On the Parallel Repetition of Multi-Player Games: The No-Signaling Case

Harry Buhrman[*1,2], **Serge Fehr**[†1], **and Christian Schaffner**[‡2,1]

1 **Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands**
2 **Institute for Logic, Language and Computation (ILLC),**
University of Amsterdam, The Netherlands

Abstract

We consider the natural extension of two-player nonlocal games to an arbitrary number of players. An important question for such nonlocal games is their behavior under parallel repetition. For *two-player* nonlocal games, it is known that both the *classical* and the *non-signaling* value of any game converges to zero exponentially fast under parallel repetition, given that the game is non-trivial to start with (i.e., has classical/non-signaling value < 1). Very recent results [8, 6, 11] show similar behavior of the *quantum* value of a two-player game under parallel repetition. For nonlocal games with three or more players, very little is known up to present on their behavior under parallel repetition; this is true for the classical, the quantum and the non-signaling value.

In this work, we show a parallel repetition theorem for the *non-signaling* value of a large class of multi-player games, for an arbitrary number of players. Our result applies to all multi-player games for which all possible combinations of questions have positive probability; this class in particular includes all *free* games, in which the questions to the players are chosen independently. Specifically, we prove that if the original game $\mathcal{G}$ has a non-signaling value $v_{\text{ns}}(\mathcal{G}) < 1$, then the non-signaling value of the n-fold parallel repetition is exponentially small in n. Stronger than that, we prove that the probability of winning more than $(v_{\text{ns}}(\mathcal{G}) + \delta) \cdot n$ parallel repetitions is exponentially small in n (for any $\delta > 0$).

Our parallel repetition theorem for multi-player games is weaker than the known parallel repetition results for two-player games in that the rate at which the non-signaling value of the game decreases not only depends on the non-signaling value of the original game (and the number of possible responses), but on the complete description of the game. Nevertheless, we feel that our result is a first step towards a better understanding of the parallel repetition of nonlocal games with more than two players.

1998 ACM Subject Classification E.4 Coding and Information Theory

Keywords and phrases Parallel repetition, non-signaling value, multi-player non-local games

Digital Object Identifier 10.4230/LIPIcs.xxx.yyy.p

1 Introduction

Background.

In an m-player nonlocal game $\mathcal{G}$, m players receive respective questions $x_1, \ldots, x_m$, chosen according to some joint probability distribution, and the task of the m players is to provide "good" answers $a_1, \ldots, a_m$, *without communicating* with each other. The players are said to

[*] h.buhrman@cwi.nl
[†] s.fehr@cwi.nl
[‡] c.schaffner@uva.nl

© Harry Buhrman, Serge Fehr, and Christian Schaffner;
licensed under Creative Commons License CC-BY

Conference title on which this volume is based on.
Editors: Billy Editor, Bill Editors; pp. 1–12
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

win the game if the given answers jointly satisfy some specific property with respect to the given questions. The *value* of a given game is defined to be the maximal winning probability of the players. One distinguishes between the classical, the quantum, and the non-signaling value, depending on whether the players are restricted to be classical, may share entanglement and do quantum measurements, or are allowed to make use of any hypothetical strategy that does not violate non-signaling.

An important question for nonlocal games is their behavior under parallel repetition. This question is somewhat understood in the case of *two* players, where $m = 2$. Indeed, Raz showed in his celebrated parallel repetition theorem [15] that if the classical value of a two-player game $\mathcal{G}$ is $v_{\mathrm{c}}(\mathcal{G}) < 1$ then the classical value $v_{\mathrm{c}}(\mathcal{G}^n)$ of the n-fold parallel repetition of $\mathcal{G}$ satisfies $v_{\mathrm{c}}(\mathcal{G}^n) \leq \bar{v}_{\mathrm{c}}(\mathcal{G})^{n/\log(s)}$, where s denotes the number of possible pairs of answers a_1 and a_2, and $\bar{v}_{\mathrm{c}}(\mathcal{G}) < 1$ only depends on $v_{\mathrm{c}}(\mathcal{G})$. Raz's result was improved and simplified by Holenstein [10], who gave an explicit and tighter dependency between $\bar{v}_{\mathrm{c}}(\mathcal{G})$ and $v_{\mathrm{c}}(\mathcal{G})$, namely $\bar{v}_{\mathrm{c}}(\mathcal{G}) = 1 - \frac{1}{6000}(1 - v_{\mathrm{c}}(\mathcal{G}))^3$. Holenstein also showed that a similar result holds for the non-signaling value of any two-player game: $v_{\mathrm{ns}}(\mathcal{G}^n) \leq \bar{v}_{\mathrm{ns}}(\mathcal{G})^n$ for $\bar{v}_{\mathrm{ns}}(\mathcal{G}) = 1 - \frac{1}{6400}(1 - v_{\mathrm{ns}}(\mathcal{G}))^2$. Parallel repetition results for the quantum value of two-player games were first derived for certain special classes of games, like XOR-games [7] or unique games [12], or for a non-standard parallel repetition where the different repetitions of the original game are intertwined with modified versions of the original game [13]. Recently, several results about the parallel repetition of more general quantum games have been obtained [8, 6, 11].

There are further improvements to the above results on two-player games. For instance, Rao [14] showed a *concentration* result for the classical value of any two-player game, saying that the probability to win more than $(v_{\mathrm{ns}}(\mathcal{G}) + \delta) \cdot n$ out of the n repetitions is exponentially small (for any $\delta > 0$).[1] Furthermore, he improved the bound on the classical value under parallel repetition for *projection* games. A similar improvement on the bound on the classical value under parallel repetition was given by Barak *et al.* [2] for *free* games, together with a further improvement, namely a *strong* parallel repetition theorem (meaning that meaning that $v_{\mathrm{c}}(\mathcal{G}^n) \leq v_{\mathrm{c}}(\mathcal{G})^{\Omega(n)}$), for *free projection* games.

When considering multi-player nonlocal games with strictly more than 2 players, to the best of our knowledge, very little is known about their behavior under parallel repetition, except for trivial cases. This applies to the classical, the quantum, and the non-signaling value. In [16], Rosen proved a parallel-repetition result for more than 2 players. While her proof strategy is very similar to ours (closely following [10]), a somewhat unnatural definition of multi-player non-signaling correlations is used where no $m - 1$ provers together can signal to the remaining prover. In our (standard) model, one also demands that any subset (of arbitrary size) of provers can not signal to the remaining provers.

Another result about multi-player games is by Briët *et al.* [3] about the related question of XOR repetition. They show the existence of a 3-player XOR game whose classical value of the XOR repetition is bounded from below by a constant (independent of the number of repetitions). Hence, XOR repetition does not hold for this game (but parallel repetition might still hold). Our result does not imply anything about those games, because the non-signaling value of XOR games is always 1.

Possible applications of our result could be of cryptographic nature where the hardness of a basic task is amplified by parallel repetition. A likely scenario for applying our results (and

[1] Rao claims the concentration result only for the classical value, but the same techniques also apply to the non-signaling value.

our original motivation to study the problem) is position-based quantum cryptography [4, 5], in the spirit of a recent result on parallel repetition of a particular game [18]. However, as our result only applies to a restricted class of games, we were not able yet to apply it to in this cryptographic context.

Our Results.

We show a parallel repetition and a concentration theorem for the non-signaling value of m-player games for any m, for a large class of games. The class of games to which our result applies consists of all multi-player games with *complete support*, meaning that all possible combinations of questions $x_1, \ldots, x_m$ must have positive probability of being asked. This class of games in particular includes all *free* games, in which the questions to the different players are chosen independently. For any m-player game $\mathcal{G}$ with complete support, we show that if $v_{\text{ns}}(\mathcal{G}) < 1$ then there exists $\bar{v}_{\text{ns}}(\mathcal{G}) < 1$ so that $v_{\text{ns}}(\mathcal{G}^n) \leq \bar{v}_{\text{ns}}(\mathcal{G})^n$, and the probability of winning more than $(v_{\text{ns}}(\mathcal{G}) + \delta) \cdot n$ out of the n repetitions with an arbitrary non-signaling strategy is exponentially small (for any $\delta > 0$).

We point out that our parallel repetition result for multi-player games (with complete support) is of a weaker nature than the parallel repetition results for two-player games discussed above, in that in our result the constant $\bar{v}_{\text{ns}}(\mathcal{G})$ depends on the complete description of the game $\mathcal{G}$, and not just on its non-signaling value $v_{\text{ns}}(\mathcal{G})$. Still, our result is the first that shows a parallel repetition result for a large class of m-player games with $m > 2$ for one of the three values (the classical, quantum or non-signaling) of interest.

For proving our results, we borrow and extend tools from [10] and [14], and combine them with some new technique. The new technique involves considering strategies that are *almost* non-signaling, meaning that the non-signaling properties only hold up to some small error. We then show (Proposition 18) and use in our proof that the non-signaling value of a game is *robust* under extending the quantification over all non-signaling strategies to all almost non-signaling strategies.

2 Preliminaries

2.1 Basic Notation

For any m-partite set $\mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_m$, any m-tuple $x = (x_1, \ldots, x_m) \in \mathcal{X}$, and any index set $I = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, m\}$, we write $\mathcal{X}_I$ to denote the k-partite set $\mathcal{X} = \mathcal{X}_{i_1} \times \cdots \times \mathcal{X}_{i_k}$, and we write x_I to denote the k-tuple $x = (x_{i_1}, \ldots, x_{i_k}) \in \mathcal{X}_I$. To denote elements from the n-fold Cartesian product of an m-partite set $\mathcal{X}$ as above, we write $\boldsymbol{x} = (x^1, \ldots, x^n) \in \mathcal{X} \times \cdots \times \mathcal{X}$ with $x^i = (x^i_1, \ldots, x^i_m) \in \mathcal{X}$. For $i \in \{1, \ldots, m\}$, we then write $\boldsymbol{x}_i$ for $\boldsymbol{x}_i = (x^1_i, \ldots, x^n_i)$, and for $I = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, m\}$, x^ℓ_I is naturally understood as $x^\ell_I = (x^\ell_{i_1}, \ldots, x^\ell_{i_k})$ and $\boldsymbol{x}_I$ as $\boldsymbol{x}_I = (\boldsymbol{x}_{i_1}, \ldots, \boldsymbol{x}_{i_k})$. Corresponding notation is used for random variables X over $\mathcal{X}$ and $\boldsymbol{X}$ over $\mathcal{X} \times \cdots \times \mathcal{X}$.

2.2 Probabilities and Random Variables

We consider finite probability spaces, given by a non-empty finite sample space Ω and a probability function $P : \Omega \to [0, 1]$. A random variable is a function $X : \Omega \to \mathcal{X}$ from Ω into some finite set $\mathcal{X}$. The distribution of X, denoted as P_X, is given by $P_X(x) = P[\,X\!=\!x\,] = P[\,\{\omega \in \Omega \,|\, X(\omega)\!=\!x\}\,]$. The joint distribution of a pair of random variables X and Y is denoted by P_{XY}, i.e., $P_{XY}(x, y) = P[\,X\!=\!x \wedge Y\!=\!y\,]$, and the conditional distribution of X given Y is denoted by $P_{X|Y}$ and defined as $P_{X|Y}(x|y) = P_{XY}(x, y)/P_Y(y)$ for all x and y

with $P_Y(y) > 0$. An event $\mathcal{E}$ is a subset of Ω, and the conditional distribution of a random variable X given $\mathcal{E}$ is denoted as $P_{X|\mathcal{E}}$ and given by $P_{X|\mathcal{E}}(x) = P[\,X{=}x \wedge \mathcal{E}\,]/P[\,\mathcal{E}\,]$.

The variational (or statistical) distance between two probability distributions P_X and Q_X for the same random variable $X : \Omega \to \mathcal{X}$ over two probability spaces (Ω, P) and (Ω, Q) (with the same Ω), is defined as

$$\|P_X - Q_X\| := \frac{1}{2} \sum_{x \in \mathcal{X}} |P_X(x) - Q_X(x)|$$

If P_X and Q_X are ε-close in variational distance, we also write $P_X \approx_\varepsilon Q_X$.

Usually, we leave the probability space (Ω, P) etc. implicit, and understand random variables $X, Y, \ldots$ to be defined by their joint distribution $P_{XY\cdots}$, or by some "experiment" that uniquely determines their joint distribution.

2.3 Some Useful Facts

The following lemma states that the variational distance cannot increase when less information is taken into account.

▶ **Lemma 1.** *Let P_{XY} and Q_{XY} be joint distributions for random variables X and Y with respective ranges $\mathcal{X}$ and $\mathcal{Y}$, and let P_X and Q_X be the corresponding marginals. Then,*

$$\|P_X - Q_X\| \leq \|P_{XY} - Q_{XY}\|\,.$$

Proof.

$$\begin{aligned}\|P_X - Q_X\| &= \frac{1}{2} \sum_{x \in \mathcal{X}} |P_X(x) - Q_X(x)| = \frac{1}{2} \sum_{x \in \mathcal{X}} \left| \sum_{y \in \mathcal{Y}} \big(P_{XY}(x,y) - Q_{XY}(x,y)\big) \right| \\ &\leq \frac{1}{2} \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} |P_{XY}(x,y) - Q_{XY}(x,y)| = \|P_{XY} - Q_{XY}\|\,.\end{aligned}$$

◀

The next lemma is due to Holenstein [10] (a simplified version of his Corollary 6).

▶ **Lemma 2.** *Let T and $U^1, \ldots, U^L$ be random variables with distribution $P_{TU^1\cdots U^L} = P_T \cdot P_{U^1|T} \cdots P_{U^L|T}$ (i.e. the U^ℓ's are conditionally independent given T), and let $\mathcal{E}$ be an event. Then*

$$\sum_{\ell=1}^{L} \left\|P_{TU^\ell|\mathcal{E}} - P_{T|\mathcal{E}} \cdot P_{U^\ell|T}\right\| \leq \sqrt{L \log\Big(\frac{1}{P[\,\mathcal{E}\,]}\Big)}\,.$$

The following is Hoeffding Inequality's for sampling without replacement [9].

▶ **Theorem 3** (Hoeffding Inequality for sampling without replacement)**.** *Let $w \in \{0,1\}^n$ be an n-bit string with $\frac{1}{n}\sum_{\ell=1}^{n} w_i = \overline{w}$. Let the random variables $D_1, D_2, \ldots, D_K$ be obtained by sampling K random entries from w* without replacement*. Then, for any $\varepsilon > 0$, the random variable $\overline{D} := \frac{1}{K}\sum_k D_k$ satisfies*

$$P\big[\,\overline{D} \leq \overline{w} - \varepsilon\,\big] \leq \exp\big(-2\varepsilon^2 K\big)\,.$$

Finally, we will make use of the Azuma-Hoeffding Inequality, stated below. We first define the notion of a supermartingale.

▶ **Definition 4** (Supermartingale). A sequence of real valued random variables $M_0, M_1, \dots, M_K$ is called a *supermartingale* if $\mathbb{E}[M_k | M_0 \cdots M_{k-1}] \le M_{k-1}$ (with probability 1) for every $k \ge 1$.

▶ **Theorem 5** (Azuma-Hoeffding Inequality). *If $M_0, M_1, \dots, M_K$ is a supermartingale with $M_k \le M_{k-1} + 1$, then*

$$P\big[\, M_K > M_0 + \varepsilon K \,\big] \le \exp\big(-\varepsilon^2 K/2\big) \, .$$

2.4 Nonlocal Games

▶ **Definition 6.** An *m-player nonlocal game*, or simply *(m-player) game* $\mathcal{G}$ consists of two m-partite sets $\mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_m$ and $\mathcal{A} = \mathcal{A}_1 \times \cdots \times \mathcal{A}_m$, a probability distribution $\pi : \mathcal{X} \to [0,1]$ on $\mathcal{X}$, i.e., $\sum_x \pi(x) = 1$, and a verification predicate $\mathsf{V} : \mathcal{X} \times \mathcal{A} \to \{0,1\}$.

▶ **Definition 7.** A *strategy* for an m-player game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, \pi, \mathsf{V})$ is a conditional probability distribution $q(\cdot|\cdot) : \mathcal{A} \times \mathcal{X} \to [0,1]$, i.e., $\sum_a q(a|x) = 1$ for all $x \in \mathcal{X}$.

▶ **Definition 8.** For any m-player game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, \pi, \mathsf{V})$ and any strategy q for $\mathcal{G}$, the *value* of the game with respect to q is given by

$$v[q](\mathcal{G}) := \sum_{\substack{x \in \mathcal{X} \\ a \in \mathcal{A}}} \pi(x)\, q(a|x)\, \mathsf{V}(x,a) \, .$$

Any m-player game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, \pi, \mathsf{V})$ and any strategy q for $\mathcal{G}$ together naturally define a probability space with random variables $X = (X_1, \dots, X_m)$ and $A = (A_1, \dots, A_m)$ with joint probability distribution P_{XA} given by $P_{XA}(x,a) = \pi(x) q(a|x)$. The random variable X describes the choice of the input $x \in \mathcal{X}$ according to π, and the random variable A then describes the reply $a \in \mathcal{A}$ chosen according to the distribution $q(\cdot|x)$. It obviously holds that $P_X = \pi$, and $P_{A|X}(\cdot|x) = q(\cdot|x)$ for any $x \in \mathcal{X}$ with $P_X(x) > 0$. A subtlety is that for $x \in \mathcal{X}$ with $P_X(x) = 0$, the distribution $P_{A|X}(\cdot|x)$ is strictly speaking not defined whereas $q(\cdot|x)$ is. The value of the game with respect to strategy q can be written in terms of these random variables as $v[q](\mathcal{G}) = P[\,\mathsf{V}(X,A) = 1\,]$. In the following we define the classical, quantum and non-signaling values of m-player games. Only the last one will be used in the rest of the paper, but we provide all of them for the sake of completeness.

▶ **Definition 9.** A *strategy* q for an m-player game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, \pi, \mathsf{V})$ is *classical* (or *local*) if there exists a probability distribution p on a set $\mathcal{W}$ and conditional probability distributions $q_1, \dots, q_m$ such that

$$q(a_1, \dots, a_m | x_1, \dots, x_m) = \sum_{w \in \mathcal{W}} p(w) \prod_{i=1}^{m} q_i(a_i | x_i, w) \, .$$

The *classical value* of a game $\mathcal{G}$ is defined as $v_{\mathrm{c}}(\mathcal{G}) := \sup_q v[q](\mathcal{G})$, where the supremum is over all classical strategies q for $\mathcal{G}$.

▶ **Definition 10.** A *strategy* q for an m-player game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, \pi, \mathsf{V})$ is *quantum* if there exists an m-partite quantum state $|\psi\rangle \in \mathcal{H}_{\mathsf{A}_1} \otimes \cdots \otimes \mathcal{H}_{\mathsf{A}_m}$ and for every $x = (x_1, \dots, x_m) \in \mathcal{X}$ there exist POVMs $\mathbf{E}^1_{x_1} = \{E^1_{x_1,a_1}\}_{a_1 \in \mathcal{A}_1}, \dots, \mathbf{E}^m_{x_m} = \{E^m_{x_m,a_m}\}_{a_m \in \mathcal{A}_m}$ such that for all $a = (a_1, \dots, a_m) \in \mathcal{A}$ and $x = (x_1, \dots, x_m) \in \mathcal{X}$:

$$q(a|x) = \langle \psi | E^1_{x_1,a_1} \otimes \cdots \otimes E^m_{x_m,a_m} | \psi \rangle$$

The *quantum value* of a game $\mathcal{G}$ is defined as $v_{\mathrm{qu}}(\mathcal{G}) := \sup_q v[q](\mathcal{G})$, where the supremum is over all quantum strategies q for $\mathcal{G}$.

▶ **Definition 11.** A *strategy* q for an m-player game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, \pi, \mathsf{V})$ is *non-signaling* if for any index subset $I \subset \{1, \dots, m\}$ and its complement $J = \{1, \dots, m\} \setminus I$, it holds that

$$\sum_{a_J \in \mathcal{A}_J} q(a_I, a_J | x_I, x_J) = \sum_{a_J \in \mathcal{A}_J} q(a_I, a_J | x_I, x'_J) \quad \text{for all } a_I \in \mathcal{A}_I,\ x_I \in \mathcal{X}_I \text{ and } x_J, x'_J \in \mathcal{X}_J\,.$$

The *non-signaling value* of a game $\mathcal{G}$ is defined as $v_{\mathrm{ns}}(\mathcal{G}) := \sup_q v[q](\mathcal{G})$, where the supremum is over all non-signaling strategies q for $\mathcal{G}$.

The following relaxed notion of non-signaling is crucial for the understanding of our parallel-repetition proof.

▶ **Definition 12.** A *strategy* q for an m-player game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, \pi, \mathsf{V})$ is ε*-almost non-signaling* if for any index subset $I \subset \{1, \dots, m\}$ and its complement $J = \{1, \dots, m\} \setminus I$, it holds that

$$\left| \sum_{a_J \in \mathcal{A}_J} q(a_I, a_J | x_I, x_J) - \sum_{a_J \in \mathcal{A}_J} q(a_I, a_J | x_I, x'_J) \right| \le \varepsilon \quad \text{for all } a_I \in \mathcal{A}_I,\ x_I \in \mathcal{X}_I \text{ and } x_J, x'_J \in \mathcal{X}_J\,.$$

3 A Multi-Player Parallel Repetition Theorem

3.1 The Parallel Repetition of Nonlocal Games

Given a game $\mathcal{G}$, the n-fold parallel repetition $\mathcal{G}^n$ is the game where the referees samples n independent inputs $\boldsymbol{x} = (x^1, \dots, x^n) \in \mathcal{X} \times \dots \times \mathcal{X}$ and $\mathcal{G}^n$ is won if and only if all its sub-games are won. For the sake of notational convenience, we also introduce the following way of denoting the fact that t of the n parallel repetitions are won.

▶ **Definition 13** (t-out-of-n Parallel Repetition)**.** For any $n \in \mathbb{N}$ and $t \in \mathbb{R}$, the *t-out-of-n parallel repetition* of a game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, \pi, \mathsf{V})$ is given by the game $\mathcal{G}^{t/n} = (\mathcal{X}^n, \mathcal{A}^n, \pi^n, \mathsf{V}^{t/n})$ where $\mathcal{X}^n = \mathcal{X} \times \dots \times \mathcal{X}$ and $\mathcal{A}^n = \mathcal{A} \times \dots \times \mathcal{A}$, and for all $\boldsymbol{x} = (x^1, \dots, x^n) \in \mathcal{X}^n$ and $\boldsymbol{a} = (a^1, \dots, a^n) \in \mathcal{A}^n$

$$\pi^n(\boldsymbol{x}) := \prod_{\ell=1}^{n} \pi(x^\ell) \qquad \text{and} \qquad \mathsf{V}^{t/n}(\boldsymbol{x}, \boldsymbol{a}) := \begin{cases} 1 & \text{if } \sum_{\ell=1}^n \mathsf{V}(x^\ell, a^\ell) \ge t \\ 0 & \text{else} \end{cases} .$$

The (standard) *n-fold parallel repetition* of a game $\mathcal{G}$ is given by the game $\mathcal{G}^n := \mathcal{G}^{n/n}$.

Similar to the observation after Definition 8, for any game $\mathcal{G}$ and for any strategy[2] $q^{(n)}$ for the t-out-of-n (or the n-fold) parallel repetition, random variables $\boldsymbol{X} = (X^1, \dots, X^n)$ and $\boldsymbol{A} = (A^1, \dots, A^n)$, together with their joint distribution $P_{\boldsymbol{XA}}$, are naturally determined.

Note that for any $\ell \in \{1, \dots, n\}$, X^ℓ is of the form $X^\ell = (X_1^\ell, \dots, X_m^\ell)$, where X_i^ℓ represents the question to the i-th player in the ℓ-th repetition of $\mathcal{G}$ (and is distributed over $\mathcal{X}_i$). Therefore, for any $i \in \{1, \dots, m\}$, we write $\boldsymbol{X}_i$ for $\boldsymbol{X}_i = (X_i^1, \dots, X_i^n)$, and for any $I = \{i_1, \dots, i_k\} \subseteq \{1, \dots, m\}$, X_I^ℓ should be understood as $X_I^\ell = (X_{i_1}^\ell, \dots, X_{i_k}^\ell)$ and $\boldsymbol{X}_I$ as $\boldsymbol{X}_I = (\boldsymbol{X}_{i_1}, \dots, \boldsymbol{X}_{i_k})$. The corresponding holds for $\boldsymbol{A}$.

To simplify notation, for the n-fold repetition of a given game $\mathcal{G}$ with a given strategy $q^{(n)}$, we define W_ℓ to be the random variable $W_\ell := \mathsf{V}(X^\ell, A^\ell)$ that indicates if the ℓ-th repetition of $\mathcal{G}$ is won, and we define $\overline{W} := \frac{1}{n} \sum_{\ell=1}^n W_\ell$ to be the fraction of repetitions that are won. Obviously, $v[q^{(n)}](\mathcal{G}^{t/n}) = P[\overline{W} \ge t/n]$.

[2] We write $q^{(n)}$ (rather than e.g. q^n) to emphasize that it is a strategy for an n-fold repetition of $\mathcal{G}$, but it is *not* (necessarily) the n-fold independent execution of a strategy q for $\mathcal{G}$.

3.2 Concentration and Parallel Repetition Theorems

Our concentration and parallel repetition theorems below hold for all multi-player nonlocal games $\mathcal{G}$ up to the following restriction on the distribution π.

▶ **Definition 14.** We say that an m-player game $\mathcal{G} = (\mathcal{X}, \mathcal{A}, \pi, \mathsf{V})$ has *complete support* if $\pi(x) > 0$ for all $x \in \mathcal{X}$, i.e., every $x \in \mathcal{X} = \mathcal{X}_1 \times \cdots \times \mathcal{X}_m$ is a "valid input" to the game.

An important class of games that satisfy the complete-support property are the so-called *free* games, as studied for instance in [2]. In a free game, π is required to be a *product distribution*, i.e., $\pi(x) = \pi_1(x_1) \cdots \pi_m(x_m)$ for all $x = (x_1, \ldots, x_m) \in \mathcal{X} = \mathcal{X}_1 \times \ldots \times \mathcal{X}_m$. Such a game has obviously full support.[3]

▶ **Theorem 15** (Concentration Theorem). *Let $\mathcal{G}$ be an arbitrary m-player game with complete support. Then there exists a constant $\mu > 0$, depending on $\mathcal{G}$, such that for any $\delta > 0$, any $n \in \mathbb{N}$, and for $t = (v_{\rm ns}(\mathcal{G}) + \delta)n$:*

$$v_{\rm ns}(\mathcal{G}^{t/n}) \leq 8 \exp\bigl(-\delta^4 \mu n\bigr) .$$

As an immediate consequence, we get the following parallel-repetition theorem.

▶ **Theorem 16** (Parallel-Repetition Theorem). *Let $\mathcal{G}$ be an arbitrary m-player game with complete support and non-signaling value $v_{\rm ns}(\mathcal{G}) < 1$. Then there exists $\nu < 1$, depending on $\mathcal{G}$, such that $v_{\rm ns}(\mathcal{G}^n) < 8\nu^n$ for any $n \in \mathbb{N}$.*

We point out that the constants μ (in Theorem 15) and ν (in Theorem 16) not only depend on the non-signaling value $v_{\rm ns}(\mathcal{G})$ of $\mathcal{G}$, but on the game $\mathcal{G}$ itself. The restriction to games with complete support stems from the fact that μ becomes 0 when the smallest probability in the distribution π goes to 0, rendering the bound useless.

3.3 The Proof

A central idea of our proof is the *robustness* of the non-signaling value of a game. We will use the following result from [17, Section 10.4] about the sensitivity analysis of linear programs.

▶ **Lemma 17.** *Let A be an $m \times n$-matrix, and let A be such that for each nonsingular submatrix B of A, all entries of B^{-1} are at most Δ in absolute value. Let c be a row n-vector, and let b' and b'' be column m-vectors such that both $\max_x\{cx \,|\, Ax \leq b'\}$ and $\max_x\{cx \,|\, Ax \leq b''\}$ are finite. Then* [4]

$$\left| \max_{x \in \mathbb{R}^n}\{cx \,|\, Ax \leq b''\} - \max_{x \in \mathbb{R}^n}\{cx \,|\, Ax \leq b'\} \right| \leq n\Delta \|c\|_1 \cdot \|b'' - b'\|_\infty .$$

▶ **Proposition 18** (Robustness of $v_{\rm ns}(\mathcal{G})$). *Let $\mathcal{G}$ be an m-player game with non-signaling value $v_{\rm ns}(\mathcal{G})$. Then, there exists a constant $c(\mathcal{G})$ such that for any $\varepsilon \geq 0$ and for any strategy q for $\mathcal{G}$ that is ε-almost non-signaling, the value of $\mathcal{G}$ with respect to q is bounded by $v[q](\mathcal{G}) \leq v_{\rm ns}(\mathcal{G}) + c(\mathcal{G}) \cdot \varepsilon$.*

[3] After possibly having restricted the sets $\mathcal{X}_1, \ldots, \mathcal{X}_m$ appropriately.

[4] For $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, the norms are defined as $\|x\|_1 = \sum_i |x_i|$ and $\|x\|_\infty = \max_i |x_i|$.

Proof. The non-signaling value $v_{\mathrm{ns}}(\mathcal{G})$ is the optimal value of the following linear program:

$$\begin{aligned}
&\text{maximize} \quad \sum_{\substack{x\in\mathcal{X}\\ a\in\mathcal{A}}} \pi(x)\,\mathsf{V}(x,a)\,q(a|x) \\
&\text{subject to} && (1)\\
&\quad q(a|x) \geq 0 \quad \text{for all } a\in\mathcal{A},\ x\in\mathcal{X}, && (2)\\
&\quad \sum_{a\in\mathcal{A}} q(a|x) = 1 \quad \text{for all } x\in\mathcal{X}, && (3)\\
&\quad \sum_{a_J\in\mathcal{A}_J} q(a_I,a_J|x_I,x_J) - q(a_I,a_J|x_I,x'_J) = 0 \quad \text{for all } I\subset\{1,\dots,m\},\ J=\{1,\dots,m\}\setminus I \\
&\qquad\qquad \text{and for all } a_I\in\mathcal{A}_I,\ x_I\in\mathcal{X}_I \text{ and } x_J,x'_J\in\mathcal{X}_J\,. && (4)
\end{aligned}$$

Lemma 17 gives a bound on how much the optimal value of this linear program can vary if we optimize over ε-almost non-signaling strategies instead of a fully non-signaling strategies. Formally, we can express the linear program above in the "standard form" $\max\{cx \mid Ax \leq b'\}$ by expanding the equality constraints (3) and (4) as $\leq$ and $\geq$ inequality constraints. According to Definition 12, ε-almost non-signaling strategies fulfill the constraints (4) only up to an error of at most 2ε. Hence, relaxing the constraints from non-signaling to ε-almost non-signaling amounts to change the b'-coordinates corresponding to the non-signaling constraints (4) from 0 to 2ε. Hence, the parameters of Lemma 17 are $\|b''-b'\|_\infty = 2\varepsilon$, $n = |\mathcal{X}|\cdot|\mathcal{A}|$, $\|c\|_1 = \sum_{\substack{x\in\mathcal{X}\\ a\in\mathcal{A}}} |\pi(x)\,\mathsf{V}(x,a)| \leq |\mathcal{A}|$ and Δ is a finite constant that depends on the number of players m and the number of answers $|\mathcal{A}|$ and questions $|\mathcal{X}|$.[5] Finally, we note that we can apply the lemma, because the objective function is at most one (and thus finite) irrespective of which strategies we are considering. Setting $c(\mathcal{G}) := 2|\mathcal{X}||\mathcal{A}|^2\Delta$ yields the claim. ◀

▶ **Lemma 19** (Main Lemma). *Let $\mathcal{G}$ be a game with complete support. Consider an n-fold repetition $\mathcal{G}^n$ of $\mathcal{G}$ with an arbitrary non-signaling strategy $q^{(n)}$ for $\mathcal{G}^n$. Let $\mathcal{E}$ be an arbitrary event (in the underlying probability space). Then for any subset $S=\{v_1,\dots,v_k\}\subset\{1,\dots,n\}$, the probability $P[\,W_V\!=\!1\,|\,\mathcal{E}\,]$ for a randomly chosen V in $\{1,\dots,n\}\setminus S$ is bounded by*

$$P\big[\,W_V\!=\!1\,\big|\,\mathcal{E}\,\big] \leq v_{\mathrm{ns}}(\mathcal{G}) + c'(\mathcal{G})\cdot\sqrt{\tfrac{1}{n-k}\log\big(\tfrac{1}{P[\,\mathcal{E}\,]}\big)}$$

where $c'(\mathcal{G}) = 3\cdot 2^m c(\mathcal{G})/\min_x \pi(x)$ is some constant that only depends on $\mathcal{G}$.

The following is an immediate consequence.

▶ **Corollary 20.** *Let $\mathcal{G}$ be a game with complete support. Consider an execution of the n-fold repetition $\mathcal{G}^n$ with an arbitrary non-signaling strategy for $\mathcal{G}^n$. For any $\ell\in\{1,\dots,n\}$, let $\mathcal{E}_\ell$ be the event that the ℓ-th repetition is accepted, i.e. $W_\ell = 1$. Then for any subset $S=\{v_1,\dots,v_k\}\subset\{1,\dots,n\}$, there exists $v_{k+1}\in\{1,\dots,n\}\setminus S$ such that*

$$P\big[\,\mathcal{E}_{v_{k+1}}\,\big|\,\mathcal{E}_{v_1}\wedge\ldots\wedge\mathcal{E}_{v_k}\,\big] \leq v_{\mathrm{ns}}(\mathcal{G}) + c'(\mathcal{G})\cdot\sqrt{\tfrac{1}{n-k}\log\big(\tfrac{1}{P[\,\mathcal{E}_{v_1}\wedge\ldots\wedge\mathcal{E}_{v_k}\,]}\big)}$$

where $c'(\mathcal{G})$ is some constant that only depends on $\mathcal{G}$.

[5] In our case, the relevant constraint matrix A has $n = |\mathcal{X}|\cdot|\mathcal{A}|$ columns and at most $2\left((|\mathcal{A}|\cdot|\mathcal{X}|+|\mathcal{X}|^2)^m + |\mathcal{X}|\right)$ rows. Let $\Delta := \max\left\{\left|(B^{-1})_{ij}\right| \mid \text{B a nonsingular submatrix of } A\right\}$, which depends only $m, |\mathcal{A}|, |\mathcal{X}|$. shown the existence of $\{0,1\}$-matrices of size $n\times n$ with the biggest entry of the inverse matrix as big as $n^{n(\frac{1}{2}+o(1))}$, and this is sharp. Exploiting the explicit structure of the non-signaling constraints, one could possibly get much better bounds.

Proof (of Lemma 19). Let $\pi_\circ > 0$ be such that $\pi(x) \geq \pi_\circ$ for all $x \in \mathcal{X}$; by assumption on $\mathcal{G}$, such a $\pi_\circ$ exists. By re-ordering the (strategies of the) n executions, we may assume without loss of generality that $S = \{n-k+1, \ldots, n\}$, and we now need to argue about the probability over a random V in $\{1, \ldots, n-k\}$. To simplify notation, let us define

$$\varepsilon := \sqrt{\tfrac{1}{n-k} \log\bigl(\tfrac{1}{P[\mathcal{E}]}\bigr)} \, .$$

Fix a subset $I \subseteq \{1, \ldots, m\}$ and let $J = \{1, \ldots, m\} \setminus I$ be the complement of I. Consider the distribution

$$P_{\boldsymbol{X}_I \boldsymbol{X}_J \boldsymbol{A}_I} = P_{\boldsymbol{X}_I \boldsymbol{A}_I} \cdot P_{\boldsymbol{X}_J | \boldsymbol{X}_I \boldsymbol{A}_I} = P_{\boldsymbol{X}_I \boldsymbol{A}_I} \cdot P_{\boldsymbol{X}_J | \boldsymbol{X}_I} = P_{\boldsymbol{X}_I \boldsymbol{A}_I} \cdot \prod_{\ell=1}^{n} P_{X_J^\ell | \boldsymbol{X}_I} = P_{\boldsymbol{X}_I \boldsymbol{A}_I} \cdot \prod_{\ell=1}^{n} P_{X_J^\ell | \boldsymbol{X}_I \boldsymbol{A}_I}$$

where the second equality is due to non-signaling, the third due to the independence of every pair (X_I^ℓ, X_J^ℓ), and the third again due to non-signaling. We can thus apply Lemma 2 (with $T = (\boldsymbol{X}_I, \boldsymbol{A}_I)$ and $U^\ell = X_J^\ell$) and obtain

$$\begin{aligned} (n-k) \cdot \varepsilon = \sqrt{(n-k) \log\bigl(\tfrac{1}{P[\mathcal{E}]}\bigr)} &\geq \sum_{\ell=1}^{n-k} \bigl\| P_{\boldsymbol{X}_I X_J^\ell \boldsymbol{A}_I | \mathcal{E}} - P_{\boldsymbol{X}_I \boldsymbol{A}_I | \mathcal{E}} \cdot P_{X_J^\ell | \boldsymbol{X}_I \boldsymbol{A}_I} \bigr\| \\ \geq \sum_{\ell=1}^{n-k} \bigl\| P_{X_I^\ell X_J^\ell A_I^\ell | \mathcal{E}} - P_{X_I^\ell A_I^\ell | \mathcal{E}} \cdot P_{X_J^\ell | X_I^\ell A_I^\ell} \bigr\| &= \sum_{\ell=1}^{n-k} \bigl\| P_{X_I^\ell X_J^\ell A_I^\ell | \mathcal{E}} - P_{X_I^\ell A_I^\ell | \mathcal{E}} \cdot P_{X_J^\ell | X_I^\ell} \bigr\| \\ = \sum_{\ell=1}^{n-k} \bigl\| P_{X_I^\ell X_J^\ell | \mathcal{E}} \cdot P_{A_I^\ell | X_I^\ell X_J^\ell \mathcal{E}} - P_{X_I^\ell | \mathcal{E}} \cdot P_{A_I^\ell | X_I^\ell \mathcal{E}} \cdot P_{X_J^\ell | X_I^\ell} \bigr\| \, . \end{aligned}$$

The first inequality holds by Lemma 2. The second inequality follows from Lemma 1 which states that the distance of the random variables $X_I^\ell, X_J^\ell, A_I^\ell$ cannot be larger than the distance of all random variables $\boldsymbol{X}_I, X_J^\ell, \boldsymbol{A}_I$. The subsequent equality holds due to the non-signaling condition between subsets I and J, and the last equality is a simple re-writing of some probabilities.

By means of Lemma 2 (setting T to be a constant), we can also conclude that $\sum_\ell \| P_{X_I^\ell X_J^\ell | \mathcal{E}} - P_{X_I^\ell X_J^\ell} \|$, and thus in particular $\sum_\ell \| P_{X_I^\ell | \mathcal{E}} - P_{X_I^\ell} \|$, is upper bounded by $(n-k)\varepsilon$. Therefore, noting that $P_{X_I^\ell X_J^\ell} = P_{X_I X_J}$, we can conclude that

$$\sum_{\ell=1}^{n-k} \bigl\| P_{X_I X_J} \cdot P_{A_I^\ell | X_I^\ell X_J^\ell \mathcal{E}} - P_{X_I X_J} \cdot P_{A_I^\ell | X_I^\ell \mathcal{E}} \bigr\| \leq 3(n-k)\varepsilon \, .$$

By summing over all subsets $I \subseteq \{1, \ldots, m\}$ (and letting J be its complement), changing the order of the summation, and defining

$$\varepsilon_\ell := \sum_I \bigl\| P_{X_I X_J} \cdot P_{A_I^\ell | X_I^\ell X_J^\ell \mathcal{E}} - P_{X_I X_J} \cdot P_{A_I^\ell | X_I^\ell \mathcal{E}} \bigr\|$$

we get

$$\sum_{\ell=1}^{n-k} \varepsilon_\ell \leq 3 \cdot 2^m (n-k) \varepsilon \, .$$

Note that by definition of ε_ℓ, for any choice of I and $J = \{1, \ldots, m\} \setminus I$, it holds that

$$\bigl\| P_{X_I X_J} \cdot P_{A_I^\ell | X_I^\ell X_J^\ell \mathcal{E}} - P_{X_I X_J} \cdot P_{A_I^\ell | X_I^\ell \mathcal{E}} \bigr\| \leq \varepsilon_\ell \, ,$$

and hence, by the lower bound $\pi_\circ$ on $P_{X_I X_J}$, that

$$\left\| P_{A_I^\ell | X_I^\ell X_J^\ell \mathcal{E}}(\cdot | x_I, x_J) - P_{A_I^\ell | X_I^\ell \mathcal{E}}(\cdot | x_I) \right\| \leq \frac{\varepsilon_\ell}{\pi_\circ}$$

for any x_I and x_J. For any $\ell \in \{1, \dots, n-k\}$, consider the strategy $\tilde{q}_\ell$ for (one execution of) $\mathcal{G}$, defined by $\tilde{q}_\ell(a|x) = P_{A^\ell | X^\ell \mathcal{E}}(a|x)$. By the above, $\tilde{q}_\ell$ is $(\varepsilon_\ell/\pi_\circ)$-almost non-signaling. Furthermore, by the definition of $\tilde{q}_\ell$, the probability $P[\,\mathcal{E}_\ell\,|\,\mathcal{E}\,]$ that the ℓ-th repetition of the n-fold repetition of $\mathcal{G}$ is accepted equals the probability $v[\tilde{q}_\ell](\mathcal{G})$ that a *single* execution of $\mathcal{G}$ is accepted when strategy $\tilde{q}_\ell$ is played. Since $\tilde{q}_\ell$ is $(\varepsilon_\ell/\pi_\circ)$-almost non-signaling, it follows from Proposition 18 that this probability is at most $v_{\rm ns}(\mathcal{G}) + c(\mathcal{G}) \cdot \varepsilon_\ell/\pi_\circ$. The claimed bound on $P[\,\mathcal{E}_V\,|\,\mathcal{E}\,]$ for a randomly chosen V in $\{1, \dots, n-k\}$ now follows from the bound on $\sum_\ell \varepsilon_\ell$, where $c'(\mathcal{G})$ is given by $3 \cdot 2^m c(\mathcal{G})/\pi_\circ$. ◀

We are now ready to prove our main concentration bound.

Proof (of Theorem 15). Let K be some integer parameter, to be defined later. Let $V_1, \dots, V_K$ be a random subset of distinct integers from $\{1, \dots, n\}$, and let D_k be the random variable $D_k = W_{V_k} = \mathsf{V}(X^{V_k}, A^{V_k})$ for any $k \in \{1, \dots, K\}$. Understanding $V_1, \dots, V_K$ as a "sample subset" of the n parallel repetitions of $\mathcal{G}$, D_k indicates whether the k-th game in the sample is won. A pair $(d_1, \dots, d_k) \in \{0,1\}^k$ and $(v_1, \dots, v_k) \in \{1, \dots, n\}$ of k-tuples is called *typical* if $P_{D_1 \cdots D_k | V_1 \cdots V_k}(d_1, \dots, d_k | v_1, \dots, v_k) \geq 2^{-2K}$. Let $\mathcal{T}_k$ be the event that $(D_1 \cdots D_k)$ and $(V_1 \cdots V_k)$ form a typical pair. Note that the corresponding complementary events satisfy $\bar{\mathcal{T}}_k \Rightarrow \bar{\mathcal{T}}_{k+1}$ as well as

$$P[\,\bar{\mathcal{T}}_k\,] = \sum_{\substack{\text{atypical pairs} \\ (d_1 \dots d_k), (v_1 \dots v_k)}} P_{V_1 \cdots V_k}(v_1, \dots, v_k)\, P_{D_1 \cdots D_k | V_1 \cdots V_k}(d_1 \cdots d_k | v_1 \cdots v_k) < 2^{-K}\,.$$

Let $\gamma := 1 - v_{\rm ns}(\mathcal{G}) - \varepsilon$ where $\varepsilon := \delta/3$. Note that we obviously may assume that $\delta \leq 1 - v_{\rm ns}(\mathcal{G})$ so that $\gamma > 0$. We now define a sequence of random variables $M_0, \dots, M_K$ as follows. Random variable M_0 takes the value 0 with certainty, and M_{k+1} is inductively defined as

$$M_{k+1} := \begin{cases} M_k + \gamma & \text{if } D_{k+1} = 1 \text{ and } \mathcal{T}_k \\ M_k - (1-\gamma) & \text{otherwise}\,. \end{cases}$$

We want to show that $M_0, \dots, M_K$ forms a supermartingale. We fix $k \in \{0, \dots, K-1\}$ and we fix values $(v_1, \dots, v_k)$ for the random variables $V_1, \dots, V_k$. Up to the end of this paragraph, all probabilities etc. are to be understood conditioned on these values. We define $\mathcal{E}$ to be the event that $D_1, \dots, D_k$ take on some arbitrary but fixed values $(d_1, \dots, d_k)$. If the pair $(d_1, \dots, d_k)$ and $(v_1, \dots, v_k)$ is atypical, then conditioned on $\mathcal{E}$ we have $M_{k+1} = M_k + \gamma - 1 < M_k$ and thus $\mathbb{E}[M_{k+1} | M_0 \cdots M_k] < \mathbb{E}[M_k | M_0 \cdots M_k] = M_k$. In the other case, if the pair $(d_1, \dots, d_k)$ and $(v_1, \dots, v_k)$ is typical then $P[\,\mathcal{E}\,] \geq 2^{-2K}$. Furthermore, Lemma 19 implies that $P_{D_{k+1}|\mathcal{E}}(1) = P[\,\mathcal{E}_{V_{k+1}}\,|\,\mathcal{E}\,] \leq v_{\rm ns}(\mathcal{G}) + c'(\mathcal{G})\sqrt{\log(1/P[\,\mathcal{E}\,])/(n-k)} \leq v_{\rm ns}(\mathcal{G}) + c'(\mathcal{G})\sqrt{2K/(n-K)}$. We want this last term to be upper bounded by $v_{\rm ns}(\mathcal{G}) + \varepsilon = 1 - \gamma$, which we achieve by choosing K as $K := \lfloor \alpha n \rfloor$ where $\alpha := \min\{\varepsilon^2/(3c'(\mathcal{G})^2), 1/3\}$, as can easily be verified. It follows that $\mathbb{E}[M_{k+1} | M_0 \cdots M_k] \leq (1-\gamma)(M_k + \gamma) + \gamma(M_k - (1-\gamma)) = M_k$ (when conditioning on $\mathcal{E}$). Since the argument that the $M_0, \dots, M_K$ form a supermartingale holds independent of the choice of $(d_1, \dots, d_k)$ and of the choice of $(v_1, \dots, v_k)$, $M_0, \dots, M_K$ indeed forms a supermartingale in the original probability space (without conditioning on the values for

$V_1, \ldots, V_k$). Therefore,

$$\begin{aligned}
P\Big[\sum_{k=1}^{K} D_k \geq (v_{\mathrm{ns}}(\mathcal{G}){+}2\varepsilon)K\Big] \;&\leq\; P\big[\,\bar{\mathcal{T}}_K\,\big] + P\big[\,M_K \geq (v_{\mathrm{ns}}(\mathcal{G}){+}2\varepsilon)K\gamma - (1{-}v_{\mathrm{ns}}(\mathcal{G}){-}2\varepsilon)K(1{-}\gamma)\,\big] \\
&\leq\; 2^{-K} + P\big[\,M_K \geq (\gamma - 1 + v_{\mathrm{ns}}(\mathcal{G}) + 2\varepsilon)K\,\big] \;=\; 2^{-K} + P\big[\,M_K \geq \varepsilon K\,\big] \\
&\leq\; 2^{-K} + \exp(-\varepsilon^2 K/2) \;<\; 2\exp(-\varepsilon^2 K/2)
\end{aligned}$$

The first inequality holds by definition of M_K, and the second by a simple manipulation of the terms. The equality holds by definition of γ, and the subsequent inequality by the Azuma-Hoeffding Inequality. Finally, the last inequality holds since $\varepsilon < 1$ and $\exp(\frac{1}{2}) < 2$.

On the other hand, setting $\overline{D} := \frac{1}{K}\sum_{k=1}^{K} D_k$, we can also write

$$P\big[\,\overline{D} \geq v_{\mathrm{ns}}(\mathcal{G}) + 2\varepsilon\,\big] \geq P\big[\,\overline{W} > v_{\mathrm{ns}}(\mathcal{G}) + \delta\,\big] \cdot P\big[\,\overline{D} \geq v_{\mathrm{ns}}(\mathcal{G}) + 2\varepsilon \,\big|\, \overline{W} > v_{\mathrm{ns}}(\mathcal{G}) + \delta\,\big]$$

where by the Hoeffding Inequality (and using that $\varepsilon = \delta/3$)

$$P\big[\,\overline{D} \geq v_{\mathrm{ns}}(\mathcal{G}){+}2\varepsilon \,\big|\, \bar{W} > v_{\mathrm{ns}}(\mathcal{G}) + \delta\,\big] \geq 1 - \exp(-2\varepsilon^2 K)\,.$$

Therefore,

$$P\big[\,\overline{W} > v_{\mathrm{ns}}(\mathcal{G}) + \delta\,\big] \leq \frac{2\exp(-\varepsilon^2 K/2)}{1 - \exp(-2\varepsilon^2 K)}\,.$$

In case that $\exp(-2\varepsilon^2 K) < \frac{1}{4}$, we obtain the bound

$$P\big[\,\overline{W} > v_{\mathrm{ns}}(\mathcal{G}) + \delta\,\big] \leq \frac{8}{3}\exp(-\varepsilon^2 K/2)\,. \tag{5}$$

Note that in the other case, if $\exp(-2\varepsilon^2 K) \geq \frac{1}{4}$, then $2\exp(-\varepsilon^2 K/2) \geq 1$ and the bound (5) holds trivially.

Setting $\mu := 1/(2 \cdot 3^5 \cdot c'(\mathcal{G})^2)$, and recalling that $\varepsilon = \delta/3$ and $K := \lfloor \alpha n \rfloor$ with α chosen as $\alpha := \min\{\varepsilon^2/(3c'(\mathcal{G})^2), 1/3\}$, leads to the claim. ◀

4 Conclusion and Open Questions

This article initiates the investigation of the behavior of multi-player nonlocal games under parallel repetition. For the case of the non-signaling value, we provide a concentration bound for games with complete support. Our results might serve as a stepping stone for the investigation of the quantum and classical values. Other interesting questions include improving the rate of repetition (e.g. by making it independent of the minimal probability that any question is asked) or finding cryptographic applications, for instance in position-based cryptography.

Acknowledgments

We would like to thank Tobias Müller for insightful discussions about the sensitivity of linear programs. HB is supported by a 7th framework EU SIQS grant. CS is supported by an NWO VENI grant.

References

1 Noga Alon and Vǎn H. Vũ. Anti-hadamard matrices, coin weighing, threshold gates, and indecomposable hypergraphs. *J. Comb. Theory Ser. A*, 79(1):133–160, July 1997.

2 Boaz Barak, Anup Rao, Ran Raz, Ricky Rosen, and Ronen Shaltiel. Strong parallel repetition theorem for free projection games. In Irit Dinur, Klaus Jansen, Joseph Naor, and José D. P. Rolim, editors, *APPROX-RANDOM*, volume 5687 of *Lecture Notes in Computer Science*, pages 352–365. Springer, 2009.

3 Jop Briët, Harry Buhrman, Troy Lee, and Thomas Vidick. Multipartite entanglement in xor games. *Quantum Information & Computation*, 13(3-4):334–360, March 2013.

4 Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 429–446. Springer Berlin / Heidelberg, 2011.

5 Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Innovations in Theoretical Computer Science, ITCS '13, Berkeley, CA, USA, January 9-12, 2013*, pages 145–158. ACM, 2013.

6 A. Chailloux and G. Scarpa. Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost. arxiv:1310.7787, 2013.

7 Richard Cleve, William Slofstra, Falk Unger, and Sarvagya Upadhyay. Perfect parallel repetition theorem for quantum xor proof systems. *Computational Complexity*, 17(2):282–299, 2008.

8 I. Dinur, D. Steurer, and T. Vidick. A parallel repetition theorem for entangled projection games. arxiv:1310.4113, 2013.

9 Wassily Hoeffding. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, 58(301):13–30, March 1963.

10 Thomas Holenstein. Parallel repetition: Simplification and the no-signaling case. *Theory of Computing*, 5(1):141–172, 2009.

11 R. Jain, A. Pereszlényi, and P. Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. arxiv:1311.6309, 2013.

12 Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. *SIAM J. Comput.*, 39(7):3207–3229, July 2010.

13 Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. In *Proceedings of the 43rd annual ACM symposium on Theory of computing*, STOC '11, pages 353–362, New York, NY, USA, 2011. ACM.

14 Anup Rao. Parallel repetition in projection games and a concentration bound. *SIAM J. Comput.*, 40(6):1871–1891, 2011.

15 Ran Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803, June 1998.

16 Ricky Rosen. A k-provers parallel repetition theorem for a version of no-signaling model. *Discrete Math., Alg. and Appl.*, 2(4):457–468, 2010.

17 A. Schrijver. *Theory of Linear and Integer Programming.* Wiley Series in Discrete Mathematics & Optimization. John Wiley & Sons, 1998.

18 Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013.