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 \textit{simultaneously}

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

\textcolor{red}{\textbf{No}} knowledge of the other players’ chosen actions

What if we allow \textit{sequential} action selection ...?
LEADER-FOLLOWER GAMES

Two players:

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

\[
\begin{array}{ccc}
\text{Leader} & \text{Follower} \\
\text{Top} & 0, 0 & 2, 1 \\
\text{Bottom} & 3, 0 & 0, 0 \\
\end{array}
\]

NE, iterated strict dominance

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

Commit to “Bottom”
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

For the case of committing to a pure strategy:

Player 1

Up

Player 2

Left  Right  Left  Right

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

Table:

<table>
<thead>
<tr>
<th></th>
<th>1, 1</th>
<th>3, 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 0</td>
<td>2, 1</td>
<td></td>
</tr>
</tbody>
</table>
**COMMITMENT TO MIXED STRATEGIES**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.49</td>
<td>1, 1</td>
<td>3, 0</td>
</tr>
<tr>
<td>0.51</td>
<td>0, 0</td>
<td>2, 1</td>
</tr>
</tbody>
</table>

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:

\[
\begin{array}{ccc}
\text{Player 1} & & \text{Player 2} \\
(1,0) & \text{Left} & \text{Left} \\
(0,1) & \text{Right} & \text{Right} \\
\end{array}
\]

• Economist: Just an extensive-form game …
• Computer scientist: Infinite-size game! Representation matters
WHAT SHOULD THE LEADER COMMIT TO?

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?

Separate LP for every column $c^*$:

\[
\text{maximize } \sum_r p_r u_{R}(r, c^*) \quad \text{Row utility}
\]

\[\text{s.t.}\]

\[\text{for all } c, \sum_r p_r u_{C}(r, c^*) \geq \sum_r p_r u_{C}(r, c) \quad \text{Column optimality}\]

\[\sum_r p_r = 1 \quad \text{Distributional constraints}\]

\[\text{for all } r, p_r \geq 0\]

Choose strategy from LP with highest objective

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

<table>
<thead>
<tr>
<th></th>
<th>1, 1</th>
<th>3, 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0, 0</td>
<td>2, 1</td>
<td></td>
</tr>
</tbody>
</table>

$maximize \ 1x + 0y \quad maximize \ 3x + 2y$

$s.t.$

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

$x + y = 1$

$x \geq 0$

$y \geq 0$

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

$x + y = 1$

$x \geq 0$

$y \geq 0$
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:

\[ E_R(\langle 1/3,1/3,1/3 \rangle) = 0 \]

Expected utility to Row by any pure commitment:

\[ E_R(\langle 1,0,0 \rangle) = -1 \]
\[ E_R(\langle 0,1,0 \rangle) = -1 \]
\[ E_R(\langle 0,0,1 \rangle) = -1 \]

<table>
<thead>
<tr>
<th></th>
<th>Rock</th>
<th>Paper</th>
<th>Scissors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rock</td>
<td>+1,-1</td>
<td>0,0</td>
<td>-1,+1</td>
</tr>
<tr>
<td>Paper</td>
<td>+1,-1</td>
<td>0,0</td>
<td>-1,+1</td>
</tr>
<tr>
<td>Scissors</td>
<td>0,0</td>
<td>-1,+1</td>
<td></td>
</tr>
</tbody>
</table>
WHAT SHOULD THE LEADER COMMIT TO?

Bayesian games: player $i$ draws type $\theta_i$ from $\Theta$

Special case: follower has only one type, leader has type $\theta$

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

$$\text{maximize } \sum_{\theta} \pi(\theta) \sum_r p_{r,\theta} u_{R,\theta}(r, c^*)$$

s.t.

for all $c$, $\sum_{\theta} \pi(\theta) \sum_r p_{r,\theta} u_{C}(r, c^*) \geq \sum_{\theta} \pi(\theta) \sum_r p_{r,\theta} u_{C}(r, c)$

for all $\theta$, $\sum_r p_{r,\theta} = 1$

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

Choose strategy from LP with highest objective
WHAT SHOULD THE LEADER COMMIT TO?

So, we showed \textit{polynomial-time} methods for:

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

In general, \textbf{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
- \textit{N}-Player, for \textit{N} > 2:
  - 1\textsuperscript{st} player commits, \textit{N}-1-Player leader-follower game, 2\textsuperscript{nd} player commits, recurse until 2-Player leader-follower
STACKELBERG SECURITY GAMES

Leader-follower $\rightarrow$ 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**

<table>
<thead>
<tr>
<th>Targets</th>
<th>Defender</th>
<th>Attacker Type $\theta_1$</th>
<th>Attacker Type $\theta_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>i</td>
<td>$u_{c,d}(i)$</td>
<td>$u_{u,d}(i)$</td>
<td>$u_{c,a}(i)$</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>-2</td>
<td>0</td>
</tr>
</tbody>
</table>

[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