APPLIED MECHANISM DESIGN FOR SOCIAL GOOD

JOHN P DICKERSON

Lecture #8 – 02/20/2018

CMSC828M
Tuesdays & Thursdays
9:30am – 10:45am

COMPUTER SCIENCE
UNIVERSITY OF MARYLAND

PRESENTATION LIST IS ONLINE!

(CLASS WEBSITE UPDATED SOON)

THIS CLASS: STACKELBERG & SECURITY GAMES

Thanks to: AGT book, Conitzer (VC), Procaccia (AP)

SIMULTANEOUS PLAY

Previously, assumed players would play simultaneously

- Two drivers simultaneously decide to go straight or divert
- Two prisoners simultaneously defect or cooperate
- Players simultaneously choose rock, paper, or scissors
- Etc …

No knowledge of the other players' chosen actions

What if we allow sequential action selection ...?

LEADER-FOLLOWER GAMES

Heinrich von Stackelberg

Two players:

- **The leader commits to acting in a specific way**
- **The follower observes the leader’s mixed strategy**

NE, iterated strict dominance

Commit to “Bottom”	
0, 0	2, 1

What is the Nash equilibrium ????????

- **Social welfare: 2**
- **Utility to row player: 1**

Row player = leader; what to do ????????

- **Social welfare: 3**
- **Utility to row player: 2**

ASIDE: FIRST-MOVER ADVANTAGE (FMA)

From the econ side of things …

- **Leader is sometimes called the Market Leader**
- **Some advantage allows a firm to move first:**
  - Technological breakthrough via R&D
  - Buying up all assets at low price before market adjusts

By committing to a strategy (some amount of production), can effectively force other players' hands.

Things we won't model:

- Significant cost of R&D, uncertainty over market demand, initial marketing costs, etc.

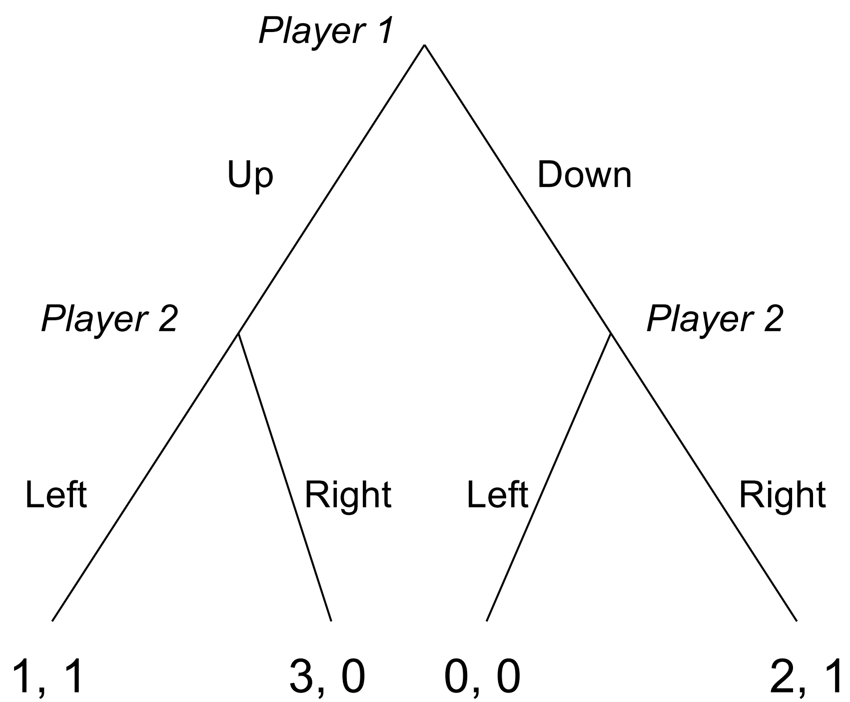
These can lead to Second-Mover Advantage

- **Atari vs Nintendo, MySpace (or earlier) vs Facebook**

COMMITMENT AS AN EXTENSIVE-FORM GAME

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

For the case of committing to a pure strategy:



COMMITMENT TO MIXED STRATEGIES

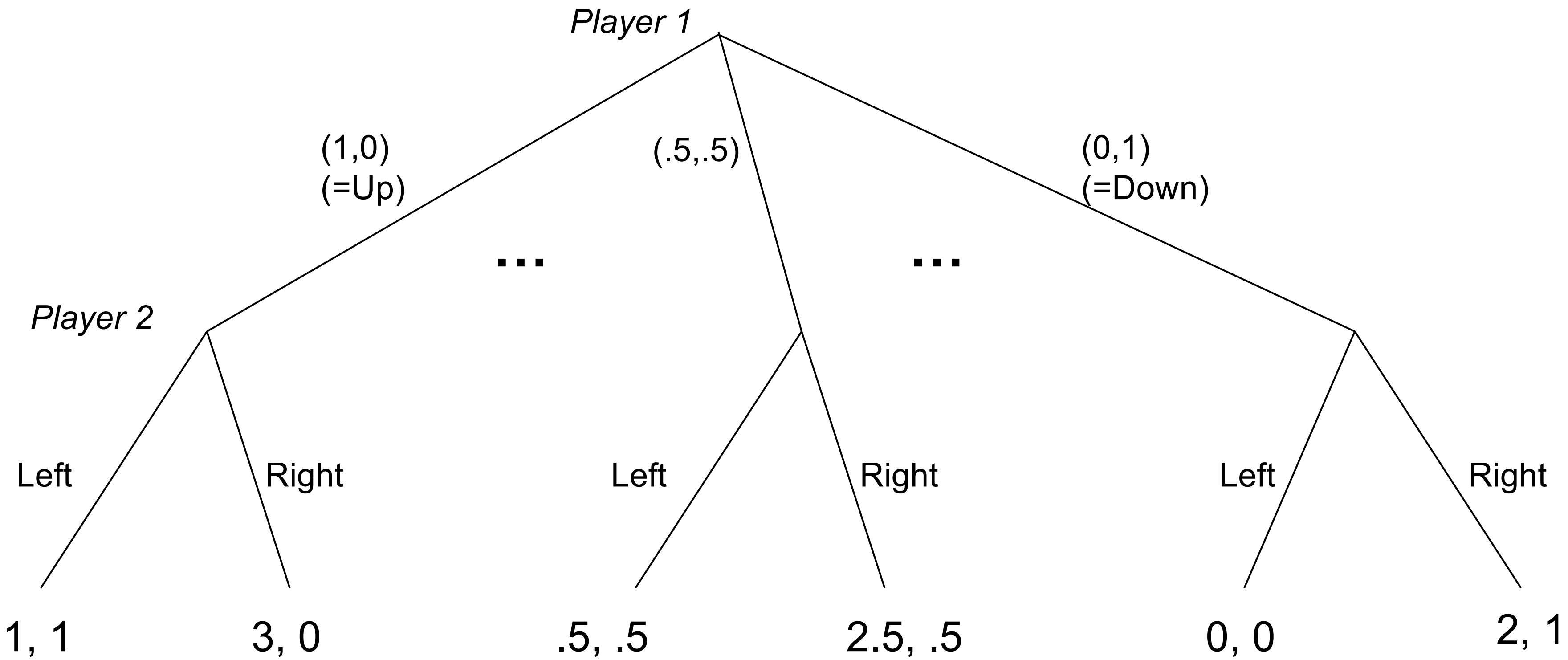
	0	1
.49	1, 1	3, 0
.51	0, 0	2, 1

What should Column do ????????

Sometimes also called a Stackelberg (mixed) strategy

COMMITMENT AS AN EXTENSIVE-FORM GAME…

For the case of committing to a mixed strategy:



- **Economist: Just an extensive-form game …**
- **Computer scientist: Infinite-size game! Representation matters**

VC

WHAT SHOULD THE LEADER COMMIT TO?

2-P
Z-S

Special case: 2-player zero-sum normal-form games

Recall: Row player plays Minimax strategy

- **Minimizes the maximum expected utility to the Col**

Doesn't matter who commits to what, when

Minimax strategies = Nash Equilibrium

= Stackelberg Equilibrium

(not the case for general games)

Polynomial time computation via LP – Lecture #4

WHAT SHOULD THE LEADER COMMIT TO?

2-P G-S

Separate LP for every column c*:

maximize $\Sigma_r\, p_r\, u_R(r, c^*)$ Row utility

s.t.

for all c, $\Sigma_r\, p_r\, u_C(r, c^*) \geq \Sigma_r\, p_r\, u_C(r, c)$ Column optimality

$\Sigma_r\, p_r = 1$

for all r, $p_r \geq 0$

Distributional constraints

Choose strategy from LP with highest objective

[Conitzer & Sandholm, Computing the optimal strategy to commit to, EC-06]

RUNNING EXAMPLE

x	1, 1	3, 0
y	0, 0	2, 1

maximize $1x + 0y$

s.t.

$1x + 0y \geq 0x + 1y$

$x + y = 1$

$x \geq 0$

$y \geq 0$

maximize $3x + 2y$

s.t.

$0x + 1y \geq 1x + 0y$

$x + y = 1$

$x \geq 0$

$y \geq 0$

IS COMMITMENT ALWAYS GOOD FOR THE LEADER?

Yes, if we allow commitment to mixed strategies

- Always weakly better to commit [von Stengel & Zamir, 2004]

What about only pure strategies?

Expected utility to Row by playing mixed Nash:
???????????

$\mathbf{E_R[\langle 1/3,1/3,1/3 \rangle] = 0}$

Expected utility to Row by any pure commitment:
???????????

$\mathbf{E_R[\langle 1,0,0 \rangle] = -1}$
$\mathbf{E_R[\langle 0,1,0 \rangle] = -1}$
$\mathbf{E_R[\langle 0,0,1 \rangle] = -1}$

	Rock	**Paper**	**Scissors**
Rock			
Paper	+1,-1	0,0	-1,+1
Scissors			

WHAT SHOULD THE LEADER COMMIT TO?

Bayesian 2-P G-S

Bayesian games: player *i* draws type θ_i from Θ

Special case: follower has only one type, leader has type θ

Like before, solve a separate LP for every column c*:

$$\textit{maximize } \Sigma_\theta \pi(\theta) \; \Sigma_r \, p_{r,\theta} \, u_{R,\theta}(r, c^*)$$

$$\textit{s.t.}$$

$$\textit{for all } c, \; \Sigma_\theta \pi(\theta) \, \Sigma_r \, p_{r,\theta} \, u_C(r, c^*) \geq \Sigma_\theta \pi(\theta) \, \Sigma_r \, p_{r,\theta} \, u_C(r, c)$$

$$\textit{for all } \theta, \; \Sigma_r \, p_{r,\theta} = 1$$

$$\textit{for all } r, \theta, \; p_{r,\theta} \geq 0$$

Choose strategy from LP with highest objective

WHAT SHOULD THE LEADER COMMIT TO?

Bayesian
N-P G-S

So, we showed polynomial-time methods for:

- **2-Player, zero-sum**
- **2-Player, general-sum**
- **2-Player, general-sum, Bayesian with 1-type follower**

In general, NP-hard to compute:

- **2-Player, general-sum, Bayesian with 1-type leader**
  - Arguably more interesting ("I know my own type")
- **2-Player, general-sum, Bayesian general**
- ***N*-Player, for *N* > 2:**
  - 1st player commits, *N*-1-Player leader-follower game, 2nd player commits, recurse until 2-Player leader-follower

STACKELBERG SECURITY GAMES

Leader-follower → Defender-attacker

- Defender is interested in protecting a set of targets
- Attacker wants to attack the targets

The defender is endowed with a set of resources

- Resources protect the targets and prevent attacks

Utilities:

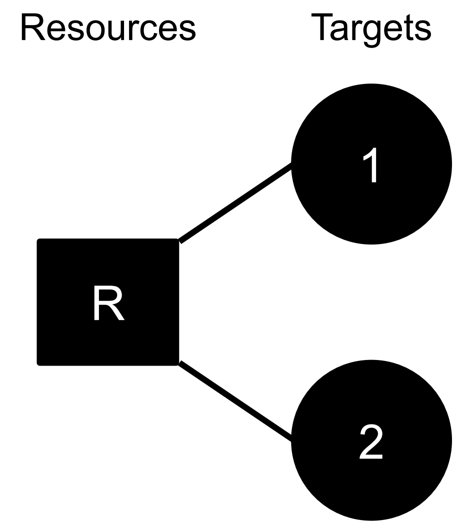
- Defender receives positive utility for preventing attacks, negative utility for “successful” attacks
- Attacker: positive utility for successful attacks, negative otherwise
- Not necessarily zero-sum

SECURITY GAMES: A FORMAL MODEL

Defined by a 3-tuple (N, U, M):

- **N: set of *n* targets**
- **U: utilities associated with defender and attacker**
- **M: all subsets of targets that can be simultaneously defended by deployments of resources**
    - A schedule $S \subseteq 2^N$ is the set of target defended by a single resource *r*
    - Assignment function $A : R \rightarrow 2^S$ is the set of all schedules a specific resource can support
- **Then we have *m* pure strategies, assigning resources such that the union of their target coverage is in M**
- **Utility $u_{c,d}(i)$ and $u_{u,d}(i)$ for the defender when target i is attacked and is covered or defended, respectively**

SIMPLE EXAMPLE



Targets	Defender		Attacker Type θ_1		Attacker Type θ_2	
i	**$u_{c,d}(i)$**	**$u_{u,d}(i)$**	**$u_{c,a}(i)$**	**$u_{u,a}(i)$**	**$u_{c,a}(i)$**	**$u_{u,a}(i)$**
1	0	-1	0	+1	0	+1
2	0	-2	0	+5	0	+1

[Blum, Haghtalab, Procaccia, Learning to Play Stackelberg Security Games, 2016]

REAL-WORLD SECURITY GAMES

Lots of deployed applications!

- Checkpoints at airports
- Patrol routes in harbors
- Scheduling Federal Air Marshalls
- Patrol routes for anti-poachers

Typically solve for strong Stackelberg Equilibria:

- Tie break in favor of the defender; always exists
- Can often "nudge" the adversary in practice

Two big practical problems: computation and uncertainty

NEXT CLASS:

SURAJ NAIR

WHEN SECURITY GAMES GO GREEN: DESIGNING DEFENDER STRATEGIES TO PREVENT POACHING AND ILLEGAL FISHING. IJCAI 2015.

BROOK STACY

DEPLOYING PAWS: FIELD OPTIMIZATION OF THE PROTECTION ASSISTANT FOR WILDLIFE SECURITY. AAAI 2016.