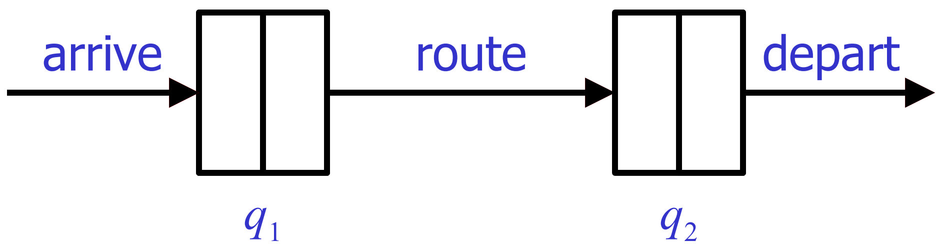
Statistical Probabilistic Model Checking

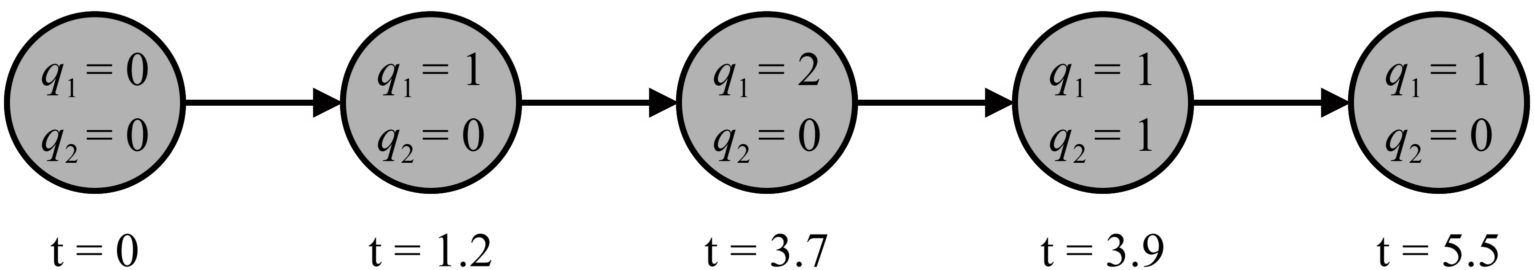
Håkan L. S. Younes
Carnegie Mellon University

Introduction

- Model checking for stochastic processes
  - Stochastic discrete event systems
  - Probabilistic time-bounded properties
- Model independent approach
  - Discrete event simulation
  - Statistical hypothesis testing

Example: Tandem Queuing Network





With both queues empty, is the probability less than 0.5 that both queues become full within 5 seconds?

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

Continuous Stochastic Logic (CSL)

- State formulas
  - Truth value is determined in a single state
- Path formulas
  - Truth value is determined over a path

Discrete-time analogue: PCTL

State Formulas

- Standard logic operators: $\neg\varphi$, $\varphi_1 \wedge \varphi_2$, …
- Probabilistic operator: $P_{\geq\theta}(\rho)$
  - Holds in state s iff probability is at least θ that ρ holds over paths starting in s
  - $P_{<\theta}(\rho) \Leftrightarrow \neg P_{\geq 1-\theta}(\rho)$

Path Formulas

- Until: $\varphi_1 \mathcal{U}^{\leq T} \varphi_2$
  - Holds over path σ iff φ_2 becomes true in some state along σ before time T, and φ_1 is true in all prior states

CSL Example

- With both queues empty, is the probability less than 0.5 that both queues become full within 5 seconds?
  - State: $q_1 = 0 \wedge q_2 = 0$
  - Property: $P_{<0.5}(\text{true } U^{\leq 5}\, q_1 = 2 \wedge q_2 = 2)$

Model Checking Probabilistic Time-Bounded Properties

- Numerical Methods
  - Provide highly accurate results
  - Expensive for systems with many states
- Statistical Methods
  - Low memory requirements
  - Adapt to difficulty of problem (sequential)
  - Expensive if high accuracy is required

Statistical Solution Method [Younes & Simmons 2002]

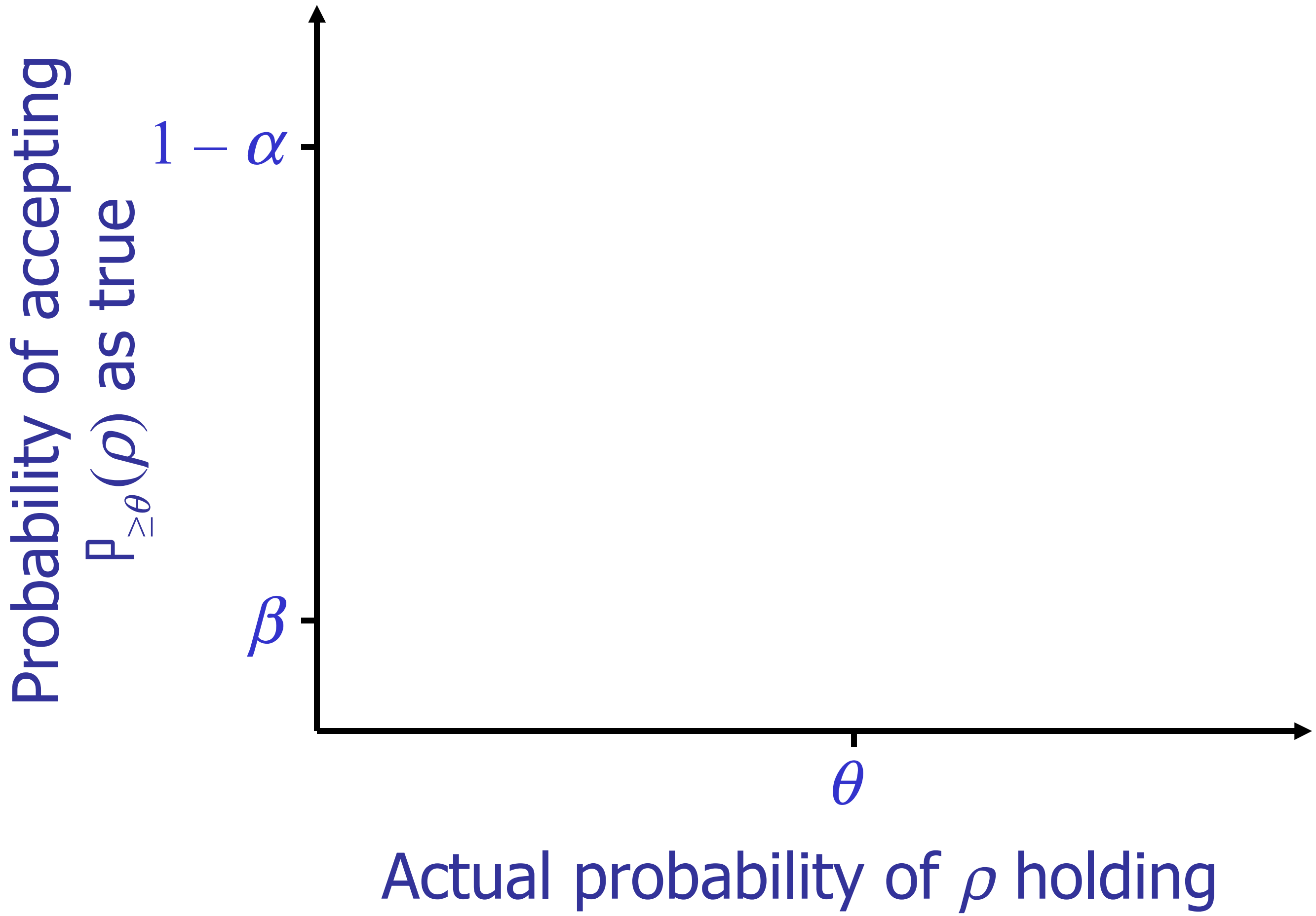
- Use discrete event simulation to generate sample paths
- Use acceptance sampling to verify probabilistic properties
  - Hypothesis: $P_{\geq\theta}(\rho)$
  - Observation: verify ρ over a sample path

Not estimation!

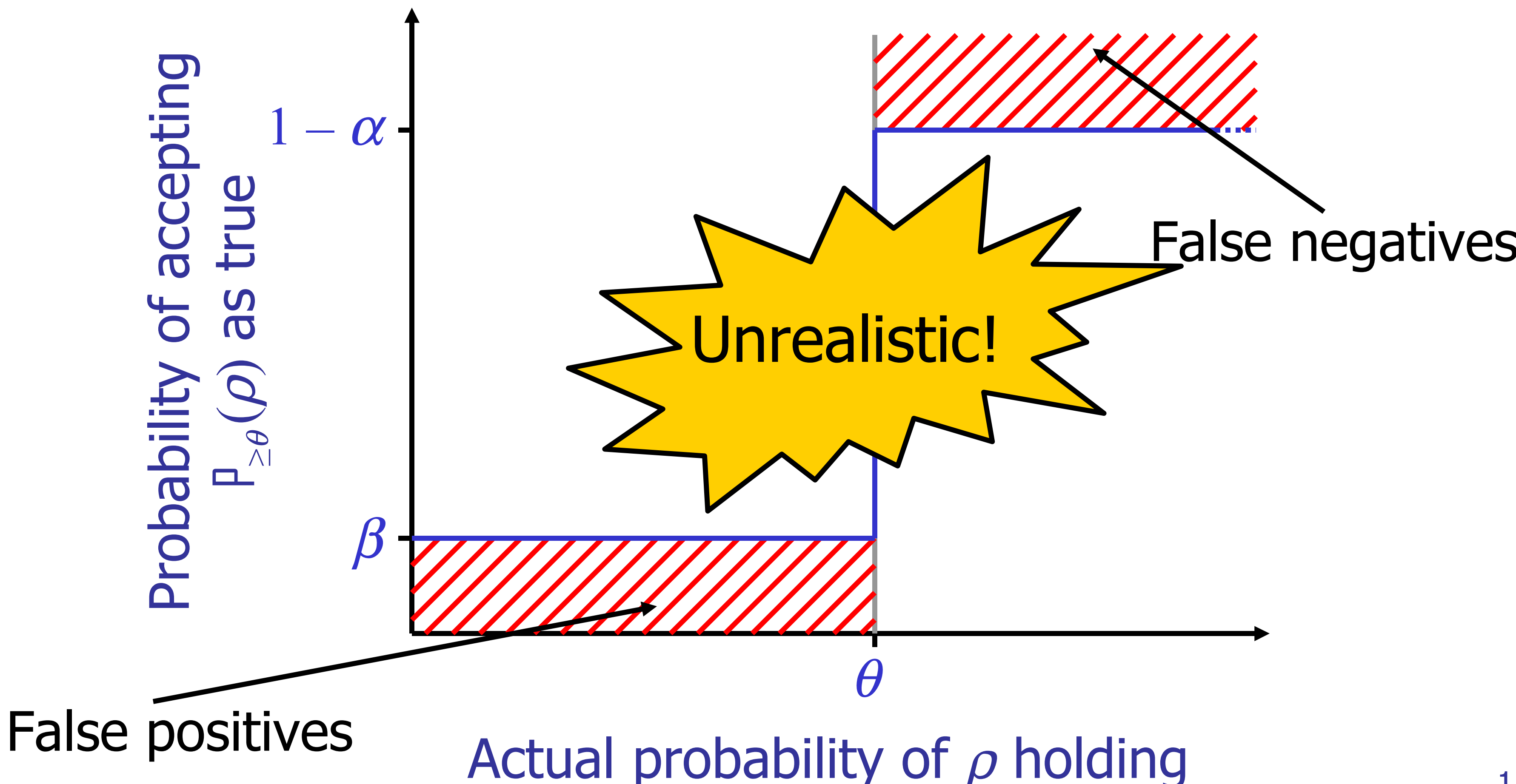
Error Bounds

- Probability of false negative: $\leq \alpha$
  - We say that φ is false when it is true
- Probability of false positive: $\leq \beta$
  - We say that φ is true when it is false

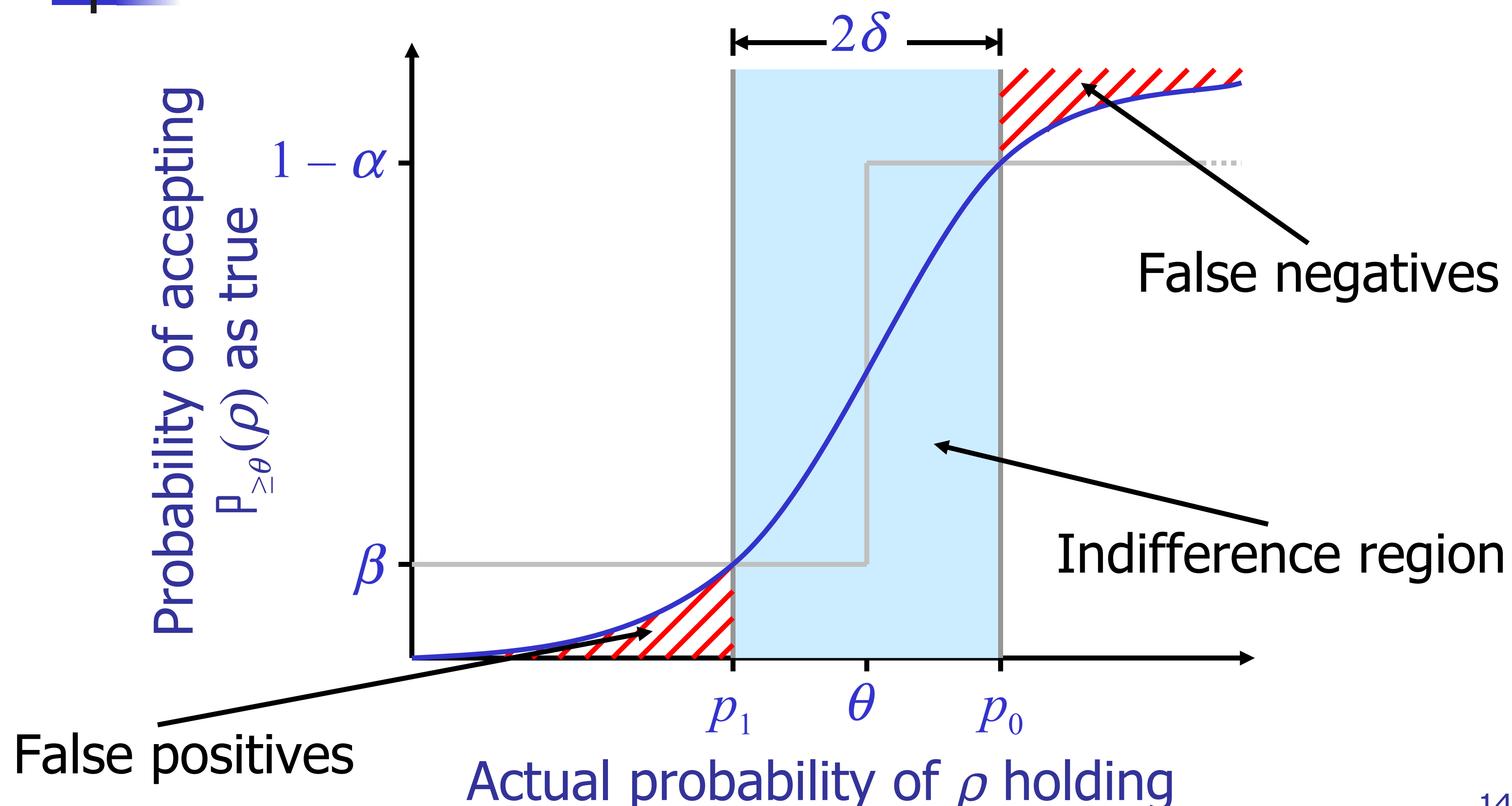
Performance of Test



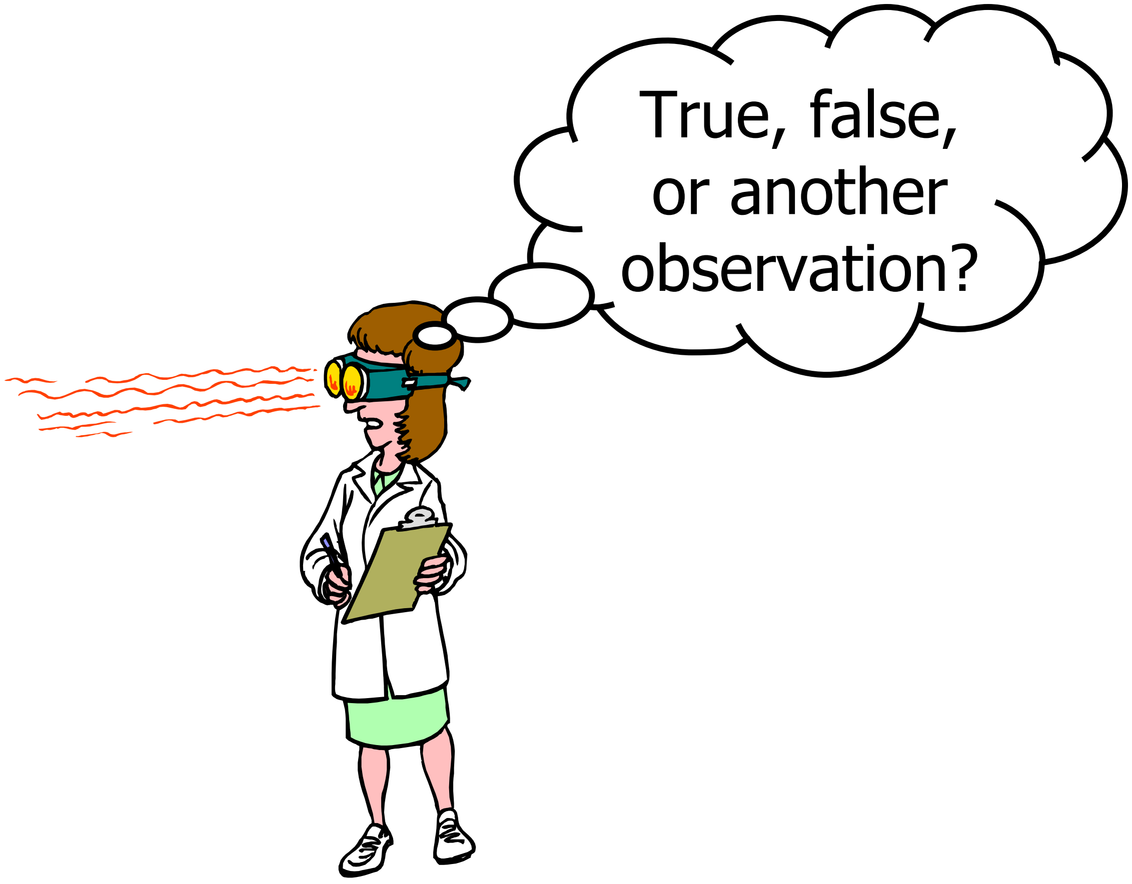
Ideal Performance of Test



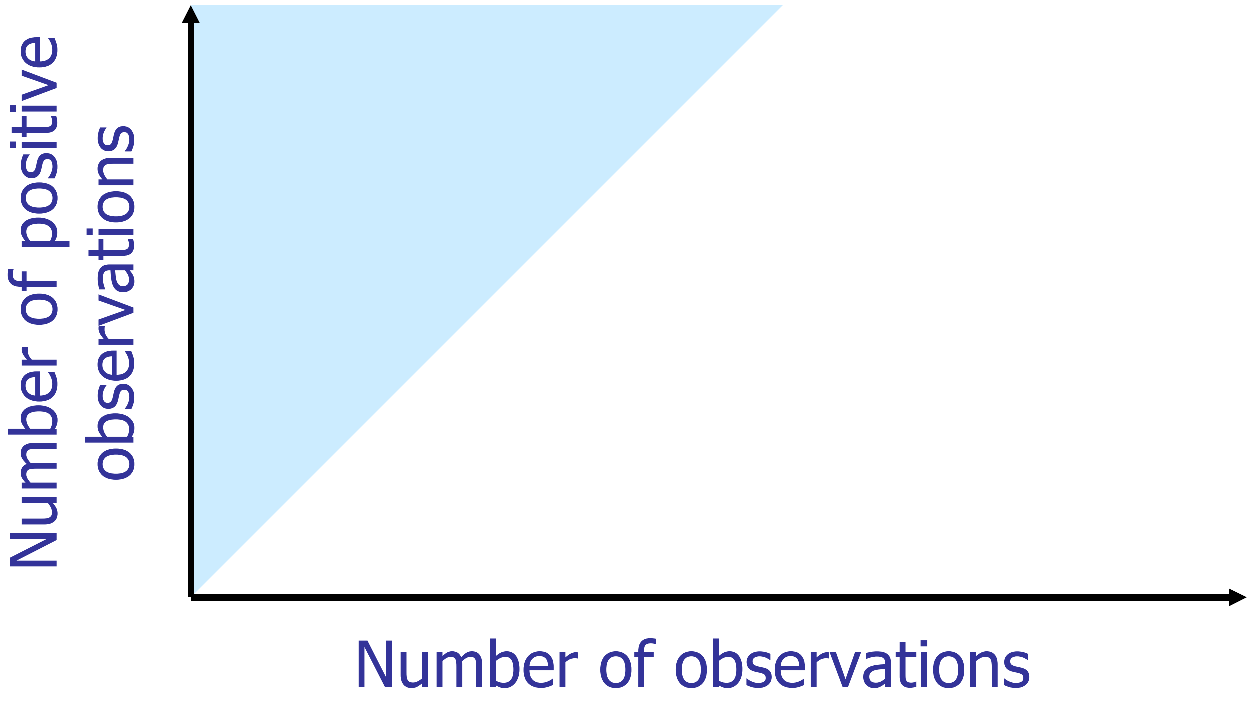
Realistic Performance of Test



Sequential Acceptance Sampling [Wald 1945]

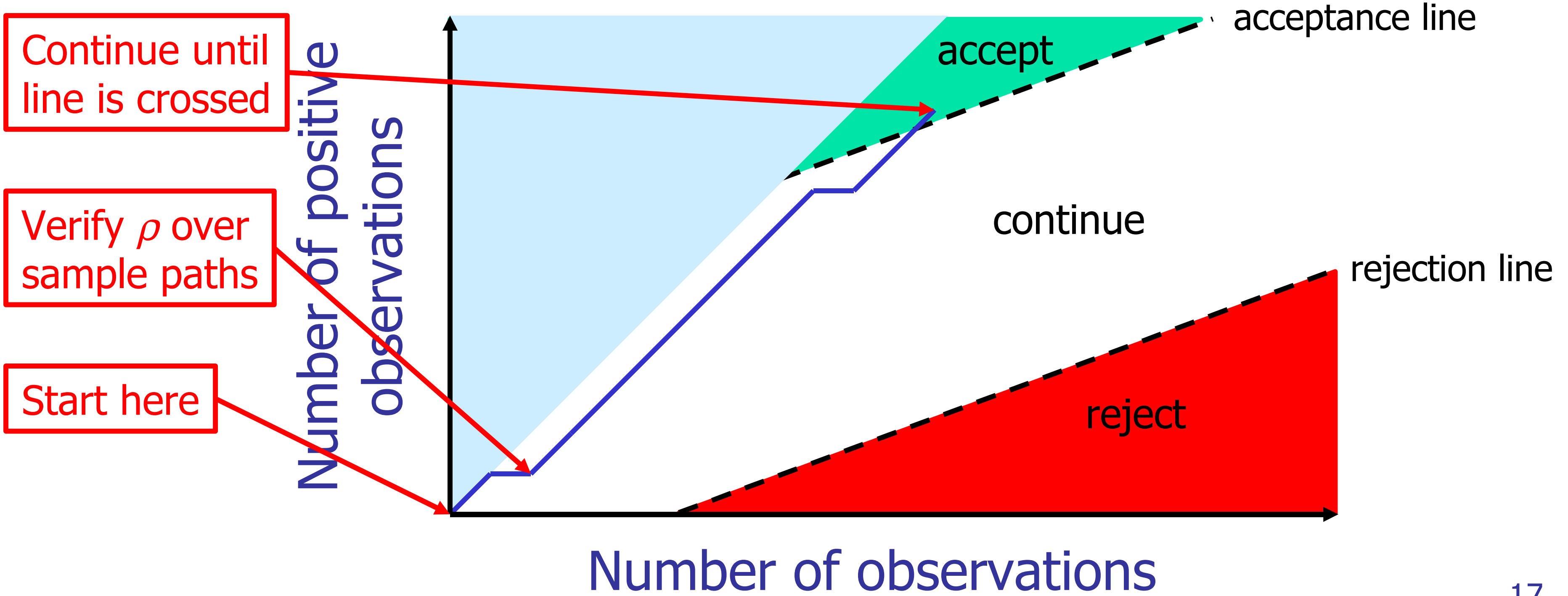


Graphical Representation of Sequential Test



Graphical Representation of Sequential Test

- We can find an acceptance line and a rejection line given θ, δ, α, and β



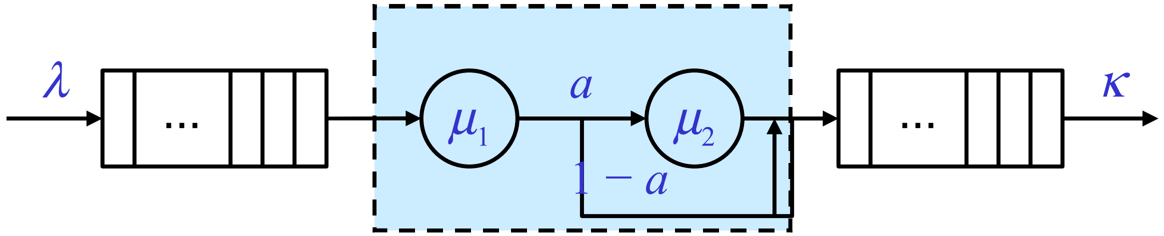
Special Case

- $p_0 = 1$ and $p_1 = 1 - 2\delta$
  - Reject at first negative observation
  - Accept at stage m if $p_1^m \le \beta$
    - Sample size at most $\lceil \log \beta / \log p_1 \rceil$
- "Five nines": $p_1 = 1 - 10^{-5}$

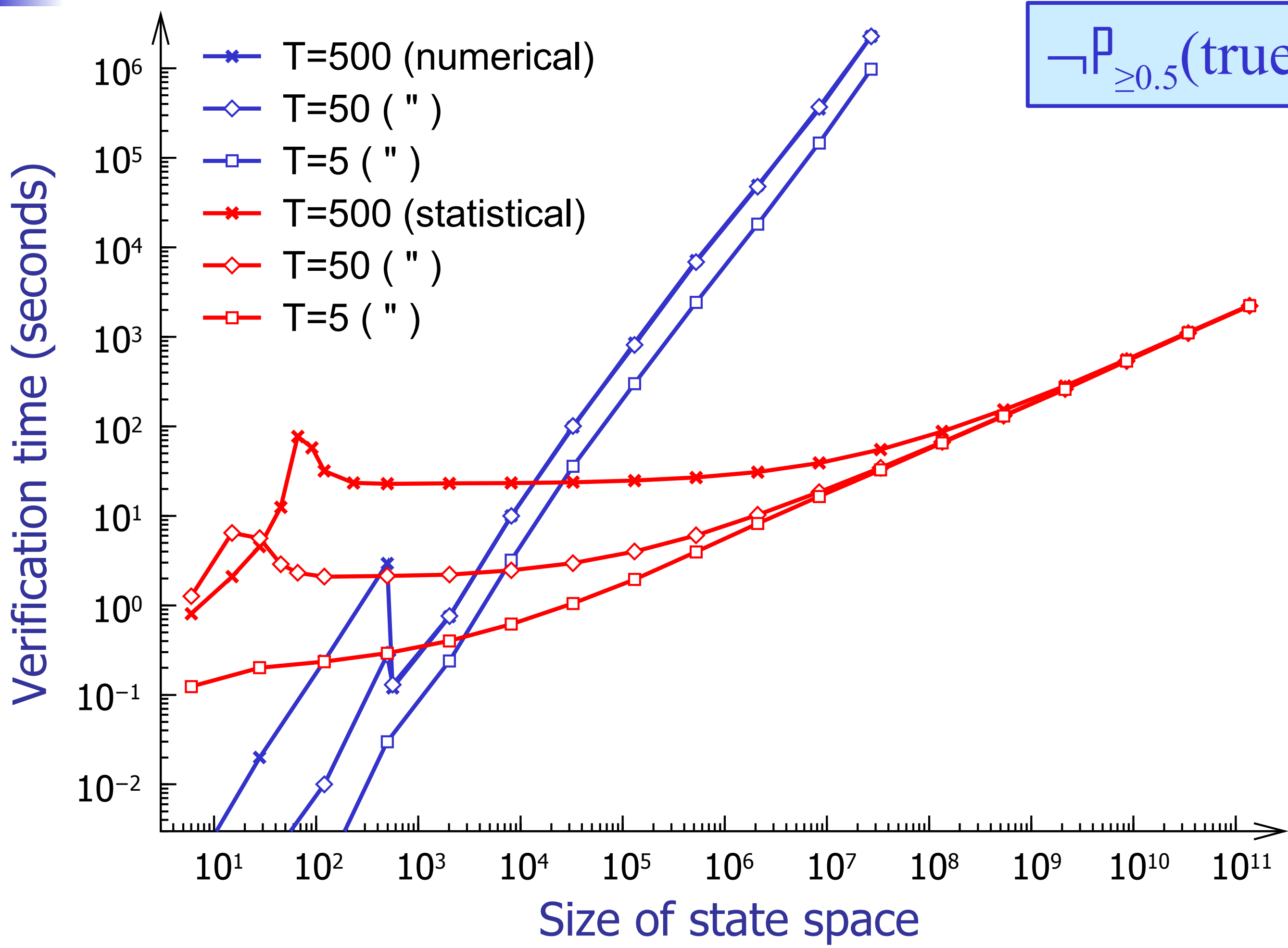
β	Maximum sample size
10^{-2}	460,515
10^{-4}	921,030
10^{-8}	1,842,059

Case Study: Tandem Queuing Network

- $M/Cox_2/1$ queue sequentially composed with $M/M/1$ queue
- Each queue has capacity n
- State space of size $O(n^2)$



Tandem Queuing Network (results) [Younes et al. 2004]



$\neg P_{\geq 0.5}(\text{true}\ U^{\leq T}\ \text{full})$

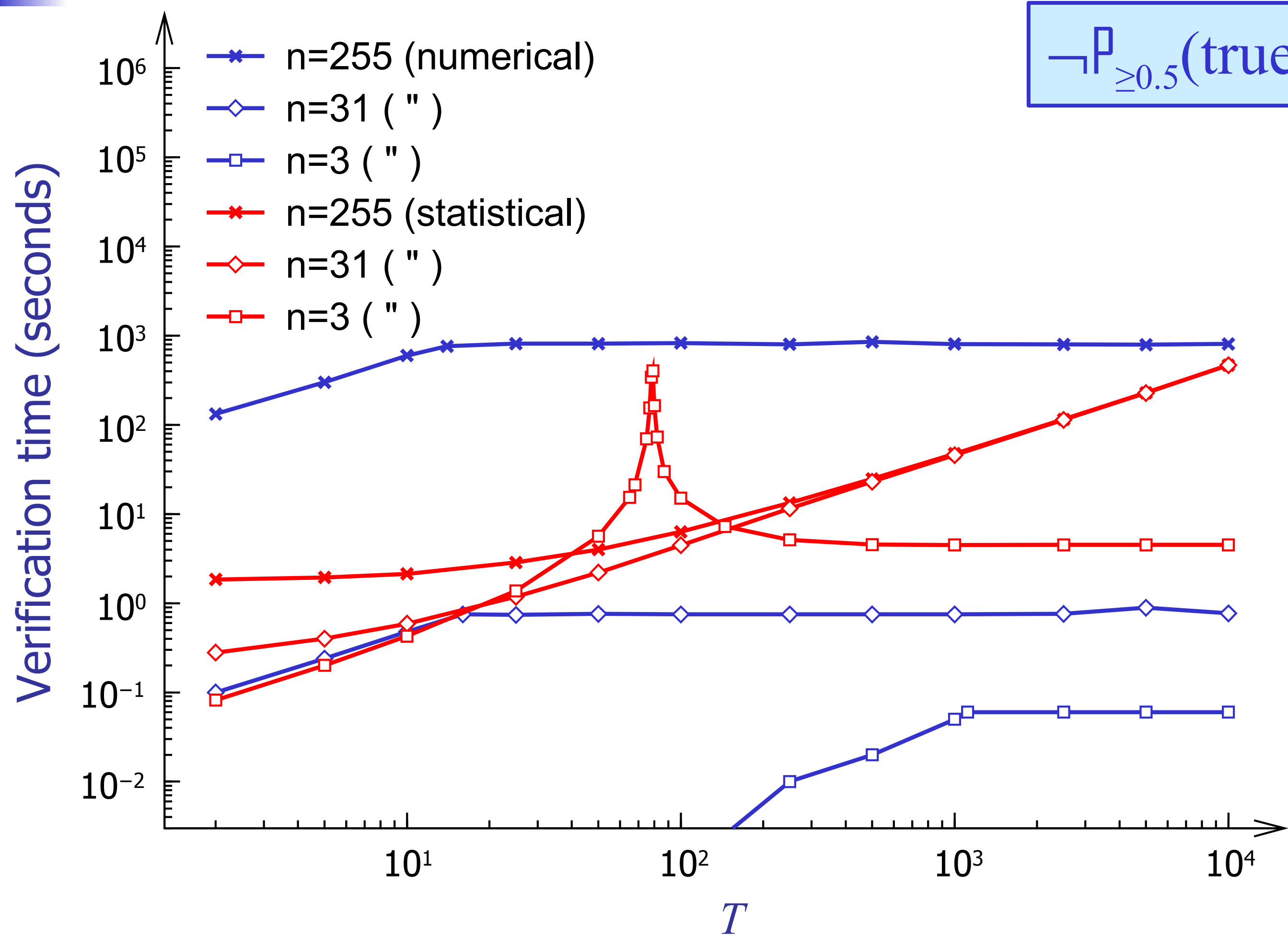
$\varepsilon = 10^{-6}$

$\alpha = \beta = 10^{-2}$

$\delta = 0.5 \cdot 10^{-2}$

Tandem Queuing Network (results) [Younes et al. 2004]

$\neg \mathcal{P}_{\geq 0.5}(\text{true}\ \mathcal{U}^{\leq T}\ \text{full})$



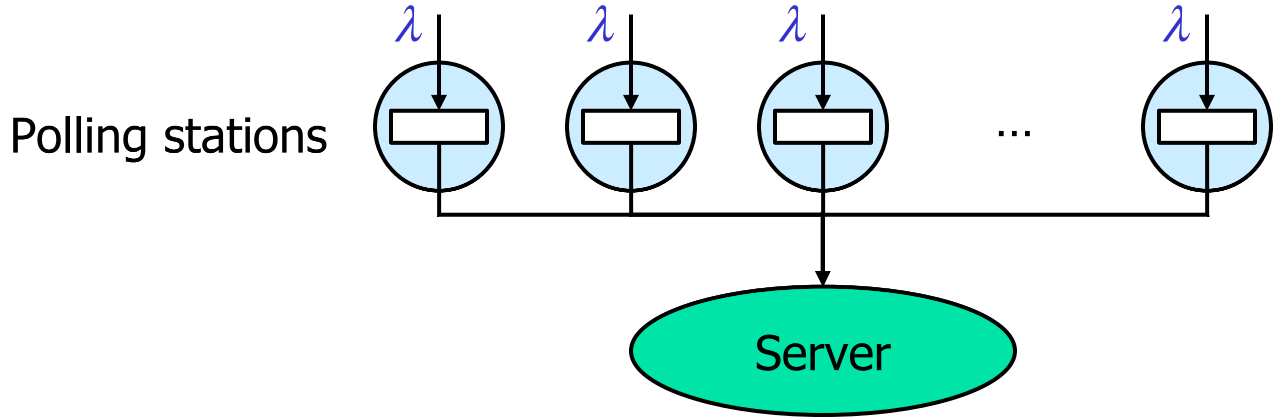
$\varepsilon = 10^{-6}$

$\alpha = \beta = 10^{-2}$

$\delta = 0.5 \cdot 10^{-2}$

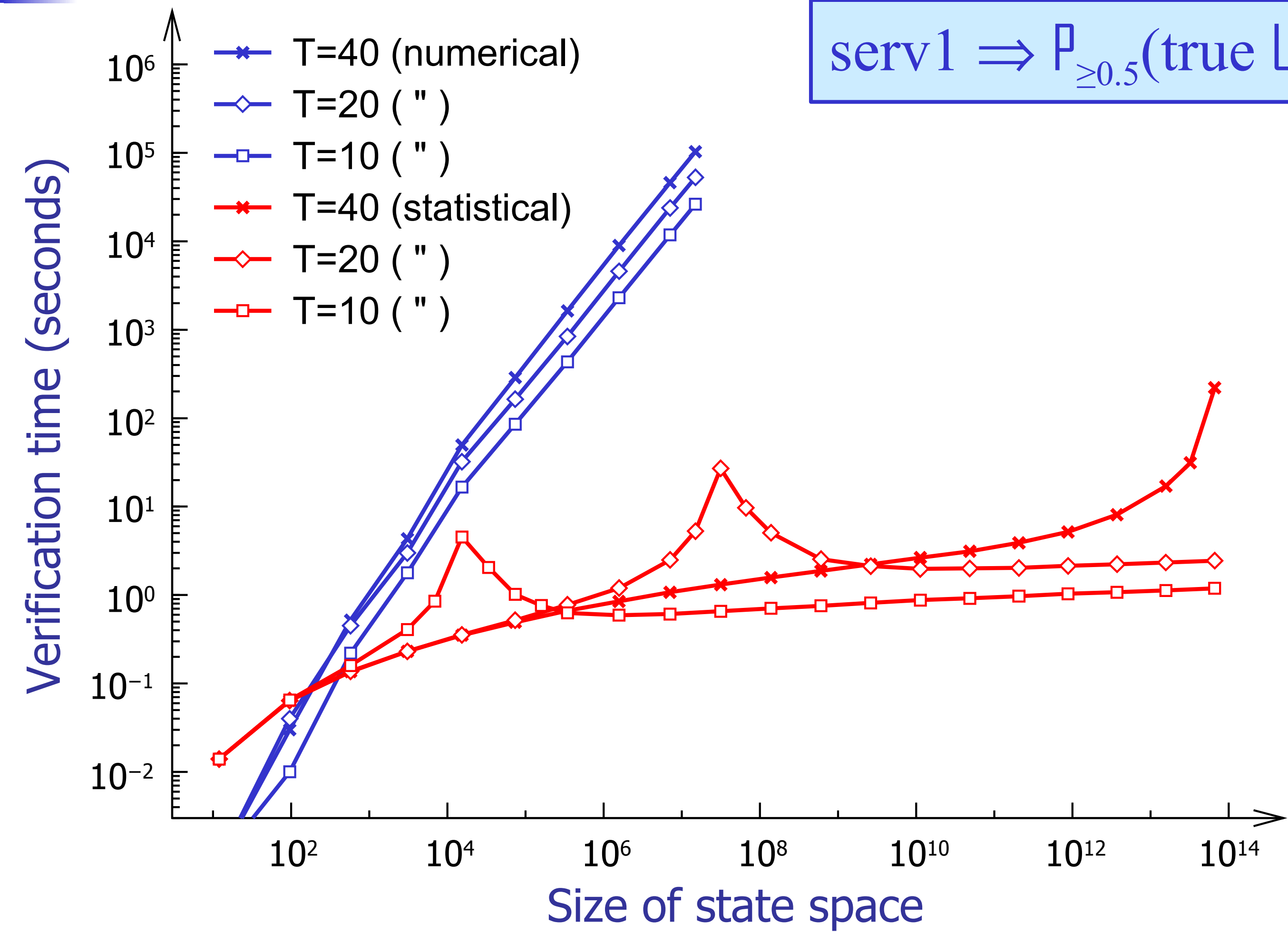
Case Study: Symmetric Polling System

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



Symmetric Polling System (results) [Younes et al. 2004]

$$\text{serv1} \Rightarrow \mathsf{P}_{\geq 0.5}(\text{true}\ \mathsf{U}^{\leq T}\ \text{poll1})$$



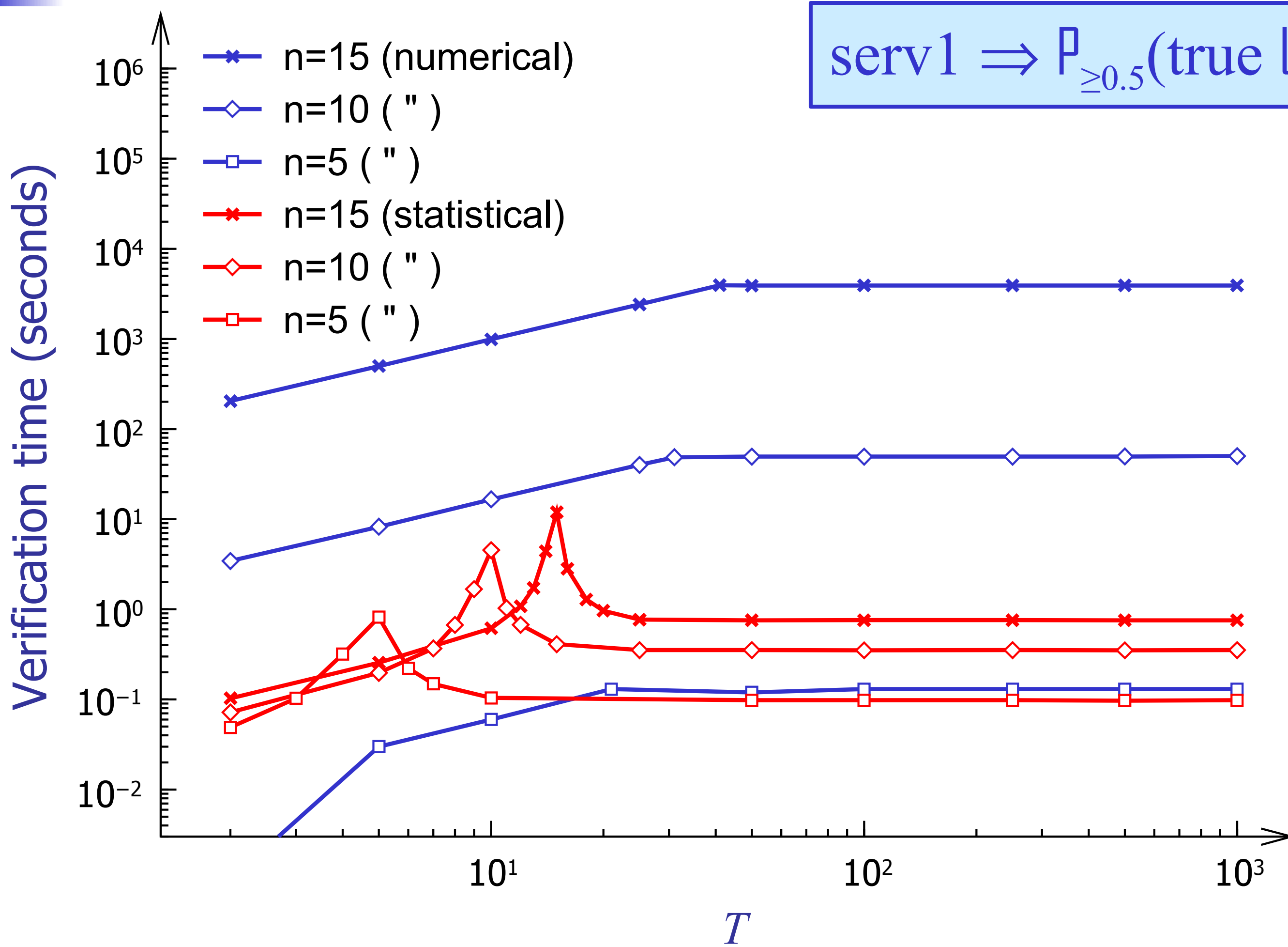
$\varepsilon = 10^{-6}$

$\alpha = \beta = 10^{-2}$

$\delta = 0.5 \cdot 10^{-2}$

Symmetric Polling System (results) [Younes et al. 2004]

$\text{serv1} \Rightarrow P_{\geq 0.5}(\text{true}\ U^{\leq T}\ \text{poll1})$



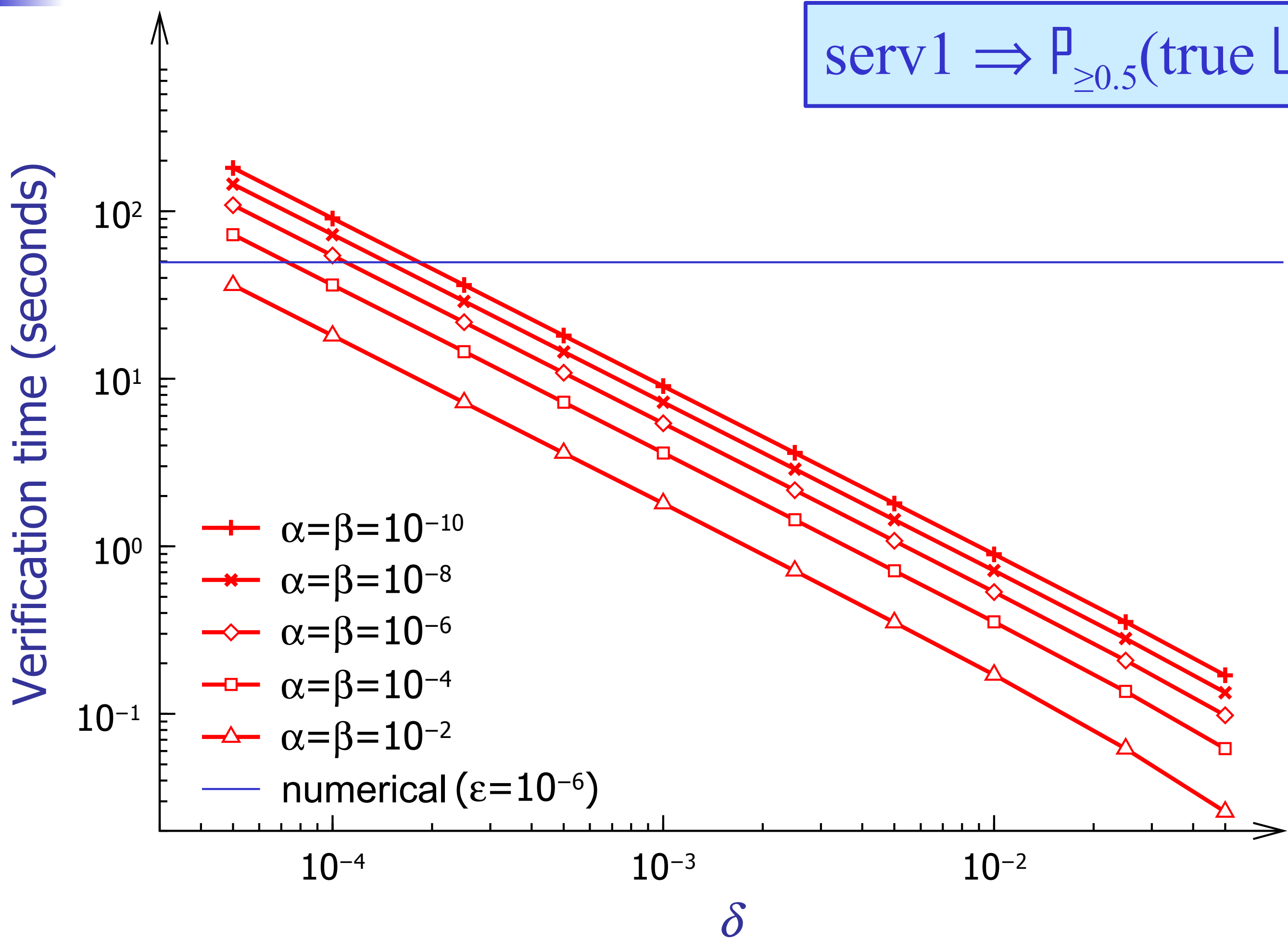
$\varepsilon = 10^{-6}$

$\alpha = \beta = 10^{-2}$

$\delta = 0.5 \cdot 10^{-2}$

Symmetric Polling System (results) [Younes et al. 2004]

$\mathrm{serv1} \Rightarrow \mathsf{P}_{\geq 0.5}(\mathrm{true}\ \mathsf{U}^{\leq T}\ \mathrm{poll1})$



$n = 10$
$T = 40$

Tandem Queuing Network: Distributed Sampling

- Use multiple machines to generate samples
  - m_1: Pentium IV 3GHz
  - m_2: Pentium III 733MHz
  - m_3: Pentium III 500MHz

	% samples				% samples			m_1 only
n	m_1	m_2	m_3	time	m_1	m_2	time	time
63	*70*	*20*	*10*	0.46	*71*	*29*	0.50	0.58
2047	*60*	*26*	*14*	1.28	*70*	*30*	1.46	1.93
65535	*65*	*21*	*14*	26.29	*67*	*33*	33.89	44.85

Summary

- Acceptance sampling can be used to verify probabilistic properties of systems
- Sequential acceptance sampling adapts to the difficulty of the problem
- Statistical methods are easy to parallelize

Other Research

- Failure trace analysis
  - “failure scenario” [Younes & Simmons 2004a]
- Planning/Controller synthesis
  - CSL goals [Younes & Simmons 2004a]
  - Rewards (GSMDPs) [Younes & Simmons 2004b]

Tools

- Ymer
  - Statistical probabilistic model checking
- Tempastic-DTP
  - Decision theoretic planning with asynchronous events

References

Wald, A. 1945. Sequential tests of statistical hypotheses. *Ann. Math. Statist.* 16: 117-186.

Younes, H. L. S., M. Kwiatkowska, G. Norman, and D. Parker. 2004. Numerical vs. statistical probabilistic model checking: An empirical study. In *Proc. TACAS-2004*.

Younes, H. L. S., R. G. Simmons. 2002. Probabilistic verification of discrete event systems using acceptance sampling. In *Proc. CAV-2002*.

Younes, H. L. S., R. G. Simmons. 2004a. Policy generation for continuous-time stochastic domains with concurrency. In *Proc. ICAPS-2004*.

Younes, H. L. S., R. G. Simmons. 2004b. Solving generalized semi-Markov decision processes using continuous phase-type distributions. In *Proc. AAAI-2004*.