Model Checking Hybrid Systems
(Invited Talk)

Edmund M. Clarke and Sicun Gao

Carnegie Mellon University

Abstract. We present the framework of delta-complete analysis for bounded reachability problems of hybrid systems. We perform bounded reachability checking through solving delta-decision problems over the reals. The techniques take into account of robustness properties of the systems under numerical perturbations. Our implementation of the techniques scales well on several highly nonlinear hybrid system models that arise in biomedical applications.

1 Introduction

Formal verification is difficult for hybrid systems with nonlinear dynamics and complex discrete controls [1,7]. A major difficulty of applying advanced verification techniques in this domain comes from the need of solving logic formulas over the real numbers with nonlinear functions, which is notoriously hard.

Recently, we have defined the *δ-decision problem* that is much easier to solve [3,2]. Given an arbitrary positive rational number δ, the δ-decision problem asks if a logic formula is false or *δ-true* (or, dually, true or *δ-false*). The latter answer can be given, if the formula *would be true* under δ-bounded numerical changes on its syntactic form [3]. The δ-decision problem is decidable for bounded first-order sentences over the real numbers with arbitrary Type 2 computable functions. Type 2 computable functions [8] are essentially real functions that can be approximated numerically. They cover almost all functions that can occur in realistic hybrid systems, such as polynomials, trigonometric functions, and solutions of Lipschitz-continuous ODEs. We can now develop a new framework for solving bounded reachability problems for hybrid systems based on solving δ-decisions. We show that this framework makes bounded reachability of hybrid systems much more tractable. Moreoever, our practical implementation can handle highly nonlinear hybrid systems.

The framework of *δ-complete analysis* consists of techniques that perform verification and allow bounded errors on the safe side. For bounded reachability problems, δ-complete analysis aims to find one of the following answers:

- safe (bounded): The system does not violate the safety property within a bounded period of time and a bounded number of discrete mode changes.
- δ-unsafe: The system would violate the safety property under some δ-bounded numerical perturbations.

T. Margaria and B. Steffen (Eds.): ISoLA 2014, Part II, LNCS 8803, pp. 385–386, 2014.

Thus, when the answer is safe, no error is involved. On the other hand, a system that is δ-unsafe would violate the safety property under bounded numerical perturbations. Realistic hybrid systems interact with the physical world and it is impossible to avoid slight perturbations. Thus, δ-unsafe systems should indeed be regarded as unsafe, under reasonable choices of δ. Note that such robustness problems can not be discovered by solving the precise decision problem, and the use of δ-decisions strengthens the verification results.

δ-Complete reachability analysis reduces verification problems to δ-decision problems of formulas over the reals. It follows from δ-decidability of these formulas [3] that δ-complete reachability analysis of a wide range of nonlinear hybrid systems is decidable. Such results stand in sharp contrast to the standard high undecidability of bounded reachability for simple hybrid systems.

We emphasize that the new framework is immediately practical. We implemented the techniques in our open-source tool dReach based on our nonlinear SMT solver dReal [4]. In our previous work, we have shown the underlying solver scales on nonlinear systems [5]. The tool has successfully verified safety properties of various nonlinear models that are beyond the scope of existing tools, such as the cardiac cells model as studied in [6].

References

1. Alur, R.: Formal verification of hybrid systems. In: EMSOFT, pp. 273–278 (2011)
2. Gao, S., Avigad, J., Clarke, E.M.: Delta-complete decision procedures for satisfiability over the reals. In: Proceedings of the 6th International Joint Conference on Automated Reasoning (IJCAR), pp. 286–300 (2012)
3. Gao, S., Avigad, J., Clarke, E.M.: Delta-decidability over the reals. In: Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), pp. 305–314 (2012)
4. Gao, S., Kong, S., Clarke, E.M.: dReal: An SMT solver for nonlinear theories over the reals. In: Bonacina, M.P. (ed.) CADE 2013. LNCS (LNAI), vol. 7898, pp. 208–214. Springer, Heidelberg (2013)
5. Gao, S., Kong, S., Clarke, E.M.: Satisfiability modulo ODEs. In: Proceedings of the 13th International Conference on Formal Methods in Computer Aided Design, FMCAD (2013)
6. Grosu, R., Batt, G., Fenton, F.H., Glimm, J., Le Guernic, C., Smolka, S.A., Bartocci, E.: From cardiac cells to genetic regulatory networks. In: Gopalakrishnan, G., Qadeer, S. (eds.) CAV 2011. LNCS, vol. 6806, pp. 396–411. Springer, Heidelberg (2011)
7. Henzinger, T.A.: The theory of hybrid automata. In: LICS, pp. 278–292 (1996)
8. Weihrauch, K.: Computable Analysis: An Introduction (2000)