Computing Conditional Probabilities: Implementation and Evaluation

Steffen Märcker,
Christel Baier, Joachim Klein, and Sascha Klüppelholz

Chair for Algebraic and Logical Foundations of Computer Science
Institute of Theoretical Computer Science - TU Dresden

September 07, 2017

Motivation

Probabilistic-Write/Copy-Select Protocol

- novel synchronization technique
- no locking but data duplication
- very low conflict probability

"What is the expected reading time under the condition that no conflict will occur?"

Motivation

What are conditional probabilities good for?

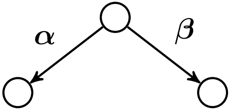
- **multi-objective reasoning**: tradeoffs between cost and utility measures
- **probabilistic programs**: formalization of loop semantics under the condition the loop terminates
- **reliability analysis**: "zoom in" failure scenarios to analyze impact of errors, recovery costs, and resilience properties
- **strong anonymity**: probability of a culprit is not increased by any observation

Markovian Models

Structure

Transition System

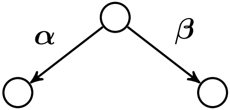
purely nondetermistic



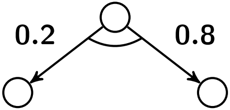
Markovian Models

Structure

Transition System
purely nondetermistic



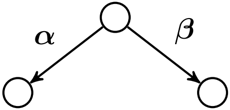
Markov Chain (MC)
purely probabilistic



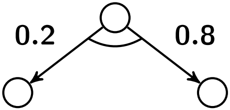
Markovian Models

Structure

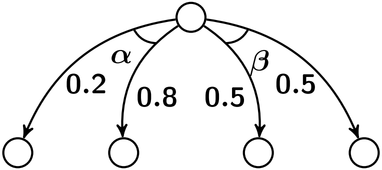
Transition System
purely nondetermistic



Markov Chain (MC)
purely probabilistic



Markov Decision Process (MDP)
combines nondeterminism and probabilism



Markovian Models

Probabilities

Markov Chains

- probabilities of reachability events:
  computable by solving systems of linear equations

Markovian Models

Probabilities

Markov Chains

- probabilities of reachability events:
  computable by solving systems of linear equations

Markov Decision Processes

- nondeterminism is resolved by **schedulers**
- maximal and minimal probabilities of reachability events:
  computable by solving linear programs

Markovian Models

Probabilities

Markov Chains

- probabilities of reachability events:
  computable by solving systems of linear equations

Markov Decision Processes

- nondeterminism is resolved by **schedulers**
- maximal and minimal probabilities of reachability events:
  computable by solving linear programs

Complex Path Formulas in Linear Temporal Logic (LTL)

- reducible to reachability via automata and product construction

Outline

Quotient Method

Straight-Forward Application of the Definition

The probability of an event $\mathcal{O}$ under the condition an event $\mathcal{C}$ occurs.

$\mathcal{O}$ the **objective**

$\mathcal{C}$ the **condition**

Quotient Method

Straight-Forward Application of the Definition

The probability of an event $\mathcal{O}$ under the condition an event $\mathcal{C}$ occurs.

$\mathcal{O}$ the **objective**

$\mathcal{C}$ the **condition**

Definition of Conditional Probability

$$\Pr(\mathcal{O} \mid \mathcal{C}) = \frac{\Pr(\mathcal{O} \wedge \mathcal{C})}{\Pr(\mathcal{C})}$$

Quotient Method

Straight-Forward Application of the Definition

The probability of an event $\mathcal{O}$ under the condition an event $\mathcal{C}$ occurs.

$\mathcal{O}$ the **objective**

$\mathcal{C}$ the **condition**

Definition of Conditional Probability

$$\Pr(\mathcal{O} \mid \mathcal{C}) = \frac{\Pr(\mathcal{O} \wedge \mathcal{C})}{\Pr(\mathcal{C})}$$

- applicable to MCs (if $\mathcal{O}$ and $\mathcal{C}$ have no time bounds)
- requires support for computing conjunctions of properties

Scale Method

Re-Scaling Probabilities in the Model

Idea

Re-scale probabilities in model according to probability of condition.

Transform Model $\mathcal{M}$ into $\mathcal{M}^{\mathcal{C}}$

$$\mathsf{Pr}_{\mathcal{M}}(\mathcal{O} \mid \mathcal{C}) = \mathsf{Pr}_{\mathcal{M}^{\mathcal{C}}}(\mathcal{O})$$

Scale Method

Re-Scaling Probabilities in the Model

Idea

Re-scale probabilities in model according to probability of condition.

Transform Model $\mathcal{M}$ into $\mathcal{M}^{\mathcal{C}}$

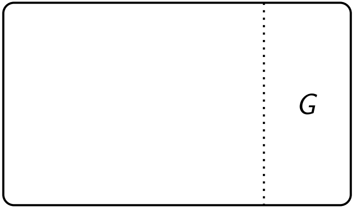
$$\mathsf{Pr}_{\mathcal{M}}(\mathcal{O} \mid \mathcal{C}) = \mathsf{Pr}_{\mathcal{M}^{\mathcal{C}}}(\mathcal{O})$$

- applicable to MCs (if $\mathcal{O}$, $\mathcal{C}$ have no time bounds)
- avoids computing conjunctions of properties
- enables computation of conditional expectations

Scale Method

Re-Scaling Transformation

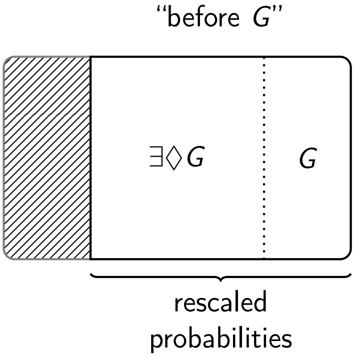
condition: "eventually G" for set of states $G \subseteq S$



Scale Method

Re-Scaling Transformation

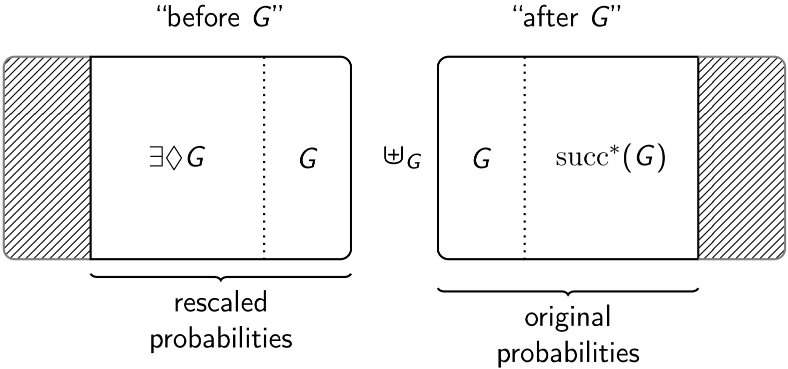
condition: “eventually G” for set of states $G \subseteq S$



Scale Method

Re-Scaling Transformation

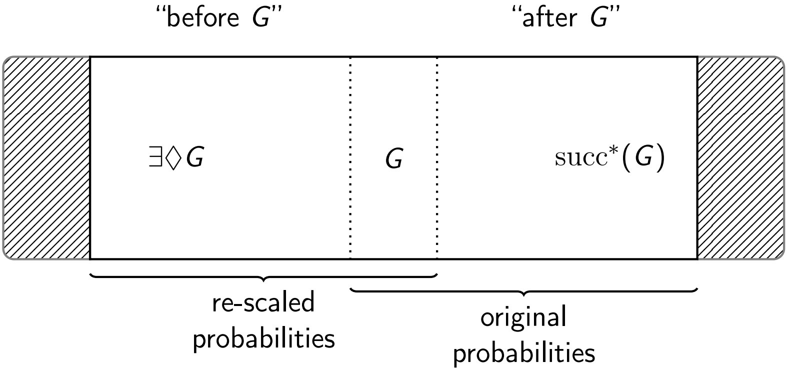
condition: "eventually G" for set of states $G \subseteq S$



Scale Method

Re-Scaling Transformation

condition: "eventually G" for set of states $G \subseteq S$



Definition of Maximal Conditional Probability

$$\mathsf{Pr}^{\max}_{\mathcal{M},s}(\mathcal{O} \mid \mathcal{C}) = \max_{\sigma} \frac{\mathsf{Pr}^{\sigma}_{\mathcal{M},s}(\mathcal{O} \wedge \mathcal{C})}{\mathsf{Pr}^{\sigma}_{\mathcal{M},s}(\mathcal{C})}$$

Quotient and scale method not applicable to MDPs.

Idea

Redistribute probabilities of all path that fail the condition.

Transform Model $\mathcal{M}$ into $\mathcal{M}^R$

$$\mathsf{Pr}^{\max}_{\mathcal{M},s}(\mathcal{O} \mid \mathcal{C}) = \mathsf{Pr}^{\max}_{\mathcal{M}^R,s}(\Diamond \mathsf{goal})$$

Reset Method

Redistributing Failed Probabilities

Idea

Redistribute probabilities of all path that fail the condition.

Transform Model $\mathcal{M}$ into $\mathcal{M}^R$

$$\mathsf{Pr}^{\max}_{\mathcal{M},s}(\mathcal{O} \mid \mathcal{C}) = \mathsf{Pr}^{\max}_{\mathcal{M}^R,s}(\Diamond \mathsf{goal})$$

- applicable to MDPs and MCs
- applicable to $\mathsf{Pr}^{\min}_{\mathcal{M},s}(\mathcal{O} \mid \mathcal{C}) = 1 - \mathsf{Pr}^{\max}_{\mathcal{M},s}(\neg\mathcal{O} \mid \mathcal{C})$
- time-complexity polynomial in size of $\mathcal{M}$

Reset Method

Reset Transformation

objective: "eventually F" for set of states $F \subseteq S$

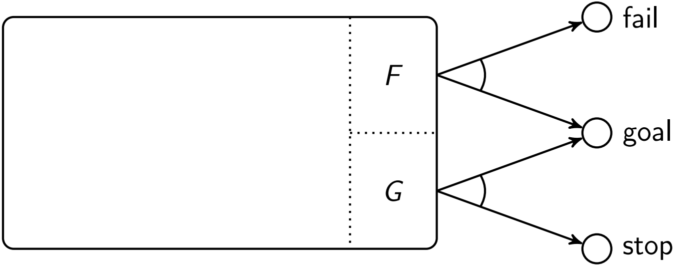
condition: "eventually G" for set of states $G \subseteq S$

Reset Method

Reset Transformation

objective: "eventually F" for set of states $F \subseteq S$

condition: "eventually G" for set of states $G \subseteq S$

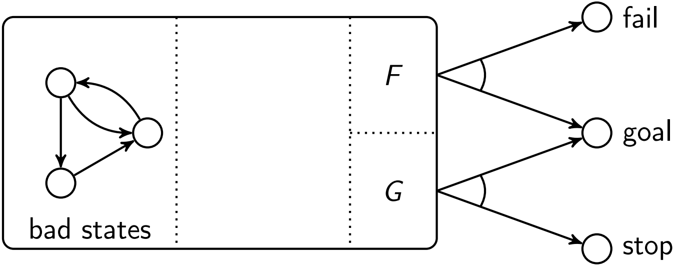


Reset Method

Reset Transformation

objective: "eventually F" for set of states $F \subseteq S$

condition: "eventually G" for set of states $G \subseteq S$

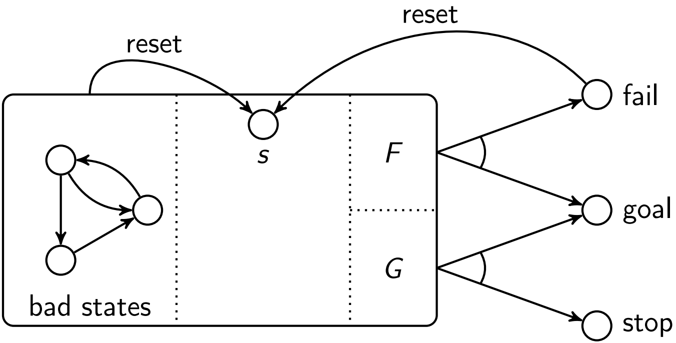


Reset Method

Reset Transformation

objective: "eventually F" for set of states $F \subseteq S$

condition: "eventually G" for set of states $G \subseteq S$



Patterns for Simple Paths Formulas

Generic Treatment of (Complex) Path Formulas

- reduction to conditional reachability probabilities via automata and product construction

Patterns for Simple Paths Formulas

Generic Treatment of (Complex) Path Formulas

- reduction to conditional reachability probabilities via automata and product construction

Special Treatment of Simple Path Formulas

- slightly generalized scale/reset transformations
- use patterns to match types of simple path formulas
- reset method: combine patterns for simple path formulas with generic handling of complex path formulas

Implementations

Prism prototype for TACAS'14

- MCs: LTL conditions, patterns for reachability conditions
- MDPs: reachability objectives and conditions
- engines: explicit

Implementations

Prism prototype for TACAS'14

- MCs: LTL conditions, patterns for reachability conditions
- MDPs: reachability objectives and conditions
- engines: explicit

Storm

- MCs, MDPs: reachability objectives and conditions
- engines: explicit and parametric (MCs)

Implementations

Prism prototype for TACAS'14

- MCs: LTL conditions, patterns for reachability conditions
- MDPs: reachability objectives and conditions
- engines: explicit

Storm

- MCs, MDPs: reachability objectives and conditions
- engines: explicit and parametric (MCs)

Prism current implementation

- MCs, MDPs: LTL objectives and conditions, patterns for all simple path formulas
- engines: explicit and (semi-)symbolic

Outline

Benchmarks

Models

- chosen from Prism benchmark suite:
  3 MCs (brp, crowds, egl) and 2 MDPs (wlan, consensus)
- criteria: meaningful conditional queries, scalability

Benchmarks

Models

- chosen from Prism benchmark suite:
  3 MCs (brp, crowds, egl) and 2 MDPs (wlan, consensus)
- criteria: meaningful conditional queries, scalability

Queries

- conditional expectations in MCs
- all combinations of patterns and LTL path formulas
- 190 runs for each MCs instance, 79 for each MDP instance

Benchmarks

Models

- chosen from Prism benchmark suite:
  3 MCs (brp, crowds, egl) and 2 MDPs (wlan, consensus)
- criteria: meaningful conditional queries, scalability

Queries

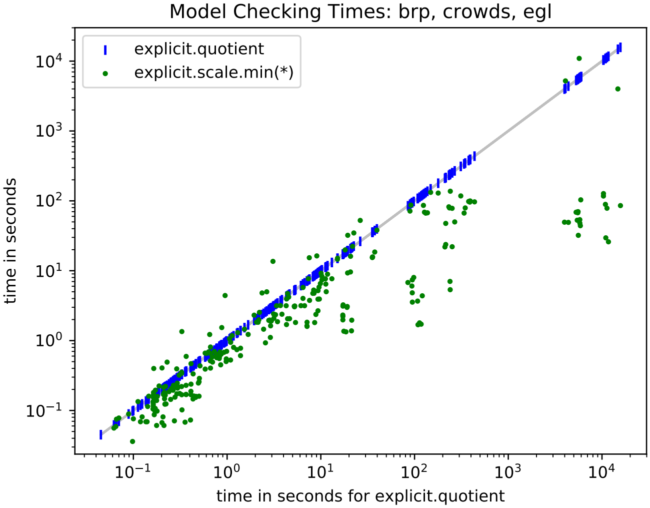
- conditional expectations in MCs
- all combinations of patterns and LTL path formulas
- 190 runs for each MCs instance, 79 for each MDP instance

Setup

- benchmark all supported engines of Prism's
- fix Java heap size and adjust the JVM's integer cache

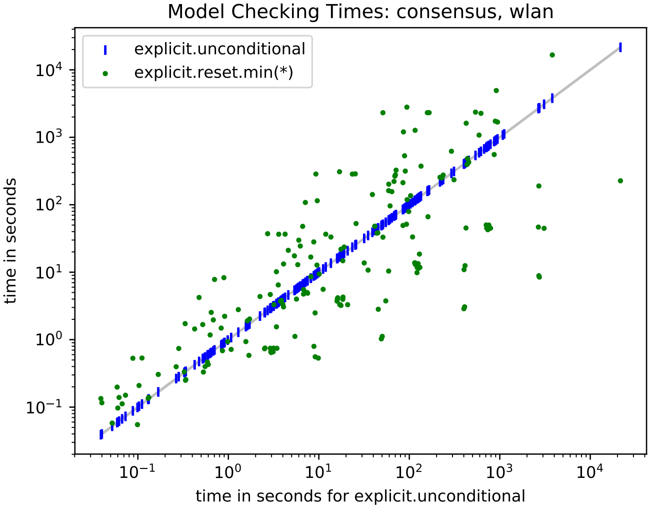
Results of Method Comparison

1) Scale method outperforms reset and quotient method.



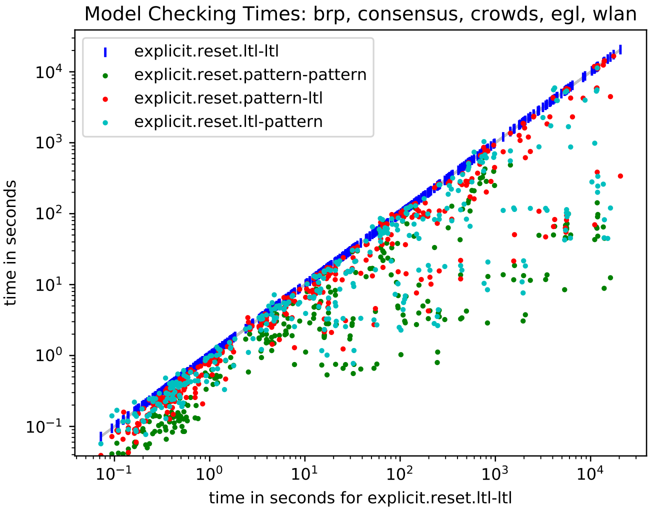
Results of Method Comparison

2) Reset method close to conjunction of objective and condition.



Results of Pattern Comparison

3) Specialized patterns perform better than generic handling.



Results of Implementations Comparison

Default Solvers

Prism Gauss-Seidel for MCs and
value iteration with Gauss-Seidel for MDPs

Storm GMRES+ILU for MCs and
value iteration with power method for MDPs

Results of Implementations Comparison

Default Solvers

Prism Gauss-Seidel for MCs and
value iteration with Gauss-Seidel for MDPs

Storm GMRES+ILU for MCs and
value iteration with power method for MDPs

	model	Prism explicit	Prism explicit'14	Storm explicit
MCs	brp	45 s	3515 s	4 s
	crowds	148 s	1933 s	55 s
	egl	242 s	2117 s	74 s
MDPs	consensus	41 s	116 s	120 s
	wlan	45 s	241 s	26 s

Results of Implementations Comparison

Same Solvers

Both Gauss-Seidel for MCs and
value iteration with power method for MDPs

	model	Prism explicit	Prism explicit'14	Storm explicit
MCs	brp	45 s	3515 s	228 s
	crowds	148 s	1933 s	192 s
	egl	242 s	2117 s	89 s
MDPs	consensus	79 s	177 s	120 s
	wlan	48 s	229 s	26 s

Outline

Conclusion

Implementation

- first full support for LTL objectives and conditions
- support for explicit and (semi-)symbolic engines

Evaluation

- scale method outperforms quotient method (MCs)
- reset method performs in the same order as computing conjunctions of events in many cases (MDPs)
- application of special patterns pays off
- competitive overall performance
- reset method may face convergence problems

Ongoing Work

Next Steps

- integration in official Prism release
- add support for interval iteration
- and support for Hanoi-framework to specify ω-regular events
- add algorithms for computing conditional expectations in MDPs

Fin
Merci encore.

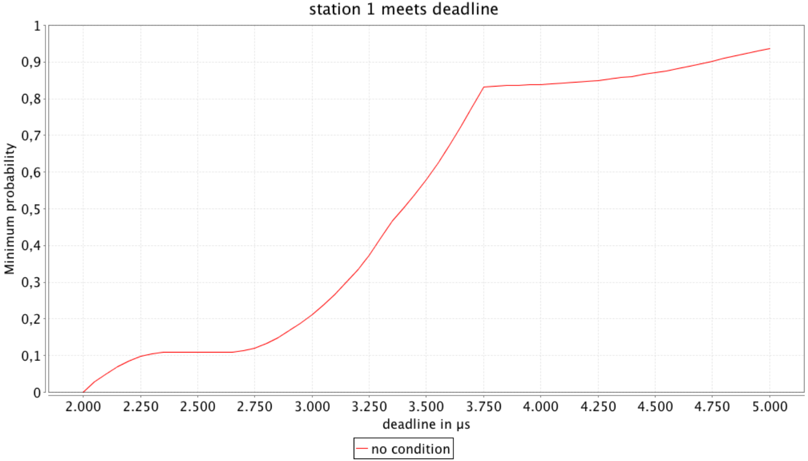
`https://wwwtcs.inf.tu-dresden.de/ALGI/PUB/SEFM17`

Example: CSMA/CA, IEEE 802.11 Wireless LAN

Example: WLAN protocol

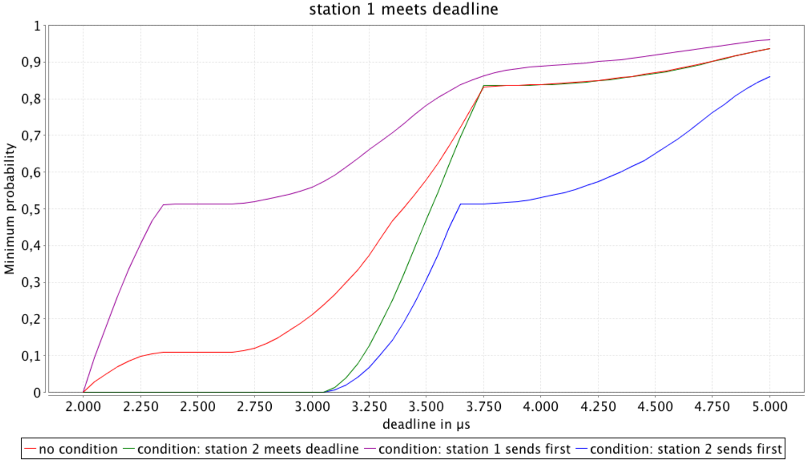
Example: CSMA/CA, IEEE 802.11 Wireless LAN

Example: WLAN protocol



Example: CSMA/CA, IEEE 802.11 Wireless LAN

Example: WLAN protocol



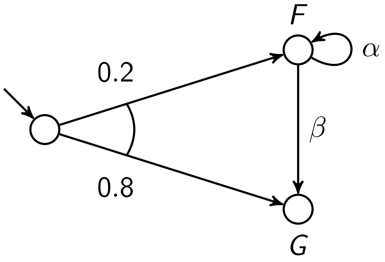
Pitfall: Conditions vs Scheduler Restrictions

Conditional probabilities do not prevent schedulers from violating the condition if this maximizes/minimizes the probability.

Pitfall: Conditions vs Scheduler Restrictions

Conditional probabilities do not prevent schedulers from violating the condition if this maximizes/minimizes the probability.

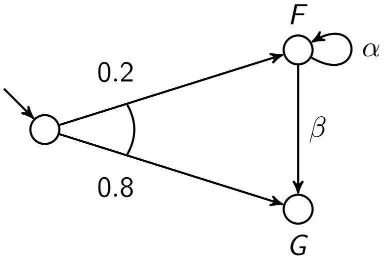
Example: Optimal But Defective Scheduler



Pitfall: Conditions vs Scheduler Restrictions

Conditional probabilities do not prevent schedulers from violating the condition if this maximizes/minimizes the probability.

Example: Optimal But Defective Scheduler



$$\Pr^{\min}(\Diamond F \mid \Diamond G) = \frac{0}{0.8} = 0 \quad \text{for} \quad \sigma(F) = \alpha$$

Literature I

- M. E. Andrés. "Quantitative Analysis of Information Leakage in Probabilistic and Nondeterministic Systems". PhD thesis. Radboud University, 2011.
- M. E. Andrés and P. van Rossum. "Conditional Probabilities over Probabilistic and Nondeterministic Systems". In: **14th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)**. Vol. 4963. Lecture Notes in Computer Science. 2008, pp. 157–172.
- M. Bhargava and C. Palamidessi. **Probabilistic anonymity**. Springer, 2005.

Literature II

- C. Dehnert, S. Junges, J. Katoen, and M. Volk. "A Storm is Coming: A Modern Probabilistic Model Checker". In: **29th International Conference on Computer Aided Verification (CAV), Part II**. LNCS 10427. Springer, 2017, pp. 592–600.
- M. Z. Kwiatkowska, G. Norman, and D. Parker. "PRISM 4.0: Verification of Probabilistic Real-Time Systems". In: **23rd International Conference on Computer Aided Verification (CAV)**. LNCS 6806. Springer, 2011, pp. 585–591.
- L. Zhang, H. Hermanns, E. M. Hahn, and B. Wachter. "Time-bounded model checking of infinite-state continuous-time Markov chains". In: **Application of Concurrency to System Design, 2008. ACSD 2008. 8th International Conference on**. IEEE. 2008, pp. 98–107.

Group's Publications I

- C. Baier, B. Engel, S. Klüppelholz, S. Märcker, H. Tews, and M. Völp. "A Probabilistic Quantitative Analysis of Probabilistic-Write/Copy-Select". In: **Proc. of the 5th NASA Formal Methods Symposium (NFM)**. Vol. 7871. Lecture Notes in Computer Science. Springer, 2013, pp. 307–321.
- C. Baier, J. Klein, S. Klüppelholz, and S. Märcker. "Computing Conditional Probabilities in Markovian Models Efficiently". In: **Proc. of the 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)**. Vol. 8413. Lecture Notes in Computer Science. Springer, 2014, pp. 515–530.

Group's Publications II

- C. Baier, J. Klein, S. Klüppelholz, and S. Wunderlich. "Maximizing the Conditional Expected Reward for Reaching the Goal". In: **23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), Part II**. LNCS 10206. Springer, 2017, pp. 269–285.

- C. Baier, J. Klein, L. Leuschner, D. Parker, and S. Wunderlich. "Ensuring the Reliability of Your Model Checker: Interval Iteration for Markov Decision Processes". In: **29th International Conference on Computer Aided Verification (CAV), Part I**. LNCS 10426. Springer, 2017, pp. 160–180.