An Algorithm for Formal Safety Verification of Complex Heterogeneous Systems

Stefan Ratschan

Institute of Computer Science, Academy of Sciences of the Czech Republic
182 07 Praha 8, Czech Republic
stefan.ratschan@cs.cas.cz

Keywords: *Hybrid dynamical systems; formal verification; software verification; complex systems*

Abstract

Modern technical systems more and more consist of a tight integration of computational devices into physical surroundings. For example, in modern cars, a large part of the development cost goes into software and digital electronics. Moreover, the complexity of such systems is growing rapidly. Hence it is of utmost importance to come up with formalisms for modeling, and algorithms for analyzing such systems.

The notion of a hybrid dynamical system is a current approach for modeling computation in physical surroundings, see Lunze and Lamnabhi-Lagarrigue [2009]. Such systems integrate ordinary differential equations with finite state machines, based on a state space that is the Cartesian product of $\mathbb{R}^n$ and a set of finitely many states. Uncertainty is usually included by also allowing differential inequalities, or by allowing uncertain parameters in the differential equations. However, finite state machines do not suffice for modeling software of the complexity occurring in modern technical systems.

In our work, we will present an extension of the hybrid system model to systems that are parametric in k data types, with k an arbitrary, but fixed, positive integer. Those data types are generic in the sense that they can be chosen arbitrarily as long as they fulfill certain conditions that are met by the most widely-used data types such as integers, arrays, and lists. The state space of the new model is formed by the Cartesian product of $\mathbb{R}^n$ and the used data types. Again, the dynamics of the continuous part of the states space is given by ordinary differential equations (or inequalities).

Moreover, we provide an algorithm for the formal safety verification of such systems (i.e., the automatic verification that the system state always stays in a certain set of states considered to be safe) based on certain operations that the basic data types are required to provide. The algorithms is an extension of our earlier algorithm for hybrid systems verification, see Dzetkulič and Ratschan [2011].

References

Tomáš Dzetkulič and Stefan Ratschan. Incremental computation of succinct abstractions for hybrid systems. In *FORMATS 2011*, volume 6919 of *LNCS*, pages 271–285. Springer, Heidelberg (2011), 2011.

Jan Lunze and Françoise Lamnabhi-Lagarrigue, editors. *Handbook of Hybrid Systems Control*. Cambridge University Press, 2009.