Preface to the special issue on Probabilistic Model Checking

Christel Baier · Marta Kwiatkowska

Published online: 17 August 2013
© Springer Science+Business Media New York 2013

As guest editors, we are delighted to introduce this special issue devoted to Probabilistic Model Checking to the wider readership. Probabilistic modelling dates back to the work of Markov in early 1900s, and over the years has established itself as a fundamental methodology in science and technology, with numerous applications across several domains. Markovian models feature in probabilistic programming; wireless communication, anonymity and security protocols; performance, reliability and dependability analysis; robotics and planning; scheduling and optimisation; predictive modelling of biological systems; population models of epidemic spread; and techniques such as page ranking of search engines. Probabilistic model checking aims to achieve automated analysis of probabilistic models against specifications given in temporal logic, and involves an intricate combination of conventional model checking algorithms with the computation of probabilities or expectations via the solution of linear equations or linear programming problems.

The origins of probabilistic model checking are rooted in the work of Hart, Sharir and Pnueli [10] and Vardi [16] in the mid-1980s, who were mainly concerned with verifying qualitative, almost sure, probabilistic properties for Markov chains and Markov decision processes. Quantitative model checking algorithms, where the actual probability value is computed, were formulated in 1990s by Courcoubetis and Yannakakis [7], Hansson and Johnsson [9], Bianco and de Alfaro [4] and Baier and Kwiatkowska [1], for both branching- and linear-time variants of temporal logic, along with the first prototype tools. The first BDD-based symbolic approach was proposed in 1997 by Baier, Clarke, Hartonas-Garmhausen, Kwiatkowska and Ryan [2], paving the way to a scalable implementation in the PRISM model checker [14] released in 2001. In the same decade, two further model

C. Baier
TU Dresden, Fakultät Informatik, 01062 Dresden, Germany
e-mail: baier@tcs.inf.tu-dresden.de

M. Kwiatkowska (✉)
Department of Computer Science, University of Oxford, Oxford, United Kingdom
e-mail: marta.kwiatkowska@cs.ox.ac.uk

checkers, MRMC that supports bisimulation minimisation and LIQUOR based on partial order reduction, were released, which stimulated the wide adoption of quantitative, probabilistic model checking techniques for research and teaching. Notably, several flaws and unusual trends were automatically discovered in real-world case studies, for example the Crowds anonymity protocol [15].

In the last few years, probabilistic model checking became established as a mature and highly active research field, opening up new and exciting lines of enquiry. A variety of more expressive models were formulated and novel methodologies put forward, for example statistical model checking, where the computation of the probability is based on statistical inference over execution paths rather than an exploration of the state transition graph. This special issue is devoted to a selection of papers which demonstrate the tremendous progress made in recent years, while at the same time highlighting the challenges that remain.

The first group of three papers is concerned with generalisations of Markovian models. First, in [5], the authors consider probabilistic models which arise from Markov chains enhanced with recursion, called probabilistic pushdown automata. In [13], a tutorial-style overview is given for model checking of probabilistic timed automata, which arise as conventional timed automata extended with discrete probability distributions to model transitions between the locations. Several model checking approaches have been developed for probabilistic timed automata, now implemented in PRISM, and the paper illustrates their use for verification and scheduler synthesis by means of modelling case studies. In a different direction, [8] consider a probabilistic extension of hybrid automata, where the continuous variables are not just clocks, as is the case with probabilistic timed automata, but are endowed with dynamics expressed in terms of (linear) differential equations. A process-algebraic modelling language called HModest, an extension of the Modest language with hybrid features, is proposed, and a compositional reduction from the terms of the language to subclasses of stochastic hybrid automata is formulated. The paper then summarises recent advances concerning safety verification of industrially-relevant case studies.

The next group of two papers focuses on extensions of the methods that go beyond the status-quo of finite-state, fully observable, closed systems. [3] consider infinite-state probabilistic systems, and prove finite-time convergence for μ -calculus formulas based on well-quasi-orderings. This work has applications to the verification of probabilistic lossy channel systems. In [6], a stochastic extension of parity games is considered, which is important for controller synthesis in robotics. The authors survey the complexity results for verification problems for such games under partial observability.

The final group of three papers represents methodological advances. In [11], game semantics is applied to obtain a compositional fully-abstract method for establishing equivalence between probabilistic call-by-value programs. The techniques have been implemented and applied to several case studies, with encouraging results. [12] consider the setting of large continuous time Markov chains, for which properties are specified using deterministic timed automata, and formulate an on-the-fly method to combat the state-space explosion problem when maximising the probability of the property being satisfied. The techniques successfully scale up to biological case studies. Finally, [17] overview Bayesian statistical model checking techniques, which avoid the need to construct the transition graph by simulating execution paths and applying statistical inference on those paths, and apply it to a Stateflow/Simulink case study.

We hope that readers will find this volume informative, and that it stimulates more research and eventual breakthroughs in probabilistic model checking that overcome the difficulties of state-space explosion and integration of discrete, continuous and stochastic dynamics, leading to effective, usable software tools.

References

1. Baier C, Kwiatkowska M (1998) Model checking for a probabilistic branching time logic with fairness. *Distrib Comput* 11(3):125–155
2. Baier C, Clarke E, Hartonas-Garmhausen V, Kwiatkowska M, Ryan M (1997) Symbolic model checking for probabilistic processes. In: Degano P, Gorrieri R, Marchetti-Spaccamela A (eds) *Proc 24th Int Colloq Automata, Languages and Programming (ICALP'97)*. LNCS, vol 1256. Springer, Berlin, pp 430–440
3. Bertrand N, Schnoebelen P (2012) Computable fixpoints in well-structured symbolic model checking. *Form Methods Syst Des*. doi:[10.1007/s10703-012-0168-y](https://doi.org/10.1007/s10703-012-0168-y)
4. Bianco A, de Alfaro L (1995) Model checking of probabilistic and nondeterministic systems. In: Thiagarajan P (ed) *Proc 15th conf Foundations of Software Technology and Theoretical Computer Science (FSTTCS'95)*. LNCS, vol 1026. Springer, Berlin, pp 499–513
5. Brázdil T, Esparza J, Kiefer S, Kucera A (2012) Analyzing probabilistic pushdown automata. *Form Methods Syst Des*. doi:[10.1007/s10703-012-0166-0](https://doi.org/10.1007/s10703-012-0166-0)
6. Chatterjee K, Doyen L, Henzinger T (2012) A survey of partial-observation stochastic parity games. *Form Methods Syst Des*. doi:[10.1007/s10703-012-0164-2](https://doi.org/10.1007/s10703-012-0164-2)
7. Courcoubetis C, Yannakakis M (1995) The complexity of probabilistic verification. *J ACM* 42(4):857–907
8. Hahn E, Hartmanns A, Hermanns H, Katoen J-P (2012) A compositional modelling and analysis framework for stochastic hybrid systems. *Form Methods Syst Des*. doi:[10.1007/s10703-012-0167-z](https://doi.org/10.1007/s10703-012-0167-z)
9. Hansson H, Jonsson B (1994) A logic for reasoning about time and reliability. *Form Asp Comput* 6(5):512–535
10. Hart S, Sharir M, Pnueli A (1983) Termination of probabilistic concurrent programs. *ACM Trans Program Lang Syst* 5(3):356–380
11. Kiefer S, Murawski A, Ouaknine J, Wachter B, Worrell J (2012) Algorithmic probabilistic game semantics. *Form Methods Syst Des*. doi:[10.1007/s10703-012-0173-1](https://doi.org/10.1007/s10703-012-0173-1)
12. Mikeev L, Neuhäuser M, Spieler D, Wolf V (2012) On-the-fly verification and optimization of DTA-properties for large Markov chains. *Form Methods Syst Des*. doi:[10.1007/s10703-012-0165-1](https://doi.org/10.1007/s10703-012-0165-1)
13. Norman G, Parker D, Sproston J (2012) Model checking for probabilistic timed automata. *Form Methods Syst Des*. doi:[10.1007/s10703-012-0177-x](https://doi.org/10.1007/s10703-012-0177-x)
14. PRISM probabilistic model checker. www.prismmodelchecker.org
15. Shmatikov V (2002) Probabilistic analysis of anonymity. In: *Proc. 15th IEEE Computer Security Foundations Workshop (CSFW'02)*. IEEE Comput. Soc., Los Alamitos, pp 119–128
16. Vardi M (1985) Automatic verification of probabilistic concurrent finite state programs. In: *Proc 26th Annual Symp Foundations of Computer Science (FOCS'85)*. IEEE Comput. Soc., Los Alamitos, pp 327–338
17. Zuliani P, Platzer A, Clarke E (2013) Bayesian statistical model checking with application to Stateflow/Simulink verification. In: *Formal methods in system design*. doi:[10.1007/s10703-013-0195-3](https://doi.org/10.1007/s10703-013-0195-3)