Real Analysis for Complex Systems

André Platzer

Carnegie Mellon University
Pittsburgh, PA, USA

Formal verification techniques are used routinely in finite-state digital circuits. Theorem proving is also used successfully for infinite-state discrete systems. But many safety-critical computers are actually embedded in physical systems. Hybrid systems [1] model complex physical systems as dynamical systems with interacting discrete transitions and continuous evolutions along differential equations. They arise frequently in many application domains, including aviation, automotive, railway, and robotics. There is a well-understood theory for proving programs. But what about complex physical systems? How can we prove that a hybrid system works as expected, e.g., an aircraft does not crash into another one?

This talk illustrates the complexities and pitfalls of hybrid systems verification. It describes a theoretical and practical foundation for deductive verification of hybrid systems called differential dynamic logic ($\mathsf{d}\mathcal{L}$). The proof calculus for this logic is interesting from a theoretical perspective, because it is a complete axiomatization of hybrid systems relative to differential equations. The approach is of considerable practical interest too. Its implementation in the theorem prover KeYmaera[1] [7] has been used successfully to verify collision avoidance properties in the European Train Control System [8] and air traffic control systems [6]. The number of dimensions and nonlinearities in they hybrid dynamics of these systems is surprisingly tricky such that they are still out of scope for other verification tools.

This talk is based on recent work [2, 3, 4]. More comprehensive details can be found in a corresponding book [5].

References

[1] Thomas A. Henzinger. The theory of hybrid automata. In *LICS*, pages 278–292, Los Alamitos, 1996. IEEE Computer Society.

[2] André Platzer. Differential dynamic logic for verifying parametric hybrid systems. In Nicola Olivetti, editor, *TABLEAUX*, volume 4548 of *LNCS*, pages 216–232. Springer, 2007.

[3] André Platzer. Differential dynamic logic for hybrid systems. *Journal of Automated Reasoning*, 41(2):143–189, 2008.

[4] André Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *Journal of Logic and Computation*, 20(1):309–352, 2010. Advance Access published on November 18, 2008.

[5] André Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, Heidelberg, 2010.

[6] André Platzer and Edmund M. Clarke. Formal verification of curved flight collision avoidance maneuvers: A case study. In Ana Cavalcanti and Dennis Dams, editors, *FM*, volume 5850 of *LNCS*, pages 547–562. Springer, 2009.

[7] André Platzer and Jan-David Quesel. KeYmaera: A hybrid theorem prover for hybrid systems. In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *IJCAR*, volume 5195 of *LNCS*, pages 171–178. Springer, 2008.

[8] André Platzer and Jan-David Quesel. European train control system: A case study in formal verification. In Karin Breitman and Ana Cavalcanti, editors, *ICFEM*, volume 5885 of *LNCS*, pages 246–265. Springer, 2009.

[1] KeYmaera is available at `http://symbolaris.com/info/KeYmaera.html`