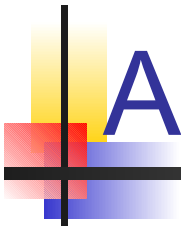


Ymer: A Statistical Model Checker

Håkan L. S. Younes

Carnegie Mellon University

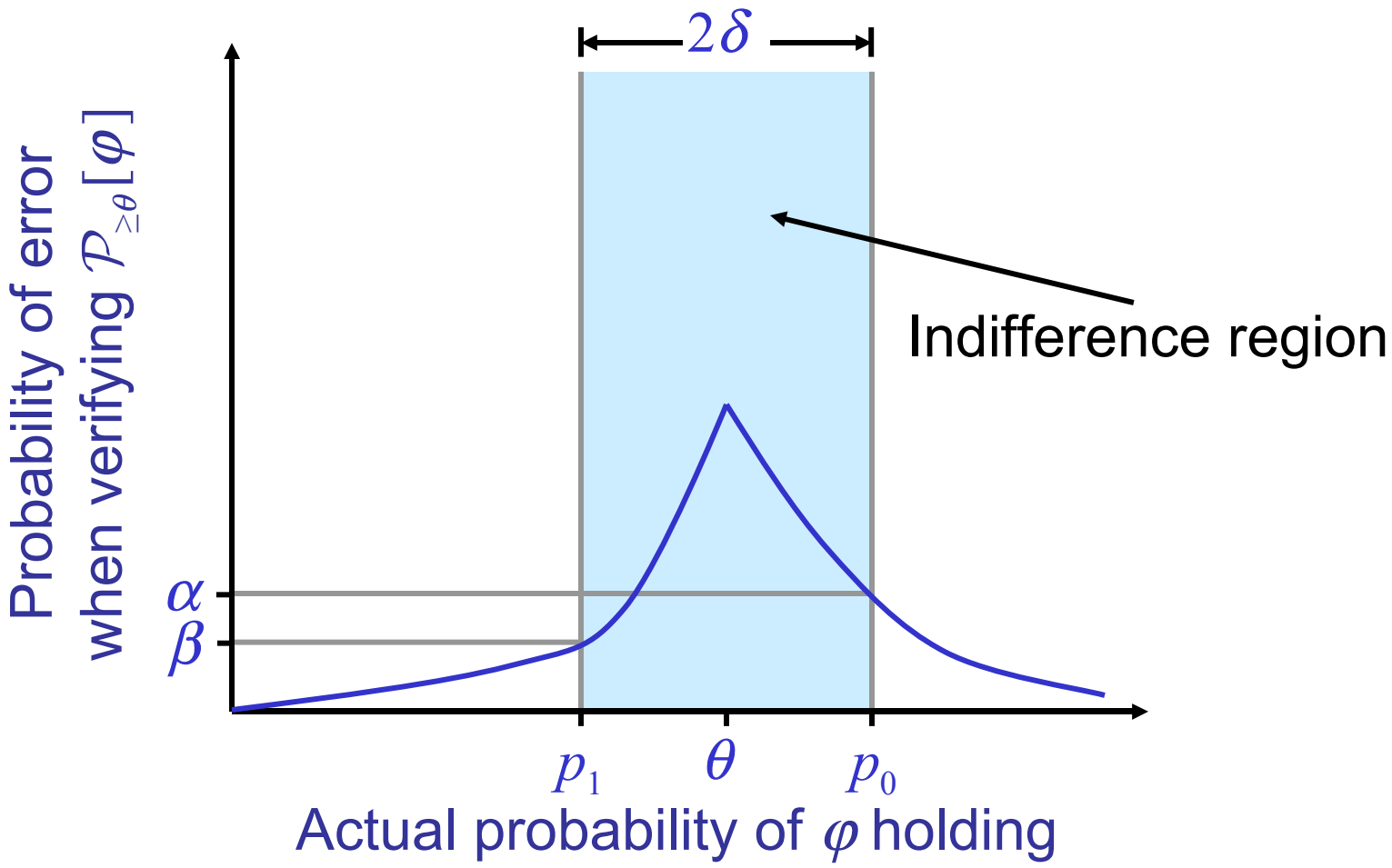
Probabilistic Model Checking

- Given a model M, a state s, and a property Φ, does Φ hold in s for M?
  - Model: stochastic discrete event system
  - Property: probabilistic temporal logic formula
    - Example: $\mathcal{P}_{\geq 0.1}[\top\, \mathcal{U}^{\leq 5}\, full\,]$

Statistical Solution Method

- Use acceptance sampling to verify probabilistic properties
  - Hypothesis: $\mathcal{P}_{\geq\theta}[\varphi]$
  - Observation: verify φ over a sample path
- Bounds on probability of verification error
  - Probability of false negative: $\leq \alpha$
  - Probability of false positive: $\leq \beta$

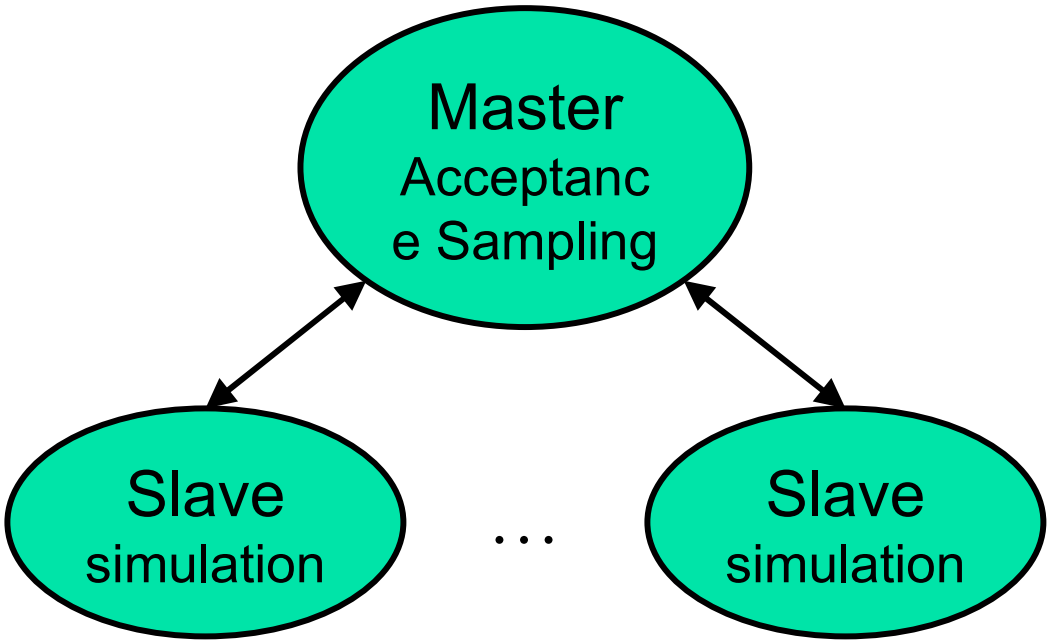
Error Bounds

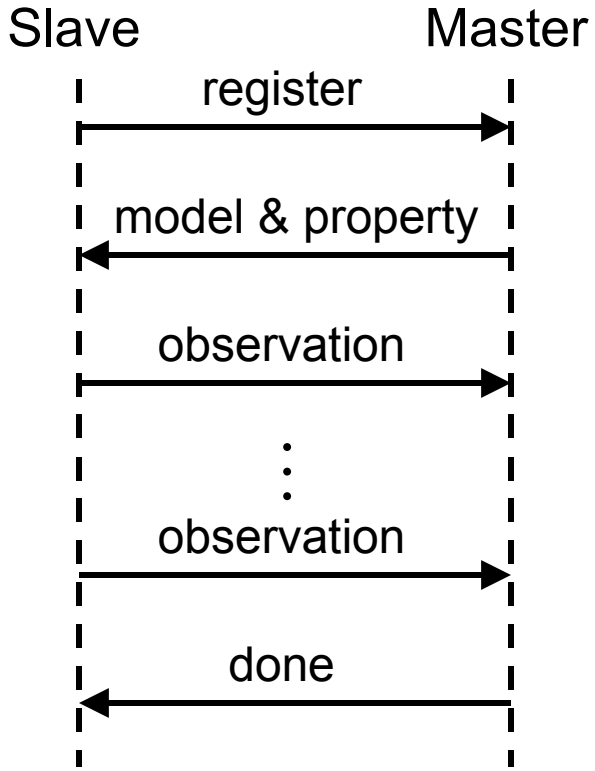


Ymer at a Glance

- Supports time-homogeneous generalized semi-Markov processes
- Limited to time-bounded properties
- Distributed acceptance sampling (even with sequential acceptance sampling)
- Purely statistical approach for verifying nested probabilistic statements

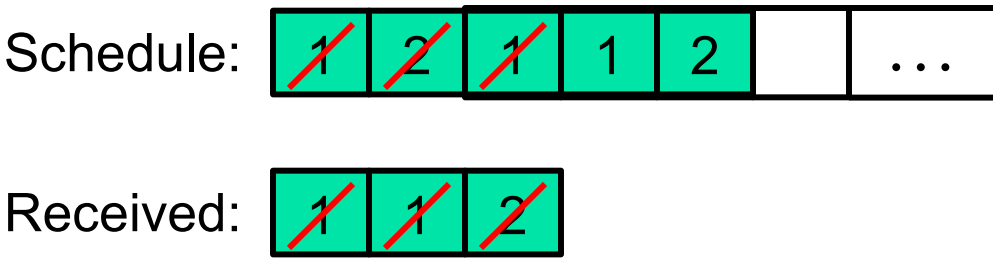
Distributed Acceptance Sampling





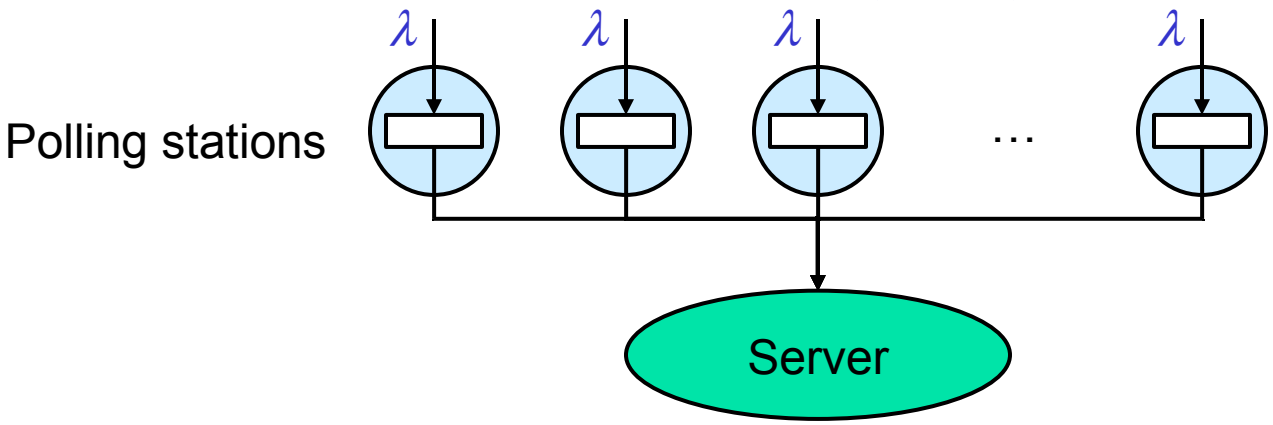
Avoiding Sample Bias

- Process observations as they come in?
  - No, bias against observations that take a long time to generate (long sample paths)
- Process observations according to a predetermined schedule

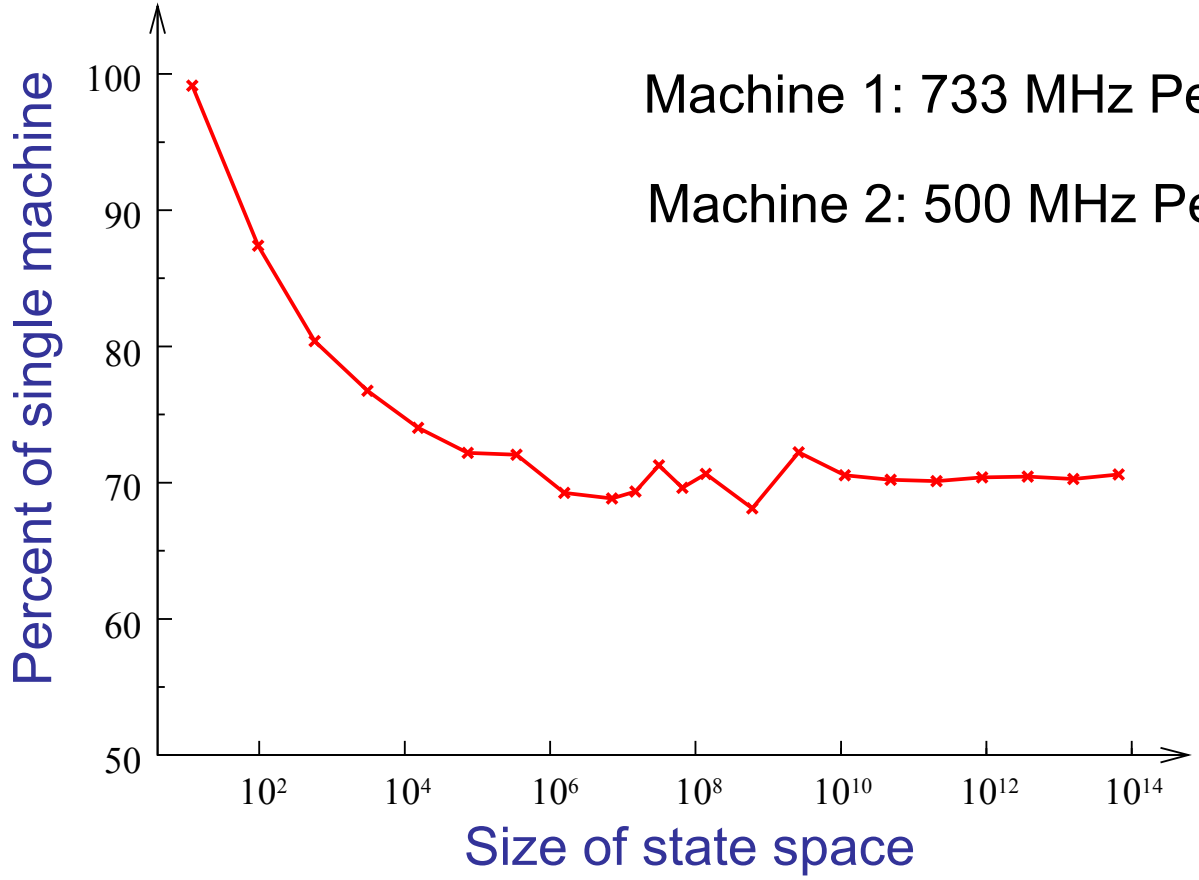


Case Study: Symmetric Polling System

- Single server, n polling stations
- Stations are attended in cyclic order
- Each station can hold one message
- State space of size $O(n \cdot 2^n)$



Results

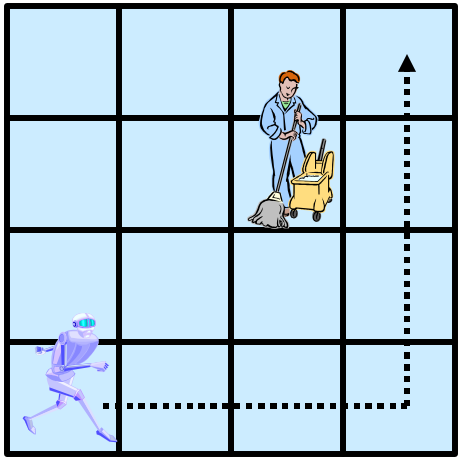


Machine 1: 733 MHz Pentium III

Machine 2: 500 MHz Pentium III

Nested Probabilistic Statements: Robot Grid World

- Probability is at least 0.9 that goal is reached within 100 seconds while periodically communicating
  - $\mathcal{P}_{\geq 0.9}[\mathcal{P}_{\geq 0.5}[\top\ \mathcal{U}^{\leq 9}\ comm]\ \mathcal{U}^{\leq 100}\ goal\ ]$



Statistical Verification of Nested Probabilistic Statements

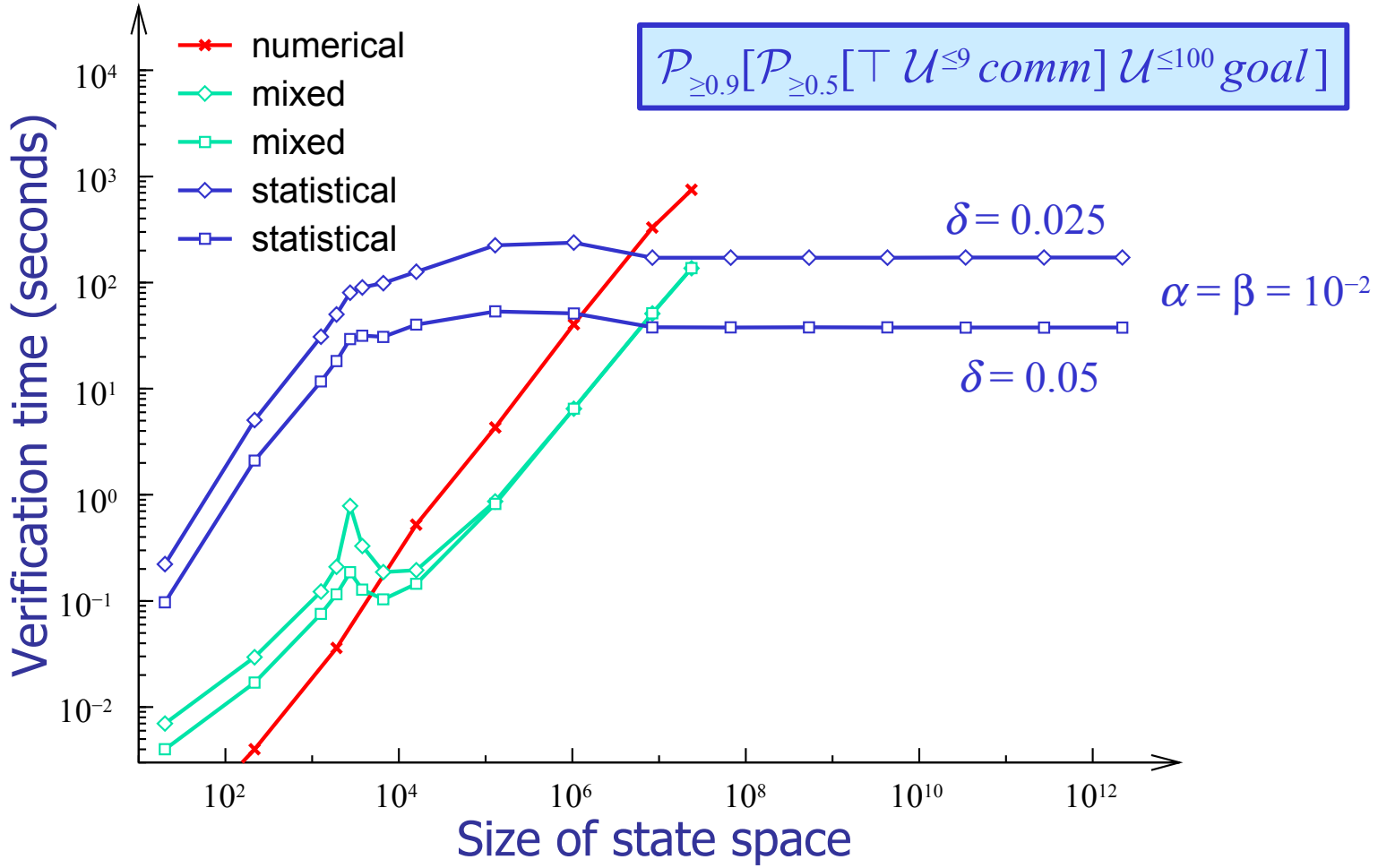
- Cannot verify path formula without some probability of error
  - Probability of false negative: $\leq \alpha'$
  - Probability of false positive: $\leq \beta'$

Observation error

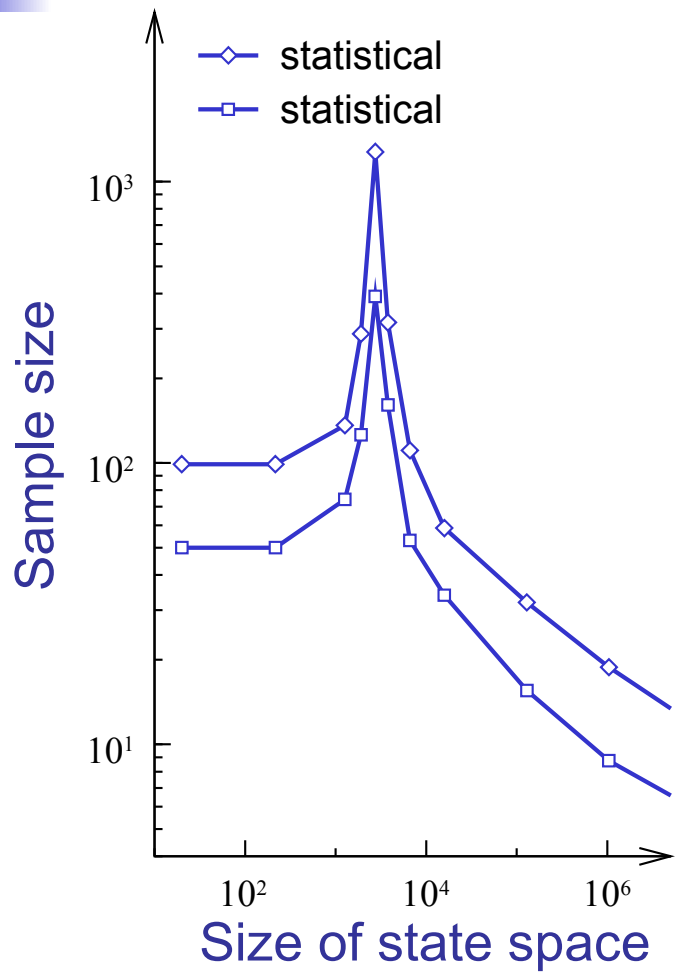
Performance Considerations

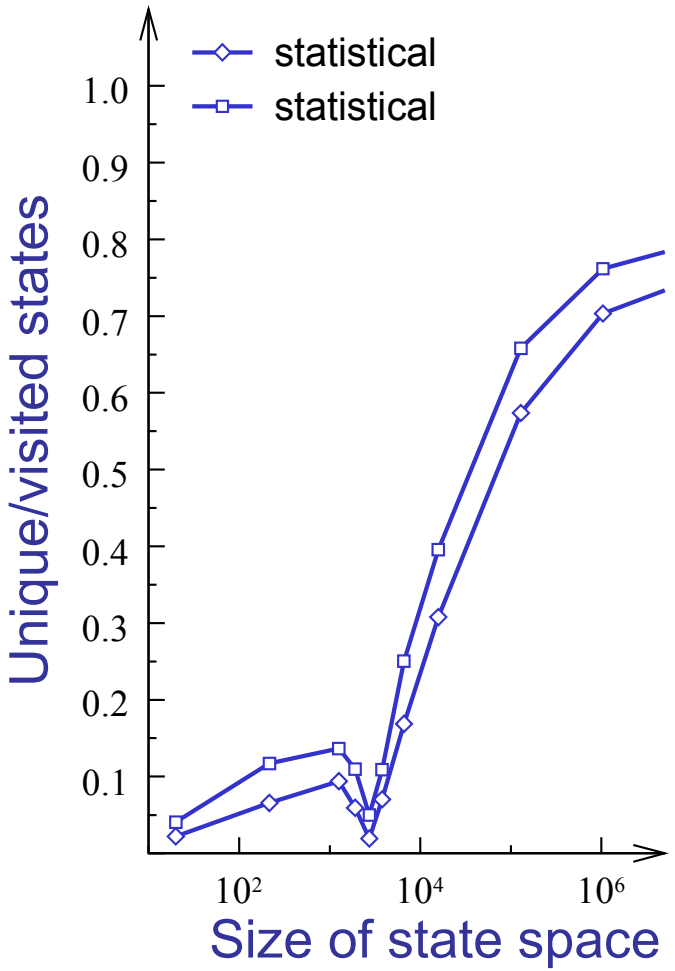
- Verification error is independent of observation error
  - Pick observation error to minimize effort
- The same state may be visited along multiple sample paths
  - Memoize verification results to avoid repeated effort

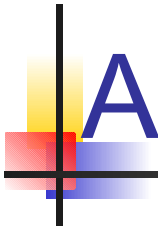
Robot Grid World (results)



Robot Grid World: Effect of Memoization







Availability

- Source code is released under GPL
  - http://sweden.autonomy.ri.cmu.edu/ymer/