E0 337: Topics in Advanced Cryptography 23/Aug/23

Lecture 2

Instructor: Dr.Bhavana Kanukurthi, Dr.Chaya Ganesh *Scribe: Arunachalaeshwaran V R*

1 Welcome to E0 337

1.1 Course Information

Contact information and office hours:

- **Lecturer:** Bhavana Kanukurthi (bhavana@iisc.ac.in), Chaya Ganesh (chaya@iisc.ac.in).
- **Presenter:** Girisha Shankar (girishabs@iisc.ac.in).

1.2 Course Topics

The course will cover the following topics:

- Brief Review of Lecture 1.
- Game Definition
- Game Types
- Equilibrium Solution Concepts
- Complexity of Computing Equilibria

2 Review

2.1 Lecture 1

- Motivation and introduction to game theory
- Definition of game
- Prisoner's Dilemma Example
- Matrix representation of 2 player games
- Tragedy of commons (Informal)
- Dominant strategy Definition
- Equilibrium Solution Concept Overview

3 Game Types

3.1 Normal Form Games

Normal form game is one way to model (typically simultaneous) games in game theory. Unlike extensive form, normal-form representations are not graphical per se, but rather represent the game by way of a multi-dimensional array (a matrix in case of two players as we have seen in lecture 1). While this approach can be of greater use in identifying strictly dominated strategies and Nash equilibria, some information is lost as compared to extensive-form representations. The normal-form representation of a game includes all perceptible and conceivable strategies, and their corresponding payoffs, for each player. Normal form games are also referred to as strategic form games.

Definition 1 (Normal Form Game)**.** A normal form game Γ is a tuple $\langle N, (S_i)_{i\in N}, (u_i)_{i\in N}\rangle$, where

- $N = \{1, 2, \ldots, n\}$ is a set of players
- $S_1, S_2, \ldots, S_n$ are called the strategy sets of the players $1, 2, \ldots n$ respectively
- $u_i : S_1 \times S_2 \times \cdots \times S_n \to \mathbb{R}$ for $i = 1, 2, \ldots, n$ are mappings called utility or payoff functions of player i

The games we have discussed so far and will be considering in the future will be mostly of this type.

3.2 Extensive Form Games

In game theory, an extensive-form game is a specification of a game allowing (as the name suggests) for the explicit representation of a number of key aspects, like the sequencing of players' possible moves, their choices at every decision point, the (possibly imperfect) information each player has about the other player's moves when they make a decision, and their payoffs for all possible game outcomes. Extensive-form games also allow for the representation of incomplete information in the form of chance events modeled as "moves by nature". Extensive-form representations differ from normal-form in that they provide a more complete description of the game in question, whereas normal-form simply boils down the game into a payoff matrix.

An information set of a player is a set of that player's decision nodes that are indistinguishable to the player.[**narahari2014game**]

An information set of a player describes a collection of all possible distinguishable circumstances in which the player is called upon to make a move. Since each decision node corresponds uniquely to a sequence of actions from the root node to the decision node, each information set of a player consists of all proper subhistories relevant to that player which are indistinguishable to that player. Clearly, in every node within a given information set, the corresponding player must have the same set of possible actions.[**narahari2014game**]

Definition 2 (Extensive Form Game)**.** An extensive form game Γ is a tuple $\langle N, (A_i)_{i\in N}, \mathbb{H}, P, (\mathbb{I}_i)_{i\in N}, (u_i)_{i\in N}\rangle$, where

- $N = \{1, 2, \ldots, n\}$ is a finite set of players
- A_i for $i = 1, 2, \ldots, n$ is the set of actions available to player i (action set of player i)
- H is the set of all terminal histories where a terminal history is a path of actions from the root to a terminal node such that it is not a proper subhistory of any other terminal history. Denote by $S_{\mathbb{H}}$ the set of all proper subhistories (including the empty history ε) of all terminal histories.
- $P : S_{\mathbb{H}} \to N$ is a player function that associates each proper subhistory to a certain player
- $\mathbb{I}_i$ for $i = 1, 2, \ldots, n$ is the set of all information sets of player i
- $u_i : \mathbb{H} \to \mathbb{R}$ for $i = 1, 2, \ldots, n$ gives the utility of player i corresponding to each terminal history.

Games like matching pennies (toy example), chess, backgammon, poker, etc are typical examples of games that are modelled in extensive form.

Example 3 (Matching Pennies)**.** *Here, the first player either chooses head or tail. The second player then also chooses head or tail. If both pennies have the same face, the second player wins; if not, the player 1 wins. A variant of this game can be that both players choose at the same time. The second player thus chooses without knowing the result of the first player (it is represented on the second graph). It is important to notice that the resulting payoffs are the same in both cases. Refer fig. 1 for game tree.*

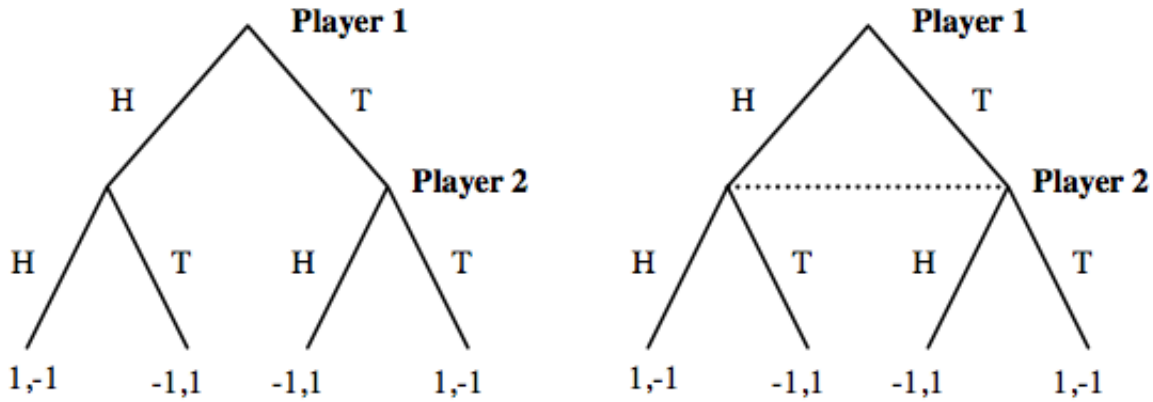

Figure 1: Matching Pennies Example (Serial variant on the left and Simultaneous Variant on the right)

4 Equilibrium Solution Concepts

4.1 Motivation

So, far we have looked into how to model games but to analyze them we will be utilizing various solution concepts. Typically, we consider equilibrium solution concepts these model the strategy profile(s) the rational players will eventually settle on.

4.2 Dominant Strategy Equilibrium

Dominant strategy equilibrium are equilibriums that are strategic proof i.e don't depend on the exact choice(s) made by other player(s).

4.2.1 Strongly Dominant Strategy Equilibrium

Definition 4 (Strongly Dominated Strategy)**.** Given a strategic form game $\langle N, (S_i)_{i\in N}, (u_i)_{i\in N}\rangle$ a strategy $s_i \in S_i$ of player i is said to be strongly dominated by another strategy $s_i' \in S_i$ if

$$u_i(s_i', s_{-i}) > u_i(s_i, s_{-i}) \forall s_{-i} \in S_{-i}$$

We also say that s_i' strongly dominates strategy s_i.

Definition 5 (Strongly Dominant Strategy)**.** A strategy $s_i^* \in S_i$ is said to be a strongly dominant strategy for player i if it strongly dominates every other strategy $s_i \in S_i$. That is, $\forall s_i \neq s_i^*$,

$$u_i(s_i^*, s_{-i}) > u_i(s_i, s_{-i}) \forall s_{-i} \in S_{-i}$$

Definition 6 (Strongly Dominant Strategy Equilibrium)**.** A strategy profile $(s_1^*, \ldots, s_n^*)$ is called a strongly dominant strategy equilibrium of the game $\langle N, (S_i)_{i\in N}, (u_i)_{i\in N}\rangle$ if, $\forall i = 1, 2, \ldots, n$, the strategy s_i^* is a strongly dominant strategy for player i.

Observe that if a strongly dominant strategy equilibrium (SDSE) exists then it is unique. A strongly dominant strategy if it exists will be played by a player in the Nash Equilibrium as well.

Example 7. *Consider the following welfare-war game (a different rendition of Prisoner's dilemma).*

		Player 2	
		Welfare	War
Player 1	Welfare	$(5, 5)$	$(0, 7)$
	War	$(7, 0)$	$(1, 1)$

Table 1: Here (War, War) is a SDSE

4.2.2 Weakly Dominant Strategy Equilibrium

Definition 8 (Weakly Dominated Strategy)**.** A strategy $s_i^* \in S_i$ is said to be weakly dominated by a strategy $s_i \in S_i$ for player i if
$u_i(s_i', s_{-i}) \geq u_i(s_i, s{-}i) \forall s_{-i} \in S_{-i}$ and $u_i(s_i', s{-}i) > u_i(s_i, s_{-i})$ for some $s{-}i \in S_{-i}$

The strategy s_i' is said to weakly dominate strategy s_i.
Note that strict inequality is to be satisfied for at least one $s{-}i$.

Definition 9 (Weakly Dominant Strategy)**.** A strategy s_i^* is said to be a weakly dominant strategy for player i if it weakly dominates every other strategy $s_i \in S_i$.

Definition 10 (Weakly Dominant Strategy Equilibrium)**.** A strategy profile $(s_1^*, \ldots, s_n^*)$ is called a weakly dominant strategy equilibrium of the game $\langle N, (S_i)_{i\in N}, (u_i)_{i\in N}\rangle$ if, $\forall i = 1, 2, \ldots, n$, the strategy s_i^* is a weakly dominant strategy for player i.

All SDSEs are weakly dominant strategy equilibriums (WDSEs). If a WDSE exists then it is unique. In the related field of mechanism design we often design games to have a WDSE.

Example 11. *Consider the following welfare-war game (a different rendition of Prisoner's dilemma).*

		Player 2	
		Welfare	War
Player 1	Welfare	$(-2, -2)$	$(-10, -2)$
	War	$(-2, -10)$	$(-5, -5)$

Table 2: Here (War, War) is a WDSE

4.2.3 Very Weakly Dominant Strategy Equilibrium

Definition 12 (Very Weakly Dominated Strategy)**.** A strategy $s_i^* \in S_i$ is said to be very weakly dominated by a strategy $s_i \in S_i$ for player i if
$u_i(s_i', s_{-i}) \geq u_i(s_i, s{-}i) \forall s_{-i} \in S_{-i}$

The strategy s_i' is said to weakly dominate strategy s_i. Note that strict inequality need not be satisfied for any strategy here.

Definition 13 (Very Weakly Dominant Strategy)**.** A strategy s_i^* is said to be a very weakly dominant strategy for player i if it very weakly dominates every other strategy $s_i \in S_i$.

Definition 14 (Very Weakly Dominant Strategy Equilibrium)**.** A strategy profile $(s_1^*, \ldots, s_n^*)$ is called a very weakly dominant strategy equilibrium of the game $\langle N, (S_i)_{i\in N}, (u_i)_{i\in N}\rangle$ if, $\forall i = 1, 2, \ldots, n$, the strategy s_i^* is a very weakly dominant strategy for player i.

Every WDSE is a very weakly dominant strategy equilibrium (VWDSE).

Example 15. *Consider the following welfare-war game (a different rendition of Prisoner's dilemma).*

		Player 2	
		Welfare	War
Player 1	Welfare	$(-2, -2)$	$(-5, -2)$
	War	$(-2, -10)$	$(-5, -10)$

Table 3: Here all the four strategic profiles are VWDSEs

4.3 Nash Equilibrium

Nash equilibrium is used to model a situtation in which no rational player has an incentive to (unilaterally, i.e only this player) deviate from the equilibrium strategic profile.

4.3.1 Pure Strategy Nash Equilibrium

Definition 16 (Pure Strategy Nash Equilibrium)**.** Given a strategic form game $\langle N, (S_i)_{i\in N}, (u_i)_{i\in N}\rangle$, the strategy profile $s^* = (s_1^*, s_2^*, \ldots, s_n^*)$ is called a pure strategy Nash equilibrium of Γ if

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*) \forall s_i \in S_i, \forall i = 1, 2, \ldots, n$$

A pure strategy Nash equilibrium (PSNE) need not always exist. For example, consider the simultaneous matching pennies game or rock, paper, scissors game.

Example 17. *Two ~~victims~~ friends Anirban and Shreyas (this is a variant of battle of sexes game) want to choose between Barbie and Oppenheimer and this is their corresponding payoff matrix*

		Shreyas	
		Oppenheimer	Barbie
Anirban	Oppenheimer	$(3, 4)$	$(0, 0)$
	Barbie	$(0, 0)$	$(5, 2)$

Table 4: Here strategy profiles in which they go to the same movie (i.e diagonal profiles) are PSNEs

4.3.2 Mixed Strategy Nash Equilibrium

A mixed strategy of a player defines a probability distribution over pure strategies of that player. Here, our goal is to maximize the expected utility rather than the utility.

Definition 18 (Mixed Strategy)**.** Given a player i with S_i as the set of pure strategies, a mixed strategy (also called randomized strategy) σ_i of player i is a probability distribution over S_i. That is, $\sigma_i : S_i \to [0, 1]$ is a mapping that assigns to each pure strategy $s_i \in S_i$, a probability $\sigma_i(s_i)$ such that

$$\sum_{s_i \in S_i} \sigma_i(s_i) = 1$$

Definition 19 (Mixed Strategy Nash Equilibrium)**.** *Given a strategic form game $\langle N, (S_i)_{i\in N}, (u_i)_{i\in N}\rangle$, a mixed strategy profile $(\sigma_1^*, \ldots, \sigma_n^*)$ is called a Nash equilibrium if $\forall i \in N$*

$$u_i(\sigma_i^*, \sigma_{-i}^*) \geq u_i(\sigma_i, \sigma_{-i}^*) \forall \sigma_i \in \Delta(S_i)$$

Where, $\Delta(S_i)$ is the set of all possible mixed strategies (i.e all probability distributions) over S_i. More formally, if $S_i = \{s_{i1}, \ldots, s_{im}\}$ then

$$\Delta(S_i) = \left\{ (\sigma_{i1}, \ldots, \sigma_{im}) \in \mathbb{R}^m : \sigma_{ij} \geq 0 \text{ for } j = 1, \ldots, m \text{ and } \sum_{j=1}^{m} \sigma_{ij} = 1 \right\}$$

Observe that all PSNEs are Mixed Strategy Nash Equilibriums (MSNEs).

Example 20. *Two ~~victims~~ friends Anirban and Shreyas (this is a variant of battle of sexes game) want to choose between Barbie and Oppenheimer and this is their corresponding payoff matrix*

		Shreyas	
		Oppenheimer	Barbie
Anirban	Oppenheimer	$(3, 4)$	$(0, 0)$
	Barbie	$(0, 0)$	$(5, 2)$

Table 5: Here strategy profiles ((1/3, 2/3), (5/8, 3/8)) is also a MSNE in addition to the PSNEs seen previously

Theorem 21 (Nash's existence theorem (informal))**.** *For all finite games (finite number of players and finite number of pure strategies for each player) there always exists a MSNE.*

Existence of MSNE in finite games can be proved using Brouwer's (or Katakuni's) fixed point theorem or Sperner's lemma.

Theorem 22 (Robert Wilson's Oddness theorem (informal))**.** *Almost all finite games have finite and a odd number of MSNEs.*

Here, "almost all" means even if the payoffs were slightly perturbed then with probabiilty one, there will be a finite odd number of MSNEs.

Example 23. *The free money game is a game in which there are an even (exactly 2 PSNEs) number of MSNEs.*

		Player 2	
		Yes	No
Player 1	Yes	$(1, 1)$	$(0, 0)$
	No	$(0, 0)$	$(0, 0)$

Table 6: Here (Yes, Yes) and (No, No) are all the MSNEs

Exercise 24. *Analyze this scene (https://www.youtube.com/watch?v=LJS7Igvk6ZM) from the movie "A beautiful mind" portraying the life of John Nash. Is the "Nash equilibrium" described here an actual Nash Equilibrium? Also, analyze how this scene relates to John Nash's Ph.D thesis and why Adam Smith was wrong.*

5 Complexity of Computing Equilibria

5.1 Dominant Strategy Equilibrium

We can compute whether a dominant strategy equilibrium (DSE i.e SDSE or WDSE or VWDSE) exists for a finite game (where the payoffs are in a reasonable representation say a rational for simplicity) using an algorithm called method of iterated deletion (here the input is the payoff multi-dimensional array). This algorithm works by computing dominant strategy for each player (if it exists, if not says no DSE exists). This is how a dominant strategy for a particular player is computed we iterate over pairs of strategies and delete strategies that fail to dominate at least one another strategy. The final set of strategies we are left with are the dominant dominant strategies of the player. This can be further optimized in case of SDSE and WDSE (essentially a reduce algorithm whose associative binary operation picks the dominating strategy among the two strategies). If a dominant strategy exists for every player pick an arbitrary dominant strategy for each player and this strategic profile is a DSE. This algorithm answers both the decison and search problem of existence of DSE. This is a polynomial time algorithm with complexity $O(npm^2)$ (and $O(npm)$ for the optimized version), where n is the number of players, m is the maximum number of strategies any player can play and p is the maximum time taken to make a single comparison (directly relates to how the payoff values are stored. Same as the precision in case of rational numbers).

5.2 Mixed Strategy Nash Equilibrium

Complexity of determining whether a given finite game has a PSNE exists is clearly a $\mathbb{NP}$ (non-deterministic polynomial time) problem. It is not known whether this problem is in $\mathbb{P}$ (polynomial time) or $\mathbb{NPC}$ (i.e $\mathbb{NP}$-complete). Many restricted variants of this problem have been considered in the literature but here we will be mainly be dealing with computing MSNEs.

The problem of computing a MSNE of a given finite game is characterized by the language NASH (often a relaxation known as $\varepsilon -$ NASH is used in place of NASH as it is easier to work with. We will ignore such technical subtleties for now for the sake of a simpler presentation). Note that problem of determining whether a given finite game has a MSNE is trivial as it is guaranteed to exist by theorem 21 (Nash's existence theorem).

A binary relation $P(x, y)$, where y is at most polynomially longer than x, is in $\mathbb{FNP}$ if and only if there is a deterministic polynomial time algorithm that can determine whether $P(x, y)$ holds given both x and y (here x is the input and y is the witness to be searched for or say no such witness exists). The subclass of $\mathbb{FNP}$ for which such y (witness) is guaranteed to exist is called $\mathbb{TFNP}$ (total $\mathbb{FNP}$). Typically, such existence guarantee is made by non-constructive (algorithmically non-constructive) arguments. The subclass of $\mathbb{TFNP}$ for which existence of witness is guaranteed by (polynomial) parity-arguments over directed graphs (these were proposed by Christos Papadimitriou (PaPADimitriou), details of which won't be covered here) is called $\mathbb{PPAD}$. NASH is $\mathbb{PPAD}$-complete under polynomial time Turing reduction. It is believed $\mathbb{PPAD}$ contains strictly superpolynomial time problems. Other examples of $\mathbb{PPAD}$-complete problems are end of line problem, MSNE for 2 player games, finding three-colored point in Sperner's lemma, finding an envy-free cake cutting where utility function is given by polynomial time algorithm, etc.