PLAYING GAMES OF INCOMPLETE INFORMATION

Jin-yi Cai
Anne Condon
Richard J. Lipton

CS-TR-238-89

December 1989

Playing Games of Incomplete Information

Jin-yi Cai[*]
Department of Computer Science
Princeton University
Princeton, New Jersey 08544

Anne Condon [†]
Computer Science Department
University of Wisconsin-Madison

Richard J. Lipton[‡]
Department of Computer Science
Princeton University
Princeton, New Jersey 08544

1 Introduction

We study two-person games of cooperation and multi-prover interactive proof systems. We first consider a two person game G, which we call a *free game*, defined as follows. A Boolean function ϕ_G is given. Player I and II each pick a random number i and j in private, where $1 \leq i, j \leq s$, and then each chooses a private number $f(i)$ and $g(j)$, $1 \leq f(i), g(j) \leq s$. If $\phi_G(i, j, f(i), g(j)) = 1$, then both players win, otherwise they lose. The objective of both players is to win collectively. We ask whether, if such a game is played n times in parallel, the probability of winning *all* the games decays exponentially in n. This question was posed in a more general context by Fortnow [4], which we discuss soon.

Formally we define the nth product game G^n as the following two person game. Player I and II each pick a vector of independent random numbers $\bar{i} = (i_1, \ldots, i_n)$ and $\bar{j} = (j_1, \ldots, j_n)$ in private, $1 \leq i_k, j_k \leq s$, and then each chooses a private sequence of numbers $f_1(\bar{i}), \ldots, f_n(\bar{i}), g_1(\bar{j}), \ldots, g_n(\bar{j})$. The goal for both players is to ensure $\bigwedge_{k=1}^n \phi_G(i_k, j_k, f_k(\bar{i}), g_k(\bar{j})) = 1$. We define the *winning probability* of the game G to be $\max_{f,g} \Pr[\phi_G(i, j, f(i), g(j)) = 1]$, where the probability is taken over all randomly and uniformly chosen i, j in the range $1, \ldots, s$, and we denote it by $w(G)$. The game G is called nontrivial if its winning probability is neither 0 nor 1. We shall only consider nontrivial free games. Similarly, the winning probability $w(G^n)$ of the product game G^n is defined to be $\max_{f_1,\ldots,f_n,g_1,\ldots,g_n} \Pr[\wedge_{k=1}^n \phi_G(i_k, j_k, f_k(\bar{i}), g_k(\bar{j})) = 1]$.

[*] Research supported by NSF grant CCR-8709818.
[†] Work supported by NSF grant number DCR-8402565
[‡] Research supported by DARPA and ONR contracts N00014-85-C-0456 and N00014-85-K-0465

Intuitively, we might first expect that $w(G^n)$ is $w(G)^n$; since all n instances of game G are drawn independently, and if the players play all instances independently, the winning probability of the n-product game is $w(G)^n$. However, Fortnow [4] showed that the answer is not so simple; he gave an example of a free game G for which $w(G^2) > (w(G))^2$. He thus demonstrated that by using strategies that depend on *all* the instances of the game G, the players can increase their chance of winning the product game G^n.

Before this work, it was unknown even if $w(G^n) \to 0$ as $n \to \infty$. The first result of this paper is that the winning probability of the product game G^n converges to 0 exponentially fast as $n \to \infty$.

Theorem (2.1) *If G is a non-trivial free game, then there exists a $q < 1 - e^{-3s}/2$ and a universal constant c_0, such that the winning probability of G^n is at most $c_0 q^n$.*

We can generalize this result to another class of games, defined as follows. Let ϕ_G be a Boolean function as before, and let L be a nonempty subset of $\{1, \ldots, s\} \times \{1, \ldots, s\}$. L is the set of *legal* instances of the game. A pair (i, j) is chosen randomly and uniformly from L; i is given to player I and j is given to player II. As before, the players choose numbers $f(i)$ and $g(j)$; and the players win if $\phi_G(i, j, f(i), g(j)) = 1$. We similarly define the winning probability of the game $w(G)$, and call a game nontrivial if $0 < w(G) < 1$. Note that free games are a special case of these games, where there is no dependency between i and j. We refer to these games simply as *games* in this paper. Then

Theorem (2.2) *If G is a non-trivial game, then there exists a $q < 1 - e^{-3s}/2$ and a universal constant c_0, such that the winning probability of G^n is at most $c_0 q^n$.*

Our study of games was motivated by recent work on multi-prover interactive proof systems (MIP's), introduced by Ben-Or et al. [2]. These are generalizations of the interactive proof systems (IPS's) of Goldwasser, Micali and Rackoff [6] and Babai [1]. Roughly, an interactive proof system for a language L is a protocol between a prover P and a verifier V. The pair shares an input; the prover must be able to convince the verifier to accept an input if and only if it is in L. We only consider interactive proofs where the verifier is probabilistic and is polynomially time bounded. In a multi-prover system (MIP), the verifier interacts with many provers; the provers cannot communicate with each other during the proof. The protocol between the verifier and the provers consists of a number of *rounds*; in each round the verifier sends a message to each prover in turn and receives a response. Because the provers cannot communicate with each other, the response of any prover can only depend on the messages it has received from the verifier so far, and not on the messages sent to other provers.

We restrict our attention in this paper to the case that the verifier interacts with two provers, P_1 and P_2. A language L is accepted by a MIP (P_1, P_2, V) with error probability $\epsilon(n)$ if

1. for all $x \in L$, $|x| = n$, (P_1, P_2, V) accepts x with probability at least $1 - \epsilon(n)$; and
2. for all $x \notin L$,$|x| = n$, and any provers P_1^*, P_2^*, (P_1^*, P_2^*, V) accepts x with probability at most $\epsilon(n)$.

Fortnow, Rompel and Sipser [5] considered the question: are two provers more powerful than one? To address this question, they considered the number of rounds of a protocol and asked whether any language accepted by an unbounded round IPS has a constant round MIP. Since an IPS can run for polynomial time, the number of rounds, or interactions between the verifier and prover can be polynomial in the input size. Results of Babai [1] and Goldwasser and Sipser [7] show that if the number of rounds of a protocol is bounded by a constant independent of the input size, the number of rounds can be collapsed to two. However, it is an open problem whether unbounded round IPS's are equivalent to constant round IPS's. Therefore, a proof that any language accepted by an unbounded round IPS has a constant round MIP would be of interest.

Fortnow et al. showed how to simulate any IPS by a 1-round MIP with the following property.

1. if x is accepted by the IPS, $|x| = n$, then the probability x is accepted by the MIP is $\geq 1 - 1/2^n$; and
2. if x is rejected by the IPS, $|x| = n$, then the probability x is accepted by the MIP is $\leq 1 - 1/p(n)$, for some polynomial p.

We call a 1-round MIP protocol that simulates an IPS using the method of Fortnow at al. an *IPS-simulation* protocol.

Fortnow et al. claimed that an IPS-simulation protocol could be run in parallel a polynomial number of times in the length of the input, to obtain a 1-round MIP accepting L with error probability ϵ, for any constant ϵ. Intuitively this seems reasonable, since each of the games played in parallel is chosen independently. However, Fortnow [4] later showed that although the verifier chooses each game independently, it cannot be assumed that the provers play the games independently.

The protocol of Fortnow et al. on a fixed input is exactly a game of the type described above. Hence, the question of whether any IPS can be simulated by a constant round, 2-prover MIP can be reduced to the following problem: Is there some polynomial p' and a constant λ, $0 < \lambda < 1$, such that for any nontrivial game G the winning probability of G^n is at most λ, for $n = p'(\frac{1}{1-w(G)})$. Unfortunately, although Theorem 2.2 implies that the winning probability of G decays exponentially as $n \rightarrow \infty$, it is not strong enough to resolve this problem.

Our next result exploits a special property of IPS-simulation protocols to solve this problem in the case of free games. In the framework of the games described above, the property is roughly as follows. Once i and j are fixed and the response of one player is fixed, there is a limit on the number of possible responses of the other player that satisfy ϕ_G. More precisely, we say G is *(l, l')-limited* if

1. given any i, j, k, $|\{k' \mid \phi_G(i, j, k, k') = 1\}| \leq l$; and
2. given any i, j, k', $|\{k \mid \phi_G(i, j, k, k') = 1\}| \leq l'$.

Then the IPS-simulation protocols of Fortnow et al. [5] are $(1, 2)$-limited. We will first develop the idea in the special case of $(1, 1)$-limited free games, and then consider the more general $(1, 2)$-limited free games. Our result for $(1, 2)$-limited free games is the following:

Theorem (4.1) *Let G be a non-trivial, (1,2)-limited free game. Let $w(G) = 1-\epsilon$. Then if $n = \lceil 1/\epsilon \rceil$, $w(G^n) \leq 11/12$.*

We conjecture that this theorem can be generalized to non-free games. Finally, we note that if this conjecture is true, then it follows that given any constant ϵ, any language accepted by an (unbounded round) IPS has a constant round 2-prover MIP that has error probability ϵ. This is because the IPS-simulation protocol can be run a polynomial number of times in parallel to reduce the error probability to 11/12. Then for any constant k, this parallel protocol can be repeated sequentially a k times to reduce the error probability to $(11/12)^k$.

2 Results on the Convergence of Free and General Games

In this section we prove Theorem 2.1 and related results.

We begin by giving precise definitions of a game. We say $G = \langle \phi, L \subseteq X \times Y, S, T \rangle$ is a *game* if each set X, Y, S, T is finite, $L \neq \emptyset$, and

$$\phi : L \times S \times T \to \{0, 1\}.$$

Without loss of generality, we assume that X, Y, S, T all equal $\{1, \ldots, s\}$. We say G is a *free game* if $L = X \times Y$. We define the winning probability of G to be $\max_{f,g} \Pr[\phi(x, y, f(x), g(y)) = 1]$, where the probability is taken over all randomly and uniformly chosen pairs $(x, y) \in L$. We call f and g the strategies of Player I and II respectively. G is *non-trivial* if $w(G)$ is neither 0 nor 1. This implies $s > 1$.

We define the *product game* G^n of G to be the game $\langle \phi^n, L^n, S^n, T^n \rangle$, where

$$\phi^n(\bar{x}, \bar{y}, f(\bar{x}), g(\bar{y})) = \bigwedge_{i=1}^{n} \phi(x_i, y_i, f_i(\bar{x}), g_i(\bar{y})).$$

Here $\bar{v}$ is the n-vector $(v_1, \ldots, v_n)$ and $f(\bar{x}), g(\bar{y})$ are the n-vectors $(f_1(\bar{x}), \ldots, f_n(\bar{x}))$ and $(g_1(\bar{y}), \ldots, g_n(\bar{y}))$, respectively.

The probability that the players win all copies of the n-product game of G is at least $w(G)^n$. This is because if f, g are optimal strategies of players I and II of G respectively, that is, $\phi(x, y, f(x), g(y)) = w(G)$, then when the players use strategies f and g in parallel on each copy, the probability of winning is $\prod_{i=1}^{n} \phi(x_i, y_i, f(x_i), g(y_i)) = w(G)^n$, since the x_i and y_i are all chosen independently and randomly. Thus for any game G, $w(G^n) \geq w(G)^n$; a natural question is whether $w(G^n) = w(G)^n$. Fortnow [4] showed that the answer to this question is no, by constructing the following free game G for which $w(G) = 1/2$ but $w(G^2) = 3/8 > (1/2)^2$. Fortnow's game G is defined by setting $X = Y = S = T = \{0, 1\}$ and defining ϕ by

$$\phi(x, y, f(x), g(y)) = [(x \vee f(x)) \neq (y \vee g(y))].$$

The winning probability of this game is $1/2$; an example of a pair of optimal strategies of the players is $f(x) = x$, $g(y) = y$. On these strategies, the players win when one receives a 0 and the other receives a 1, which occurs with probability $1/2$. Next consider the product game G^2. In this game, player I receives bits x_1 and x_2, player II receives bits y_1 and y_2; and the goal of the players is to ensure that

$$((x_1 \vee f_1(x_1, x_2)) \neq (y_1 \vee g_1(y_1, y_2))) \wedge ((x_2 \vee f_2(x_1, x_2)) \neq (y_2 \vee g_2(y_1, y_2))).$$

Suppose the players use the following strategy: $f(x_1, x_2) = (0, 0)$ if $x_1 = x_2 = 0$; otherwise $f(x_1, x_2) = (1, 1)$. Symmetrically, $g(y_1, y_2) = f(y_1, y_2)$. This pair of strategies guarantees that the players win with probability $3/8$: when $x_1 = x_2 = 0$, the players win when y_1 and y_2 are not both 0; and by symmetry when $y_1 = y_2 = 0$, the players win when x_1 and x_2 are not both 0. Hence the players win on 6 of the 16 possible random choices for x_1, x_2, y_1, y_2.

Fortnow also observed that the winning probability of the product game G^n is at most $(3/4)^n$, since the players can never win if $x_i = y_i = 1$ for some i. In general though, such an argument is not sufficient to show that $w(G^n) \to 0$ as $n \to \infty$, since there may not be an instance of the game on which the players *always* lose. For example, by modifying Fortnow's game so that the players automatically win when $x = y = 1$, that is, letting $\phi(x, y, f(x), g(y)) = ((x \vee f(x)) \neq (y \vee g(y))) \vee (x \wedge y)$, we obtain a non-trivial game for which this argument fails. Our first theorem uses a result of Zarankiewicz [3] to show that if a free game G is non-trivial, then the winning probability of the n-product game converges to 0 exponentially fast as $n \to \infty$.

Theorem 2.1 *If G is a non-trivial free game, then there exists a $q < 1 - e^{-3s}/2$, and a universal constant c_0, such that $w(G^n) < c_0 q^n$.*

Proof: Suppose a pair of strategies f, g for the two players are given. Let $N = s^n$, the size of the sample space in the product game. Define a bipartite graph (X, Y, E), where X and Y consist of all inputs to each player, thus $|X| = |Y| = N$. An edge $e(x, y)$ exists between x and y *iff* $\bigwedge_{k=1}^{n} \phi_G(x_k, y_k, f_k(x_1, \ldots, x_n), g_k(y_1, \ldots, y_n))$, where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$. We show that $|E| = O(N^{2-\lambda(s)})$, for some $\lambda(s) > 0$. This clearly implies a bound on the probability of winning the product game.

Consider the set of all pairs of (ordered) s-tuples from X and Y, $S = \{((x^1, \ldots . x^s), (y^1, \ldots, y^s)) | x^i \in X, y^i \in Y\}$. Given any such pair $((x^1, \ldots . x^s), (y^1, \ldots, y^s)) \in S$ and any k, $1 \le k \le n$, consider the pair of s-tuples formed by "the kth coordinates", $((x_k^1, \ldots . x_k^s), (y_k^1, \ldots, y_k^s))$. The number of such pairs where both entries are permutations of 1 to s is $s!^2$. Thus the number of such pairs where at least one entry is not a permutation of 1 to s is $s^{2s} - s!^2$. Now consider the set of the pairs $((x^1, \ldots . x^s), (y^1, \ldots, y^s)) \in S$ so that for all $k, 1 \le k \le n,$ at least one of $(x_k^1, \ldots . x_k^s)$ or $(y_k^1, \ldots, y_k^s)$ is not a permutation of 1 to s. This set has cardinality $(s^{2s} - s!^2)^n$. Hence, the set of the pairs $((x^1, \ldots . x^s), (y^1, \ldots, y^s)) \in S$ such that there exists $k, 1 \le k \le n,$ both $(x_k^1, \ldots . x_k^s)$ and $(y_k^1, \ldots, y_k^s)$ are permutations of 1 to s has cardinality $N^{2s} - (s^{2s} - s!^2)^n$. Each of these has been counted exactly $s!^2$ times in the totality of all (ordered) pairs of (unordered) set of s distinct elements from X and Y, thus the number of (ordered) pairs of (unordered) set of s distinct elements from X and Y, where, for all k "the kth coordinate tuple" $((x_k^1, \ldots . x_k^s), (y_k^1, \ldots, y_k^s))$ do not both form permutations, is

$$\begin{aligned}
& \binom{N}{s}^2 - \frac{N^{2s} - (s^{2s} - s!^2)^n}{s!^2} \\
\le & \frac{(s^{2s} - s!^2)^n}{s!^2} \\
\le & \frac{1}{s!^2}(s^{2s}(1 - \frac{1}{e^{2s}}))^n \\
= & \frac{N^{2s + \log_s(1 - \frac{1}{e^{2s}})}}{s!^2} \\
\le & \frac{N^{2s - \frac{1}{\log s \cdot e^{2s}}}}{s!^2}.
\end{aligned}$$

Let's consider the following sum

$$\sum_{A \subset X, B \subset Y, |A| = |B| = m} e(A, B) = |E| \binom{N}{m-1}^2,$$

where $e(A, B)$ denotes the number of edges between A and B, and $s \le m \le N$.

Let

$$\mathcal{M} = \{\ (A, B) \mid |A| = |B| = m \ \&\ e(A, B) \ge \frac{|E|}{2} \frac{\binom{N}{m-1}^2}{\binom{N}{m}^2}\ \}.$$

The size of $\mathcal{M}$ can be estimated as follows:

$$|E| \binom{N}{m-1}^2 \le |\mathcal{M}| m^2 + \frac{|E|}{2} \binom{N}{m-1}^2,$$

$$|\mathcal{M}| m^2 \ge \frac{|E|}{2} \binom{N}{m-1}^2.$$

Applying Zarankiewicz's Theorem [3] to the bipartite graph induced on $A \times B$ for each $(A, B) \in \mathcal{M}$, we get a complete subgraph $K_{s,s}$, provided the number of edges is at least $(s-1)^{1/s} m^{2-1/s} + \frac{s-1}{2} m$. An easy consequence is that if the number of edges $e(A, B) > 2m^{2-1/s}$, then there is a subgraph $K_{s,s}$.

Now let $\lambda = \frac{1}{\log s(1+2s^2)e^{2s}}$, and suppose $|E| \geq 2eN^{2-\lambda}$. Let $n \geq 1/\lambda s = \log s \cdot (1+2s^2) \cdot e^{2s}/s$ and $m = \lceil N^{\lambda s} \rceil$. As $N = s^n$, clearly $m \geq s$. Moreover for $(A, B) \in \mathcal{M}$, $e(A, B) \geq eN^{2-\lambda} (\frac{m}{N-m+1})^2 > 2m^{2-1/s}$. Therefore we have at least one $K_{s,s}$ for each $(A, B) \in \mathcal{M}$. Each such $K_{s,s}$ can appear in at most $\binom{N}{m-s}^2$ many pairs, thus there are at least $\frac{|\mathcal{M}|}{\binom{N}{m-s}^2}$ many $K_{s,s}$.

We have

$$\begin{aligned} \frac{|\mathcal{M}|}{\binom{N}{m-s}^2} &\geq \frac{|E|}{2m^2} \frac{\binom{N}{m-1}^2}{\binom{N}{m-s}^2} \\ &\geq eN^{2-\lambda} \frac{(N-m+1)^{2(s-1)}}{m^{2s}} \\ &= \frac{eN^{2s-\lambda}}{m^{2s}} \left(1 - \frac{m-1}{N}\right)^{2(s-1)}. \end{aligned}$$

Since $m < N^{\lambda s} + 1$,

$$\frac{1}{m^{2s}} > \frac{1}{(N^{\lambda s}+1)^{2s}} \geq \frac{1}{e^2 N^{\lambda 2s^2}},$$

as $N^{\lambda s} \geq s$.

Also, $m - 1 < N^{\lambda s}$, thus,

$$\left(1 - \frac{m-1}{N}\right)^{2(s-1)} > \left(1 - \frac{1}{N^{1-\lambda s}}\right)^{2(s-1)} = \left(1 - \frac{1}{s^{(1-\lambda s)n}}\right)^{2(s-1)}.$$

Since $(1-\lambda s)n \geq \frac{1}{\lambda s} - 1 = \frac{\log s(1+2s^2)e^{2s} - s}{s} \geq 2 \log s \cdot s \cdot e^{2s}$,

$$\begin{aligned} \left(1 - \frac{m-1}{N}\right)^{2(s-1)} &> \left(1 - \frac{1}{s^{2 \log s \cdot s \cdot e^{2s}}}\right)^{2(s-1)} \\ &> \frac{e}{s!^2}. \end{aligned}$$

Hence

$$\begin{aligned} \frac{|\mathcal{M}|}{\binom{N}{m-s}^2} &> \frac{eN^{2s-\lambda(1+2s^2)}}{e^2} \frac{e}{s!^2} \\ &= \frac{N^{2s - \frac{1}{\log s \cdot e^{2s}}}}{s!^2}. \end{aligned}$$

It follows that there are $K_{s,s}$ on some pair of (unordered) s-sets, such that, for some k, $1 \leq k \leq n$, "the kth coordinates" $((x_k^1, \ldots . x_k^s), (y_k^1, \ldots, y_k^s))$ both form permutations of 1 to s. Therefore the original game G has a perfect strategy, and is thus trivial.

Therefore, the winning probability of the product game for a nontrivial game is bounded by $2eq^n$, for $n \geq \log s(1+2s^2)e^{2s}/s$, where $q = e^{-1/(1+2s^2)e^{2s}} = 1 - \frac{1}{(1+2s^2)e^{2s}} + \cdots$, which is less than, say,

$1 - e^{-3s}/2$, for all s. Note that for $n < \log s(1+2s^2)e^{2s}/s$, q^n is bounded below by $1 - \log 2/2 > 1/2$, so that the bound $w(G^n) \leq 2eq^n$ holds for all n and s. □

For a nontrivial game G that is not free, one can easily extend ϕ to $\hat{\phi} = \phi \vee [(x,y) \notin L]$, so that the extended game $\hat{G}$ is free, and since $w(G) \leq w(\hat{G})$, and $1 - w(\hat{G}) \geq \frac{|L|}{s^2}(1 - w(G)) > 0$, $\hat{G}$ is nontrivial. Applying Theorem 2.1, we have

Theorem 2.2 *If G is a non-trivial game, then there exists a $q < 1 - e^{-3s}/2$ and a universal constant c_0, such that the winning probability of G^n is at most $c_0 q^n$.*

3 Games with the Uniqueness Property

In this section we consider games that satisfy the uniqueness property, that is, games such that for all x, y, x' there is at most one y' such that $\phi(x,y,x',y') = 1$ and for all x, y, y' there is at most one x' such that $\phi(x,y,x',y') = 1$. We need the following technical lemma.

Lemma 3.1 *Suppose $p_1, \ldots, p_s$ and $q_1, \ldots, q_s$ are nonnegative real numbers such that $\sum p_i \leq 1$ and $\sum q_i \leq 1$. Let $1/2 \leq \alpha \leq 1$. If $\sum p_i q_i > \alpha$, then for some k, $p_k > \alpha$ and $q_k > \alpha$.*

Proof: Without loss of generality suppose that $p_1 \geq p_2 \geq \ldots \geq p_s$. First note that $p_1 > \alpha$. Otherwise for all i, $p_i \leq \alpha$. Then $\sum p_i q_i \leq \alpha \sum q_i = \alpha$, contradicting the fact that $\sum p_i q_i > \alpha$.

Therefore we must show that $q_1 > \alpha$. We first argue that $\sum_{i=2}^{s} p_i q_i \leq (1-p_1)(1-q_1)$. This is because

$$\sum_{i=2}^{s} p_i q_i \leq p_2 \sum_{i=2}^{s} q_i \leq (1-p_1)(1-q_1).$$

Now, suppose to the contrary that $q_1 \leq \alpha$. Then since $p_1 > 1 - p_1$,

$$\sum p_i q_i \leq p_1 q_1 + (1-p_1)(1-q_1) \leq \alpha p_1 + (1-\alpha)(1-p_1) \leq \alpha p_1 + \alpha(1-p_1) = \alpha.$$

This contradicts the fact that $\sum p_i q_i > \alpha$. □

Theorem 3.1 *Let G be a non-trivial free game that satisfies the uniqueness property. Let $w(G) = 1 - \epsilon$. Then if $n = \lceil 1/\epsilon \rceil$, $w(G^n) \leq 7/8$.*

Proof: Let G be the game $\langle \phi, X \times Y, S, T \rangle$ and assume that $|X| = |Y| = |S| = |T| = s$. To prove the theorem, we show by induction on n that if $n \leq \lceil 1/\epsilon \rceil$, then $w(G^n) \leq (1 - (1/4)\epsilon)^n$. From this the theorem follows easily, since when $n = \lceil 1/\epsilon \rceil$, $(1 - (1/4)\epsilon)^n \leq 7/8$.

The basis case, when $n = 1$, is trivial, since $w(G) = 1 - \epsilon \leq 1 - (1/4)\epsilon$. Let $n > 1$. Fix strategies f and g of the players in game G^n that maximize $w(G^n)$. With respect to these strategies, define $w(G^n | x_1 = a, y_1 = b)$ to be the probability that the players win the game G^n, given that $x_1 = a$ and $y_1 = b$. Note that for any pair (a,b), this probability is at most $w(G^{n-1})$. Also, let H be the set of pairs (a,b) in $X \times Y$ for which $w(G^n | x_1 = a, y_1 = b) \geq (3/4)(1 - (1/4)\epsilon)^{n-1}$.

$$\begin{aligned} w(G^n) &= 1/s^2 \sum_{(a,b) \in X \times Y} w(G^n | x_1 = a, y_1 = b) \\ &\leq 1/s^2 [\sum_{(a,b) \in H} w(G^{n-1}) + \sum_{(a,b) \in (X \times Y) - H} (3/4)(1 - (1/4)\epsilon)^{n-1}] \\ &\leq \frac{(1 - (1/4)\epsilon)^{n-1}}{s^2} [\sum_{(a,b) \in H} 1 + \sum_{(a,b) \in (X \times Y) - H} (3/4)]. \end{aligned}$$

We claim that $|H| \leq (1-\epsilon)s^2$. From this the lemma follows easily, since then

$$w(G^n) \leq (1-(1/4)\epsilon)^{n-1}[(1-\epsilon)+(3/4)\epsilon] = (1-(1/4)\epsilon)^n.$$

It remains to prove the claim. For each $a \in X$, $k \in S$, let a_k be the probability that $f_1(a, x_2, \ldots x_n) = k$, where $x_2, \ldots x_n$ are chosen randomly and uniformly from X. Similarly, for each $b \in Y$ and $k' \in T$, let $b_{k'}$ be the probability that $g_1(b, y_2, \ldots y_n) = k'$, where $y_2, \ldots y_n$ are chosen randomly and uniformly from Y.

We define the set $U(a,b)$ to be $\{(k,k')|\phi(a,b,k,k') = 1\}$. By the uniqueness property, each k occurs in at most one pair and each k' occurs in at most one pair. Hence $\sum_{(k,k') \in U(a,b)} a_k \leq 1$ and $\sum_{(k,k') \in U(a,b)} b_{k'} \leq 1$.

Then $w(G^n|x_1 = a, y_1 = b) \leq \sum_{(k,k') \in U(a,b)} a_k b_{k'}$. To see this, note that if $\bar{x} = (a, x_2, \ldots, x_n)$ and $\bar{y} = (b, y_2, \ldots, y_n)$, the players win only if for some pair $(k,k') \in U(a,b)$, $f_1(\bar{x}) = k$ and $g_1(\bar{y}) = k'$. The probability of this is $a_k b_{k'}$ for each pair (k,k'), since the x_i's and the y_i's are chosen independently.

Hence if $(a,b) \in H$, $\sum_{(k,k') \in U(a,b)} a_k b_{k'} \geq (3/4)(1-(1/4)\epsilon)^{n-1}$. Since $n \leq \lceil 1/\epsilon \rceil$, $(1-(1/4)\epsilon)^{n-1} \geq 3/4$, and so $\sum a_k b_{k'} \geq (3/4)^2 > 1/2$. By Lemma 3.1, if $(a,b) \in H$ then for some pair $(k,k') \in U(a,b)$, $a_k > 1/2$ and $b_{k'} > 1/2$.

We now define strategies f' and g' for players I and II of G and show that if the players use these strategies, the probability of winning the game G is at least $|H|/s^2$. From this it follows that $|H| \leq (1-\epsilon)s^2$, since $w(G) = 1-\epsilon$. For any $a \in X$, let $f'(a) = i$ where i is an arbitrary element of S such that $a_i = \max_k a_k$. Similarly, for any $b \in Y$, let $g'(b) = j$, where j is an arbitrary element of T such that $b_j = \max_k b_k$.

Finally, we show that on these strategies, the players win on all pairs $(a,b) \in H$. This is because if $(a,b) \in H$ and $f'(a) = i$, $g'(b) = j$, then $a_i > 1/2$ and $b_j > 1/2$. We already showed that if $(a,b) \in H$ then for some pair (k,k'), $a_k > 1/2$ and $b_{k'} > 1/2$. Also, since $\sum a_k \leq 1$ and $\sum b_{k'} \leq 1$, there must be a unique i,j for which $a_i > 1/2$ and $b_j > 1/2$. From this it follows that $(i,j) \in U(a,b)$. Hence, $\phi(a,b,i,j) = 1 \Rightarrow \phi(a,b,f'(a),g'(b)) = 1$. This completes the proof that $|H| \leq (1-\epsilon)s^2$. □

4 Results on $(1,2)$-limited Free Games

In this section we extend Theorem 3.1 to free games that are $(1,2)$-limited. A game is $(1,2)$-limited if for all x, y, x' there is at most one y' such that $\phi(x,y,x',y') = 1$ and for all x, y, y' there are at most two x' such that $\phi(x,y,x',y') = 1$.

Theorem 4.1 *Let G be a non-trivial, (1,2)-limited free game. Let $w(G) = 1-\epsilon$. Then if $n = \lceil 1/\epsilon \rceil$,* $w(G^n) \leq 11/12$.

Proof: Let G be the game $\langle \phi, X \times Y, S, T \rangle$ and assume that $|X| = |Y| = |S| = |T| = s$. Just as in Theorem 3.1, we show by induction on n that if $n \leq \lceil 1/\epsilon \rceil$, then $w(G^n) \leq (1-(1/6)\epsilon)^n$. From this the theorem follows easily, since when $n = \lceil 1/\epsilon \rceil$, $(1-(1/6)\epsilon)^n \leq 11/12$.

The basis case, when $n = 1$, is trivial, since $w(G) = 1-\epsilon \leq 1-(1/6)\epsilon$. Let $n > 1$. Fix strategies f and g of the players in game G^n that maximize $w(G^n)$. With respect to these strategies, define

$w(G^n|x_1 = a, y_1 = b)$ to be the probability that the players win the game G^n, given that $x_1 = a$ and $y_1 = b$. Note that for any pair (a, b), this probability is at most $w(G^{n-1})$. Also, let H be the set of pairs (a, b) in $X \times Y$ for which $w(G^n|x_1 = a, y_1 = b) \geq (5/6)(1-(1/6)\epsilon)^{n-1}$.

$$\begin{aligned} w(G^n) &= 1/s^2 \sum_{(a,b)\in X\times Y} w(G^n|x_1 = a, y_1 = b) \\ &\leq 1/s^2[\sum_{(a,b)\in H} w(G^{n-1}) + \sum_{(a,b)\in(X\times Y)-H} (5/6)(1-(1/6)\epsilon)^{n-1}] \\ &\leq \frac{(1-(1/6)\epsilon)^{n-1}}{s^2}[\sum_{(a,b)\in H} 1 + \sum_{(a,b)\in(X\times Y)-H} (5/6)]. \end{aligned}$$

We claim that $|H| \leq (1-\epsilon)s^2$. From this the lemma follows easily, since then

$$w(G^n) \leq (1-(1/6)\epsilon)^{n-1}[(1-\epsilon)+(5/6)\epsilon] = (1-(1/6)\epsilon)^n.$$

It remains to prove the claim. For each $b \in Y$, $k \in T$, let b_k be the probability that $g_1(b, y_2, \ldots y_n) = k$, where $y_2, \ldots y_n$ are chosen randomly and uniformly from Y. Clearly $\sum_k b_k = 1$.

Let $S(a, b, k)$ be the subset of S such that $k' \in S(a, b, k)$ if and only if $\phi(a, b, k', k) = 1$. Since G is (1,2)-limited, $|S(a, b, k)| \leq 2$ for all a, b, k. Also, if $k_1 \neq k_2$ then $S(a, b, k_1) \cap S(a, b, k_2)$ is empty. This is because if $k' \in S(a, b, k_1) \cap S(a, b, k_2)$, then $\phi(a, b, k', k_1) = \phi(a, b, k', k_2) = 1$. Since G is (1,2)-limited, there is at most one k for which $\phi(a, b, k', k) = 1$; hence $k_1 = k_2$. Let $a_{b,k}$ be the probability that $f_1(a, x_2, \ldots, x_n) \in S(a, b, k)$, where $x_2, \ldots x_n$ are chosen randomly and uniformly from X. Since the sets $S(a, b, k)$ are disjoint for fixed (a, b), $\sum_k a_{b,k} \leq 1$. Then

$$\begin{aligned} w(G^n|x_1 = a, y_1 = b) &\leq \Pr[(f_1(a, x_2, \ldots, x_n) \in S_k) \text{ and } (g_1(b, y_2, \ldots y_n) = k)] \\ &= \Pr[f_1(a, x_2, \ldots, x_n) \in S_k] \Pr[g_1(b, y_2, \ldots y_n) = k] \\ &\qquad \text{(since the } x_i \text{ and } y_i \text{ are independent)} \\ &= \textstyle\sum_k a_{b,k} b_k. \end{aligned}$$

Hence if $(a, b) \in H$, $\sum_k a_{b,k} b_k \geq (5/6)(1-(1/6)\epsilon)^{n-1}$. Since $n \leq \lceil 1/\epsilon \rceil$, $(1-(1/6)\epsilon)^{n-1} \geq 5/6$, and so $\sum a_{b,k} b_k \geq (5/6)^2 > 2/3$. By Lemma 3.1, if $(a, b) \in H$ then for some k, $a_{b,k} > 2/3$ and $b_k > 2/3$.

We now define strategies f' and g' for players I and II of G and show that if the players use these strategies, the probability of winning the game G is at least $|H|/s^2$. From this it follows that $|H| \leq (1-\epsilon)s^2$, since $w(G) = 1-\epsilon$. For any $b \in Y$, let $g'(b) = j$, where j is the first element of T such that $b_j = \max_k b_k$. Note that for any a and any b such that $(a, b) \in H$, $\Pr[f(a, x_2, \ldots, x_n) \in S(a, b, g'(b))] > 2/3$, since this probability is $a_{b,g'(b)}$.

For any $a \in X$, if $(a, b) \notin H$ for some b, define $f'(a)$ arbitrarily. Otherwise, let $f'(a)$ be the first element of

$$\cap_{\{b|(a,b)\in H\}} S(a, b, g'(b)).$$

The fact that f' is well-defined follows easily from the next claim.

Claim: Fix a, and suppose that $(a, b) \in H$ for some b. Then $\cap_{\{b|(a,b)\in H\}} S(a, b, g'(b))$ is not empty.

To prove the claim, fix some b such that $(a,b) \in H$. Then since $\Pr[f(a,x_2,\dots,x_n) \in S(a,b,g'(b))] > 2/3$ and $|S(a,b,g'(b))| \leq 2$, there must exist $k' \in S(a,b,g'(b))$ such that $\Pr[f(a,x_2,\dots,x_n) = k'] > 1/3$. Hence for all b' such that $(a,b') \in H$, $k' \in S(a,b',g'(b'))$: otherwise, $\Pr[f(a,x_2,\dots,x_n) \in S(a,b',g'(b'))] \leq 1 - 1/3 < 2/3$. Hence $k' \in \cap_{\{b|(a,b)\in H\}} S(a,b,g'(b))$, completing the proof of the claim.

Finally, we show that on these strategies, the players win on all pairs $(a,b) \in H$. This is because if $(a,b) \in H$, $f'(a) \in S(a,b,g'(b))$, by the above claim. Then by the definition of $S(a,b,g'(b))$, $\phi(a,b,f'(a),g'(b)) = 1$. This completes the proof that $|H| \leq (1-\epsilon)s^2$. □

Theorem 4.1 can easily be extended to $(1,l)$-limited games, by replacing $11/12$ in the statement of the above theorem by $\frac{4(l+1)-1}{4(l+1)}$.

5 Conclusions and Open Problems

Theorem 2.1 shows that the winning probability of the product G^n of a free game G converges to 0 exponentially fast as $n \to \infty$; the rate of convergence is $O(q^n)$, where $q < 1 - e^{-3s}/2$. This theorem can be improved by decreasing the number q. Ideally, we would like to show that the winning probability of G^n is $O(w(G)^n)$; that is, the winning probability converges to 0 at the same rate as $w(G^n)$. However, we do not know how to prove this.

Another problem that remains unsolved is to generalize this result to other types of two-person games. In particular, the computation of a general class of 1-round, 2-prover interactive proof systems on a fixed input can be modeled by the following type of game: $\langle \phi, E \subseteq X \times Y, S, T \rangle$, where ϕ is a *probabilistic* function, $\phi : E \times S \times T \to [0,1]$. Can Theorem 2.2 be extended to this class of games?

References

[1] L. Babai, Trading Group Theory for Randomness, Proceedings of 17th STOC, 1985, pp 421-429.

[2] M. Ben-Or, S. Goldwasser, J. Killian and A. Wigderson, Multi-Prover Interactive Proofs: How to Remove Intractability, Proceedings of the 20th STOC, May, 1988.

[3] B. Bollobás, *Extremal Gaph Theory*, Academic Press, 1978.

[4] L. Fortnow, Complexity-Theoretic Aspects of Interactive Proof Systems, Ph. D. Thesis, Tech Report #MIT/LCS/TR-447, MIT.

[5] L. Fortnow, J. Rompel and M. Sipser, On the Power of Multi-Prover Interactive Protocols, Proceedings of the conference on Structure in Complexity Theory, 1988, pp 156-161.

[6] S. Goldwasser, S. Micali and C. Rackoff, The knowledge complexity of interactive protocols, Proceedings of 17th STOC, 1985, pp 291-304.

[7] S. Goldwasser and M. Sipser, Private Coins versus Public Coins in Interactive Proof Systems, Proceedings of 18th STOC, 1986, pp 59-68.