Towards the parallel repetition conjecture¹

Oleg Verbitsky

Department of Mathematical Logic, Mechanical and Mathematical Faculty,
Moscow State University, Moscow, 119899 Russia

Abstract

We consider the behavior of the error probability of a two-prover one-round interactive protocol repeated \( n \) times in parallel. We point out the connection of this problem with the density form of the Hales–Jewett theorem in Ramsey theory. This allows us to show that the error probability converges to 0 as \( n \to \infty \).

1. Introduction

We consider a two-person cooperative game \( G \) of incomplete information defined as follows. Let \( X, Y, S, T \) be finite sets. Let \( \psi \) be a predicate on \( X \times Y \times S \times T \). A pair \( (x, y) \) is chosen randomly and uniformly from a set \( Q \subseteq X \times Y \). The element \( x \) is revealed to Player 1, the element \( y \) is revealed to Player 2. Players 1 and 2 reply with \( f(x) \in S \) and \( h(y) \in T \) in accordance with their strategies \( f : X \to S \) and \( h : Y \to T \). If \( \phi(x, y, f(x), h(y)) = 1 \), then both players win; otherwise, they lose. The objective of Players 1 and 2 is to maximize collectively the winning probability (taken over the uniform distribution of \( (x, y) \) on \( Q \)). The winning probability for the optimal players' strategies is denoted by \( \omega(G) \). So,

\[
\omega(G) = \max_{f, h} \mathbb{P}[\phi(x, y, f(x), h(y)) = 1].
\]

We call the game \( G \) nontrivial if \( \omega(G) \neq 1 \). If \( Q = X \times Y \), the game \( G \) is called a free game.

We define an \( n \)-product game \( G^n \) as the execution of \( n \) independent copies of \( G \) in parallel. More formally, a collection \( ((x_1, y_1), \ldots, (x_n, y_n)) \) is chosen at random from \( Q^n \). Players 1 and 2 each are supplied with \( n \)-vectors \( \bar{x} = (x_1, \ldots, x_n) \) and \( \bar{y} = (y_1, \ldots, y_n) \), and reply with \( n \)-vectors \( F(\bar{x}) = (f_1(\bar{x}), \ldots, f_n(\bar{x})) \) and \( H(\bar{y}) = (h_1(\bar{y}), \ldots, h_n(\bar{y})) \), respectively. Now the players win in the case \( \bigwedge_{i=1}^n \phi(x_i, y_i, f_i(\bar{x}), h_i(\bar{y})) = 1 \), and

¹ Research supported in part by Grant No. MQT 000 from the International Science Foundation. A preliminary version of the paper appeared in Structure in Complexity Theory Conference'94.
we define

\[ \omega(G^n) = \max_{F,H} \mathbb{P} \left[ \bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(x), h_i(y)) = 1 \right] . \]

The only presently known relations between \( \omega(G) \) and \( \omega(G^n) \) are

\[ (\omega(G))^n \leq \omega(G^n) \leq \omega(G). \]

Players 1 and 2 achieve the winning probability \( (\omega(G))^n \) in the game \( G^n \) by playing each parallel copy of \( G \) independently from the others, using the optimal strategies \( f \) and \( h \) of \( G \). The second inequality is true because, given the optimal in \( G^n \) strategies \( F \) and \( H \), in the game \( G \) the players can use the strategies \( f_1(-, \hat{x}_2, \ldots, \hat{x}_n) \) and \( h_1(-, \hat{y}_2, \ldots, \hat{y}_n) \) where the elements \( \hat{x}_2, \ldots, \hat{x}_n, \hat{y}_2, \ldots, \hat{y}_n \) are chosen in the best way and fixed.

In this note we are interested in the behavior of \( \omega(G^n) \) for increasing \( n \). This question arose in the research on multi-prover interactive proofs originated in [2].

A multi-prover interactive proof system is a probabilistic computational model for recognizing a language \( L \), where the polynomial-time verifier, interacting separately with several computationally unlimited provers, must determine whether or not an input \( w \) belongs to \( L \). The game \( G \) described above is essentially the simplest but still powerful two-prover interactive protocol on a fixed input \( w \). The value \( \omega(G) \) corresponds to the probability of the verifier making the erroneous decision. The sequential repetition of the protocol \( n \) times reduces the error probability to \( (\omega(G))^n \) but increases the number of interactions. Fortnow et al. [8] suggested to decrease the error probability by running the interactive protocol independently \( n \) times in parallel. They supposed that the value \( \omega(G^n) \) decreases quite rapidly, similarly to \( (\omega(G))^n \). However, later Fortnow [7] presented a game \( G \) for which \( \omega(G^2) > (\omega(G))^2 \). Feige [5] improved this by giving an example of the nontrivial game \( G \) with \( \omega(G^2) = \omega(G) \).

Before this paper, it was unknown even whether for any \( G \) there exists \( n \) such that \( \omega(G^n) < \omega(G) \) (see the discussion in [6]). We prove the following assertion.

**If \( G \) is nontrivial game, then \( \omega(G^n) \to 0 \) for \( n \to \infty \).**

This answers affirmatively the question posed by Feige [5]. For free games such a result was established by Cai et al. [4]. Moreover, they proved that for a free game \( G \) the value \( \omega(G^n) \) converges to 0 exponentially fast in \( n \). Their estimate on \( \omega(G^n) \) was improved by Lapidot and Shamir [11] and Peleg [12] in the case \( |X| = |Y| = 2 \) and by Feige [5] and Alon [1] in the general case.

Some examples of nonfree games with exponentially decreasing \( \omega(G^n) \) were used in [3]. Feige and Lovász [6] obtained the exponentially small upper bounds on \( \omega(G^n) \) for the class of (nonfree) games with the uniqueness property defined in [4]. A game \( G \) has the uniqueness property if for all \( x, y, s \) there is at most one \( t \) satisfying \( \phi(x, y, s, t) \), and for all \( x, y, t \) there is at most one \( s \) satisfying \( \phi(x, y, s, t) \).

The analysis of the case of free games was based on extremal properties of bipartite graphs. Feige and Lovász’s approach relies on quadratic programming. In this note
we point out the connection between the problem under discussion and one subject well-known in Ramsey theory. We apply the result of Furstenberg and Katznelson [9] which is the density form of the Hales-Jewett theorem (see [10]).

Furstenberg and Katznelson employ the methods of ergodic theory, that do not yield effective upper bounds (see the discussion in [13]). So, the question about the rate of decrease of \( \omega(G^n) \) remains open. Feige and Lovász [6] formulated the parallel repetition conjecture which says that the rate is exponential for any nontrivial \( G \).

2. The result

We begin with formal definitions and then cite the needed results from Ramsey theory.

We say that \( G = \langle \phi, Q \subseteq X \times Y, S, T \rangle \) is a game if \( X, Y, S \) and \( T \) are finite sets and

\[
\phi: Q \times S \times T \to \{0, 1\}
\]

is a predicate. We regard arbitrary functions \( f : X \to S \) and \( h : Y \to T \) as strategies (of Players 1 and 2). We define a value of the game \( G \) by

\[
\omega(G) = \max_{f,h} \mathbb{P}[\phi(x, y, f(x), h(y)) = 1],
\]

where the probability is taken over all randomly and uniformly chosen pairs \((x, y) \in Q\). \( G \) is nontrivial if \( \omega(G) \neq 1 \).

Given \( G \), we define the product game \( G^n \) to be the game \( \langle \phi^n, Q^n, S^n, T^n \rangle \) (more accurately, the Cartesian power \( Q^n \) is thought of as a subset of \( X^n \times Y^n \) by identifying a collection \((x_1, y_1), \ldots, (x_n, y_n)\) with a pair \((x_1, \ldots, x_n), (y_1, \ldots, y_n)\), where

\[
\phi^n(x, y, s, t) = \left( \prod_{i=1}^{n} \phi(x_i, y_i, s_i, t_i) \right).
\]

Here \( \vec{v} \) is an \( n \)-vector \((v_1, \ldots, v_n)\). For players' strategies \( F : X^n \to S^n \) and \( H : Y^n \to T^n \), we designate \( F(\vec{x}) = (f_1(\vec{x}), \ldots, f_n(\vec{x})) \) and \( H(\vec{y}) = (h_1(\vec{y}), \ldots, h_n(\vec{y})) \).

Now we turn to some notions of Ramsey theory. Let \( A = \{a_1, \ldots, a_k\} \) be a finite set and \( z \) be a variable that can be replaced with any element of \( A \). Let \( u(z) \) be an \( n \)-vector from \((A \cup \{z\})^n\) with at least one component \( z \). Then the set

\[
L = \{u(a_1), \ldots, u(a_k)\}
\]

is called a (combinatorial) line in \( A^n \). In other words, \( L \) consists of \( k \) distinct elements of \( A^n \) which, treated as rows, can be formed into a \( k \times n \) matrix whose columns are either \((a_1, a_2, \ldots, a_j)^T\) for some \( j \leq k \) or \((a_1, a_2, \ldots, a_k)^T\).

The Hales–Jewett theorem says that for any \( k \) and \( r \) there is \( N(k, r) \) such that for \( n \geq N(k, r) \) there exists a monochromatic line in any \( r \)-coloring of the set \( A^n \) (see [10]).
Denote by $R_k(n)$ the maximal cardinality of the set $W \subseteq A^n$ without lines. Furstenberg and Katznelson [9] proved that for any fixed $k$,

$$R_k(n) = o(k^n).$$

The result of this paper is the following

**Theorem 2.1.** For any nontrivial game $G = (\phi, Q \subseteq X \times Y, S, T)$,

$$o(G^n) \leq R_{|Q|}(n)/|Q|^n.$$

Applying the Furstenberg and Katznelson theorem, we have

**Corollary 2.1.** For any nontrivial game $G$, $o(G^n) \to 0$ as $n \to \infty$.

**Proof of Theorem 2.1.** Let $Q = \{a_1, \ldots, a_k\}$, where $a_j = (x(a_j), y(a_j))$, $x(a_j) \in X$, $y(a_j) \in Y$ for $j \leq k$. Fix the strategies $F$ and $H$ optimal in $G^n$. Define $W \subseteq Q^n$ to be the set of successes of $F$ and $H$ in $G^n$, that is,

$$W = \left\{ (z_1, \ldots, z_n) \in Q^n : \bigwedge_{i=1}^n \phi(x(z_i), y(z_i), f_i(x(z_1), \ldots, x(z_n)), h_i(y(z_1), \ldots, y(z_n))) = 1 \right\}.$$

So, $o(G^n) = |W|/k^n$.

To apply the result of Furstenberg and Katznelson, it suffices to show that $W$ does not contain any of the lines in $Q^n$. Suppose, to the contrary, that there is the line $L = \{l_1, \ldots, l_k\} \subseteq W$. Our goal is to prove that in this case $G$ should be trivial.

Let $C = C_1 \ldots C_n$ be a $k \times n$ matrix whose $k$ rows are $\tilde{b}_1, \ldots, \tilde{b}_k$ and $n$ columns $C_1, \ldots, C_n$ each are either $(a_j, a_j, \ldots, a_j)^T$ for some $j \leq k$ or $(a_1, a_2, \ldots, a_k)^T$ (see Fig. 1). There exists at least one column $C_i = (a_1, a_2, \ldots, a_k)^T$. We suppose $L$ to be ordered so that the row $\tilde{b}_j$ intersects the column $C_i$ at the matrix element $a_j$. Now let us expand $C$ to the $2k \times n$ matrix $D$ by replacing each matrix element $a_j$ with the column $x(a_j)/y(a_j)$. Denote the rows of $D$ by $\tilde{x}_1, \tilde{y}_1, \ldots, \tilde{x}_k, \tilde{y}_k$, where $\tilde{x}_j \in X^n$ and $\tilde{y}_j \in Y^n$ are the result of splitting the row $\tilde{b}_j$ of the matrix $C$.

Fig. 1. An example. The rows of this matrix constitute a line in the set $\{a_1, a_2, a_3\}^6$ generated by $u(z) = (a_2, a_1, a_1, a_2, a_3)$. 

<table>
<thead>
<tr>
<th>$a_2$</th>
<th>$a_1$</th>
<th>$a_1$</th>
<th>$a_2$</th>
<th>$a_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_2$</td>
<td>$a_2$</td>
<td>$a_1$</td>
<td>$a_2$</td>
<td>$a_3$</td>
</tr>
<tr>
<td>$a_2$</td>
<td>$a_3$</td>
<td>$a_1$</td>
<td>$a_2$</td>
<td>$a_3$</td>
</tr>
</tbody>
</table>
Fig. 2. This fragment of the matrix D illustrates the correctness of the definition of strategy $f$.

Define the strategy $f$ in the game $G$ by $f(x) = f_1(x_m)$ with $m$ being chosen so that $x = x(a_m)$. The definition is correct since for distinct such $m$ and $m'$ it holds $x_m = x_{m'}$.

Similarly, we define $h(y)$ to be equal to $h_1(y_{m'})$, where $y(a_{m'}) = y$. The defined strategies $f$ and $h$ turn out to be perfect. Indeed, for arbitrary $a_j = (x, y) \in Q$ we have

$$\phi(x, y, f(x), h(y)) = \phi(x(a_j), y(a_j), f_1(x), h_1(y)) = 1,$$

since $b_j \in W$ and, in particular, $F$ and $H$ win in the $l$th copy of $G$.

Thus, our assumption that $W$ contains a line yields a contradiction.

Remark 2.1. Theorem 2.1 admits a formal improvement. Namely, for a given game $G = (\phi, Q \subseteq X \times Y, S, T)$, we can extend the definition of the combinatorial line as follows. We call an arbitrary (not necessarily injective) mapping $\sigma: Q \rightarrow Q$ incidence-preserving if $x(a_j) = x(a_{j'})$ implies $x(\sigma(a_j)) = x(\sigma(a_{j'}))$ and, similarly, $y(a_j) = y(a_{j'})$ implies $y(\sigma(a_j)) = y(\sigma(a_{j'}))$. Define the set of columns $E = \{(\sigma(a_1), \ldots, \sigma(a_k))^T : \sigma \text{ is incidence-preserving}\}$. Call the set $L = \{b_1, \ldots, b_k\} \subseteq Q^n$ to be a $Q$-shaped line if the matrix consisting of the rows $b_1, \ldots, b_k$ has columns only from $E$ and there is at least one column $(a_1, \ldots, a_k)^T$.

Clearly, any combinatorial line is a $Q$-shaped line. Theorem 2.1 holds true if we use the notion of $Q$-shaped line instead of the usual notion of line. The same proof applies.

Acknowledgements

I would like to thank Uriel Feige for drawing my attention to the discussed problem and Alexander Razborov for his interest and encouragement.
References


