CSC304 Lecture 6

Game Theory : Security games, Applications to security

Recap

- Last lecture
  - Zero-sum games
  - The minimax theorem

- Assignment 1 posted
  - Might add one or two questions (more if you think it's a piece of cake)
  - Kept my promise (approximately)
  - Due: October 11 by 3pm

Till now…

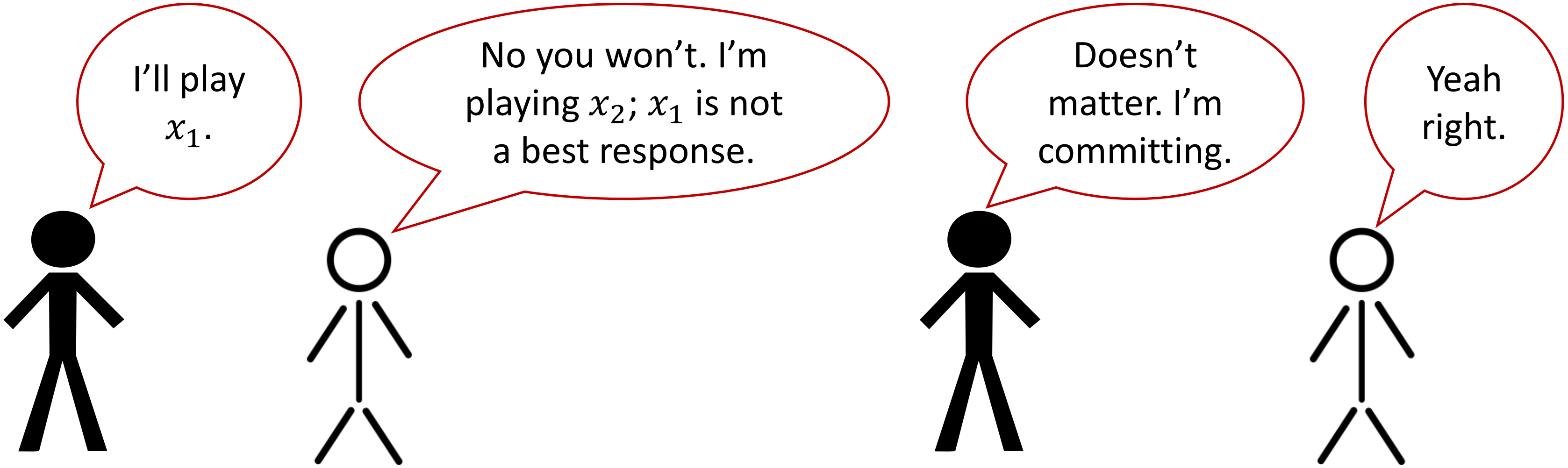
- Simultaneous-move Games
- All players act simultaneously
- Nash equilibria = stable outcomes
- Each player is best responding to the strategies of all other players

Sequential Move Games

- Focus on two players: “leader” and “follower”
- Leader first commits to playing a (possibly mixed) strategy x_1
  - Cannot later backtrack
- Leader communicates x_1 to follower
  - Follower must believe leader’s commitment is credible
- Follower chooses the best response x_2
  - Can assume to be a pure strategy

Sequential Move Games

- Wait. Does this give us anything new?
  - Can't I, as player 1, commit to playing x_1 in a simultaneous-move game too?
  - Player 2 wouldn't believe you.

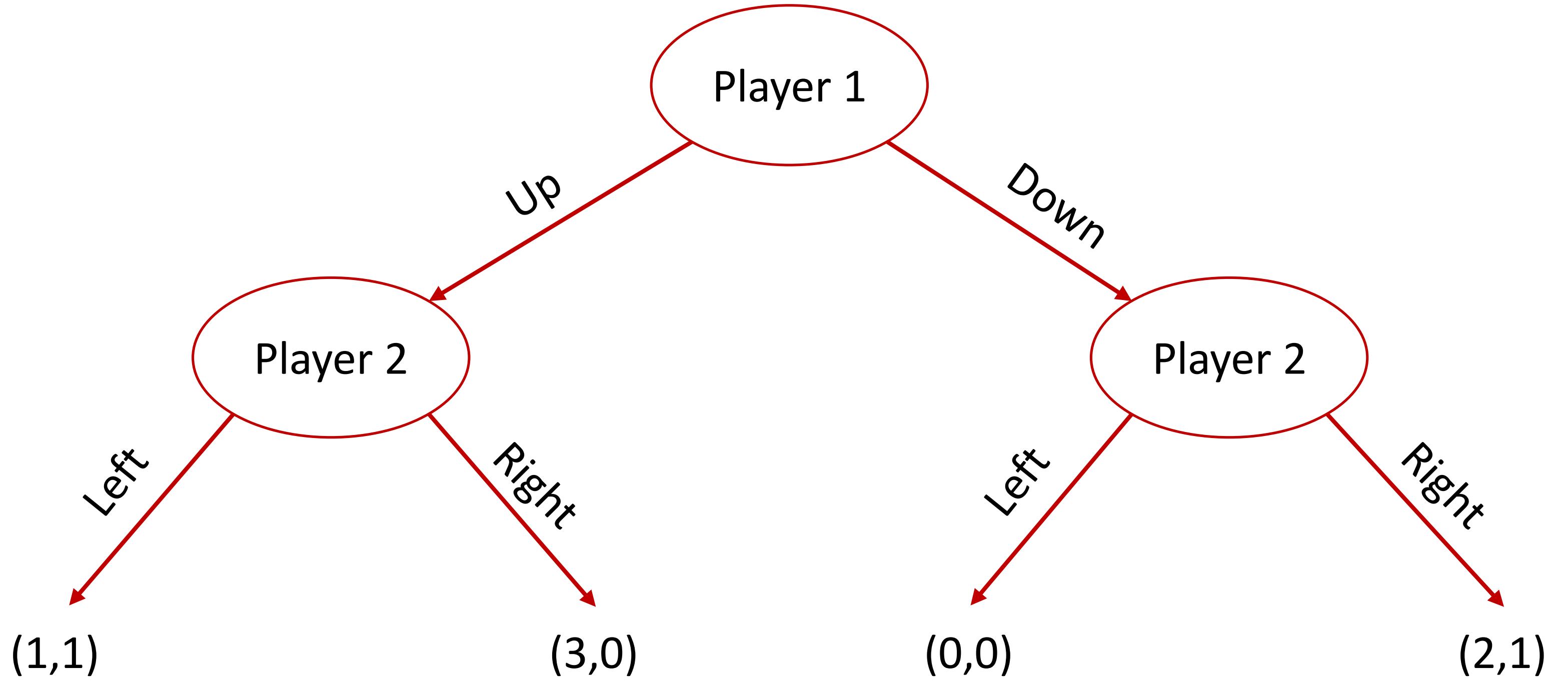


That’s unless…

- You’re as convincing as this guy.

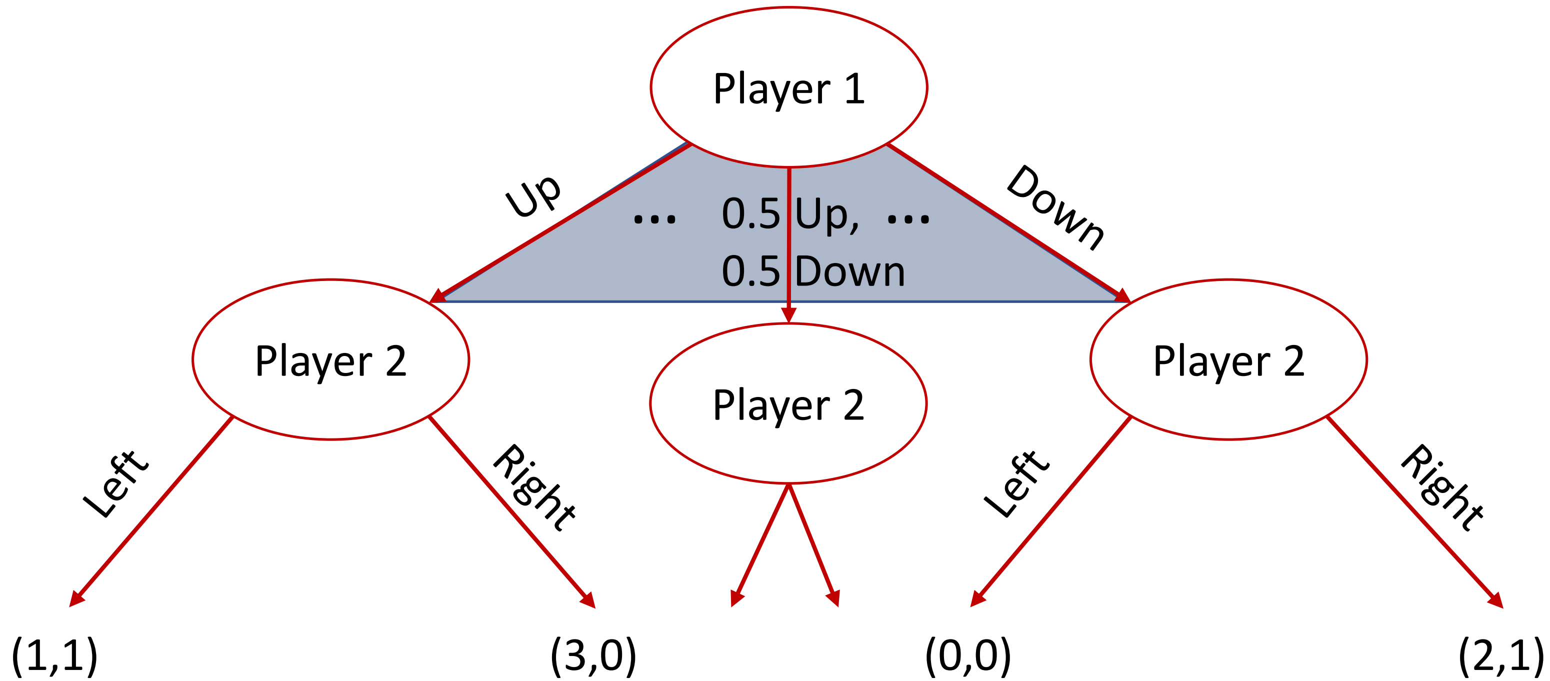
How to represent the game?

- Extensive form representation
  - Can also represent “information sets”, multiple moves, …



How to represent the game?

- Mixed strategies are hard to visually represent
  - Continuous spectrum of possible actions



A Curious Case

P2 / P1	Left	Right
Up	(1 , 1)	(3 , 0)
Down	(0 , 0)	(2 , 1)

- Q: What are the Nash equilibria of this game?
- Q: You are P1. What is your reward in Nash equilibrium?

A Curious Case

P1 \ P2	Left	Right
Up	(1 , 1)	(3 , 0)
Down	(0 , 0)	(2 , 1)

- Q: As P1, you want to commit to a pure strategy. Which strategy would you commit to?

- Q: What would your reward be now?

Commitment Advantage

P1 \ P2	Left	Right
Up	(1 , 1)	(3 , 0)
Down	(0 , 0)	(2 , 1)

- Reward in the only Nash equilibrium = 1
- Reward when committing to Down = 2

- Again, why can't P1 get a reward of 2 with simultaneous moves?

Commitment Advantage

P2 / P1	Left	Right
Up	(1 , 1)	(3 , 0)
Down	(0 , 0)	(2 , 1)

- With commitment to mixed strategies, the advantage could be even more.
  - If P1 commits to playing Up and Down with probabilities 0.49 and 0.51, respectively…
  - P2 is still better off playing Right than Left, in expectation
  - $\mathbb{E}$[Reward] for P1 increases to ~2.5

Stackelberg vs Nash

- Commitment disadvantage?

- Q: Can the leader lose in Stackelberg equilibrium compared to a Nash equilibrium?
  - In Stackelberg, he must commit in advance, while in Nash, he can change his strategy at any point.
  - A: No. The optimal reward for the leader in the Stackelberg game is always greater than or equal to his maximum reward under any Nash equilibrium of the simultaneous-move version.

Stackelberg vs Nash

- What about police trying to catch a thief, and the thief trying to avoid?

- It is important that..
  - the leader can commit to mixed strategies
  - the follower knows (and trusts) the leader's commitment
  - the leader knows the follower's reward structure

- Will later see practical applications

Stackelberg and Zero-Sum

- Recall the minimax theorem for 2-player zero-sum games

$$\max_{x_1} \min_{x_2} \ (x_1)^T A \, x_2 = \min_{x_2} \max_{x_1} \ (x_1)^T A \, x_2$$

- What would player 1 do if he were to go first?
- What about player 2?

Stackelberg and General-Sum

- 2-player non-zero-sum game with reward matrices A and $B \neq -A$ for the two players

$$\max_{x_1} \ (x_1)^T A \, f(x_1)$$

$$\text{where } f(x_1) = \max_{x_2} \ (x_1)^T B \, x_2$$

- How do we compute this?

Stackelberg Games via LPs

- S_1, S_2 = sets of actions of leader and follower
- $|S_1| = m_1, |S_2| = m_2$
- $x_1(s_1)$ = probability of leader playing s_1
- π_1, π_2 = reward functions for leader and follower

$$\max \Sigma_{s_1 \in S_1} x_1(s_1) \cdot \pi_1(s_1, s_2^*)$$

subject to

$$\forall s_2 \in S_2, \quad \Sigma_{s_1 \in S_1} x_1(s_1) \cdot \pi_2(s_1, s_2^*) \geq \Sigma_{s_1 \in S_1} x_1(s_1) \cdot \pi_2(s_1, s_2)$$

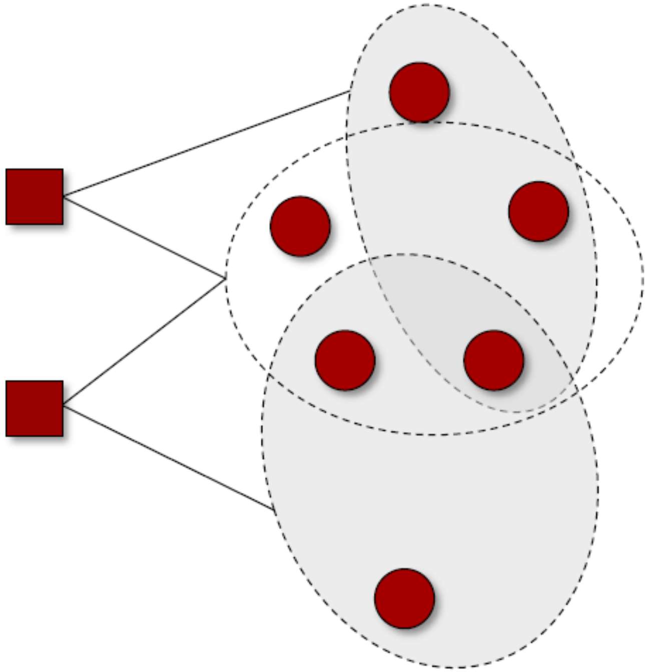
$$\Sigma_{s_1 \in S_1} x_1(s_1) = 1$$

$$\forall s_1 \in S_1, x_1(s_1) \geq 0$$

- One LP for each s_2^*, take the maximum over all m_2 LPs
- The LP corresponding to s_2^* optimizes over all x_1 for which s_2^* is the best response

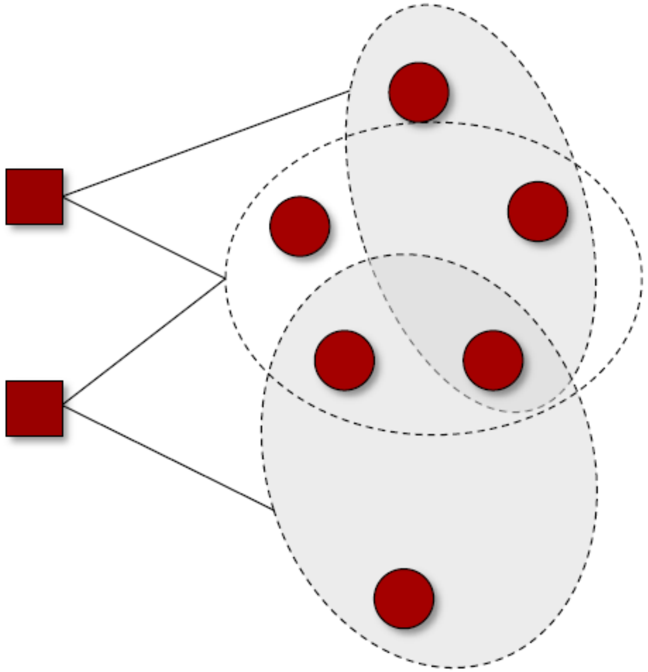
Real-World Applications

- Security Games
  - Defender (leader) has k identical patrol units
  - Defender wants to defend a set of n targets T
  - In a pure strategy, each resource can protect a subset of targets $S \subseteq T$ from a given collection $\mathcal{S}$
  - A target is covered if it is protected by at least one resource
  - Attacker wants to select a target to attack



Real-World Applications

- Security Games
  - For each target, the defender and the attacker have two utilities: one if the target is covered, one if it is not.
  - Defender commits to a mixed strategy; attacker follows by choosing a target to attack.



Ah!

- Q: Because this is a 2-player Stackelberg game, can we just compute the optimal strategy for the defender in polynomial time…?

- Time is polynomial in the number of pure strategies of the defender
  - In security games, this is $|\mathcal{S}|^k$
  - Exponential in k

- Intricate computational machinery required…

LAX

Newsweek National News

Subscribe Now | Make Newsweek Your Homepage | Newsletters | RSS

The Element of Surprise

To help combat the terrorism threat, officials at Los Angeles Inter Airport are introducing a bold new idea into their arsenal: random of security checkpoints. Can game theory help keep us safe?

WEB EXCLUSIVE

By Andrew Murr
Newsweek
Updated: 1:00 p.m. PT Sept 28, 2007

Security forces work the sidewalk

Sept. 28, 2007 - Security officials at Los Angeles International Airport now have a new weapon in their fight against terrorism: complete, baffling randomness. Anxious to thwart future terror attacks in the early stages while plotters are casing the airport, LAX security patrols have begun using a new software program called ARMOR, NEWSWEEK has learned, to make the placement of security checkpoints completely unpredictable. Now all airport security officials have to do is press a button labeled "Randomize," and they can throw a sort of digital cloak of invisibility over where they place the cops' antiterror checkpoints on any given day.

Real-World Applications

- Protecting entry points to LAX
- Scheduling air marshals on flights
  - Must return home
- Protecting the Staten Island Ferry
  - Continuous-time strategies
- Fare evasion in LA metro
  - Bathroom breaks !!!
- Wildlife protection in Ugandan forests
  - Poachers are not fully rational
- Cyber security

…