SRI International

Verifying Components While Guaranteeing Compositionality

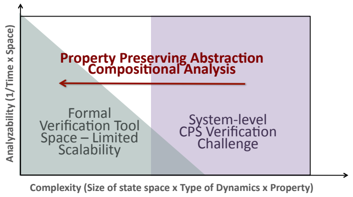
Abstraction-Based Tool and Method Tackles Complexity of CPS Verification

SRI International, Menlo Park, California

CPS Verification: Need and Challenge

- Simulation of CPS with complex dynamics can yield misleading results and does not provide proofs
- Verification tools cannot handle differential equations of CPS dynamics

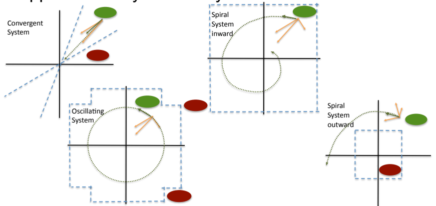
Solution: Abstraction and Compositionality


Analyzability (1/Time x Space)
Property Preserving Abstraction
Compositional Analysis
Formal Verification Tool Space – Limited Scalability
System-level CPS Verification Challenge
Complexity (Size of state space x Type of Dynamics x Property)

Qualitative Abstraction	Relational Abstraction
• Abstracts state space • E.g., dynamics abstracted to increasing/decreasing or positive/negative	• Abstracts transition relation • E.g., dynamics abstracted to increasing/decreasing at certain rate or amount of pos/neg

Relational Abstraction

- Applies to all dynamical systems

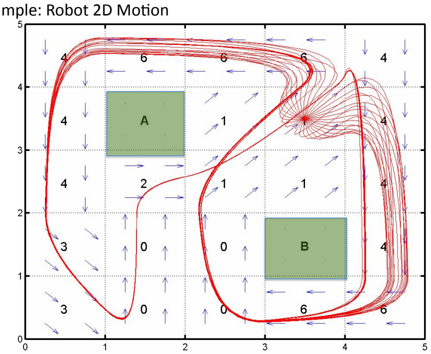


- Effective relational abstractions can be automatically computed for several system dynamics classes

Class	$d\vec{x} / dt$	Relational Abstraction
Timed Systems	$\dot{x} = 1, \dot{y} = 1$	$x' - x = y' - y$
Multirate Systems	$\dot{x} = 2, \dot{y} = 3$	$\frac{x' - x}{2} = \frac{y' - y}{3}$
Linear Hybrid Systems	$\dot{\vec{x}} = A\vec{x}$	$0 \le p' \le p \vee 0 \ge p' \ge p, p = \vec{c}^T \vec{x}$, $\vec{c}$ Eigenvector of A^T corr. to neg. eigenval

Demonstrated Verification on Several Hybrid System Benchmarks

Example: Robot 2D Motion

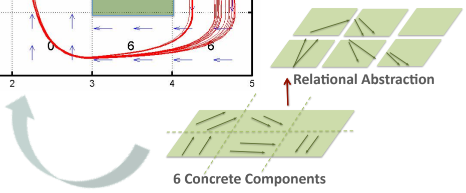


- Does robot stay clear of A and B?
- System dynamics:

$$\dot{\vec{x}} = \vec{v}$$
$$\vec{v} = A(\vec{v} - \vec{v}_d)$$

- The direction $\vec{v}_d$ depends on the position in the grid.
- Rel. Abstraction tool verifies instances in minutes

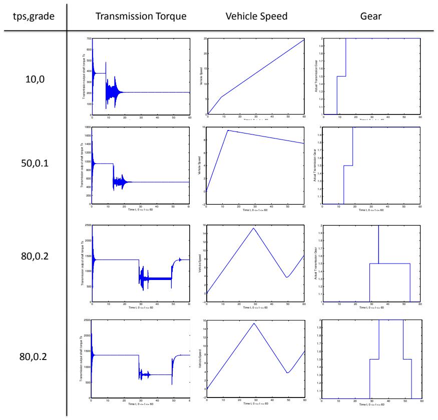
From [Ansgar and Ivancic, 2004]



Rel. Abs. done for each mode/component, each corresponding to open system

Verification results hold for composed system

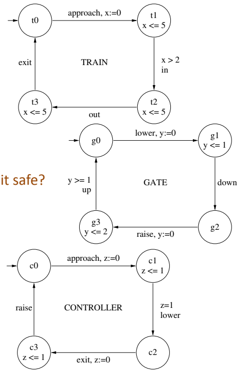
Example: Vehicle Powertrain



- Does there exist "second-to-first-to-second" gear transition?

Example: Train Gate Controller

- Is it safe?

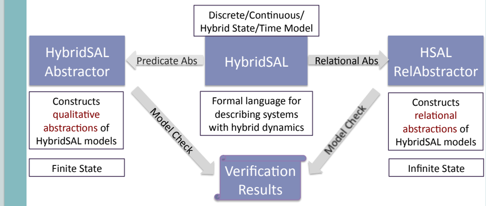


From [Dutertre and Sorea, 2004]

Approach

- Relational Abstraction is an over-approximation of the transitive closure of the transition relation
- Useful for proving safety properties and establishing conservative safety bounds

Automated Verification Tool


Discrete/Continuous/ Hybrid State/Time Model
HybridSAL Abstractor
Predicate Abs
HybridSAL
Relational Abs
HSAL RelAbstractor
Constructs qualitative abstractions of HybridSAL models
Formal language for describing systems with hybrid dynamics
Constructs relational abstractions of HybridSAL models
Model Check
Model Check
Finite State
Verification Results
Infinite State

The results produced by abstraction techniques enable compositional verification when components are put together to build systems

Other Work: Few automated tools for verifying systems with mixed discrete/continuous dynamics, and none are compositional

Benefits

- Enables analyzability of complex systems
- On Hybrid System benchmarks, verification time reduces from 10 hours to few minutes (100x improvement)

Feature

- Compositional analysis handles open components with hybrid dynamics

Best of Breed

- Approach compatible with other abstraction and model-checking techniques

Contact: Ashish.Tiwari@sri.com