared entanglement, Alice's behavior is determined by the observables A_0 and A_1, and Bob's behavior is determined by the observables B_0 and B_1. On input (s, t), Alice computes a by measuring with respect to A_s, and Bob computes b by measuring with respect to B_t. It is straightforward to deduce that the bias of this strategy is

$$(A.1) \qquad \left\langle \psi \left| \left(-\frac{1}{3} A_0 B_0 + \frac{1}{3} A_0 + \frac{1}{3} B_0 \right) \right| \psi \right\rangle$$

(curiously, the bias does not depend on A_1 or B_1). Once A_0 and B_0 are determined, the optimal bias is the largest eigenvalue of M, where $M = -\frac{1}{3} A_0 B_0 + \frac{1}{3} A_0 + \frac{1}{3} B_0$. Since $M^2 = -\frac{2}{3} M + \frac{1}{3} I$, this eigenvalue λ must satisfy $\lambda^2 = -\frac{2}{3} \lambda + \frac{1}{3}$, which implies that $\lambda = 1/3$ or $\lambda = -1$. This implies that $\omega_q(G) \leq 2/3$. Combining this with the fact that $2/3 = \omega_c(G \wedge G) \leq \omega_q(G \wedge G) \leq \omega_q(G)$, we obtain $\omega_q(G \wedge G) = \omega_q(G) = 2/3$.

B. Connections with other relaxations of classical game values

In this appendix, we show that, whenever $G_1, \ldots, G_n$ are XOR games, the quantum value of $\wedge_{j=1}^n G_j$ coincides with its associated Feige–Lovász relaxations [13]. (It should be noted that this does not reduce our Theorem 1.4 to the results in [13], since we invoke Theorem 1.4 to deduce that the quantum value and the Feige–Lovász relaxations are the same.)

In [13] it is shown that computing the classical value of a game is equivalent to optimizing a quadratic programming problem. In the same paper, Feige and Lovász considered two relaxations for the quadratic programming problem. For any game G, the optimum value of the first relaxation (given by Eqns. (5)–(9) in [13]) is denoted by $\sigma(G)$ and the optimum value of the second relaxation (given by Eqns. (12)–(17) in [13]) is denoted by $\bar{\sigma}(G)$. The feasible region of the first relaxation is subset of the feasible region of second relaxation, so $\sigma(G) \leq \bar{\sigma}(G)$. For the sake of completeness, we write both the SDPs given in [13] for the special case of XOR games.

First, let C be the matrix with entries $C_{(s,a),(t,b)} = \pi(s,t)V(a,b|s,t)$, and let $\hat{C}$ be the symmetric matrix

$$\hat{C} = \frac{1}{2} \begin{pmatrix} 0 & C \\ C^T & 0 \end{pmatrix}.$$

The following two SDPs are relaxations of the classical value of an XOR game, as given in [13], with optimum value $\sigma(G)$ and $\bar{\sigma}(G)$, respectively:

$$\sigma(G) = \max \ \mathrm{Tr}(\hat{C}P)$$

subject to

(B.1) $$\sum_{a \in \{0,1\}} \sum_{b \in \{0,1\}} P_{(s,a),(t,b)} = 1, \quad \forall s,t \in S \cup T,$$

(B.2) $$P_{(s,a),(t,b)} \geq 0, \quad \forall s,t \in S \cup T, a,b \in \{0,1\},$$
$$P \succeq 0,$$

and

$$\bar{\sigma}(G) = \max \ \mathrm{Tr}(\hat{C}P)$$

subject to

(B.3) $$\sum_{a \in \{0,1\}} \sum_{b \in \{0,1\}} |P_{(s,a),(t,b)}| \leq 1, \quad \forall s,t \in S \text{ or } s,t \in T,$$

(B.4) $$P_{(s,a),(t,b)} \geq 0, \quad \forall s \in S, t \in T, a,b \in \{0,1\},$$
$$P \succeq 0.$$

We have the following theorem.

THEOREM B.5. *For any XOR game G, $\omega_q(G) = \sigma(G) = \bar{\sigma}(G)$.*

PROOF.   Let G be an XOR game. From [13] we know that $\sigma(G) \leq \bar{\sigma}(G)$. We will first show that $\omega_q(G) \leq \sigma(G)$. For this, assume an optimal strategy for G. By Theorem 2.2, we can assume that $|\psi\rangle$ is a maximally entangled state. Now let the optimal quantum strategy for G be described by the POVMs $\{M_s^a\}_{a\in\{0,1\}}$, $\{N_t^b\}_{b\in\{0,1\}}$, where $s \in S$ and $t \in T$, along with the state $|\psi\rangle$. Define

$$x_s^a = \begin{cases} (M_s^a \otimes I)|\psi\rangle & s \in S \\ (I \otimes N_s^a)|\psi\rangle & s \in T. \end{cases}$$

Let $\hat{P}_{(s,a),(t,b)} = x_s^a \cdot x_t^b$, so $\hat{P} \succeq 0$. It is easy to check that (B.1) holds, using the fact that $M_s^0 + M_s^1 = I$ and $N_t^0 + N_t^1 = I$. For positive semidefinite matrices like M_s^a and N_t^b we have that

$$\langle\psi|M_s^a \otimes N_t^b|\psi\rangle \geq 0.$$

Since $|\psi\rangle = \frac{1}{\sqrt{d}}\sum_{k=1}^d |k\rangle|k\rangle$ is a maximally entangled state, we also have

$$\langle\psi|I \otimes N_s^a N_t^b|\psi\rangle = \frac{1}{d}\mathrm{Tr}\big((N_s^a N_t^b)^T\big) \geq 0$$

$$\langle\psi|M_s^a M_t^b \otimes I|\psi\rangle = \frac{1}{d}\mathrm{Tr}(M_s^a M_t^b) \geq 0.$$

Therefore $\hat{P}_{(s,a),(t,b)} \geq 0$ for all $s,t \in S \cup T$ and $a,b \in \{0,1\}$ and hence (B.2) holds. With this formulation, we can turn an optimal quantum strategy for G (on a maximally entangled state $|\psi\rangle$) into a feasible solution of (5)–(9) in [13] with same objective value. Hence, $\omega_q(G) \leq \sigma(G)$.

Now, we will show that $\bar{\sigma}(G) \leq \omega_q(G)$. Assume an optimal solution $\bar{P}$ for (12)–(17) in [13]. Since, $\bar{P}$ is a positive semidefinite matrix, we can find vectors x_s^a, for $s \in S$, $a \in \{0,1\}$ and y_t^b, for $t \in T$, $b \in \{0,1\}$, such that

$$\bar{P}_{(s,a),(t,b)} = \begin{cases} x_s^a \cdot x_t^b & s,t \in S \\ y_s^a \cdot y_t^b & s,t \in T \\ x_s^a \cdot y_t^b & s \in S, t \in T. \end{cases}$$

We can view $\{x_s^a\}_{a\in\{0,1\}}$ as Alice's collection of vectors for each question $s \in S$ and $\{y_t^b\}_{b\in\{0,1\}}$ as Bob's collection of vectors for each question $t \in T$. From (B.3),

$$\sum_{a,b\in\{0,1\}} |x_s^a \cdot x_s^b| \leq 1$$

which implies

$$\left| \sum_{a,b\in\{0,1\}} x_s^a \cdot x_s^b \right| = \left\| \sum_{a\in\{0,1\}} x_s^a \right\|^2 \le 1 \,.$$

Therefore, $\sum_{a\in\{0,1\}} x_s^a$ lie in a unit ball. By similar argument, $\sum_{b\in\{0,1\}} y_t^b$ also lie in a unit ball. Define $x_s := x_s^0 - x_s^1$ and $y_t := y_t^0 - y_t^1$. Now,

$$(B.6) \qquad \left(\sum_{a\in\{0,1\}} x_s^a \right) \cdot \left(\sum_{b\in\{0,1\}} y_t^b \right) = x_s^0 \cdot y_t^0 + x_s^1 \cdot y_t^1 + x_s^0 \cdot y_t^1 + x_s^1 \cdot y_t^0 \le 1$$

and we have

$$(B.7) \qquad x_s.y_t = x_s^0 \cdot y_t^0 + x_s^1 \cdot y_t^1 - x_s^0 \cdot y_t^1 - x_s^1 \cdot y_t^0 \,.$$

Therefore $x_s^0 \cdot y_t^0 + x_s^1 \cdot y_t^1 \le 1 - (x_s^0 \cdot y_t^1 + x_s^1 \cdot y_t^0)$ and $x_s \cdot y_t \le 1 - 2(x_s^0 \cdot y_t^1 + x_s^1 \cdot y_t^0)$, which implies

$$(B.8) \qquad x_s^0 \cdot y_t^1 + x_s^1 \cdot y_t^0 \le \frac{(1 - x_s \cdot y_t)}{2} \,.$$

Similarly, $x_s^0 \cdot y_t^1 + x_s^1 \cdot y_t^0 \le 1 - (x_s^0 \cdot y_t^0 + x_s^1 \cdot y_t^1)$ and $x_s \cdot y_t \ge 2(x_s^0 \cdot y_t^0 + x_s^1 \cdot y_t^1) - 1$, which implies

$$(B.9) \qquad x_s^0 \cdot y_t^0 + x_s^1 \cdot y_t^1 \le \frac{(1 + x_s \cdot y_t)}{2} \,.$$

From (B.8) and (B.9), $\bar{\sigma}(G)$ is upper bounded by

$$\sum_{s,t} \pi(s,t) \frac{1}{2} \begin{cases} (1 + x_s \cdot y_t) & \text{if the correct answer is } 0 \\ (1 - x_s \cdot y_t) & \text{if the correct answer is } 1 \,, \end{cases}$$

which is at most $\omega_q(G)$ (see Proposition 5.7 in [8]). Hence, $\bar{\sigma}(G) \le \omega_q(G)$. $\square$

   In [13], it is also shown that the second relaxation is multiplicative but the first relaxation is not. Combining our Theorem 1.4 and the multiplicativity of $\bar{\sigma}$, we can deduce the following.

PROPOSITION B.10. *For any XOR games $G_1, \ldots, G_n$,*

$$\omega_q(\wedge_{i=1}^n G_i) = \sigma(\wedge_{i=1}^n G_i) = \bar{\sigma}(\wedge_{i=1}^n G_i) \,.$$

Richard Cleve
School of Computer Science and
    Institute for Quantum Computing
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada

Perimeter Institute for Theoretical
    Physics
31 Caroline St. N.
Waterloo, Ontario, N2L 2Y5, Canada

William Slofstra
Department of Mathematics
University of California at Berkeley
Berkeley, CA 94720-3840, USA
Research carried out while at the
    University of Waterloo

Falk Unger
CWI
Kruislaan 413
1098 SJ Amsterdam, The Netherlands

Sarvagya Upadhyay
School of Computer Science and
    Institute for Quantum Computing
University of Waterloo
Waterloo, Ontario, N2L 3G1, Canada