An Excerpt From: Rational Secure Function Evaluation and Ideal Mechanism Design

Sergei Izmalkov and Matt Lepinski and Silvio Micali

November 22, 2005

1. GAME THEORETIC PRELIMINARIES

In this section we establish the notation used throughout our paper and recall some basic notions of Game Theory. All the games we study are finite games having incomplete information and perfect recall. In recalling these game theoretic notions, we find it useful to "re-assemble" them from the (sub)notions of contexts, mechanisms and game forms.[1]

1.1. *Notation*

We denote by A^L the Cartesian product of a set A with itself L times; by $S|s$ the sequence $s_1, \ldots, s_k, s$ whenever S is the sequence $s_1, \ldots, s_k$; by Σ the set of all finite strings over the alphabet consisting of English letters, arabic numerals, and punctuation marks; by S_L the group of all permutations of L elements; by $x \leftarrow y$ the operation that assigns value y to variable x. If X is probability distribution over a set S, by $rand(X)$ we denote the function that selects (independently) a element of S according to X. If X is a finite set —for which no distribution has been specified— $rand(X)$ returns a random element selected in X uniformly and independently.

1.2. *Contexts*

Informally, a context describes the players who are playing a game, their preferences and the possible outcomes that can result from playing the game.

DEFINITION 1: A context is a tuple $C = (N, T, Y, p, \{u_i\}_{i \in N})$, where

- N, is a finite set.
- T is the Cartesian product of n sets, $T = \times_{i \in N} T_i$.
- Y is a finite set.
- p is a probability distribution over T.
- u_i is the a function, $u_i : T \times Y \to \mathbb{R}$.[2]

[1]Note that the definitions in this section are equivalent to standard formalizations.

[2]Individual utilities may depend on the realized types of the others. Most of the analysis in game theory is done under this assumption. Preferences admit a utility representation if a real number can be associated with every possible choice of a player, so that two choices are ranked exactly as their corresponding numbers are compared. An expected utility representation implies that for any choice with random consequences the number assigned to it is an expectation of utility over consequences. Preferences admit an expected utility representation if they satisfy von Neumann-Morgenstern axioms.

In a context, N is called *the players*; T_i is called the *type set* of player i; Y is called the outcomes; and u_i is called the *expected utility* function of player i. (As usual, all components of C are common knowledge among the players.)In a game with context $(N, T, Y, p, \{u_i\}_{i \in N})$, the realized types of the players are selected from T according to p. Player i knows t_i and that the realized types of the others, $t_{-i} = t \setminus \{t_i\}$, are generated according to the conditional (posterior) distribution $p_{t_{-i}|t_i}$.)

1.3. Game Forms

Informally, game forms specify when a player acts; what he knows before he acts; what actions are available to him; and when the game is over.

DEFINITION 2: A *normal game form* is a pair $(N, \{A_i\}_{i \in N})$ where N and each S_i are finite sets.

In such a game form, N is called *the players* and S_i is called the *pure strategies* (or actions) available to player i. In such a game, the players act simultaneously, each player i selecting an action from S_i with no information about the action of the other players.

DEFINITION 3: An *extensive game form* with imperfect information is a tuple $(N, H, Z, \{A_h\}_{h \in (H-Z)}, P, f_{Chance}, \{I_i\}_{i \in N})$ whose components satisfy the following properties:

- N is a finite set.
- H is a set of finite sequences which includes the empty sequence $\emptyset$.
- Z is a subset of H such that $h|a \notin H$ whenever $h \in Z$.
- A_h is a finite set such that the sequence $h|a \in H$ whenever $a \in A_h$.
- P is a function mapping $H - Z$ to $N \cup \{Chance\}$.
- f_{Chance} is a function mapping a history $h \in H - Z$ such that $P(h) = Chance$ to a probability distribution over A_h.
- I_i is a function mapping H to a sequence of strings such that $\forall\, h|a \in H$, $\forall i \in N$, $I_i(h)$ is a prefix of $I_i(h|a)$ and $\forall h, h' \in H$, $\forall i \in N$, $I_i(h) = I_i(h')$ implies $P(h) = P(h')$.

In such a game form, N is called *the players*; H is called the *set of histories*; Z is called the *terminal histories*; A_h is called the *set of actions available* at history h; P is called the *player function*. At history h, player $P(h)$ selects an action $a \in A_h$ and the new history becomes (h, a). If $P(h) = Chance$, then a random action is selected in A_h according to distribution $f_{Chance}(h)$. Each I_i is called the *information function* for player i. For each $h \in H$, $I_i(h)$ represents the information available to player i after history h. For a sequence X in the range of I_i, the *information set* for player i corresponding to sequence X is $IS_i(X) = \{h \in H : I_i(h) = X\}$.[3] We define $A_{I_i} = A_h$, if $h \in I_i$.

A *pure strategy* of a player $i \in N$ is a function that assigns to each information set I_i an element of A_{I_i}. We denote by S_i the set of all pure strategies for player i.

1.4. Games and Mechanisms

DEFINITION 4: A *normal-form game of incomplete information* is a pair $\Gamma = (C, (GF, g))$ where:

- $C = (N, T, Y, p, \{u_i\}_{i \in N})$ is a context.

[3]Traditionally, notions of information for player i apply only to histories in which it is player i's turn to act. However, formalizing the information available to player i at an arbitrary history is useful when defining our notion of an ideal game. Traditional notions can easily be fit into our framework by specifying that for any history h in which it it not player i's turn to act, $I_i(h) = I_i(h')$ where h' is the longest prefix of h such that $P(h) = i$.

- $GF = (N, \{A_i\}_{i \in N})$ is a normal game form.
- g is a (probabilistic) function, $g : \times_{i \in N} A_i \to Y$.

In such a game, we call (GF,g) a *normal-form* mechanism, and g *the outcome function.* We say that Γ is a *direct game* if for each i, $S_i = T_i$. If Γ is a direct game, then we refer to $((N,T), g)$ as a *direct mechanism.*

DEFINITION 5: An *extensive form game of incomplete and imperfect* information is a pair $\Gamma = (C, (GF, g))$ where:

- $C = (N, T, Y, p, \{u_i\}_{i \in N})$ is a context.
- $GF = (N, H, Z, \{A_h\}_{h \in (H-Z)}, P, f_{Chance}, \{I_i\}_{i \in N})$ is an extensive game form with imperfect information.
- g is a (probabilistic) function, $g : Z \to Y$.

In such a game, we call (GF,g) a *normal-form* mechanism, and g *the outcome function.*