Abstract of PhD Thesis

Author:	Mark Timmer
Title:	Efficient Modelling, Generation and Analysis of Markov Automata
Language:	English
Supervisor:	Joost-Pieter Katoen, Jaco van de Pol and Mariëlle Stoelinga
Institute:	University of Twente, The Netherlands
Date:	13 September 2013

Abstract

Quantitative model checking is concerned with the verification of both quantitative and qualitative properties over models incorporating quantitative information. Increases in expressivity of the models involved allow more types of systems to be analysed, but also raise the difficulty of their efficient analysis.

Three years ago, the Markov automaton (MA) was introduced as a generalisation of probabilistic automata and interactive Markov chains, supporting nondeterminism, discrete probabilistic choice as well as stochastic timing (Markovian rates). Later, the tool IMCA was developed to compute time-bounded reachability probabilities, expected times and long-run averages for sets of goal states within an MA. However, an efficient formalism for modelling and generating MAs was still lacking. Additionally, the omnipresent state space explosion also threatened the analysability of these models. This thesis solves the first problem and contributes significantly to the solution of the second.

First, we introduce the process-algebraic language MAPA for modelling MAs. It incorporates the use of static as well as dynamic data (such as lists), allowing systems to be modelled efficiently. A transformation of MAPA specifications to a restricted part of the language—enabled through an encoding of Markovian rates in action—allows for easy parallel composition, state space generation and syntactic optimisations (also known as reduction techniques).

Second, we introduce five reduction techniques for MAPA specifications: constant elimination, expression simplification, summation elimination, dead variable reduction and confluence reduction. The first three aim to speed up state space generation by simplifying the specification, while the last two aim to speed up analysis by reductions in the size of the state space. Dead variable reduction resets data variables the moment their value becomes irrelevant, while conflu-

ence reduction detects and resolves spurious nondeterminism often arising in the presence of loosely coupled parallel components. Since MAs generalise labelled transition systems, discrete-time Markov chains, continuous-time Markov chains, probabilistic automata and interactive Markov chains, our techniques and results are also applicable to all these subclasses.

Third, we thoroughly compare confluence reduction to the ample set variant of partial order reduction. Since partial order reduction has not yet been defined for MAs, we restrict both to the context of probabilistic automata. We precisely pinpoint the differences between the two methods on a theoretical level, resolving the long-standing uncertainty about the relation between these two concepts: when preserving branching-time properties, confluence reduction strictly subsumes partial order reduction and hence is slightly more powerful. Also, we compare the techniques in the practical setting of statistical model checking, demonstrating that the additional potential of confluence indeed may provide larger reductions (even compared to a variant of the ample set method that only preserves linear-time properties).

We developed a tool called SCOOP, which contains all our techniques and is able to export to the IMCA tool. Together, these tools for the first time allow the analysis of MAs. Case studies on a handshake register, a leader election protocol, a polling system and a processor grid demonstrate the large variety of systems that can be modelled using MAPA. Experiments additionally show significant reductions by all our techniques, sometimes reducing state spaces to less than a percent of their original size. Moreover, our results enable us to provide guidelines that indicate for each technique the aspects of case studies that predict large reductions.

In the end, MAPA indeed enables us to efficiently specify systems incorporating nondeterminism, discrete probabilistic choice and stochastic timing. It also allows several advanced reduction techniques to be applied rather easily, leading us to define a variety of such techniques. Our comparison of confluence reduction and partial order reduction provides several novel insights in their relation. Also, experiments show that our techniques greatly reduce the impact of the state space explosion: a major step forward in efficient quantitative verification.

Author's correspondence address Mark Timmer
University of Twente
Formal Methods and Tools, Zilverling
P.O. Box 217, 7500 AE Enschede
The Netherlands
Email: *timmer@cs.utwente.nl*