ANALYSIS AND VERIFICATION OF STOCHASTIC HYBRID SYSTEMS

NANKYA PHIONA

April 19, 2017

1 Abstract

In this paper we propose a testing based method for safety/ reachability analysis of stochastic hybrid systems. Testing based methods are characterized by analysis based on the execution traces of the system or the simulation thereof. Testing based method is very appealing because of the simplicity of its execution, the possibility of having a partial verification and its highly parallel structure.

2 Introduction

Hybrid systems are systems containing both physical components which evolve continuously over time, as well as discrete components which can influence the continuous dynamics. Also cyber-physical systems can be seen as hybrid systems, where communication between distributed components plays a further important role. As hybrid systems are often safety critical, in the last two decades much effort was put into the development of efficient algorithms and powerful tools to support their safety analysis. Whereas there is a deep-rooted research for pure continuous and for pure discrete systems, their hybrid combination requires novel methodologies and the adaptation, integration and extension of previous results. Nowadays, a number of analysis tools to verify hybrid systems are available, such as Ariadne [13], Cora [1], dReach [26], Flow* [12], HSolver [36], HyCreate[25], iSAT-ODE [15], KeYmaera [32] and SpaceEx [20].

3 Background to the Problem

As safety verification and reachability analysis of hybrid systems become more complicated, new formal verification concepts are needed. Testing based verification has emerged as an alternative way to perform such task [1]. By testing based verification, we mean the analysis methods that are based on the execution traces of the system or the simulation thereof. Each test run is characterized by a test parameter. Testing based verification is very appealing because of several

reasons. The first reason is its simplicity. Running or simulating the execution traces of a system is generally much simpler than performing symbolic analysis on it. This is particularly true for systems with complex dynamics. The second reason is that when coupled with an appropriate notion of coverage, testing can lead to partial verification. It is generally known that when a to-be-verified system does not robustly satisfy the desired property, the complexity of its full verification becomes prohibitively high. Testing based safety verification can, for example, provide a safety guarantee for a subset of the initial conditions that is robustly safe after only executing a few runs.

4 Problem Statement

The construction and analysis of models suited for performance and reliability studies of real-world phenomena is a difficult task. To a large extent this problem is attacked using human intelligence and experience. Due to increasing size and complexity of systems, this tendency seems even growing: performance as well as reliability modeling becomes a task dedicated to specialists, in particular for systems exhibiting a high degree of irregularity. Traditional performance models such as queuing networks lack hierarchical composition and abstraction means, significantly hampering the modeling of systems that are developed nowadays.

5 Solution

Those above problems can be solved by using the efficient algorithms that were developed, by analyzing the problem and build its algorithm and verifying them.

6 Objectives

6.1 Main Objective

Describing current analysis techniques, available tools and their individual properties, Providing exemplary evaluation of a few tools on some benchmarks, and discussing general problems related to tool evaluation and comparison.

6.2 Other Objective

Collecting some important challenges for future research in this area.

7 Methodology

7.1 Analysis techniques.

In practise, three fundamentally different techniques are used to analyse stochastic models. They differ with respect to accuracy, applicability and computa-

tional requirements. 1. Simulation. The stochastic model is mimicked by a simulator throwing dice and producing statistics of simulated time spent in states. The fraction of simulated time spent in a particular state is used as an estimate for the state probability. This technique is generally applicable, in particular it is suitable also for non-Markov stochastic models. However, it should be noticed that good accuracy tends to require long simulation runs, and hence limits applicability in practise: To increase the accuracy of the simulation by a factor of n, one needs to increase the length of the simulation runs (and hence the run-time of the simulation) by a factor of n2.

2.Numerical solution. The transient or steady-state behavior of a stochastic model is obtained by an exact or approximate numerical algorithm where model parameters are instantiated with numerical values. This approach gives accurate results in general, up to numerical precision. Typically the solution time increases logarithmically with an increase in accuracy. On the other hand, its applicability is restricted to finite Markov chains (with a few exceptions, see e.g. [22, 32]). Furthermore the number of states of the model is a limiting factor, because of computational and especially storage requirements. A very readable textbook on numerical solution methods is [41].

3.Analytical solution. The transient or steady state property of interest is expressed as a closed formula over the parameters of the model. This is the most simple, accurate and elegant technique. However, analytical solutions are available only for highly restricted classes of stochastic models.

7.2 Verification:

There are vast of tools we can use for verification and some of them are as follows; 1.Ariadne is a software package implementing functionalities for the reachability analysis of hybrid systems. The package is based on the theory of computable analysis and on a rigorous function calculus with provable approximation bounds on the computations. Ariadnecan handle expressive models with non-linear differential equations, where state sets can be represented by Taylor models or grid pavings. Besides others, interval arithmetic along with interval solvers and propagation mechanisms are applied in the computations. The support for parallel composition and assume-guarantee reasoning improve scalability.

2.Cora [1] is an object-oriented Matlab toolbox which can be used for the fast implementation of different reachability analysis algorithms for continuous and hybrid systems. It implements different state set representation types, conversion algorithms between them, and operations needed for reachability analysis. Additionally to well-known representations such as boxes, polytopes and zonotopes, it provides also non-convex representations (polynomial zonotopes) and representations dedicated to stochastic verification (probabilistic zonotopes). Coracan be used for the analysis of systems with linear, linear stochastic and non-linear dynamics with uncertain parameters, where non-linear systems are abstracted by linear or polynomial systems.

8 Outcomes

To Increase applicability and scalability in Standardization, competitions, and the strengthening of the functionality and the efficiency of analysis techniques and to ensure that verification tools may increase visibility and intensify the developments in this relevant research area.

9 References

1. Althoff, M., Dolan, J.M.: Online verification of automated road vehicles using reachability analysis. IEEE Trans. Robot. 30(4), 903918 (2014)

13. Collins, P., Bresolin, D., Geretti, L., Villa, T.: Computing the evolution of hybrid systems using rigorous function calculus. In: Proceedings of ADHS 2012, pp. 284290. IFAC-PapersOnLine (201