

# A $k$ -Provers Parallel Repetition Theorem for a version of No-Signaling Model

Ricky Rosen \*

February 10, 2010

## Abstract

The parallel repetition theorem states that for any two provers one round game with value at most  $1 - \epsilon$  (for  $\epsilon < 1/2$ ), the value of the game repeated  $n$  times in parallel is at most  $(1 - \epsilon^3)^{\Omega(n/\log s)}$  where  $s$  is the size of the answers set [Raz98],[Hol07]. It is not known how the value of the game decreases when there are three or more players. In this paper we address the problem of the error decrease of parallel repetition game for  $k$ -provers where  $k > 2$ . We consider a special case of the No-Signaling model and show that the error of the parallel repetition of  $k$  provers one round game, for  $k > 2$ , in this model, decreases exponentially depending only on the error of the original game and on the number of repetitions. There were no prior results for  $k$ -provers parallel repetition for  $k > 2$  in any model.

## 1 Introduction

In a  $k$  provers one round game there are  $k$  provers and a verifier. The verifier selects randomly  $(x_1, \dots, x_k) \in X_1 \times \dots \times X_k$ , a question for each prover, according to some distribution  $P_{X_1 \dots X_k}$  where  $X_i$  is the questions set of prover  $i$  where  $i \in 1, \dots, k$ . Each prover knows only the question addressed to her, prover 1 knows only  $x_1$  and prover  $i$  knows only  $x_i$ . The provers cannot communicate during the transaction. The provers send their answers to the verifier,  $a_i \in A_i$  where  $A_i$  is the answers set of prover  $i$ . The verifier evaluates an acceptance predicate  $V(x_1, \dots, x_k, a_1, \dots, a_k)$  and accepts or rejects based on the outcome of the predicate. The acceptance predicate as well as the distribution of the questions are known in advance to the provers. The provers answer the questions according to a strategy. The strategy of the provers is also called a protocol. The type of the protocol determines the type of model. In the *classic model* the provers' strategy is a  $k$  tuple of functions, one for each prover, where each function is from her questions to her answers, i.e., for all  $i$ ,  $f_{a_i} : X_i \rightarrow A_i$ . We also call this model  $MIP(k, 1)$ . In the *No-Signaling model* the provers' strategy is a  $k$  tuple of functions, one for each prover, where each function is a random function from the questions of **all** the provers to her answers but in a way that does not reveal any information about the other provers' questions. We denote this model by  $MIP^\diamond(k, 1)$ . The No Signaling condition ensures that the answer of each prover given its question is independent of the questions of the other provers (but not of the other provers answers). This definition is the natural generalization of the no-signaling model of two provers one round game to no signaling model of  $k$  provers one round game. However, in this paper we generalize the no-signaling model in a different

---

\*Department of Computer Science, Tel-Aviv University, Tel-Aviv 69978, Israel.

way. In this variation, no  $k-1$  provers together can signal to the remaining prover. In the standard model one also demands that no player can signal to the other players when the other  $k-1$  players can talk to each other. To get a sense of such games, let us consider a generalization of the CHSH [CHSH69] game for 3 players. Let us denote the three provers by Alice, Bob and Charlie. The verifier chooses uniformly at random three questions  $x, y, z \in \{0, 1\}$  and sends  $x$  to Alice,  $y$  to Bob and  $z$  to Charlie. The provers send their answers, denoted by  $a, b, c$  and the verifier accepts if and only if  $x \wedge y \wedge z = a \oplus b \oplus c$ . We will consider the following strategy: if  $x \wedge y \wedge z = 0$  then  $(a, b, c)$  is distributed uniformly over  $\{(0, 0, 0), (1, 0, 1), (1, 1, 0), (0, 1, 1)\}$ . If  $x \wedge y \wedge z = 1$  then  $(a, b, c)$  is distributed uniformly over  $\{(1, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)\}$ . This is a no-signaling strategy since for every question of Alice, knowing her answer to that question does not reveal any information about Bob's or Charlie's questions. Similar argument apply to Bob and Charlie.

The *value* of the game is the maximum of the probability that the verifier accepts, where the maximum is taken over all the provers strategies. More formally, the value of the game is:

$$\max_{f_{a_1}, \dots, f_{a_k}} \mathbb{E}_{x_1, \dots, x_k} [V(x_1, \dots, x_k, f_{a_1}(x_1), \dots, f_{a_k}(x_k))]$$

where the expectation is taken with respect to the distribution  $P_{X_1 \dots X_k}$ . We denote the value of the game in the classical model by  $w(G)$  and the value of the game in the No-Signaling model by  $\omega^\diamond(G)$ .

Roughly speaking, the *n-fold parallel repetition* of the game, denoted by  $(G^{\otimes n})$ , is playing the game  $n$  times in parallel, i.e. the verifier sends  $n$  questions to each prover and receives  $n$  answers from each prover. The verifier evaluates the acceptance predicate on each game and accepts if and only if all the predicates were true. Obviously  $\omega^\diamond(G^{\otimes n}) \leq \omega^\diamond(G)$  but one might expect that  $\omega^\diamond(G^{\otimes n}) = (\omega^\diamond(G))^n$ . However, although the verifier treats each game of the  $n$  games independently, the provers may not. The answer of each question addressed to a prover may depend on all the questions addressed to that prover. There are examples for the MIP(2, 1) model [For89], [FL92], [Raz98], [FV02], [Hol07], and for the  $MIP^\diamond(2, 1)$  model [Hol07] for which the  $\omega^\diamond(G^{\otimes n}) = (\omega^\diamond(G))^n$  for small  $n$ . Raz provided an example [Fei95] for MIP( $k, 1$ ) where  $\omega^\diamond(G^{\otimes k}) = (\omega^\diamond(G))^k$ .

Another model of  $k$ -provers one round game is the *quantum model*, denote by  $MIP^*(k, 1)$ , in which the provers have a joint quantum state and so the function of each prover is from the questions of all the provers to her answers but only for such functions that can be implemented by an entangled quantum state.

Clearly, the value of a game in the MIP( $k, 1$ ) model is less or equal to the value of the game in the  $\omega^*(G)$  model which is less or equal to the value of the game in  $MIP^\diamond(k, 1)$  model. However, this bound does not imply a bound for the parallel repetition of the MIP( $k, 1$ ) model since there are games for which the value of the game in the MIP( $k, 1$ ) model is strictly less than 1 but the value of the game in  $MIP^\diamond(k, 1)$  model is 1, therefore implying only the trivial bound. If the value of the game in  $MIP^\diamond(k, 1)$  model is strictly less than 1 then we obtain a non trivial bound on the value of the game for the MIP( $k, 1$ ) model. <sup>1</sup>

Many fundamental questions related to the MIP(2, 1) model have been answered by now, but there was no known upper bounds on MIP( $k, 1$ ) for  $k > 2$  in any model. However, it was conjectured that the error decreases exponentially. Although this model of no-signaling is not the natural no-signaling model, it allows us to obtain a first upper bound result for the MIP( $k, 1$ ) for  $k > 2$  for special types of games<sup>2</sup> and it raises explicitly the questions for what models one can look at more

<sup>1</sup>It decreases exponentially and does not depend on the size of the answers support.

<sup>2</sup>Namely, games where the value of the game played according to a no-signaling protocol is strictly less than 1.

than 2 provers.

## 1.1 Related Work

A series of papers deals with the nature of the error decrease of parallel repetition game [CCL92], [Fei91], [FK94], [Raz98], [Hol07]. The breakthrough result was done by Raz's [Raz98]. In his celebrated result, Raz proved that the error of  $MIP(2, 1)$  decreases exponentially depending also on the size of the answer set. Holenstein [Hol07] lately simplified this result and revealed new insights on the nature of the problem. Holenstein also improved the constants to give a tighter bound on the error of the  $n$  parallel repetition. Holenstein also proved that in the  $MIP^\diamond(2, 1)$  model, the error decreases exponentially and does not depend on the size of the answer set.

## 2 Our results

A 3-provers one round No-Signaling game

$$G = (X, Y, Z, A, B, C, P_{XYZ}, Q)$$

is an object consisting on three finite question sets  $X, Y, Z$ , a probability measure  $P_{XYZ}$  on  $XYZ$

$$P_{XYZ} : X \times Y \times Z \rightarrow \mathbb{R}^+,$$

answer sets  $A, B, C$  and an acceptance predicate

$$Q : X \times Y \times Z \times A \times B \times C \rightarrow \{0, 1\}.$$

A No-Signaling protocol is a set of three No-Signaling functions: the function

$$p_1 : X \times Y \times Z \times R \rightarrow A,$$

the function

$$p_2 : X \times Y \times Z \times R \rightarrow B$$

and the function:

$$p_3 : X \times Y \times Z \times R \rightarrow C.$$

A function

$$p_1 : X \times Y \times Z \times R \rightarrow A$$

is a No-Signaling function if:

$$\forall x \in X, a \in A, y, y' \in Y, z, z' \in Z \quad \Pr_R[p_1(x, y, z, R) = a] = \Pr_R[p_1(x, y', z', R) = a].$$

For  $k$  provers, a function  $p_i$  is no-signaling if:

$$\begin{aligned} \forall x \in X_i, a \in A_i, x_j, x'_j \in X_j \text{ for } j \neq i \quad \Pr_R[p_i(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_k, R) = a] = \\ \Pr_R[p_i(x'_1, \dots, x'_{i-1}, x, x'_{i+1}, \dots, x'_k, R) = a]. \end{aligned}$$

**Definition 2.1 (value of the game)** *The value of the game is defined as:*

$$\omega^\diamond(\mathsf{G}) = \max_{p_1, p_2, p_3} \mathbb{E}_{XYZR}[Q(X, Y, Z, p_1(X, Y, Z, R), p_2(X, Y, Z, R), p_3(X, Y, Z, R))]$$

where the expectation is taken with respect to  $P_{XYZ}$  and the maximum is taken over all No-Signaling protocols.

The  $n$ -fold parallel repetition 3-provers game  $\mathsf{G}^{\otimes n}$  consists of the sets  $X^n, Y^n, Z^n$ , a probability measure on those sets,  $P_{X^n Y^n Z^n}^{\otimes n}$  where

$$P_{X^n Y^n Z^n}^{\otimes n}(x^n, y^n, z^n) = \prod_{i=1}^n P_{XYZ}(x_i, y_i, z_i)$$

for  $x^n \in X^n$ ,  $y^n \in Y^n$ ,  $z^n \in Z^n$ . It also consists of the sets  $A^n, B^n, C^n$  and an accepting predicate  $Q^{\otimes n}$  where

$$Q^{\otimes n}(x^n, y^n, z^n, a^n, b^n, c^n) = \bigwedge_{i=1}^n Q(x_i, y_i, z_i, a_i, b_i, c_i)$$

for  $x^n \in X^n$ ,  $y^n \in Y^n$ ,  $z^n \in Z^n$ ,  $a^n \in A^n$ ,  $b^n \in B^n$ ,  $c^n \in C^n$ . The  $n$ -fold parallel repetition for  $k$ -provers game (for every  $k > 3$ ) is defined in the obvious way and therefore omitted.

For a game  $\mathsf{G}^n$  and a strategy  $(p_1, p_2, p_3)$  we define:

$$P_{X^n Y^n Z^n A^n B^n C^n}^{\otimes n}(x^n, y^n, z^n, a^n, b^n, c^n) \triangleq P_{X^n Y^n Z^n}^{\otimes n}(x^n, y^n, z^n) \cdot \Pr[p_1(x^n) = a^n \wedge p_2(y^n) = b^n \wedge p_3(z^n) = c^n]$$

We can now present our theorem:

**Theorem 2.2** *For every  $k \geq 2$ , every positive integer  $n$ , all games  $\mathsf{G} = (X, Y, Z, A, B, C, P_{XYZ}, Q)$ , played in the  $\text{MIP}^\diamond(k, 1)$  model satisfy:*

$$\omega^\diamond(\mathsf{G}^{\otimes n}) \leq \left(1 - \frac{(1 - \omega^\diamond(\mathsf{G}))^2}{100(1 + 4k)^2}\right)^n$$

Holenstein [Hol07] proved the theorem for  $k = 2$ . For simplicity, we will prove the theorem for  $k = 3$  and generalize it for  $k > 3$  in Appendix C .

### 3 Preliminaries

We denote an  $n$ -dimensional vector by superscripts  $n$ , e.g.,  $A^n = (A_1, \dots, A_n)$  where  $A_i$  is its  $i^{\text{th}}$  entry and  $A^{-i} = (A_1, \dots, A_{i-1}, A_{i+1}, \dots, A_n)$ . The statistical difference between two probability distributions  $P$  and  $Q$ , defined over the same sample space  $\Omega$ , is  $\|P - Q\|_1 = 1/2 \sum_{x \in \Omega} |P(x) - Q(x)|$ .

**Definition 3.1 (Divergence)** *We define the Kullback-Leibler divergence, also called the informational divergence or simply divergence. Let  $P$  and  $Q$  be two probability measures defined on the same sample space,  $\Omega$ . The divergence of  $P$  with respect to  $Q$  is:*

$$\mathcal{D}(P \| Q) = \sum_{x \in \Omega} P(x) \log \frac{P(x)}{Q(x)}$$

where  $0 \log \frac{0}{0}$  is defined to be 0 and  $p \log \frac{p}{0}$  where  $p \neq 0$  is defined to be  $\infty$ .

Vaguely speaking, we could think of the divergence as a way to measure the information we gained by knowing that a random variable is distributed according to  $P$  rather than  $Q$ . This indicates how *far*  $Q$  is from  $P$ , if we don't gain much information then the two distributions are very *close* in some sense.

## 4 Proof sketch

We closely follow Holenstein’s proof [Hol07] and generalize it for three provers one round No-Signaling game. Furthermore, in Appendix C, we generalize the result for every  $k \geq 3$  provers.

Fixing a No-Signaling strategy  $(p_1, p_2, p_3)$ , we define  $W_i$  to be the probability of winning game  $i$ . Using this notation the parallel repetition is an upper bound for  $\Pr[W_1 \wedge W_2 \dots \wedge W_n]$ . Since

$$\Pr[W_1 \wedge \dots \wedge W_n] = \Pr[W_{i_1}] \Pr[W_{i_2} | W_{i_1}] \dots \Pr[W_{i_n} | W_{i_1} W_{i_2} \dots W_{i_{n-1}}]$$

we will upper bound  $\Pr[W_{i_m} | W_{i_1} \dots W_{i_{m-1}}]$  for every  $m \leq n^\delta$  (where  $\delta$  is just some small constant).

We will show that conditioning on the event of winning all  $m - 1$  games, i.e., conditioning on  $W_{i_1} \dots W_{i_{m-1}}$ , there is a game  $i_m$  on which the probability of winning that game is at most  $\omega^\diamond(\mathsf{G}) + \epsilon$ . The way to do so, is by showing that given a No-Signaling strategy for the game  $\mathsf{G}^{\otimes n}$  and conditioned on winning  $m - 1$  games, the provers can use this strategy to obtain a No-Signaling strategy for  $\mathsf{G}$ . To obtain a strategy for  $\mathsf{G}$  we will need two lemmas. The first lemma, Lemma 5.2 shows that fixing a strategy and conditioning on the event of winning  $m - 1$  games, there is a coordinate  $i_m$  for which  $P_{X^n Y^n Z^n | W_{i_1} \dots W_{i_{m-1}}}(x^n, y^n, z^n)$  projected on the  $i_m$ th coordinate is similar to  $P_{XYZ}$ . This lemma is Claim 5.1 in Raz’s paper [Raz98] and Lemma 5 in Holenstein’s paper [Hol07]. The second lemma, Lemma 5.4 shows that we can obtain a No-Signaling strategy to play the  $i_m$ th coordinate from a No-Signaling strategy for  $\mathsf{G}^{\otimes n}$  after conditioning on the event  $W_{i_1} \wedge \dots \wedge W_{i_{m-1}}$  (after conditioning we may not obtain a No-Signaling function but we show that there is a No-Signaling function which is very close to it.). This is a generalization of Lemma 23 in Holenstein’s paper [Hol07]. We then conclude that the provers can not win the game  $i_m$  with probability greater than  $\omega^\diamond(\mathsf{G}) + \epsilon$ .

## 5 Technical Lemmas

**Lemma 5.1 (RazHolenstein)** *Let  $P_{U^\ell} = P_{U_1} P_{U_2} \dots P_{U_\ell}$  be a probability distribution over  $U^\ell$  (i.e.,  $P_{U^\ell}$  is a product distribution over  $U_1, \dots, U_\ell$ ) and let  $W$  be some event, then the following holds:*

$$\sum_{i=1}^{\ell} \|P_{U_i | W} - P_{U_i}\| \leq \sqrt{\ell \cdot \log \frac{1}{\Pr[W]}}$$

For completeness, we include the proof of the lemma in Appendix A.

We need the following corollary of Lemma 5.1.

**Corollary 5.2** *Let  $P_{TU^\ell} = P_T P_{U_1 | T} P_{U_2 | T} \dots P_{U_\ell | T}$  and let  $W$  be some event, then the following holds:*

$$\sum_{i=1}^{\ell} \|P_{TU_i | W} - P_T P_{U_i | T}\| \leq \sqrt{\ell \cdot \log \frac{1}{\Pr[W]}}$$

For the proof see Appendix B.

For the second lemma we will need to use the following proposition.

**Proposition 5.3** *Let  $P_{RST}$  be a probability distribution over  $RST$  and let  $\tilde{P}_R$  be some distribution over  $R$ . There exists a distribution  $Q_{RST}$  satisfying the following:*

$$\|Q_{RST} - P_{RST}\| \leq \|P_R - \tilde{P}_R\| \quad (1)$$

$$\|Q_R - \tilde{P}_R\| = 0 \quad (2)$$

$$\|Q_S - P_S\| = 0 \quad (3)$$

$$\|Q_T - P_T\| = 0 \quad (4)$$

The proof is following closely Holenstein's [Hol07] proof of Lemma 22.

**Proof:** We show a finite process for changing  $P_{RST}$  into  $Q_{RST}$  with the desired properties. Let  $H = \{r \mid P_R(r) > \tilde{P}_R(r)\}$  and let  $L = \{r \mid P_R(r) < \tilde{P}_R(r)\}$ . Until  $|H| \neq 0$ , fix some  $r \in H$  and  $r' \in L$  and fix  $s, t$  such that  $P_{RST}(r, s, t) > 0$ . Define,

$$\alpha := \min\{P_{RST}(r, s, t), |P_R(r) - \tilde{P}_R(r)|, |P_R(r') - \tilde{P}_R(r')|\}$$

and set  $P_{RST}(r, s, t) := P_{RST}(r, s, t) - \alpha$  and  $P_{RST}(r', s, t) := P_{RST}(r', s, t) + \alpha$ . The process only decreases  $\|P_R - \tilde{P}_R\|$  and therefore Condition 1 holds. By definition, we continue the process until Condition 2 holds. Since in every iteration, the process decreases some fixed  $(r, s, t)$  by  $\alpha$  and increases  $(r', s, t)$  by  $\alpha$ , for the same  $s, t$  then Condition 3 and Condition 4 are satisfied. ■

**Lemma 5.4** *Let  $P_{XYZRST}$  be a probability distribution over  $XYZRST$  and let  $\bar{P}_{XYZ}$  be some distribution over  $XYZ$ . If*

$$\|\bar{P}_{XYZ}P_{R|X} - P_{XYZR}\| \leq \epsilon_1 \quad (5)$$

$$\|\bar{P}_{XYZ}P_{S|Y} - P_{XYZS}\| \leq \epsilon_2 \quad (6)$$

$$\|\bar{P}_{XYZ}P_{T|Z} - P_{XYZT}\| \leq \epsilon_3 \quad (7)$$

then, there exists a conditional distribution  $Q_{RST|X=x, Y=y, Z=z}$  satisfying the following:

$$\|\bar{P}_{XYZ}Q_{RST|XYZ} - P_{XYZRST}\| \leq \min\{\epsilon_1, \epsilon_2, \epsilon_3\} + 2(\epsilon_1 + \epsilon_2 + \epsilon_3) \quad (8)$$

$$\|Q_{R|X=x, Y=y, Z=z} - Q_{R|X=x}\| = 0 \quad (9)$$

$$\|Q_{S|X=x, Y=y, Z=z} - Q_{S|Y=y}\| = 0 \quad (10)$$

$$\|Q_{T|X=x, Y=y, Z=z} - Q_{T|Z=z}\| = 0 \quad (11)$$

**Proof:** For fixed  $x, y, z$  we apply Lemma 5.3 three times. We first apply the lemma on  $P_{RST|X=x, Y=y, Z=z}$  and  $P_{R|X=x}$  to obtain  $\hat{Q}_{RST|X=x, Y=y, Z=z}$  such that

$$\|\hat{Q}_{RST|X=x, Y=y, Z=z} - P_{RST|X=x, Y=y, Z=z}\| \leq |P_{R|X=x, Y=y, Z=z} - P_{R|X=x}|$$

$$\|\hat{Q}_{R|X=x, Y=y, Z=z} - P_{R|X=x}\| = 0$$

$$\|\hat{Q}_{S|X=x, Y=y, Z=z} - P_{S|X=x, Y=y, Z=z}\| = 0$$

$$\|\hat{Q}_{T|X=x, Y=y, Z=z} - P_{T|X=x, Y=y, Z=z}\| = 0$$

Applying Lemma 5.3 on  $\hat{Q}_{RST|X=x,Y=y,Z=z}$  and  $P_{S|Y=y}$  and combining the previous result we obtain  $\tilde{Q}_{RST|X=x,Y=y,Z=z}$  such that

$$\begin{aligned} \|\tilde{Q}_{RST|X=x,Y=y,Z=z} - \hat{Q}_{RST|X=x,Y=y,Z=z}\| &\leq \|P_{S|X=x,Y=y,Z=z} - P_{S|Y=y}\| \\ \|\tilde{Q}_{R|X=x,Y=y,Z=z} - P_{R|X=x}\| &= 0 \\ \|\tilde{Q}_{S|X=x,Y=y,Z=z} - P_{S|Y=y}\| &= 0 \\ \|\tilde{Q}_{T|X=x,Y=y,Z=z} - \hat{Q}_{T|X=x,Y=y,Z=z}\| &= 0 \end{aligned}$$

Apply Lemma 5.3 again, this time on  $\tilde{Q}_{RST|X=x,Y=y,Z=z}$  and  $\tilde{Q}_{T|Z=z}$ , we obtain  $Q_{RST|X=x,Y=y,Z=z}$  such that

$$\begin{aligned} \|Q_{RST|X=x,Y=y,Z=z} - \tilde{Q}_{RST|X=x,Y=y,Z=z}\| &\leq \|P_{T|X=x,Y=y,Z=z} - P_{T|Z=z}\| \\ \|Q_{R|X=x,Y=y,Z=z} - P_{R|X=x}\| &= 0 \\ \|Q_{S|X=x,Y=y,Z=z} - P_{S|Y=y}\| &= 0 \\ \|Q_{T|X=x,Y=y,Z=z} - P_{T|Z=z}\| &= 0 \end{aligned}$$

From Condition 5, Condition 6 and Condition 7 we obtain:  $\|\bar{P}_{XYZ} - P_{XYZ}\| \leq \min\{\epsilon_1, \epsilon_2, \epsilon_3\}$   
Hence,

$$\begin{aligned} &\|\bar{P}_{XYZ}Q_{RST|XYZ} - P_{XYZ}RST\| \\ &\leq \min\{\epsilon_1, \epsilon_2, \epsilon_3\} + \|P_{XYZ}Q_{RST|XYZ} - P_{XYZ}RST\| \\ &= \min\{\epsilon_1, \epsilon_2, \epsilon_3\} + \sum_{xyz} P_{XYZ}(x, y, z) \|Q_{RST|X=x,Y=y,Z=z} - P_{RST|X=x,Y=y,Z=z}\| \\ &\leq \min\{\epsilon_1, \epsilon_2, \epsilon_3\} + \sum_{xyz} P_{XYZ}(x, y, z) \cdot \\ &\quad (|P_{R|X=x,Y=y,Z=z} - P_{R|X=x}| + \|P_{S|X=x,Y=y,Z=z} - P_{S|Y=y}\| + \|P_{T|X=x,Y=y,Z=z} - P_{T|Z=z}\|) \\ &\leq \min\{\epsilon_1, \epsilon_2, \epsilon_3\} + \|P_{XYZR} - P_{XYZ}P_{R|X}\| + \|P_{XYZS} - P_{XYZ}P_{S|Y}\| + \|P_{XYZT} - P_{XYZ}P_{T|Z}\| \\ &\leq \min\{\epsilon_1, \epsilon_2, \epsilon_3\} + 2(\epsilon_1 + \epsilon_2 + \epsilon_3) \end{aligned}$$

■

## 6 Parallel Repetition Theorem

**Proposition 6.1** *For every game  $G = (X, Y, Z, A, B, C, P_{XYZ}, Q)$  fix any No-Signaling strategy for the  $n$ -fold parallel repetition game,  $G^{\otimes n}$ , and let  $W = W_{i_1} \wedge \dots \wedge W_{i_{m-1}}$  be the event of winning on some fixed  $i_1, \dots, i_{m-1}$  coordinates with respect to that strategy. There exists a coordinate  $i_m$  such that*

$$\Pr[W_{i_m}|W] \leq \omega^\diamond(G) + 13\sqrt{\frac{1}{n-m} \log\left(\frac{1}{\Pr[W]}\right)}$$

**Proof:** Assume without loss of generality that  $i_1, \dots, i_{m-1} \in \{n-m+1, \dots, n\}$  (the last  $m$  coordinates). Let  $T = (X^n, A^n)$  and  $U^{n-m} = (Y^{n-m}, Z^{n-m})$  then from Lemma 5.2 we obtain:

$$\sum_{i=1}^{n-m} \|P_{X^n A^n Y_i Z_i | W} - P_{X^n A^n | W} P_{Y_i Z_i | X^n A^n}\| \leq \sqrt{(n-m) \log \frac{1}{\Pr[W]}}$$

Since the strategy is No-Signaling:

$$\sum_i^{n-m} \|\mathbb{P}_{X^n A^n Y_i Z_i | W} - \mathbb{P}_{X^n A^n | W} \mathbb{P}_{Z_i Y_i | X_i}\| \leq \sqrt{(n-m) \log \frac{1}{\Pr[W]}}.$$

This can be written as:

$$\sum_i^{n-m} \|\mathbb{P}_{X^n A^n Y_i Z_i | W} - \mathbb{P}_{X_i | W} \mathbb{P}_{X^{-i} A^n | X_i, W} \mathbb{P}_{Z_i Y_i | X_i}\| \leq \sqrt{(n-m) \log \frac{1}{\Pr[W]}}. \quad (12)$$

Applying Lemma 5.1 with  $U^{n-m} = X^{n-m}$  we obtain:

$$\sum_i^{n-m} \|\mathbb{P}_{X_i | W} - \mathbb{P}_{X_i}\| \leq \sqrt{(n-m) \log \frac{1}{\Pr[W]}} \quad (13)$$

Combining Equation 12 and Equation 13 yields:

$$\sum_i^{n-m} \|\mathbb{P}_{X^n A^n Y_i Z_i | W} - \mathbb{P}_{X_i} \mathbb{P}_{X^{-i} A^n | X_i, W} \mathbb{P}_{Z_i Y_i | X_i}\| \leq 2 \sqrt{(n-m) \log \frac{1}{\Pr[W]}}$$

This can be written as:

$$\sum_i^{n-m} \|\mathbb{P}_{X^n A^n Y_i Z_i | W} - \mathbb{P}_{X_i Y_i Z_i} \mathbb{P}_{X^{-i} A^n | X_i, W}\| \leq 2 \sqrt{(n-m) \log \frac{1}{\Pr[W]}}$$

Since  $\mathbb{P}_{X_i Y_i Z_i} = \mathbb{P}_{XYZ}$ ,

$$\sum_i^{n-m} \|\mathbb{P}_{X^n A^n Y_i Z_i | W} - \mathbb{P}_{XYZ} \mathbb{P}_{X^{-i} A^n | X_i, W}\| \leq 2 \sqrt{(n-m) \log \frac{1}{\Pr[W]}} \quad (14)$$

Similar argument for  $T = (Y^n, B^n)$  and  $U^{n-m} = (X^{n-m}, Z^{n-m})$  yields:

$$\sum_i^{n-m} \|\mathbb{P}_{Y^n B^n X_i Z_i | W} - \mathbb{P}_{XYZ} \mathbb{P}_{Y^{-i} B^n | Y_i, W}\| \leq 2 \sqrt{(n-m) \log \frac{1}{\Pr[W]}} \quad (15)$$

And for  $T = (Z^n, C^n)$  and  $U^{n-m} = (X^{n-m}, Y^{n-m})$  yields:

$$\sum_i^{n-m} \|\mathbb{P}_{Z^n C^n X_i Y_i | W} - \mathbb{P}_{XYZ} \mathbb{P}_{Z^{-i} C^n | Z_i, W}\| \leq 2 \sqrt{(n-m) \log \frac{1}{\Pr[W]}} \quad (16)$$

By Lemma 5.4, there exists a distribution  $\mathbb{Q}_{X^{-i} A^n Y^{-i} B^n Y^{-i} C^n | X_i=x, Y_i=y, Z_i=z}$  which can be implemented by a No-Signaling function and satisfy:

$$\sum_{i=1}^{n-m} \|\mathbb{P}_{XYZ} \mathbb{Q}_{X^{-i} A^n Y^{-i} B^n Y^{-i} C^n | XYZ} - \mathbb{P}_{XYZ} \mathbb{P}_{X^{-i} A^n Y^{-i} B^n Y^{-i} C^n | W}\| \leq 13 \sqrt{(n-m) \log \left( \frac{1}{\Pr[W]} \right)}.$$

Therefore, there exists a coordinate  $i_m$  such that

$$\|\mathbb{P}_{XYZ} \mathbb{Q}_{X^{-i_m} A^n Y^{-i_m} B^n Y^{-i_m} C^n | XYZ} - \mathbb{P}_{XYZ} \mathbb{P}_{X^{-i_m} A^n Y^{-i_m} B^n Y^{-i_m} C^n | W}\| \leq 13 \sqrt{\frac{1}{n-m} \log \left( \frac{1}{\Pr[W]} \right)}.$$

Hence, given input  $(X, Y, Z)$  for the game  $G$ , Alice, Bob and Charlie can use the No-Signaling Strategy for  $G^{\otimes n}$  to obtain a No-Signaling strategy for  $G$ . The provers play  $G$  in the  $i_m$  coordinate and answer  $A_{i_m}, B_{i_m}, C_{i_m}$  (and ignoring the redundant information). Thus there is a coordinate  $i_m$  on which

$$\Pr[W_{i_m} | W] \leq \omega^\diamond(G) + 13\sqrt{\frac{1}{n-m} \log\left(\frac{1}{\Pr[W]}\right)}$$

■

**Theorem 6.2** For all games  $G = (X, Y, Z, A, B, C, P_{XYZ}, Q)$  and any positive integer  $n$ ,

$$\omega^\diamond(G^{\otimes n}) \leq \left(1 - \frac{(1 - \omega^\diamond(G))^2}{4000}\right)^n$$

**Proof:** Fix any strategy for the  $n$ -folded parallel repetition game  $G^{\otimes n}$  and let  $q_m = \Pr[W_{i_1} \wedge \dots \wedge W_{i_m}]$ . By Proposition 6.1 we obtain:

$$q_{m+1} \leq q_m \cdot \left(\omega^\diamond(G) + 13\sqrt{\frac{1}{n-m} \log\left(\frac{1}{q_m}\right)}\right)$$

We show by induction that  $q_{m+1} \leq \left(\frac{1+\omega^\diamond(G)}{2}\right)^{m+1}$  for any  $m+1 \leq \frac{(1-\omega^\diamond(G))(n-m)}{1000}$ . If  $q_m \leq \left(\frac{1+\omega^\diamond(G)}{2}\right)^{m+1}$  then the claim immediately follows. If  $q_m > \left(\frac{1+\omega^\diamond(G)}{2}\right)^{m+1}$  then,

$$\log\left(\frac{1}{q_m}\right) \leq \log\left(\frac{1+\omega^\diamond(G)}{2}\right)^{-(m+1)}.$$

Since for any  $\alpha, \beta < 1$ ,  $(1-\alpha)^b \leq 1-\alpha\beta$ , then  $(1-\frac{1}{2})^{1-\omega^\diamond(G)} \leq (1-\frac{1-\omega^\diamond(G)}{2})$  and we obtain that

$$\log\left(\frac{1+\omega^\diamond(G)}{2}\right)^{-(m+1)} = \log\left(1 - \frac{1-\omega^\diamond(G)}{2}\right)^{-(m+1)} \leq \log\left(\frac{1}{2}\right)^{-(m+1)(1-\omega^\diamond(G))} = (m+1)(1-\omega^\diamond(G))$$

Thus for any  $m$  satisfying  $m+1 \leq \frac{(1-\omega^\diamond(G))(n-m)}{1000}$ ,

$$q_{m+1} \leq q_m \cdot \left(\omega^\diamond(G) + 13\sqrt{\frac{1}{n-m} (m+1)(1-\omega^\diamond(G))}\right) \leq q_m \cdot \left(\frac{1+\omega^\diamond(G)}{2}\right)$$

combining the induction hypothesis we obtain  $q_m \cdot \left(\frac{1+\omega^\diamond(G)}{2}\right) \leq \left(\frac{1+\omega^\diamond(G)}{2}\right)^{m+1}$ . Taking  $m = n\frac{(1-\omega^\diamond(G))}{2000}$  we get,

$$q_m \leq \left(1 - \frac{1-\omega^\diamond(G)}{2}\right)^{\frac{n(1-\omega^\diamond(G))}{2000}} \leq \left(1 - \frac{(1-\omega^\diamond(G))^2}{4000}\right)^n$$

■

## 7 Acknowledgement

We would like to express my deepest gratitude to Oded Regev and Ran Raz for very valuable discussions on this subject and for their comments on the previous version of this paper.

## References

- [CCL92] J.-Y. Cai, A. Condon, and R. J. Lipton. On games of incomplete information. *Theoret. Comput. Sci.*, 103(1):25–38, 1992. ISSN 0304-3975. 7th Annual Symposium on Theoretical Aspects of Computer Science (STACS 90) (Rouen, 1990).
- [CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, Oct 1969. doi:10.1103/PhysRevLett.23.880.
- [CT06] T. M. Cover and J. A. Thomas. *Elements of information theory*. Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, second edition, 2006. ISBN 978-0-471-24195-9; 0-471-24195-4.
- [Fei91] U. Feige. On the success probability of the two provers in one-round proof systems. In *Structure in Complexity Theory Conference*, pages 116–123. 1991.
- [Fei95] U. Feige. Error reduction by parallel repetition - the state of the art. Technical Report CS95-32, Weizmann Institute, 1, 1995.
- [FK94] U. Feige and J. Kilian. Two prover protocols: low error at affordable rates. In *Proceedings of the 26th Annual Symposium on the Theory of Computing*, pages 172–183. ACM Press, New York, May 1994. ISBN 0-89791-663-8.
- [FL92] U. Feige and L. Lovász. Two-prover one-round proof systems: their power and their problems (extended abstract). In *STOC '92: Proceedings of the twenty-fourth annual ACM symposium on Theory of computing*, pages 733–744. ACM Press, New York, NY, USA, 1992. ISBN 0-89791-511-9. doi:<http://doi.acm.org/10.1145/129712.129783>.
- [For89] L. J. Fortnow. Complexity - theoretic aspects of interactive proof systems. Technical Report MIT-LCS//MIT/LCS/TR-447, Department of Mathematics, Massachusetts Institute of Technology, 1989.
- [FV02] U. Feige and O. Verbitsky. Error reduction by parallel repetition—a negative result. *Combinatorica*, 22(4):461–478, 2002. ISSN 0209-9683.
- [Hol07] T. Holenstein. Parallel repetition: simplifications and the no-signaling case. In *STOC'07: Proceedings of the 39th Annual ACM Symposium on Theory of Computing*. 2007.
- [Raz98] R. Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803 (electronic), 1998. ISSN 0097-5397.

## A Proof of Lemma 5.1

**Lemma A.1 (Raz)** *Let  $P_{U^\ell} = P_{U_1}P_{U_2}\cdots P_{U_\ell}$  and let  $W$  be some event, then the following holds:*

$$\sum_i^\ell \|P_{U_i|W} - P_{U_i}\| \leq \sqrt{\ell \cdot \log \frac{1}{\Pr[W]}}$$

**Proof:** This lemma appears in [Raz98] and in [Hol07]. We present Holenstein's [Hol07] proof of the lemma. For the proof of the lemma we'll need to use some known entropy arguments such as  $\mathcal{D}(P\|Q) \geq (\|P - Q\|_1)^2$  where  $P$  and  $Q$  are two distributions over the same sampling space. The proof can be found in [CT06] Lemma 12.6.1. Another argument we will use is that for a probability distribution  $P_U^\ell$  which is a product distribution over  $U_1 \dots U_\ell$  the following holds:  $\sum_{i=1}^\ell \mathcal{D}(P_{U_i}\|Q_{U_i}) \leq \mathcal{D}(P_{U^\ell}\|Q_{U^\ell})$ . We can now prove the lemma:

$$\begin{aligned} \sum_{i=1}^\ell (\|P_{U_i|W} - P_{U_i}\|)^2 &\leq \sum_{i=1}^\ell \mathcal{D}(P_{U_i|W}\|P_{U_i}) \leq \mathcal{D}(P_{U^\ell|W}\|P_{U^\ell}) = \sum_{u^\ell \in U^\ell} P_{U^\ell|W}(u^\ell) \log \left( \frac{P_{U^\ell|W}(u^\ell)}{P_{U^\ell}(u^\ell)} \right) \\ &= \sum_{u^\ell \in U^\ell} P_{U^\ell|W}(u^\ell) \log \left( \frac{\Pr[W|U^\ell = u^\ell]}{\Pr[W]} \right) \\ &\leq \log \left( \frac{1}{\Pr[W]} \right) + \sum_{u^\ell \in U^\ell} P_{U^\ell|W}(u^\ell) \log(\Pr[W|U^\ell = u^\ell]) \leq \log \left( \frac{1}{\Pr[W]} \right) \end{aligned}$$

■

## B Proof of Corollary 5.2

**Proof:**

$$\begin{aligned} \sum_{i=1}^\ell \|P_{TU_i|W} - P_{T|W}P_{U_i|T}\| &= \sum_{i=1}^\ell \sum_{t \in T, u \in U_i} |P_{TU_i|W}(t, u) - P_{T|W}(t)P_{U_i|T=t}(u)| \\ &= \sum_{i=1}^\ell \sum_{t \in T, u \in U_i} |P_{T|W}(t)P_{U_i|W, T=t}(u) - P_{T|W}(t)P_{U_i|T=t}(u)| \\ &= \sum_{t \in T} P_{T|W}(t) \cdot \sum_{i=1}^\ell \|P_{U_i|W, T=t}(u) - P_{U_i|T=t}(u)\| \\ &\leq \sum_{t \in T} P_{T|W}(t) \cdot \sqrt{\ell \cdot \log \left( \frac{1}{\Pr[W|T=t]} \right)} \\ &\leq \sqrt{\ell \cdot \log \left( \sum_{t \in T} P_{T|W}(t) \frac{1}{\Pr[W|T=t]} \right)} \\ &= \sqrt{\ell \cdot \log \left( \sum_{t \in T} \frac{\Pr(T=t \wedge W)}{\Pr[W]} \frac{\Pr[T=t]}{\Pr[W \wedge T=t]} \right)} \\ &= \sqrt{\ell \cdot \log \frac{1}{\Pr[W]}} \end{aligned}$$

Where the first inequality follows from Lemma 5.1 and the second follows from Jensen's inequality on the concave function  $\sqrt{\log(\cdot)}$  ■

## C generalizing for $k > 3$

Lemma 5.4 for  $k > 3$

**Lemma C.1** *Let  $P_{V_1, \dots, V_k}$  be a probability distribution over  $V_1 \dots V_k$  and for every  $1 \leq i \leq k$ , let  $P_{\tilde{V}_i}$  be some distribution over  $V_i$ . If for every  $i \in \{1, \dots, k\}$ ,  $\|P_{V_i} - P_{\tilde{V}_i}\| \leq \epsilon_i$  then, there exists a distribution  $Q_{V_1, \dots, V_k}$  satisfying the following:*

$$\|Q_{V_1, \dots, V_k} - P_{V_1, \dots, V_k}\| \leq 2 \sum_{i=1}^k \epsilon_i + \min_i \epsilon_i$$

and for every  $i$   $\|Q_{V_i} - P_{\tilde{V}_i}\| = 0$

**Lemma C.2** *Let  $P_{U_1, \dots, U_k, V_1, \dots, V_k}$  be a probability distribution over  $U_1, \dots, U_k, V_1, \dots, V_k$  and let  $P_{U'_1, \dots, U'_k}$  be some distribution over  $U_1, \dots, U_k$ . If for every  $i$ ,*

$$\|P_{U'_1, \dots, U'_k} P_{V_i|U_i} - P_{U_1, \dots, U_k, V_i}\| \leq \epsilon_1$$

then, there exists a conditional distribution  $Q_{V_1, \dots, V_k|X=x, Y=y, Z=z}$  satisfying the following:

$$\|Q_{V_1, \dots, V_k|U_1=u_1, \dots, U_k=u_k} - P_{V_1, \dots, V_k|U_1=u_1, \dots, U_k=u_k}\| \leq \min_i \{\epsilon_i\} \quad (17)$$

$$\forall i \in \{1, \dots, k\}, \quad \|Q_{V_i|U_1=u_1, \dots, U_k=u_k} - Q_{V_i|U_i=u_i}\| = 0 \quad (18)$$

$$(19)$$

**Theorem C.3** *For every  $k \geq 3$ , every positive integer  $n$ , all games  $G = (X, Y, Z, A, B, C, P_{XYZ}, Q)$ , played in the  $\text{MIP}^\diamond(k, 1)$  model satisfy:*

$$\omega^\diamond(G^{\otimes n}) \leq \left(1 - \frac{(1 - \omega^\diamond(G))^2}{100(1 + 4k)^2}\right)^n$$

**Proof:** Fix any strategy for the  $n$ -folded parallel repetition game  $G^{\otimes n}$  and let  $q_m = \Pr[W_{i_1} \wedge \dots \wedge W_{i_m}]$ . By Proposition 6.1 we obtain:

$$q_{m+1} \leq q_m \cdot \left( \omega^\diamond(G) + 13 \sqrt{\frac{1}{n-m} \log\left(\frac{1}{q_m}\right)} \right)$$

We show by induction that  $q_{m+1} \leq \left(\frac{1+\omega^\diamond(G)}{2}\right)^{m+1}$  for any  $m+1 \leq \frac{(1-\omega^\diamond(G))(n-m)}{1000}$ . If  $q_m \leq \left(\frac{1+\omega^\diamond(G)}{2}\right)^{m+1}$  then the claim immediately follows. If  $q_m > \left(\frac{1+\omega^\diamond(G)}{2}\right)^{m+1}$  then,

$$\log\left(\frac{1}{q_m}\right) \leq \log\left(\frac{1+\omega^\diamond(G)}{2}\right)^{-(m+1)}.$$

Since for any  $\alpha, \beta < 1$ ,  $(1 - \alpha)^b \leq 1 - \alpha\beta$ , then  $(1 - \frac{1}{2})^{1 - \omega^\diamond(G)} \leq (1 - \frac{1 - \omega^\diamond(G)}{2})$  and we obtain that

$$\log \left( \frac{1 + \omega^\diamond(G)}{2} \right)^{-(m+1)} = \log \left( 1 - \frac{1 - \omega^\diamond(G)}{2} \right)^{-(m+1)} \leq \log \left( \frac{1}{2} \right)^{-(m+1)(1 - \omega^\diamond(G))} = (m+1)(1 - \omega^\diamond(G))$$

Thus for any  $m$  satisfying  $m + 1 \leq \frac{(1 - \omega^\diamond(G))(n - m)}{1000}$ ,

$$q_{m+1} \leq q_m \cdot \left( \omega^\diamond(G) + 13 \sqrt{\frac{1}{n - m} (m + 1)(1 - \omega^\diamond(G))} \right) \leq q_m \cdot \left( \frac{1 + \omega^\diamond(G)}{2} \right)$$

combining the induction hypothesis we obtain  $q_m \cdot \left( \frac{1 + \omega^\diamond(G)}{2} \right) \leq \left( \frac{1 + \omega^\diamond(G)}{2} \right)^{m+1}$ . Taking  $m = n \frac{(1 - \omega^\diamond(G))}{2000}$  we get,

$$q_m \leq \left( 1 - \frac{1 - \omega^\diamond(G)}{2} \right)^{\frac{n(1 - \omega^\diamond(G))}{2000}} \leq \left( 1 - \frac{(1 - \omega^\diamond(G))^2}{4000} \right)^n$$

■