Models, Over-approximations and Robustness

Eugenio Moggi, Genova Univ.

Abstract

Hybrid systems, and related formalisms, have been successfully used to model Cyber-Physical Systems. However, mathematical models are always a simplification of the system they are meant to describe, and one must be aware of this mismatch, when using these models for system analyses. In safety analysis it is acceptable to use over-approximations of the system behavior, indeed they are the bread and butter of counterexample guided abstraction refinement (CEGAR). We propose a notion of system behavior robust wrt arbitrary small over-approximations, and argue that it is particularly appropriate for safety analysis.

For a transition system (TS), ie a binary relation $\rightarrow$ on a set of states, reachability is well-understood and clearly defined, namely the reflexive and transitive closure of $\rightarrow$. Reachability plays an important role in computer-assisted verification and analysis [1], since **safety** is usually formalized in terms of **reachability**.
For finite state TS reachability is decidable. For TS with a countable *discrete* state space (eg the rewriting relation for a term rewriting system), reachability could be undecidable (even when the transition relation is decidable).
For hybrid systems (HS), where state spaces are uncountable and *continuous* (eg $\mathbb{R}^n$), even the definition of reachability becomes an issue! For instance, in HS with *Zeno behaviors* (where infinitely many discrete jumps may occur in finite time) the transitive and reflexive closure (of suitable transition relation) may fail to include some states reachable in finite time. Zeno behaviors arise naturally when modeling rigid body dynamics with impacts.

Contributions. The first contribution is the notion of **safe reachability**, which gives an over-approximation of the states reachable in finite time, even for Zeno HS. Models are always *simplifications* of *real systems*, and abstractions are *artifacts of modeling* that are essential in managing complexity. For safety analysis the use of over-approximations is acceptable, since it can only lead to false negatives, ie wrongly conclude that the system is unsafe.
Safe reachability is a map on a complete lattice, which is always monotonic, but may fail to be *Scott continuous*.
The second contribution is a way to get the **best Scott continuous approximation** of a monotonic map between complete lattices. Applying this construction to safe reachability results in another over-approximation, that may have more false negatives, but forcing Scott continuity ensures that the over-approximation is *robust* wrt perturbations of the initial states (and also of the HS).
In safety analysis robust over-approximations are important, because in modeling, observing and building physical systems inaccuracies are unavoidable: a mathematical model is always a simplification of the real system, and a physical measurement is always affected by errors.

Related Work. From [5] we borrow from the definition of hybrid system; from [3] we take the notion of topological transition system (TTS), the natural setting for defining safe reachability; from [4] we take the continuous lattices for enforcing robustness of reachability maps.
Reachability maps can be viewed as arrows in the category of complete lattices and monotonic maps, a standard setting for abstract interpretation [2]. To enforce continuity we move to the category of complete lattices and Scott continuous maps.

References

[1] R.Alur, C.Courcoubetis, N.Halbwachs, T.A.Henzinger, P-H.Ho, X.Nicollin, A.Olivero, J.Sifakis, and S.Yovine. The algorithmic analysis of hybrid systems. *Theoretical computer science*, 138(1):3–34, 1995.

[2] P.Cousot and R.Cousot. Abstract interpretation frameworks. *Journal of logic and computation*, 2(4):511–547, 1992.

[3] P.J.L. Cuijpers and M.A.Reniers. Topological (bi-) simulation. *Electronic Notes in Theoretical Computer Science*, 100:49–64, 2004.

[4] A.Edalat and D.Pattinson. Denotational semantics of hybrid automata. *The Journal of Logic and Algebraic Programming*, 73(1):3–21, 2007.

[5] R.Goebel, R.G.Sanfelice, and A.Teel. Hybrid dynamical systems. *Control Systems, IEEE*, 29(2):28–93, 2009.