Non-signalling parallel repetition using de Finetti reductions*

(Abstract submitted to QIP 2015)

Rotem Arnon-Friedman[1], Renato Renner[1], and Thomas Vidick[2]

[1] *Institute for Theoretical Physics, ETH-Zürich, CH-8093, Zürich, Switzerland*
[2] *Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, CA, USA*

Abstract

In the context of multiplayer games, the parallel repetition problem can be phrased as follows: given a game G with optimal winning probability $1-\alpha$ and its repeated version G^n (in which n games are played together, in parallel), can the players use strategies that are substantially better than ones in which each game is played independently? This question is relevant in physics for the study of correlations and plays an important role in computer science in the context of complexity and cryptography. In this work the case of multiplayer non-signalling games is considered, i.e., the only restriction on the players is that they are not allowed to communicate during the game. For complete-support games (games where all possible combinations of questions have non-zero probability to be asked) with any number of players we prove a threshold theorem stating that the probability that non-signalling players win more than a fraction $1-\alpha+\beta$ of the n games is exponentially small in $n\beta^2$, for every $0 \leq \beta \leq \alpha$. For games with incomplete support we derive a similar statement, for a slightly modified form of repetition. The result is proved using a new technique, based on a recent de Finetti theorem, which allows us to avoid central technical difficulties that arise in standard proofs of parallel repetition theorems.

Motivation – the question of parallel repetition

Multiplayer games are relevant in many areas of both theoretical physics and theoretical computer science. In physics, multiplayer games give an intuitive way to study the role and implications of entanglement and correlations, e.g., in the setting of Bell inequalities [2, 3]. In computer science such games arise as an important tool in the context of complexity [4–6] and cryptography [7, 8].

Depending on the context, one can analyse any game under different restrictions on the players (in addition to not being allowed to communicate). In classical computer science the players are usually assumed to have only local resources, or strategies, and shared randomness. In contrast, one can also consider quantum strategies. Before the game starts the players create a multipartite quantum state. When the game begins each player locally measures their own part of the state and base the answer on their measurement result. An even more general set of strategies is the set where the players can use any type of correlations that do not allow them to communicate, also called non-signalling correlations. That is, the *only* restriction on the players is that they are not allowed to communicate.

Considering the non-signalling case is interesting for several reasons. A first reason is to minimise the set of assumptions to the mere necessary one. Indeed, if the players are allowed to communicate by sending signals they can win any game. Minimising the set of assumptions can be useful in cryptography when one wishes to get the strongest result possible, without restricting the uncontrolled malicious parties (as in [9–11] for example). Moreover, from the point of view of theoretical physics, it allows a study of correlations without assuming anything about quantum physics to begin with. It is also important to mention that, due to the linearity of the non-signalling constraints, the non-signalling case is often easier to analyse than the quantum or the classical case. Hence, considering it can sometimes serve as a way to get first bounds on quantum and classical strategies, or to gain some new intuition and insights.

When considering multiplayer games, an interesting question is the question of parallel repetition: given a game G with optimal winning probability $1-\alpha$, can the players win more than a fraction $1-\alpha$

*Full version [1]: `http://arxiv.org/abs/1411.1582`

of the n repetitions of G (when played together, in parallel) with non-negligible probability? A negative answer to this question will tell us that "one cannot fight independence with correlations". As long as the questions are asked, and the answers are verified, in an independent way, creating correlations between the different answers using a correlated strategy cannot help much.

Related work. Recently, closely following the proof technique of [12–14] which was used to prove parallel repetition results for two-player classical and non-signalling games, a threshold theorem for multiplayer non-signalling complete-support games, i.e., games where all possible combinations of questions to the players must have non-zero probability of being asked, was proven in [15]. This was the first and only result where more than two players were considered (in both the classical, quantum and non-signalling case). The question of parallel repetition in the quantum case is less understood. All currently known results (e.g., [16–21]) deal with limited classes of two-player games and no general proof is known.

de Finetti theorems in the context of parallel repetition. The main difficulty in proving a parallel repetition result comes from the arbitrary correlations that the players introduce between the different question-answers pairs. Yet, there is one symmetry which one can take advantage of but is usually ignored – permutation invariance symmetry. As the game G^n itself is invariant under joint permutation of the tuples of questions and answers, we can restrict our attention to permutation-invariant strategies, strategies which are indifferent to the ordering of the questions given by the referee, without loss of generality.

Once we restrict our attention to permutation-invariant strategies, de Finetti theorems seem like a natural tool. A de Finetti theorem is any type of theorem which relates any permutation-invariant state to a more structured state, having the form of a convex combination of independent and identically distributed (i.i.d.) states, called a de Finetti state. There are many different types of de Finetti theorems (e.g., [22–28]) but the common feature of all de Finetti theorems is that they enable a substantially simplified analysis of information-processing tasks by exploiting permutation invariance symmetry (as in [26, 27, 29–31]).

In the context of games and strategies, de Finetti theorems suggest one may be able to reduce the analysis of general permutation-invariant strategies to the analysis of a de Finetti strategy, i.e., a convex combination of i.i.d. strategies. As the behaviour of i.i.d. strategies is trivial under parallel repetition, a reduction of this type could simplify the analysis of parallel repetition theorems and threshold theorems.

Yet, de Finetti theorems were not used in the past in this context, and for a good reason. The many versions of quantum de Finetti theorems (e.g., [25, 27]) could not have been used as they depend on the dimension of the underlying quantum strategies, while in the multiplayer game setting one does not wish to restrict the dimension. Non-signalling de Finetti theorems, as in [32, 33], were also not applicable for non-signalling parallel repetition theorems (for details see [1]). In this work we use the recent de Finetti theorem of [28], which imposes no assumptions at all regarding the structure of the strategies (apart from permutation invariance), and is therefore applicable in the context of parallel repetition.

Our contribution – the results and their importance

We prove the following threshold theorem for the n-fold repetition of any complete-support m-player non-signalling game (and a slightly modified theorem for games with incomplete-support, see [1]).

Theorem. *For any complete-support game G with optimal non-signalling winning probability $1-\alpha$ there exist $\mathcal{C}_1(G,n)$ and $\mathcal{C}_2(G)$, where $\mathcal{C}_1(G,n)$ is polynomial in the number of repetitions n, such that for every $0<\beta\leq\alpha$ and large enough number of repetitions, the probability that non-signalling players win more than a fraction $1-\alpha+\beta$ of n questions in the repeated game G^n is at most $\mathcal{C}_1(G,n)\exp\left[-\mathcal{C}_2(G)n\beta^2\right]$.*

That is, for large enough number of repetitions the probability to win more than a fraction $1-\alpha+\beta$ of the n games is exponentially small. The constant $\mathcal{C}_1(G,n)$ is such that $\mathcal{C}_1(G,n)<10m|\mathcal{Q}||\mathcal{A}|\left(n+1\right)^{2(|\mathcal{Q}||\mathcal{A}|-1)}$ where m is the number of players, and $|\mathcal{Q}|$ and $|\mathcal{A}|$ are the number of possible questions and answers,

respectively, in G. $\mathcal{C}_2(G)$ is a finite constant that can be computed by solving a polynomial-size linear program. A sufficient condition on n for the theorem to hold is $n = \Omega\left(|\mathcal{Q}||\mathcal{A}|\frac{\mathcal{C}_2}{\beta^2}\ln^2(|\mathcal{Q}||\mathcal{A}|\frac{\mathcal{C}_2}{\beta})\right)$. As far as we are aware, this is the first threshold theorem where optimal dependency on β (as follows from optimal formulations of the Chernoff bound) is achieved. For further details and a complete comparison between the exponential bound we prove and the previously known bound of [15], see Section IA in [1].

In addition to the bound itself, our most important contribution is a new proof technique. While most of the known parallel repetition results build on the proof technique of [12] we give a different proof, with ideas emerging from quantum information theory, such as de Finetti theorems and quantum tomography.

Apart from allowing a different point of view on the question of parallel repetition, and the study of correlations in general, the new proof technique has several advantages over previous proofs. For instance, our proof technique allows us to avoid the usual difficulties which arise in proofs of parallel repetition theorems, such as conditioning on some of the questions and answers or considering an arbitrary number of players. In this sense our proof can be seen as more natural than previous proofs, and therefore more likely to be extendable to the classical and quantum multiplayer cases as well.

We stress that de Finetti theorems are very general and come in many flavours; in addition to its intrinsic interest we think of the present application to parallel repetition as a further demonstration of their strength, and we expect it to find further extensions in the future.

Main ideas of the proof. A strategy for G is a conditional probability distribution $\mathrm{O}_{A|Q} : \mathcal{A} \times \mathcal{Q} \to [0,1]$, where q is an m-tuple question in the game and a is an m-tuple answer. Similarly, a strategy for a repeated game G^n is a conditional probability distribution denoted by $\mathrm{P}_{\vec{A}|\vec{Q}} : \mathcal{A}^n \times \mathcal{Q}^n \to [0,1]$.

The first trivial, but crucial, observation made is that one can concentrate without loss of generality on permutation-invariant strategies for G^n (see Lemma 22 in [1] for the formal argument). This allows us to use the de Finetti theorem of [28] which relates any permutation-invariant strategy to a de Finetti strategy. The exact statement of the de Finetti theorem is not relevant to understand the main ideas of the proof. For now, one can see any permutation-invariant strategy for the repeated game as having the form of convex combination of i.i.d. strategies[1]:

$$\mathrm{P}_{\vec{A}|\vec{Q}} \approx \int \mathrm{O}_{A|Q}^{\otimes n} \mathrm{dO}_{A|Q} \tag{1}$$

where $\mathrm{dO}_{A|Q}$ is some measure on the space of one-game strategies and $\mathrm{O}_{A|Q}^{\otimes n}$ is a product of n identical strategies $\mathrm{O}_{A|Q}$. Unfortunately, the convex combination itself (meaning, the measure $\mathrm{dO}_{A|Q}$) is unknown. Moreover, even though we assume that the strategy $\mathrm{P}_{\vec{A}|\vec{Q}}$ does not allow the m players to communicate as it is non-signalling, the convex combination might still include signalling parts, i.e., signalling $\mathrm{O}_{A|Q}$.

For the non-signalling parts of the convex combination one can easily prove a threshold theorem. The only thing which is left to prove is therefore that the *signalling* part of the convex combination of Equation (1) has an exponentially small weight. We find this question interesting by itself, and of course, the same question can be asked in the classical and quantum case as well – given a classical or quantum strategy $\mathrm{P}_{\vec{A}|\vec{Q}}$, what is the weight of the non-classical or non-quantum i.i.d. parts in the convex combination?

To bound the weight of the signalling part we take an operational approach, following ideas from quantum tomography [30]. We define a hypothetical signalling test which, when applied to questions and answers which are distributed according to an i.i.d. strategy $\mathrm{O}_{A|Q}^{\otimes n}$, estimates a signalling value of the strategy $\mathrm{O}_{A|Q}$ (see Definition 13 in [1]) and accepts only if it is above a certain threshold. In order to bound the weight of the signalling part in Equation (1) we can equivalently bound the acceptance probability of the test, when applied to data distributed according to $\mathrm{P}_{\vec{A}|\vec{Q}}$. This, in turn, is done by using a reduction to a guessing game that we construct which shows that if the probability of the test accepting is not exponentially small, then the original strategy $\mathrm{P}_{\vec{A}|\vec{Q}}$ must have been signalling – a contradiction.

[1] We emphasise once again that this is not a quantitive statement that we claim to be correct.

References

[1] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Non-signalling parallel repetition using de finetti reductions. *arXiv preprint arXiv:1411.1582*, 2014.

[2] John S Bell et al. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[4] Uriel Feige, Shafi Goldwasser, Laszlo Lovász, Shmuel Safra, and Mario Szegedy. Interactive proofs and the hardness of approximating cliques. *J. ACM*, 43(2):268–292, 1996.

[5] Uriel Feige and László Lovász. Two-prover one-round proof systems: Their power and their problems. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing (STOC)*, pages 733–744, 1992.

[6] Irit Dinur. The PCP theorem by gap amplification. *J. ACM*, 54(3), June 2007.

[7] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 113–131, 1988.

[8] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. Delegation for bounded space. In *Proc. 45th STOC*, pages 565–574, New York, NY, USA, 2013. ACM.

[9] E. Hänggi, R. Renner, and S. Wolf. Quantum cryptography based solely on Bell's theorem. *arXiv preprint arXiv:0911.4171*, 2009.

[10] Lluis Masanes. Universally composable privacy amplification from causality constraints. *Physical Review Letters*, 102(14):140501, 2009.

[11] Lluís Masanes, Renato Renner, Matthias Christandl, Andreas Winter, and Jonathan Barrett. Full security of quantum key distribution from no-signaling constraints. *Information Theory, IEEE Transactions on*, 60(8):4973–4986, 2014.

[12] Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[13] Thomas Holenstein. Parallel repetition: simplifications and the no-signaling case. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 411–419. ACM, 2007.

[14] Anup Rao. Parallel repetition in projection games and a concentration bound. *SIAM Journal on Computing*, 40(6):1871–1891, 2011.

[15] Harry Buhrman, Serge Fehr, and Christian Schaffner. On the parallel repetition of multi-player games: The no-signaling case. *arXiv preprint arXiv:1312.7455*, 2013.

[16] André Chailloux and Giannicola Scarpa. Parallel repetition of free entangled games: Simplification and improvements. *arXiv preprint arXiv:1410.4397*, 2014.

[17] Rahul Jain, Attila Pereszlényi, and Penghui Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. *arXiv preprint arXiv:1311.6309*, 2013.

[18] Irit Dinur, David Steurer, and Thomas Vidick. A parallel repetition theorem for entangled projection games. *arXiv preprint arXiv:1310.4113*, 2013.

[19] Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. In *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on*, pages 457–466. IEEE, 2008.

[20] 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.

[21] Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 353–362. ACM, 2011.

[22] B. de Finetti. Sulla proseguibilità di processi aleatori scambiabili. *Rend. Matem. Trieste*, pages 53–67, 1969.

[23] Persi Diaconis and David Freedman. Finite exchangeable sequences. *The Annals of Probability*, pages 745–764, 1980.

[24] Carlton M Caves, Christopher A Fuchs, and Rüdiger Schack. Unknown quantum states: the quantum de-Finetti representation. *Journal of Mathematical Physics*, 43:4537, 2002.

[25] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.

[26] Fernando GSL Brandao and Aram W Harrow. Quantum de Finetti theorems under local measurements with applications. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 861–870. ACM, 2013.

[27] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102(2):020504, 2009.

[28] Rotem Arnon-Friedman and Renato Renner. de Finetti reductions beyond quantum theory. *arXiv preprint arXiv:1308.0312*, 2013.

[29] M. Berta, M. Christandl, and R. Renner. The quantum reverse shannon theorem based on one-shot information theory. *Communications in Mathematical Physics*, 306(3):579–615, 2011.

[30] Matthias Christandl and Renato Renner. Reliable quantum state tomography. *Physical Review Letters*, 109(12):120403, 2012.

[31] Anthony Leverrier. Composable security proof for continuous-variable quantum key distribution with coherent states. *arXiv preprint arXiv:1408.5689*, 2014.

[32] Jonathan Barrett and Matthew Leifer. The de Finetti theorem for test spaces. *New Journal of Physics*, 11(3):033024, 2009.

[33] Matthias Christandl and Ben Toner. Finite de Finetti theorem for conditional probability distributions describing physical theories. *Journal of Mathematical Physics*, 50:042104, 2009.