# A Counterexample to Strong Parallel Repetition

Ran Raz*
Weizmann Institute

**Abstract**

The parallel repetition theorem states that for any *two-prover game*, with value $1-\epsilon$ (for, say, $\epsilon \leq 1/2$), the value of the game repeated in parallel $n$ times is at most $(1-\epsilon^c)^{\Omega(n/s)}$, where $s$ is the answers' length (of the original game) and $c$ is a universal constant [R95]. Several researchers asked wether this bound could be improved to $(1-\epsilon)^{\Omega(n/s)}$; this question is usually referred to as the *strong parallel repetition problem*. We show that the answer for this question is negative.

More precisely, we consider the *odd cycle game* of size $m$; a two-prover game with value $1-1/2m$. We show that the value of the odd cycle game repeated in parallel $n$ times is at least $1-(1/m)\cdot O(\sqrt{n})$. This implies that for large enough $n$ (say, $n \geq \Omega(m^2)$), the value of the odd cycle game repeated in parallel $n$ times is at least $(1-1/4m^2)^{O(n)}$. Thus:

1. For parallel repetition of general games: the bounds of $(1-\epsilon^c)^{\Omega(n/s)}$ given in [R95, Hol07] are of the right form, up to determining the exact value of the constant $c \geq 2$.
2. For parallel repetition of XOR games, unique games and projection games: the bounds of $(1-\epsilon^2)^{\Omega(n)}$ given in [FKO07] (for XOR games) and in [Rao07] (for unique and projection games) are tight.
3. For parallel repetition of the odd cycle game: the bound of $1-(1/m)\cdot\tilde{\Omega}(\sqrt{n})$ given in [FKO07] is almost tight.

A major motivation for the recent interest in the strong parallel repetition problem is that a strong parallel repetition theorem would have implied that the *unique game conjecture* is equivalent to the NP hardness of distinguishing between instances of Max-Cut that are at least $1-\epsilon^2$ satisfiable from instances that are at most $1-(2/\pi)\cdot\epsilon$ satisfiable. Our results suggest that this cannot be proved just by improving the known bounds on parallel repetition.

## 1 Introduction

In a *two-prover* (alternatively, *two-player*) game, a referee chooses questions $(x, y)$ according to a (publicly known) distribution, and sends $x$ to the first player and $y$ to the second player.

*ran.raz@weizmann.ac.il, Research supported by the Israel Science Foundation (ISF), the Binational Science Foundation (BSF) and the Minerva Foundation.

The first player responds by $a = a(x)$ and the second by $b = b(y)$ (without communicating with each other). The players jointly win if a (publicly known) predicate $V(x, y, a, b)$ holds. The value of the game is the maximal probability of success that the players can achieve, where the maximum is taken over all protocols $a = a(x), b = b(y)$.

Roughly speaking, a parallel repetition of a two-prover game is a game where the players try to win $n$ copies of the original game simultaneously. More precisely, the referee generates questions $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$, where each pair $(x_i, y_i)$ is chosen independently according to the original distribution. The players respond by $a = (a_1, \ldots, a_n) = a(x)$ and $b = (b_1, \ldots, b_n) = b(y)$. The players win if they win simultaneously on all the coordinates, that is, if for every $i$, $V(x_i, y_i, a_i, b_i)$ holds.

The parallel repetition theorem states that for any two-prover game, with value $\leq 1 - \epsilon$ (for, say, $\epsilon \leq 1/2$), the value of the game repeated in parallel $n$ times is

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

where $s$ is the answers' length of the original game, and $c$ is a universal constant [R95]. The constant $c$ implicit in [R95] is $c = 32$. A beautiful recent result by Holenstein simplifies the proof of [R95] and gives an improved constant of $c = 3$ [Hol07]. Another beautiful very recent result by Rao gives for the special case of, so called, *unique* and *projection* games, improved bounds of

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

(Previously, such bounds were known for the special case of, so called, XOR games; see [FKO07]).

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; this question is usually referred to as the *strong parallel repetition problem*. The problem appeared as an open problem in [FKO07] and the answer was conjectured in [SS07] to be positive for certain special cases.

We show that the, so called, *odd cycle game* is an example for 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

$$\geq (1 - \epsilon^2)^{O(n)}.$$

Since the odd cycle game is a projection game, a unique game, and a XOR game, this answers negatively all versions of the strong parallel repetition problem.

Previous to our result, an example by Feige and Verbitsky [FV96] shows that the dependency on $s$ in Inequality 1 is necessary. For the case of answers of length 1, we are not aware of any previous example where the value of the game repeated in parallel $n$ times is (provenly) larger than $(1 - \epsilon)^{n/2}$. In other words, we are not aware of any previous example where a protocol for the game repeated in parallel $n$ times saves more than a factor of 2 in the exponent, over the trivial product protocol.

A major motivation for the recent interest in the strong parallel repetition problem is that a positive answer for this problem would have implied that the *unique game conjecture* [Kho02] is very related to the hardness of approximation of Max-Cut. More precisely, it was proved in [KKMO04] that the unique game conjecture implies that for any small enough $\epsilon > 0$, it is NP hard to distinguish between instances of Max-Cut that are at least $1 - \epsilon^2$ satisfiable from instances that are at most $1-(2/\pi)\cdot\epsilon$ satisfiable. A strong parallel repetition theorem, or even improving the constant $c$ in the current bounds to anything smaller than 2 (even for the special case of games that are induced by instances of Max-Cut), would have implied that a reduction in the other direction also holds, that is, that the unique game conjecture is equivalent to the NP hardness of distinguishing between instances of Max-Cut that are at least $1 - \epsilon^2$ satisfiable from instances that are at most $1 - (2/\pi) \cdot \epsilon$ satisfiable. Moreover, this was one of the main directions suggested for proving the unique game conjecture: first prove that it is equivalent to the NP hardness of distinguishing these instances of Max-Cut, and then prove the NP hardness of distinguishing these instances of Max-Cut. Since our counterexample is induced by an instance of Max-Cut, it suggests that this cannot be proved just by improving the known bounds on parallel repetition.

### 1.1 Followup Works

Since the distribution of a preliminary version of this paper, several wonderful followup works have appeared.

Barak, Hardt, Haviv, Rao, Regev and Steurer generalize our results and techniques to other unique games, and show that a wide class of unique games yield similar counterexamples to strong parallel repetition. They show a connection between the semidefinite relaxation of unique games and their behavior under parallel repetition. They use this connection to determine asymptotically the value of the repeated version of any unique game, up to a logarithmic factor in the exponent ! [BHHRRS08].

Kindler, O'Donnell, Rao and Wigderson generalize our results and techniques to the continuous case, and use it to solve important geometrical problems about tiling the space $\mathbb{R}^n$. Their main result is the existence of a body with volume 1 and surface area $O(\sqrt{n})$ that tiles $\mathbb{R}^n$ by $\mathbb{Z}^n$ (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 but its surface area is similar to the surface area of a (volume 1) sphere ! [KORW08]. The connection between parallel repetition of the odd cycle game and this geometrical problem of tiling the space $\mathbb{R}^n$ was previously discovered by Feige, Kindler and O'Donnell [FKO07]. Another beautiful followup work, by Alon and Klartag, further studies these geometrical applications and related combinatorial problems, using the isoperimetric inequality of Cheeger and its discrete analogues [AK08].

## 2 The Odd Cycle Game

The odd cycle game is a two-prover game, first suggested in [CHTW04] and further motivated and studied in [FKO07, AS08]. Let $m \geq 3$ be an odd integer and consider a graph of a single

cycle of length $m$. Intuitively, the two players are trying to convince the referee that the graph is 2-colorable. With probability one half the referee asks the two players about the color of the same node in the graph and accepts their answers if they are the same. With probability one half the referee asks the two players about the colors of two adjacent nodes in the graph and accepts their answers if they are different.

Formally, the question $x$ is chosen uniformly in $\{0, \ldots, m-1\}$ and the question $y$ is chosen to be: $x$ with probability $1/2$, $x-1$ with probability $1/4$, and $x+1$ with probability $1/4$ (where $x+1$ and $x-1$ are taken modulo $m$). The predicate $V(x, y, a, b)$ holds if both $a, b \in \{0, 1\}$ and: if $x = y$ then $a = b$, and if $x \neq y$ then $a \neq b$. It is easy to see that the value of the odd cycle game is $1 - 1/2m$.

In this paper, we are interested in the value of the odd cycle game repeated in parallel $n$ times. It was proved in [FKO07] that (for $n < m^2$) the value of the repeated game is at most

$$1 - (1/m) \cdot \tilde{\Omega}(\sqrt{n}),$$

(where $\tilde{\Omega}$ is the same as the usual $\Omega$ notation, up to poly-logarithmic factors). Our main result is a probabilistic protocol for the repeated game, that achieves a value of

$$1 - (1/m) \cdot O(\sqrt{n}).$$

Note that since a probabilistic protocol can be presented as a convex combination of deterministic protocols, the same value can be achieved by a deterministic protocol. Note also that for large enough $n$ (say, $n \geq \Omega(m^2)$), this also gives a protocol for the repeated game that achieves a value of

$$(1 - 1/4m^2)^{O(n)}.$$

This is done as follows: Let $\alpha$ be a small enough constant. Partition $[n]$ into $\approx \frac{n}{\alpha \cdot m^2}$ blocks of size at most $\alpha \cdot m^2$ each, and apply the previous protocol on each block separately.

# 3 A Technical Lemma

Let $m = 2k + 1$ be an odd integer. For integers $i \leq j$, let $[i, j]$ be the set $\{i, i+1, \ldots, j\}$. Let $I$ be the set $[-k, k]$ of size $m$. Addition and subtraction of elements of $I$ will be taken modulo $m$ and the result will be viewed as an element of $I$.

**Lemma 3.1.** *There exists a probability distribution $f : I \to \mathbb{R}$, such that:*

1. *For every $i \in I$, $f(i) > 0$*
2. *$f(k), f(-k) \leq O(1/m^3)$*
3. $$\sum_{i \in I} \frac{f(i)^2}{f(i+1)} + \frac{f(i)^2}{f(i-1)} \leq 2 + O(1/m^2)$$

*Proof.* Define $f : I \to \mathbb{R}$ by[1]

$$f(i) = \gamma \cdot (k + 1 - |i|)^2,$$

where $\gamma = \Theta(1/m^3)$ is a normalization factor that ensures that $f$ is a distribution. The first and second requirements in the statement of the lemma obviously hold. It remains to prove the third requirement.

For $j \geq 2$, $\frac{j^2}{(j+1)^2} + \frac{j^2}{(j-1)^2} = 2 + O\left(1/j^2\right)$. Using this equality for $j = k + 1 - |i|$, we have for every $i \in I \setminus \{-k, 0, k\}$,

$$\frac{f(i)^2}{f(i+1)} + \frac{f(i)^2}{f(i-1)} = f(i) \cdot \left(\frac{f(i)}{f(i+1)} + \frac{f(i)}{f(i-1)}\right) = 2f(i) + O(\gamma)$$

For $i = 0$,

$$\frac{f(i)^2}{f(i+1)} + \frac{f(i)^2}{f(i-1)} = 2f(i) \cdot \frac{(k+1)^2}{k^2} = 2f(i) \cdot (1 + O(1/k)) = 2f(i) + O(1/m^2)$$

For $i \in \{-k, k\}$,

$$\frac{f(i)^2}{f(i+1)} + \frac{f(i)^2}{f(i-1)} = f(i) \cdot O(1) = O(\gamma)$$

Thus,

$$\sum_{i \in I} \frac{f(i)^2}{f(i+1)} + \frac{f(i)^2}{f(i-1)} \leq 2 + O(1/m^2)$$

□

# 4 A Protocol for the Repeated Odd Cycle Game

Let $m = 2k + 1$ be an odd integer. For integers $i \leq j$, let $[i, j]$ be the set $\{i, i + 1, \ldots, j\}$.

Let $U$ be the set $[-k, k]$ of size $m$. Addition and subtraction of elements of $U$ will be taken modulo $m$ and the result will be viewed as an element of $U$. We think of $U$ as the set of nodes of the cycle of size $m$. Denote by $E = \{\{i, i + 1\} : i \in U\}$ the set of edges of the cycle of size $m$. We identify the set $E$ with the set $[-k, k]$ by naming every edge in $E$ the same as the node opposite to it (that is, the edge $\{i, i + 1\}$ is named by $i + (m + 1)/2$).

Let $x = (x_1, \ldots, x_n) \in U^n$ (questions to the first player) be uniformly distributed in $U^n$. Let $y = (y_1, \ldots, y_n) \in U^n$ (questions to the second player) be such that each $y_i$ is chosen (independently) as follows: with probability $1/2$, $y_i = x_i$, with probability $1/4$, $y_i = x_i + 1$, and with probability $1/4$, $y_i = x_i - 1$.

For $x, y \in U^n$ and $a, b \in \{0, 1\}^n$, let $\bar{V}(x, y, a, b)$ be the following predicate: for every $i$, $(x_i = y_i) \iff (a_i = b_i)$.

[1] Our original proof used a more complicated distribution. Following a preliminary version of the paper, the distribution $\gamma \cdot \sin^2(\pi i/m + \pi/2)$ was suggested to us by Guy Kindler and Avi Wigderson. Here, we use the related distribution $\gamma \cdot (k + 1 - |i|)^2$.

**Theorem 1.** *There exist $a, b : U^n \to \{0,1\}^n$, such that,*

$$\Pr_{x,y}[\bar{V}(x, y, a(x), b(y))] \geq 1 - (1/m) \cdot O(\sqrt{n})$$

*(where the probability is over $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$, chosen as above).*

## 4.1 Proof of Theorem 1

We will show a probabilistic protocol $(a, b)$, using a shared random string for the two players. Note that this implies that there exists a deterministic protocol that achieves the same value, since a probabilistic protocol is just a convex combination of deterministic ones.

Let $f : [-k, k] \to \mathbb{R}$ be the probability distribution from Lemma 3.1. For every node $u \in U$, define a probability distribution over edges, $P_u : E \to \mathbb{R}$, as follows. For every $e \in E$,

$$P_u(e) = f(e - u)$$

(recall that we identify both $U, E$ with the set $[-k, k]$ and additions and subtractions are taken modulo $m$ in this set).

For every tuple of $n$ nodes, $u = (u_1, \ldots, u_n) \in U^n$, define a probability distribution over tuples of $n$ edges, $P_u : E^n \to \mathbb{R}$, as follows. For every $e = (e_1, \ldots, e_n) \in E^n$,

$$P_u(e_1, \ldots, e_n) = \prod_{i=1}^{n} P_{u_i}(e_i) = \prod_{i=1}^{n} f(e_i - u_i)$$

Consider the two distributions $P_x, P_y$, where $x, y \in U^n$ are the inputs for the two players. The following lemma bounds the $l_1$ distance of these two distributions.

**Lemma 4.1.**

$$E_{x,y} \|P_x - P_y\|_1 \leq (1/m) \cdot O(\sqrt{n})$$

*Proof.* Assume without loss of generality that $n < \alpha \cdot m^2$, for a small enough constant $\alpha > 0$ (otherwise, $(1/m) \cdot \sqrt{n} \geq \Omega(1)$, and the lemma holds trivially).

First note that by symmetry, $\mathrm{E}_y \|P_x - P_y\|_1$ is the same for every $x$. Thus, it is enough to fix $x = \bar{0} = (0, \ldots, 0)$ and to bound $\mathrm{E}_z \|P_{\bar{0}} - P_z\|_1$, where $z = (z_1, \ldots, z_n) \in [-1, 1]^n$ is such that each $z_i$ is chosen (independently) as follows: with probability $1/2$, $z_i = 0$, with probability $1/4$, $z_i = 1$, and with probability $1/4$, $z_i = -1$.

$$(\mathrm{E}_z \|P_{\bar{0}} - P_z\|_1)^2 = \left( \mathrm{E}_z \sum_{e \in E^n} |P_{\bar{0}}(e) - P_z(e)| \right)^2 = \left( \mathrm{E}_z \sum_{e \in E^n} P_z(e) \cdot \left| \frac{P_{\bar{0}}(e)}{P_z(e)} - 1 \right| \right)^2$$

By Jensen's inequality,

$$\leq \mathrm{E}_z \sum_{e \in E^n} P_z(e) \cdot \left( \frac{P_{\bar{0}}(e)}{P_z(e)} - 1 \right)^2 = \mathrm{E}_z \sum_{e \in E^n} \left( P_z(e) - 2P_{\bar{0}}(e) + \frac{P_{\bar{0}}(e)^2}{P_z(e)} \right)$$

By the fact that $P_{\bar{0}}, P_z$ are probability distributions,

$$= 1 - 2 + \mathrm{E}_z \sum_{e \in E^n} \frac{P_{\bar{0}}(e)^2}{P_z(e)} = -1 + \mathrm{E}_{z_1,\ldots,z_n} \sum_{e_1,\ldots,e_n} \prod_{i=1}^{n} \frac{f(e_i)^2}{f(e_i - z_i)}$$

$$= -1 + \prod_{i=1}^{n} \left( \mathrm{E}_{z_i} \sum_{e_i} \frac{f(e_i)^2}{f(e_i - z_i)} \right) = -1 + \prod_{i=1}^{n} \left( \sum_{e_i} \frac{1}{2} \cdot \frac{f(e_i)^2}{f(e_i)} + \frac{1}{4} \cdot \frac{f(e_i)^2}{f(e_i + 1)} + \frac{1}{4} \cdot \frac{f(e_i)^2}{f(e_i - 1)} \right)$$

By the fact that $f$ is a probability distribution and by Lemma 3.1,

$$= -1 + \prod_{i=1}^{n} \left(1 + O(1/m^2)\right) = O(1/m^2) \cdot O(n) = (1/m^2) \cdot O(n)$$

Thus,

$$\mathrm{E}_{x,y} \|P_x - P_y\|_1 = \mathrm{E}_z \|P_{\bar{0}} - P_z\|_1 \leq (1/m) \cdot O(\sqrt{n})$$

□

Assume without loss of generality that $n < \alpha \cdot m^2$, for a small enough constant $\alpha > 0$ (otherwise, $(1/m) \cdot \sqrt{n} \geq \Omega(1)$, and the theorem holds trivially).

In [Hol07], Holenstein proved the following lemma[2]: Let $W$ be a finite set. Assume that Alice knows a distribution $P_A : W \to \mathbb{R}$ and Bob knows a distribution $P_B : W \to \mathbb{R}$, such that, $\|P_A - P_B\|_1 \leq \delta$. Then, using a shared random string, Alice can choose $w_A \in W$ distributed according to $P_A$, and Bob can choose $w_B \in W$ distributed according to $P_B$, such that, $w_A = w_B$ with probability of at least $1 - O(\delta)$.

(Roughly speaking, this is done as follows: Alice and Bob interpret the shared random string as a sequence of pairs $(w_j, r_j)$, where $w_j \in W$ is a uniformly distributed random element and $0 \leq r_j \leq 1$ is a uniformly distributed real number between 0 and 1. Alice chooses $w_A$ to be the first $w_j$ such that $r_j \leq P_A(w_j)$, and Bob chooses $w_B$ to be the first $w_j$ such that $r_j \leq P_B(w_j)$).

In our case, the first player knows $x$ and hence $P_x$, and the second player knows $y$ and hence $P_y$. By Holenstein's lemma and by Lemma 4.1, the first player can choose $e = (e_1, \ldots, e_n) \in E^n$ distributed according to $P_x$, and the second player can choose $e' = (e'_1, \ldots, e'_n) \in E^n$ distributed according to $P_y$, such that, $e = e'$ with probability of at least $1 - (1/m) \cdot O(\sqrt{n})$, (where the probability is taken over $x, y$ and over the shared random string).

By property 2 of Lemma 3.1 and by the union bound, the probability that for some $i$ the edge $e_i$ touches $x_i$ is at most $O(1/m)$ (which is negligible). Thus, with probability of at least $1 - (1/m) \cdot O(\sqrt{n})$, both players got the same $e = (e_1, \ldots, e_n) \in E^n$, such that, for every $i$, the edge $e_i$ doesn't touch the node $x_i$. Given such $(e_1, \ldots, e_n)$, the two players can easily give answers $a(x), b(y)$ such that $\bar{V}(x, y, a(x), b(y))$ holds. This is done as follows.

For every $i$, let $C_i : U \to \{0, 1\}$ be the coloring that colors the two nodes that touch $e_i$ by 0 and all other nodes by 0,1 alternately, so that every edge except $e_i$ is 2-colored.

[2]Variants of this lemma were previously proved by Broder [Bro97] and by Kleinberg and Tardos [KT99]

For every coordinate $i$, both players will act according to $C_i$. Formally, $a_i(x) = C_i(x_i)$ and $b_i(y) = C_i(y_i)$. Since no node $x_i$ touches the corresponding edge $e_i$, $\bar{V}(x, y, a(x), b(y))$ holds.

Thus, $\bar{V}(x, y, a(x), b(y))$ holds with probability of at least $1 - (1/m) \cdot O(\sqrt{n})$.


# Acknowledgement

I am grateful to Guy Kindler, Ricky Rosen and Avi Wigderson for many helpful conversations.


# References


[AK08] Noga Alon, Boaz Klartag. Economical toric spines via Cheeger's Inequality. Manuscript 2008

[AS08] Kooshiar Azimian, Mario Szegedy. Parallel Repetition of the Odd Cycle Game. LATIN 2008: 676-686

[Bro97] Andrei Broder. On the Resemblance and Containment of Documents. In *Proc. of Compression and Complexity of Sequences*, 21-29, 1997

[BHHRRS08] Boaz Barak, Moritz Hardt, Ishay Haviv, Anup Rao, Oded Regev, David Steurer. Rounding Parallel Repetitions of Unique Games. FOCS 2008

[CHTW04] Richard Cleve, Peter Hoyer, Benjamin Toner, John Watrous. Consequences and Limits of Nonlocal Strategies. CCC 2004: 236-249

[FKO07] Uriel Feige, Guy Kindler, Ryan O'Donnell. Understanding Parallel Repetition Requires Understanding Foams. CCC 2007: 179-192

[FV96] Uriel Feige, Oleg Verbitsky: Error Reduction by Parallel Repetition - A Negative Result. *Combinatorica* 22(4): 461-478 (2002) (preliminary version in CCC 1996)

[Hol07] Thomas Holenstein. Parallel Repetition: Simplifications and the No-Signaling Case. STOC 2007: 411-419

[Kho02] Subhash Khot. On The Power Of Unique 2-Prover 1-Round Games. STOC 2002: 767-775

[KKMO04] Subhash Khot, Guy Kindler, Elchanan Mossel, Ryan O'Donnell. Optimal Inapproximability Results for MAX-CUT and Other 2-Variable CSPs?. *SIAM J. Comput.* 37(1): 319-357 (2007) (preliminary version in FOCS 2004)

[KORW08] Guy Kindler, Ryan O'Donnell, Anup Rao and Avi Wigderson. Rounding Schemes and Cubical Tilings with Sphere-Like Surface Area. FOCS 2008

[KT99] Jon Kleinberg, Eva Tardos. Approximation Algorithms for Classification Problems with Pairwise Relationships: Metric Labeling and Markov Random Fields. *J. ACM* 49(5): 616-639 (2002) (preliminary version in STOC 2009)

[Rao07] Anup Rao. Parallel Repetition in Projection Games and a Concentration Bound. STOC 2008: 1-10

[R95] Ran Raz. A Parallel Repetition Theorem. *SIAM J. Comput.* 27(3): 763-803 (1998) (preliminary version in STOC 1995)

[SS07] Muli Safra, Oded Schwartz. On Parallel-Repetition, Unique-Game and Max-Cut. Manuscript 2007