# Real Analysis for Complex Systems

Andre Platzer (CMU)

June 13, 2011

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 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. 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 has been used successfully to verify collision avoidance properties in the European Train Control System and air traffic control systems. The number of dimensions and nonlinearities in the hybrid dynamics of these systems is surprisingly tricky such that they are still out of scope for other verification tools.