SAT with differential equations

Tomáš Kolárik
Faculty of Information Technology, Czech Technical University in Prague
Thákurova 9, 160 00 Praha 6, Czech republic

tomaqa@gmail.com

Keywords. SAT, SMT (Satisfiability Modulo Theories), SMT-LIB, numerical methods for ODEs (ordinary differential equations), formal verification, embedded systems, hybrid systems model analysis.

Abstract

Many nowadays systems, namely embedded, are insisted to satisfy high specification requirements, which often depend on physical features of real world. Formal verification showed to be convenient method to guarantee specifications fulfillment in complex systems.

Formal verification checks mathematical model of a system exactly; one of used approaches is e.g. SAT. Problem arises when one needs to use another means of modelling—differential equations (ODEs), which describe physical features natively.

Goal of this paper is to prove a concept which combines SAT with ODEs and can be used e.g. to formally verify models of embedded systems. Such solvers already exist (e.g. dReal), but their usage in industry is limited due to their preference of accuracy over speed in ODEs. The objective was to apply classic numerical methods for solving ODEs, which are less accurate, but faster.

This work includes prototype implementation named SOS (SMT+ODE Solver), which combines SMT (extension of SAT) with ODEs. SMT and ODE solvers are both independent of rest components. Used solvers are odeint and from SMT solvers CVC4 and z3.

The major observations are that using classic numerical methods fastens overall computation, and that computation time of tasks with precise initial values (initial value problem, IVP) is much smaller than at tasks with intervals (IIVP). And intervals can be effectively approximated by value enumerations in logical sum. These observations approve our chosen concept and were verified in some examples, where our procedure was faster than in current solver dReal.

Thus the goal of a more appropriate method for industry needs, in the field of formal verification with ODEs, has been reached. This work is assumed to serve as a source of inspiration to industry tools' designers. Or, it can be developing and improving henceforth inside the current open-source project.

Acknowledgment

Thesis supervisor: doc. Dipl.-Ing. Dr. techn. Stefan Ratschan.