Parallel Repetition of Two Prover Games

Ran Raz*
Weizmann Institute

Abstract

The parallel repetition theorem states that for any two-prover game with value smaller than 1, parallel repetition reduces the value of the game in an exponential rate. We give a short introduction to the problem of parallel repetition of two-prover games and some of its applications in theoretical computer science, mathematics and physics. We will concentrate mainly on recent results.

1 Introduction

Two-Prover Games

A *two-prover* game is played between two players called *provers* and an additional player called *verifier*. The game consists of four finite sets X, Y, A, B, a probability distribution P over $X \times Y$ and a predicate $V : X \times Y \times A \times B \to \{0, 1\}$. All parties know X, Y, A, B, P, V. Intuitively: X is the set of possible questions for the first prover. Y is the set of possible questions for the second prover. A is the set of possible answers of the first prover. B is the set of possible answers of the second prover. The distribution P is used to generate questions for the two provers, and the predicate V is used to accept or reject after the answers from both provers are obtained.

The game proceeds as follows. The verifier chooses a pair of questions $(x, y) \in_P X \times Y$ (that is, (x, y) are chosen according to the distribution P), and sends x to the first prover and y to the second prover. Each prover knows only the question addressed to her, and the provers are not allowed to communicate with each other. The first prover responds by $a = a(x) \in A$ and the second by $b = b(y) \in B$. The provers jointly win if $V(x, y, a, b) = 1$.

The provers answer the questions according to a pair of functions $a : X \to A$, $b : Y \to B$. The pair (a, b) is called the provers' *strategy* or the provers' *protocol*. The *value* of the game is the maximal probability of success that the provers can achieve, where the maximum is taken over all protocols (a, b). That is, the value of the game is

$$\max_{a,b} \mathbb{E}_{(x,y)}[V(x, y, a(x), b(y))]$$

where the expectation is taken with respect to the distribution P.

*ran.raz@weizmann.ac.il

Unique and Projection Games

A two-prover game is called a *projection game* if for every pair of questions $(x, y) \in X \times Y$ there is a function $f_{x,y} : B \to A$, such that, for every $a \in A$, $b \in B$, we have: $V(x, y, a, b) = 1$ if and only if $f_{x,y}(b) = a$. If in addition, for every $(x, y) \in X \times Y$ the function $f_{x,y}$ is a bijection (that is, it is one to one and onto), the game is called *unique*. A unique game with $A, B = \{0, 1\}$ is called a *xor* game.

Parallel Repetition of Two-Prover Games

Roughly speaking, the *parallel repetition* of a two-prover game G is a game where the provers try to win simultaneously n copies of G. The parallel repetition game is denoted by $G^{\otimes n}$. More precisely, in the game $G^{\otimes n}$ the verifier generates questions $x = (x_1, \ldots, x_n) \in X^n$, $y = (y_1, \ldots, y_n) \in Y^n$, where each pair $(x_i, y_i) \in X \times Y$ is chosen independently according to the original distribution P. The provers respond by $a = (a_1, \ldots, a_n) = a(x) \in A^n$ and $b = (b_1, \ldots, b_n) = b(y) \in B^n$. The provers win if they win simultaneously on all n coordinates, that is, if for every i, we have $V(x_i, y_i, a_i, b_i) = 1$.

Note that the verifier treats each of the n copies of G independently, but the provers may not; the answer for each question addressed to a prover may depend on all the questions addressed to that prover.

The value of the game $G^{\otimes n}$ is not necessarily the same as the value of the game G raised to the power of n. For example, there exist simple two-prover games G, such that, the value of the game G and the value of the game $G^{\otimes 2}$ are both $1/2$.

Parallel Repetition Theorem

Feige and Lovász conjectured [15] that for any two-prover game G with value smaller than 1, the value of the game $G^{\otimes n}$ decreases exponentially fast to 0. The conjecture was proved in [22].

More precisely, the parallel repetition theorem [22] states that for any two-prover game G, with value $\leq 1 - \epsilon$ (for any $0 < \epsilon \leq 1/2$), the value of the game $G^{\otimes n}$ is at most

$$(1 - \epsilon^c)^{\Omega(n/s)}, \tag{1}$$

where $s = \log |A \times B| + 1$ is the answers' length of the original game, and c is a universal constant. The constant c implicit in [22] is $c = 32$. An example by Feige and Verbitsky [16] shows that the dependency on s in Inequality 1 is necessary.

A beautiful recent work by Thomas Holenstein [18] simplified the proof of [22] and obtained an improved constant of $c = 3$. An intriguing followup work by Anup Rao [21] gave for the special case of projection games, an improved bound of

$$(1 - \epsilon^2)^{\Omega(n)}. \tag{2}$$

Thus, for projection games, Rao obtained an improved constant of $c = 2$ and removed the dependency on s. Previously, such a bound was known for the special case of xor games [14].

Several researchers asked wether or not these bounds could be improved to $(1-\epsilon)^{\Omega(n/s)}$, for general two-prover games, or at least for interesting special cases, such as, projection games, unique games, or xor games (see for example [14, 24]); this question is usually referred to as the *strong parallel repetition problem*. However, a recent analysis shows that the, so called, *odd cycle game* (first studied in [14, 10]) is a counterexample to strong parallel repetition [23]. More precisely, for any $0 < \epsilon \leq 1/2$, there exists a two-prover game with value $\leq 1-\epsilon$, such that, (for large enough n) the value of the game repeated in parallel n times is $\geq (1-\epsilon^2)^{O(n)}$ [23] (see also [8]). Since the odd cycle game is a projection game, a unique game, and a xor game, this answers negatively most variants of the strong parallel repetition problem. This example also shows that Inequality 2 is tight.

Finally, let us mention that for games where the distribution P on $X \times Y$ is a product distribution, improved bounds of $(1-\epsilon^2)^{\Omega(n/s)}$ (for general games) and $(1-\epsilon)^{\Omega(n)}$ for projection games, where recently obtained [9]. Thus, for projection games with product distributions a strong parallel repetition theorem is known.

2 Applications

Direct Sum and Direct Product

Direct sum and *direct product* problems are an important paradigm in understanding the power of a computational model, and have been studied for a variety of models.

In a direct sum problem, one asks the following question. If a model requires cost C (in some complexity measure) to solve a certain problem on one input, how costly would it be to solve it on n independent inputs? For instance; is this cost close to $\Omega(C \cdot n)$ for every problem in the model, or maybe significant savings can be obtained by combining computations?

In a direct product problem, a dual view is taken. We fix the cost C and study the probability that n independent inputs (over some input distribution) are solved correctly. For instance; is it true that for every problem in the model, for a fixed cost, the probability to solve n independent inputs correctly drops exponentially with n?

The parallel repetition theorem can be viewed as a direct product result for two-prover games, and turned out to be related to both direct sum and direct product results in communication complexity:

In [20] the parallel repetition theorem was used to prove general direct product results in communication complexity. The main idea there was to encode the entire communication protocol (in the communication complexity model) into the answers given by the two provers in a two-prover game. A beautiful recent work by Barak, Braverman, Chen and Rao proves general direct sum results in communication complexity [5]. Their proofs do not use the parallel repetition theorem directly, but make an extensive use in the techniques used in the proof of the parallel repetition theorem.

Entangled Games and the EPR Paradox

An *entangled* two-prover game is the same as a two-prover game, except that the two provers share between them an arbitrary entangled quantum state and each prover may measure her part of the state before answering the question addressed to her by the verifier. More precisely, the two provers share between them an arbitrary entangled quantum state, partitioned into two parts (one for each prover). After receiving the questions addressed by the verifier, each prover may apply an arbitrary quantum measurement (that may depend on the question addressed to her) on her part of the quantum state, and her answer may depend on the outcome of the measurement. (As before, the provers are not allowed to communicate with each other). This enables complicated correlations between the two answers. The *entangled* (or *quantum*) value of a two-prover game is defined to be the maximal probability of success that the provers can achieve using such protocols.

Bell's celebrated theorem [4], building over the famous Einstein-Podolsky-Rosen paradox [11], can be stated as follows: There are two-prover games with entangled value strictly larger than their (classical) value. Moreover, there are known examples for two-prover games with entangled value 1 and (classical) value strictly smaller than 1 (see for example [10]). Hence, as observed by Cleve, Høyer, Toner and Watrous [10], one can use parallel repetition to obtain two-prover games with entangled value 1 and (classical) value arbitrarily close to 0. This gives a sharper version of Bell's theorem.

Foams and Tiling the Space $\mathbb{R}^n$

Feige, Kindler and O'Donnell discovered [14] that deep geometrical problems of understanding n-dimensional foams and tiling the space $\mathbb{R}^n$ are closely related to analyzing the value of the parallel repetition of one particular two-prover game; the (above mentioned) odd cycle game.

The odd cycle game is a two-prover game, first suggested and motivated in [10, 14]. Let $m \geq 3$ be an odd integer and consider a graph of a single cycle of length m. Intuitively, the two provers are trying to convince the verifier that the graph is 2-colorable. The game proceeds as follows. With probability one half the verifier asks the two provers about the color of the same node in the graph and accepts their answers if they are the same (and are in $\{0,1\}$). With probability one half the verifier asks the two provers about the colors of two adjacent nodes in the graph and accepts their answers if they are different (and are in $\{0,1\}$). It is easy to see that the value of the game is $1 - \Theta(1/m)$.

A recent analysis of the odd cycle game [23] shows that the value of the game repeated in parallel n times is at least $1 - (1/m) \cdot O(\sqrt{n})$. (This matches, up to a logarithmic factor, an upper bound proved in [14]). This is somewhat surprising since the probability of failure grows linearly in $\sqrt{n}$, rather than linearly in n.

By generalizing these results and techniques to the continuous case, and using the connection discovered by Feige, Kindler and O'Donnell [14], Kindler, O'Donnell, Rao and Wigderson obtained amazing results about tiling the space $\mathbb{R}^n$ [19]. Their main result is the existence of a body with volume 1 and surface area $O(\sqrt{n})$ that tiles $\mathbb{R}^n$ by the lattice $\mathbb{Z}^n$ (in the sense

that its translations by vectors from $\mathbb{Z}^n$ cover $\mathbb{R}^n$). In other words, this body tiles $\mathbb{R}^n$ as a cube (that is, it tiles $\mathbb{R}^n$ by the lattice $\mathbb{Z}^n$), but its surface area is similar to the surface area of a (volume 1) sphere! A beautiful followup work, by Alon and Klartag [1], further studies these geometrical applications and related combinatorial problems, and relates them to Cheeger's isoperimetric inequality and its discrete analogues.

PCP and Hardness of Approximation

The PCP theorem [6, 13, 3, 2] can be stated as follows: Given (as an input) a projection game G with answers of length $O(1)$ (that is, with $|A|, |B| = O(1)$), it is NP-hard to distinguish between the case where the value of the game is 1 and the case where the value of the game is at most 0.9. Using parallel repetition (a constant number of times), one obtains the following sharper version of the PCP theorem: For any constant $\epsilon > 0$, given a projection game G with answers of length $O(1)$, it is NP-hard to distinguish between the case where the value of the game is 1 and the case where the value of the game is at most ϵ.

It turned out that this version of the PCP theorem is very useful as a starting point for proving results on hardness of approximation. This started by Bellare, Goldreich and Sudan [7], and continued in a large number of works that studied a large number of problems. In particular, some of the most central results on hardness of approximation, such as, Håstad's celebrated optimal results on the hardness of approximation of 3-SAT and 3-LIN [17], are proved using this approach. Other central results, such as, Feige's optimal results on the hardness of approximation of Set-Cover [12], are obtained by applying parallel repetition more than a constant number of times.

References

[1] Noga Alon, Boaz Klartag. Economical Toric Spines via Cheeger's Inequality. *Journal of Topology and Analysis*, 1 : 101-111 (2009)

[2] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, Mario Szegedy. Proof Verification and the Hardness of Approximation Problems. *J. ACM* 45(3): 501-555 (1998) (preliminary version in FOCS 1992)

[3] Sanjeev Arora, Shmuel Safra. Probabilistic Checking of Proofs: A New Characterization of NP. *J. ACM* 45(1): 70-122 (1998) (preliminary version in FOCS 1992)

[4] John Bell. On the Einstein-Podolsky-Rosen Paradox. *Physics* 1: 195-200 (1964)

[5] Boaz Barak, Mark Braverman, Xi Chen, Anup Rao. How to Compress Interactive Communication. STOC 2010

[6] László Babai, Lance Fortnow, Carsten Lund. Non-Deterministic Exponential Time has Two-Prover Interactive Protocols. *Computational Complexity* 1: 3-40 (1991) (preliminary version in FOCS 1990)

[7] Mihir Bellare, Oded Goldreich, Madhu Sudan. Free Bits, PCPs, and Nonapproximability-Towards Tight Results. *SIAM J. Comput.* 27(3): 804-915 (1998) (preliminary version in FOCS 1995)

[8] Boaz Barak, Moritz Hardt, Ishay Haviv, Anup Rao, Oded Regev, David Steurer. Rounding Parallel Repetitions of Unique Games. FOCS 2008: 374-383

[9] Boaz Barak, Anup Rao, Ran Raz, Ricky Rosen, Ronen Shaltiel. Strong Parallel Repetition Theorem for Free Projection Games. APPROX-RANDOM 2009: 352-365

[10] Richard Cleve, Peter Høyer, Benjamin Toner, John Watrous. Consequences and Limits of Nonlocal Strategies. CCC 2004: 236-249

[11] Albert Einstein, Boris Podolsky, Nathan Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* 47: 777-780 (1935)

[12] Uriel Feige. A Threshold of ln n for Approximating Set Cover. *J. ACM* 45(4): 634-652 (1998) (preliminary version in STOC 1996)

[13] Uriel Feige, Shafi Goldwasser, László Lovász, Shmuel Safra, Mario Szegedy. Interactive Proofs and the Hardness of Approximating Cliques. *J. ACM* 43(2): 268-292 (1996) (preliminary version in FOCS 1991)

[14] Uriel Feige, Guy Kindler, Ryan O'Donnell. Understanding Parallel Repetition Requires Understanding Foams. CCC 2007: 179-192

[15] Uriel Feige, László Lovász. Two-Prover One-Round Proof Systems: Their Power and Their Problems STOC 1992: 733-744

[16] Uriel Feige, Oleg Verbitsky: Error Reduction by Parallel Repetition - A Negative Result. *Combinatorica* 22(4): 461-478 (2002) (preliminary version in CCC 1996)

[17] Johan Håstad. Some Optimal Inapproximability Results. *J. ACM* 48(4): 798-859 (2001) (preliminary version in STOC 1997)

[18] Thomas Holenstein. Parallel Repetition: Simplifications and the No-Signaling Case. *Theory of Computing* 5(1): 141-172 (2009) (preliminary version in STOC 2007)

[19] Guy Kindler, Ryan O'Donnell, Anup Rao and Avi Wigderson. Rounding Schemes and Cubical Tilings with Sphere-Like Surface Area. FOCS 2008: 189-198

[20] Itzhak Parnafes, Ran Raz, Avi Wigderson. Direct Product Results and the GCD Problem, in Old and New Communication Models. STOC 1997: 363-372

[21] Anup Rao. Parallel Repetition in Projection Games and a Concentration Bound. STOC 2008: 1-10

[22] Ran Raz. A Parallel Repetition Theorem. *SIAM J. Comput.* 27(3): 763-803 (1998) (preliminary version in STOC 1995)

[23] Ran Raz. A Counterexample to Strong Parallel Repetition. FOCS 2008: 369-373

[24] Muli Safra, Oded Schwartz. On Parallel-Repetition, Unique-Game and Max-Cut. Manuscript 2007