ANALYSIS AND VERIFICATION OF STOCHASTIC HYBRID SYSTEMS

NANGWALE JOSHUA

April 15, 2017

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

2 Objective

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

3 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.

4 Methodology

4.1 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.

4.2 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.

5 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.