Strong Parallel Repetition Theorem
for Quantum XOR Proof Systems

Richard Cleve∗† William Slofstra∗
Falk Unger‡ Sarvagya Upadhyay∗

August 16, 2007

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. Such proof systems, called XOR proof systems, have previously been shown to characterize MIP (= NEXP) in the case of classical provers but to reside in EXP in the case of quantum provers (who are allowed to share a priori entanglement). We show that, in the quantum case, a perfect parallel repetition theorem holds for such proof systems 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, it does not hold. The theorem is proved by analyzing an XOR operation on XOR proof systems. Using semidefinite programming techniques, we show that this operation satisfies a certain additivity property, which we then relate to parallel repetitions of XOR games.

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 investigated and shown to have interesting consequences [17]. 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 (nondegenerate) XOR games. For a predicate \( f: S \times T \to \{0, 1\} \) and a probability distribution \( \pi \) on \( S \times T \), define the XOR game \( G = (f, \pi) \) operationally as follows.

∗David R. Cheriton School of Computer Science and Institute for Quantum Computing, University of Waterloo. cleve@cs.uwaterloo.ca, weslofst@student.cs.uwaterloo.ca, supadhyay@cs.uwaterloo.ca
†Perimeter Institute for Theoretical Physics.
‡CWI, Amsterdam. F.Unger@cwi.nl
• The Verifier selects a pair of questions \((s, t) \in S \times T\) according to distribution \(\pi\).

• 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** for a language \(L\) associates an XOR game with every input string \(x\), such that, for some constants \(0 \leq s < c \leq 1\):

• \(S_x\) and \(T_x\) consist of strings of length polynomial in \(|x|\), \(\pi_x\) 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 \(x \not\in L\) then the maximum acceptance probability over prover’s strategies is at most \(s\).

In [8] it is pointed out that results in [4, 13] imply that, in the case of classical provers, these proof systems have sufficient expressive power to recognize every language in \(\text{NEXP}\) (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, 18] it is shown that any language recognized by a quantum XOR proof system is in \(\text{EXP}\). Thus, assuming \(\text{EXP} \neq \text{NEXP}\), 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 \(\text{CHSH}\) game, named after the authors of [7]. In this game, \(S = T = \{0, 1\}\), \(\pi\) is the uniform distribution on \(S \times T\), and \(f(s, t) = s \land t\). It is well known that, for the \(\text{CHSH}\) 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, 15].

Following [3], 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. It is convenient to also define the classical and quantum **bias** of an XOR game as \(\varepsilon_c(G) = 2\omega_c(G) - 1\) and \(\varepsilon_q(G) = 2\omega_q(G) - 1\), respectively.

Our main results are Theorem 1 of Section 2 and Theorem 7 of Section 3.

\(^1\)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.
2 Additivity 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 two) as the XOR game

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

In this game, the verifier chooses 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 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 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 $\omega_c(G_1)\omega_c(G_2) + (1 - \omega_c(G_1))(1 - \omega_c(G_2))$. Equivalently, the bias of the success probability is $\varepsilon_c(G_1)\varepsilon_c(G_2)$. In this section, we consider the question: 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 $a = s_1 \land s_2$ and Bob to output $b = t_1 \land t_2$. It is straightforward to verify that this latter strategy succeeds with probability $3/4$.

The main result of this section is that the answer is yes for quantum strategies.

**Theorem 1.** 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 $b = b_1 \oplus b_2$.

In this sense, we say that quantum strategies for XOR games are additive, whereas classical strategies are not.

The proof of Theorem 1 employs the known characterization of quantum strategies for XOR games in terms of semidefinite programming, and a number of techniques in semidefinite programming.

A quantum strategy for a 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. We make use of a vector characterization of XOR games due to [10] (also pointed out in [8]), which is a consequence of the following.

**Theorem 2.** ([10]) 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 $\pm 1$ 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 $2^{[N/2]}$, $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$.
and $|\psi\rangle$ be a maximally entangled state on $\mathcal{H}$. Then there exists observables $X_s$ and $Y_t$ with eigenvalues $\pm 1$, 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, we can characterize Alice and Bob’s strategies by a choice of unit vectors $\{x_s\}_{s \in S}$ and $\{y_t\}_{t \in T}$. Using this characterization, the bias becomes

$$\varepsilon(G) = \max_{\{x_s\},\{y_t\}} \sum_{s,t} \pi(s,t)(-1)^{f(s,t)} x_s \cdot y_t. \quad (2)$$

The cost matrix for the game 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 games with cost matrices $A_1$ and $A_2$ respectively, then the cost matrix of $G_1 \oplus G_2$ is $A_1 \otimes A_2$.

The bias of a quantum XOR game may be stated as a semidefinite programming problem (SDP). We refer to Boyd and Vandenberghe for a detailed introduction to semidefinite programming (SDP). The bias is in fact equivalent to the problem

$$\max \ Tr \left( A^T U_1^T U_2 \right) : \ diag \left( U_1^T U_1 \right) = diag \left( U_2^T U_2 \right) = \bar{e}, \quad (3)$$

where $\{x_s\}$ and $\{y_t\}$ appear as the columns of $U_1$ and $U_2$ respectively. Here $diag(M)$ denotes the column vector of diagonal entries of the matrix $M$, and $\bar{e}$ is the column vector $(1, \ldots, 1)^T$. This problem is in turn equivalent to the SDP $P_A$ defined by

$$\max \ Tr \left( \begin{array}{cc} 0 & \frac{1}{2}A \\ \frac{1}{2}A^T & 0 \end{array} \right) X : \ diag(X) = \bar{e}, \quad X \succeq 0.$$ 

The notation $A \succeq B$ means that the matrix $A - B$ lies in the cone of positive semidefinite matrices. That $P_A$ is equivalent to problem (3) 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 $P_A$ exists, we can examine the Lagrange-Slater dual of $P_A$. The dual, denoted by $D_A$, is defined to be

$$\min \ \bar{e}^T y : \Delta(y) \succeq \begin{pmatrix} 0 & \frac{1}{2}A \\ \frac{1}{2}A^T & 0 \end{pmatrix},$$

where $\Delta(y)$ denotes the diagonal matrix with entries given by the vector $y$. Both $P_A$ and $D_A$ have Slater points—that is, feasible points in the interior of the semidefinite cone. Explicitly, the identity matrix is a Slater point for $P_A$, and for large $c$, $c\bar{e}$ is a Slater point for $D_A$. The strong duality theorem states that when both the primal and dual problem have Slater points, the optimal values of $P_A$ and $D_A$ are the same and both problems have optimal solutions obtaining this value.

The next proposition illustrates how the SDP formulation may be used. Intuitively, it corresponds to the fact that if Alice and Bob play games $G_1$ and $G_2$ optimally, taking the sum of their outputs as the solution to $G_1 \oplus G_2$, they will succeed with bias $\varepsilon(G_1)\varepsilon(G_2)$. Theorem 4 will follow when we show the reverse inequality, that $\varepsilon(G_1 \oplus G_2) \leq \varepsilon(G_1)\varepsilon(G_2)$. 

Theorem 4 will follow when we show the reverse inequality, that $\varepsilon(G_1 \oplus G_2) \leq \varepsilon(G_1)\varepsilon(G_2)$. 

4
Proposition 3. For two XOR games $G_1$ and $G_2$, $\varepsilon(G_1 \oplus G_2) \geq \varepsilon(G_1)\varepsilon(G_2)$.

Proof. Let game $G_i$ have cost matrix $A_i$, and let $X_i$ be an optimal solution for $P_{A_i}$. We may write $X_i$ as $(U_iV_i)^T(U_iV_i)$. The cost matrix for $G_1 \oplus G_2$ is $A_1 \otimes A_2$. Then $X = (U_1 \otimes U_2 \ V_1 \otimes V_2)^T(U_1 \otimes U_2 \ V_1 \otimes V_2)$ is a feasible solution for $P_{A_1 \otimes A_2}$. The optimal value of $P_{A_1 \otimes A_2}$ is greater than the value of this feasible solution, which is

$$\text{Tr}(A_1U_1^TV_1)\text{Tr}(A_2U_2^TV_2) = \varepsilon(G_1)\varepsilon(G_2).$$

We consider two methods, differing from the sum, by which new XOR games may be derived from those on hand. For a game $G$ with cost matrix $A$, we define $G^T$ to be the game with cost matrix $A^T$. In other words, Alice and Bob switch places to play $G^T$. Suppose $G_1$ and $G_2$ to be XOR games with cost matrices $A_1$ and $A_2$ respectively. For $0 \leq \lambda \leq 1$, we may define the convex combination $\lambda G_1 + (1 - \lambda) G_2$ to be the XOR game with cost matrix

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

There is a simple interpretation of this convex combination. If, in $G_i$, Alice and Bob are posed questions from $S_i$ and $T_i$ respectively, then in $\lambda G_1 + (1 - \lambda) G_2$ Alice and Bob are either posed a question from $S_1$ and $T_1$ with probability $\lambda$, or a question from $S_2$ and $T_2$ with probability $1 - \lambda$. The next proposition summarizes some simple facts.

Proposition 4. 1. $\varepsilon(G^T) = \varepsilon(G)$ and $\varepsilon(G_1 \oplus G_2) = \varepsilon(G_2 \oplus G_1)$.

2. A limited distributive law holds:

$$[\lambda G_1 + (1 - \lambda) G_2] \oplus H = \lambda G_1 \oplus H + (1 - \lambda) G_2 \oplus H$$

for any three games $G_1$, $G_2$, and $H$.

3. The convex combination of games is additive with respect to $\varepsilon$:

$$\varepsilon(\lambda G_1 + (1 - \lambda) G_2) = \lambda \varepsilon(G_1) + (1 - \lambda) \varepsilon(G_2).$$

The next lemma will complete the proof of additivity for the sum of symmetric games. The proof of this lemma requires two properties of positive semidefinite matrices. The first, is that if $A \succeq 0$ and non-singular, then

$$\begin{pmatrix} A & X \\ X^T & M \end{pmatrix} \succeq 0$$

if and only if $M - X^TA^{-1}X \succeq 0$. The matrix $M - X^TA^{-1}X$ is known as Schur complement of the block matrix given above. The second fact, stated as the next proposition, compensates for the fact that $X \succeq W$ and $Y \succeq Z$ does not necessarily imply $X \otimes Y \succeq W \otimes Z$.

Proposition 5. If $X \succeq W \succeq 0$ and $Y \succeq Z \succeq 0$, then $X \otimes Y \succeq W \otimes Z$. 

5
Proof. This is a simple consequence of the fact that if $A, B \succeq 0$, then $A \otimes B \succeq 0$. Since $X, W \succeq 0$, thus $X + W \succeq 0$. Thus $(X + W) \otimes (Y - Z) \succeq 0$. Similarly, $(X - W) \otimes (Y + Z) \succeq 0$. Averaging these two inequalities, we get the result. \hfill \Box

Lemma 6. If $G_1$ and $G_2$ are XOR games with symmetric cost matrices, then $\varepsilon(G_1 \oplus G_2) \leq \varepsilon(G_1) \varepsilon(G_2)$.

Proof. Let $A$ be the cost matrix of a game $G$. We now consider the dual SDP $D_A$ for this game. A vector $y = (y_1, y_2)$ is feasible in $D_A$ if and only if

$$
\begin{pmatrix}
\Delta(y_1) & -\frac{1}{2}A \\
-\frac{1}{2}A^T & \Delta(y_2)
\end{pmatrix} \succeq 0.
$$

(4)

For a feasible point $y$, the diagonal entries of this matrix must be non-negative. If some entry of $y_i$ is zero, then $A$ will have a zero row and a zero column. By removing questions which never arise, we may assume that $A$ has no zero rows or columns, and thus that any feasible point of $y$ has strictly positive entries. We extend this assumption to all cost matrices appearing in this proof.

Now if equation (4) holds, then by rearranging rows and columns we get

$$
\begin{pmatrix}
\Delta(y_2) & -\frac{1}{2}A^T \\
-\frac{1}{2}A & \Delta(y_1)
\end{pmatrix} \succeq 0.
$$

Thus when $A$ is symmetric, if $y = (y_1, y_2)$ is optimal, then $(y_2, y_1)$ is optimal. By setting $\bar{y} = \frac{1}{2} (y_1 + y_2)$, we may conclude that $D_A$ has an optimal solution of the form $(\bar{y}, \bar{y})$.

Suppose that $y$ has strictly positive entries. By the Schur complement, equation (4) holds for $y$ if and only if

$$
\Delta(y_2) \geq \frac{1}{4} A^T \Delta(y_1)^{-1} A \succeq 0.
$$

(5)

Now we consider the two games $G_1$ and $G_2$ of the hypothesis. Let $A_1$ and $A_2$ be the associated symmetric cost matrices. There is an optimal solution to $D_{A_1}$ of the form $(\bar{x}, \bar{x})$, so that $\varepsilon(G_1) = 2\bar{c}_1^T \bar{x}$. Similarly $D_{A_2}$ has an optimal solution $(\bar{y}, \bar{y})$ so that $\varepsilon(G_2) = 2\bar{c}_2^T \bar{y}$.

Applying equation (4) and Proposition 5 we get that

$$
\Delta(\bar{x}) \otimes \Delta(\bar{y}) \succeq \frac{1}{16} (A_1 \otimes A_2) \left(\Delta(\bar{x})^{-1} \otimes \Delta(\bar{y})^{-1}\right) (A_1 \otimes A_2),
$$

or in other words that $2(\bar{x} \otimes \bar{y}, \bar{x} \otimes \bar{y})$ satisfies equation (4) for cost matrix $A_1 \otimes A_2$, and is thus a feasible point of $D_{A_1 \otimes A_2}$, the dual problem for $G_1 \otimes G_2$.

The optimal value of $D_{A_1 \otimes A_2}$ is less than the value of $2(\bar{x} \otimes \bar{y}, \bar{x} \otimes \bar{y})$, which is $4 \left(\bar{c}_1^T \bar{x}\right) \left(\bar{c}_2^T \bar{y}\right) = \varepsilon(G_1) \varepsilon(G_2)$. Thus $\varepsilon(G_1 \otimes G_2) \leq \varepsilon(G_1) \varepsilon(G_2)$. \hfill \Box

Now we may prove Theorem 4.

Proof of Theorem 4. For a game $G$, let $\tilde{G}$ denote the convex combination $\frac{1}{2} (G + G^T)$. Note that $\tilde{G}$ has a symmetric cost matrix, and that $\varepsilon(\tilde{G}) = \varepsilon(G)$. 6
Now let $G_1$ and $G_2$ be two XOR games. Then applying Proposition 4,
\[
\varepsilon(\tilde{G}_1 \oplus \tilde{G}_2) = \frac{1}{4} \left[ \varepsilon(G_1 \oplus G_2) + \varepsilon(G_1^T \oplus G_2^T) + \varepsilon(G_1^T \oplus G_2^T) \right]
\]
\[
= \frac{1}{2} \left[ \varepsilon(G_1 \oplus G_2) + \varepsilon(G_1^T \oplus G_2) \right]
\]
\[
= \frac{1}{2} \left[ \varepsilon(G_1 \oplus G_2) + \varepsilon(G_1 \oplus G_2^T) \right].
\]

Thus from the lemma,
\[
\varepsilon(G_1)\varepsilon(G_2) = \varepsilon(\tilde{G}_1)\varepsilon(\tilde{G}_2) \geq \varepsilon(\tilde{G}_1 \oplus \tilde{G}_2)
\]
\[
= \frac{1}{2} \left[ \varepsilon(G_1 \oplus G_2) + \varepsilon(G_1 \oplus G_2^T) \right]
\]
\[
\geq \frac{1}{2} \left[ \varepsilon(G_1)\varepsilon(G_2) + \varepsilon(G_1)\varepsilon(G_2^T) \right] = \varepsilon(G_1)\varepsilon(G_2).
\]

Equality must hold throughout this calculation, and so $\varepsilon(G_1 \oplus G_2) = \varepsilon(G_1)\varepsilon(G_2)$. \qed

3 Parallel repetition of XOR games

For any sequence of XOR games $G_1 = (f_1, \pi_1), \ldots, G_n = (f_n, \pi_n)$, 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 $n > 1$.)

A simple way for Alice and Bob to play $\wedge_{j=1}^n G_j$ is to independently play each game optimally. This strategy succeeds with probability $\prod_{j=1}^n \omega(G_j)$. In this section, we consider the question: is this the optimal way to play $\wedge_{j=1}^n G_j$?

The answer is no for classical strategies [2], where it is shown\(^2\) that $\omega_c(CHSH \wedge CHSH) = 10/16 > 9/16 = \omega_q(CHSH \wedge CHSH)$.

Our main result in this section is that the answer is yes for quantum strategies.

**Theorem 7.** For any XOR games $G_1, \ldots, G_n$, $\omega_q(\wedge_{j=1}^n G_j) = \prod_{j=1}^n \omega_q(G_j)$.

This is a quantum version of Raz’s parallel repetition theorem [14] for the restricted class of XOR games. We call it a strong parallel repetition theorem because the probabilities are multiplicative in the exact sense (as opposed to an asymptotic sense, as in [14]).

The proof of Theorem 7 is based on a combination of Theorem 4 and the following probabilistic lemma.

**Lemma 8.** For any binary random variables $X_1, X_2, \ldots, X_n$,
\[
\frac{1}{2^n} \sum_{M \subseteq [n]} \mathbb{E} \left[ (-1)^{\oplus_{j \in M} X_j} \right] = \Pr[X_1 \ldots X_n = 0 \ldots 0]. \quad (6)
\]

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

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

\[
= \Pr [X_1 \ldots X_n = 0 \ldots 0],
\]

where the last equality follows from the fact that \( \prod_{j=1}^{n} (1 + (-1)^{X_j}) \neq 0 \) only if \( X_1 \ldots X_n = 0 \ldots 0 \).

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

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

1. Run protocol \( S \), yielding \( a_1, \ldots, a_n \) for Alice and \( b_1, \ldots, b_n \) for Bob.

2. Alice outputs \( \bigoplus_{j \in M} a_j \) and Bob outputs \( \bigoplus_{j \in M} b_j \).

Lemma 9.

\[
\frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon(S_M, \bigoplus_{j \in M} G_j) = \omega(S, \bigwedge_{j=1}^{n} G_j). \tag{10}
\]

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 \( E[(-1)^{\oplus_{j \in M} X_j}] = \varepsilon(S_M, \bigoplus_{j \in M} G_j) \), and \( \Pr[X_1 \ldots X_n = 0 \ldots 0] = \omega(S, \bigwedge_{j=1}^{n} G_j) \). The result now follows from Lemma 8. \qed

Corollary 10.

\[
\omega_c(\bigwedge_{j=1}^{n} G_j) \leq \frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_c(\bigoplus_{j \in M} G_j) \tag{11}
\]

and

\[
\omega_q(\bigwedge_{j=1}^{n} G_j) \leq \frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_q(\bigoplus_{j \in M} G_j). \tag{12}
\]

Now we may prove Theorem \( \square \)

\[\text{Proof of Theorem } \square \text{ By Theorem } \square \text{ we have} \]

\[
\frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_q(\bigoplus_{j \in M} G_j) = \frac{1}{2^n} \sum_{M \subseteq [n]} \prod_{j=1}^{n} \varepsilon_q(G_j) = \prod_{j=1}^{n} \left( 1 + \varepsilon_q(G_j) \right) = \prod_{j=1}^{n} \omega_q(G_j). \tag{15}\]
Combining this with Eq. [12] we deduce \(\omega_q(\wedge_{j=1}^n G_j) = \prod_{j=1}^n \omega_q(G_j)\).  

We comment that, although Eq. [12] was used to prove a tight upper bound on \(\omega_q(\wedge_{j=1}^n G_j)\), Eq. [11] 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 \(G_1 = G_2 = G_3 = CHSH\), we have \(\frac{1}{8} \sum_{M \subseteq [3]} \varepsilon_c(\oplus_{j \in M} G_j) = 34.5/64\), whereas \(\omega_c(\wedge_{j=1}^3 G_j)\) must be expressible as an integer divided by 64.

Acknowledgments

We would like to thank Scott Aaronson, John Watrous, and Ronald de Wolf for helpful discussions.

References


