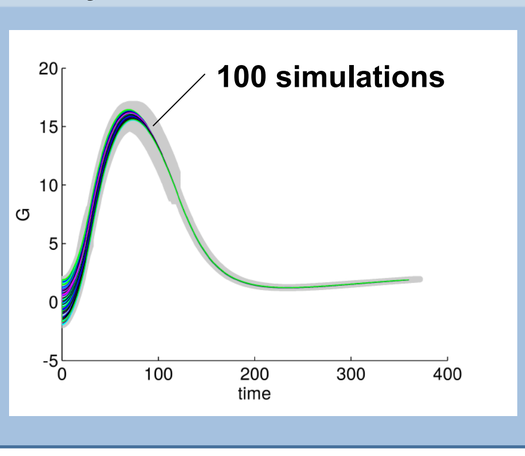
Efficient Analysis of Cyber-Physical Systems using Symbolic Methods

Sergiy Bogomolov

IST Austria, Austria

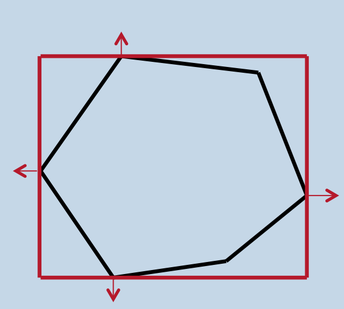
Analysis Methods for CPS

- Simulation based methods
- Symbolic methods account for
  - Dependencies between space and time
  - Uncertainties in the system behavior

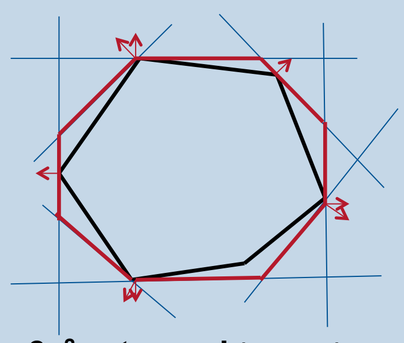


Approximating Convex Sets

- Constraint polyhedra - PHAVer
- Support Function - SpaceEx
  - Direction → position of supporting halfspace
  - Arbitrarily precise set representation

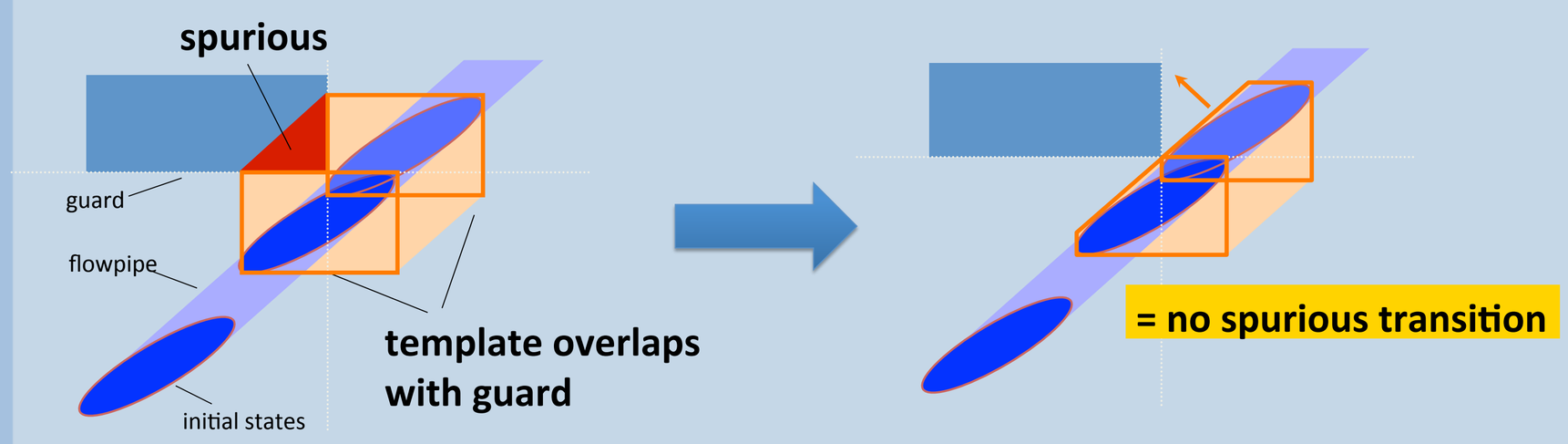


2n bounding box ($\pm x_i$)



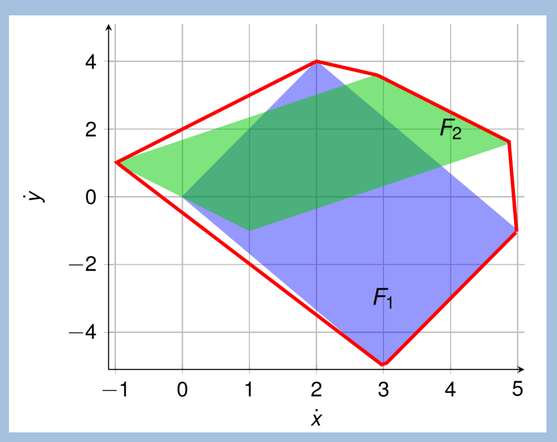
2n² octagonal ($\pm x_i \pm x_j$)

Region representation refinement [1,2]



- Coarse region representation might lead to spurious transitions
- Region representation can be refined by adding new template directions

Compositional reasoning [4]



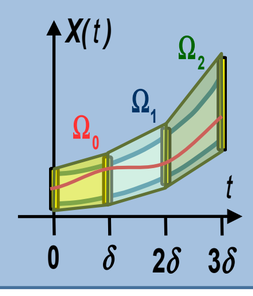
Assume-guarantee reasoning for hybrid systems:

$$\frac{H_1 \,||\, A \models P \quad H_2 \models A}{H_1 \,||\, H_2 \models P}$$

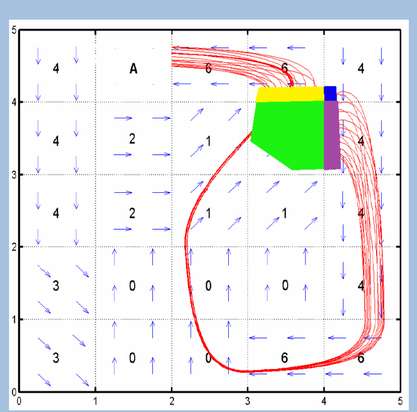
where H_1, H_2 are hybrid systems, A an assumption, and P a safety proposition.

SpaceEx [6]

- Recent and powerful model checking tool (Frehse et al., CAV 2011).
- Applies symbolic search in the region space.



Guided Search [3,5]



Prioritization of the search space exploration:

- Box-based heuristic which relies on geometric interpretation of symbolic states
- PDB heuristic which exploits the flexible granularity of modern reachability analysis algorithm

References

1. Abstraction Refinement for the Reachability Analysis of Convex Hybrid Systems. Sergiy Bogomolov, Goran Frehse, Mirco Giacobbe, Thomas A. Henzinger. Submitted to POPL 2017
2. Eliminating Spurious Transitions in Reachability with Support Functions. Goran Frehse, Sergiy Bogomolov, Marius Greitschus, Thomas Strump and Andreas Podelski. HSCC 2015
3. Guided Search for Hybrid Systems Based on Coarse-Grained Space Abstractions. Sergiy Bogomolov, Alexandre Donze, Goran Frehse, Radu Grosu, Taylor T. Johnson, Hamed Ladan, Andreas Podelski and Martin Wehrle. STTT 2015
4. Assume-Guarantee Abstraction Refinement Meets Hybrid Systems. Sergiy Bogomolov, Goran Frehse, Marius Greitschus, Radu Grosu, Corina Pasareanu, Andreas Podelski, and Thomas Strump, HVC 2014. Best Paper Award.
5. A Box-based Distance between Regions for Guiding the Reachability Analysis of SpaceEx. Sergiy Bogomolov, Radu Grosu, Goran Frehse, Hamed Ladan, Andreas Podelski and Martin Wehrle. CAV 2012
6. SpaceEx: Scalable Verification of Hybrid Systems. Goran Frehse, Colas Le Guernic, Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel, Rodolfo Ripado, Antoine Girard, Thao Dang, Oded Maler. CAV 2011