Graduate AI

Lecture 19: Game Theory II

Teachers:
Zico Kolter
Ariel Procaccia (this time)

Correlated equilibrium

- Let $N = \{1,2\}$ for simplicity
- A mediator chooses a pair of strategies (s_1, s_2) according to a distribution p over S^2
- Reveals s_1 to player 1 and s_2 to player 2
- When player 1 gets $s_1 \in S$, he knows that the distribution over strategies of 2 is

$$\Pr[s_2 | s_1] = \frac{\Pr[s_1 \wedge s_2]}{\Pr[s_1]} = \frac{p(s_1, s_2)}{\sum_{s_2' \in S} p(s_1, s_2')}$$

Correlated equilibrium

- Player 1 is best responding if for all $s_1' \in S$

$$\sum_{s_2 \in S} \Pr[s_2 | s_1]\, u_1(s_1, s_2) \geq \sum_{s_2 \in S} \Pr[s_2 | s_1]\, u_1(s_1', s_2)$$

- Equivalently,

$$\sum_{s_2 \in S} p(s_1, s_2) u_1(s_1, s_2) \geq \sum_{s_2 \in S} p(s_1, s_2) u_1(s_1', s_2)$$

- p is a correlated equilibrium (CE) if both players are best responding

Game of chicken

http://youtu.be/u7hZ9jKrwvo

Game of chicken

- Social welfare is the sum of utilities
- Pure NE: (C,D) and (D,C), social welfare = 5
- Mixed NE: both (1/2,1/2), social welfare = 4
- Optimal social welfare = 6

	Dare	Chicken
Dare	0,0	4,1
Chicken	1,4	3,3

Game of chicken

- Correlated equilibrium:
  - (D,D): 0
  - (D,C): $\frac{1}{3}$
  - (C,D): $\frac{1}{3}$
  - (C,C): $\frac{1}{3}$

	Dare	Chicken
Dare	0,0	4,1
Chicken	1,4	3,3

- Social welfare of CE $= \frac{16}{3}$

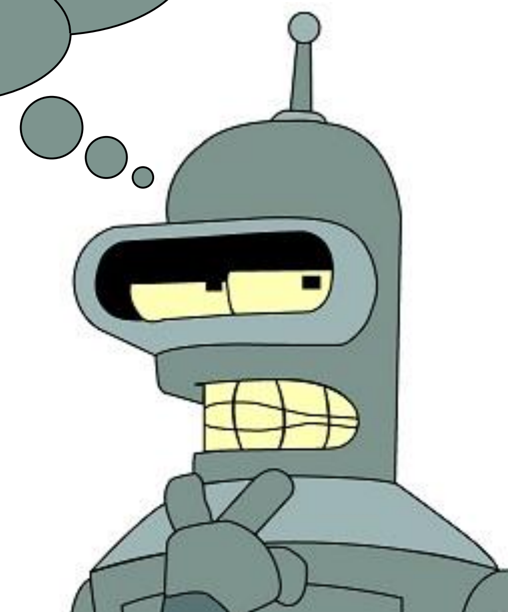
Implementation of CE

- Instead of a mediator, use a hat!
- Balls in hat are labeled with "chicken" or "dare", each blindfolded player takes a ball
- Poll 1: Which balls implement the distribution of slide 6?
  1. 1 chicken, 1 dare
  2. 2 chicken, 1 dare
  3. 2 chicken, 2 dare
  4. 3 chicken, 2 dare

CE vs. NE

- Poll 2: What is the relation between CE and NE?
  1. CE $\Rightarrow$ NE
  2. NE $\Rightarrow$ CE
  3. NE $\Leftrightarrow$ CE
  4. NE $\|$ CE

CE of slide 6 is NE?



CE As LP

- Can compute CE via linear programming in polynomial time!

find $\forall s_1, s_2 \in S, p(s_1, s_2)$

s.t. $\forall s_1, s_1', s_2 \in S, \sum_{s_2 \in A} p(s_1, s_2) u_1(s_1, s_2) \geq \sum_{s_2 \in A} p(s_1, s_2) u_1(s_1', s_2)$

$\forall s_1, s_2, s_2' \in S, \sum_{s_1 \in A} p(s_1, s_2) u_2(s_1, s_2) \geq \sum_{s_1 \in A} p(s_1, s_2) u_2(s_1, s_2')$

$\sum_{s_1, s_2 \in S} p(s_1, s_2) = 1$

$\forall s_1, s_2 \in S, p(s_1, s_2) \in [0,1]$

A curious game

- Playing up is a dominant strategy for row player
- So column player would play left
- Therefore, (1,1) is the only Nash equilibrium outcome

1,1	3,0
0,0	2,1

Commitment is good

- Suppose the game is played as follows:
  - Row player commits to playing a row
  - Column player observes the commitment and chooses column
- Row player can commit to playing down!

1,1	3,0
0,0	2,1

Commitment to mixed strategy

- By committing to a mixed strategy, row player can guarantee a reward of 2.5
- Called a Stackelberg (mixed) strategy

	0	1
.49	1,1	3,0
.51	0,0	2,1

Computing Stackelberg

- Theorem [Conitzer and Sandholm, EC 2006]: In 2-player normal form games, an optimal Stackelberg strategy can be found in poly time
- Theorem [ditto]: the problem is NP-hard when the number of players is ≥ 3

TRACTABILITY: 2 PLAYERS

- For each pure follower strategy s_2, we compute via the LP below a strategy x_1 for the leader such that
  - Playing s_2 is a best response for the follower
  - Under this constraint, x_1 is optimal
- Choose x_1^* that maximizes leader value

$$\max \sum_{s_1 \in S} x_1(s_1) u_1(s_1, s_2)$$

$$\text{s.t.} \quad \forall s_2' \in S,\ \sum_{s_1 \in S} x_1(s_1) u_2(s_1, s_2) \geq \sum_{s_1 \in S} x_1(s_1) u_2(s_1, s_2')$$

$$\sum_{s_1 \in S} x_1(s_1) = 1$$

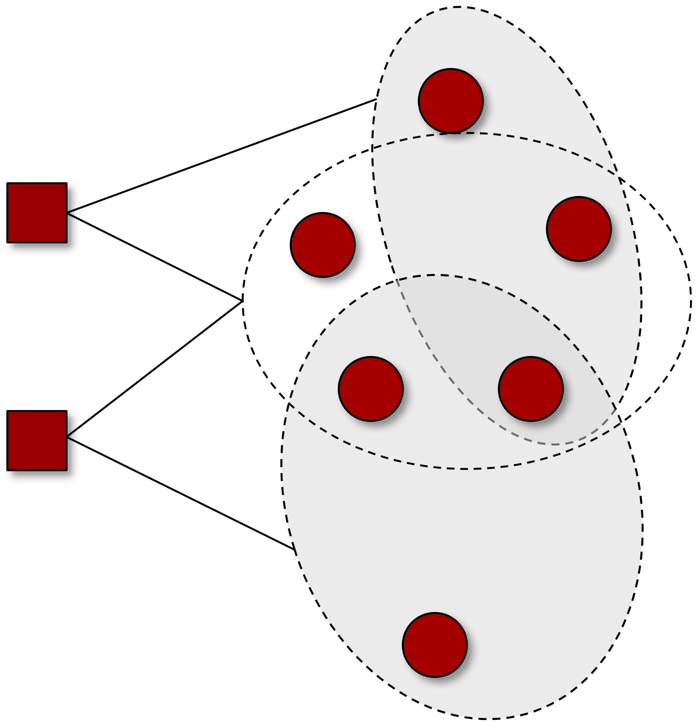
$$\forall s_1 \in S, x_1(s_1) \in [0,1]$$

Application: security

- Airport security: deployed at LAX
- Federal Air Marshals
- Coast Guard
- Idea:
  - Defender commits to mixed strategy
  - Attacker observes and best responds

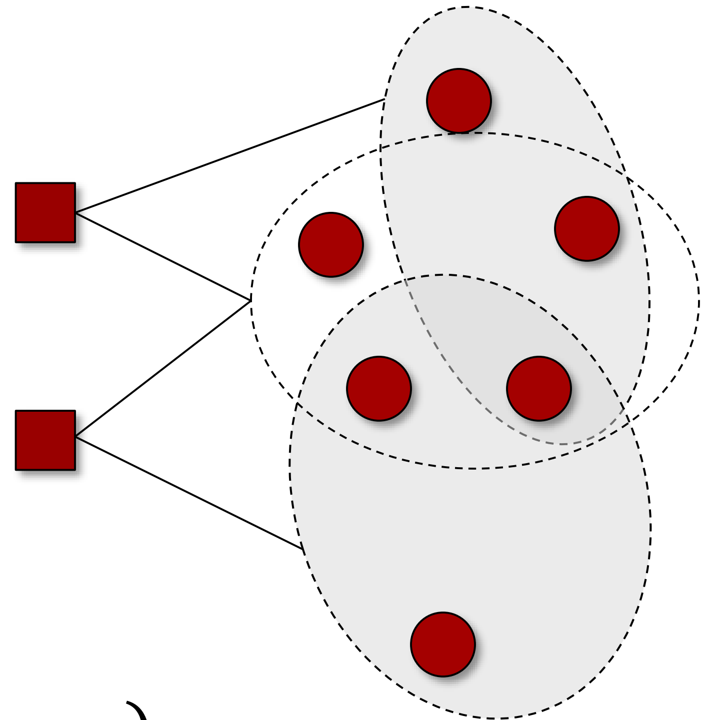
Security games

- Set of targets $T = \{1, \ldots, n\}$
- Set of m security resources Ω available to the defender (leader)
- Set of schedules $\Sigma \subseteq 2^T$
- Resource ω can be assigned to one of the schedules in $A(\omega) \subseteq \Sigma$
- Attacker chooses one target to attack

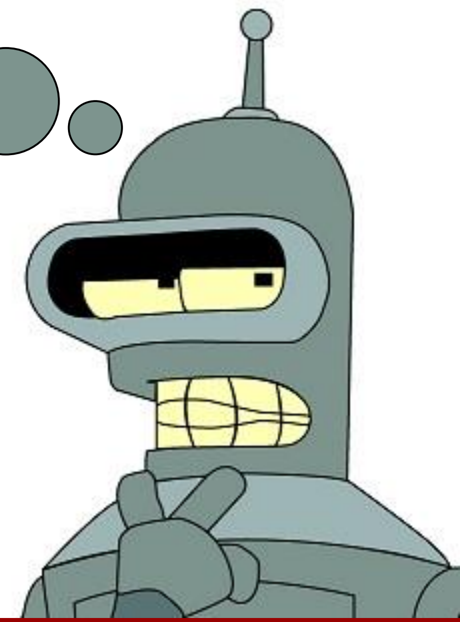


Security games

- For each target t, there are four numbers: $u_d^+(t) \geq u_d^-(t)$, and $u_a^+(t) \leq u_a^-(t)$
- Randomized defender strategy induces coverage probabilities $\boldsymbol{c} = (c_1, \ldots, c_n)$
- The utilities to the defender/attacker under $\mathbf{c}$ if target t is attacked are
$u_d(t, \boldsymbol{c}) = u_d^+(t) \cdot c_t + u_d^-(t)(1 - c_t)$
$u_a(t, \boldsymbol{c}) = u_a^+(t) \cdot c_t + u_a^-(t)(1 - c_t)$



This is a 2-player Stackelberg game, so we can compute an optimal strategy for the defender in polynomial time...?



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: randon 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

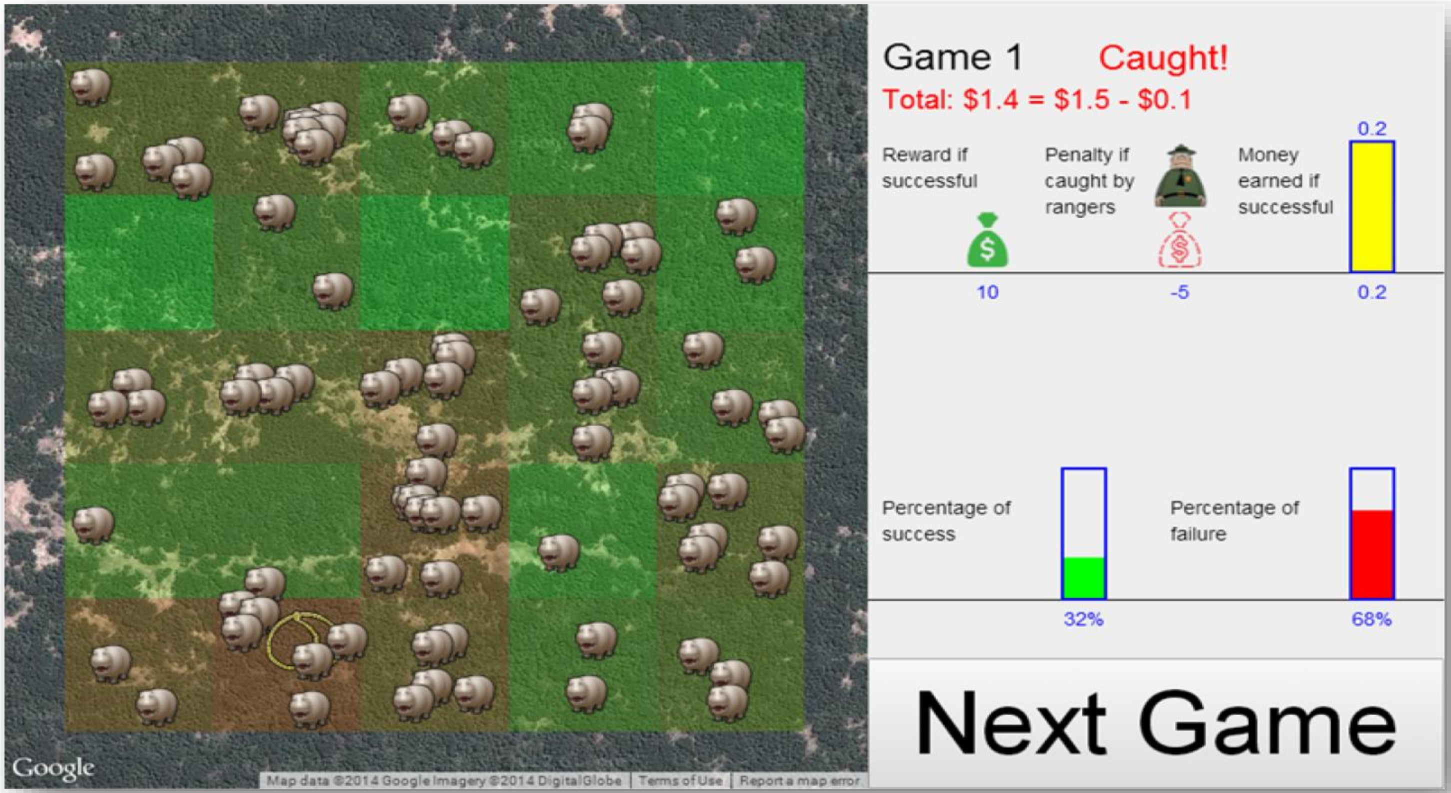
Security forces work the sidewalk

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.

Limitations

- The defender knows the utility function of the attacker
  - Solution: machine learning
- The attacker perfectly observes the defender's randomized strategy
  - MDPs, although this may not be a major concern
- The attacker is perfectly rational, i.e., best responds to the defender's strategy
  - Solution: bounded rationality models

Testing bounded rationality



[Kar et al., 2015]

SUMMARY

- Terminology and algorithms:
  - Correlated equilibrium: Polytime algorithm
  - Stackelberg game: Polytime algorithm
  - Security game
- Nobel-prize-winning ideas:
  - Correlated equilibrium ☺
- Other big ideas:
  - Stackelberg games for security