INFORMATION AND CONTROL 59, 84–93 (1983)

Mental Poker with Three or More Players

IMRE BÁRÁNY*

C.O.R.E. Université Catholique de Louvain, Belgium

AND

ZOLTÁN FÜREDI

Mathematical Institute of the Hungarian Academy of Sciences, Budapest, Hungary

A protocol is given which deals cards to three or more players in a fair way. Some related questions are also discussed.

1. INTRODUCTION

Four players want to play poker. This is not a mathematical problem yet. But suppose they can only communicate by telephone, i.e., they can send messages and not real playing cards to each other. The first problem they meet is how to deal the cards in a fair way using messages only.

To solve this problem, they exchange a sequence of messages according to some agreed-upon procedure, called the protocol. This may require them to use some randomizing devices to compute the next message or their hands, etc. At the end of the protocol each player must know which cards are in his hand but must not have any information about which cards are in the other players' hands and in the remaining deck. The protocol should also ensure that the hands are disjoint and that the deal is fair in the usual sense. (We will have more to say about this point later.) Moreover, at the end of the game, each players must be able to check that the deal was indeed fair and that no player has cheated.

This problem originates from D. Grigoriev (Matiasevitch, 1982). It was solved by him, and also by Yu. Matiasevitch (Matiasevitch, 1982). Their solution works for bridge, i.e., the protocol deals the 52 cards to four players, 13 cards to each. In this paper we give another solution which works in a more general situation, for instance, for poker when, during the

* This research was partly done while the author was visiting C.O.R.E., Université Catholique de Louvain, Belgium.

0019-9958/83 $3.00

game, the players may want to draw new cards from the remaining deck. They will be able to do so without obtaining any information on the other players' hands and the remaining deck.

Mental poker with two players has recently been investigated in several papers: Adleman, Rivest, and Shamir (1981), Goldwasser and Micali (1981), and Lipton (1981). We mention two results.

THEOREM A (Adleman *et al.*, 1981). *There is no fair-dealing protocol for two players.*

THEOREM B (Adleman *et al.*, 1981; Goldwasser and Micali, 1981). *There is a fair-dealing potocol for two players is the thinking time of the players is bounded (and some problems are indeed computationally intractable).*

We do not go into details about this second result because our dealing protocol (for three or more players) is provably fair without any assumption on intractability. This protocol works because each player gets "partial information," sufficient to compute his hand but insufficient to determine the whereabouts of any card which is not in his hand.

2. Assumptions and Results

Let L denote the set of cards in which each card is identified with one of the numbers $1, 2,..., |L|$. The players are $P_1, P_2,..., P_n$, their hands are $L_1, L_2,..., L_n$. Set $k_i = |L_i|$ and $k = |L|$. Of course, $\sum_{i=1}^{n} k_i \leqslant k$.

We make two assumptions about the possible behaviour of the players:

(A1) The players do not form coalitions.

(A2) There is a perfectly secure secret channel between every pair of players.

A dealing protocol works in the following way. At the beginning of the kth step, the information known to players P_i $(i = 1,..., n)$ consists of the set of messages $M_i^{(k)}$ he obtained or transmitted so far and the random choices $\xi_i^{(k)}$ he made so far. This information plus the rules of the protocol determine uniquely which player P_i is to be active in the kth step and what exactly he should do: He has to make a new random choice ξ and using $M_i^{(k)}$, $\xi_i^{(k)}$, ξ he has to compute either a card in his hand or his next message and transmit it to player P_j (who is again uniquely determined by $M_i^{(k)}$, $\xi_i^{(k)}$, ξ, and the rules of the protocol). The dealing protocol should also include a stopping rule.

Let us denote by ξ_i and M_i the set of all random choices made by P_i and the set of messages obtained or transmitted by P_i, respectively, during the

protocol. Once the random choices $\xi_1,\ldots,\xi_n$ have been made, $M_1,\ldots,M_n$ are determined uniquely though M_i depends on ξ_j $(j\neq i)$ through M_j only. In this sense, every M_i is a random variable composed from the random variables $\xi_1,\ldots,\xi_n$. Similarly, L_i is determined by ξ_i and M_i so L_i is a random variable composed from $\xi_1,\ldots,\xi_n$.

DEFINITION 1. A deal is *good* if the hands are pairwise disjoint.

DEFINITION 2. A dealing protocol is *fair* if

(1) It always produces good deals,

(2) all possible partitions of L into $L_1,\ldots,L_n$, $L\setminus\bigcup_{i=1}^n L_i$ are equally likely (where $|L_i|=k_i$, $i=1,\ldots,n$),

(3) for every player P_i, for every M_i, all possible partitions of $L\setminus L_i$ into $L_1,\ldots,L_{i-1},L_{i+1},\ldots,L_n$, $L\setminus\bigcup_{j=1}^n L_j$ are equally likely (again $|L_j|=k_j$, $j=1,\ldots,n$),

(4) "afterward checking" is possible, i.e., when the game is over, each player can prove by revealing his random choices that he sent his messages according to the rules of the protocol and his hand L_i was what it has to be according to these rules.

As an example of a "nongood" dealing protocol suppose that every player picks (randomly) his own hand L_i from L. In this case, of course, $L_i\cap L_j\neq\varnothing$ can happen. As an example of a good but unfair protocol suppose that the two players split the 52 cards into two groups of 26 cards and then each of them picks five cards from his group.

Now we can state the main result of this paper.

THEOREM 1. *For three or more players there exists a fair dealing protocol.*

For the proof we will give a protocol that deals the cards one-by-one, thus it solves the problem of how to draw new cards from the remaining deck.

As a matter of fact, we expect more from afterward checking then condition (4) requires. Namely, that L_i is determined uniquely by M_i, the set of messages obtained or given by P_i. If this were not the case, i.e., P_i could have two hands L_i and L_i' with the same M_i, then he could choose his hand to be L_i or L_i' according to his preferences, or during the game, when some other players revealed some of their cards. But we do not have to postulate this in (4) because it follows from (1) and (3).

LEMMA 2. *Conditions* (1) *and* (3) *assure that* M_i *determines* L_i *uniquely.*

This lemma implies Theorem A at once:

THEOREM 3. *For two players, conditions* (1) *and* (3) *are contradicting, so there is no fair-dealing protocol for two players.*

To see this, we mention that in case of two players M_1 is known to P_2 and consequently, L_1 is known to P_2 contradicting (3). However, the actual computation of L_i from M_i (without the knowledge of ξ_i) might be very time-consuming. This is what the proof of Theorem B is based upon.

We mention here that for $n \geqslant 3$ conditions (1) and (3) of Definition 2 imply condition (2). To see this let L_2' and L_3' be obtained from L_2 and L_3 by exchanging one card of L_2 to one card of L_3. Then

$$\begin{aligned}\text{Prob}(L_1,\ldots, L_n) &= \text{Prob}(L_2, L_3, L_4,\ldots, L_n \mid L_1)\,\text{Prob}(L_1)\\ &= \text{Prob}(L_2', L_3', L_4,\ldots, L_n \mid L_1)\,\text{Prob}(L_1)\\ &= \text{Prob}(L_1, L_2', L_3', L_4,\ldots, L_n).\end{aligned}$$

It is clear that using a sequence of such or similar exchanges one can reach any deal from the fixed deal $L_1,\ldots, L_n$.

Theorem 3 does not rule out the following possibility. Suppose the two players have already got their hands somehow (they picked them randomly, say) but that they do not know if the hands are disjoint or not. So they are to construct a "goodness-checking protocol," or checking protocol, for short. Of course they want it to be fair.

DEFINITION 3. A checking protocol is fair, if

(1c) it claims "the deal is good" if and only if it is good,

(3c) in case of a good deal, for every player P_i, for every M_i, all possible partitions of $L \backslash L_i$ into $L_1,\ldots, L_{i-1}, L_{i+1},\ldots, L_n$, $L \backslash \bigcup_{j=1}^{n} L_j$ are equally likely (where $|L_j| = k_j, j = 1,\ldots, n$),

(4c) afterward checking is possible, i.e., when the protocol is finished (or after the game) each player can prove by revealing his random choices and his hand that he sent his messages according to the rules of the protocol.

Once again, we expect more from afterward checking than (4c) requires, namely, that L_i is determined by M_i uniquely provided the deal is good. But this follows from (1c) and (3c):

LEMMA 4. *Conditions* (1c) *and* (3c) *assure that M_i determines L_i uniquely, if the deal is good.*

THEOREM 5. *There is no fair checking protocol for two players.*

THEOREM 6. *For three or more players there exists a fair checking protocol.*

The last theorem gives a nondeterministic fair dealing protocol for three or more players: every P_i picks his hand L_i randomly and then, using the protocol of Theorem 6 they check if the hands are disjoint or not. However, the expected number of iterations can be very large, and even more significantly, there is no way of checking that the players selected their hands randomly.

3. Proofs

It is perhaps instructive to start with the proof of Theorem 6.

Proof of Theorem 6. A code κ is a permutation of the cards L. It is enough to show how to check if L_i and L_j are disjoint or not. For this end P_i and P_j agree upon a (random) code which is known only to them, and send their encoded hands $\kappa(L_i)$ and $\kappa(L_j)$ to some P_k $(k \neq i, j)$. P_k determines if $\kappa(L_i) \bigcap \kappa(L_j)$ is empty (or not) and sends the messages "P_i and P_j have disjoint hands" (or "the deal is not good") to every other player.

Proof of Lemma 2. If $\sum_{i=1}^{n} |L_i| = |L|$, then M_i determines L_i uniquely because for any L_i' different from L_i the deal cannot be good. If $\sum_{i=1}^{n} |L_i| < |L|$, then let L_i and L_i' be two hands for P_i consistent with his messages M_i. By (1), no other player can have card from $L_i \cup L_i'$, contradicting (3).

Proof of Lemma 4. This is identical with the previous proof. The only thing we have to mention is that each M_i includes the message "the deal is good."

Proof of Theorem 1. We describe the protocol in the following form. Suppose players $P_1,..., P_n$ have their hands $L_1,..., L_n$. $(L_1 = \cdots = L_n = \varnothing$ can be the initial step of the protocol.) We suppose further that $L_i \cap L_j = \varnothing$ and that the players do not know anything about the other players' hands. We denote P_n by Q, P_{i+1} is just P_1 if $i = n - 1$. Greek letters will stand for a code of L, i.e., for a permutation of $L = \{1,..., |L|\}$. So $\kappa: L \to L$ is a bijection with inverse κ^{-1}, $\kappa(j)$ denotes the κ-code of card j.

Step 1. P_i chooses a random κ_i $(i = 1,..., n - 1)$, Q chooses a random code π.

Step 2. P_i transmits κ_i to Q $(i = 1,..., n - 1)$, Q transmits $\kappa_i \pi^{-1}$ to P_{i+1} $(i = 1,..., n - 1)$.

Step 3. P_i transmits $\kappa_i(L_i)$ to P_{i+1} $(i = 1,..., n - 1)$.

At this moment, P_{i+1} knows not only the κ_i-code of L_i but its π-code as well because $(\kappa_i \pi^{-1})^{-1}(\kappa_i(L_i)) = \pi(L_i)$.

Step 4. P_{i+1} transmits $\pi(L_i)$ to P_j $(j = 1,..., n-1, j \neq i+1)$, transmits $\pi(L_n)$ to P_i $(i = 1,..., n-1)$.

At this stage players $P_1,..., P_{n-1}$ know every player's hand in π-code. All known information is summed up like this:

$$\begin{aligned}
&P_1 \text{ knows } \kappa_1, \kappa_{n-1}\pi^{-1}, \pi(L_1),..., \pi(L_{n-1}), \pi(L_n), L_1\\
&\vdots\\
&P_i \text{ knows } \kappa_i, \kappa_{i-1}\pi^{-1}, \pi(L_1),..., \pi(L_{n-1}), \pi(L_n), L_i\\
&\vdots\\
&P_{n-1} \text{ knows } \kappa_{n-1}, \kappa_{n-2}\pi^{-1}, \pi(L_1),..., \pi(L_{n-1}), \pi(L_n), L_{n-1}\\
&Q \text{ knows } \kappa_1,..., \kappa_{n-1}, \pi, L_n.
\end{aligned}$$

If the protocol is initialized with $L_1 = \cdots = L_n = \varnothing$, Steps 3, 4 are omitted. Then the tableau can be built up using Steps 1, 2 and the following "dealing" steps.

Now Q wants to draw a new card from the remaining deck. He will get it from P_1 (see Fig. 1).

Step 5a. P_1 chooses $j \in \pi(L) \backslash \bigcup_{i=1}^{n} \pi(L_i)$ and transmits j to every other player.

Then Q computes his new card as $\pi^{-1}(j)$ and sets $L_n \leftarrow L_n \cup \{\pi^{-1}(j)\}$, and every other player sets $\pi(L_n) \leftarrow \pi(L_n) \cup \{j\}$.

Now P_i wants to draw a new card, he gets it from P_{i+1} (Fig. 2).

Step 5b. P_{i+1} chooses $j \in \pi(L) \backslash \bigcup_{l=1}^{n} \pi(L_l)$ and transmits it to every other player except for Q. P_{i+1} transmits $\kappa_i \pi^{-1}(j)$ to P_i.

Then every P_j sets $\pi(L_i) \leftarrow \pi(L_i) \cup \{j\}$ and P_i himself computes his new card as $\pi^{-1}(j) = \kappa_i^{-1}(\kappa_i \pi^{-1}(j))$ and sets $L_i \leftarrow L_i \cup \{\pi^{-1}(j)\}$.

This protocol clearly yields disjoint hands. It is also evident that it satisfies condition (4) of Definition 2. So it suffices to show that condition (3) holds as well because, as we have seen, it implies condition (2) if $n \geqslant 3$.

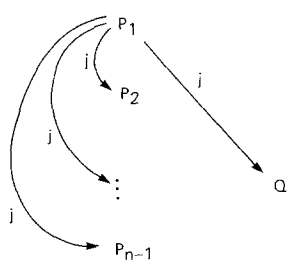

FIGURE 1

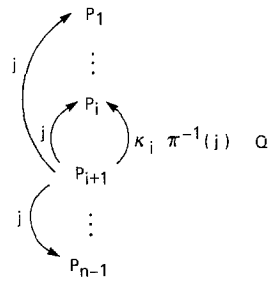

FIGURE 2

Define $J_i = \pi(L_i)$ $(i = 1,..., n)$. Actually J_i is the set of numbers chosen in step 5 by some player, namely by P_1 if $i = n$ or $n-1$ and P_{i+1} otherwise. So each J_i is a random variable. Denote the actual values of the random variables L_i, J_i, $\kappa_{n-1}\pi^{-1}$ by $\bar{L}_i$, $\bar{J}_i$, and $\bar{\rho}$, respectively.

We consider first (and mainly) the case $i = 1$. Observe that the information known to P_1 is $L_1 = \bar{L}_1$, $J_1 = \bar{J}_1$, $J_2 = \bar{J}_2$,... $J_n = \bar{J}_n$, $\kappa_1 = \bar{\kappa}_1$, $\kappa_{n-1}\pi^{-1} = \bar{\rho}$. Then

$$\text{Prob}(L_2 = \bar{L}_2, L_3 = \bar{L}_3,..., L_n = \bar{L}_n \mid \xi_1, M_1) = \frac{\text{Prob}(L_i = \bar{L}_i, J_i = \bar{J}_i\ (i = 1,..., n), \kappa_1 = \bar{\kappa}_1, \kappa_{n-1}\pi^{-1} = \bar{\rho})}{\text{Prob}(L_1 = \bar{L}_1, J_i = \bar{J}_i\ (i = 1,..., n), \kappa_1 = \bar{\kappa}_1, \kappa_{n-1}\pi^{-1} = \bar{\rho})}.$$

Here the denominator is equal to

$$D = \sum_{\pi} \text{Prob}(L_i = \bar{L}_i, J_i = \bar{J}_i\ (i = 1,..., n), \kappa_1 = \bar{\kappa}_1, \kappa_{n-1}\pi^{-1} = \bar{\rho} \mid \pi)\ \text{Prob}(\pi),$$

where the summation is taken over all codes π with $\bar{J}_i = \pi(\bar{L}_i)$ $(i = 1,..., n)$, so

$$D = \sum_{\substack{\pi:\, \bar{J}_i = \pi(\bar{L}_i) \\ i = 1,\ldots,n}} \text{Prob}(J_i = \bar{J}_i\ (i = 1,..., n), \kappa_1 = \bar{\kappa}_1, \kappa_{n-1} = \bar{\rho}\pi \mid \pi)\ \text{Prob}(\pi).$$

Similarly, the numerator can be written as

$$N = \sum_{\pi:\, \bar{J}_1 = \pi(\bar{L}_1)} \text{Prob}(J_i = \bar{J}_i\ (i = 1,..., n), \kappa_1 = \bar{\kappa}_1, \kappa_{n-1} = \bar{\rho}\pi \mid \pi)\ \text{Prob}(\pi).$$

As all terms of the last two sums are the same because of the independence of the random variables J_i, κ_i, and π, we have

$$\text{Prob}(L_2 = \bar{L}_i,..., L_n = \bar{L}_n \mid \xi_1, M_1) = \frac{D}{N} = \frac{|\{\pi: \bar{J}_i = \pi(\bar{L}_i)\ (i = 1,..., n)\}|}{|\{\pi: \bar{J}_1 = \pi(\bar{L}_1)\}|} = \frac{k_1! \cdots k_n!(k - \sum_1^n k_i)!}{k_1!(k - k_1)!}.$$

Thus we have checked condition (3) for P_1. For reasons of symmetry this condition holds for $P_2,\ldots, P_{n-1}$ as well. To check it for $P_n = Q$ is similar and is left to the reader.

So the protocol given above is fair in the sense of Definition 2. But we can prove more about it. For $l \in L$ and $k = 1,\ldots, n$, let us call $l \in L_k$ or $l \notin L_k$ an "elementary event," and let A and B be two events formed from some elementary events using the operations of conjunction or disjunction. Fix $i \in \{1,\ldots, n\}$ and assume that B is consistent with the event $L_i = \bar{L}_i$. Then

$$\text{Prob}(A \mid B, \xi_i, M_i) = \text{Prob}(A \mid B, L_i = \bar{L}_i),$$

where the first probability measure comes from the above protocol and the second one comes from the usual shuffling of the cards which is assumed to be perfect. The meaning of this equality is that for P_i, ξ_i and M_i do not contain more information on the deal than L_i, even it it has been revealed to him somehow that some cards $l_1,\ldots, l_r$ are (or are not) in some other players' hand. This can actually happen during the game.

The proof of this fact is not difficult but a bit technical and is, therefore, omitted.

We observe further that this equality implies condition (3) of Definition 2 and, as a matter of fact, it ought to hold in any protocol which is "fair in common sense."

Finally, we mention that the number of messages in this protocol is $O(|L| \cdot n)$.

4. Some Remarks on Bridge

In the game of bridge four players, North, South, East, and West get 13 cards each in the deal and then E and W play against S and N. Suppose they use the protocol of Theorem 1, then E and W (and S and N) can directly communicate with each other, so they can send their partners extra information on their random choices, hands and so on. Actually, by Theorem 3, if N and S form a coalition during the dealing protocol and so do E and W, then there is no fair dealing protocol.

This difficulty can be removed by the further "splitting" of the messages. We still use the protocol of Theorem 6. Suppose that, according to that protocol, S has to send a message, a permutation π, say, to N (see Fig. 3).

Then S chooses a random permutation α, computes $\beta = \alpha^{-1}\pi$ and transmits α to W and β to E. W sends α and E sends β to N who computes π as $\pi = \alpha\beta$.

This method does not give any extra information to W and E, but S may choose α so that α and β give more information to N than π. To avoid this

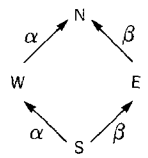

FIGURE 3

possibility we make some assumptions on the behaviour of the players. Let $P_1,\ldots,P_n$ be the players and suppose that a graph G is given with vertex set $P_1,\ldots,P_n$. G is the graph of the "permitted communications." Now we assume

(A1) the players do not form coalitions,

(A3) there is a perfectly secure secret channel between P_i and P_j if and only if P_iP_j is an edge of G.

In this model we have

THEOREM 7. *There is a fair dealing protocol if and only if G is doubly connected.*

A sketch of the *proof*. The if part follows from Menger's theorem (see Lovász, 1979) using the same method as in bridge. The *only if* part is similar to the proof of Lemma 2: Assume G is not doubly connected and still there is a fair dealing protocol. Then the deletion of a vertex, P_1 say, produces (at least) two connected components, C_1 and C_2. Then one can prove in the same way as in Lemma 2 that M_1 determines uniquely the sets $L^{(1)} = \bigcup \{L_i : P_i \in C_1\}$ and $L^{(2)} = \bigcup \{L_i : P_i \in C_2\}$. This contradicts to condition (3) of Definition 2.

Finally we mention that one can further enlarge the class of graphs of permitted communications if a set of "pre-protocol communication" can take place. For instance, in the case of bridge E and W previously (i.e., before the dealing protocol started) agreed upon a secret permutation γ. Now S wants to send π to N, so he writes $\pi = \alpha\beta$ (where α is a random permutation) and sends α to W and β to E. Then W sends $\alpha\gamma$ to N and E send $\gamma^{-1}\beta$ to N who computes π as $(\alpha\gamma)(\gamma^{-1}\beta) = \alpha\beta = \pi$ (see Fig. 4).

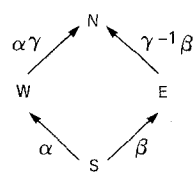

FIGURE 4

ACKNOWLEDGMENTS

We are indebted to L. Babai and L. Lovász for several inspiring discussions. They improved this paper a great deal.

RECEIVED: July 1, 1983; ACCEPTED: December 28, 1983

REFERENCES

ADLEMAN, L., RIVEST, R., AND SHAMIR, A. (1981), Mental poker, *in*: "The Mathematical Gardner" (D. A. Klarner, Ed.), Wadsworth International.

GOLDWASSER, S., AND MICALI, S. (1981), Probabilistic encryption and how to play mental poker keeping secret all partial information, *in* "Proc. 14th ACM STOC Meeting," pp. 365–377, San Francisco, 1982.

LIPTON, R. (1981), Proceedings of the AMS short course in cryptology.

LOVÁSZ, L. (1979), "Combinatorial Problems and Exercises," North-Holland, New York.

MATIASEVITCH, YU. (1982), Private communication.