Chapter 7

Parallel repetition of quantum XOR games

This chapter is based on the paper


7.1 Introduction

7.1.1 Motivation

Complexity classes

A large part of theoretical computer science is concerned with classifying the difficulty of computational problems. Usually the difficulty of a problem is defined as the amount of resources (for example time or storage space) a Turing machine needs to solve the problem. The most important class of problems is the well-known class P, that contains all problems which can be solved by a polynomial time Turing machine. Polynomial-time solvable problems are considered to be efficiently solvable. The class P contains interesting problems, like (the decision version) of Linear Programming, finding the shortest path between two nodes in a graph, testing whether a given natural number is prime and many others. Readers not familiar with computational complexity theory can find some concise definitions in Section 2.3 on page 23.

Another approach to define complexity classes does not ask how difficult it is to solve a problem, but rather how much resources are needed to become
“convinced” that a solution exists. The most important class defined this way is NP, which contains all problems for which a polynomial time Turing machine can check that a solution to a problem is correct. A particular example is the satisfiability problem SAT, which is the problem of deciding whether for a given Boolean formula there is an assignment of values to the variables which makes the formula evaluate to true. Obviously, if one sees an assignment it is easy to verify (i.e., it is possible to decide in polynomial time in the length of the formula) whether it makes the formula true. In the example of NP “being convinced” means that it is possible to be sure without doubt that a solution exists. It is widely believed that for this strong version of being convinced it is essentially necessary to see a solution.

**Interactive proof systems**

There is a more liberal version of “being convinced” in which one only wants to be sure that a solution exists beyond “reasonable doubt”. Here it might not be necessary to see the solution in order to believe that there is one. This notion can be explained more formally in the framework of *multi-prover interactive proof systems* (MIP proof systems), in which games—the focus of this chapter—show up naturally. An MIP system is a protocol between two provers Alice and Bob and a verifier. The computational power of the verifier is usually that of a probabilistic polynomial-time machine. He wants to know if some instance \( x \) of a problem has a solution (i.e. whether \( x \) satisfies some predicate \( L \)), and in order to do that
he can interact with the two provers by sending them questions generated by some probabilistic procedure and receive their answers. The only restriction on the provers is that they are not allowed to interact once the protocol has started. They see the verifier’s input $x$ and they may agree on a strategy which depends on $x$. At the end of the protocol the verifier outputs a single bit, indicating whether he believes that $x$ has a solution or not. We say that problem $C$ can be decided by an MIP system, if there is a verifier $V$ (i.e. a probabilistic polynomial-time machine) and constants $c > s$, such that for any $x$ it holds: If $x \in C$ then there is a strategy of the provers which makes the verifier $V$ accept with probability at least $c$ and if $x \notin C$ then every strategy of the provers makes the verifier accept with probability at most $s$. The class of problems which can be characterized this way is called MIP. The parameter $c$ is called the *correctness parameter* and $s$ the *soundness parameter*. This model is very powerful. Every problem in NEXP has an MIP proof system [9]. Recall that NEXP is the class of all problems which can be verified by a Turing-machine whose running time is at most exponential in the input size. It is not hard to see that $\text{MIP} \subseteq \text{NEXP}$, since a NEXP-verifier can just guess the prover’s best strategy. Hence, $\text{MIP} = \text{NEXP}$.

The number of rounds needed in such MIP systems is only 1, that is, it is enough for the verifier to send one question to Alice and one to Bob and then accept or not depending on the replies. In this way, we can say that for each input $x$ Alice and Bob are playing a game $G_x$ in which they always try to make the verifier accept. If $x$ has a solution then the provers can win $G_x$ with probability at least $c$, if there is no solution then they can win with probability at most $s$.

**Uncertainty versus acceptance power**

Recall (see also Section 2.3) that the class NEXP is incredibly more powerful than NP. This means that the verifier can trade some uncertainty about the correctness of his output (if $c < 1$ or $s > 0$) against the ability to verify “exponentially” harder problems. How much uncertainty do we have to accept such that we get the full expressive power of the class MIP? Surprisingly, it turns out that it is possible to choose $c = 1$ and $s$ an arbitrarily small constant. Note though, that it is impossible to choose $s = 0$ in addition to $c = 1$, because then the proof system becomes deterministic and therefore characterizes only NP, which is known to be different from NEXP. In other words, if we are willing to tolerate some small uncertainty in the result, then we can characterize problems in NEXP instead of NP only.

**Error-reduction by parallel repetition**

Constructing MIP proof systems which achieve $c = 1$ and $s > 0$ arbitrarily small is clearly desirable. In particular because it makes the definition of the class MIP independent of the exact values of $c$ and $s$. One way (but not the
to see that there are MIP proof systems which match the above minimal requirements is as follows: Show that there is a proof system, with parameters $c = 1$ and $s < 1$. This is always possible for NEXP and can even be achieved with one-round protocols, see [42]. Then just repeat the same protocol again and again. Accept if the provers have won all instances. Clearly, if the provers had a perfectly convincing strategy for one protocol, then they can just use the same strategy on all instances and win them all. If their strategy allowed them to win only with probability $s$ then the probability for winning $T$ protocols has probability at most $s^T$ and increasing $T$ makes the soundness error go to 0 very quickly. This strategy has one obvious drawback. The verifier might need to involve in a very lengthy discussion, $T$ times longer than the original protocol. This might be inefficient but also theoretically bad, because sequential repetition might not preserve certain properties of a proof system (like Zero-knowledge, see [78]). The other solution is to run all the $T$ protocols in parallel, sending the questions of all the protocols at the same time to the respective provers. Clearly, the expected number of protocols the provers can win in this case cannot go up. However, for our purposes this is not enough yet, because the provers might use their knowledge about which question are asked in the other protocols in a sophisticated way: For instance, if one protocol can be won with probability $s$ then there could be a collective strategy that wins all parallel protocols with probability $s$ and looses all of them with probability $1 - s$. Unfortunately, this would not help in reducing the error probability. In fact, we will later see an example in which two parallelized protocols have the same winning probability as one, see Section 7.6.2. So, does repeating protocols in parallel help to reduce winning probabilities?

The answer is yes and is established by the celebrated Parallel Repetition Theorem by Raz [78], see also [54, 77]. For any protocol that can be won with probability $s < 1$ there is some $s' < 1$, such that $k$ parallel repetitions can be won with probability at most $s^k$. This means that the above mentioned procedure for reducing the soundness error to almost 0 works, without increasing the number of rounds needed. And so the exact value of $s$ is inessential, as long as $s > 0$.

**XOR proof systems**

The main result of this chapter considers a particular variant of this model, called *quantum XOR proof systems*. In *XOR proof systems* the protocol is restricted to one round only and the provers Alice and Bob reply with one bit $a$ resp. $b$ only. The verifier’s verdict depends only on the parity $a \oplus b$.\(^1\) If the provers are not allowed to share an entangled state, we speak of a (classical) *XOR proof system* and the complexity class they characterize is called $\oplus$MIP. In Section 7.2.1 we will see that even this restricted class is powerful enough to characterize NEXP.

\(^1\) $a \oplus b$ is equal to 0 if $a = b$ and otherwise 1.
It holds that $\oplus\text{MIP} = \text{NEXP} [32]$ (although only with parameters $c = 12/16 - \epsilon$ and $s = 11/16 + \epsilon$ for arbitrarily small $\epsilon$). If the provers are allowed to share an entangled state, we call it a quantum XOR proof system and the complexity class they characterize is called $\oplus\text{MIP}^*$. When entanglement is allowed the complexity can be bounded by $\oplus\text{MIP}^* \subseteq \text{EXP} [33, 101]$, so assuming that $\text{NEXP} \neq \text{EXP}$, entanglement strictly weakens the expressive power of XOR proof systems.

**Main result**

Our main result in this chapter is a perfect parallel repetition theorem for quantum XOR proof systems, which states that if one protocol can be won with probability $p$, then $k$ parallel repetitions of the protocol can be won exactly with probability $p^k$ but not more. This means that the optimal collective strategy is to play all protocols individually optimal, i.e., there is no way in which knowledge of the other instances can help.
Chapter 7. Parallel repetition of quantum XOR games

systems. We will not attempt to be in any way complete or reflect the historical line of events and only review certain aspects.

Further, we want to mention that it is also possible to define interactive proof systems in which the verifier and the prover(s) communicate quantum messages. We will not go into this subject in this thesis. The interested reader might find the following articles [58, 99, 60, 56] interesting and can find further pointers to the literature in there.

Number of provers

Let us first see how the number of provers influences the expressive power. It is known that allowing more than two classical provers does not increase the power of these proof systems [14]. However, if there is only one prover, then the resulting class IP exactly captures the problems in PSPACE, or more succinctly: IP=\text{PSPACE} [85]. Hence, it seems that at least 2 provers are needed to unleash the full power of the model. Further, the number of rounds needed is at most one, which follows by Raz’s parallel repetition theorem [78]. A natural question is whether a parallel repetition theorem also holds for any other number of provers. Under the reasonable assumption that PSPACE≠\Pi_p^2 it is impossible that a classical parallel repetition theorem for one prover only holds, since it is known that IP(m)=IP(2)⊆\Pi_p^2, but PSPACE=IP.

XOR proof systems

As mentioned in the introduction, the simplest case of MIP systems are XOR multi-prover interactive proof systems in which the verifiers reply only with one bit each, and the verifier accepts depending on \(a\oplus b\). We defined the corresponding complexity classes \(\oplus\text{MIP}\) (no entanglement) and \(\oplus\text{MIP}^*\) (with entanglement). In [32] it is pointed out that results in [13, 53] imply that, in the case of classical provers, these \(\oplus\text{MIP}\) systems are sufficient 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 the same languages as unrestricted multi-prover interactive proof system. Moreover, in [33, 101] it is shown that any language recognized by a quantum XOR proof system is in EXP, which uses a semidefinite programming characterization due to Tsirelson [94, 32], which is given in Section 7.3. Thus, assuming EXP ≠ NEXP, quantum entanglement strictly weakens the expressive power of XOR proof systems.

\(^2\text{Though we should remark that it is not needed.}\)
Parallel repetition for quantum games

The only other parallel repetition theorem along the lines of [78] for quantum games (where the players share entanglement) we know of is for unique games [57]. Unique games are two-prover games where for each pair of questions to the verifier and each answer of Alice, there is always exactly one answer of Bob that makes the verifier accept. Note that XOR games are a particular kind of unique games. The result in [57] is not “perfect” in our sense though, since it does not imply that the trivial strategy (of playing all parallel games independently) achieves the best success probability for winning all games. We do not know about a parallel repetition theorem for general quantum games. A perfect parallel repetition theorem cannot be true in general as was pointed out by Watrous [100], who has shown that there is a binary game (that is not an XOR game) for which the success probability $\omega_q(G)$ of winning one game and the success probability $\omega_q(G \land G)$ of winning two games played in parallel is in both cases $2/3$, as in the classical case. This is explained in Section 7.6.2.

This chapter is about parallel repetition of 2-prover games. We do not know about any results for more than two provers.

7.2.2 XOR games

The definition of XOR interactive proof systems can be based on XOR games, which we define first. 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.

- 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 not allowed to communicate 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 appears in [32]. 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.

3Except 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.
Chapter 7. Parallel repetition of quantum XOR games

Following [32], for an XOR game $G$, define its classical value $\omega_c(G)$ as the maximum success probability achievable by a classical strategy, i.e., if the provers do not share entanglement. Similarly, define its quantum value $\omega_q(G)$ as the maximum success probability achievable by a quantum strategy. It is convenient to define the bias of a quantum XOR game as $\varepsilon_q(G) = 2\omega_q(G) - 1$ and similarly $\varepsilon_c(G) = 2\omega_c(G) - 1$ in the classical case.

Using the definition of XOR games it is straightforward to define XOR interactive proof systems. A language $L$ has an XOR interactive proof systems (with soundness probability $s$ and completeness probability $c > s$) if it is possible to associate to each $x$ an efficient XOR game $G_x$ such that if $x \in L$ then the maximum acceptance probability over the prover’s strategies is at least $c$ and if $x \notin L$ then the maximum acceptance probability over prover’s strategies is at most $s$.

The game $G_x = (f, \pi)$ is efficient if the verifier can be efficiently implemented: More precisely we demand that $S$ and $T$ consist of strings of length polynomial in $|x|$, $\pi$ can be sampled in time polynomial in $|x|$, and $f$ can be computed in time polynomial in $|x|$. It is clear that the restriction to efficient XOR games is crucial for the definition of $\oplus$-MIP systems. However, our parallel repetition theorem will hold for all XOR games and therefore we will not talk about efficiency anymore.

7.2.3 XOR games and non-locality

It is interesting to note that quantum physicists have, in a sense, been studying quantum XOR games since the 1960s, when John Bell introduced his celebrated results that are now known as Bell inequality violations [12]. An example is the CHSH game, named after the authors of [25]. This game will play a prominent role in Chapter 8, but we will quickly explain it here. In this game, $S = T = \{0, 1\}$, $\pi$ is the uniform distribution on $S \times T$, and $f(s, t) = s \land t$. In other words, the provers win if and only if they output bits $a$ and $b$ which satisfy $a \oplus b = s \land t$.

The best possible classical strategy succeeds with probability $3/4$, whereas the best possible quantum strategy succeeds with higher probability of $(1+1/\sqrt{2})/2 \approx 0.85$ [25, 93], which can be straightforwardly computed from the characterization in Section 7.3. This difference in success probabilities can be used to show that classical physics cannot explain all physical phenomena.\footnote{Although it should be noted that because of the inaccuracies in today’s quantum hardware it is not possible to completely rule out classical theories.}

7.3 Characterization of quantum XOR games

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

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

Tsirelson’s vector characterization

We make use of a vector characterization of XOR games due to [94] (also pointed out in [32]), which is a consequence of the following.

**7.3.1. Theorem ([94, 32]).** 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 exist 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 spaces 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 exist 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 $t \in T$.

A proof of this theorem can be found in Appendix D.

Using Theorem 7.3.1, 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

$$\varepsilon_q(G) = \max_{\{x_s\},\{y_t\}} \sum_{s,t} \pi(s,t)(-1)^{f(s,t)} x_s \cdot y_t. \quad (7.1)$$

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.

Symmetry considerations and convex combinations of XOR games

We start by some symmetry considerations. If $G_1$ and $G_2$ are XOR games with cost matrices $A_1$ and $A_2$, then 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 $\lambda$, 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 following facts are easy to verify.

7.3.2. Proposition. 1. $\varepsilon_q(G) = \varepsilon_q(G^T)$.

2. For all $0 \leq \lambda \leq 1$,

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

Value of XOR games as SDP

The bias of a quantum XOR game may be stated as a semidefinite programming problem (SDP). We refer to Boyd and Vandenberghe [97] for a detailed introduction to semidefinite programming. For cost matrix $A$, the bias is equivalent to the objective value of problem

$$\begin{align*}
\max & \quad \operatorname{Tr}(A^T U_1^T U_2) \\
\text{s.t.} & \quad \operatorname{diag}(U_1^T U_1) = \operatorname{diag}(U_2^T U_2) = \bar{e}, \quad X \succeq 0
\end{align*}$$

(7.2)
Dual of SDP

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 (see Section 2.6)

\[
\min \ (x, y) \bar{e} \\
\text{s.t.} \ \Delta(x, y) \succeq B
\]

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 and are therefore strictly feasible. 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.

7.3.3. Remark. For any XOR game \(G\), the semidefinite programming relaxations of \(G\) due to Feige and Lovász [42] have value equal to the quantum value of \(G\), given by equations (7.3) and (7.3). We say more about the relation of our result to the ones in [42] in Section 7.6.3.

7.4. Additivity theorem

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

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

(7.3)

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 \(a \oplus b = f_1(s_1, t_1) \oplus f_2(s_2, t_2)\). If \(G_1\) and \(G_2\) have 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 next proposition summarizes some simple facts.

7.4.1. Proposition. 1. \(\varepsilon_q(G_1 \oplus G_2) = \varepsilon_q(G_2 \oplus G_1)\)

2. For all \(0 \leq \lambda \leq 1,\)

\[
G_1 \oplus (\lambda G_2 + (1 - \lambda)G_3) = \lambda(G_1 \oplus G_2) + (1 - \lambda)(G_1 \oplus G_3).
\]

(7.4)

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

\[
\omega(G_1)\omega(G_2) + (1 - \omega(G_1))(1 - \omega(G_2)),
\]

(7.4)
where $\omega$ (and later $\varepsilon$) can be indexed by $q$ or $c$ depending on whether Alice and Bob share entanglement. Then it is easy to see that the bias $\varepsilon^{\text{trivial}}(G_1 \oplus G_2)$ for this particular strategy of playing $G_1 \oplus G_2$ is

$$\varepsilon^{\text{trivial}}(G_1 \oplus G_2) = \varepsilon(G_1)\varepsilon(G_2). \quad (7.5)$$

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 $\text{CHSH} \oplus \text{CHSH}$, 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 $3/4$.

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

7.4.2. **Theorem (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 uses the characterization of quantum strategies for individual XOR games as semidefinite programs from Section 7.3.

Recall that we defined the quantum bias of an XOR game as $\varepsilon_q(G) = 2\omega_q(G) - 1$. Then, due to equation (7.5), we already have one part of Theorem 7.4.2.

7.4.3. **Proposition.** 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 of Theorem 7.4.2 is the reverse inequality.

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 $G_1 \oplus G_2$).

7.4.4. **Lemma.** If $G_1$ and $G_2$ are XOR games, then

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

**Proof:** Let $G_1$ and $G_2$ be two games with cost matrices $A_1$ and $A_2$, respectively, and let

$$B_1 = \begin{pmatrix} 0 & \frac{1}{2}A_1 \\ \frac{1}{2}A_1^T & 0 \end{pmatrix} \quad \text{and} \quad B_2 = \begin{pmatrix} 0 & \frac{1}{2}A_2 \\ \frac{1}{2}A_2^T & 0 \end{pmatrix}. \quad (7.6)$$

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 equation (7.6). 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,
\[
(\Delta(x_1, y_1) - B_1) \otimes (\Delta(x_2, y_2) + B_2) \succeq 0 \quad \text{and} \quad (\Delta(x_1, y_1) + B_1) \otimes (\Delta(x_2, y_2) - B_2) \succeq 0,
\]
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 \((\mathcal{D}_{B_1 \otimes B_2})\), which obtains the objective value \(\varepsilon_q(G_1)\varepsilon_q(G_2)\). Noting that \((\frac{1}{2}G_1 + \frac{1}{2}G_1^T) \oplus (\frac{1}{2}G_2 + \frac{1}{2}G_2^T)\)
has cost matrix \(B_1 \otimes B_2\) implies the Lemma. \(\blacksquare\)

Now we may complete the proof of Theorem 7.4.2. Using Proposition 7.4.3 for line (7.7), Lemma 7.4.4 for line (7.8) and Propositions 7.3.2 and 7.4.1 and some easy algebra for the rest we can derive the following
\[
\varepsilon_q(G_1 \oplus G_2) \geq \varepsilon_q(G_1) \varepsilon_q(G_2) \quad \text{(7.7)}
\]
\[
\varepsilon_q \left( (\frac{1}{2}G_1 + \frac{1}{2}G_1^T) \oplus (\frac{1}{2}G_2 + \frac{1}{2}G_2^T) \right) \geq \varepsilon_q \left( \frac{1}{2}(G_1 \oplus G_2) + \frac{1}{2}(G_1 \oplus G_2^T) + \frac{1}{2}(G_2 \oplus G_2^T) \right) \geq \varepsilon_q \left( \frac{1}{2} \left[ \frac{1}{2}(G_1 \oplus G_2) + \frac{1}{2}(G_1 \oplus G_2^T) \right] + \frac{1}{2} \left[ \frac{1}{2}(G_1 \oplus G_2) + \frac{1}{2}(G_1 \oplus G_2^T) \right] \right) \geq \frac{1}{2} \varepsilon_q(G_1 \oplus G_2) \geq \varepsilon_q(G_1 \oplus G_2^T) \quad \text{(7.8)}
\]
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 7.4.2.

### 7.5 Parallel repetition theorem

For any sequence of XOR games \(G_1 = (f_1, \pi_1), \ldots, G_n = (f_n, \pi_n)\), define their conjunction, denoted by \(\bigwedge_{j=1}^{n} G_j\), 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 \( \wedge^n_{j=1} G_j \) is not itself an XOR game for \(n > 1\).)

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

The answer is again \(\text{no}\) for classical strategies. It is shown in [11] that
\[ \omega_c(CHSH \wedge CHSH) = 10/16 > 9/16 = \omega_c(CHSH) \omega_c(CHSH). \]

Our second result is that the answer is \(\text{yes}\) for quantum strategies.

7.5.1. **Theorem (Parallel Repetition)**. For any XOR games \(G_1, \ldots, G_n\), we have that 
\[ \omega_q(\wedge^n_{j=1} G_j) = \prod^n_{j=1} \omega_q(G_j). \]

This is a quantum version of Raz’s parallel repetition theorem [78] 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 [78]). The proof of Theorem 7.5.1 is based on Theorem 7.4.2 combined with Fourier analysis techniques for boolean functions. Section 7.5 contains the proof.

In this section we prove Theorem 7.5.1, which is stated in Section 7.5.

We begin with the following simple probabilistic lemma.

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

**Proof:** By the linearity of expectation,
\[ \frac{1}{2^n} \sum_{M \subseteq [n]} \mathbb{E} \left[ (-1)^{\oplus_{j \in M} X_j} \right] = \mathbb{E} \left[ \frac{1}{2^n} \sum_{M \subseteq [n]} (-1)^{\oplus_{j \in M} X_j} \right] = \mathbb{E} \left[ \prod_{j=1}^n \left( 1 + (-1)^{X_j} \right) \right] = \Pr[X_1 \ldots X_n = 0 \ldots 0], \]

\(^6\)After posing this question about \(\omega_c(CHSH \wedge CHSH)\), the answer was first shown to us by S. Aaronson, who later found that this result was already stated in [11].
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 \(\mathcal{S}\)—classical or quantum—and 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 \(\land_{j=1}^{n}G_j\). 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 \(\oplus_{j \in M}b_j\).

7.5.3. Lemma.
\[
\frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon(\mathcal{S}_M, \oplus_{j \in M}G_j) = \omega(\mathcal{S}, \land_{j=1}^{n}G_j).
\]

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 \(E[(-1)^{\oplus_{j \in M}X_j}] = \varepsilon(\mathcal{S}_M, \oplus_{j \in M}G_j)\), and \(\Pr[X_1 \ldots X_n = 0 \ldots 0] = \omega(\mathcal{S}, \land_{j=1}^{n}G_j)\). The result now follows from Lemma 7.5.2.

7.5.4. Corollary.
\[
\omega_c(\land_{j=1}^{n}G_j) \leq \frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_c(\oplus_{j \in M}G_j) \quad (7.9)
\]

and
\[
\omega_q(\land_{j=1}^{n}G_j) \leq \frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_q(\oplus_{j \in M}G_j). \quad (7.10)
\]

Now, to complete the proof of Theorem 7.5.1, using Theorem 7.4.2, we have
\[
\frac{1}{2^n} \sum_{M \subseteq [n]} \varepsilon_q(\oplus_{j \in M}G_j) = \frac{1}{2^n} \sum_{M \subseteq [n]} \prod_{j \in M} \varepsilon_q(G_j) = \prod_{j=1}^{n} \frac{1 + \varepsilon_q(G_j)}{2} = \prod_{j=1}^{n} \omega_q(G_j). \quad (7.11)
\]
Combining this with equation (7.10), we deduce \(\omega_q(\land_{j=1}^{n}G_j) = \prod_{j=1}^{n} \omega_q(G_j)\), which completes the proof of Theorem 7.5.1.
Chapter 7. Parallel repetition of quantum XOR games

7.6 Discussion

A natural question to ask is whether it is possible to extend the proof for other kinds of games. We have already mentioned that a perfect parallel repetition cannot hold for classical XOR games, since it does not even hold for classical CHSH games. The next remark gives some more details about how the classical CHSH game behaves under repetition. The second remark in this section will show that a perfect parallel repetition theorem can also not hold for general quantum games. We will conclude by explaining the connection of our results to Feige-Lovász games games.

7.6.1 Perfect parallel repetition of classical XOR games

Although equation (7.10) is used to prove a tight upper bound on $\omega_q(\land_j^k G_j)$, equation (7.9) cannot be used to obtain a tight upper bound on $\omega_c(\land_j^k G_j)$ 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 equation (7.9) is $\frac{1}{8} \sum_{M \subseteq [3]} \varepsilon_c(\oplus j \in M G_j) = 34.5/64$, whereas $\omega_c(\land_j^3 G_j)$ must be expressible as an integer divided by 64 (in fact, $\omega_c(\land_j^3 G_j) = 31/64$).

7.6.2 Parallel repetition of general games

We give the unpublished proof due to Watrous [100] that there is a binary game $G$ (that is not an XOR game) for which $\omega_q(G) = \omega_q(G \land G) = 2/3$. The game used was originally proposed by Fortnow, Feige and Lovász [45, 42], who showed that $\omega_c(G) = \omega_c(G \land G) = 2/3$.

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 $s \lor a \neq t \lor b$.

Consider a quantum strategy for this game, where $|\phi\rangle$ is the shared entangled state. We may assume that 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 $B_1$ and that all observables have only eigenvalues $\pm 1$. 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

$$\langle \phi | \left( -\frac{1}{2} A_0 \otimes B_0 + \frac{1}{3} A_0 \otimes I_B + \frac{1}{3} I_A \otimes B_0 \right) | \phi \rangle$$

(7.12)

This was independently calculated by S. Aaronson and B. Toner, by searching over a finite number of deterministic classical strategies.
(curiously, the bias does not depend on $A_1$ or $B_1$). We can rewrite $-\frac{1}{3}A_0 \otimes B_0 + \frac{1}{3}A_0 \otimes I_B + \frac{1}{3}I_A \otimes B_0 = \frac{1}{3}(I_A - A_0) \otimes (B_0 - I_B) + \frac{1}{3}(I_A \otimes I_B)$, and the bias becomes

$$\frac{1}{3}\langle \phi | (I_A - A_0) \otimes (B_0 - I_B) | \phi \rangle + \frac{1}{3}.$$  \hfill (7.13)

We note that $I_A - A_0$ has eigenvalues 0 and 2 and $B_0 - I_B$ has eigenvalues 0 and $-2$, from which we can conclude that the hermitian matrix $(I_A - A_0) \otimes (B_0 - I_B)$ has no positive eigenvalues. This implies that $\varepsilon_q(G) = 1/3$ and further $\omega_q(G) = 2/3$. Combining this with the fact that $2/3 = \omega_c(G \land G) \leq \omega_q(G \land G) \leq \omega_q(G)$, we obtain $\omega_q(G \land G) = \omega_q(G) = 2/3$.

### 7.6.3 Feige-Lovász games

For a broad class of games, Feige and Lovász [42] 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 7.5.1. For any XOR game $G$, the Feige-Lovász relaxations of its classical value are equal to the quantum value of $G$. This was noted first in [40, 41] and an explicit proof appears in the appendix of [30]. 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.

Using this relation between the value of a quantum XOR game and the value of its Feige-Lovász relaxation combined with Theorem 7.5.1, it follows that for XOR games $G_1, \ldots, G_n$, the quantum value of $\land_{j=1}^n G_j$ is also determined by its associated Feige-Lovász relaxation. However, it should be stressed that the parallel repetition property for Feige-Lovász relaxations does not imply our Theorem 7.5.1, since we do not know a priori that for the non-XOR game $\land_{j=1}^n G_j$ the same relation between its quantum value and the value of its Feige-Lovász relaxation holds. Our Theorem 7.5.1 shows this.