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

(extended abstract of [BFS14] for QIP 2015, arXiv:1312.7455)

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

July 22, 2014

We consider the natural extension of two-player nonlocal games to an arbitrary number of players. 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 *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 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 [DSV13, CS13, JPY13] 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.

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. 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 $v_{\text{ns}}(\mathcal{G}^n)$ of the n-fold parallel repetition of $\mathcal{G}$ is exponentially small

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

in n: $v_{\mathrm{ns}}(\mathcal{G}^n) \leq \bar{v}_{\mathrm{ns}}(\mathcal{G})^n$ for some $\bar{v}_{\mathrm{ns}}(\mathcal{G}) < 1$. Stronger than that, we prove that the probability of winning more than $(v_{\mathrm{ns}}(\mathcal{G}) + \delta) \cdot n$ parallel repetitions is exponentially small in n (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 classical two-player games, in that in our result the constant $\bar{v}_{\mathrm{ns}}(\mathcal{G})$ depends on the complete description of the game $\mathcal{G}$, and not just on its non-signaling value $v_{\mathrm{ns}}(\mathcal{G})$. 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 [Hol09] and [Rao11], 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 in [BFS14]) 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.

Related Work The problem of parallel repetition is somewhat understood in the case of *two* players, where $m = 2$. Indeed, Raz showed in his celebrated parallel repetition theorem [Raz98] 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 [Hol09], 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 [CSUU08] or unique games [KRT10], or for a non-standard parallel repetition where the different repetitions of the original game are intertwined with modified versions of the original game [KV11]. Recently, several results about the parallel repetition of more general quantum games have been obtained [DSV13, CS13, JPY13].

There are further improvements to the above results on two-player games. For instance, Rao [Rao11] 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.* [BRR$^+$09] for *free* games, together with a further improvement, namely a *strong* parallel repetition theorem (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 [Ros10], Rosen proved a parallel-repetition result for more than 2 players. However, a somewhat unnatural definition of multi-player non-signaling correlations is used where no $m - 1$ players together can signal to the remaining player. In our (standard) model, one demands that *any subset* (of arbitrary size) of players cannot signal to the remaining players.

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

Another result about multi-player games is by Briët *et al.* [BBLV13] 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.

Relevance to the QIP community Non-local games have become a key tool for quantifying the fundamental differences between the classical and quantum world (as well as their generalizations). The behavior of non-local games under parallel repetition is of fundamental importance. Our work gives the first results for the case of more than two players.

Possible applications of our results are of quantum-cryptographic nature where it is common practice to amplify the hardness of a basic task by parallel repetition. A likely scenario for applying our results (and our original motivation to study the problem) is position-based quantum cryptography [BCF$^+$11, BFSS13], in the spirit of a recent result on parallel repetition of a so-called monogamy-of-entanglement game [TFKW13]. In particular, the attack scenario on a particular (one-dimensional) position-verification protocol can be seen as a non-local 3-party game between one of the verifiers and the two attackers. If one finds a protocol for which the non-signaling value of such a 3-player game is strictly smaller than 1, a parallel-repetition result will allow to amplify the gap in success probability between the honest and dishonest scenario arbitrarily. However, as our result only applies to a restricted class of games, we were not able yet to apply it in this cryptographic context. The problem is that there is a promise on the input distribution (namely that the two attackers always receive the same classical input), and hence, these games fall outside of the class we can analyze with our techniques.

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, with direct applications to quantum cryptography, for instance in position-based cryptography. Other interesting questions include improving the rate of repetition (e.g. by making it independent of the minimal probability that any question is asked).

References

[BBLV13] Jop Briët, Harry Buhrman, Troy Lee, and Thomas Vidick. Multipartite entanglement in xor games. *Quantum Information & Computation*, 13(3-4):334–360, March 2013.

[BCF$^+$11] 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.

[BFS14] H. Buhrman, S. Fehr, and C. Schaffner. On the parallel repetition of multi-player games: The no-signaling case. to appear at TQC14, `http://arxiv.org/abs/1312.7455`, 2014.

[BFSS13] 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.

[BRR+09] 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.

[CS13] A. Chailloux and G. Scarpa. Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost. arxiv:1310.7787, 2013.

[CSUU08] 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.

[DSV13] I. Dinur, D. Steurer, and T. Vidick. A parallel repetition theorem for entangled projection games. arxiv:1310.4113, 2013.

[Hol09] Thomas Holenstein. Parallel repetition: Simplification and the no-signaling case. *Theory of Computing*, 5(1):141–172, 2009.

[JPY13] 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.

[KRT10] Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. *SIAM J. Comput.*, 39(7):3207–3229, July 2010.

[KV11] 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.

[Rao11] Anup Rao. Parallel repetition in projection games and a concentration bound. *SIAM J. Comput.*, 40(6):1871–1891, 2011.

[Raz98] Ran Raz. A parallel repetition theorem. *SIAM J. Comput.*, 27(3):763–803, June 1998.

[Ros10] 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.

[TFKW13] Marco Tomamichel, Serge Fehr, Jdrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, 2013.