Advances in Probabilistic Model Checking

Marta Kwiatkowska
University of Oxford, United Kingdom

Probabilistic model checking is a formal verification technique for the analysis of systems that exhibit stochastic behaviour. Such behaviour occurs, for example, due to randomisation, commonly used as a symmetry breaker in distributed coordination, security and communication protocols. Stochastic modelling is also important in performability, dependability and fault-tolerance. Probabilistic model checking enables a range of quantitative analyses of probabilistic models against specifications such as the worst-case probability of intrusion within 10 seconds or the minimum expected power consumption over all possible schedulings. In recent years, increasing interest in the topic of probabilistic verification has led to significant advances in the applicability and efficiency of these techniques, as well as the discovery of interesting and anomalous behaviour in a wide range of real-life case studies.

This course will give an introduction to probabilistic model checking, as well as presenting material on some recent advances in the area. The first half of the course will introduce two types of probabilistic models, *discrete-time Markov chains* and *Markov decision processes*, explaining the underlying theory and model checking algorithms for temporal logics such as PCTL and LTL. The second half of the course will cover two more advanced topics:

- *compositional probabilistic verification techniques* for MDPs, based on assume-guarantee methods and multi-objective model checking; and
- *verification of probabilistic real-time systems*, namely probabilistic timed automata.

The course will also introduce PRISM [4,6], a state-of-the-art probabilistic model checker, and illustrate several case studies that have been modelled and analysed in PRISM, such as Bluetooth device discovery, Zeroconf link-local addressing and probabilistic contract signing.

Preparatory reading material

The following tutorial papers provide comprehensive introductory material for the topics covered in this course:

- [3] (sections 1-3), for discrete-time Markov chains (DTMCs);
- [2] (sections 1-7), for Markov decision processes (MDPs);
- [2] (sections 8-9), for assume-guarantee verification;
- [5] for probabilistic timed automata (PTAs).

Chapter 10 of [1] is also highly recommended for further background material on model checking of DTMCs and MDPs. Students interested in learning more about PRISM [4] are suggested to consult the tool web site [6], which includes a tutorial, case study repository and much more.

References

[1] C. Baier, J.-P. Katoen. *Principles of Model Checking.* MIT Press, 2008.

[2] V. Forejt, M. Kwiatkowska, G. Norman, D. Parker. *Automated Verification Techniques for Probabilistic Systems.* In: M. Bernardo, V. Issarny (eds), Formal Methods for Eternal Networked Software Systems (SFM'11), Springer, 2011.

[3] M. Kwiatkowska, G. Norman, D. Parker. *Stochastic Model Checking.* In: M. Bernardo, J. Hillston (eds), Formal Methods for the Design of Computer, Communication and Software Systems: Performance Evaluation (SFM'07), LNCS 4486 (Tutorial Volume), pp. 220-270, Springer, 2007.

[4] M. Kwiatkowska, G. Norman, D. Parker. *PRISM 4.0: Verification of Probabilistic Real-time Systems.* In: Proc. 23rd International Conference on Computer Aided Verification (CAV'11), LNCS, Springer, 2011.

[5] M. Kwiatkowska, G. Norman, D. Parker, J. Sproston. *Verification of Real- Time Probabilistic Systems.* In: Modeling and Verification of Real-Time Systems: Formalisms and Software Tools, pp. 249-288, John Wiley & Sons, 2008.

[6] PRISM web site. `http://www.prismmodelchecker.org/`