MATHEMATICS OF OPERATIONS RESEARCH
Vol 17, No. 2, May 1992
Printed in U S.A

FAIR DISTRIBUTION PROTOCOLS OR HOW THE PLAYERS REPLACE FORTUNE*†

IMRE BÁRÁNY

There are $n \geq 2$ players $P_1, P_2, \dots, P_n$, each of them having a finite alphabet $A_1, \dots, A_n$, and there is a probability distribution p on $A = A_1 \times \cdots \times A_n$. The players want to choose $a \in A$ according to p in such a way that P_k knows only the kth component, a_k, of a. This can be done with the help of an impartial person or "fortune" who chooses $a \in A$ according to p and informs P_k on a_k only. But what happens if no such person is available? Can the players find a procedure that replaces fortune? It is proved here that the answer is yes when $n \geq 4$. As an application it is shown that a correlated equilibrium of a noncooperative n-person game ($n \geq 4$) coincides with a Nash equilibrium of an extended game involving, in addition, plain conversations only.

1. Introduction. The basic situation this paper is concerned with is: there are $n \geq 2$ players $P_1, P_2, \dots, P_n$, each of them having a finite alphabet or strategy set (we prefer the word alphabet) $A_1, \dots, A_n$, and there is a probability distribution p on $A = A_1 \times \cdots \times A_n$. What the players want to do is to choose $a \in A$ according to p in such a way that P_k knows only the kth component, a_k, of a. This can be done with the help of an impartial person or "fortune" who chooses $a \in A$ according to p and informs P_k on a_k only. But what happens if no such person is available? Can the players find a procedure, or protocol, as we will call it, that replaces fortune?

A *protocol* is an agreed upon procedure according to which the players exchange a set of messages. A *message* is a piece of information transmitted from one player to another one. To compute a message may require the sender to use some randomizing device and the set of information he has obtained so far. At each step of the protocol there is only one message and both the sender and the receiver are determined uniquely. When the protocol is over player P_k has a set of information I_k known to him. I_k consists of the set of messages M_k he sent or received during the protocol and the set of random choices ξ_k he made. M_k is a random variable determined by the random choices of all players: $M_k = M_k(\xi_1, \dots, \xi_n)$. So P_k is informed on the other players' random choices through the messages only. As a matter of fact, each I_k is a random variable and each message is of the form "$I_k^{(r)} \in B$," where B is some event and $I_k^{(r)}$ is the information obtained by the sender P_k during the first r steps of the protocol. We mention that this kind of exchanging messages is similar to the situation when the players are pairwise connected by phone and can exchange information by phone only.

A *distribution protocol* or DP, for short, that replaces fortune should satisfy the following properties. For each $k = 1, \dots, n$, I_k determines the letter $a_k \in A_k$

*Received April 29, 1987; revised September 10, 1990.
AMS 1980 subject classification. Primary: 90D10, 90D15.
IAOR 1973 subject classification. Main: Games.
OR/MS Index 1978 subject classification. Primary: 238 Games/Noncooperative
Key words. Games, fair distribution protocols, equilibrium, Nash equilibrium.
†This work was partially done while the author was on leave from the Mathematical Institute of the Hungarian Academy of Sciences, 1364 Budapest, P.O. Box 127, Hungary.

0364-765X/92/1702/0327/$01.25

uniquely, i.e., there is a map f_k (known to P_k) with $f_k(I_k) = a_k$ such that

(1) $\text{Prob}(f_1(I_1) = a_1, \ldots, f_n(I_n) = a_n) = p(a_1 \ldots a_n)$ for $a_1 \ldots a_n \in A$,

(2) $\text{Prob}(f_1(I_1) = a_1, \ldots, f_n(I_n) = a_n \mid I_k) = p(a_1 \ldots a_n \mid a_k)$ for $k = 1, \ldots, n$, $a_1 \ldots a_n \in A$ with $p(a_k) > 0$ and $f_k(I_k) = a_k$.

The meaning of the second condition is that I_k does not give more information to P_k than the knowledge of a_k.

These conditions are satisfactory only in the case of players with "good intentions," that is, when the players do not cheat although they want to get as much information from the protocol as possible. In this case *afterward checking* can take place: when the protocol is over, each player can prove by revealing his random choices that he sent his messages according to the rules of the protocol and computed $f_k(I_k) = a_k$ properly.

We are going to consider cases when the players are ready to cheat, i.e., they are inclined to deviate from the rules of the protocol in order to get more information even if conditions (1) and (2) must fail to hold with this deviation. This case occurs in correlated equilibrium situations in noncooperative n-person games (see [1], [2]).

In a noncooperative n-person game each player P_k has a payoff function H_k: $A \to R^1$ representing the amount $H_k(a)$ of money he gets if the players have chosen their strategies to be $a = a_1 \ldots a_n \in A$. In a correlated equilibrium situation a probability space (S, μ) is given together with measurable functions c_k: $S \to A_k$ $(k = 1, \ldots, n)$. The game proceeds as follows. Fortune chooses $\omega \in S$ and suggests the strategy $c_k(\omega) = a_k$ to player P_k $(k = 1, \ldots, n)$. The functions c_k have the property that the expected payoff of P_k is maximal if he plays his suggested strategy, i.e., if for any k and any $a'_k \in A_k$

$$\text{Exp}\big(H_k(c_1(\omega), \ldots, c_k(\omega), \ldots, c_n(\omega)) \mid c_k(\omega) = a_k\big)$$

$$\geq \text{Exp}\big(H_k(c_1(\omega), \ldots, a'_k, \ldots, c_n(\omega)) \mid c_k(\omega) = a_k\big).$$

In a correlated equilibrium no player is inclined to unilaterally deviate from his suggested strategy if he knows his suggested strategy only.

A correlated equilibrium gives rise to a probability distribution p on A:

$$p(a) = \mu\big(\{\omega \in S\colon c_k(\omega) = a_k \text{ for } k = 1, \ldots, n\}\big).$$

(Actually, S can be identified with A and the function $(c_1, \ldots, c_n)$ can be taken to be the identity $A \to A$ but we will not need this in the sequel.) To replace fortune the players want to choose an $a \in A$ according to p in such a way that P_k knows a_k only $(k = 1, \ldots, n)$. If they are going to use a DP for this end, some of the players may indeed want to deviate from the rules of the protocol if through this deviation he can get more information on the other players' strategies and possibly more expected payoff. In order to avoid this, afterward checking is not satisfactory, and *built-in checking* is needed. Built-in checking is a very natural thing: as we observed earlier the information I_k obtained by P_k is an event in the σ-algebra which is the product of the n σ-algebras underlying the random choices of the players. Now P_k concludes that cheating has occurred if his set of information is contradictory, i.e., I_k is empty or, but this will be the same in our understanding, I_k has probability zero.

There are two possible kinds of deviation. The first is when a player does not compute his message properly, i.e., instead of the message "$I_k^{(r)} \in B$" he transmits the message "$I_k^{(r)} \in B'$" with $B \neq B'$. This kind of deviation which we call *deviation* *from the rules* can possibly be detected by built-in checking. The second kind of deviation is *deviation in probability*: player P_k has a given probability space to choose ξ_k from but he may use another, not the prescribed distribution, to choose ξ_k. This kind of deviation cannot be detected. (In game theory literature, deviation from the rules and deviation in probability, respectively, are sometimes called detectable and undetectable deviation.) We are going to present protocols with properties

(3) any unilateral deviation in probability does not influence conditions (1) and (2),

(4) any unilateral deviation from the rules is detected with probability one.

A *sure protocol* or SP, for short, is a protocol satisfying conditions (1), (2), (3) and (4).

The main result of this paper is that there is an SP for four and more players (if the probability distribution p is rational valued). This result has the following application in game theory. Let G_0 be an n-person game and let x be a correlated equilibrium payoff of G_0 (with finite and rational valued underlying probability distribution). Then there exists a direct communication game G extending G_0 (i.e., one where plain conversation is allowed before moving) such that x is a Nash equilibrium payoff of G.

Throughout the paper we use the following two assumptions. The first is that the players are not allowed to form coalitions. The second is a technical one: we assume that the probability distribution p on A is rational valued. This may be justified by the fact that the players' underlying probability space (to choose ξ_k from) is finite and rational valued in every physically realizable model. Furthermore, every nonrational distribution can be approximated with arbitrary precision by rational ones.

We also assume that the players have perfect recall, meaning that they remember all the messages they sent or received and all the random choices they made.

A different approach to protocols has recently been considered in [9], [5] and [8]. Their assumption is that the thinking time of each player is limited (to ten minutes, say) and that some problems are indeed computationally intractable, for instance, the factors of a 200-digit number cannot be found in a lifetime if this number is the product of two 100-digit "random" primes. The question is then to find a DP with afterward checking for the problems "coin flipping on phone" and "dealing cards on phone to two players" [9], [8]. These problems can be described in our model as well though the type of checking may be different. For coin flipping there are two players with $A_1 = A_2 =$ {heads, tails} and the distribution is

	heads	tails
heads	1/2	0
tails	0	1/2

For dealing cards the alphabets $A_1 = A_2$ are the set of all possible hands and $p(a_1 a_2) = 0$ if the two hands have a card in common, otherwise $p(a_1 a_2)$ is a constant. A protocol for dealing cards on phone to three or more players without any assumption on intractability is given in [4].

2. The theorems. First we give the formal description of a protocol. A *protocol* is a set of rules (known to each player) specifying the actions of the players. These rules describe which player P_k is to be active in the rth step and what exactly his action should be. This action can be any one of the following three:

(i) to make a random choice $\zeta_k^{(r)}$ from a given probability space with a given probability distribution, then compute a message $m_k^{(r)}$ from the information $I_k^{(r)}$

known to P_k in the rth step (this includes $\zeta_k^{(r)}$), and to transmit it to another player P_j who is specified by the rules,

(ii) to compute his letter as $a_k = f_k(I_k^{(r)})$,

(iii) if $I_k^{(r)}$ is contradictory,[1] then P_k sends the message "deviation has occurred" to every other player.

The protocol terminates if either case (iii) comes up or if every player has computed his letter.

A *distribution protocol* (or DP) is a protocol satisfying conditions (1) and (2). In a DP case (iii) never comes up by definition.

The information $I_k^{(r)}$ known to P_k in the rth step consists of two parts: The set of messages $M_k^{(r)}$ sent or received by P_k so far and the set of random choices $\xi_k^{(r)}$ made by P_k so far. Let T_k be the set of indices of steps when P_k is active, i.e., when P_k sends or receives a message. Then $\xi_k^{(r)} = \{\zeta_k^{(q)}: q \in T_k \text{ and } q \leq r\}$.

Now we give the definition of unilateral *deviation from the rules*. Clearly, $m_k^{(r)} = g(I_k^{(r)}) = g(M_k^{(r)}, \xi_k^{(r)})$ for $r \in T_k$ where the function g is given by the protocol. Assume all other players act according to the rules of the protocol. Then P_k deviates from the rules if there is no random choice sequence $\{\zeta_k^{(r)}: r \in T_k\}$ such that $m_k^{(r)} = g(M_k^{(r)}, \xi_k^{(r)})$ for each $r \in T_k$. This definition is explained by the fact that if such a sequence existed, then P_k could claim that his random choices were just this sequence and then he acted according to the rules of the protocol. Of course, if P_k deviates from the rules, then $m_k^{(r)} \neq g(M_k^{(r)}, \xi_k^{(r)})$ for some $r \in T_k$.

When would now a player, P_i say, claim that his information is contradictory? Assume that P_i has not deviated from the rules. Then his $I_i^{(r)}$ is *contradictory* if, the set of information $I_i^{(r)}$ being kept fixed, there are no random choices of all the other players $\zeta_k^{(r)}$ $(k = 1, \ldots, n,\ k \neq i,\ r \in T_k)$ that would produce this set of information.

A *protocol with sure checking* (SP for short) is a protocol satisfying conditions (1), (2), (3) and (4). Here (4) means that any unilateral deviation from the rules leads to case (iii).

If case (iii) occurs, the players can find the deviating player in the following way. Note that the unilaterally deviating player may also claim that his set of information is contradictory.

One can think of a protocol as a set of rules that builds up a matrix whose rows are indexed by $1, \ldots, n$ and the columns by the steps. If in the rth step P_k has to send a message $m_k^{(r)}$ to P_j (case (i) above), then the (k, r) entry of the matrix is P_k's random choice $\zeta_k^{(r)}$ and the message $m_k^{(r)}$, and its (j, r) entry is $m_k^{(r)}$. Now we assume that the following condition holds:

(5) the message $m_k^{(r)}$ is the same in both entries (k, r) and (j, r), even if P_k or P_j deviates from the rules.

All other entries of the rth column are blank. As long as case (iii) does not come up every player knows "his own row" only which coincides with his set of information. But when case (iii) occurs, everybody reveals his row and the players collectively check every action of every player. By condition (5) everybody learns every message properly and the player P_k who deviated unilaterally from the rules is identified as the sender of a message $m_k^{(r)} \neq g(I_k^{(r)})$ for some $r \in T_k$. Condition (5) is needed here because otherwise, when the faulty message is identified, the sender can claim that he sent the proper message $g(I_k^{(r)})$, and the receiver can claim that he got the faulty message $m_k^{(r)}$ and there is no way to decide who is lying.

In this matrix model unilateral deviation from the rules by P_k means that the kth row is not consistent with itself. And "$I_k^{(r)}$ is contradictory" means that, the kth row

[1]We will soon define when an information set is contradictory.

being kept fixed, the matrix cannot be filled in such a way that each row be consistent with itself.

Now we present the results. We remind the reader that the distribution p is supposed to be rational valued.

THEOREM 1. *There exists an SP for four or more players.*

We give an example showing that there is no SP for three players in general.

THEOREM 2. *There is a DP for three players.*

It is perhaps possible to characterize the distributions with three players for which there exists an SP. The characterization of distributions with two players for which a DP exists can be found. Some definitions are needed.

A probability distribution p on $A_1 \times A_2$ is said to be *reducible* in $a_1, a_1' \in A_1$ if there is a constant c such that $p(a_1 a_2) = cp(a_1' a_2)$ for all $a_2 \in A_2$. In this case let us replace a_1 and a_1' by a new letter b. More precisely, define A' as $(A_1 \setminus \{a_1, a_1'\}) \cup \{b\}$ and $p'(a)$ as $p(a_1 a_2) + p(a_1' a_2)$ if $a = ba_2 \in A' \times A_2$ and $p'(a) = p(a)$ otherwise. Observe that if there is a DP for $p', A' \times A_2$, then this DP will work for $p, A_1 \times A_2$ as well. The only thing we have to add is that if $f_1(I_1) = b$ is the outcome, then P_1 chooses a_1 with probability $p(a_1 a_2)/p'(ba_2)$ and chooses a_1' with probability $p(a_1' a_2)/p'(ba_2)$. (These ratios are independent of a_2.) This implies that one has to look for DPs only if the distribution is irreducible.

THEOREM 3. *There is a DP for two players if and only if the distribution is reducible to a diagonal one.*

A distribution p on $A_1 \times A_2$ is said to be *diagonal* if for each $a_1 \in A_1$ there is only one $a_2 \in A_2$ with $p(a_1 a_2) > 0$ and for each $a_2 \in A_2$ there is only one $a_1 \in A_1$ with $p(a_1 a_2) > 0$. (One can clearly assume that for each $a_1 \in A_1$ there is at least one $a_2 \in A_2$ with $p(a_1 a_2) > 0$ as otherwise the letter a_1 is never used. The same assumption can be made about each letter in A_2.) So if the distribution is diagonal, then the knowledge of a_1 (or a_2) completely determines the outcome $a = (a_1 a_2)$.

The proof of Theorem 3 is based on

LEMMA 4. *Given a DP for an irreducible distribution with two players, a_k is uniquely determined by M_k, the set of messages obtained or given by P_k $(k = 1, 2)$.*

In the definition of a DP we require only that $I_k = \{M_k, \xi_k\}$ determine a_k uniquely by $f_k(I_k) = a_k$. Lemma 4 shows that this is done by M_k alone already (if the distribution is irreducible). Lemma 4 can be extended, and the proof is identical with the one given below, to the case of n players. From this extension it follows that when the protocol is over, $P_1, \ldots, P_{k-1}, P_{k+1}, \ldots, P_n$ can prove or disprove P_k's claim that "$f_k(I_k) = a_k$" by simply putting together M_k from their M_j.

3. An application. As a consequence of Theorem 1 we have the following result about correlated equilibria of noncooperative n-person games.

THEOREM 6. *Let G_0 be an n-person game and let x be a correlated equilibrium payoff of G_0 with rational valued underlying probability distribution. Then there exists a direct communication game G extending G_0 (i.e., one where plain conversation is allowed before moving) such that x is a Nash equilibrium payoff of G.*

This theorem shows that no mediator is needed for the actual realization of a correlated equilibrium (when $n \geq 4$ and the distribution is rational). A recent result of Aumann says that a correlated equilibrium can be viewed as a result of Bayesian rationality (see [2] for a precise statement). On the other hand, our result shows that a correlated equilibrium is a Nash equilibrium (when $n \geq 4$).

We will see from the protocol to be given that the extended game has some additional properties: Any unilateral deviation from the rules is detected with probability one. Furthermore, no unilateral division in probability influences the expected payoff.

We mention one more point here. We will see from the proof of Theorem 1 that each message of the protocol is sent by two players to a third one. Thus the receiver can check if the two messages coincide or not and if they do not he announces that cheating has occurred. In this case all messages are traced back and the cheating player is identified (when condition (5) holds) and is punished at his minmax level: the noncheating players choose the corresponding action when they have to move. It is important to remark that if a receiver claims that cheating has occurred while it has not, he himself is punished by his opponents.

A nice application of the results presented here can be found in [6]. Another relevant result is in [7].

We do not give the proof of Theorem 6 because it follows from Theorem 1 immediately.

4. **Proof of Theorem 1.** We give the proof for four players first. The extension for the case of more players will be given at the end of this section. The proof is split into several parts.

The (X, E) model. When giving a protocol we shall invariably work in the so-called (X, E) model. This is constructed from the set A using the distribution p and its rationality in the following way. Each point $a \in A$ is replaced by a set of points X_a with $X_a \cap X_b = \varnothing$ if $a \neq b$ and $a, b \in A$ such that $|X_a| = L$ for every $a \in A$. Further, for $k = 1, \dots, n$, let the projection pr_k: $A \to A_k$ be defined by $\mathrm{pr}_k(a) = a_k$ if $a = a_1 \dots a_k \dots a_n$. Set $X = \bigcup\{X_a \colon a \in A\}$ and extend each pr_k to X as follows:

$$\mathrm{pr}_k(x) = a_k \text{ if } x \in X_a \quad \text{and} \quad \mathrm{pr}_k(a) = a_k.$$

Finally we fix a set $E \subset X$ in such a way that

$$|E \cap X_a|/L = p(a) \quad \text{for all } a \in A.$$

This is possible if L is chosen suitably because $p(a)$ is rational for each $a \in A$. Now in the (X, E) model a DP or SP works like this: the players choose a point $e \in E$ with uniform distribution on E in such a way that each player P_k gets the information $\mathrm{pr}_k(e)$ only. If this can be done, then the protocol works on the original A with distribution p as well.

We assume, when it is convenient, that $X = \{1, \dots, |X|\}$ and $E = \{1, \dots, |E|\}$.

We assume, further, that in the protocol to be given below the players agree on an (X, E) model which is known to every player and is kept fixed throughout the protocol.

The random choices. Having fixed the (X, E) model the players make their random choices. P_1 and P_2 jointly choose a random permutation α: $X \to X$.

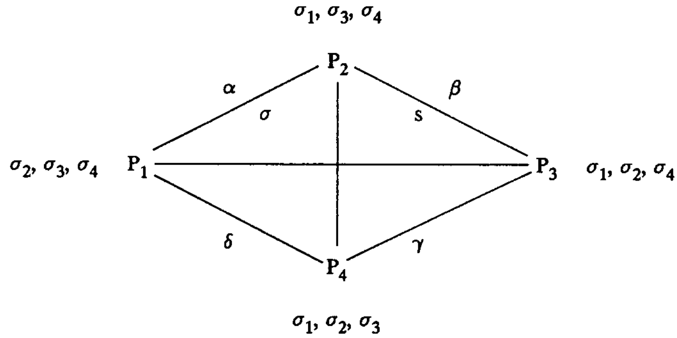


FIGURE 1

Similarly, P_2 and P_3 choose $\beta: X \to X$, P_3 and P_4 choose $\gamma: X \to X$, and P_4 and P_1 choose $\delta: X \to X$. Players $\{P_1, P_2, P_3, P_4\} \backslash \{P_k\}$ choose an ordering σ_k of X for $k = 1, 2, 3, 4$. (This is the same as a permutation yet we prefer the name ordering here.) Moreover, P_1 and P_3 jointly pick a permutation $\sigma: E \to E$ and P_2 and P_4 jointly pick a number $s \in \{1, \dots, m\}$ where $m = |E|$. The chosen element of E will be $e_s = \sigma^{-1}(s)$. Every choice is made according to the uniform distribution of the underlying finite probability space and every choice is made independently of all other random choices. We will explain later what is meant by "picking a random permutation jointly".

Sketch of the protocol. Think of α as a "language" known to P_1 and P_2 but unknown to P_3 and P_4. So $\alpha(x)$ is the α-name of a point $x \in X$. Similarly, β, γ, δ are languages. In the first step of the protocol P_1 gets a $\beta - \gamma$ "dictionary" of the points of X, i.e., a list of the pairs $(\beta(x), \gamma(x))$ $(x \in X)$ from the other three players. (σ_1 is a technical device to make the handover of the dictionary safe.) Now P_1 can, using this dictionary, tell whether the words $\alpha(x)$ and $\beta(y)$ mean the same point of X or not without having any idea about what that point is. In the following steps P_2, P_3, P_4, respectively, get a $\gamma - \delta$, $\delta - \alpha$, and $\alpha - \beta$ dictionary. In the next step P_1 and P_3 give P_2 (and P_4) the list of the pairs $(\gamma(e), \delta(e))$ (and $(\alpha(e), \beta(e))$ for $e \in E$ shuffled according to σ). Then P_2 and P_4 pick the sth element of the corresponding lists which we denote by (γ^*, δ^*) (and (α^*, β^*)). Actually, $\gamma^* = \gamma(\sigma^{-1}(s))$, but we choose this simpler notation. Then P_2 and P_4 tell γ^* and β^* to P_1 and δ^* and α^* to P_3.

Now, how will P_1 learn his letter $a_1 = \mathrm{pr}_1(e_s)$? This is quite simple: P_3 and P_4 tell P_1 the map $\mathrm{pr}_1 \gamma^{-1}: X \to A_1$ who computes now a_1 as

$$\mathrm{pr}_1 \gamma^{-1}(\gamma^*) = \mathrm{pr}_1 \gamma^{-1}\big(\gamma(\sigma^{-1}(s))\big) = \mathrm{pr}_1(e_s).$$

The protocol.

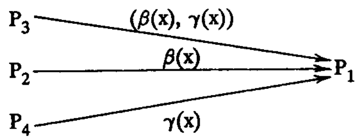
Step 1. P_3 sends the pairs $(\beta\sigma_1^{-1}(i), \gamma\sigma_1^{-1}(i))$ to P_1 for $i = 1, 2, \dots, |X|$. Instead of this we will say that P_3 sends the pairs $(\beta(x), \gamma(x))$ to P_1 in the ordering σ_1.

P_2 sends $\beta(x)$ to P_1 in the ordering σ_1.

P_4 sends $\gamma(x)$ to P_1 in the ordering σ_1.

P_1 checks if the messages are O.K., i.e., if the first (second) component of P_3's ith pair coincides with P_2's (P_4's) ith message or not.

Comment. At the end of Step 1, P_1 knows the pairs $(\beta(x), \gamma(x))$ (for $x \in X$), i.e., the $\beta - \gamma$ dictionary. This is actually the same as the permutation $\beta^{-1}\gamma\colon X \to X$.



In Steps 2, 3 and 4 (which are similar to Step 1) P_2, P_3 and P_4 learn and check the pairs $(\gamma(x), \delta(x))$, $(\delta(x), \alpha(x))$ and $(\alpha(x), \beta(x))$ for all $x \in X$.

Step 5. P_1 sends $\delta(e)$ to P_2 in the ordering σ, i.e., P_1 sends $\delta(\sigma^{-1}(i))$ to P_2 for $i = 1, 2, \dots, m$.

P_1 sends $\alpha(e)$ to P_4 in the ordering σ.

P_3 sends $\gamma(e)$ to P_2 in the ordering σ.

P_3 sends $\beta(e)$ to P_4 in the ordering σ.

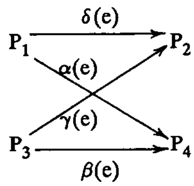
P_2 checks the pairs $(\gamma(e), \delta(e))$ in his "dictionary."

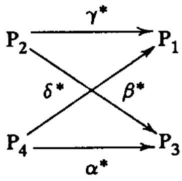
P_4 checks the pairs $(\alpha(e), \beta(e))$ in his "dictionary."

Step 6. (Recall that $e_s = \sigma^{-1}(s)$.) P_4 sends $\alpha^* = \alpha(e_s)$ to P_3 and $\beta^* = \beta(e_s)$ to P_1. P_2 sends $\gamma^* = \gamma(e_s)$ to P_1 and $\delta^* = \delta(e_s)$ to P_3.

P_1 checks the pair (β^*, γ^*) in his dictionary.

P_3 checks the pair (δ^*, α^*) in his dictionary.





Step 7. P_3 sends the map $\mathrm{pr}_1\,\gamma^{-1}\colon X \to A_1$ to P_1.

P_4 sends the map $\mathrm{pr}_1\,\gamma^{-1}\colon X \to A_1$ to P_1.

P_1 checks if the messages are identical. Then he computes his letter as $a_1 = \mathrm{pr}_1\,\gamma^{-1}(\gamma^*) = \mathrm{pr}_1(e_s)$.

In Steps 8, 9 and 10 (which are similar to Step 7) P_2, P_3 and P_4, respectively, obtain $\mathrm{pr}_2\,\delta^{-1}$ (from P_4 and P_1), $\mathrm{pr}_3\,\alpha^{-1}$ (from P_1 and P_2) and $\mathrm{pr}_4\,\beta^{-1}$ (from P_2 and P_3). Then they check if the messages are identical and finally compute their letter as

$$a_2 = \mathrm{pr}_2\,\delta^{-1}(\delta^*) = \mathrm{pr}_2(e_s),$$

$$a_3 = \mathrm{pr}_3\,\alpha^{-1}(\alpha^*) = \mathrm{pr}_3(e_s),$$

$$a_4 = \mathrm{pr}_4\,\beta^{-1}(\beta^*) = \mathrm{pr}_4(e_s).$$

In this protocol deviation from the rules is checked after each step and any such deviation is detected surely.

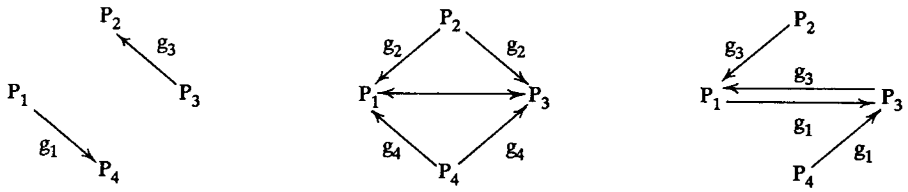
Now we describe a subprotocol for "picking a random permutation jointly." Assume P_1 and P_3 are to choose a random element g from a group G with uniform distribution. In our case G will be either the permutation group of X (or E) or the additive group mod m. We mention that the subprotocol that follows is similar to a jointly controlled lottery without simultaneous moves (see [3]).

The group-protocol.

Step (i). P_k picks $g_k \in G_k$ uniformly and independently of everything else ($k = 1, 2, 3, 4$).

Step (ii). P_1 sends g_1 to P_4, P_3 sends g_3 to P_2,

Step (iii). P_2 sends g_2 to P_1 and to P_3, P_4 sends g_4 to P_1 and to P_3, P_1 and P_3 check (between themselves) if the messages are identical or not.



Step (iv). P_1 and P_4 send g_1 to P_3, P_2 and P_3 send g_3 to P_1, P_1 (and P_3) check if the messages are the same.

Step (v). P_1 (and P_3) computes g as $g = g_1 g_2 g_3 g_4$.

It may happen that P_2, say, chooses, g_2 only after having received g_3 and then he chooses g_2 neither uniformly nor independently of g_2. Still, g_2 will be independent of g_1 and g_4, and so g will have uniform distribution and will be independent of g_1, g_2 and g_3. Even more generally, the following lemma is true.

LEMMA 5. *Assume s_i ($i = 1, 2, 3, 4$) are random variables taking values in $\{1, 2, \ldots, m\}$, σ_i ($i = 1, 2, 3, 4$) are random permutations of $\{1, 2, \ldots, m\}$ and $\xi_1, \ldots, \xi_r$ are random variables. Assume that s_4 is of uniform distribution and is independent of the joint distribution of $s_1, s_2, s_3, \sigma_1, \ldots, \sigma_4, \xi_1, \ldots, \xi_r$. Let $\sigma = \sigma_1\sigma_2\sigma_3\sigma_4$ and $s = s_1 + s_2 + s_3 + s_4 \mod m$. Then the random variable $\sigma(s)$ is uniformly distributed on $\{1, \ldots, m\}$ and is independent of the joint distribution of $s_1, s_2, s_3, \sigma_1, \ldots, \sigma_4, \xi_1, \ldots, \xi_r$.*

PROOF. First we show that $\sigma(s)$ is uniformly distributed. Let $a \in \{1, \ldots, m\}$ and set $a' = \sigma^{-1}(a)$.

$$\begin{aligned}
\operatorname{Prob}(\sigma(s) = a) &= \operatorname{Prob}(s_4 = a' - s_1 - s_2 - s_3) \\
&= \sum_{x=1}^{m} \operatorname{Prob}(s_4 = x, a' - s_1 - s_2 - s_3 = x) \\
&= \sum_{x} \operatorname{Prob}(s_4 = x) \operatorname{Prob}(a' - s_1 - s_2 - s_3 = x) \\
&= \sum_{x} (1/m) \operatorname{Prob}(a' - s_1 - s_2 - s_3 = x) = 1/m.
\end{aligned}$$

We denote the random variable $\{s_1, s_2, s_3, \sigma_1, \ldots, \sigma_4, \xi_1, \ldots, \xi_r\}$ by η. Let us see now that $\sigma(s)$ is independent of η:

$$\begin{aligned}
\operatorname{Prob}(\sigma(s) = a, \eta = \eta') &= \operatorname{Prob}(s_4 = a' - s_1 - s_2 - s_3, \eta = \eta') \\
&= \operatorname{Prob}(s_4 = a' - s_1 - s_2 - s_3) \operatorname{Prob}(\eta = \eta') \\
&= (1/m) \operatorname{Prob}(\eta = \eta') \\
&= \operatorname{Prob}(\sigma(s) = a) \operatorname{Prob}(\eta = \eta'). \quad \square
\end{aligned}$$

We will need this lemma with the roles of s_4 and σ_4 interchanged, too. The proof is almost identical.

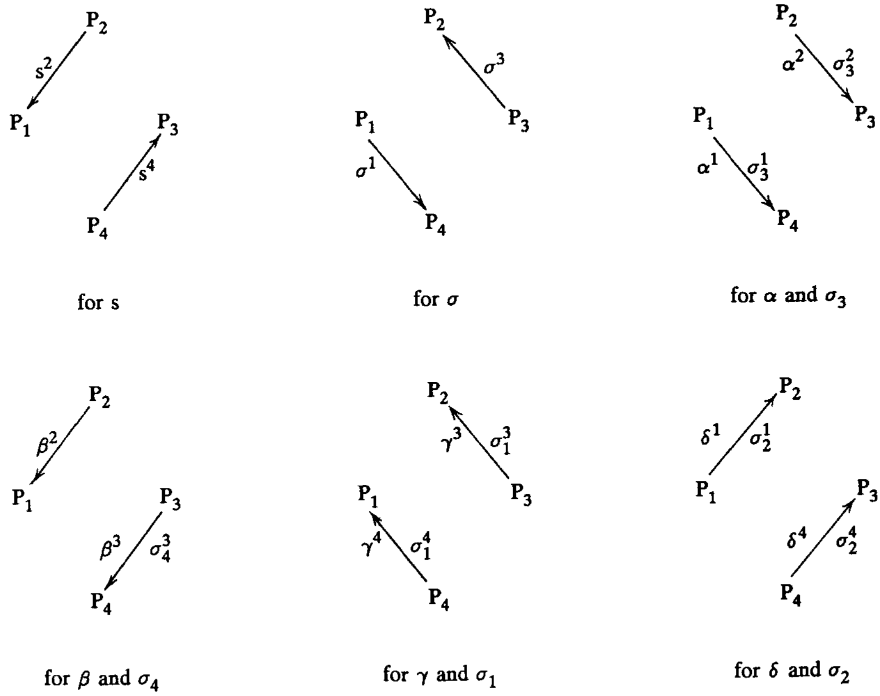


FIGURE 2. The upper index in σ^i shows that this is P_i's choice for σ and $\sigma = \sigma^1\sigma^2\sigma^3\sigma^4$.

There are altogether 10 random choices $s, \sigma, \alpha, \beta, \gamma, \delta, \sigma_1, \sigma_2, \sigma_3, \sigma_4$ in the original protocol, each of them being a function of four other random choices. We organize the group-protocols for the determination of these 10 random choices as follows. First, Step (i) of the 10 group-protocols is carried out; Figure 2 shows how this happens.

Then Step (ii) is carried out in each of the ten group-protocols, then Step (iii), etc. (An obvious sixth step is needed to inform P_4 on σ_3, P_1 on σ_4, P_2 on σ_1 and P_3 on σ_2.)

The advantage of the above scheme is that even if P_k deviates in probability when choosing $s^k, \sigma^k, \alpha^k, \beta^k, \gamma^k, \delta^k, \sigma_1^k, \sigma_2^k, \sigma_3^k, \sigma_4^k$, there is a player P_j all of whose random choices will be independent of all the random choices of P_k. For $k = 1, 2, 3$ and 4, respectively, j will be 3, 4, 1 and 2.

Verification of condition (3). Now we are in a position to prove (3); i.e., that conditions (1) and (2) hold for the proposed protocol even if a player deviates in probability. Let us see first (1):

$$\begin{aligned}\mathrm{Prob}(f_i(I_i) = a_i, i = 1,\dots,4) &= \mathrm{Prob}(\mathrm{pr}_i(e_s) = a_i, i = 1,\dots,4)\\ &= (1/|E|)\left|\{e \in E\colon \mathrm{pr}_i(e) = a_i,\ i = 1,\dots,4\}\right|\\ &= (1/m)\left|X_{a_1a_2a_3a_4} \cap E\right| = p(a_1a_2a_3a_4),\end{aligned}$$

because, according to Lemma 5, $e_s = \sigma^{-1}(s)$ is of uniform distribution.

Let us see now why (2) holds even if P_k unilaterally deviates from the rules. We will compute $\mathrm{Prob}(f_i(I_i) = a_i, i = 1,\dots,4 \mid I_k)$ for $k = 1$ only, for the other cases are very similar. Clearly,

$$I = \{\sigma^1, \sigma^2, \sigma^3, \sigma^4, s^1, s^2, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \beta^1, \beta^2, \gamma^1, \gamma^4, \delta^1, \delta^2, \delta^3, \delta^4,$$
$$\sigma_1^1, \sigma_1^4, \sigma_2^1, \sigma_2^2, \sigma_2^3, \sigma_2^4, \sigma_3^1, \sigma_3^2, \sigma_3^3, \sigma_3^4, \sigma_4^1, \sigma_4^2, \sigma_4^3, \sigma_4^4, \beta^{-1}\gamma, \beta^*, \gamma^*, \mathrm{pr}_1\, \gamma^{-1}, \mathrm{pr}_1(e_s)\}.$$

(Actually P_1 does not know σ_4^3 and σ_4^2 and knows σ_4 but this does not matter.) Now either P_1 or P_2 does not deviate in probability. Consequently, e_s is uniformly distributed and is independent of

$$I_1' = I_1 \setminus \{\beta^*, \gamma^*, \mathrm{pr}_1(e_s)\}$$

where, as we know, $\beta^* = \beta(e_s)$ and $\gamma^* = \gamma(e_s)$. Then

$$\begin{aligned}
&\mathrm{Prob}(f_i(I_i) = a_i, i = 1, \dots, 4 \mid I_1) \\
&\quad = \mathrm{Prob}(f_i(I_i) = a_i, i = 1, \dots, 4, I_1)/\mathrm{Prob}(I_1) \\
&\quad = \mathrm{Prob}(\mathrm{pr}_i(e_s) = a_i, i = 1, \dots, 4, I_1')/\mathrm{Prob}(\mathrm{pr}_1(e_s) = a_1, I_1') \\
&\quad = \mathrm{Prob}(\mathrm{pr}_i(e_s) = a_i, i = 1, \dots, 4)/\mathrm{Prob}(\mathrm{pr}_1(e_s) = a_1) \\
&\quad = |\{e \in E: \mathrm{pr}_i(e) = a_i, i = 1, \dots, 4\}| / |\{e \in E: \mathrm{pr}_1(e) = a_1\}| \\
&\quad = p(a_1 a_2 a_3 a_4 \mid a_1).
\end{aligned}$$

In the last steps we made use of the (X, E) model and of Lemma 5.

More than four players. Now let P_k be a player with $k > 4$. After Step 6 P_1 and P_2 send him γ^* and P_k checks if the messages coincide or not. Then P_3 and P_4 send him the map $\mathrm{pr}_k\, \gamma^{-1}: X \to A_k$. P_k checks, again, if the messages coincide or not and if they do, he computes his letter as

$$a_k = \mathrm{pr}_k\, \gamma^{-1}(\gamma') = \mathrm{pr}_k\, \gamma^{-1}(\gamma(e_s)). \quad \square$$

5. The example. This example shows a three-person game with no SP.

Let $A_1 = \{0\}$, $A_2 = \{T, B\}$ and $A_3 = \{L, R\}$ be the alphabets of players P_1, P_2 and P_3, respectively. The distribution p is defined on A as $p(OTR) = 0$ and $p(OTL) = p(OBL) = p(OBR) = 1/3$.

T	1/3	0
B	1/3	1/3
	L	R

Denote the set of messages between P_i and P_j by M_{ij} $(= M_{ji})$. Assume there is a sure protocol. Then there is a legal run with outcome OBL and messages M_{12}, M_{23} and M_{31}. We claim that M_{23} does not determine the third letter of the outcome L by itself. For if it did, then P_2 would know the outcome OBL completely from his set of information. This means that M_{23} is consistent with a random choice ξ_3' and messages M_{13}' such that $f_3(\xi_3', M_{23}, M_{13}') = f_3(I_3') = R$. Similarly, M_{23} does not determine the second letter of the outcome, B. Thus there exist a random choice ξ_2'' and messages M''_{12} with $f_2(\xi''_2, M_{23}, M''_{12}) = f_2(I''_2) = T$. Both I'_3 and I''_2 occur with positive probability. Now P_1 can deviate from the rules: he tries to exchange messages M'_{13} with P_3 and M''_{12} with P_2. There is a positive probability that this goes undetected because both ξ''_2 and ξ'_3 occur with positive probability. But in this case the outcome is OTR and $p(OTR) = 0$, a contradiction. □

So this example shows that in case of three players, there cannot be an SP in general. We mention that the example is essentially the same as the "game of the chicken" (see [1]).

6. Proof of Theorem 2. Assume the (X, E) model is fixed. The protocol starts with the random choices of the players. Each random choice is made independently of all the other random choices and according to the uniform distribution of the underlying probability space which will always be finite.

For $i = 1, 2$, P_i chooses a permutation π_i: $X \to X$ and another permutation μ_i: $A_i \to A_i$. There are eventually encodings of the names of the elements of X and A_i, respectively. Then P_1 and P_2 choose jointly an ordering $(e_1, e_2, \dots, e_m)$ of the elements of E. Finally P_3 chooses a permutation μ_3: $A_3 \to A_3$ and an integer $s \in \{1, \dots, m\}$.

Define $\kappa_i = \mu_i \, \mathrm{pr}_i$: $X \to A_i$ for $i = 1, 2, 3$.

The steps of a DP for three players follow:

1. P_1 sends $\kappa_1 \pi_1^{-1}$ to P_2.
2. P_2 sends $\kappa_2 \pi_2^{-1}$ to P_1.
3. P_3 sends κ_3 to P_2.
4. P_2 sends $\kappa_3 \pi_2^{-1}$ to P_1.
5. P_1 sends $\pi_1(e_1), \pi_1(e_2), \dots, \pi_1(e_m)$ to P_3 in this order.
6. P_2 sends $\pi_2(e_1), \pi_2(e_2), \dots, \pi_2(e_m)$ to P_3 in this order.
7. P_3 sends $\pi_2(e_s)$ to P_1.
8. P_3 sends $\pi_1(e_s)$ to P_2.
9. P_1 sends $\kappa_2(e_s) = \kappa_2 \pi_2^{-1}(\pi_2(e_s))$ to P_2.
10. P_1 sends $\kappa_3(e_s) = \kappa_3 \pi_2^{-1}(\pi_2(e_s))$ to P_3.
11. P_2 sends $\kappa_1(e_s) = \kappa_1 \pi_1^{-1}(\pi_1(e_s))$ to P_1.
12. P_i computes his letter as $a_i = \mu_i^{-1}(\kappa_i(e_s))$ for $i = 1, 2, 3$.

Now we have to prove that this protocol satisfies conditions (1) and (2). This is quite easy compared to the proof of Theorem 1 and it is, therefore, left to the reader. (The protocol satisfies condition (3) as well but we do not need this.)

7. Proof of Theorem 3. We prove Lemma 4 first. We consider the case $i = 1$ only. Arguing by contradiction, let M_1 be the set of messages sent or received by P_1 during the protocol and assume that both a_1 and a'_1 are consistent with M_1. This means that there are random choices, ξ_1 and ξ'_1, of P_1 such that $f_1(\xi_1, M_1) = a_1$ and $f_1(\xi'_1, M_1) = a'_1$. Then, for all a_2, the outcome $a_1 a_2$ or $a'_1 a_2$ depends only on P_1's choice between ξ_1 and ξ'_1. This means that the event $f_2(I_2) = a_2$ is independent of ξ_1 conditional to M_1. Then

$$\begin{aligned}
&\mathrm{Prob}(f_1(I_1) = a_1, f_2(I_2) = a_2 \mid \xi, M_1) \\
&= \mathrm{Prob}(f_2(I_2) = a_2, \xi_1 \mid M_1)/\mathrm{Prob}(\xi_1 \mid M_1) \\
&= \mathrm{Prob}(f_2(I_2) = a_2 \mid M_1)\,\mathrm{Prob}(\xi_1 \mid M_1)/\mathrm{Prob}(\xi_1 \mid M_1) \\
&= \mathrm{Prob}(f_2(I_2) = a_2 \mid M_1),
\end{aligned}$$

and similarly

$$\text{Prob}(f_1(I_1') = a_1', f_2(I_2) = a_2 \mid \xi_1', M_1) = \text{Prob}(f_2(I_2) = a_2 \mid M_1).$$

By condition (2)

$$\text{Prob}(f_1(I_1) = a_1, f_2(I_2) = a_2 \mid \xi_1, M_1) = p(a_1a_2 \mid a_1) = p(a_1a_2)/p(a_1),$$

$$\text{Prob}(f_1(I_1') = a_1', f_2(I_2) = a_2 \mid \xi_1', M_1) = p(a_1'a_2 \mid a_1) = p(a_1'a_2)/p(a_1')$$

where $p(a_1) = \Sigma\{p(a)\colon a \in A \text{ and } \text{pr}_1(a) = a_1\}$.

Hence $p(a_1a_2)/p(a_1) = p(a_1'a_2)/p(a_1')$, the distribution is reducible in a_1, a_1'. This contradiction proves the lemma.

The proof of Theorem 3. The basic observation is that $M_1 = M_2$ in case of two players. Assume, again by way of contradiction, that $p(a_1a_2) > 0$ and $p(a_1'a_2) > 0$. Then $p(a_1a_2 \mid a_2) > 0$ and $p(a_1'a_2 \mid a_2) > 0$ as well as any M_2 consistent with a_2 must be consistent with both a_1 and a_1'. But as $M_1 = M_2$, this contradicts the lemma. □

To give a DP for a diagonal distribution with two players consider the corresponding (X, E) model. P_1 chooses an ordering $e_1, \dots, e_m$ of E (with uniform distribution on the space of all orderings) and P_2 chooses number $s \in \{1, 2, \dots, m\}$ with uniform distribution again. Then P_2 transmits s to P_1 who informs P_2 that the choice is e_s. P_i determines his letter as $a_i = \text{pr}_i(e_s) \in A$ $(i = 1, 2)$. □

This does not seem to be a very fair protocol (having in mind a correlated equilibrium, say) for P_1 may choose the ordering of E only after having received s. A somewhat fairer protocol can be constructed using a single parallel message: P_1 and P_2 agree upon an ordering of E and then P_1 sends P_2 s_1 and P_2 sends P_1 s_2 simultaneously. Their choice is then $e_s \in E$ where $s = s_1 + s_2$ is taken mod m. Observe that this protocol satisfies conditions (3) and (4), so it is an SP (with simultaneous moves, however).

8. Some open questions. Our results do not cover the case of three players completely: there is no SP in general but there is a DP always. This does not say much of a correlated equilibrium, for instance. Yet there is a possibility for the following. Call a DP a *positive protocol* if it satisfies condition (3) and such that every unilateral deviation from the rules is detected with positive probability. The first open question is this: Is there a positive protocol for three players (with rational probability distribution)? An affirmative answer would imply a weaker version of Theorem 6 in case of three players.

Another question of interest is whether the technical condition on the rationality of p can be removed. More precisely, is Theorem 1 true for arbitrary distributions?

The last question is this. Let G_0 be a noncooperative n-person game, $n \geq 4$. Does there exist a "universal" direct communication game G extending G_0 and containing all correlated equilibria of G_0 as Nash equilibrium of G?

Acknowledgements. My thanks are due to Jean François Mertens and to Françoise Forges for raising the problem, for several inspiring discussions and for pointing out some errors in an earlier version of this paper.

References

[1] Aumann, R. J. (1974). Subjectivity and Correlation in Randomized Strategies. *J. Math. Economics* **1** 67–96.

[2] ______ (1987). Correlated Equilibrium as an Expression of Bayesian Rationality. *Econometrica* **55** 1–18.

[3] ______, Maschler, M. and Stearns, R. E. (1968). Repeated Games of Incomplete Information: An Approach to the Non-zero-sum Case. Report to the U.S. Arms Control and Disarmament Agency, Contract S. T. 143, prepared by Mathematica Inc., Princeton, NJ.

[4] Bárány, I. and Füredi, Z. (1983). Mental Poker with Three or More Players. *Information and Control* **59** 84–93.

[5] Blum, M. (1983). How to Exchange (Secret) Keys. *ACM Trans. Computer Systems* **1** 175–193.

[6] Forges, F. (1988). Can Sunspots Replace a Mediator? *J. Math. Economics* **17** 347–368.

[7] ______ (1990). Universal Mechanisms. *Econometrica.*

[8] Goldwasser, S. and Micali, S. (1982). Probabilistic Encryption and How to Play Mental Poker Keeping all Partial Information Secret. Proc. 14th ACM STOC Meeting, San Francisco, CA, 365–377.

[9] Rivest, R. L., Shamir, A. and Adleman, L. L. (1978). A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Comm. ACM* **21** 120–126.

DEPARTMENT OF MATHEMATICS, UNIVERSITY COLLEGE LONDON, GOWER STREET, LONDON, UNITED KINGDOM