SMT-based Counterexample Generation for Markov Chains

Bettina Braitling[1] Ralf Wimmer[1] Bernd Becker[1]
Nils Jansen[2] Erika Ábrahám[2]

[1]Computer Architecture
Albert-Ludwigs-University Freiburg, Germany

[2]Software Modeling and Verification
RWTH Aachen, Germany

ROCKS Workshop
March 27th, 2011

Motivation

- Complex (embedded) systems everywhere:

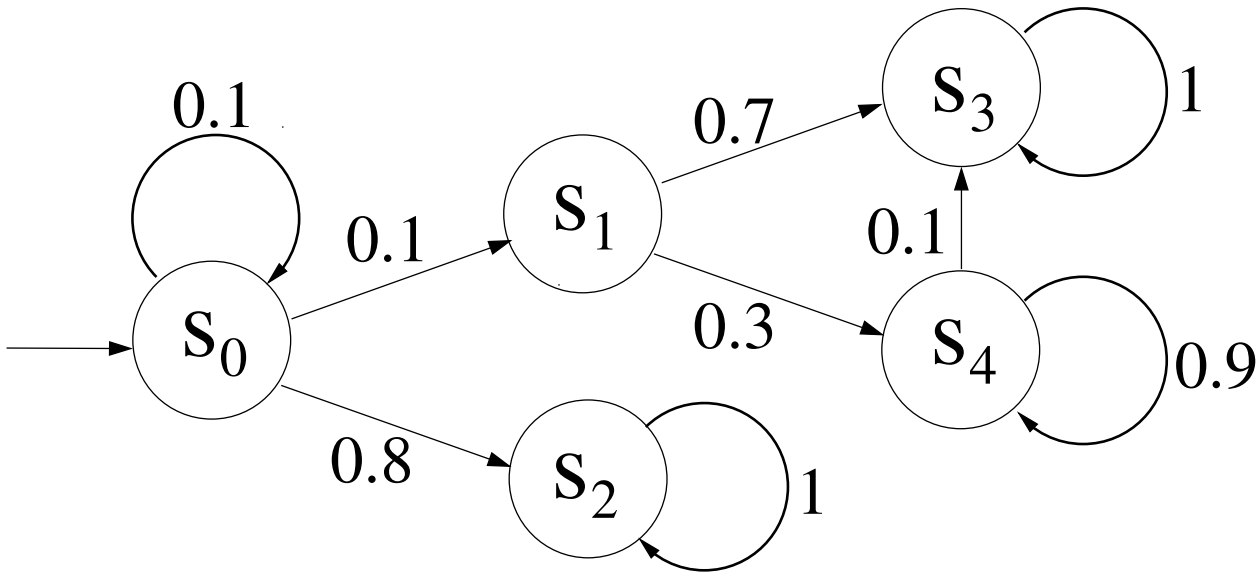
- Correct behaviour has to be ensured.
- Verification is needed.
  $\Rightarrow$ Counterexamples
  $\Rightarrow$ Bounded Model Checking (BMC)
- Some systems have probabilistic elements.
  $\Rightarrow$ Stochastic Bounded Model Checking

Table of Contents

Table of Contents

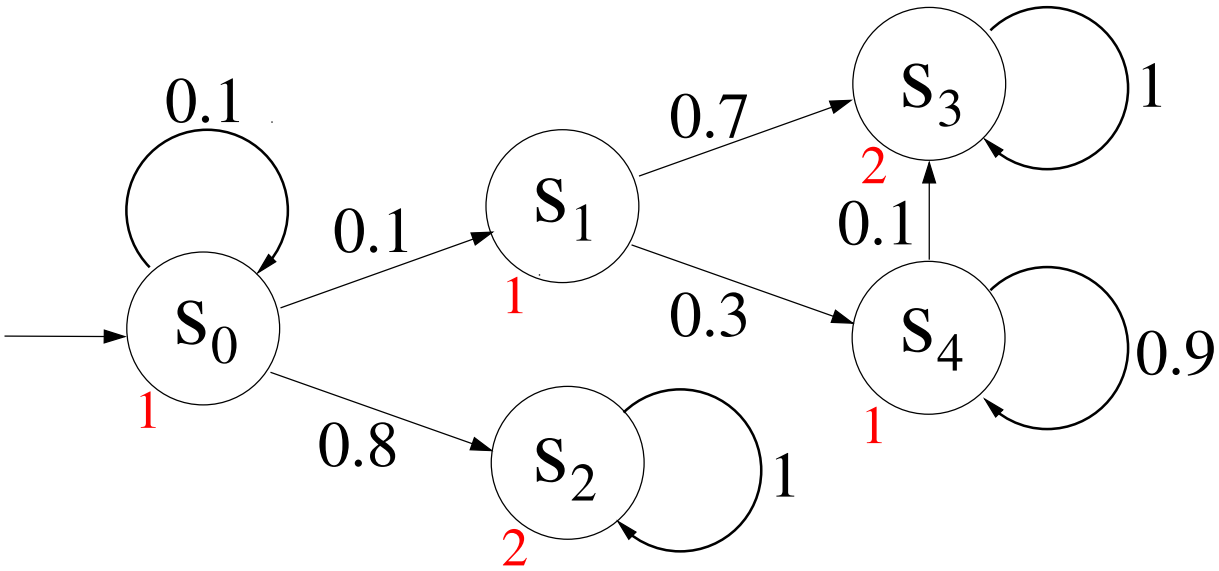
Stochastic Models

- A **Discrete-Time Markov Chain** (DTMC)
  $M = (S, s_I, P, L)$ consists of
  - S: finite set of states with initial state s_I,
  - $P : S \times S \to [0, 1]$: matrix of transition probabilities,
  - $L : S \to 2^{AP}$: labeling function.

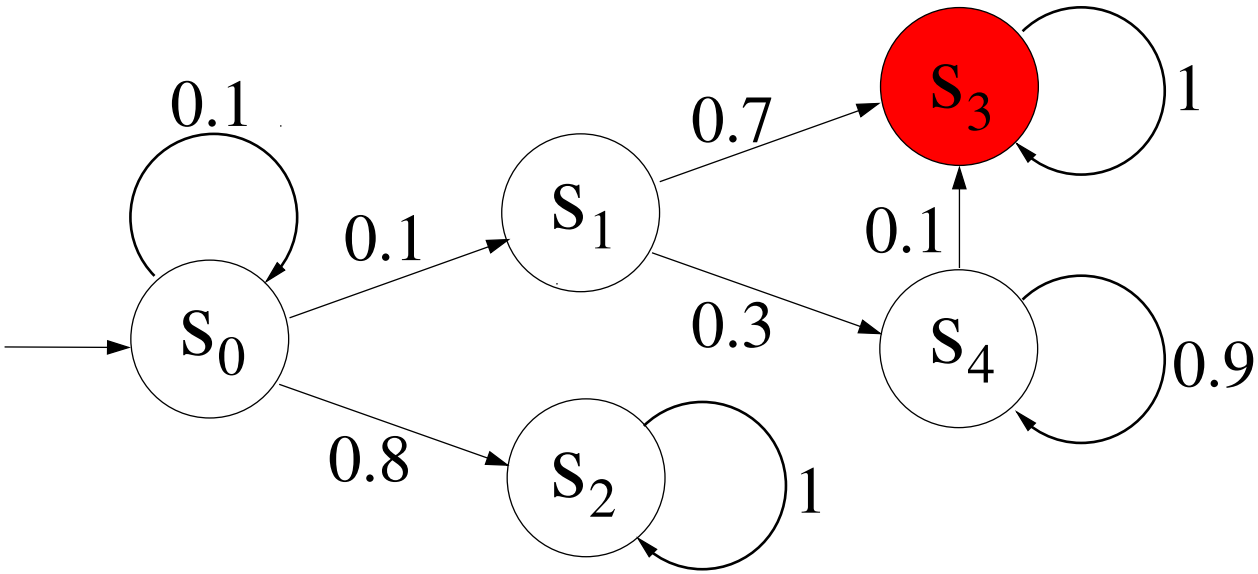


Stochastic Models

- A **Markov Reward Model (MRM)**
  (M, R) consists of a DTMC $M = (S, s_I, P, L)$ and a reward function $\mathbf{R} : S \to \mathbb{R}$.



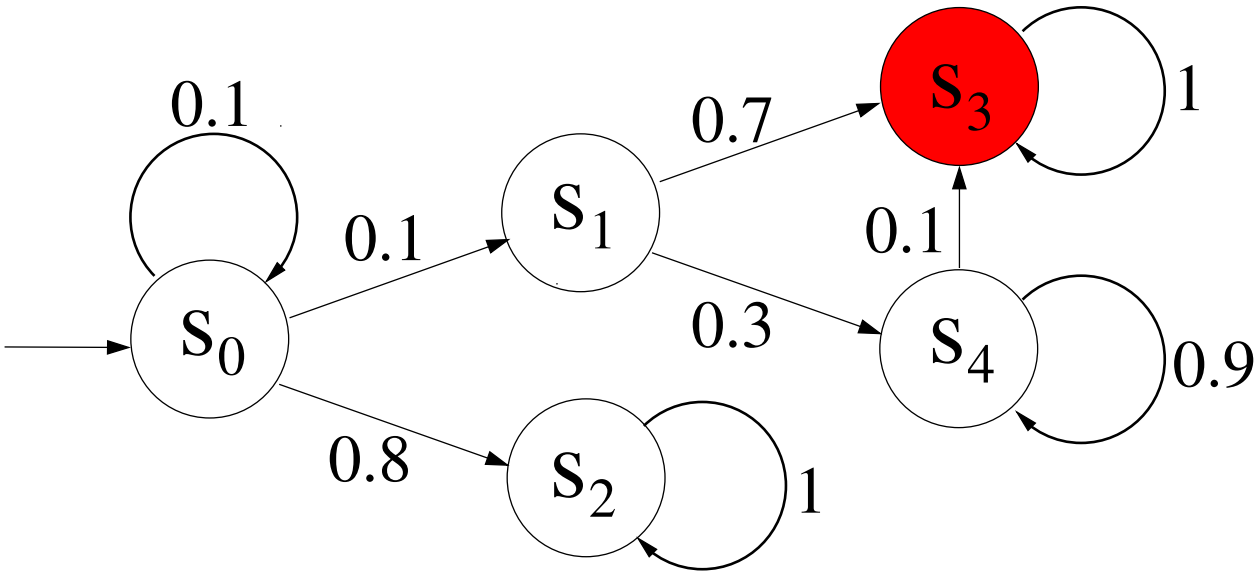
Counterexample for DTMCs (1)



Critical state s_3.
Should be reached with a probability of at most 0.08:

$$\mathcal{P}_{\leq 0.08}(\top \mathsf{U} s_3)$$

Counterexample for DTMCs (1)



Critical state s_3.
Should be reached with a probability of at most 0.08:

$$\mathcal{P}_{\leq 0.08}(\top \mathsf{U} s_3)$$

Does this property hold?

Counterexample for DTMCs (2)

Given: A DTMC M and a PCTL-property $\varphi = \mathcal{P}_{\leq p}(a \mathsf{U} b)$.

Counterexample for DTMCs (2)

Given: A DTMC M and a PCTL-property $\varphi = \mathcal{P}_{\leq p}(a \mathsf{U} b)$.

- An **evidence** is a finite path $\pi = s_0, s_1, \ldots, s_n$ with $s_0 = s_I$ and $\pi \models a \mathsf{U} b$. π is not a prefix of another evidence.
  π has the probability $\Pr(\pi) = \prod_{i=0}^{n-1} P(s_i, s_{i+1})$.

Counterexample for DTMCs (2)

Given: A DTMC M and a PCTL-property $\varphi = \mathcal{P}_{\leq p}(a \mathsf{U} b)$.

- An **evidence** is a finite path $\pi = s_0, s_1, \ldots, s_n$ with $s_0 = s_I$ and $\pi \models a \mathsf{U} b$. π is not a prefix of another evidence.
  π has the probability $\Pr(\pi) = \prod_{i=0}^{n-1} P(s_i, s_{i+1})$.
- A **counterexample** is a set C of evidences such that $\Pr(C) > p$.

Counterexample for MRMs (1)

Given: An MRM M and a PCTL-property $\varphi = \mathcal{P}_{\leq p}(a \mathsf{U}^{\mathcal{J}} b)$, $\mathcal{J} \subseteq \mathbb{R}$.

Counterexample for MRMs (1)

Given: An MRM M and a PCTL-property $\varphi = \mathcal{P}_{\leq p}(a \mathrm{U}^{\mathcal{J}} b)$, $\mathcal{J} \subseteq \mathbb{R}$.

- An **evidence** is a finite path $\pi = s_0, s_1, \ldots, s_n$ with $s_0 = s_I$ and $\pi \models a \mathrm{U} b$. π is not a prefix of another evidence.
  π has the probability $\Pr(\pi) = \prod_{i=0}^{n-1} P(s_i, s_{i+1})$.

- A **counterexample** is a set C of evidences such that $\Pr(C) > p$.

Counterexample for MRMs (1)

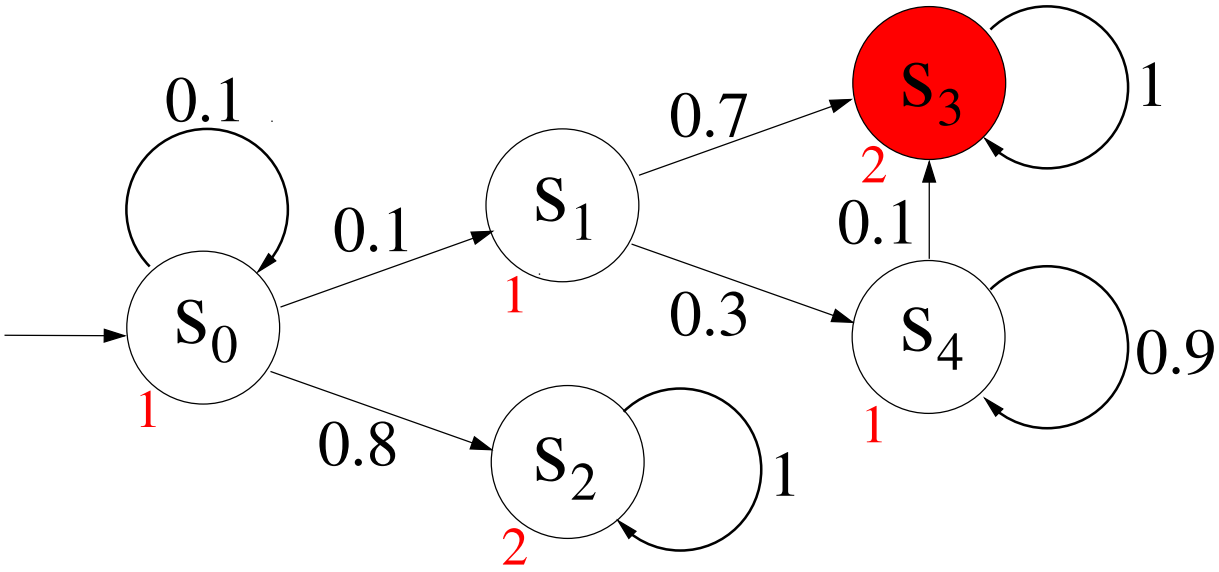
Given: An MRM M and a PCTL-property $\varphi = \mathcal{P}_{\leq p}(a \mathsf{U}^{\mathcal{J}} b)$, $\mathcal{J} \subseteq \mathbb{R}$.

- An **evidence** is a finite path $\pi = s_0, s_1, \ldots, s_n$ with $s_0 = s_I$ and $\pi \models a \mathsf{U} b$. π is not a prefix of another evidence.

  π has the probability $\Pr(\pi) = \prod_{i=0}^{n-1} P(s_i, s_{i+1})$.

  π has the reward $\mathrm{Re}(\pi) = \sum_{i=0}^{n-1} \mathbf{R}(s_i)$ and $\mathrm{Re}(\pi) \in \mathcal{J}$.
- A **counterexample** is a set C of evidences such that $\Pr(C) > p$.

Counterexample for MRMs (2)



Critical state s_3.
Should be reached with a probability of at most 0.08, rewards ≤ 2:

$$\mathcal{P}_{\leq 0.08}(\top \mathsf{U}^{[0,2]} s_3)$$

Does this property hold?

Table of Contents

Previous Approaches

Explicit:

Symbolic:

Previous Approaches

Explicit:

- Shortest path:
  - Aljazzar & Leue, 2010
  - Han, Katoen & Damman, 2009
- Regular expressions:
  - Han, Katoen, & Damman, 2009
- Strongly Connected Components (SCCs):
  - Andrés, D'Argenio & van Rossum, 2008
  - Ábrahám, Jansen, Wimmer, Katoen & Becker, 2010

Symbolic:

Previous Approaches

Explicit:

- Shortest path:
  - Aljazzar & Leue, 2010
  - Han, Katoen & Damman, 2009
- Regular expressions:
  - Han, Katoen, & Damman, 2009
- Strongly Connected Components (SCCs):
  - Andrés, D'Argenio & van Rossum, 2008
  - Ábrahám, Jansen, Wimmer, Katoen & Becker, 2010

Symbolic:

- Shortest path:
  - Günther, Schuster & Siegle, 2010
- Stochastic BMC (SBMC):
  - Wimmer, Braitling & Becker, 2009

Table of Contents

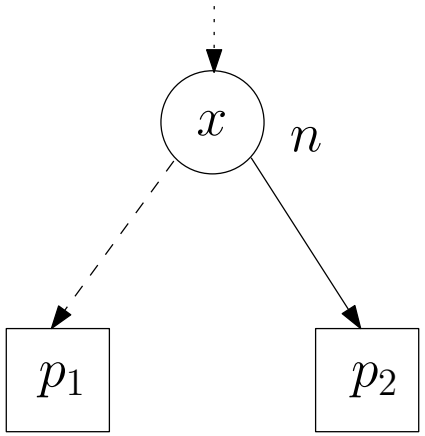
SMT-based Stochastic BMC (SSBMC) (1)

Consider transition probabilities during search:

$$I(s_0) \wedge \bigwedge_{i=0}^{k-1} T_{\mathrm{SMT}}(s_i, s_{i+1}, \hat{p}_i) \wedge L_b(s_k) \wedge \left(\sum_{i=0}^{k-1} \hat{p}_i \geq \log p_t \right)$$

- Solved by an SMT-solver.
- Solution corresponds to an evidence π of length k, $\Pr(\pi) \geq p_t$.
- Binary search by re-adjusting p_t.

SMT-based Stochastic BMC (SSBMC) (2)



$$n \leftrightarrow ((x \wedge \hat{p} = \log p_2) \vee (\neg x \wedge \hat{p} = \log p_1))$$

SMT-based Stochastic BMC (SSBMC) (3)

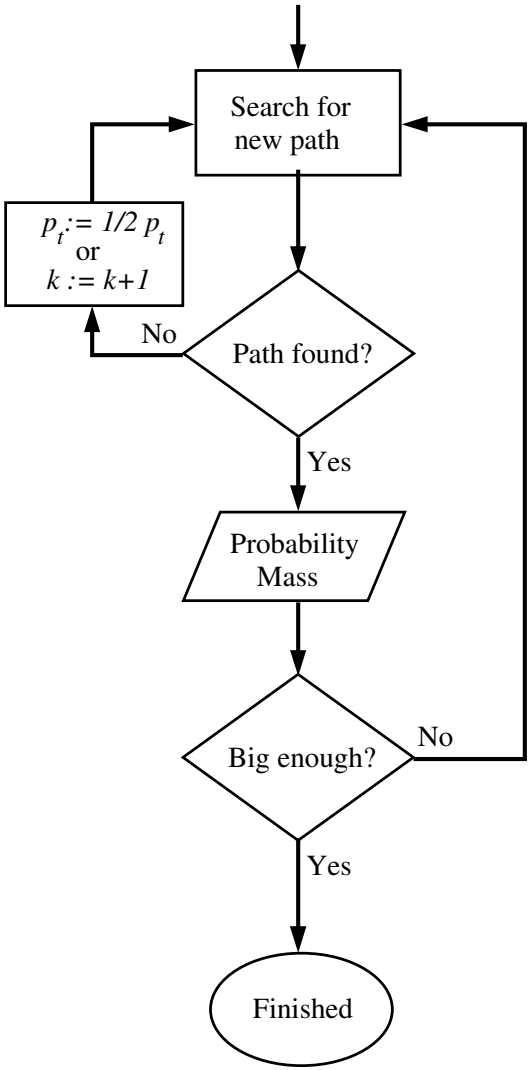


Table of Contents

Counterexamples for MRMs

SMT allows us to consider rewards:

$$I(s_0) \wedge \bigwedge_{i=0}^{k-1} T_{\text{SMT}}(s_i, s_{i+1}, \hat{p}_i) \wedge L_b(s_k) \wedge \left(\sum_{i=0}^{k-1} \hat{p}_i \geq \log p_t \right)$$
$$\wedge \bigwedge_{i=0}^{k-1} R(s_i, \hat{r}_i) \wedge \left(\min(\mathcal{I}) \leq \sum_{i=0}^{k-1} \hat{r}_i \leq \max(\mathcal{I}) \right)$$

Only paths with rewards within interval $\mathcal{I}$ are regarded.

Table of Contents

Experimental Results

Comparison between SSBMC and SBMC.

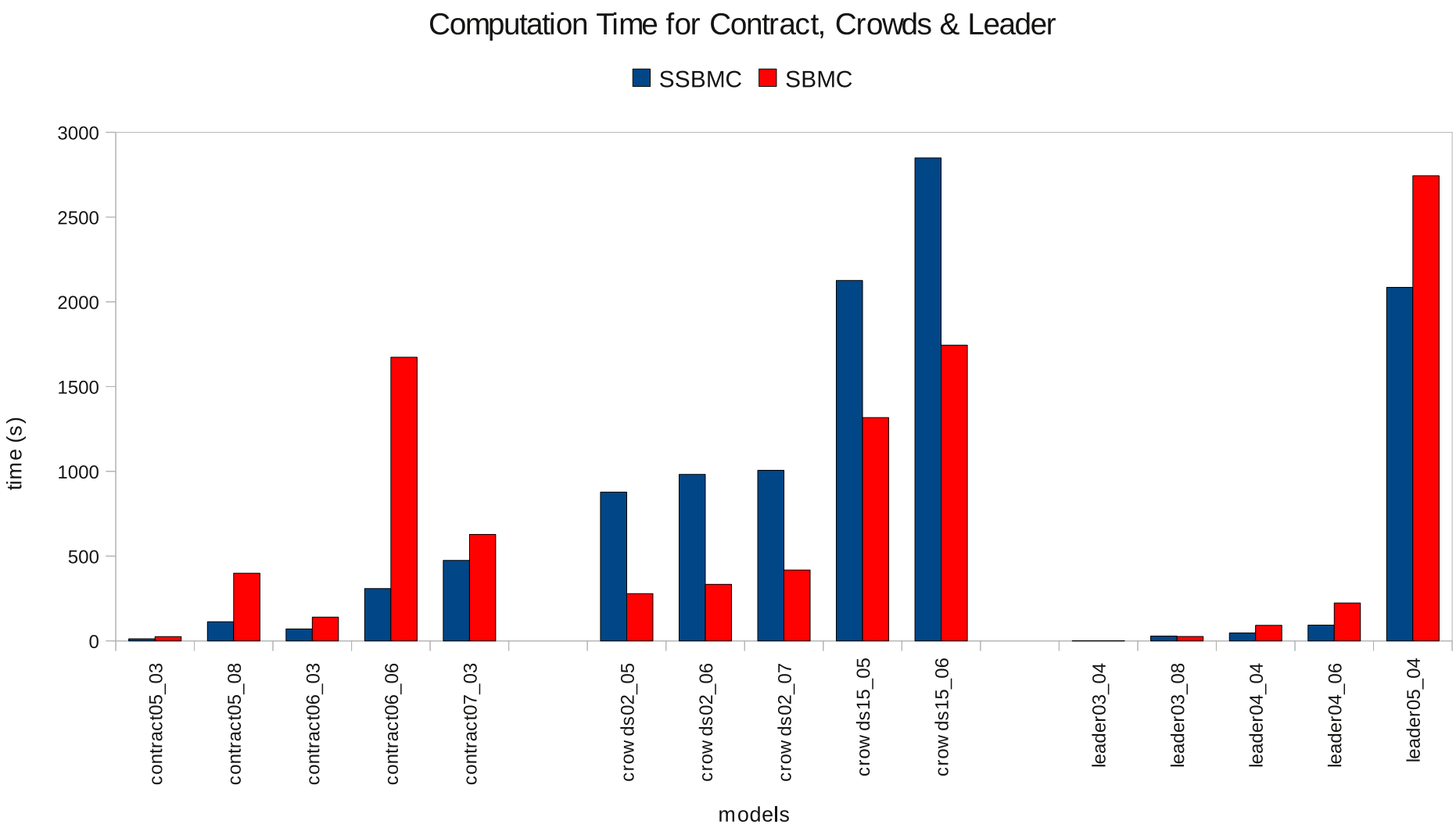
Benchmarks:

- Contract signing protocol
- Crowds protocol
- Leader election protocol
- Self-stabilizing minimal spanning tree algorithm

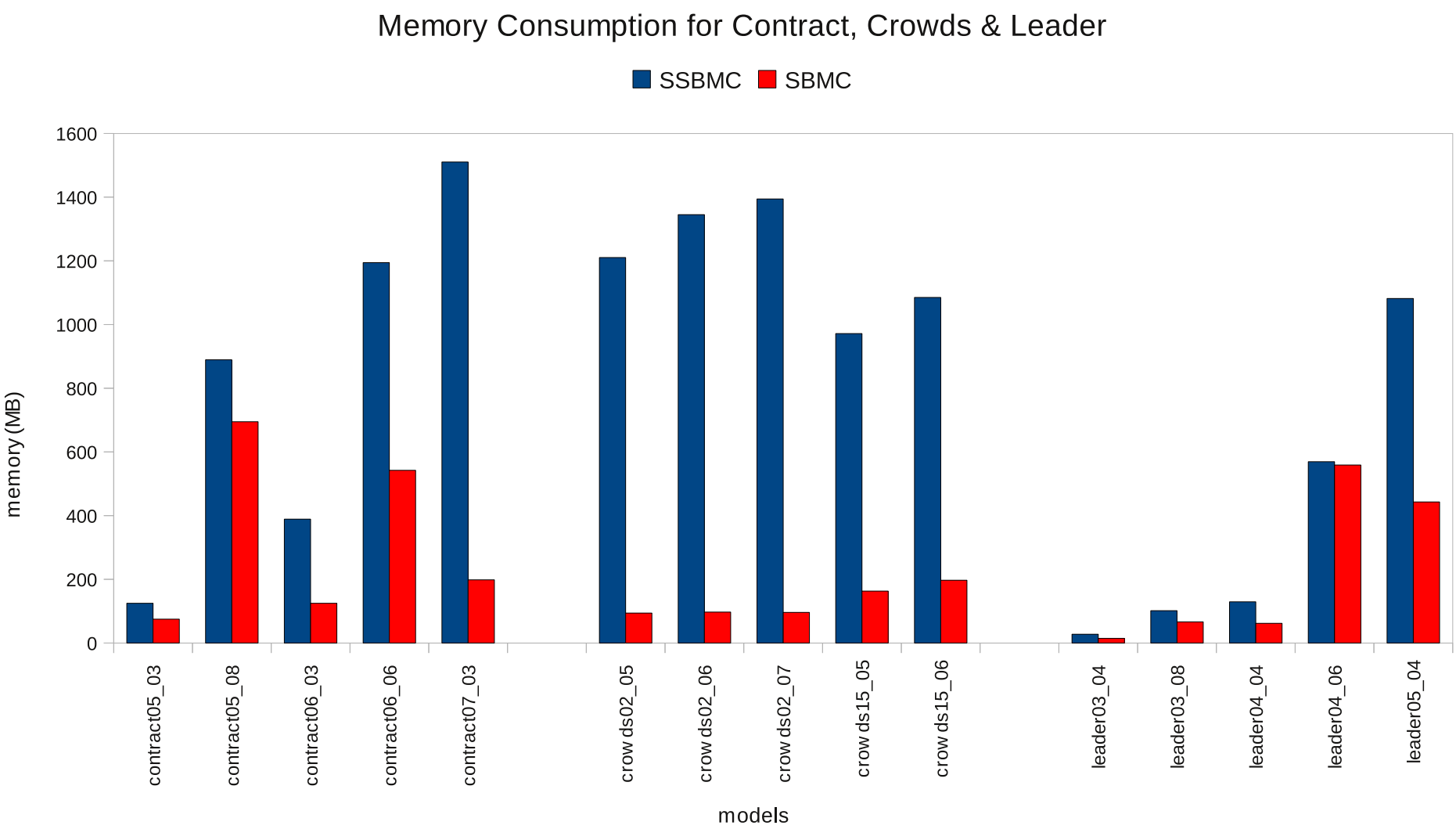
Setup:

- Underlying solvers: Yices (SMT-solver), Minisat (SAT-solver).
- Dual Core AMD Opteron with 2.4 GHz per core, 4 GB RAM.
- Time limit: 2 h, memory limit: 2 GB

SMT vs. SAT (1)


Computation Time for Contract, Crowds & Leader
SSBMC
SBMC
time (s)
3000
2500
2000
1500
1000
500
0
contract05_03
contract05_08
contract06_03
contract06_06
contract07_03
crowds02_05
crowds02_06
crowds02_07
crowds15_05
crowds15_06
leader03_04
leader03_08
leader04_04
leader04_06
leader05_04
models

SMT vs. SAT (2)


Memory Consumption for Contract, Crowds & Leader
SSBMC
SBMC
memory (MB)
1600
1400
1200
1000
800
600
400
200
0
contract05_03
contract05_08
contract06_03
contract06_06
contract07_03
crow ds02_05
crow ds02_06
crow ds02_07
crow ds15_05
crow ds15_06
leader03_04
leader03_08
leader04_04
leader04_06
leader05_04
models

Further Results

- Minimal Spanning Tree:

			SSBMC			**SBMC**		
Name	p	$k_{\max}$	#paths	time	mem.	#paths	time	mem.
mst15	0.049	15	4531	98.58	148.82	$>$ 600000	– TO –	
mst16	0.047	16	4648	107.27	158.25	$>$ 600000	– MO –	
mst18	0.036	18	4073	109.26	164.24	$>$ 600000	– MO –	
mst20	0.034	20	452	19.57	58.21	$>$ 500000	– TO –	

Further Results

- Minimal Spanning Tree:

			SSBMC			**SBMC**		
Name	p	k_{max}	#paths	time	mem.	#paths	time	mem.
mst15	0.049	15	4531	98.58	148.82	$>$ 600000	– TO –	
mst16	0.047	16	4648	107.27	158.25	$>$ 600000	– MO –	
mst18	0.036	18	4073	109.26	164.24	$>$ 600000	– MO –	
mst20	0.034	20	452	19.57	58.21	$>$ 500000	– TO –	

- SSBMC for MRMs:

Model	k_{max}	p	#paths	time	mem.
leader03_02	25	0.06226	360	1.00	29.61
leader04_02	25	0.21875	37376	912.11	1110.54
leader05_02	23	0.14771	4840	40.16	163.06
leader06_02	25	0.12378	32448	907.33	1360.11

Table of Contents

Conclusion & Outlook

- Conclusion:
  - SMT for Stochastic BMC.
  - Find paths with higher probabilities sooner.
  - Counterexamples for MRMs.
  - Promising results.

Conclusion & Outlook

- Conclusion:
  - SMT for Stochastic BMC.
  - Find paths with higher probabilities sooner.
  - Counterexamples for MRMs.
  - Promising results.
- Outlook:
  - Optimize the search for paths with higher probabilities.
  - Additional features: Loop detection, bisimulation minimization, transition rewards, ...
  - More benchmarks, especially MRMs.