Applications of Compositional and Distributed Verification to Automotive Challenge Problems

Sarah M. Loos, André Platzer, Ping Hou, David Renshaw, Ligia Nistor
Computer Science Department, Carnegie Mellon University, Pittsburgh, PA

Carnegie Mellon Electrical & Computer ENGINEERING
Carnegie Mellon SCHOOL OF COMPUTER SCIENCE

CMACS
NSF Expeditions in Computing

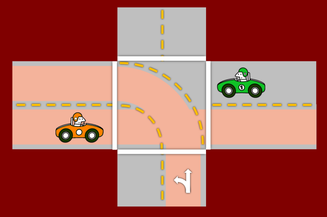
Overview

Issue: The major difficulties in the verification of advanced cyber-physical systems and biological systems are caused by scalability issues, nonlinearities in the system dynamics, and distribution mechanisms.

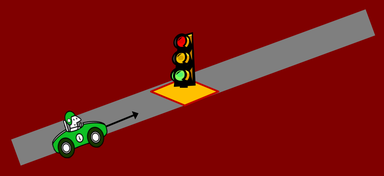
Objective: Develop compositional verification approaches for analyzing cyber-physical systems such as distributed hybrid systems. Verifying the system compositionally with hierarchical reasoning principles enables us to tackle systems which would be too big to handle otherwise.

Safe Intersections:
At the Crossing of Hybrid Systems and Verification

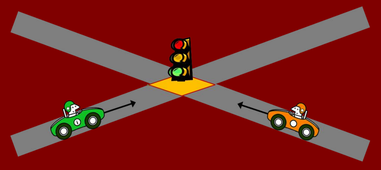
The Intersection Problem:



Real world intersection scenario



Single lane stoplight



X-Intersection

Modeling and Verification:

Cars can stop initially → [X-Intersection] No collision

discrete control / continuous dynamics

Initially safe → [((check if stoplight is red); (stoplight is green); $x' = v, v' = a)^*$] No collision

✔ **Verified semi-automatically in KeYmaera**

Challenges:

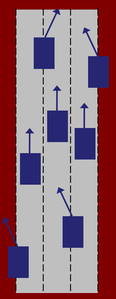
- Infinite, continuous, and evolving state space, $\mathbb{R}^\infty$
- Continuous dynamics
- Discrete control decisions
- Distributed dynamics
- Arbitrary number of cars, changing over time
- Emergent behaviors
- Simulation and testing only partially prove safety
- Large branching factor

Solutions:

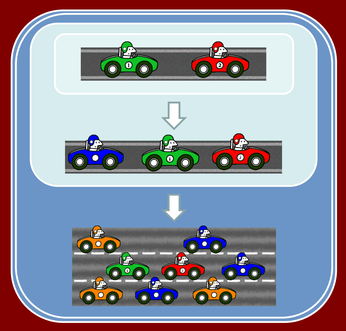
- Quantifiers for distributed dynamics and changing numbers of cars
- Compositionality – using small problems to solve the big ones
- Hierarchical and modular verification
- Verification for X-intersection with 2 cars
- Semi-automated verification
- Verification can handle high branching factor (9184 branches)

Adaptive Cruise Control:
Hybrid, Distributed, and Now Formally Verified

The Distributed Car Control Problem:

Local Lane Control	Global Lane Control	Local Highway Control	Global Highway Control
			
2 vehicles 1 lane No lane change	n vehicles 1 lane No lane change	n vehicles 1 lane lane changes	n vehicles m lanes lane changes

Hierarchical Modularity



Modeling and Verification:

discrete control / continuous dynamics

$(x_f < x_l) \rightarrow [(\text{ctrl};\text{dyn})^*]\ (x_f < x_l)$

✔ **Verified semi-automatically in KeYmaera**

discrete control / continuous dynamics

$(x_f < x_l) \rightarrow [((\text{if } Safe_\varepsilon, \text{set } a \in [-B, A]);\ (\text{otherwise set } a \in [-B, -b]);\ x' = v, v' = a)^*]\ (x_f < x_l)$

Street-Level Verification