GAMES AND ECONOMIC BEHAVIOR 1, 80–93 (1989)

Nash and Correlated Equilibria: Some Complexity Considerations

ITZHAK GILBOA AND EITAN ZEMEL

Department of Managerial Economics and Decision Sciences, J. L. Kellogg Graduate School of Management, Northwestern University, Evanston, Illinois 60208

This paper deals with the complexity of computing Nash and correlated equilibria for a finite game in normal form. We examine the problems of checking the existence of equilibria satisfying a certain condition, such as "Given a game G and a number r, is there a Nash (correlated) equilibrium of G in which all players obtain an expected payoff of at least r?" or "Is there a unique Nash (correlated) equilibrium in G?" etc. We show that such problems are typically "hard" (NP-hard) for Nash equilibria but "easy" (polynomial) for correlated equilibria.
© 1989 Academic Press, Inc.

1. INTRODUCTION

1.1. *Motivation*

Game-theoretic solution concepts may be theoretically interpreted and practically applied in numerous ways and in a variety of contexts. For some of these interpretations, the complexity of computing the equilibrium may be absolutely irrelevant. For instance, one may think of a Nash equilibrium as a condition which must be satisfied by any steady state in a certain dynamic biological system. Such an application may be supported without assumptions on the players' rationality and, more specifically, without assuming that any of them "computed" the equilibrium.

However, there is a large class of applications—especially in economic theory—which does implicitly assume that a rational decision maker is faced with the technical problem of computing equilibria. For instance, whenever the Nash equilibrium concept is interpreted as a self-enforcing

0899-8256/89 $3.00
Copyright © 1989 by Academic Press, Inc.
All rights of reproduction in any form reserved.

agreement among rational players, which is attained by negotiation or suggested to them by another party or even read by the players from a certain "game theory guide," it is implicitly assumed that someone computes Nash equilibria. This "someone" may be the players themselves, or the "other party," or the "game theory guide" author. At any rate, this "someone" is not an omniscient superbeing—it eventually turns out to be a person or a machine for which bounded rationality considerations and computational restrictions do apply.

We therefore believe that the complexity of computing a certain solution concept is one of the features determining its plausibility for a whole range of theoretical and practical applications.

This paper deals with two of the most widely used solution concepts for noncooperative games: the Nash equilibrium (introduced by Nash (1951)) and the correlated equilibrium (introduced by Aumann (1974)). The main results, given in the next subsection, may be summarized, in very bold strokes, as saying that Nash equilibrium is a complicated solution concept, whereas correlated equilibrium is a simple one.

Related results, also demonstrating the computational difficulties associated with Nash equilibria, are contained in Gilboa (1988) and Ben Porath (1988).

In Section 2 we present some preliminaries and provide the basic definitions. The proofs are in Section 3. Section 4 is devoted to some technical remarks.

1.2. *The Results*

Assuming familiarity with the standard definitions quoted in Section 2, we may state our main results. We first define the problems.

In the following definitions, the word "game" should be interpreted as a finite game with rational payoffs given in its normal form. Each definition relates to two problems—one for Nash equilibrium (NE) and one for correlated equilibrium (CE):

(1) *NE (CE) max payoff:* Given a game G and a number r, does there exist a NE (CE) in G in which each player obtains the expected payoff of at least r?

(2) *NE (CE) uniqueness:* Given a game G, does there exist a unique NE (CE) in G?

(3) *NE (CE) in a subset:* Given a game G and a subset of strategies T_i for each player i, does there exist a NE (CE) of G in which all strategies not included in T_i (for each i) are played with probability zero?

(4) *NE (CE) containing a subset:* Given a game G and a subset of strategies T_i for each player i, does there exist a NE (CE) of G in which every strategy in T_i (for every player i) is played with positive probability?

TABLE I

	NE	CE
Max payoff	NP-hard[a]	P
Uniqueness	NP-hard[b]	P
In a subset	NP-hard[a]	P
Containing a subset	NP-hard[a]	P
Maximal support	NP-hard[a]	P
Minimal support	NP-hard[a,d]	NP-hard[c,d]

[a] NP-complete for two players.
[b] CoNP-complete for two players.
[c] NP-complete for any number of players.
[d] NP-hard even for zero-sum games.

(5) *NE (CE) maximal support:* Given a game G and an integer $r \geq 1$, does there exist a NE (CE) of G in which each player uses at least r strategies with positive probability?

(6) *NE (CE) minimal support:* Given a game G and an integer $k \geq 1$, does there exist a NE (CE) of G in which each player uses no more than k strategies with positive probability?

THEOREM. (a) *The following problems are NP-hard (NPH): NE max payoff, NE uniqueness; NE in a subset, NE containing a subset, NE maximal support, NE minimal support, CE minimal support.*

(b) *The following problems are of polynomial time complexity (P): CE max payoff, CE uniqueness, CE in a subset, CE containing a subset, CE maximal support.*

These results may be summarized in Table I.

2. Preliminaries

2.1. *Game Theory Definitions*

A *game* (to be precise, a noncooperative game in normal form) is a triple $(N, (S^i)_{i \in N}, (h^i)_{i \in N})$ where N is a nonempty set (of *players*), S^i is a nonempty set (of *strategies* of player i) for every $i \in N$, and h^i: $S \rightarrow \mathbb{R}$ for every i, where $S \equiv \Pi_{i \in N} S^i$ (h^i is the *payoff function* of player i). A game $G = (N, (S^i)_{i \in N}, (h^i)_{i \in N})$ is called *finite* if the set N and all sets $(S^i)_{i \in N}$ are finite. We will henceforth discuss only finite games. Since we are interested in computational issues, we will also assume that the game data are *rational,* i.e., h^i: $S \rightarrow Q$ rather than $S \rightarrow R$.

Given a finite game $G = (N, (S^i)_{i \in N}, (h^i)_{i \in N})$ in which we assume, without loss of generality, that $N = \{1, \ldots, n\}$, we define the (mixture) *extension* of G to be the game $\overline{G} = (N, (\Sigma^i)_{i \in N}, (H^i)_{i \in N})$ where:

(1) Σ^i is the set of all probability vectors over S^i (the set of *mixed strategies* of player i);

(2) For every $\sigma = (\sigma^1, \sigma^2, \ldots, \sigma^n) \in \Sigma \equiv \Pi_{i=1}^n \Sigma^i$ we define a measure P_σ on S by $P_\sigma(s) = \Pi_{i=1}^n \sigma^i(s^i)$ where $s = (s^1, s^2, \ldots, s^n)$, and $H^i(\sigma)$ is the expected payoff to player i according to P_σ, i.e.,

$$H^i(\sigma) = \Sigma_{s \in S} P_\sigma(s) h^i(s).$$

An n-tuple of mixed strategies $\bar{\sigma} = (\bar{\sigma}^1, \bar{\sigma}^2, \ldots, \bar{\sigma}^n) \in \Sigma$ is called a *Nash equilibrium* of G (in mixed strategies) if the following condition holds for every $i \in N$ and $\sigma^i \in \Sigma^i$:

$$H^i(\bar{\sigma}) \geq H^i(\bar{\sigma}^1, \bar{\sigma}^2, \ldots, \bar{\sigma}^{i-1}, \sigma^i, \bar{\sigma}^{i+1}, \ldots, \bar{\sigma}^n).$$

That is to say, $\bar{\sigma}$ is a Nash equilibrium if no player can increase his/her expected payoff by a unilateral deviation from the (equilibrium) strategy suggested for him/her by $\bar{\sigma}$.

Nash (1951) has shown that every finite game has a Nash equilibrium in mixed strategies as above. The proof uses topological arguments (Brauer's fixed point theorem); to the best of our knowledge, there is no "elementary" proof of this fact. Hence it seems unlikely that the existing proofs of existence will be used to develop a polynomial algorithm for the computation of Nash equilibria, although they may give some insight into the development of iterative algorithms which, in turn, may prove useful for practical purposes (see, for instance, Samuelson, 1988).

We now turn to correlated equilibria. In these, it is assumed that the players have some randomization device they may all observe simultaneously. Hence any probability distribution on S may now be considered a solution of the game, rather than the smaller set of distributions which are the product of independent marginal distributions. A *correlated equilibrium* is therefore defined to be a probability distribution p on S which satisfies the following condition:

For every $s = (s_1, s_2, \ldots, s_n) = (s^1_{j_1}, s^2_{j_2}, \ldots, s^n_{j_n}) \in S$ such that $p(s) > 0$, for every player $i \in N$ and for every strategy $\bar{s}^i \in S^i$,

$$\Sigma_{\{s \in S | s_i = s^i_{j_i}\}} p(s) h^i(s) \geq \Sigma_{\{s \in S | s_i = s^i_{j_i}\}} p(s) h^i(s^1_j, \ldots, \bar{s}^i, \ldots, s^n_{jn}).$$

The intuition which stands behind this definition is the following. Suppose an $(n + 1)$st party chooses each $s \in S$ with probability $p(s)$ and reveals to each player only his/her component s_i of s. Given this information, and assuming that the other players will play the strategy "recommended" to them by the $(n + 1)$st party, player i has a conditional probability regarding the other players' choices. It is required that the strategy "recommended" to player i, that is, $s^i_{j_i}$, will be optimal for him/her given this conditional probability.

Aumann (1974), who introduced the concept of correlated equilibria, also noted that every Nash equilibrium in mixed strategies induces a correlated equilibrium defined by the product of the players' mixed strategies. This also implies that for every game there are correlated equilibria. However, Hart and Schmeidler (1986) noted that correlated equilibria are defined by a finite set of linear inequalities, and showed (without using Nash's result) that the feasible set induced by these inequalities is nonempty for all games. (Their result also deals with games with an infinite number of players, for which there is no Nash equilibrium in general.) In fact, all the results presented in this paper, which prove that a certain CE problem is easy, use this observation and that linear programming problems can be solved in polynomial time.

2.2. *Computer Science Definitions*

Unfortunately, we cannot provide succinct and formal definitions for all the terms we will use. For the sake of brevity, we will provide only short and intuitive explanations, and the interested reader is referred to Aho *et al.* (1974) and Garey and Johnson (1979) for formal definitions.

By *problem* we refer to a YES/NO problem, i.e., a function $A(\cdot)$ from the set of inputs to the set {YES,NO}. An *instance* of a problem is a given input. The *size*, $|x|$, of an instance x is the number of digits in the encoding of x.

An *algorithm* T is a well-defined set of instructions which may be identified with a Turing machine and thought of as a computer program with a specific output state denoted YES. Let T_1 be the set of inputs such that T, when given x, reaches the output state YES within a finite number of steps. In that case, the number of steps is called the *running time* of T on x.

An algorithm T is said to *solve the problem* A if $T_1 = \{x\colon A(x) = \text{YES}\}$; i.e., it reaches the state YES precisely on the correct set of inputs. The computational complexity of T, $c(n)$, is the maximum running time, over all inputs $x \in T_1$ such that $|x| \leq n$. Note that this definition is *not symmetric* with respect to replacing YES by NO. We will focus on the order of magnitude of $c(n)$, rather than on the function itself. More specifically, we will be interested in the existence of "polynomial algorithms," that is, algorithms for which the time complexity $c(n)$ is bounded from above by some polynomial of n. The set of all problems for which there exists such an algorithm is denoted by P. Most of the well-known optimization problems, such as the traveling salesman problem, the set covering problem, and the knapsack problem, are generally believed to be outside P. Rather, they are known to be in a set containing P, which is called NP.

A problem is called *NP* (or belongs to the class NP) if there is a nondeterministic Turing machine which solves it in polynomial time. One may think of a nondeterministic Turing machine as a computer with an unbounded number of processors working in parallel. Intuitively, a problem A is in NP if one can prove in polynomial time, possibly using a guess, that $A(x)$ = YES. For example, the problem of deciding whether a certain graph contains a Hamiltonian tour is not known to be in P; i.e., we do not know of a polynomial algorithm for it. However, this problem is in NP since we can prove in polynomial time that a given graph is in fact Hamiltonian using a guess that consists of a Hamiltonian tour. Note that the definition does not specify how the tour is obtained. The only polynomial requirement is to be able to check in polynomial time that the presented tour is in fact Hamiltonian.

As noted previously, the definition of running time is not invariant under complementation of YES and NO. The class of problems whose complements are in NP is called CoNP. In other words, a problem A is in CoNP if one can prove in polynomial time that $A(x)$ = NO. Obviously, $P \subseteq$ NP but the question of whether the containment is strict is still open. It is also not known whether or not NP = CoNP. The "evidence" so far suggests a negative answer to both these questions.

On the set of problems one may define the binary relation "is (polynomially) easier than" or "can be polynomially reduced to" as follows. A problem A is easier than B if there is a polynomial algorithm which translates every possible input of A to an input of B, such that all A-inputs for which the A-answer is "YES," and only those, are mapped to B-inputs for which the B-answer is "YES." (In this case, we will also say that B is harder than A.)

A problem in NP which is "harder," in the above sense, than all problems in NP is called *NP-complete* (NPC). The set CoNPC is defined in a similar fashion. Both sets NPC and CoNPC are subsets of a larger set called NP-hard (NPH). For a precise definition of this set (which is based on a more general notion of the "harder than" relation) see Garey and Johnson (1979). However, for our purposes it suffices to recall that if a problem A is harder than an NPH problem, then A itself is NPH. Also, the following conditional statement is true for each problem A in NPH: if there were a polynomial algorithm solving A, there would also be one for every problem in NP and in CoNP. In that case P = NP = CoNP (see Garey and Johnson, 1979, p. 156). For this reason NP-hard problems are considered hard: there are no known polynomial algorithms for them, and it is generally believed that such algorithms are unlikely to exist.

3. Proofs

In this section we provide the proof of our theorem. To each problem we devote a subsection showing whether it is NPH or P. Then, in Subsection 3.13, we show that for the case of two players, the NE problems are in NP except for NE uniqueness which is in CoNP. Finally, we show that minimal support CE is also in NP.

3.1. *NE Max Payoff*

The proof is by reduction of the clique problem, defined as follows. Given an undirected graph Gr = (V, E) and an integer k, does there exist a clique of size k in Gr? That is, does there exist $V' \subseteq V$, $|V'| = k$ such that $\{i, j\} \in E$ for all $i, j \in V'$?

(The clique problem is known to be NPC.)

Given a graph Gr = (V, E) where, without loss of generality, $V = \{1, \ldots, n\}$ and a number k, construct a two-person game G as

$$h^1((1, i), (1, j)) = h^2((1, i), (1, j)) = \begin{cases} 1 + \varepsilon & \text{if } i = j \\ 1 & \text{if } i \neq j, \{i, j\} \in E \\ 0 & \text{otherwise,} \end{cases}$$

where $\varepsilon = 1/nk$,

$$h^1((2, i)), (1, j)) = \begin{cases} k, & i = j \\ 0, & i \neq j \end{cases}$$

$$h^2((2, i), (1, j)) = \begin{cases} -M, & i = j \\ 0, & i \neq j \end{cases}$$

$$h^1((1, i), (2, j)) = \begin{cases} -M, & i = j \\ 0, & i \neq j \end{cases}$$

$$h^2((1, i), (2, j)) = \begin{cases} k, & i = j \\ 0, & i \neq j \end{cases}$$

$$h^1((2, i), (2, j)) = h^2((2, i), (2, j)) = 0,$$

where $M = nk^2$. The game matrix is given in Fig. 1.

CLAIM. *G has a NE with expected payoff of at least $r \equiv 1 + \varepsilon/k$ for both players iff Gr has a clique of size k.*

Proof. First assume that Gr has such a clique, say $\{i_1, i_2, \ldots, i_k\}$. Define mixed strategies p for player 1 and q for player 2 by

$$p_{(1,i_j)} = q_{(1,i_j)} = 1/k \qquad \text{for } 1 \leq j \leq k.$$

It is easy to verify that p and q constitute a Nash equilibrium in which both players obtain the payoff r.

$$
\begin{array}{c|ccc|ccc}
 & (1,1) & \cdots & (1,n) & (2,1) & \cdots & (2,n) \\ \hline
(1,1) & (1+\varepsilon,1+\varepsilon) & & (e_{ij},e_{ij}) & (-M,k) & & (0,0) \\
 & & \ddots & & & \ddots & \\
(1,n) & (e_{ij},e_{ij}) & & (1+\varepsilon,1+\varepsilon) & (0,0) & & (-M,k) \\ \hline
(2,1) & (k,-M) & & (0,0) & & & \\
 & & \ddots & & & (0,0) & \\
(2,n) & (0,0) & & (k,-M) & & &
\end{array}
$$

$e_{ij} = 1_{\{\{i,j\}\in E\}}$

FIGURE 1

Conversely, assume that $p = (p_{(1,1)}, \ldots, p_{(2,n)})$ and $q = (q_{(1,1)}, \ldots, q_{(2,n)})$ are two strategies which form a NE in G, such that the expected payoff of each player is at least r. We want to show that Gr has a clique of size k.

CLAIM 1. *For every* $1 \le i \le n$, $p_{(2,i)}, q_{(2,i)} < 1/nkM$.

Proof. For a given $i \le i \le n$, assume $p_{(2,i)} > 0$. This implies that $E(h^1|(2, i), q) \ge r$. (Here and in the sequel, this expression means the expected payoff of player 1 given that he/she plays the pure strategy $(2, i)$ and that player 2 plays the mixed strategy q. We will also use the obvious variations of this notation.) This is possible only if $q_{(1,i)} > 0$. But by the same argument, the latter implies $E(h^2|p, (1, i)) \ge r$. A simple calculation shows that $p_{(2,i)} < 1/nkM$. The proof for q is symmetric. ■

We now know that most of the probability mass of the mixed strategy of each player is concentrated on the first n strategies. Using this fact we will show that at least k of them are chosen with positive probability:

CLAIM 2. $|\{i|p_{(1,i)} > 0\}|, |\{i|q_{(1,i)} > 0\}| \ge k$.

Proof. Assume the contrary, say $|\{i|q_{(1,i)} > 0\}| < k$. Using Claim 1, this implies that for at least one index $1 \le i \le n$, $q_{(1,i)} > (1 - 1/kM)/(k - 1)$. Simple and not-too-tedious calculations then show that $E(h^1|(2, i), q) > 1 + \varepsilon$. But this is possible only if $p_{(1,j)} = 0$ for all $j \le n$, which is known to be false. ■

CLAIM 3. *For all* $i \le n$, *if* $p_{(1,i)} > 0$ *then* $q_{(1,i)} \ge 1/k$; *and if* $q_{(1,i)} > 0$ *then* $p_{(1,i)} \ge 1/k$.

Proof. Assume $p_{(1,i)} > 0$. The only payoff which exceeds 1 in the $(1, i)$ row is attained in column $(1, i)$. Hence $E(h^1|(1, i), q) \geq r = 1 + \varepsilon/k$ only if $q_{(1,i)} \geq 1/k$. (And the other part is proved symmetrically.) ∎

Combining the conclusions of Claims 2 and 3 we deduce that there are k indices $1 \leq j_1 < j_2 < \cdots < j_k \leq n$ such that $p_{(1,jl)} = q_{(1,jl)} = 1/k$ for $1 \leq l \leq k$. It is now obvious that these indices correspond to a clique of size k in Gr. ∎

3.2. NE Uniqueness

Again we use the clique problem. Given a graph Gr we construct a game G as in Subsection 3.1, only now we add another strategy—say O—to each player. Each player may guarantee himself/herself the payoff r by choosing the strategy O, but if only one of them chooses O, the other one gets the payoff $-M$. Hence (O, O) is certainly a NE. However, there are no Nash equilibria in which either one of the players obtains less than r. We already know from 3.1 that there exists a NE which does not use the strategy pair (O, O), iff there exists a clique of size k. It remains to be seen that there can be no NE which mixes the strategy O with the old strategies. But this can be easily obtained by replicating Claims 1–3 of 3.1. The only modification needed is to note that the conclusion of Claim 1 can be strengthened to $p_{(2,i)} + p_0 < 1/nkM$, and similarly for q. It follows that (O, O) is the unique NE iff the graph Gr *does not* have a clique of size k.

3.3. *NE is a Subset*

Use the construction of Subsection 3.2 and define the subsets to be all strategies (of each player) but the one denoted O.

3.4. *NE Containing a Subset*

The proof uses the clique problem again. Given a graph Gr and a number k, construct a graph Gr′ by adding one vertex which is connected to all the previous ones. Obviously Gr has a clique of size k iff Gr′ has a clique of size $(k + 1)$ which includes the new node. Then construct a game G as described in Subsection 3.2 for the graph Gr′ and the integer $(k + 1)$. This game will have a NE in which the strategy, corresponding to the new node in Gr′, is played with positive probability iff Gr has a clique of size k.

3.5. *NE Maximal Support*

Again, use the construction of 3.2 with $k \geq 2$. If a NE which uses more than one strategy exists, it must correspond to a clique of size k as in 3.2.

3.6. *NE Minimal Support*

In this subsection we will prove a stronger result than originally stated: we will prove that the NE minimal support problem is NPH even if the input is restricted to be a two-person *zero-sum* game. This result will also be used to show that CE-minimal support is also NPH. To this end we need a new construction, and this time we will use the set cover problem, which is also known to be NPC. The version we use is the following.

SET COVER. *Given a number* $n \geq 1$ *and* r *subsets* $T_1, T_2, \ldots, T_r$ *of* $N = \{1, \ldots, n\}$ *such that* $\cup_{1 \leq j \leq r} T_j = N$, *and a number* $k \leq r$, *are there* k *indices* $1 \leq j_1 < j_2 < \cdots < j_k \leq r$ *such that* $\cup_{1 \leq l \leq k} T_{i_j} = N$?

We will now show that set cover can be reduced to the following problem.

ZERO-SUM NE MINIMAL SUPPORT. *Given a two-person zero-sum game* G *and a number* $k \geq 1$, *is there a NE in* G *in which both players use no more than* k *strategies with positive probability*?

Proof. Let there be given an integer $n \geq 1$, r subsets $T_1, \ldots, T_r$ of $N = \{1, \ldots, n\}$ such that $\cup_{1 \leq j \leq r} T_j = N$, and an integer $k \leq r$. Define the following game G:

$$s^1 = \{1, 2, \ldots, r, r + 1\}$$

$$s^2 = \{1, 2, \ldots, n, n + 1\}$$

$$h^1(j, i) = -h^2(j, i) = \begin{cases} 1, & j \leq r,\ i \leq n,\ i \in T_j \\ 0, & j \leq r,\ i \leq n,\ i \notin T_j \\ 1/k, & j \leq r,\ i = n + 1 \\ 1/2r, & j = r + 1. \end{cases}$$

CLAIM. *The set* N *has a cover of size* k *out of* $\{T_1, \ldots, T_r\}$ *iff the game* G *has a NE in which both players do not use more than* k *strategies with positive probabilities.*

Proof of Claim. First assume that G has a NE as required. Consider player 1's strategy given by $p_j = 1/r$ for $1 \leq j \leq r$ (and $p_{r+1} = 0$). This strategy ensures player 1 the expected payoff $1/r$. Hence the pure strategy $r + 1$ is *not* an optimal (maxmin) strategy for player 1 and cannot be played with probability 1 at any equilibrium. Hence, if p and q are the equilibrium strategies of players 1 and 2, respectively, the set $J = \{1 \leq j \leq r | p_j > 0\}$ is nonempty. We claim that $\cup_{j \in J} T_j = N$. Indeed, if the sets $\{T_j\}_{j \in J}$ fail to cover the set N, there exists an $i \in N$ for which $E(h^1 | p, i) < 1/2r$. In this case, p again is not a maxmin strategy for player 1. We then conclude that $\{T_j\}_{j \in J}$ is a cover of N. But our assumption on the Nash equilibrium under consideration implies that $|J| \leq k$. This completes the first half of the proof.

Conversely, assume that there are $1 \leq j_1 < j_2 < \cdots < j_k \leq r$ such that $\cup_{1 \leq l \leq k} T_{j_l} = N$. Let p be a mixed strategy of player 1 defined by $P_{j_l} = 1/k$ for $1 \leq l \leq k$, and let q be player 2's strategy defined *by* $q_{n+1} = 1$. The minimal expected payoff for player 1, should he/she choose p, is $1/k$. This is also the maximal expected loss incurred on player 2 should he/she choose q. Hence these are optimal strategies and they constitute a NE of G. ■

3.7. *CE Minimal Support*

In order to prove that this problem is NPH we will use the proof in Subsection 3.6. The main point is that for zero-sum games the two concepts of equilibria coincide in terms of both the equilibrium payoffs and the strategies which may be used (at equilibrium) with positive probability.

We first note the following.

CLAIM 1. *Let p be a correlated equilibrium in a two-person zero-sum game G. Then $E(h^1|p)$ equals the value of the game V ($\equiv \max_p \min_q E(h^1|p, q) = \min_q \max_p E(h^1|p, q)$).*

Proof. Assume the contrary, e.g., $E(h^1|p) < V$. (The other case is symmetric.) This implies that there are $(i, j) \in S$ such that $p_{ij} > 0$ and

$$\Sigma_j \, (p_{ij}/\Sigma_k p_{ik}) h^1(i, j) < V.$$

By definition, player 1 has an optimal strategy which assures him the payoff V against any strategy of player 2, in particular $(p_{ij}/\Sigma_k p_{ik})_{j \in S^2}$. This strategy may be a mixed one, but there must be at least one pure strategy $l \in S^1$ such that $E(h^1|l, (p_{ij}/\Sigma_k p_{ik})_{j \in S^2}) \geq V$. This implies that p is not a CE. ■

CLAIM 2. *Let p be a CE of a two-person zero-sum game G. Then for every $(i, j) \in S$ such that $p_{ij} > 0$, $(p_{il}/\Sigma_k p_{ik})_l$ and $(p_{mj}/\Sigma_k p_{kj})_m$ are optimal strategies for players 2 and 1, respectively.*

Proof. Let us consider player 2's strategy (the argument for player 1 is, of course, symmetric.) Consider

$$\operatorname*{Max}_{m \in S^1} \Sigma_{l \in S^2} (p_{il}/\Sigma_k p_{ik}) h^1(m, l).$$

Since p is a CE, this maximum is obtained at $m = i$. But Claim 1 shows that the maximal value is then the value of the game V. This is just the definition of a minimax strategy for player 2. ■

The proof will now be completed by the following:

PROPOSITION. *Let there be given a two-person zero-sum G and an integer k. G has a NE in which each player uses no more than k strategies with positive probability iff it has such a CE.*

Proof. The "only if" part is trivial since each NE also constitutes a CE (in which exactly the same strategies are played with positive probability). For the "if" part, assume that there exists such a CE p, and pick a pair $(i, j) \in S$ such that $p_{ij} > 0$. By Claim 2, $(p_{il}/\Sigma_k p_{ik})_l$ and $(p_{mj}/\Sigma_k p_{kj})_m$ are optimal strategies, hence a NE. Obviously, in this NE the strategies which are played with positive probability are also played with positive probability in the CE p. ■

3.8. *CE Maximal Payoff*

In view of the observations in Subsection 2.1, this problem can be transformed into a linear program. It is well known that the latter can be solved in polynomial time.

3.9. *CE Uniqueness*

Given the set of linear constraints on $(p_s)_{s \in S}$ defining a CE in a given game, one may solve two LP problems for each $s \in S$. One of them will have the objective function Max p_s, and the other Min p_s, while both share the same feasible set. Obviously, the constraints define a unique CE iff all these problems have the same solution.

3.10. *CE in a Subset*

This problem is again solved by linear programming where one constrains the appropriate variables to be zero.

3.11. *CE Containing a Subset*

Again, for each $s \in S$, one solves the LP problem defined by the feasible set of CE and the objective function Max p_s. Then one takes the arithmetic average of all solution vectors obtained. Of course, this is a CE since the set of CE is convex. Furthermore, if there exists a CE at which $p_s > 0$ for some $s \in S$, then $p_s > 0$ also in this average solution. Hence, for given sets T_i (for every player i) it only remains to check whether for every $s_j^i \in T_i$ and every $i \in N$ there is an $s = (s^1, s^2, \ldots, s_j^i, \ldots, s^n)$ with $p_s > 0$. (Note that this may be carried out in time complexity which is polynomial in the size of the game.)

3.12. *CE Maximal Support*

Identical to 3.11.

3.13. *Membership in NPC and CoNPC*

We briefly show here that for two players the NE problems are in NP except for uniqueness which is in CoNP. Then we show that CE minimal support is also NPC for any number of players.

We start by analyzing NE for two players. In this case, each NE is a solution to a polynomial set of linear equalities involving the (rational) matrices h^1 and h^2 as coefficients. Specifically, once one has "guessed" the support of the equilibrium strategies, the equilibrium conditions turn out to be linear inequalities in the corresponding variables (each pure strategy played at equilibrium should yield an expected payoff which is at least as high as any other). Furthermore, note that for all the problems under discussion, one may restrict one's attention to basic solutions. It is well known that basic solutions of rational systems are themselves rational, of size polynomial in the original data. Thus, all basic NE for a given game are of polynomial size. This means that if the answer to any of the NE problems is YES, there exists a solution of polynomial size. Also, given an alleged solution of polynomial size, it is easy to verify in polynomial time that it is, in fact, a NE satisfying any of the additional properties such as max payoff, maximal support, etc. For the case of NE uniqueness, we can easily *disprove* this property in polynomial time by presenting a pair of distinct NE. This proves that the NE problems for two players are in NP, except for NE uniqueness, which is in CoNP.

We now consider the case of CE minimal support for any number of players. As mentioned earlier, CE can be presented as a linear programming problem so that its basic solution is of polynomial size. Furthermore, a CE satisfying the minimal support property can be chosen basic. Thus the problem is in NP.

This completes the proof of our main theorem.

4. Some Remarks

4.1. Our results do not imply NP hardness for the problem of computing *any* NE for a given game. (The YES/NO problem which corresponds to this question is the trivial problem of existence of NE.) In fact, Megiddo (1988) has shown that, for the case of two players, the problem is not NP hard unless NP = CoNP, an unlikely event. The problem for the general case is still open.

4.2. All the complexity analysis carried out here referred to the "worst case" complexity of exact algorithms. It is conceivable that problems which are hard with respect to this measure are in fact easy in the "average" case or if approximations, rather than exact algorithms, are concerned. This topic is currently under further study.

4.3. Our results about minimal and maximal support for CE can also be used to show that, for a given general set of linear constraints, it is "easy" to find a solution with the maximal number (or the maximal set) of positive variables, but it is "hard" to find the solution with the minimal number of positive variables.

Acknowledgments

We thank Ehud Kalai, Nimrod Megiddo, Roger Myerson, Dov Samet, and Israel Zang for helpful comments and stimulating discussions.

References

Aho, A. V., Hopcroft, J. E., and Ullman, J. D. (1974). *The Design and Analysis of Computer Algorithms*. Reading, MA: Addison–Wesley.

Aumann, R. J. (1974). "Subjectivity and Correlation in Randomized Strategies," *J. Math Econ.* **1,** 67–95.

Ben Porath, E. (1988). "The Complexity of Computing Best Response Automata in Repeated Games with Mixed Strategies," mimeo.

Garey, N. R., and Johnson, D. S. (1979). *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York: Will, Freeman and Company.

Gilboa, I. (1988). "The Complexity of Computing Best Response Automata in Repeated Games," *J. Econ. Theory* **45,** 342–352.

Hart, S., and Schmeidler, D. (1986). "Correlated Equilibria: An Elementary Proof of Existence," mimeo.

Megiddo, N. (May 1988). *A Note on Complexity of P-Matrix L ⊂ P and Computing an Equilibrium*. IBM Almaden Research Center.

Nash, J. F. (1951). "Non-cooperative Games," *Ann. Math.* **54,** 86–295.

Samuelson, L. (1988). "Evolutionary Foundations of Solution Concepts for Finite, Two-Player, Normal-Form Games," in *Proceedings of the Second Conference on the Theoretical Aspects of Reasoning About Knowledge* (M. Vardi, Ed), pp. 211–225. Los Altos, CA: Morgan-Kaufman.