Verification of Hybrid Systems with HSOLVER

Stefan Ratschan, Institute of Computer Science, Czech Academy of Sciences
Zhikun She, Beihang University, Beijing, China

Motivation

- Most computing devices appear in the form of embedded systems
- Here: computing device discrete, environment continuous
- Hence: hybrid dynamical systems (discrete automata + differential equations)
- Goal: use computer to automatical prove properties of hybrid systems

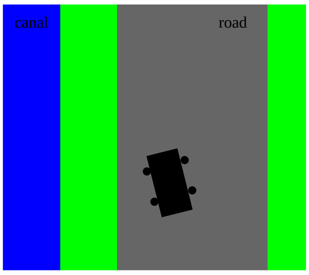
The Problem

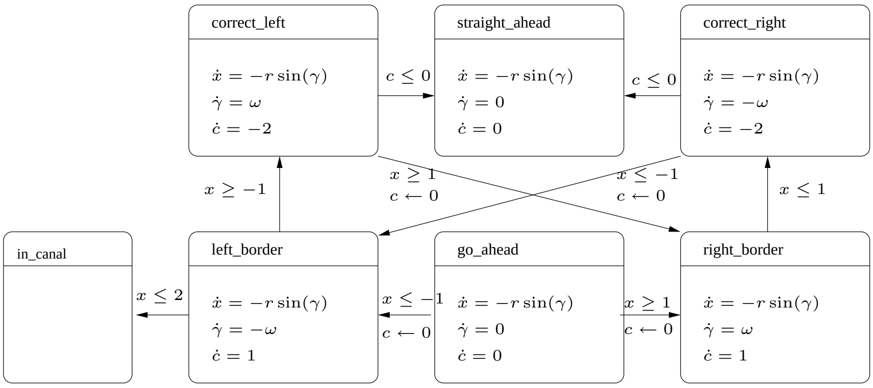
Given: Hybrid System

Verify:

- Safety: never reaches an unsafe state
- Progress: eventually reaches a desired state
- . . .

Car Steering Example (Clarke et al. 2003)





The Method

- abstraction refinement: construct finite overapproximation by partitioning continuous state space into finitely many pieces
- if overapproximation not safe/stable, refine using finer partitioning
- conditions for transitions between abstract states formulated as constraints in the first-order theory of the real numbers (overapproximating the differential equations)
- solve constraints using RSOLVER (using interval constraint propagation)

`http://hsolver.sourceforge.net`