CERIAS

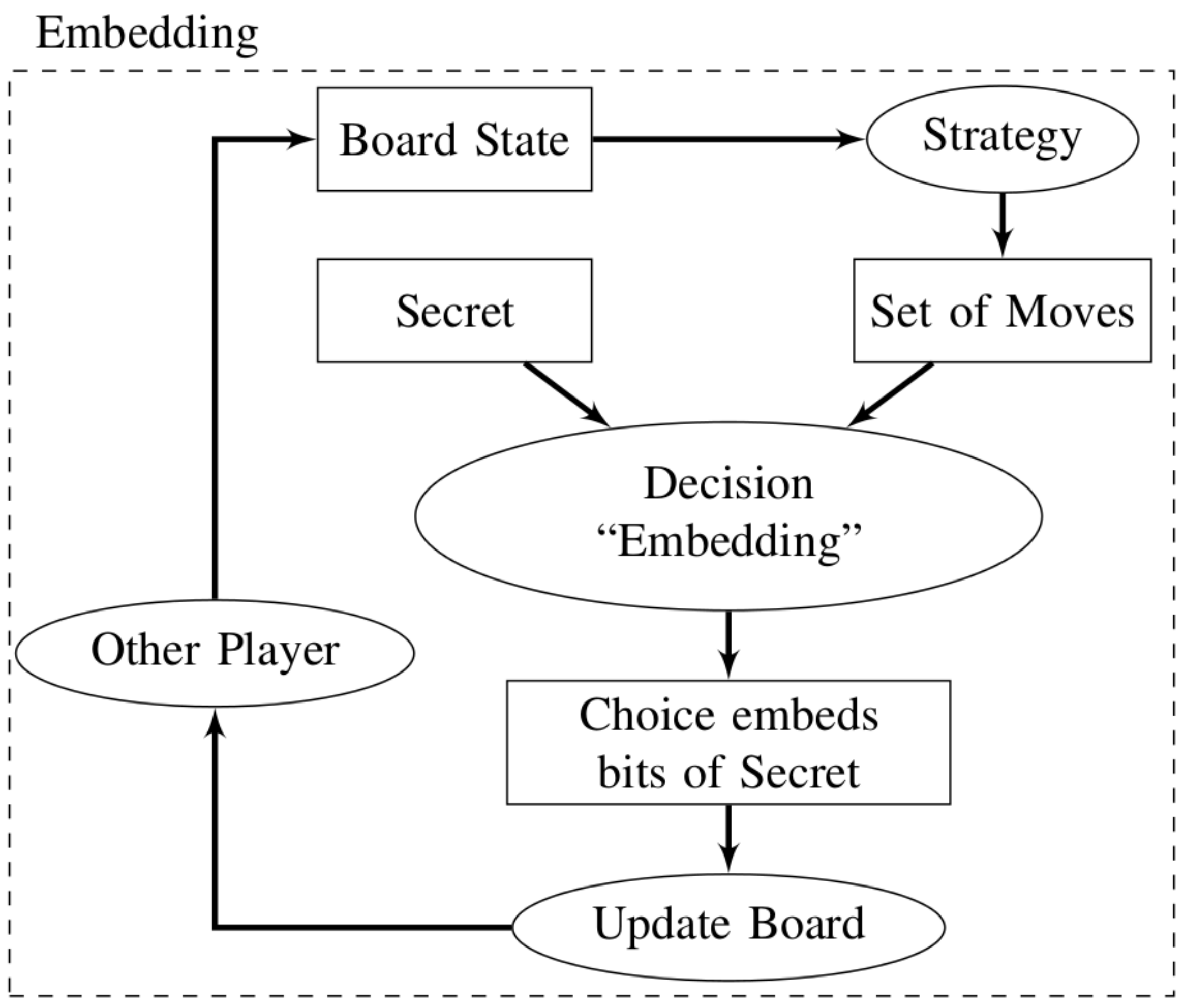
The Center for Education and Research in Information Assurance and Security

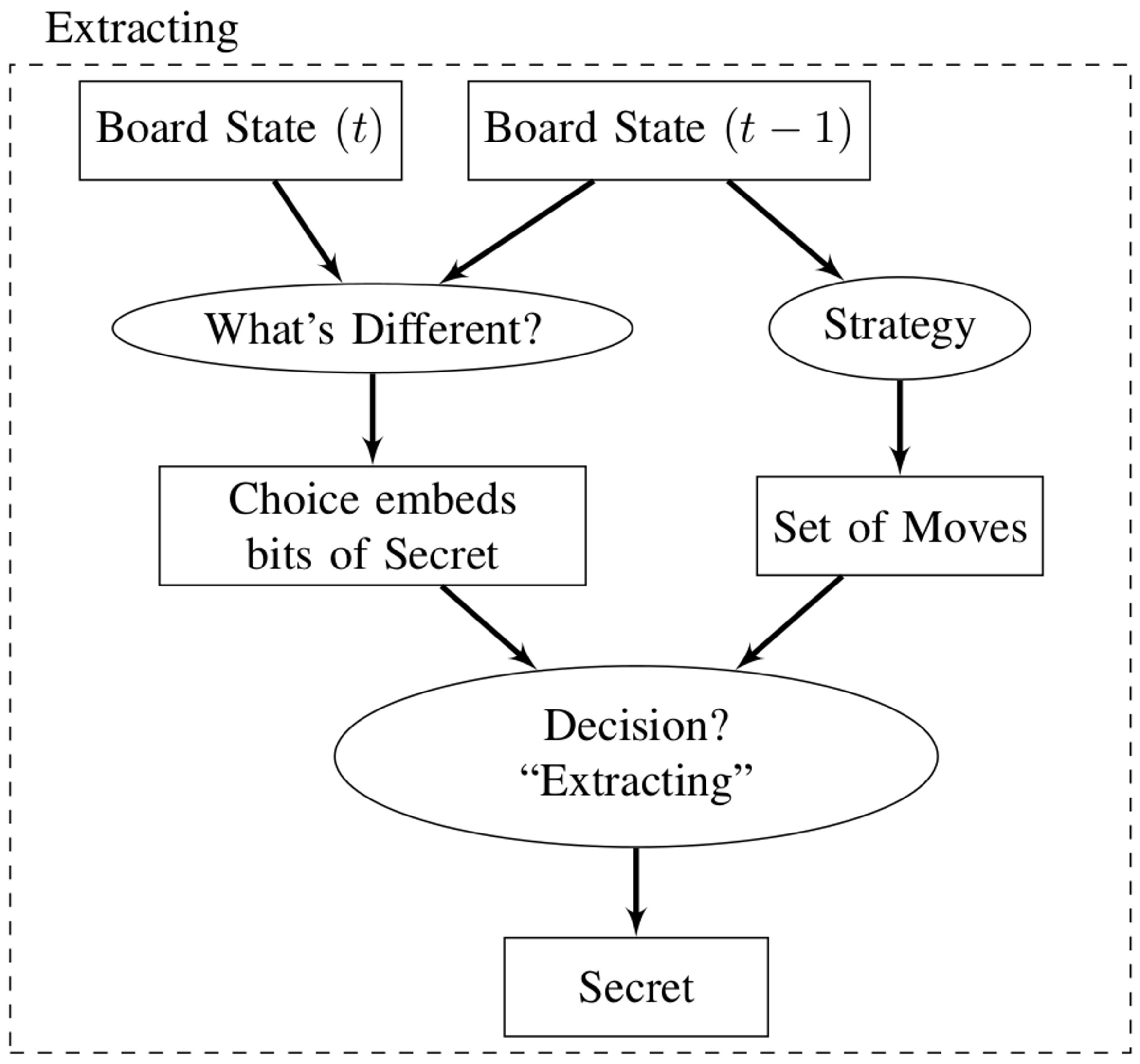
Detecting Tic-Tac-Stego: Anomaly Detection for Steganalysis in Games

Philip C. Ritchey and Vernon J. Rego

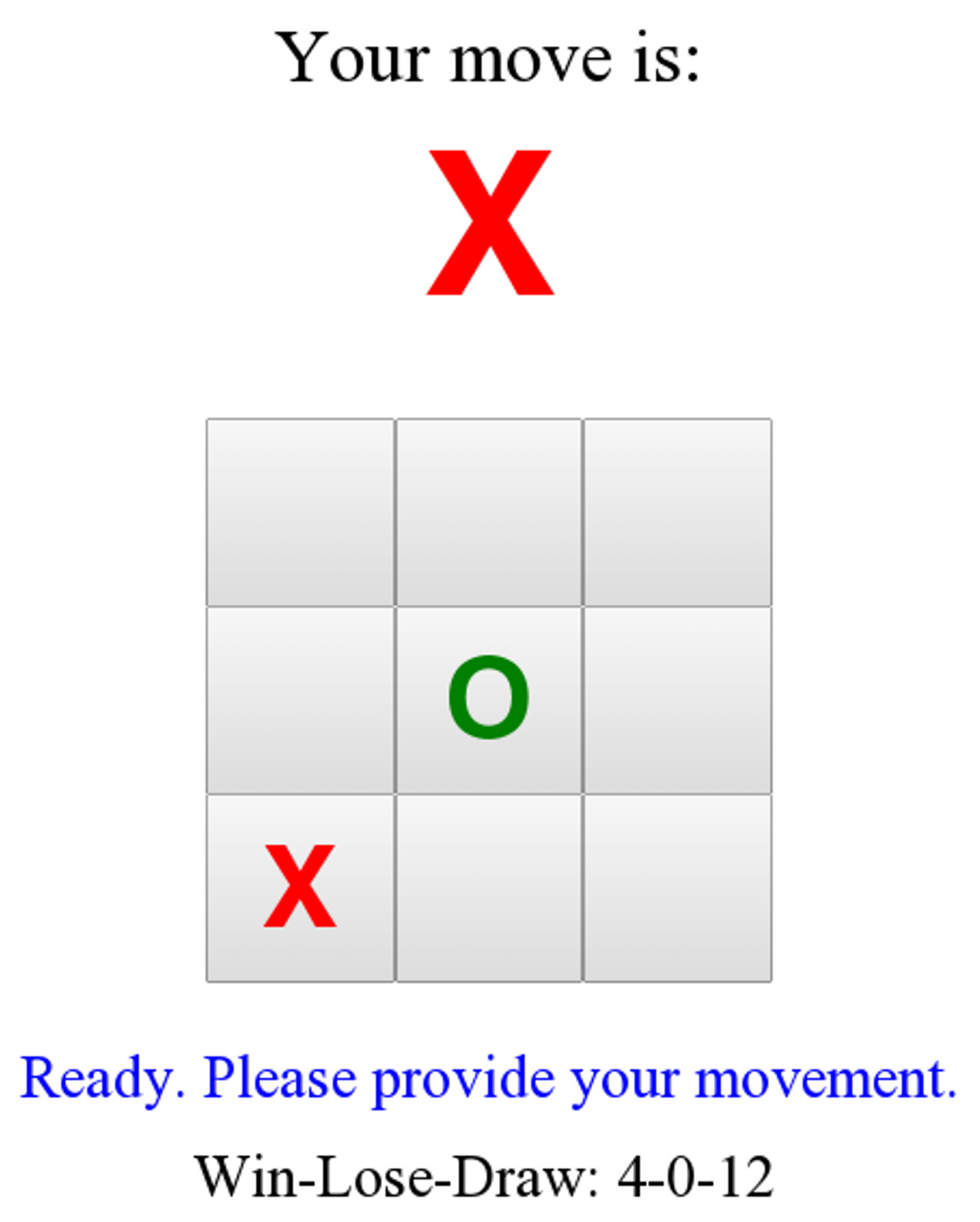
Department of Computer Science, Purdue University

The Tic-Tac-Stego Methodology





Tic-Tac-Toe Data Collection


Your move is:

X

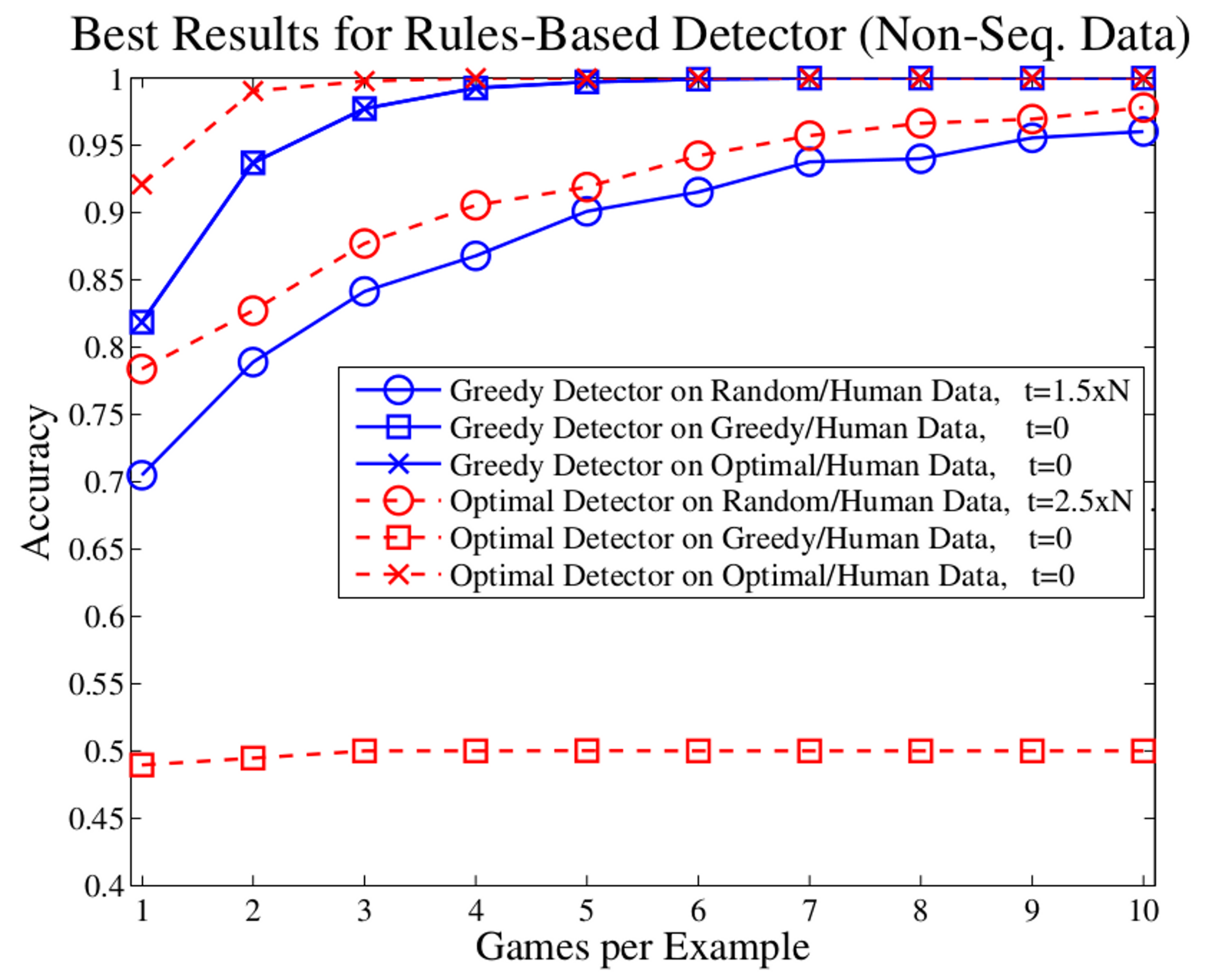
Ready. Please provide your movement.

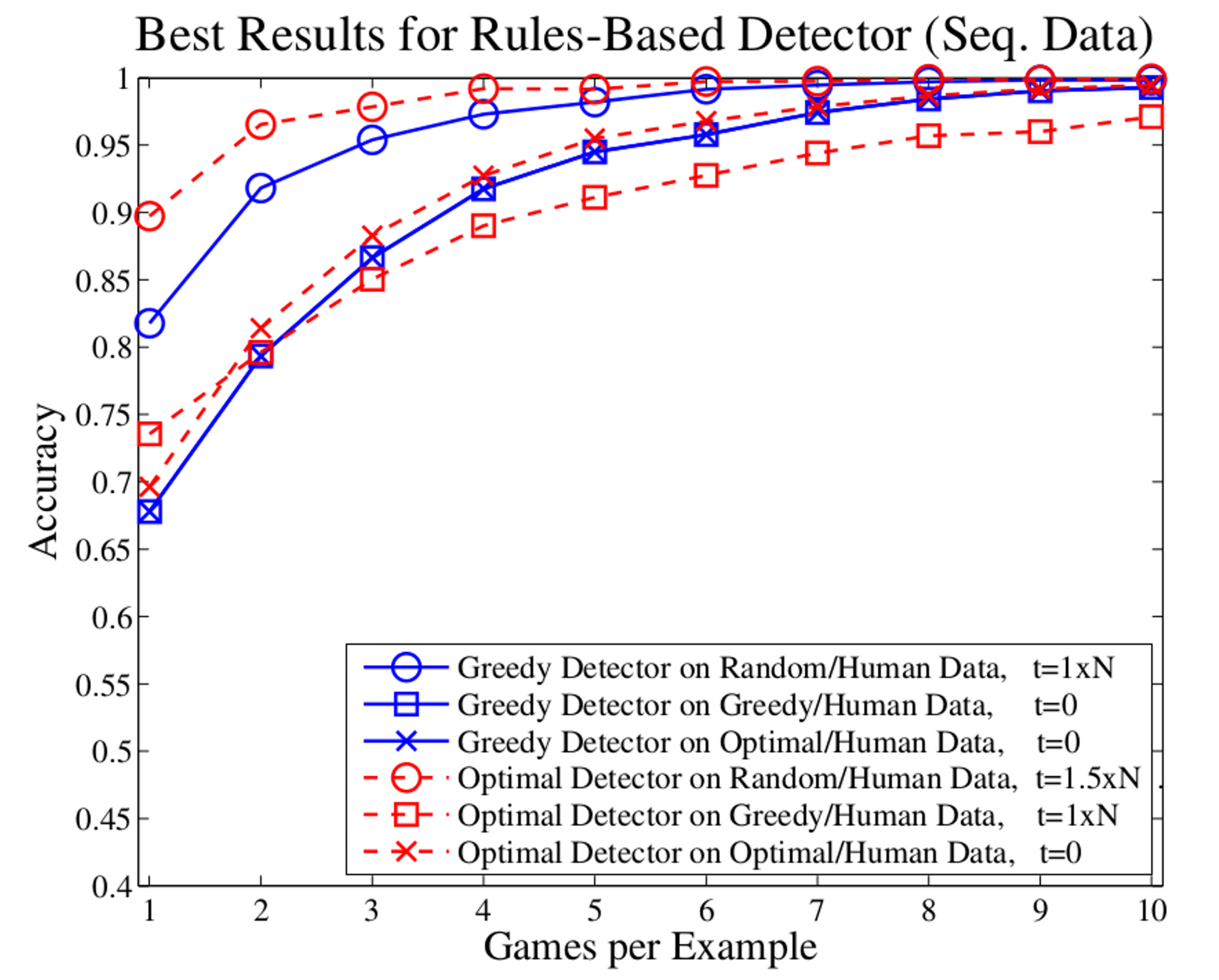
Win-Lose-Draw: 4-0-12

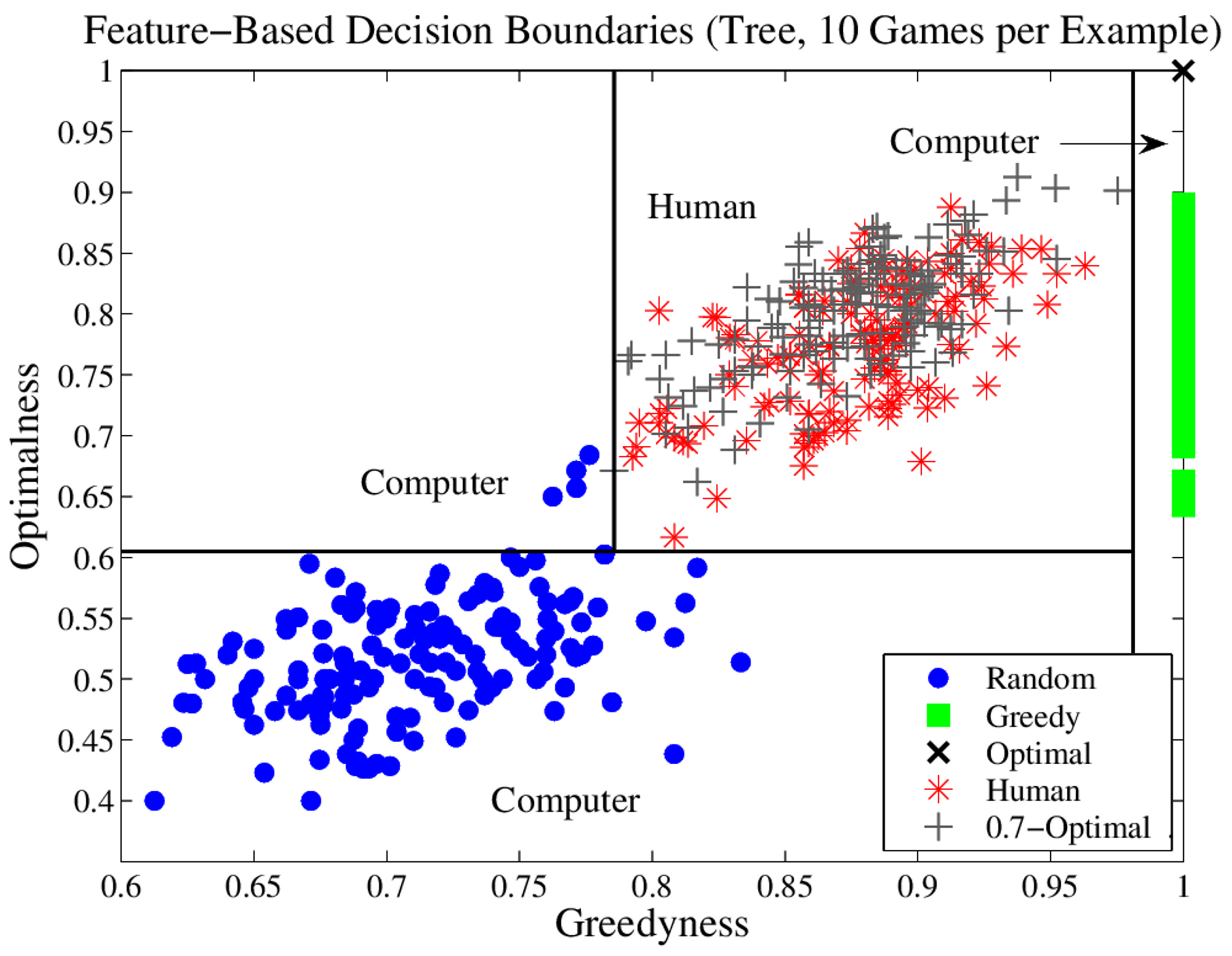
18990 human-generated moves recorded

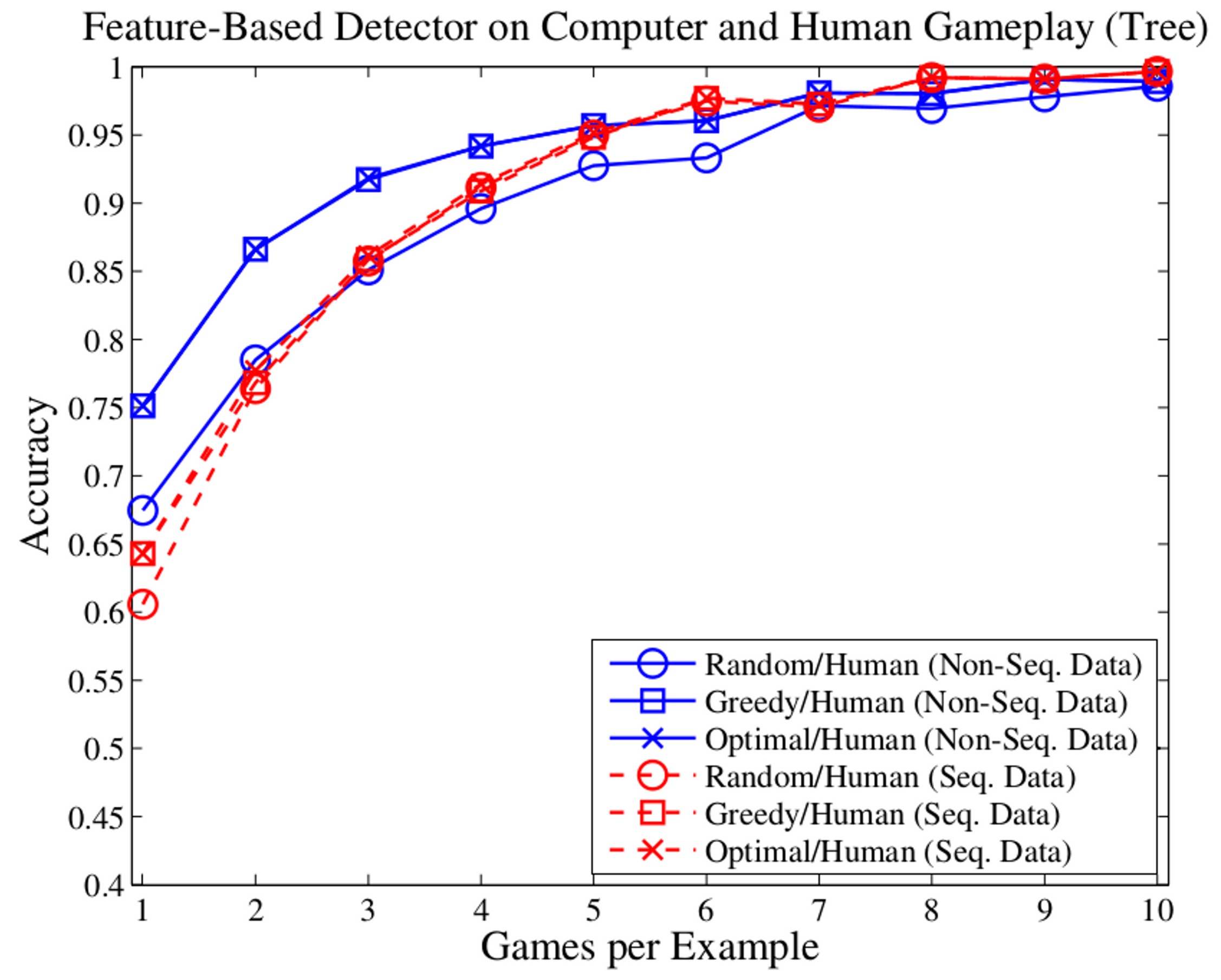
Three Anomaly Detectors

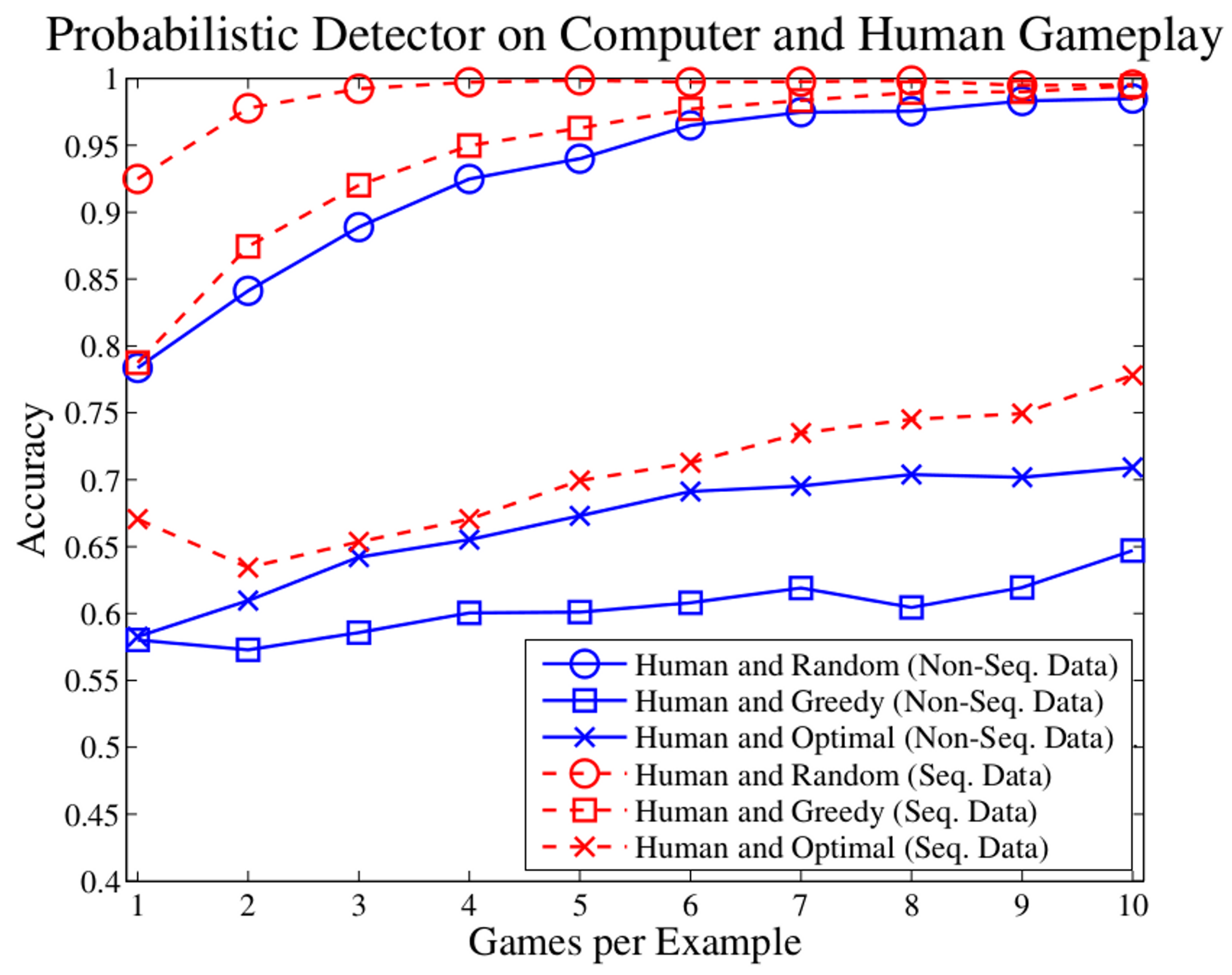
- Rules-based
  - Dirty if count of rule violations exceeds threshold.
- Feature-based
  - Learn decision boundaries from training data.
  - Dirty if gameplay features are too far from human.
- Probabilistic-based
  - Learn Markov chains for computers and humans.
  - Learn decision threshold from training data.
  - Dirty if gameplay is not sufficiently likely human.


Best Results for Rules-Based Detector (Non-Seq. Data)


Best Results for Rules-Based Detector (Seq. Data)


Feature–Based Decision Boundaries (Tree, 10 Games per Example)


Feature-Based Detector on Computer and Human Gameplay (Tree)


Probabilistic Detector on Computer and Human Gameplay

Conclusions

- Humans do not make optimal play.
  - Agrees with results from cognitive psychology.
- Humans do not even make greedy play.
  - Sometimes humans make stupid plays.
- Data collection methodology matters.
  - Sequential: more natural, more accurate for detection, less likely to capture human quirks.
- The warden can very accurately distinguish between human gameplay and pure rules-based synthetic gameplay.
  - If the warden cannot predict the stego-agent, feature-based detection is the best.
  - If the warden *can* predict the stego-agent, rules-based detection is the best.
- Results suggest improvements can be made to the stego-agent to decrease the warden's ability to distinguish authentic gameplay from synthetic.
  - See 0.7-Optimal gameplay features.

CERIAS

PURDUE UNIVERSITY