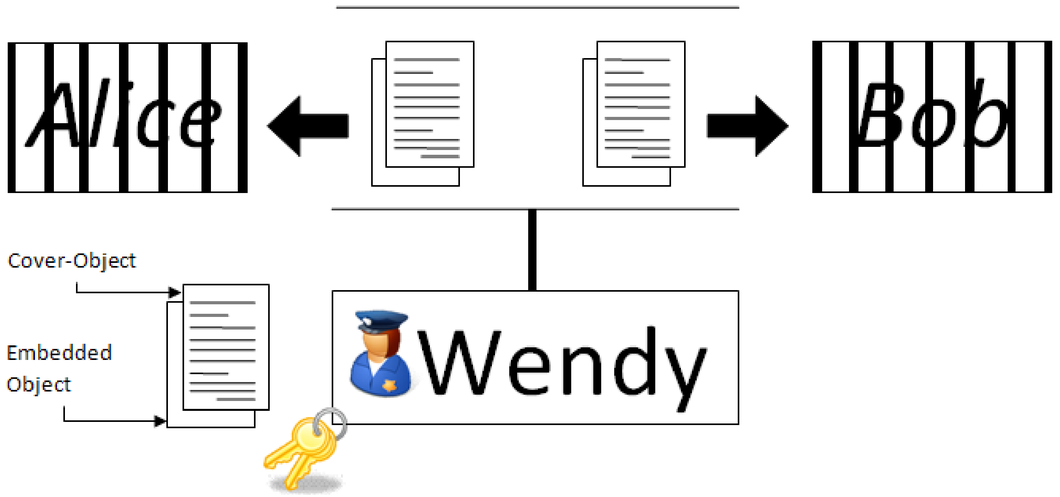
CERIAS

The Center for Education and Research in Information Assurance and Security

Covert Channels in Combinatorial Games

Philip Ritchey and Vernon Rego
Department of Computer Science, Purdue University

The Prisoners' Problem



Combinatorial Games

- 2 players
- Perfect Information
- No Chance Moves

Why Games?

- Dynamic
- Interactive
- Easy To Play
- Ubiquitous

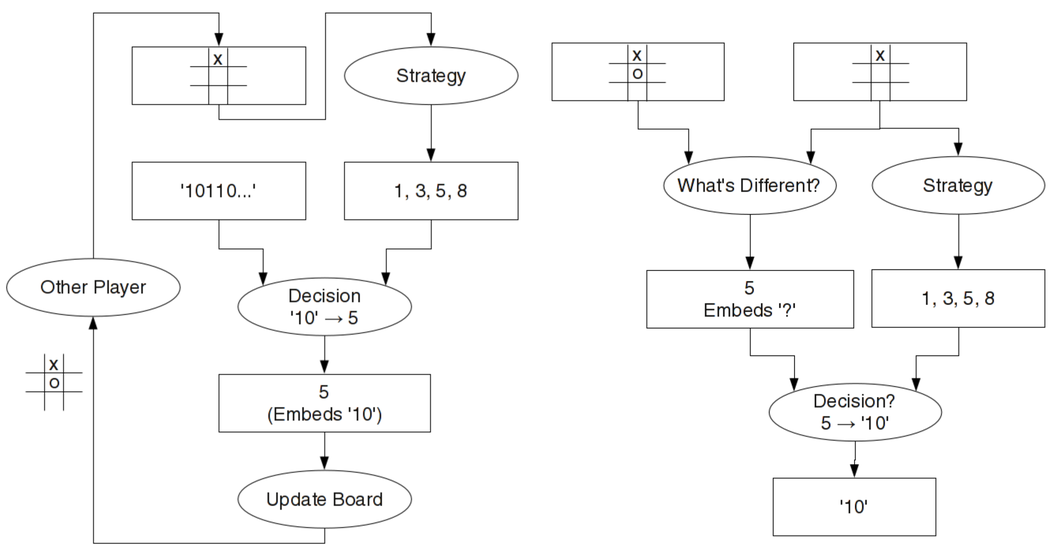
Examples:

- Angels and Devils
- Chess
- Checkers
- Chomp
- Connect-4
- Dots
- Go

…

- Tic-Tac-Toe

Methodology



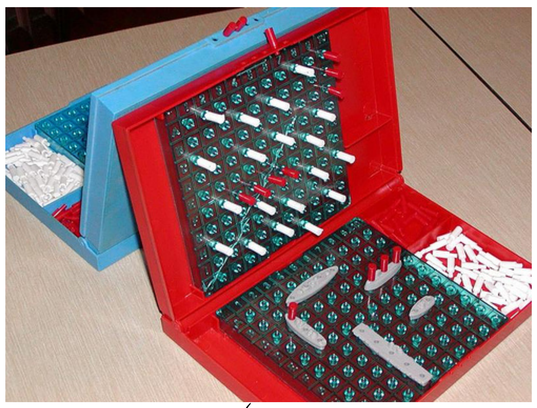
Detection Strategies

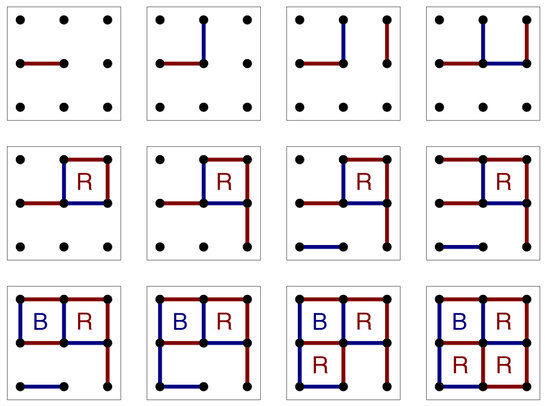
- Stupid move → suspicious
  - Mean capacity for X = 7.455 bits/game
  - Mean capacity for O = 6.650 bits/game
- Non-optimal move → suspicious
  - Mean capacity for X = 7.489 bits/game
  - Mean capacity for O = 4.326 bits/game
- Optimality out of bounds → suspicious
  - Mean capacity for X = 7.644 bits/game
  - Mean capacity for O = 5.429 bits/game
- Compare to Model of Human Gameplay
  - What model? "We're working on it!"

Other Games

$$C = \frac{1}{N} \sum_{i=1}^{2n(n-1)} [\log_2(i)]$$

C(n=10,N=2) = 506 C(n=20,N=11) = 529





$$C = \frac{1}{2} \sum_{i=100-m}^{100} [\log_2(i)]$$

C(m=16) = 51 C(m=99) = 240

$$C_P = [\log_2(1{,}925{,}751{,}392)] = 30$$

Games ~ Structured Interactions

- Why study games?
  - Generalizable
  - Human problem solving **not** well understood
  - Playing games is computationally trivial
  - Playing games *well* or *human-like* is not.
- Structured Interactions
  - N participants interacting according to a set of rules
  - Rules and actions are public
  - Captures many real-world systems
    - Network Protocols, Traffic, Natural Language, Stock Market, Negotiation.
- Anomaly Detection
  - Detecting covert channel usage is anomaly detection
  - Requires models of normal system behavior
  - How should we model human behavior?
    - Impact: Identification, Authentication, Insider Threat.

CERIAS

PURDUE UNIVERSITY