Application of SMT Solvers to Hybrid System Verification

Alessandro Cimatti

Fondazione Bruno Kessler, Trento, Italy

Abstract

Hybrid automata are a widely used framework to model complex critical systems, where continuous physical dynamics are combined with discrete transitions. Application areas include automotive, railway, aerospace, and industrial production.

The expressive power of Satisfiability Modulo Theories (SMT) solvers can be used to symbolically model networks of hybrid automata, using formulas in the theory of reals.

In this tutorial, we survey state-of-the-art SMT-based verification for hybrid systems.

We show how SAT-based techniques such as bounded model checking, k-induction, predicate abstraction, and IC3, can be naturally lifted to the SMT case. The expressive power of the SMT framework allows us to exploit a local time semantics, where the timescales of the automata in the network are synchronized upon shared events. The approach fully leverages the advanced features of modern SMT solvers, such as incrementality, unsatisfiable core extraction, and interpolation.

We then concentrate on the problem of scenario-based verification, i.e. checking if a network of hybrid automata accepts some desired interactions among the components, expressed as Message Sequence Charts (MSCs).

We conclude by investigating the problem of requirements analysis for hybrid systems.

978-0-9835678-2-0/12/$31.00