18734 Recitation

Course Project
Audit Games
Course Project

• Teams finalized?
• 10 teams on the doc.

• Project Idea
• Related readings
Project Proposal

- Pdf document (1-2 pages):
  - Team members
  - Motivation & Problem Statement
  - Approach
  - Deliverables & Timeline

- In-class presentation by members
Game Theory
Game Theory

• Developed to explain the optimal strategy in two-person interactions.
An example:
Big Monkey and Little Monkey

One coconut per tree.
A Coconut yields 10 Calories

Big Monkey expends 2 Calories climbing the tree.
Little Monkey expends 0 Calories climbing the tree.
An example: Big Monkey and Little Monkey

- If BM climbs the tree
  - BM gets 6 C, LM gets 4 C
  - LM eats some before BM gets down
- If LM climbs the tree
  - BM gets 9 C, LM gets 1 C
  - BM eats almost all before LM gets down
- If both climb the tree
  - BM gets 7 C, LM gets 3 C
  - BM hogs coconut
- How should the monkeys each act so as to maximize their own calorie gain?
An example:
Big Monkey and Little Monkey

• Assume BM decides first
  – Two choices: wait or climb

• LM has four choices:
  – Always wait (ww), always climb (cc), same as BM (wc), opposite of BM (cw).
  – The first letter indicates Little Monkey’s move if Big Monkey waits, and the second is Little Monkey’s move if Big Monkey climbs.
An example:
Big Monkey and Little Monkey

What should Big Monkey do?
- If BM waits, LM will climb – BM gets 9
- If BM climbs, LM will wait – BM gets 4
- BM should wait.
- What about LM?
- Opposite of BM (even though we’ll never get to the right side of the tree)
An example:
Big Monkey and Little Monkey

Normal Form:

<table>
<thead>
<tr>
<th></th>
<th>Little Monkey</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cc</td>
</tr>
<tr>
<td>Big Monkey</td>
<td></td>
</tr>
<tr>
<td>w</td>
<td>9,1</td>
</tr>
<tr>
<td>c</td>
<td>5,3</td>
</tr>
</tbody>
</table>
An example: Big Monkey and Little Monkey

• These strategies (w and cw) are called best responses.
  – Given what the other guy is doing, this is the best thing to do.

• A solution where everyone is playing a best response is called a Nash equilibrium.
  – No one can unilaterally change and improve things.
An example: Big Monkey and Little Monkey

- What if the monkeys have to decide simultaneously?

Now Little Monkey has to choose before he sees Big Monkey move
two Nash equilibria (c,w), (w,c)
An example: Big Monkey and Little Monkey

• What if the monkeys have to decide simultaneously?

<table>
<thead>
<tr>
<th>Big Monkey</th>
<th>Little Monkey</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>5,3</td>
</tr>
<tr>
<td>w</td>
<td>9,1</td>
</tr>
</tbody>
</table>
Regret Minimization
Regret by Example

Strategy: outputs an action for every round

\[
\text{Total Regret}(s, s\downarrow 1) = -5 - (-6) = 1 \\
\text{regret}(s, s\downarrow 1) = 1/2
\]

Players
- Emp
- Org: \(s\)

Round 1
- 3, 2
- 1 ($6)

Round 2
- 3, 1
- 2 ($0)

Total Payoff
- Unknown
- $6

Emp: $5
Org: $6

Org: $5
Emp: $0

Total: $5
Audit Algorithm Choices

Consider 4 possible allocations of the available 30 inspections

<table>
<thead>
<tr>
<th>0</th>
<th>10</th>
<th>20</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>20</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

Weights

| 1.0 | 1.0 | 1.0 | 1.0 |

Choose allocation probabilistically based on weights
Audit Algorithm Run

<table>
<thead>
<tr>
<th>No. of Access</th>
<th>Actual Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>2</td>
</tr>
<tr>
<td>70</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Int. Caught</th>
<th>Ext. Caught</th>
<th>Observed Loss</th>
<th>Estimated Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>$2000</td>
<td>$1000</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>$750</td>
<td>$1500</td>
</tr>
</tbody>
</table>

Updated weights: 0.5, 1.0, 2.0, 1.0

Learn from observed and estimated loss
Regret Minimizing Algorithm

\[ w_s = 1 \text{ for all strategies } s \]

New audit cycle starts. Find AWAKE

Update weight* of strategies \( s \) in AWAKE

Pick \( s \) in AWAKE with probability \( D_t(s) \propto w_s \)

Estimate payoff vector Pay using Pay(\( s \))

Violation caught; obtain payoff Pay(\( s \))

\[ * \quad w_s \leftarrow w_s \cdot e^{-\text{Pay}(s) + \gamma \sum_{s'} D_t(s') \text{Pay}(s')} \]
Model/Algorithm by Example

Auditing budget: $3000/ cycle
Cost for one inspection: $100
Only 30 inspections per cycle
Employee incentives unknown

Access divided into 2 types
30 accesses
70 accesses

Loss from 1 violation (internal, external)
$500, $1000
$250, $500
Utilities

\[ U(\vec{s}, \vec{O}) = \sum_k U_1(s_k) + \sum_k U_2(O_k) \]

- Audit Cost
- Violation Cost

Average utility over \( T \) rounds

\[ = \frac{1}{T} \sum_{t=1}^{T} U(\vec{s}^t, \vec{O}^t) \]

Adversary utility unknown