MONOTONIC MAXIMIN:

A ROBUST STACKELBERG SOLUTION AGAINST BOUNDEDLY RATIONAL FOLLOWERS

Albert Xin Jiang, Thanh H. Nguyen, Milind Tambe
University of Southern California

Ariel D. Procaccia
Carnegie Mellon University

GameSec, Nov. 11, 2013

Deployed Physical Security Applications

- Limited security resources: selective checking
- Adversary monitors defense, exploits pattern

Stackelberg Games

- Leader (defender) commits to mixed strategy
- Follower (adversary) conducts surveillance and responds

Adversary

	Target #1	Target #2
Target #1	5, -3	-1, 1
Target #2	-5, 5	2, -1

Bounded Rationality

- Strong Stackelberg equilibrium: Classical game theory
  - *Assumes perfect rationality (maximize expected utility)*

- In reality, adversaries are humans

- Quantal Response (McFadden; Mckelvey & Palfrey; Yang et al)

$$q_i(x) = \frac{e^{\lambda U_i^a(x)}}{\sum_j e^{\lambda U_j^a(x)}}$$

  - Need data to estimate parameter

Robust Optimization Approaches

- Uncertainty set: set of possible response functions by the adversary
- Optimize worst-case defender utility
- Allow arbitrary adversary response: Maximin
  - *Robust but very conservative*
- Are there more interesting ways to define uncertainty set that captures bounded-rational behavior?

Monotonic Maximin

- Monotonicity: actions with higher expected utility are played with higher probability
  - QR satisfies monotonicity

- Monotonic maximin: optimize defender utility against worst-case monotonic adversary
  - A robust alternative to QR
  - Provides guarantee against all “reasonably rational” adversary

- Computing monotonic maximin
  - MILP formulation
  - Approximations

Game

- Defender mixed strategy $x \in X \subset \mathbb{R}^m$
  - *X* convex
- Adversary mixed strategy $y \in Y$

$$Y = \{y \in R^n | y \geq 0, 1^T y = 1\}$$

- Payoff Matrices $A, B \in \mathbb{R}^{m \times n}$

- Expected utility $x^T A y$ $x^T B y$

Behavior Models of Adversary

- Logit Quantal Resposne

$$q_i(x) = \frac{e^{\lambda U_i^a(x)}}{\sum_j e^{\lambda U_j^a(x)}}$$

- Regular Quantal Response (Goeree et al)

1. Interiority: $P_j(\boldsymbol{u}) > 0$ for all j.
2. Continuity: $P_j(\boldsymbol{u})$ is continuously differentiable.
3. Responsiveness: $\frac{\partial P_j(\boldsymbol{u})}{\partial u_j} > 0$ for all j.
4. Monotonicity: $u_j > u_k \Rightarrow P_j(\boldsymbol{u}) > P_k(\boldsymbol{u})$ for all j, k.

Monotonic Maximin

Definition 1. *Given $x \in X, y \in Y$, we say y satisfies* closed monotonicity *if for all $i, j \in [n]$, $x^T B e_i \geq x^T B e_j \Rightarrow y_i \geq y_j$.*

- $Q(x) \subseteq Y$ the set of closed monotonic adversary strategies
- Monotonic Maximin:

$$\arg\max_{x \in X} \min_{y \in Q(x)} x^T A y$$

Properties of Monotonic Maximin

- Monotonic maximin exists in all Stackelberg games
- For zero-sum games, coincides with maximin
- Captures all Regular Quantal Response models
  - Worst-case monotonic response is arbitrarily close to worst-case Regular QR
- Captures other model uncertainties, e.g. payoff
  - add i.i.d. noise (smooth, zero mean) to adversary payoff, assuming adversary best responds, the resulting behavior is monotonic

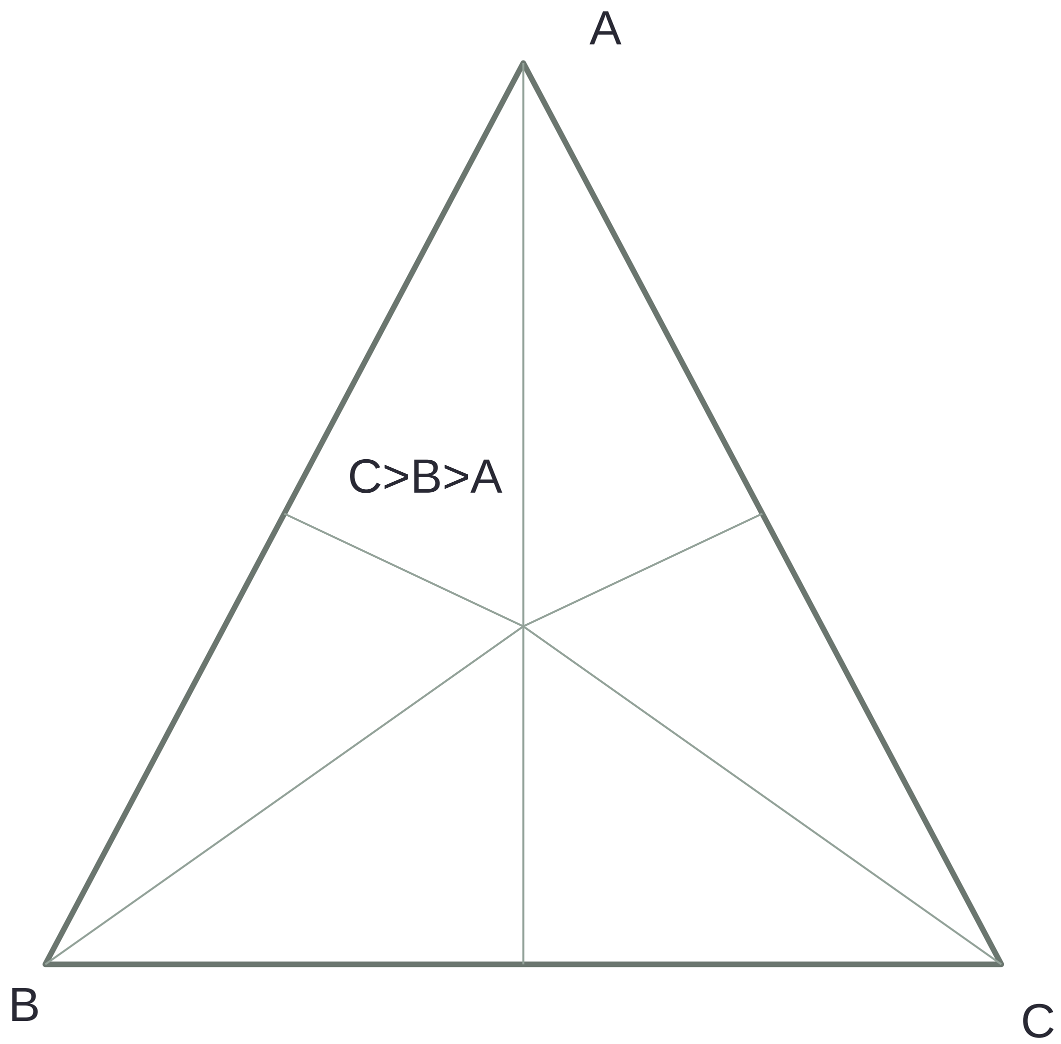
Computation

$$\arg\max_{\boldsymbol{x}\in X} \min_{\boldsymbol{y}\in Q(\boldsymbol{x})} \boldsymbol{x}^T A \boldsymbol{y}$$

- Nontrivial because feasible space of follower depends on leader strategy

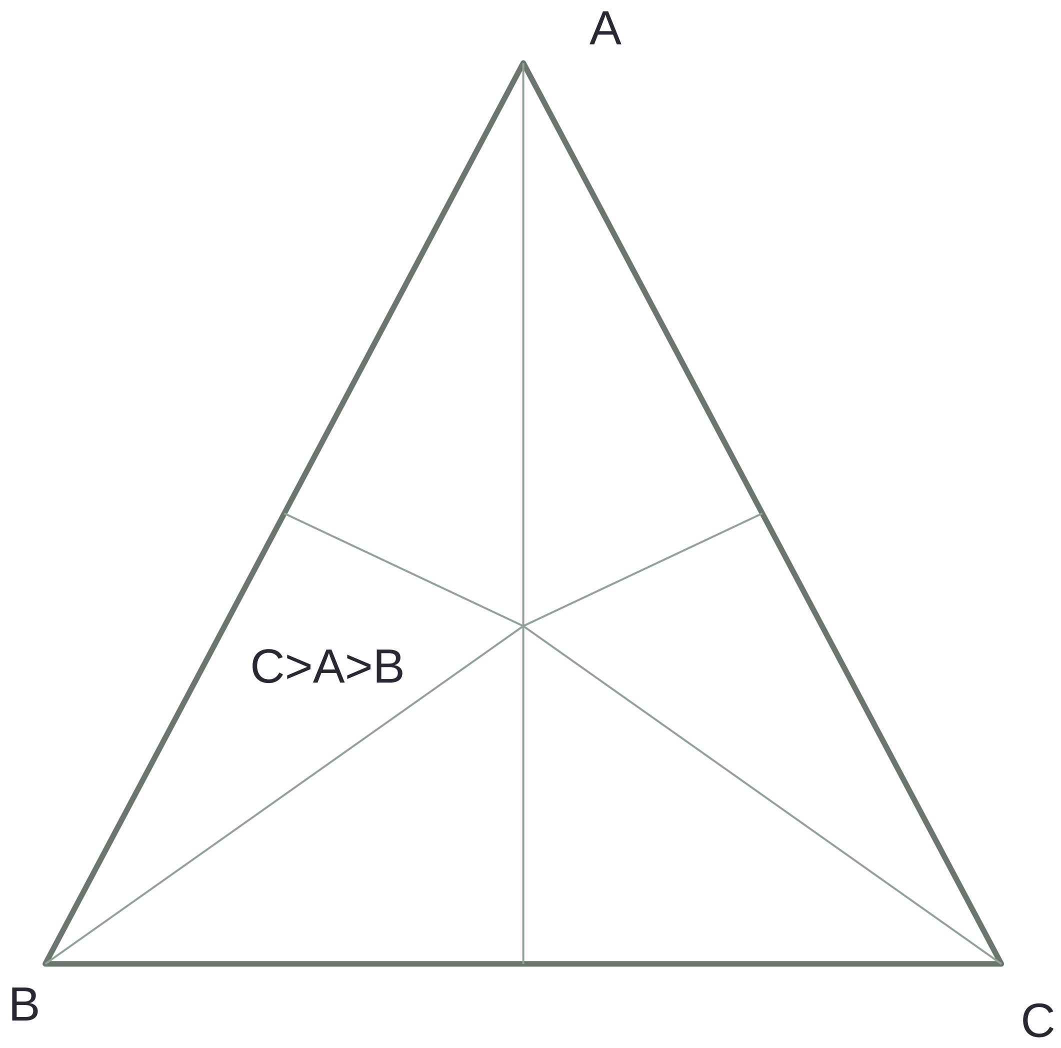
- The set Q(x) depends only on the ordering of actions in terms of adversary expected utilities
  - *Finite # of orderings, thus finite # of possible Q(x)*

Partitioning of leader strategy space X



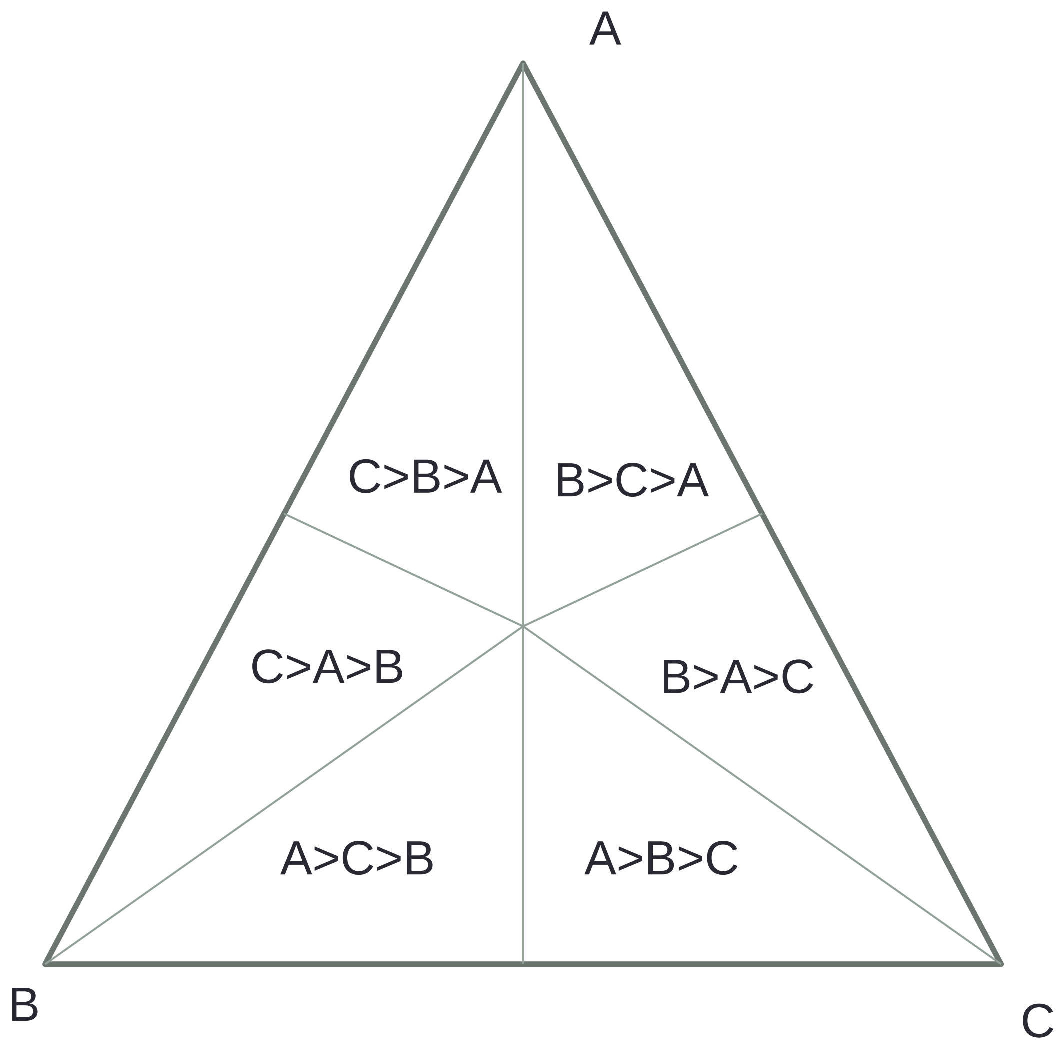
Corresponding Q(x):
$y_C >= y_B >= y_A$

Partitioning of leader strategy space X



Corresponding Q(x):
$y_C >= y_A >= y_B$

Partitioning of leader strategy space X



Multiple-LP approach

- For each total order on the set of actions, solve

$$\max_{\boldsymbol{x} \in E^{-1}(\mathcal{E})} \min_{\boldsymbol{y} \in Q(x)} x^T A y$$

- Can be formulated as LP

$$\begin{aligned} V_F = \max_{\boldsymbol{x}, \boldsymbol{\lambda}, t} \; & t \\ & Cx \leq d \\ & x^T BF \geq 0 \\ & F\lambda + t1 \leq A^T x \\ & \lambda \geq 0 \end{aligned}$$

- Only need to look at strict orders (permutations)
  - Still exponential # of LPs!

MILP formulation

- Use integer variables to encode the ordering
- z_{ij} binary integer that indicates whether adversary utility for action i is better than utility for action j

- Mixed integer quadratic program; can transform to MILP

$$
\begin{aligned}
\max_{\boldsymbol{x},\boldsymbol{w},t,\boldsymbol{z}} \quad & t \\
& C\boldsymbol{x} \leq d \\
& \boldsymbol{x}^T B \boldsymbol{e_i} + M(1 - z_{ij}) \geq \boldsymbol{x}^T B \boldsymbol{e_j}, \ \forall i, j \\
& \sum_{i,j} w_{ij}(\boldsymbol{e_i} - \boldsymbol{e_j}) + t\mathbf{1} \leq A^T \boldsymbol{x} \\
& 0 \leq w_{ij} \leq z_{ij} N \\
& z_{ij} \in \{0, 1\} \\
& z_{ij} + z_{ji} \geq 1 \\
& (1 - z_{ij}) + (1 - z_{jk}) + z_{ik} \geq 1.
\end{aligned}
$$

Top-monotonic maximin

- Top-monotonicity: the best response action is played with higher probability than other actions
  - For each action i,

$$x^T B e_i \geq x^T B e_j \; \forall j \Rightarrow y_i \geq y_j \; \forall j.$$

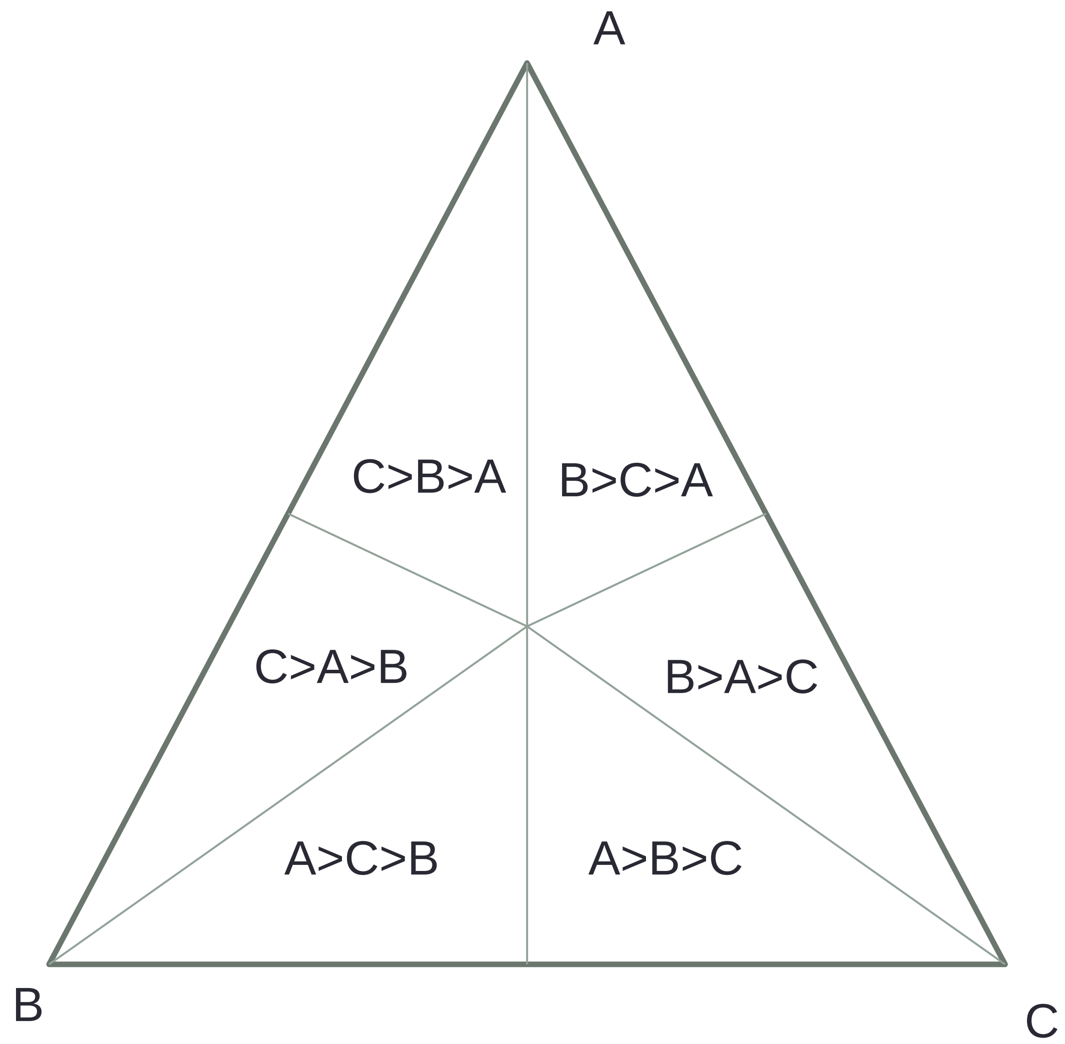
- Top-monotonic maximin: defined analogously

$$\arg\max_{x \in X} \min_{y \in \widehat{Q}(x)} x^T A y$$

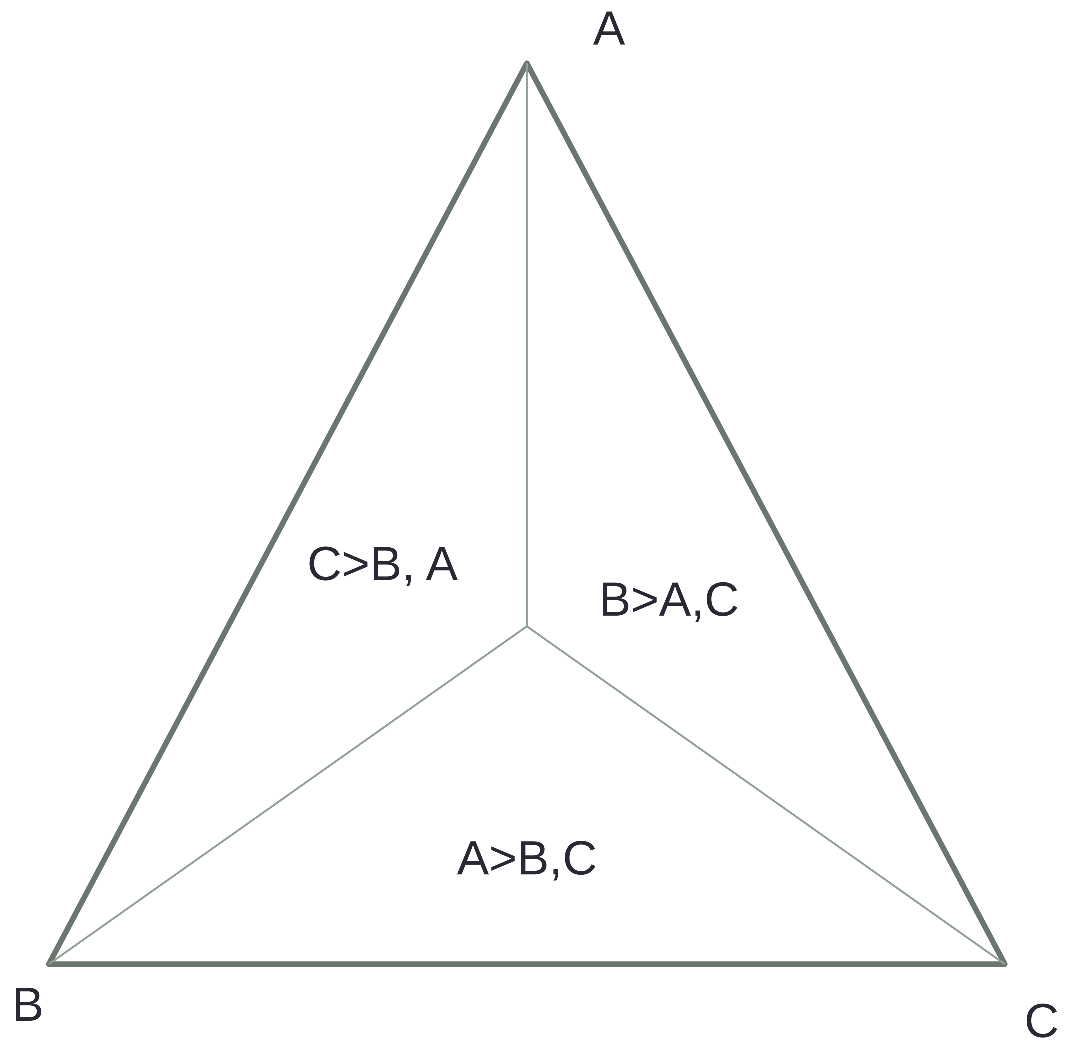
  - Lower bound on MM, i.e. more conservative

- Computation: polynomial time
  - solve n LPs, one for the case of action i being best response

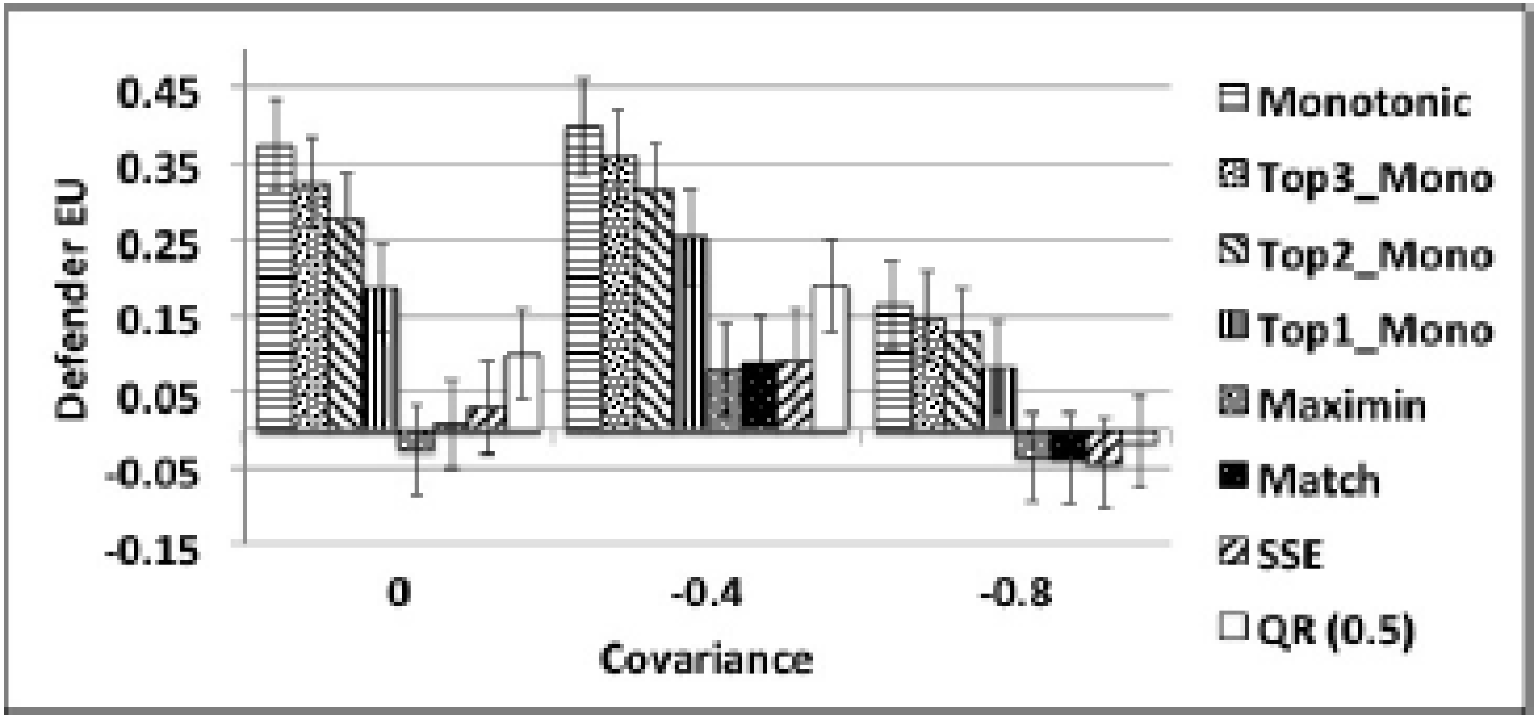
Partitioning of X: monotonic maximin



Partitioning of X: top-monotonic

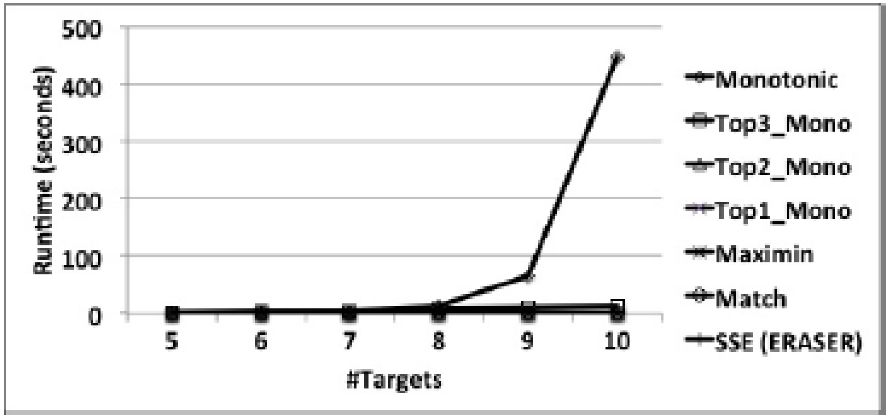


Experiments: solution quality

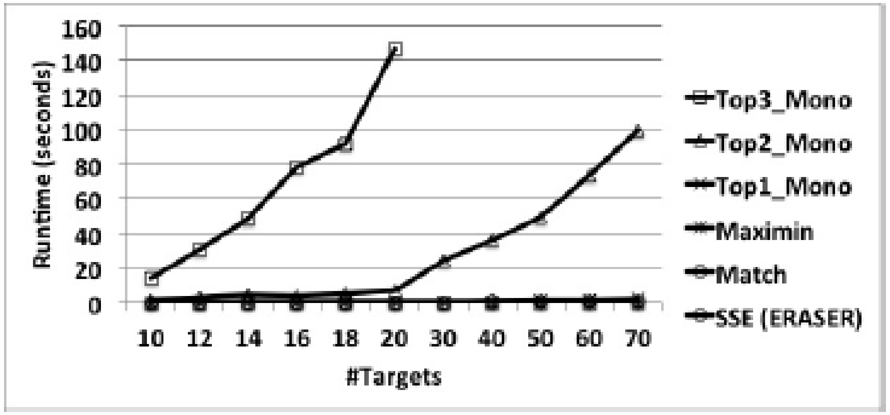


(a) 6 Targets, 3 Defender Resources

Runtime performance



(a) 5-10 Targets, 3 Defender Resources



(b) 10-70 Targets, 6 Defender Resources

Conclusions

- A robust-optimization approach to dealing with bounded rationality in Stackelberg games
  - *Monotonic maximin: robust against any monotonic adversary*
  - *Computing MM: formulate as MILP*
  - *Top-monotonic maximin: a more conservative solution; easier to compute*

Future Work and Open Problems

- More efficient computation
- Relations to / combining with other uncertainties
- How to incorporate data
- Multiple followers
  - Replacing QRE with monotonic version