Counterexamples for Timed Probabilistic Reachability

Husain Aljazzar

Software Engineering
University of Constance

Joint work with

- Holger Hermanns, Saarland University
- Stefan Leue, University of Constance

Overview

- Introduction
- (Directed) Explicit-State Model Checking (D)ESMC for Timed Probabilistic Reachability
- Probabilistic Quality Measure for (D)ESMC
- Case Study and Experimental Results
- Conclusion & Future Work

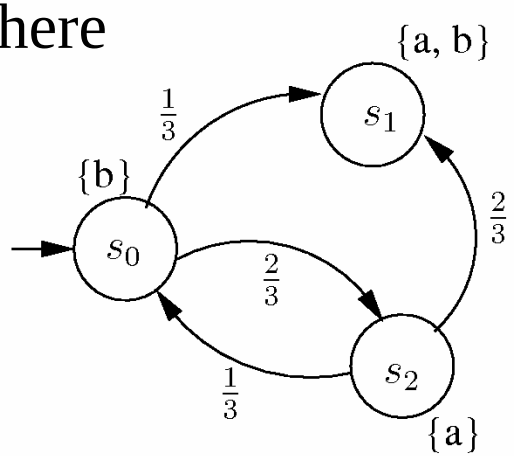
Overview

- Introduction
- (Directed) Explicit-State Model Checking (D)ESMC for Timed Probabilistic Reachability
- Probabilistic Quality Measure for (D)ESMC
- Case Study and Experimental Results
- Conclusion & Future Work

Stochastic Models

Software Engineering

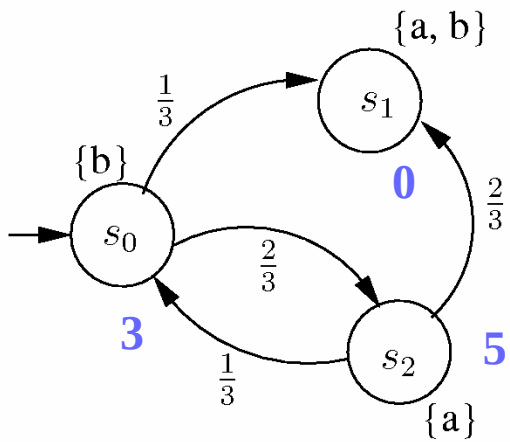
- Stochastic models, e.g. *DTMCs* and *CTMCs*: modeling and analysis of system performance and dependability.
  - communication protocols,
  - embedded systems,
  - etc…
- A DTMC is a quadruple (S, s_0, P, L), where
  - S is a finite set of states, and
  - $s_0 \in S$ is an initial state
  - $P : S \times S \to \mathbb{R}$ is the transition probability matrix,
  - $L : S \to 2^{AP}$ is labeling function.



Stochastic Models

Software Engineering

- A CTMC is a quintuple (S, s_0, P, L, E), where
  - (S, s_0, P, L) *is a DTMC*
  - E: S $\rightarrow \mathbb{R}$ is a function assigning each state an exit rate
  - Exit times are exponentially distributed
  - E.g. $E := \{(s_0, 3), (s_1, 0), (s_2, 5)\}$



Runs and Paths

- In a DTMC, we call a *finite/infinite* sequence of states *finite/infinite* ***RUN***

$$s_0 \longrightarrow s_1 \longrightarrow s_2 \longrightarrow \ldots \longrightarrow s_n,$$

$$s_0 \longrightarrow s_1 \longrightarrow s_2 \longrightarrow \ldots,$$

- In a CTMC, a *finite/infinite* ***PATH*** is a timed variant of a run in the underlying DTMC.

$$s_0 \xrightarrow{t_0} s_1 \xrightarrow{t_1} s_2 \xrightarrow{t_2} \cdots \xrightarrow{t_{n-1}} s_n,$$

$$s_0 \xrightarrow{t_0} s_1 \xrightarrow{t_1} s_2 \xrightarrow{t_2} \ldots,$$

- Infinite branching tree due to varying transition time durations of transitions.

Analysis of Stochastic Models

- Various model checking approaches for stochastic models have been presented.
- Our point of reference: CSL model checking

  Baier, C., Haverkort, B., Hermanns, H., Katoen, J.P.
  "Model-Checking Algorithms for Continuous-Time Markov chains"
  IEEE Transitions on Software Engineering 29, 2003

  - Continuous Stochastic Logic (CSL):
  - CSL model checking algorithms: efficient, approximate, numerical
- **Common weakness: Inability to give detailed debugging information (Counterexamples).**
  - Problematic for debugging
- **Approach:** Use explicit state space algorithms to select offending system runs (counterexamples).

Timed Probabilistic Reachability Analysis

- Timed Reachability Property:
  - *The probability to reach a state* ***s*** *violating a state proposition* ϑ*, i.e., satisfying* $\varphi := \neg\, \vartheta$*, within a given time period* ***t*** *does not exceed a probability bound* ***p****.*
  - Specification using Continuous Stochastic Logic (CSL)

$$\phi := \mathcal{P}_{<p}(\Diamond^{\leq t}\varphi)$$

$\mathcal{P}_{<p}$: Transient probability does not exceed *p*.
$\Diamond^{\leq t}$: Timed reachability within *[0, t]*

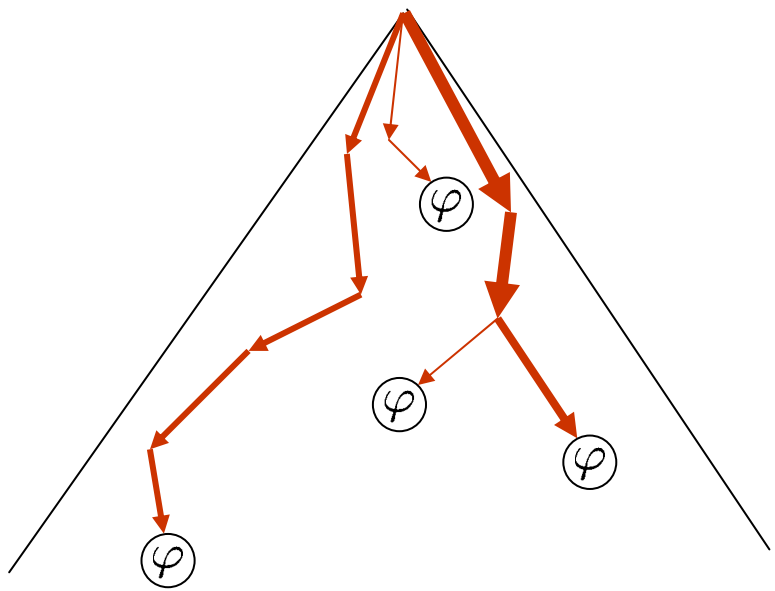
Overview

- Introduction
- (Directed) Explicit-State Model Checking (D)ESMC for Timed Probabilistic Reachability
- Probabilistic Quality Measure for (D)ESMC
- Case Study and Experimental Results
- Conclusion & Future Work

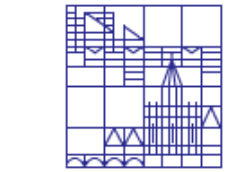
What is a Counterexample?
(of Timed Probabilistic Reachability)

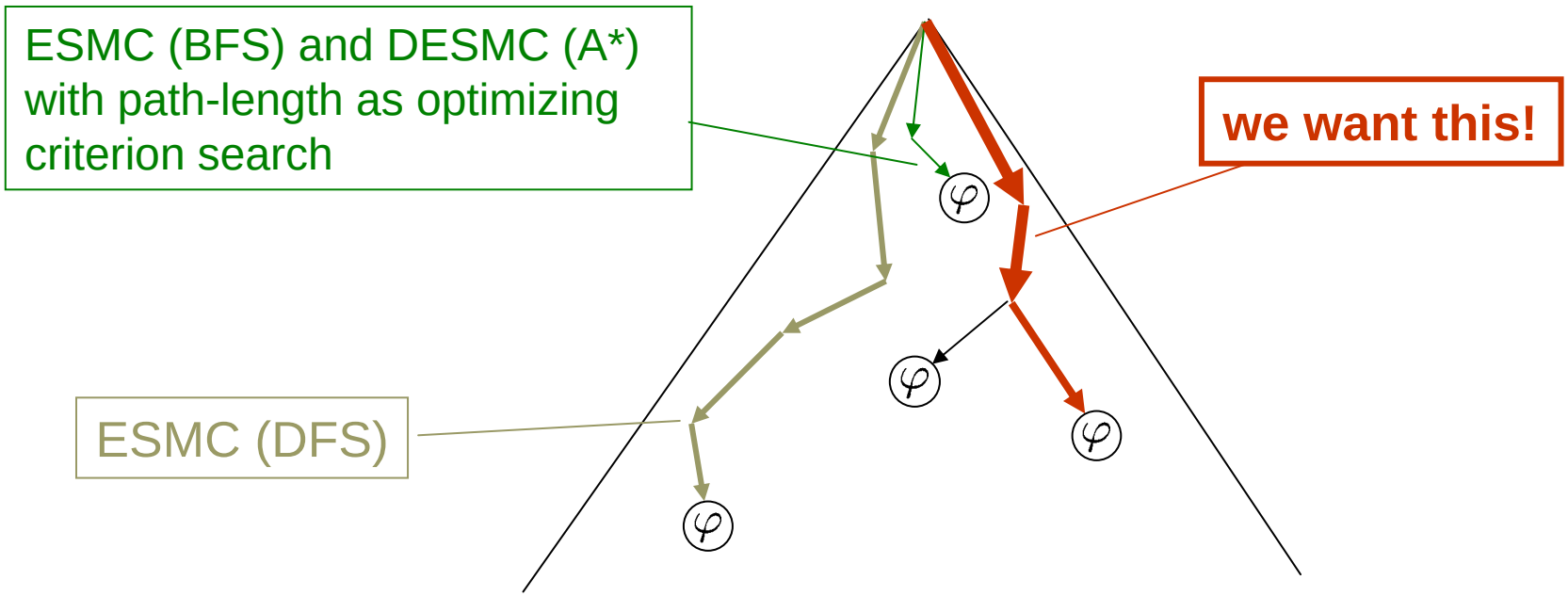
- **In non-stochastic models:** a counterexample is an offending run.
- **In stochastic models:**
  - DTMC: All offending runs
  - CTMC: The infinite cylinder set containing all paths that reach an error state within the time period ***t.***
    - A single path of the cylinder set**?**
    - Runs in the underlying DTMC
  - A counterexample is an offending run in the (underlying) DTMC.

$$\phi := \mathcal{P}_{<p}(\Diamond^{\leq t}\varphi)$$



(Directed) Explicit-State Model Checking (D)ESMC





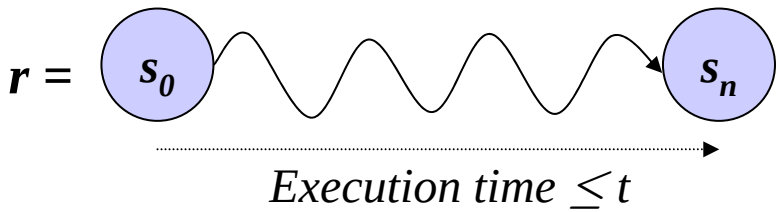
- A mass to measure the quality of runs is required.

Overview

- Introduction
- (Directed) Explicit-State Model Checking (D)ESMC for Timed Probabilistic Reachability
- Probabilistic Quality Measure for (D)ESMC
- Case Study and Experimental Results
- Conclusion & Future Work

Timed Run Probability

- Let $r = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots \rightarrow s_n$ be a run.
- The ***timed run probability*** of ***r*** in the time period ***t***.



- Computation:
  - In CT-case:

$$\gamma(r,t) = \int_0^t \left(p(s_1, s_0, t_1) \cdot \left(\ldots \left(\int_0^{t-t_{n-1}} p(s_n, s_{n-1}, t_n) \cdot dt_n \right) \ldots \right) \right) \cdot dt_1,$$

  - In DT-case:

$$\gamma'(r,t) = P(s_{n-1}, s_n) \cdot \sum_{i=0}^{t-1} \pi(s_{n-1}, i)$$

Uniformization

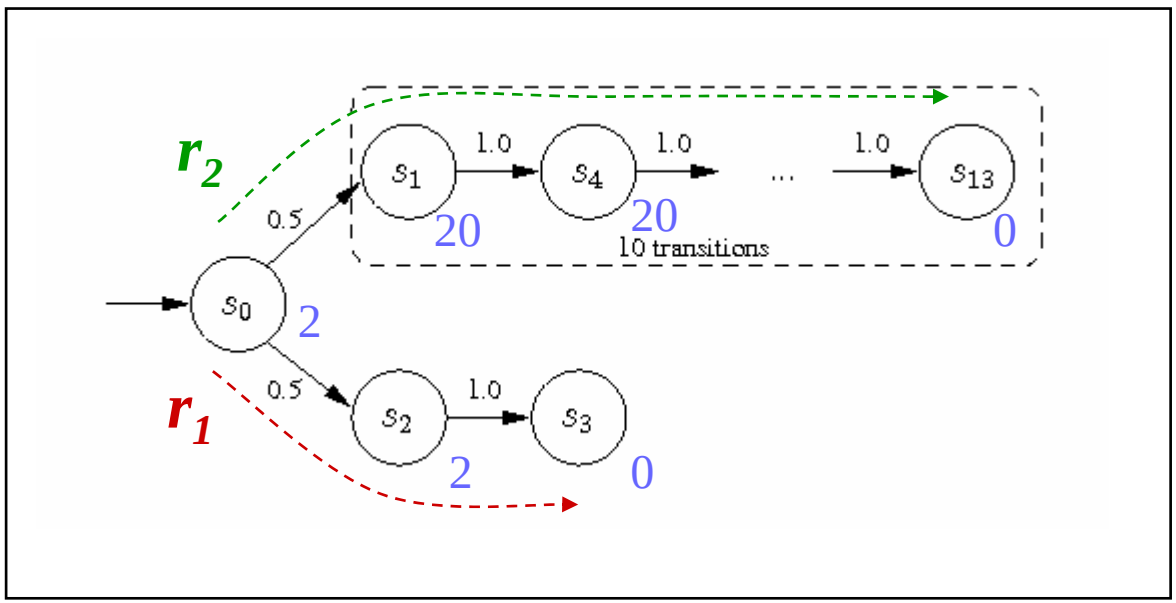
- Using the uniformization we turn a CTMC ***A*** into a DTMC ***A´*** for which we can efficiently compute the *timed run probability* γ'.

- ***A´*** is embedded into a Poisson process which describes the probability that a particular discrete number of events ***k*** occurs within a real time period ***t.***

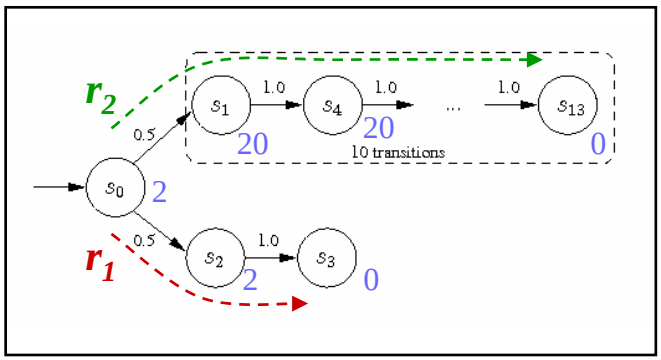
Approximation for the Timed Run Probability in CTMC

- We denote the expected value of the Poisson process after time period ***t*** as ***N***.
- We assume that the derived DTMC ***A´*** makes ***N*** hops within the time period ***t***.
- $\gamma(r, t)$ (in ***A***) is approximated by $\gamma'(r, N)$ (in ***A´***), which is much easier to compute.
- Our search algorithms use $\gamma'(r, N)$ as a quality measure for runs of the CTMC (optimizing criterion).

Intriguing Example

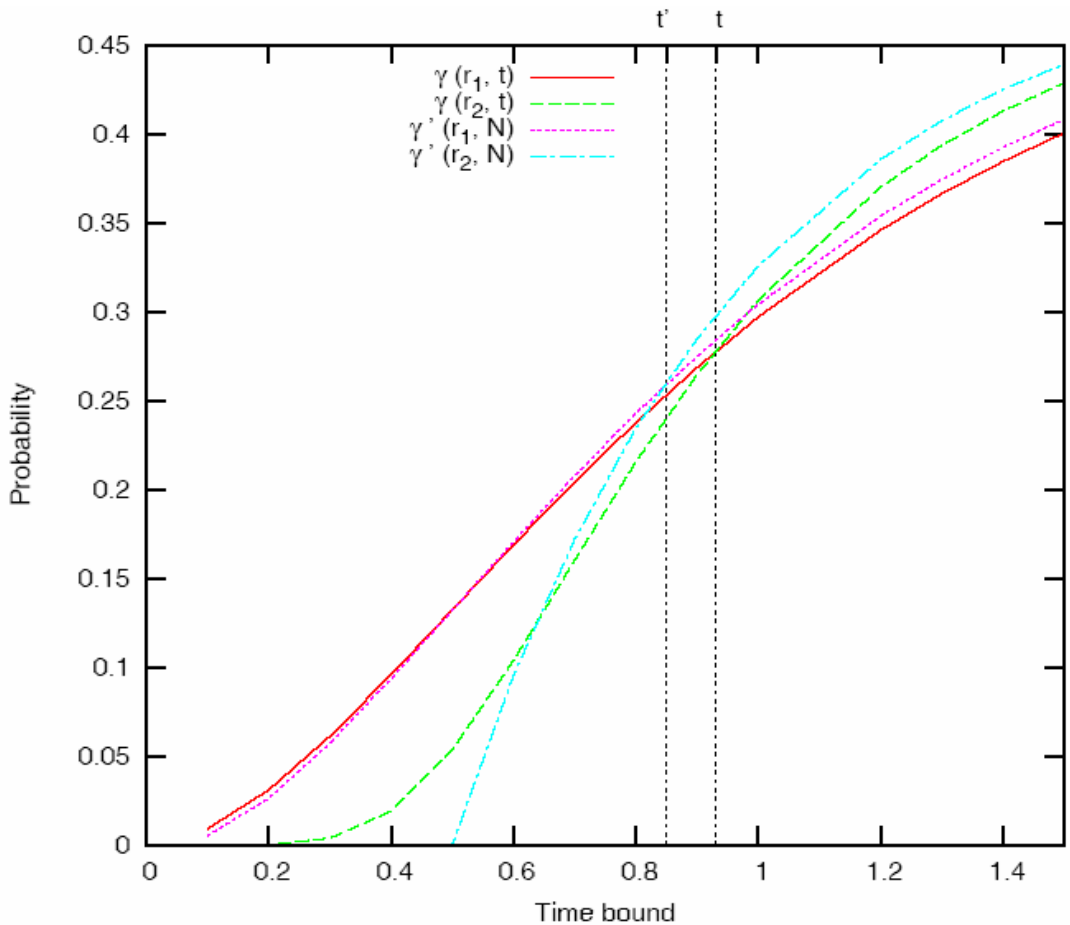


Quality of Uniformization Approximation



Note: the run with optimal *timed run probability* changes with the time bound ***t***!

- Time bound smaller than ***t*** → ***r*** $_1$ is optimal
- Time bound larger than ***t*** → ***r*** $_2$ is optimal



ESMC and DESMC for Stochastic Models

- Now we are able to
  - explore CTMCs (and DTMCs) using optimizing algorithms, and
  - select counterexamples which are approximating the optimal *timed run probability* values.

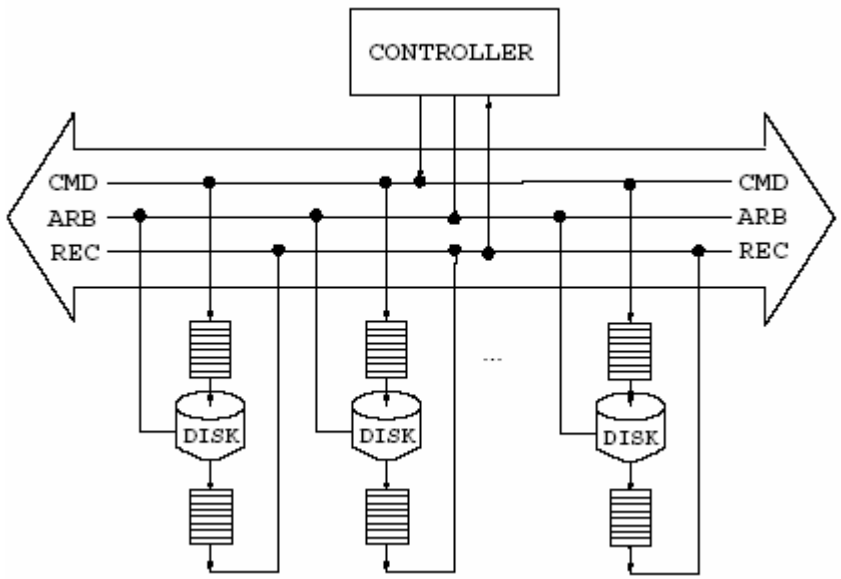
- Search Algorithms
  - Dijkstra (undirected, **ESMC**)
  - Directed search algorithms (**DESMC**)
    - Z* and Greedy Best First Search (GBestFS)
    - Directed search algorithms use knowledge about
      - the state space or/and
      - the specification of the goal state
    - A heuristic function ***h*** is used in the state evaluation**.**
    - Advantages of DESMC: Improving the performance
      - Memory consumption
      - Runtime

Overview

- Introduction
- (Directed) Explicit-State Model Checking (D)ESMC for Timed Probabilistic Reachability
- Probabilistic Quality Measure for (D)ESMC
- Case Study and Experimental Results
- Conclusion & Future Work

Case-Study: SCSI-2-Protocol

- In our experiments:
  - One Controller
  - One main disk (frequently used)
  - Two backup disks (rarely used)



- LOTOS model
  → Interactive Markov chain (IMC)
  → CTMC

SCSI-2-Protocol: A Timed Reachability Property

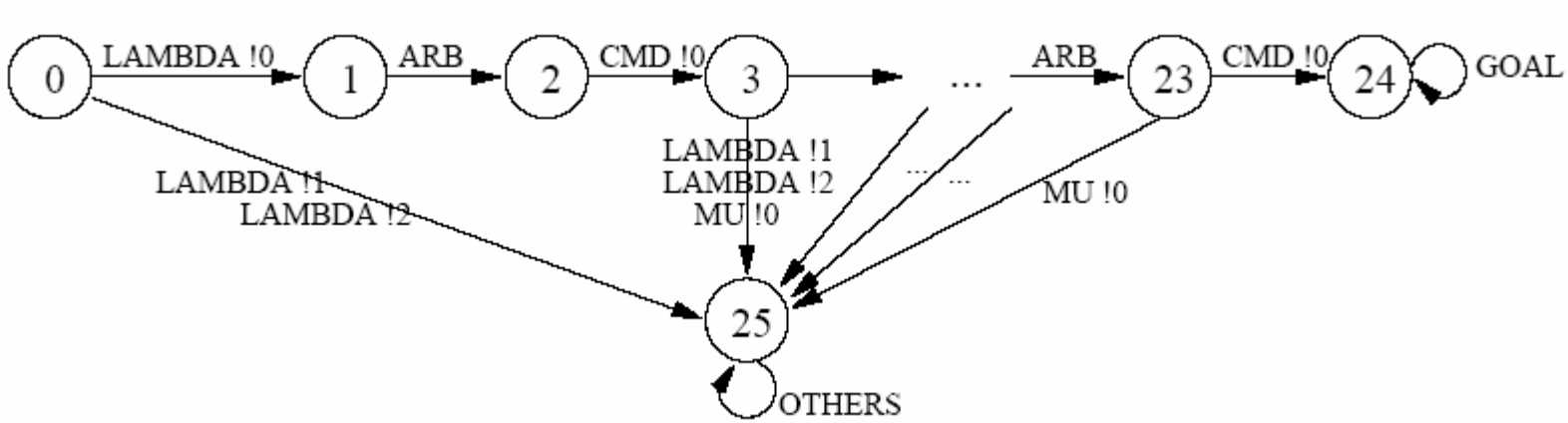
- Main disk overload (MDOL): The main disk is overloaded while the backup disks are not accessed.
- **Timed Reachability Property:** The probability to reach a MDOL state within the time period ***t*** does not exceed 30%.

$$\mathcal{P}_{<0.3}(\Diamond^{\leq t}\ MDOL)$$

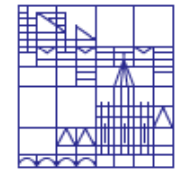
- A heuristic function based on the status of the disk queues.

SCSI-2-Protocol: Counterexample

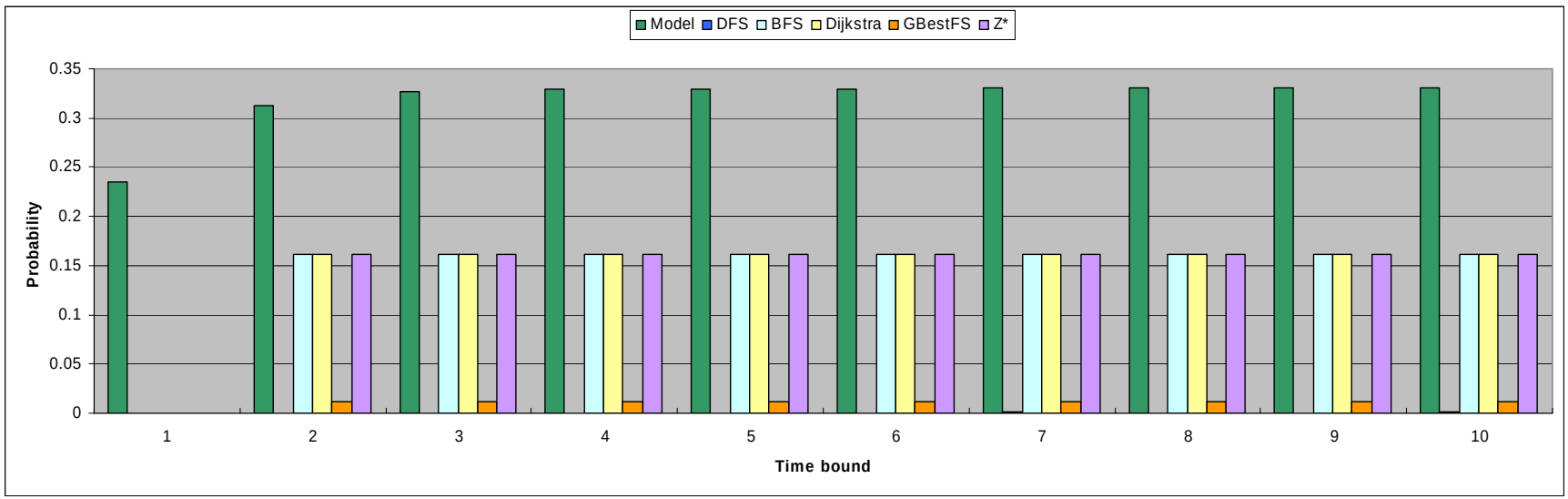
- The counterexample delivered by Z*



SCSI-Protocol: Experimental Results



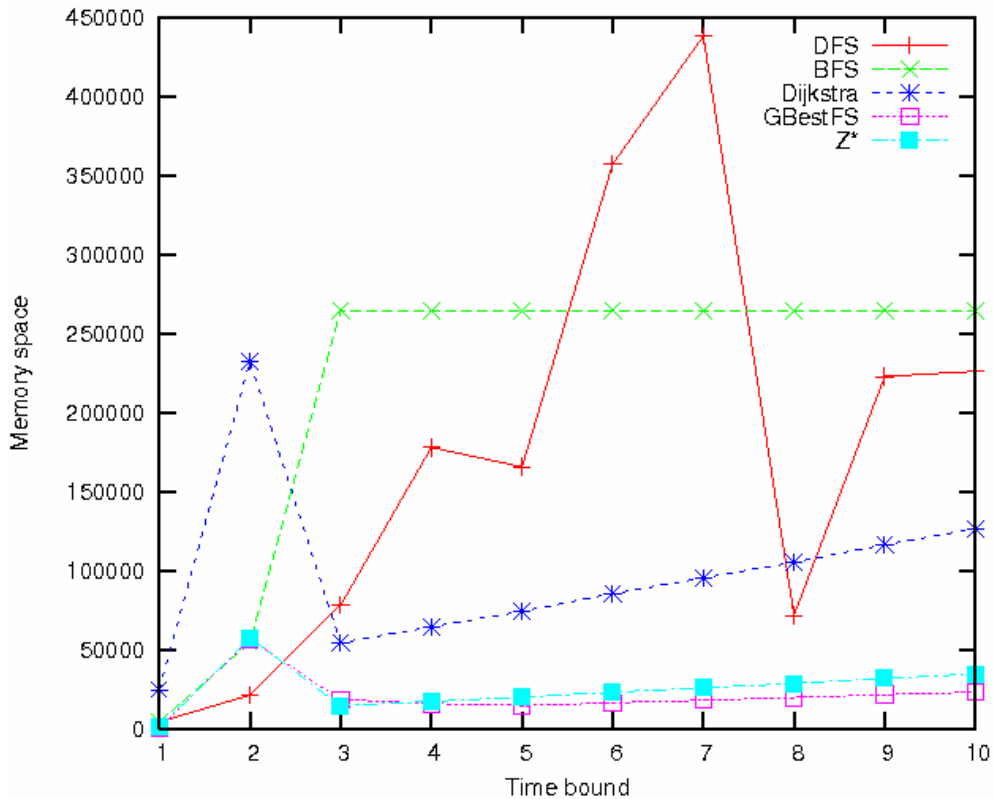
- For each time bound from 1 to 10:
  - Probability to violate the property
  - Timed run probability for the counterexamples delivered by the search algorithms.



SCSI-Protocol: Experimental Results

Software Engineering

- Memory consumption
  - The behavior of DFS and BFS is unacceptable.
  - Dijkstra is OK but not excellent
  - Z* and GBestFS bring significant improvement
  - GBestFS has the best behavior.
- Similar results for runtime



Overview

- Introduction
- (Directed) Explicit-State Model Checking (D)ESMC for Timed Probabilistic Reachability
- Probabilistic Quality Measure for (D)ESMC
- Case Study and Experimental Results
- Conclusion & Future Work

Conclusion

- Counterexamples
  - defined counterexamples for CTMCs, including their probability mass: timed run probabilities
  - approximate the computationally expensive timed run probabilities through uniformisation
- Directed CTMC Exploration
  - use approximative timed run probability in determining generating path costs
  - combine with domain specific information to compute admissible heuristic estimates (admissible in the approximated model)
- Experimental Evaluation (SCSI-2)
  - using approximated timed run probabilities allows Dijkstra and heuristic search algorithms to find meaningful counterexamples
  - heuristics guided search is computationally superior to uninformed search

Future Work

- Threats to Valitidy
  - more experimental data
    - convergence to PRISM tool environment, more models available
    - use randomly generated models
- Underapproximation of Timed Probabilistic Reachability
  - find tree of offending system runs so that combined probability mass exceeds probability bound
  - potentially computationally much more efficient than precise solution of problem
- Application to Other Stochastic Models
  - Continuous Time Markov Decision Processes
    - contain non-determinism

Thanks for your attention!