Theoretical Computer Science 103 (1992) 25–38
Elsevier

On games of incomplete information

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

Anne Condon**
Computer Science Department, University of Wisconsin-Madison, USA

Richard J. Lipton***
Department of Computer Science, Princeton University, Princeton, New Jersey 08544, USA

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. Players I and II each pick a random number i and j in private, where $1 \leqslant i,j \leqslant s$, and then each chooses a private number $f(i)$ and $g(j)$, $1 \leqslant f(i), g(j) \leqslant s$. 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 [10], which we will discuss soon.

Formally, we define the nth product game G^n as the following two-person game. Players 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, $1 \leqslant i_k, j_k \leqslant s$, and then each chooses a private sequence of numbers $f_1(\bar{i}),\ldots,f_n(\bar{i})$ and $g_1(\bar{j}),\ldots,g_n(\bar{j})$. 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 consider only

* Research supported by a Presidential Young Investigator Award, NSF grant number CCR-9057486.
** Work supported by NSF grant number DCR-8402565.
*** Research supported by DARPA and ONR contracts N00014-85-C-0456 and N00014-85-K-0465.

nontrivial games. Similarly, the winning probability $w(G^n)$ of the product game G^n is defined to be $\max_{f_1, \ldots, f_n, g_1, \ldots, g_n} \Pr[\bigwedge_{k=1}^{n} \phi_G(i_k, j_k, f_k(\bar{i}), g_k(\bar{j}) = 1]$.

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 [10] 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 whether $w(G^n) \to 0$ as $n \to \infty$. Thc first result of this paper is that the winning probability of the product game G^n converges to 0 exponentially fast as $n \to \infty$.

If G is a nontrivial free game, then there exists a $q < 1 - e^{-3s}/2$ such that the winning probability of G^n is at most $2eq^n$ (cf. Theorem 2.1).

Our study of games was motivated by a recent work on multi-prover interactive proof tems (MIPs), introduced by Ben-Or et al. [3]. These are generalizations of the interactive proof systems (IPSs) of Goldwasser et al. [12] 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 consider only 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 depend only 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 where 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 $\varepsilon(n)$ if

(1) for all $x \in L$, $|x| = n$, (P_1, P_2, V) accepts x with a probability of at least $1 - \varepsilon(n)$; and

(2) for all $x \notin L$, $|x| = n$, and any provers P_1^*, P_2^*, (P_1^*, P_2^*, V) accepts x with a probability of at most $\varepsilon(n)$.

Fortnow et al. [11] considered the following 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 [13] 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.

Fortnow et al. [11] showed how to simulate any IPS by a 1-round MIP with the following properties:

(1) If x is accepted by the IPS, $|x|=n$, then the probability that x is accepted by the MIP is $\geqslant 1-1/2^n$.

(2) If x is rejected by the IPS, $|x|=n$, then the probability that x is accepted by the MIP is $\leqslant 1-1/p(n)$, for some polynomial p.

(3) The message the verifier sends to each prover is computed before receiving a response from the other prover.

In a previous work, Ben-Or et al. [3] also described a 1-round MIP with the first two properties but not the third. We call a 1-round MIP protocol that simulates an IPS using the method of Fortnow et al. [11] an *IPS-simulation* protocol.

Fortnow et al. [11] 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 [10] 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. [11] 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 $n=p'(1/(1-w(G)))$. Although Theorem 2.1 implies that the winning probability of a free game G decays exponentially as $n\to\infty$, it is not strong enough to resolve this probem, even for free games.

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 that G is *(l,l')-limited* if

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

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

Then the IPS-simulation protocols of Fortnow et al. [11] 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.

Let G be a nontrivial, $(1,2)$-limited free game. Let $w(G)=1-\varepsilon$. Then if $n=\lceil 1/\varepsilon\rceil$, $w(G^n)\leqslant 11/12$ (cf. Theorem 4.1).

1.1. Related work

Since the time this work first appeared [6], there have been many new results on multi-prover interactive proof systems and two-person games of cooperation. We summarize these results here.

Cai et al. [7] solved the motivating problem of the current paper, namely, any unbounded-round single-prover interactive proof system can be simulated by a bounded-round two-prover interactive proof system. The number of rounds in the multi-prover interactive proof system, however, remains dependent on the error probability. Later, using an idea of Lipton [16] on the permanent function, Lund et al. [18] showed that the class IP of languages accepted by an unbounded-round single-prover interactive proof system contains the polynomial-time hierarchy. It was generalized by Shamir [19] to show that IP is exactly PSPACE. Cai et al. [8] combined their work with ideas in [7] to show that all languages in PSPACE. have 2-prover 1-round interactive proof systems. Moreover, the error can be made exponentially small.

Babai et al. [2] showed that the class of languages having two-prover interactive protocols with *two provers* and an unbounded number of rounds is exactly the class of languages accepted by a nondeterministic Turing machine in exponential time. Feige [9] shows that any language in nondeterministic exponential time has a 1-round 2IPS, with error probability $<1/2$. The same result is also attributed to Kilian (private communication in [9]). Very recently, Lapidot and Shamir [14, 15] studied 1-round 2IPSs and have constructed a multi-prover IPS with exponentially small error probability for any language in nondeterministic exponential time, based partly on our methods. Feige (personal communication), has reduced the number of provers in their protocol to two.

Lapidot and Shamir [14] also showed that a 1-round, 2-prover interactive proof for the Hamiltonian Circuit problem can be parallelized to obtain a new 1-round 2-prover interactive proof that has exponentially small probability. Their result shows that any language in NP has a 1-round, 2-prover interactive proof with exponentially small error probability, which is a *zero-knowledge* proof. Feige [9] generalized the work of Lapidot and Shamir [14] to obtain upper bounds on $w(G^n)$ which are an exponential improvement on the bounds of Theorem 2.1. His result is that for any free nontrivial game G, $w(G^n)<\mathrm{e}^{-k}(1-\mathrm{o}(1))$, where $k=n/(4s^2\ln s)$. Feige also constructs a simple free game for which $w(G)=w(G^2)$.

2. Results on the convergence of free games

In this section we prove Theorem 2.1. We begin by giving precise definitions of a game. We say that $G=\langle\phi, L\subseteq X\times Y, S, T\rangle$ is a *game* if each set X, Y, S, T is finite, $L\neq\emptyset$, and

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

Without loss of generality, we assume that X, Y, S, T all equal $\{1,\ldots,s\}$. We say that 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 players I and II, respectively. G is *nontrivial* if $w(G)$ is neither 0 nor 1. This implies that $s > 1$.

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 $(f_1(\bar{x}), \ldots, f_n(\bar{x}))$, $(g_1(\bar{y}), \ldots, g_n(\bar{y}))$, 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, i.e., $\phi(x, y, f(x), g(y)) = w(G)$, 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 [10] 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 $x = y = 1$, i.e., letting $\phi(x,y,f(x),g(y))=((x \vee f(x)) \neq (y \vee g(y))) \vee (x \wedge y)$, we obtain a nontrivial game for which this argument fails. Our first theorem uses a result of Zarankiewicz, Kovari, Sos and Turan (cf. [4]) to show that if a free game G is nontrivial, then the winning probability of the n-product game converges to 0 exponentially fast as $n \rightarrow \infty$.

Theorem 2.1. *If G is a nontrivial free game, then there exists a $q<1-\mathrm{e}^{-3s}/2$ such that $w(G^n)<2\mathrm{e}q^n$.*

Proof. Suppose a pair of strategies f, g for the two players in the game G^n is given. Let $N=s^n$ be the size of the sample space in the product game. We model the game G^n as a bipartite graph (X, Y, E), where X and Y consist of all inputs to each player in the game G^n; thus, $|X|=|Y|=N$. Think of X and Y consisting of n-tuples $x=(x_1,\ldots,x_n)$ and $y=(y_1,\ldots,y_n)$, where each x_i and y_j ranges from 1 to s. An edge $e(x,y)$ exists between $x=(x_1,\ldots,x_n)$ and $y=(y_1,\ldots,y_n)$ if and only if the players win on inputs x, y, using the strategies f and g. That is, if $\bigwedge_{k=1}^{n} \phi_G(x_k, y_k, f_k(x_1,\ldots,x_n), g_k(y_1,\ldots,y_n))$. We will show that $|E|=\mathrm{O}(N^{2-\lambda(s)})$, for some $\lambda(s)>0$. This clearly implies a bound on the probability of winning the product game.

Roughly, the idea of the proof is as follows. We will define a notion of a *forbidden subgraph* in (X, Y, E), whose existence will imply that the original game G is trivial, i.e., there exists a perfect winning strategy for both players. However if the product game has too high a winning probability we will show that a *forbidden subgraph* must exist in (X, Y, E); thus, we reach a contradiction.

We now define a *forbidden subgraph* in (X, Y, E). Let $K_{s,s}$ be a complete bipartite graph on s nodes each. We also denote by $K_{s,s}$ any subgraph of (X, Y, E) isomorphic to the complete bipartite graph, i.e., a bipartite graph on $A \times B$, where $A \subseteq X$, $B \subseteq Y$, $|A|=|B|=s$, such that there is an edge from every node of A to every node of B. An induced subgraph on the nodes $\{x^1,\ldots,x^s\} \subseteq X$, $\{y^1,\ldots,y^s\} \subseteq Y$ is a *permutation subgraph* if on some coordinate k, both $x_k^1,\ldots,x_k^s$ and $y_k^1,\ldots,y_k^s$ are permutations of 1 to s. Finally, a *forbidden subgraph* is a permutation subgraph that is isomorphic to $K_{s,s}$.

If (X, Y, E) contains a forbidden subgraph, say on the nodes $\{x^1,\ldots,x^s\} \times \{y^1,\ldots,y^s\}$, then G is trivial. To see this, consider the strategies f and g for the game G, defined by $f(x)=f_k(x^i)$ and $g(y)=g_k(y^j)$, where the kth coordinate of x^i is x and the kth coordinate of y^j is y. The players win at all times.

In the next two lemmas, we show that if $|E|$ is large, then (X, Y, E) contains a forbidden subgraph. In Lemma 2.2, we obtain an upper bound for the number of pairs (A, B), where $|A|=|B|=s$, and yet they do not form permutation subgraphs. In Lemma 2.3, we show that if $|E|$ is large, then the number of distinct embeddings of $K_{s,s}$ in (X, Y, E) exceeds the upper bound given in Lemma 2.2 and, thus, they must be forbidden subgraphs.

Lemma 2.2. *The number of nonpermutation subgraphs of (X, Y, E) of the form $(A, B, E \cap (A \times B))$, where $|A|=|B|=s$, is at most $(N^{2s-1/\log s \cdot \mathrm{e}^{2s}})/s!^2$.*

Proof. Consider the set of all pairs of (ordered) s-tuples from X and Y:

$$S=\{((x^1,\dots,x^s),(y^1,\dots,y^s))\,|\,x^i\in X, y^i\in Y\}.$$

Given any such pair $((x^1,\dots,x^s),(y^1,\dots,y^s))\in S$ and any k, $1\leqslant k\leqslant n$, consider the pair of s-tuples formed by the kth coordinates $((x_k^1,\dots,x_k^s),(y_k^1,\dots,y_k^s))$. 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 $((x^1,\dots,x^s),(y^1,\dots,y^s))\in S$ so that for all k, $1\leqslant k\leqslant n$, at least one of $(x_k^1,\dots,x_k^s)$ or $(y_k^1,\dots,y_k^s)$ is not a permutation of 1 to s. This set has cardinality $(s^{2s}-s!^2)^n$. Hence, the set of the pairs $((x^1,\dots,x^s),(y^1,\dots,y^s))\in S$ such that for all k, $1\leqslant k\leqslant n$, both $(x_k^1,\dots,x_k^s)$ and $(y_k^1,\dots,y_k^s)$ 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) sets of s distinct elements from X and Y. Thus, the number of (ordered) pairs of (unordered) sets of s distinct elements from X and Y, where, for all k, $(x_k^1,\dots,x_k^s)$ and $(y_k^1,\dots,y_k^s)$ do not both form permutations, is

$$\begin{aligned}&\binom{N}{s}^2-\frac{N^{2s}-(s^{2s}-s!^2)^n}{s!^2}\\&\leqslant\frac{(s^{2s}-s!^2)^n}{s!^2}\\&\leqslant\frac{1}{s!^2}\left(s^{2s}\left(1-\frac{1}{e^{2s}}\right)\right)^n\\&=\frac{N^{2s+\log_s(1-1/e^{2s})}}{s!^2}\\&\leqslant\frac{N^{2s-1/\log s\cdot e^{2s}}}{s!^2}.\qquad\square\end{aligned}$$

Lemma 2.3. *Suppose that* $|E|\geqslant 2eN^{2-\lambda}$, *where* $\lambda=1/(\log s(1+2s^2)e^{2s})$. *Then the number of distinct embeddings of* $K_{s,s}$ *in* (X,Y,E) *is more than* $(N^{2s-1/\log s\cdot e^{2s}})/s!^2$.

Proof. The proof of this lemma uses the following theorem from extremal graph theory, due to Kovari, Sos and Turan (KST theorem; see [4]), who answered a problem raised by Zarankiewicz. The Zarankiewicz problem is the following: Suppose G is a bipartite graph on $m\times m$ nodes. Under what condition does the graph G necessarily contain a complete bipartite subgraph $K_{s,s}$ on s nodes each? In particular, does the density of the graph G of the form $|E|\geqslant m^{2-\lambda(s)}$ suffice to ensure the existence of a complete bipartite subgraph $K_{s,s}$? The KST theorem is the following: Suppose G is a bipartite graph on $m\times m$ nodes such that G does not contain a $K_{s,s}$. Then the number of edges of G is at most $\frac{1}{2}(s-1)^{1/s}m^{2-1/s}+\frac{1}{2}(s-1)m$.

Let

$$\mathcal{M}=\left\{(A,B)\,\middle|\,|A|=|B|=m\ \&\ e(A,B)\geqslant\frac{|E|}{2}\frac{\binom{N-1}{m-1}^2}{\binom{N}{m}^2}\right\},$$

where $e(A,B)$ denotes the number of edges between A and B, and $s \leqslant m \leqslant N$. The set $\mathscr{M}$ represents the induced $m \times m$ subgraphs of (X, Y, E), such that the number of edges are at least 1/2 of the "average" number of edges in an induced subgraph of size $m \times m$.

By considering how many times every edge $e \in E$ is counted in the following sum, we have

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

Thus, the size of $\mathscr{M}$ can be estimated as follows:

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

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

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

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

We have

$$\begin{aligned} \frac{|\mathscr{M}|}{\binom{N-s}{m-s}^2} &\geqslant \frac{|E|}{2m^2} \frac{\binom{N-1}{m-1}^2}{\binom{N-s}{m-s}^2} \\ &\geqslant \mathrm{e} N^{2-\lambda} \frac{(N-m+1)^{2(s-1)}}{m^{2s}} \\ &= \frac{\mathrm{e} N^{2s-\lambda}}{m^{2s}} \left(1 - \frac{m-1}{N}\right)^{2(s-1)} \end{aligned}$$

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

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

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

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 $(1-\lambda s)n \geqslant (1/\lambda s) - 1 = (\log s(1+2s^2)\mathrm{e}^{2s} - s)/s \geqslant 2 \log s \cdot s \cdot \mathrm{e}^{2s}$,

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

The last inequality is rather trivial, as for large s the middle term goes to 1 while the right-hand side approaches 0. One only needs to verify the cases for small s, which is simple. Hence,

$$\frac{|\mathscr{M}|}{\binom{N}{m-s}^2} > \frac{\mathrm{e}N^{2s-\lambda(1+2s^2)}}{\mathrm{e}^2}\frac{\mathrm{e}}{s!^2}$$

$$= \frac{N^{2s-1/\log s\cdot \mathrm{e}^{2s}}}{s!^2}. \qquad \square$$

Proof of Theorem 2.1 (*conclusion*). Therefore, since the original game G is nontrivial, we must have $|E| < 2\mathrm{e}N^{2-\lambda}$. Applying the definition for these quantities, we have arrived at the following conclusion: The winning probability of the product game for a nontrivial game is bounded by $2\mathrm{e}q^n$, for $n \geqslant \log s(1+2s^2)\mathrm{e}^{2s}/s$, where $q = \mathrm{e}^{-1/(1+2s^2)\mathrm{e}^{2s}} = 1 - 1/(1+2s^2)\mathrm{e}^{2s} + \cdots$, which is less than, say, $1 - \mathrm{e}^{-3s}/2$, for all s. Note that for $n < \log s(1+2s^2)\mathrm{e}^{2s}/s$, q^n is bounded below by $1 - \frac{1}{2}\log 2 > 1/2$, so that the bound $w(G^n) \leqslant 2\mathrm{e}q^n$ holds for all n and s. This completes the proof of Theorem 2.1. $\square$

3. Results on (1, 1)-limited free games

In this section we consider games that are (1, 1)-limited, i.e., games with the property 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 $\sum p_i \leqslant 1$ and $\sum q_i \leqslant 1$. Let $1/2 \leqslant \alpha \leqslant 1$. 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 $p_1 \geqslant p_2 \geqslant \cdots \geqslant p_s$. First note that $p_1 > \alpha$. Otherwise, for all i, $p_i \leqslant \alpha$. Then $\sum p_i q_i \leqslant \alpha \sum q_i = \alpha$, contradicting the fact that $\sum p_i q_i > \alpha$.

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

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

Therefore, $\sum p_i q_i \leqslant p_1 q_1 + (1-p_1)(1-q_1) \leqslant q_1(2p_1 - 1) + (1-p_1)$, by rearranging the terms.

Now, suppose to the contrary that $q_1 \leqslant \alpha$. Then, from the above, $\sum p_i q_i \leqslant q_1(2p_1 - 1) + (1-p_1) \leqslant \alpha(2p_1 - 1) + (1-p_1)$. The last inequality follows since $p_1 > \alpha \geqslant 1/2$, and so $2p_1 - 1 > 0$. Rearranging the terms again, it follows that

$$\sum p_i q_i \leqslant \alpha p_1 + (1-\alpha)(1-p_1) \leqslant \alpha p_1 + \alpha(1-p_1) \quad (\text{since } \alpha \geqslant 1/2)$$

$$= \alpha.$$

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

Theorem 3.2. *Let G be a nontrivial free game that is $(1,1)$-limited. Let $w(G)=1-\varepsilon$. Then if $n=\lceil 1/\varepsilon \rceil$, $w(G^n) \leqslant 7/8$.*

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 $n \leqslant \lceil 1/\varepsilon \rceil$, then $w(G^n) \leqslant (1-(1/4)\varepsilon)^n$. From this the theorem follows easily since, when $n=\lceil 1/\varepsilon \rceil$, $(1-(1/4)\varepsilon)^n \leqslant 7/8$.

The basis case, when $n=1$, is trivial since $w(G)=1-\varepsilon \leqslant 1-(1/4)\varepsilon$. 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 $w(G^n \mid x_1=a,\ y_1=b)$ 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 $w(G^n \mid x_1=a,\ y_1=b) \geqslant (3/4)(1-(1/4)\varepsilon)^{n-1}$.

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

We claim that $|H| \leqslant (1-\varepsilon)s^2$. From this the lemma follows easily since, in that case,

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

It remains to prove the claim. We need the following notation. 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 $\{(k,k') \mid \phi(a,b,k,k')=1\}$. We show that if $(a,b) \in H$, then for some pair $(k,k') \in U(a,b)$, $a_k > 1/2$ and $b_{k'} > 1/2$.

Since the game is $(1,1)$-limited, each k occurs in at most one pair and each k' occurs in at most one pair. Hence,

$$\sum_{(k,k')\in U(a,b)} a_k \leqslant 1 \quad \text{and} \quad \sum_{(k,k')\in U(a,b)} b_{k'} \leqslant 1.$$

Then

$$w(G^n \mid x_1=a, y_1=b) \leqslant \sum_{(k,k')\in U(a,b)} a_k b_{k'}.$$

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 $(a, b)\in H$,

$$\sum_{(k,k')\in U(a,b)} a_k b_{k'} \geqslant (3/4)(1-(1/4)\varepsilon)^{n-1}.$$

Since $n \leqslant \lceil 1/\varepsilon \rceil$, $(1-(1/4)\varepsilon)^{n-1} \geqslant 3/4$ and, so, $\sum a_k b_{k'} \geqslant (3/4)^2 > 1/2$. 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 $|H| \leqslant (1-\varepsilon)s^2$ since $w(G)=1-\varepsilon$. 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 $\sum a_k \leqslant 1$ and $\sum b_{k'} \leqslant 1$, 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 $|H| \leqslant (1-\varepsilon)s^2$. □

4. Results on $(1, 2)$-limited free games

In this section we extend Theorem 3.2 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 nontrivial, $(1, 2)$-limited free game. Let $w(G)=1-\varepsilon$. Then if $n=\lceil 1/\varepsilon \rceil$, $w(G^n) \leqslant 11/12$.*

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 3.2, we show by induction on n that if $n \leqslant \lceil 1/\varepsilon \rceil$, then $w(G^n) \leqslant (1-(1/6)\varepsilon)^n$. From this the theorem follows easily since, when $n=\lceil 1/\varepsilon \rceil$, $(1-(1/6)\varepsilon)^n \leqslant 11/12$.

The basis case, when $n=1$, is trivial since $w(G)=1-\varepsilon \leqslant 1-(1/6)\varepsilon$. 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 $w(G^n \mid x_1=a, y_1=b)$ 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 $w(G^n \mid x_1 = a, y_1 = b) \geqslant (5/6)(1-(1/6)\varepsilon)^{n-1}$.

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

We claim that $|H| \leqslant (1-\varepsilon)s^2$. From this the lemma follows easily since, in that case,

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

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, $|S(a,b,k)| \leqslant 2$ 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), $\sum_k a_{b,k} \leqslant 1$. Then

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

Hence, if $(a,b) \in H$, $\sum_k a_{b,k} b_k \geqslant (5/6)(1-(1/6)\varepsilon)^{n-1}$. Since $n \leqslant \lceil 1/\varepsilon \rceil$, $(1-(1/6)\varepsilon)^{n-1} \geqslant 5/6$ and, so, $\sum a_{b,k} b_k \geqslant (5/6)^2 > 2/3$. 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 $|H| \leqslant (1-\varepsilon)s^2$ since $w(G) = 1 - \varepsilon$. 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 $(a,b)\in H$, $\Pr[f(a,x_2,\dots,x_n)\in S(a,b,g'(b))]>2/3$ 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

$$\bigcap_{\{b\mid(a,b)\in H\}} S(a,b,g'(b)).$$

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 $\bigcap_{\{b\mid(a,b)\in H\}}S(a,b,g'(b))$ is not empty.*

Proof of claim. 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 $|S(a,b,g'(b))|\leqslant 2$, 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, $\Pr[f(a,x_2,\dots,x_n)\in S(a,b',g'(b'))]\leqslant 1-1/3<2/3$. Hence, $k'\in\bigcap_{\{b\mid(a,b)\in H\}}S(a,b,g'(b))$, completing the proof of the claim. □

Proof of Theorem 4.1 (*conclusion*). 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 $|H|\leqslant(1-\varepsilon)s^2$. □

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

References

[1] L. Babai, Trading group theory for randomness, in: *Proc. 17th Ann. ACM Symp. on the Theory of Computing (STOC)* (1985) 421–429.

[2] L. Babai, C. Lund and L. Fortnow, Non-deterministic exponential time has two-prover interactive protocols, in: *Proc. 30th IEEE Symp. on the Foundations of Computer Science (FOCS)* (1990) 16–25.

[3] M. Ben-Or, S. Goldwasser, J. Kilian and A. Wigderson, Multi-prover interactive proofs: how to remove intractability, in: *Proc. 20th ACM Ann. Symp. on the Theory of Computing (STOC)* (1988) 113–131.

[4] B. Bollobás, *Extremal Graph Theory* (Academic Press, New York, 1978).

[5] J. Cai, PSPACE is provable by two provers in one round, Technical Report CS-TR-260-90, Computer Science Department, Princeton University, 1990.

[6] J. Cai, A. Condon and R.J. Lipton, Playing games of incomplete information, *Proc. Symp. on Theoretical Aspects of Computer Science (STACS)* (1990) 58–69.

[7] J. Cai, A. Condon and R.J. Lipton, On bounded round multi-prover interactive proof systems, *Proc. of Fifth Ann. Conf. on Structure in Complexity Theory* (1990) 45–54.

[8] J. Cai, A. Condon and R.J. Lipton, PSPACE is provable by two provers in one round, in *Proc. Sixth Ann. Conf. on Structure in Complexity Theory* (1991) 110–115.

[9] U. Feige, On the success probability of the two provers in one-round proof systems, in: *Proc. Sixth Ann. Conf. on Structure in Complexity Theory* (1991) 116–123.

[10] L. Fortnow, Complexity-theoretic aspects of interactive proof systems, Ph.D. Thesis, Tech. Report #MIT/LCS/TR-447, MIT, 1989.

[11] L. Fortnow, J. Rompel and M. Sipser, On the power of multi-prover interactive protocols, in: *Proc. Third Ann. Conf. on Structure in Complexity Theory* (1988) 156–161.

[12] S. Goldwasser, S. Micali and C. Rackoff, The knowledge complexity of interactive protocols, in: *Proc. 17th Ann. ACM Symp. on the Theory of Computing (STOC)* (1985) 291–304.

[13] S. Goldwasser and M. Sipser, Private coins versus public coins in interactive proof systems, in: *Proc. 18th Ann. ACM Symp. on the Theory of Computing (STOC)* (1986) 59–68.

[14] D. Lapidot and A. Shamir, Parallel two prover zero knowledge protocols, manuscript from the Applied Mathematics Department, The Weizmann Institute of Science, 1990.

[15] D. Lapidot and A. Shamir, Fully parallelized multi prover protocols for NEXP-time, manuscript from the Applied Mathematics Department, The Weizmann Institute of Science, 1991.

[16] R.J. Lipton, New directions in testing, in: J. Feigenbaum and M. Merritt, eds., *Distributed Computing and Cryptography*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 2 (American Mathematical Soc., Providence, RI, 1991) 191–202.

[17] R.J. Lipton, Efficient checking of computations, in: *Proc. Symp. on Theoretical Aspects of Computer Science (STACS)* (1990) 207–215.

[18] C. Lund, L. Fortnow, H. Karloff and N. Nisan, The polynomial-time hierarchy has interactive proofs, in: *Proc. 30th IEEE Symp. on the Foundations of Computer Science (FOCS)* (1990) 2–10.

[19] A. Shamir, IP = PSPACE, in: *Proc. 30th IEEE Symp. on the Foundations of Computer Science (FOCS)* (1990) 11–15.