Hybrid dynamical systems: verification and error trajectory search

Ratschan, Stefan
2010

Ratschan, Stefan. Hybrid dynamical systems: verification and error trajectory search. In Seminar on Numerical Analysis. Modelling and Simulation of Challenging Engineering Problems. Prague : Institute of Computer Science AS CR, 2010, S. 125-126. ISBN 978-80-87136-07-2. [SNA '10. Seminar on Numerical Analysis, Nové Hrady, 18.01.2010-22.01.2010, CZ].

Hybrid dynamical systems: verification and error trajectory search

S. Ratschan

Institute of Computer Science
Academy of Sciences of the Czech Republic

Modern complex technical systems usually consist not only of physical components, but also of computer equipment interacting with these physical components. As a consequence, such systems cannot be modeled based on physical laws formulated in the language of continuous mathematics alone. In addition, one needs discrete modeling formalisms. Hybrid (dynamical) systems are a formalism for modeling the resulting combined continuous-discrete behavior. In the talk we will describe this formalism, and discuss algorithms for the automatic analysis of such hybrid systems.

When restricted to their continuous part, such hybrid systems amount to ordinary differential equations, when restricted to their discrete part, to finite state machines. However, the interaction between those two parts introduces significant additional difficulty that obstructs the use of classical numerical error analysis. Moreover, such systems are usually non-deterministic, in the sense that they not only have a single initial state, but a whole set of initial stats, and in the sense that starting from a given unique state, they may allow an uncountable set of trajectories (e.g., resulting from differential inequalities). A further difficulty results from the fact that one is often interested in analyzing the behavior of hybrid systems over an unbounded time horizon.

As a consequence, more or less all problems of analyzing hybrid systems are undecidable [4], although one can get much further with a weaker notion of quasi-decidability [3, 1, 5].

In the talk we will discuss discuss algorithms for proving that a given hybrid system does not reach an element of a set of states considered to be unsafe (in whatever unbounded time) [6, 2]. Moreover, we will discuss the use of optimization techniques to find trajectories the violate this property [7].

Acknowledgement: This work has been supported by GAČR grant 201/08/J020 and by the institutional research plan AV0Z100300504.

References

[1] W. Damm, G. Pinto, and S. Ratschan. Guaranteed termination in the verification of LTL properties of non-linear robust discrete time hybrid systems. *International Journal of Foundations of Computer Science (IJFCS)*, 18(1):63–86, 2007.

[2] T. Dzetkulič and S. Ratschan. How to capture hybrid systems evolution into slices of parallel hyperplanes. In *ADHS'09: 3rd IFAC Conference on Analysis and Design of Hybrid Systems*, pages 274–279, 2009.

[3] M. Fränzle. Analysis of hybrid systems: An ounce of realism can save an infinity of states. In J. Flum and M. Rodriguez-Artalejo, editors, *Computer Science Logic (CSL'99)*, number 1683 in LNCS. Springer, 1999.

[4] T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya. What's decidable about hybrid automata. *Journal of Computer and System Sciences*, 57:94–124, 1998.

[5] S. Ratschan. Safety verification of non-linear hybrid systems is quasi-decidable. 2009. submitted.

[6] S. Ratschan and Z. She. Safety verification of hybrid systems by constraint propagation based abstraction refinement. *ACM Transactions in Embedded Computing Systems*, 6(1), 2007.

[7] S. Ratschan and J.-G. Smaus. Finding errors of hybrid systems by optimising an abstraction-based quality estimate. In C. Dubois, editor, *Tests and Proofs*, volume 5668 of *LNCS*, pages 153–168. Springer, 2009.