ANALYSIS AND VERIFICATION OF STOCHASTIC HYBRID SYSTEMS

NANGWALE JOSHUA,WACA DAVID, NANYA PHIONA,GIMBO IMELDA THRESA

April 20, 2017

1 Abstract

Stochastic hybrid system (SHS) models can be used to analyze and design complex embedded systems that operate in the presence of uncertainty and variability. Verification of reachability properties for such systems is a critical problem. Developing sound computational methods for verification is challenging because of the interaction between the discrete and the continuous stochastic dynamics. In this paper, we propose a probabilistic method for verification of SHSs based on discrete approximations focusing on reachability and safety problems. We show that reachability and safety can be characterized as a viscosity solution of a system of coupled Hamilton-Jacobi-Bellman equations. We present a numerical algorithm for computing the solution based on discrete approximations that are derived using finite-difference methods. An advantage of the method is that the solution converges to the one for the original system as the discretization becomes finer. We also prove that the algorithm is polynomial in the number of states of the discrete approximation. Finally, we illustrate the approach with two benchmarks: a navigation and a room heater example, which have been proposed for hybrid system verification.

2 Introduction

Hybrid systems are systems containing both physical components which evolve continuously with time as well as discrete components that influence the continuous dynamics. Uncertainty and randomness are however inherent in most practical systems. Stochastic Hybrid Systems are models which take into account the probabilistic evolution of systems. SHS models can be used to analyse and design complex embedded systems that operate in the presence of uncertainty and variability.According to [**?**] a Stochastic Hybrid System (or automata) is defined as

$$H = ((Q, d, X), b, \sigma, Init, \lambda, R)$$

where

- Q is a set of discrete states (modes),
- $d : Q \rightarrow \mathrm{N}$ is a map that defines the continuous state space dimension for each $q \subseteq Q$,
- $X : Q \rightarrow R^{d(.)}$ is a map that describes the invariant for each $q \in Q$ as an open set $X^q \subseteq R^{d(q)}$,
- $b : Q \times X^q \rightarrow R^{d(q)}$ and $\sigma : Q \times X^q \rightarrow R^{d(q)*p}$ are driftvectors and dispersion matrices respectively,
- $Init : B(S) \rightarrow [0; 1]$ is an initial probability measure on S,
- $\lambda : \bar{S} \rightarrow R_+$is a nonnegative transition rate function, and
- $R : \bar{S} \times B(\bar{S}) \rightarrow [0; 1]$ is a transition measure.

The reachability problem of an automaton refers to the problem of deciding whether a given set of states is reachable. More formally, given a target set and an unsafe set of states, the objective of the reachability problem is to compute the probability that the system execution from an arbitrary initial state will reach the target set while avoiding the unsafe set. Reachability analysis of SHS is important because it provides a formal framework to analyse complex systems. However, developing computational methods for verification of reachability is somewhat challenging because of the interaction of discrete and continuous stochastic dynamics. In a safety problem, given a set of states, compute the probability that system execution from an initially safe state will lead to an unsafe set.

3 Objective

To investigate and describe the analysis and verification techniques that are applied in Stochastic Hybrid Systems.

4 Problem statement

Stochastic Hybrid Systems incorporate complex dynamics, uncertainty, multiple modes of operation and support high level control specification. Verification of reachability of SHS aims at determining the probability that the system will reach a set of desirable or unsafe states.

5 Methodology

5.1 Over-approximation techniques

In over approximation verification techniques, each step of the algorithm produces an over approximation of the forward or backward reachable set. If the

reachable set is found to be unsafe, the verification variables and approximations are tightened. Therefore multiple iterations are necessary to verify the system. There is however no guarantee that a solution will be found.

5.2 Convergent approximation techniques

Convergent approximation techniques solve the verification problem by approximating the hybrid system with another model of computation for which there exists well understood verification methods. The state space is made discrete and the user is allowed to the state the level of approximation. A benefit of convergent methods is they dont restrict the reachable set.

6 Outcome

To show that reachability of a Stochastic Hybrid System can be represented by a measurable function that is interpreted as the probability that an initial state can reach a target set while avoiding an unsafe set.

7 Research Scope

The system is limited to science and engineering. In a number of practical instances the presence of a discrete number of continuously operating modes (e.g., in fault-tolerant industrial systems), the effect of uncertainty (e.g., in safety-critical air-traffic systems), or both occurrences (e.g., in models of biological entities) advocate the use of a mathematical framework, such as that of SHS, which is structurally predisposed to model such heterogeneous systems.

8 References

[1] Xenofon Koutsoukos and Derek Riley. Computational methods for veri ca- tion of stochastic hybrid systems. IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, 38(2):385396, March 2008.

[2] Alur, R., Courcoubetis, C., Halbwachs, N., Henzinger, T.A., Ho, P.H., Nicollin, X., Olivero, A., Sifakis, J., Yovine, S.: The algorithmic analysis of hybrid systems. Theor. Comput. Sci. 138(1), 334 (1995