Information and Computation 232 (2013) 38–65

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Compositional probabilistic verification through multi-objective model checking

Marta Kwiatkowska [a], Gethin Norman [b], David Parker [c,*], Hongyang Qu [a,1]

[a] *Department of Computer Science, University of Oxford, Oxford, OX1 3QD, UK*
[b] *School of Computing Science, University of Glasgow, Glasgow, G12 8RZ, UK*
[c] *School of Computer Science, University of Birmingham, Birmingham, B15 2TT, UK*

ARTICLE INFO

Article history:
Received 7 May 2012
Received in revised form 1 June 2013
Available online 9 October 2013

Keywords:
Probabilistic verification
Compositional verification
Assume-guarantee reasoning
Probabilistic automata

ABSTRACT

Compositional approaches to verification offer a powerful means to address the challenge of scalability. In this paper, we develop techniques for compositional verification of probabilistic systems based on the assume-guarantee paradigm. We target systems that exhibit both nondeterministic and stochastic behaviour, modelled as probabilistic automata, and augment these models with costs or rewards to reason about, for example, energy usage or performance metrics. Despite significant theoretical advances in compositional reasoning for probabilistic automata, there has been a distinct lack of practical progress regarding automated verification. We propose a new assume-guarantee framework based on multi-objective probabilistic model checking which supports compositional verification for a range of quantitative properties, including probabilistic ω-regular specifications and expected total cost or reward measures. We present a wide selection of assume-guarantee proof rules, including asymmetric, circular and asynchronous variants, and also show how to obtain numerical results in a compositional fashion. Given appropriate assumptions to be used in the proof rules, our compositional verification methods are, in contrast to previously proposed approaches, efficient and fully automated. Experimental results demonstrate their practical applicability on several large case studies, including instances where conventional probabilistic verification is infeasible.

1. Introduction

Many computerised systems exhibit probabilistic behaviour, for example due to the use of randomisation (e.g., in distributed communication or security protocols), or the presence of failures (e.g., in faulty devices or unreliable communication media). The prevalence of such systems in today's society makes techniques for their formal verification a necessity. This requires models and formalisms that incorporate both *probability* and *nondeterminism*. Although efficient algorithms for verifying such models are known [1–3] and mature tool support exists [4,5], applying these techniques to large, real-life systems remains challenging, and hence techniques to improve scalability are essential.

In this paper, we focus on *compositional* verification techniques for probabilistic and nondeterministic models, in which a system comprising multiple interacting components can be verified by analysing each component in isolation, rather than verifying the much larger model of the whole system. In the case of non-probabilistic models, a successful approach is

[*] Corresponding author.
E-mail addresses: marta.kwiatkowska@cs.ox.ac.uk (M. Kwiatkowska), gethin.norman@glasgow.ac.uk (G. Norman), d.a.parker@cs.bham.ac.uk (D. Parker), h.qu@sheffield.ac.uk (H. Qu).
[1] Hongyang Qu is now with the Department of Automatic Control and Systems Engineering, University of Sheffield.

http://dx.doi.org/10.1016/j.ic.2013.10.001

the use of *assume-guarantee* reasoning [6,7]. This is based on checking queries of the form $\langle \Psi_A \rangle \mathcal{M} \langle \Psi_G \rangle$, with the meaning "whenever component $\mathcal{M}$ is part of a system satisfying the *assumption* Ψ_A, then the system is *guaranteed* to satisfy property Ψ_G". Proof rules can then be established to show, for example, that, if a component $\mathcal{M}_1$ satisfies assumption Ψ_A and $\langle \Psi_A \rangle \mathcal{M}_2 \langle \Psi_G \rangle$ holds for a second component $\mathcal{M}_2$, then the combined system $\mathcal{M}_1 \parallel \mathcal{M}_2$ satisfies Ψ_G.

For *probabilistic* systems, compositional approaches have also been studied, but a distinct lack of practical progress has been made. In this paper, we present novel assume-guarantee techniques for compositional verification of systems exhibiting both probabilistic and nondeterministic behaviour, and illustrate their applicability and efficiency on several large case studies. This is the first approach that, given appropriate assumptions about components, can perform compositional verification in an efficient and fully-automated manner.

We use *probabilistic automata* (PAs) [8,9], a well-studied formalism that is naturally suited to modelling multi-component probabilistic systems. We also augment PAs with *rewards* (or, dually, *costs*), which can be used to model a variety of quantitative measures of system behaviour, such as execution time or power consumption. We present compositional techniques for verification of a range of *quantitative* properties, including probabilistic ω-regular properties (which subsume, for example, probabilistic LTL and probabilistic safety properties) and expected total reward/cost properties (which can also encode the expected reward/cost to reach a target and time-bounded reward measures).

Probabilistic automata were developed as a formalism for the modelling and analysis of distributed, randomised systems [8], and a rich underlying theory has been developed, in particular for models in which PAs are combined through parallel composition. A variety of elegant proof techniques have been created and used to manually prove the correctness of large, complex randomised algorithms [10]. Key ingredients of the underlying theory of PAs include probabilistic versions of strong and weak (bi)simulation [9] and trace distribution inclusion [8]. The branching-time preorders (simulation and bisimulation) have been shown to be compositional [9] (i.e., preserved under parallel composition), but are often too fine to give significant practical advantages for compositional verification. Trace distribution inclusion, which is defined in terms of probability distributions over sequences of observable actions, is a natural generalisation of the (non-probabilistic) notion of trace inclusion but is known *not* to be preserved under parallel composition [11]. Thus, other proposals for compositional verification frameworks based on PAs tend to restrict the forms of parallel composition that are allowed [12,13]. By contrast, the approach we present in this paper does not impose restrictions on the parallel composition permitted between components, allowing greater flexibility to model complex systems.

Our assume-guarantee framework uses *multi-objective* probabilistic model checking [14,15], which is a technique for verifying multiple, possibly conflicting properties of a probabilistic automaton. Conventional verification techniques for PAs quantify over its *adversaries*, which represent the various different ways in which nondeterminism in the model can be resolved. A typical property to be verified states, for example, "the probability of a system failure is at most 0.01, *for any possible adversary*". Multi-objective model checking, on the other hand, permits reasoning about the existence of an adversary satisfying two or more distinct properties, for example, "is there an adversary under which the probability of a system failure is at most 0.005 and the expected battery lifetime remains below 2 hours?".

Our compositional approach to verification is based on queries of the form $\langle \Psi_A \rangle \mathcal{M} \langle \Psi_G \rangle$, with the meaning "under any adversary of PA $\mathcal{M}$ for which assumption Ψ_A is satisfied, Ψ_G is guaranteed to hold". The assumptions Ψ_A and guarantees Ψ_G are *quantitative multi-objective properties* [15], which are conjunctions of predicates, each of which imposes a bound on either the probability of an ω-regular property or the expected total value of some reward structure. A simple example of an assumption is "with probability 1, component $\mathcal{M}_1$ eventually sends a request, and the expected time before this occurs is at most 5 seconds". We show that checking these assume-guarantee queries can be reduced to existing multi-objective model checking techniques [14,15], which can be implemented efficiently using linear programming.

Building upon this notion of probabilistic assume-guarantee reasoning, we formulate and prove several compositional proof rules, which can be used to decompose the process of verifying a multi-component probabilistic system into several smaller sub-tasks. One important class of such proof rules is those that restrict assumptions and guarantees to be *probabilistic safety properties*, which impose a bound on the probability of satisfying a regular safety property. These are slightly cheaper to verify than the other properties we consider, but still represent a useful set of system properties. In order to present proof rules for the more general class of quantitative properties (probabilistic ω-regular and expected total reward), we incorporate a notion of *fairness*, restricting our analysis to cases where each component in a system executes a step infinitely often.

For both of these classes of properties, we present several different assume-guarantee proof rules, including variants that are asymmetric (using assumptions only about one component) and circular (assumptions about all components). We also give proof rules for systems with components that are asynchronous and methods to decompose the analysis of reward-based properties. Finally, we describe how to obtain *numerical* results from compositional verification, in particular, obtaining lower and upper bounds on the actual probability that a system satisfies a property and constructing Pareto curves to investigate trade-offs between multiple system properties in a compositional fashion.

We have implemented our assume-guarantee verification techniques by extending the PRISM model checker [4], and present experimental results from its application to several large case studies. We demonstrate significant speed-ups over conventional, non-compositional verification, and also successfully verify models that are too large to be analysed without compositional techniques.