SPeeDI – a Verification Tool for Polygonal Hybrid Systems

GERARDO SCHNEIDER

Joint work with

EUGENE ASARIN, GORDON PACE AND SERGIO YOVINE

VÉRIMAG, GRENOBLE

Introduction

- Verification of Hybrid Systems
- Reachability problem
  - For 3 and higher dimensional systems: undecidable in general
  - For many 2 dimensional systems: decidable

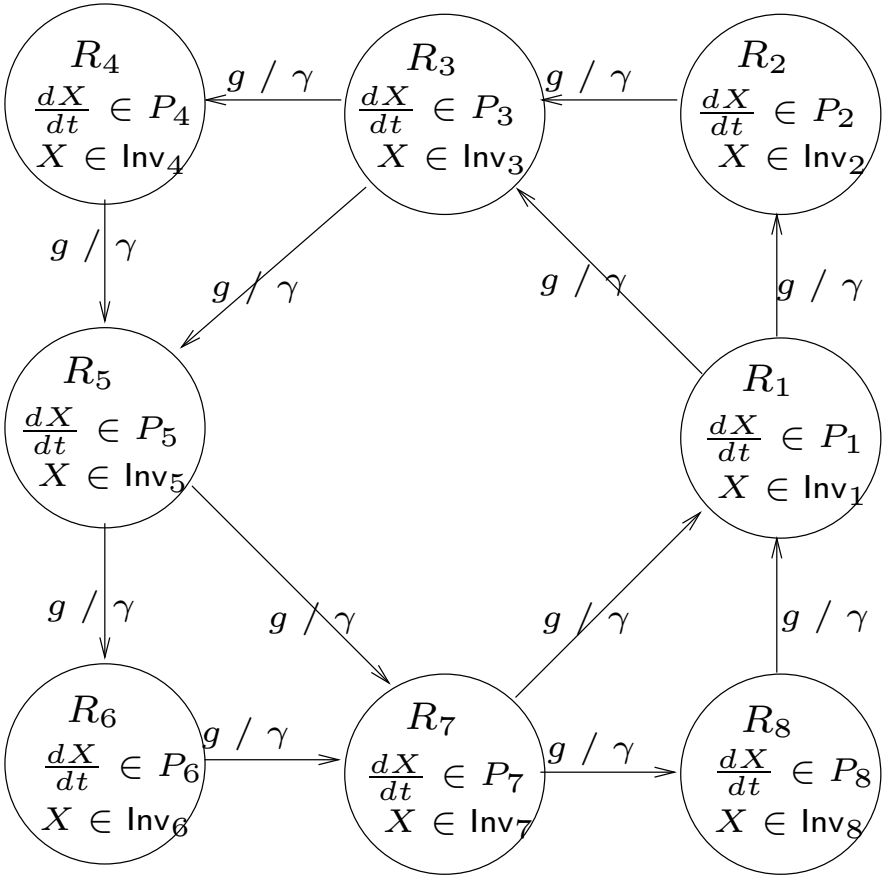
Introduction

- Verification of Hybrid Systems
- Reachability problem
  - For 3 and higher dimensional systems: undecidable in general
  - For many 2 dimensional systems: decidable

- In this work we implement our reachability algorithm for a general class of non-deterministic 2-dim systems: SPDIs

Introduction

- Representation: Hybrid Automata

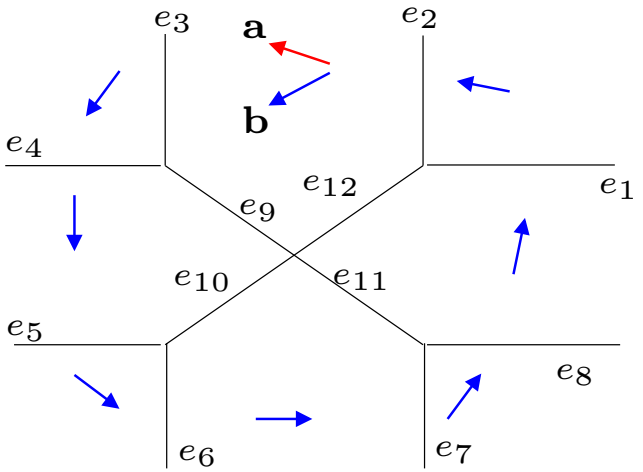


Polygonal Differential Inclusion Systems (SPDIs)

- A partition of the plane into convex polygonal regions (states)
- Dynamic for each state

$$\frac{dX}{dt} \in \angle_{\mathbf{a}}^{\mathbf{b}} \text{ if } X \in R_i$$

That is, X moves in a direction between $\mathbf{a}$ and $\mathbf{b}$

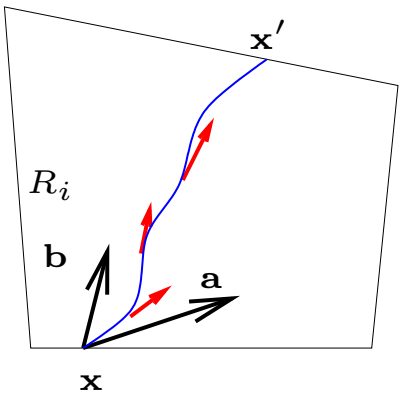


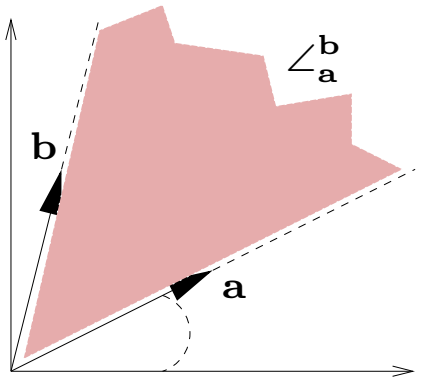
Polygonal Differential Inclusion Systems (SPDIs)

- A partition of the plane into convex polygonal regions (states)
- Dynamic for each state

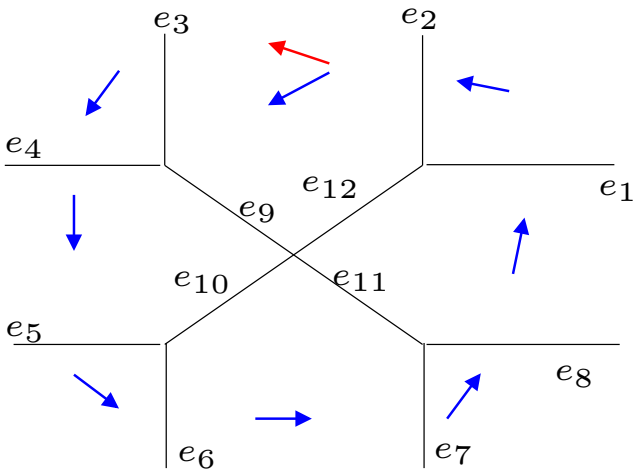
$$\frac{dX}{dt} \in \angle_{\mathbf{a}}^{\mathbf{b}} \text{ if } X \in R_i$$

That is, X moves in a direction between $\mathbf{a}$ and $\mathbf{b}$

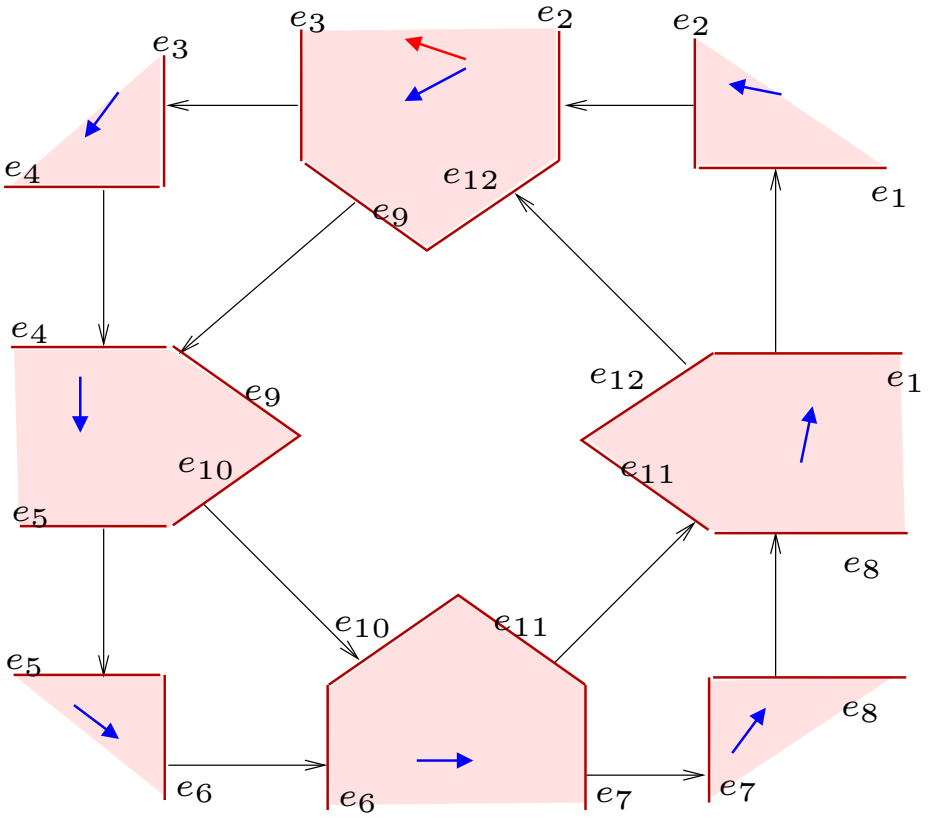




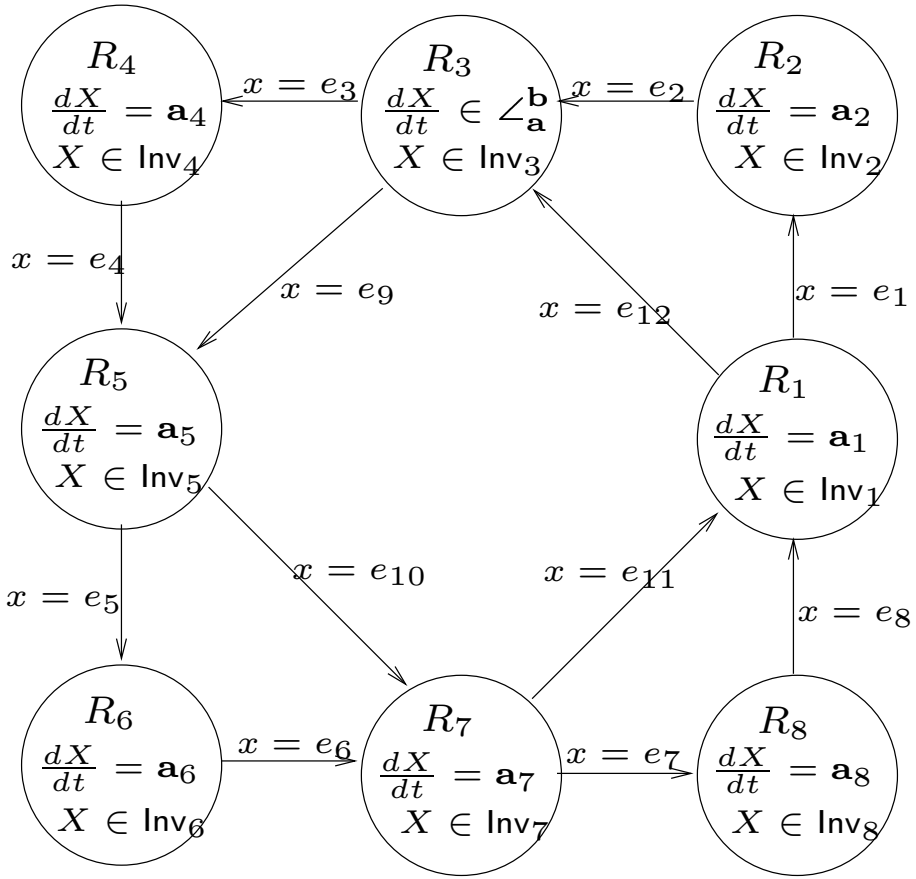
SPDIs are Hybrid Automata



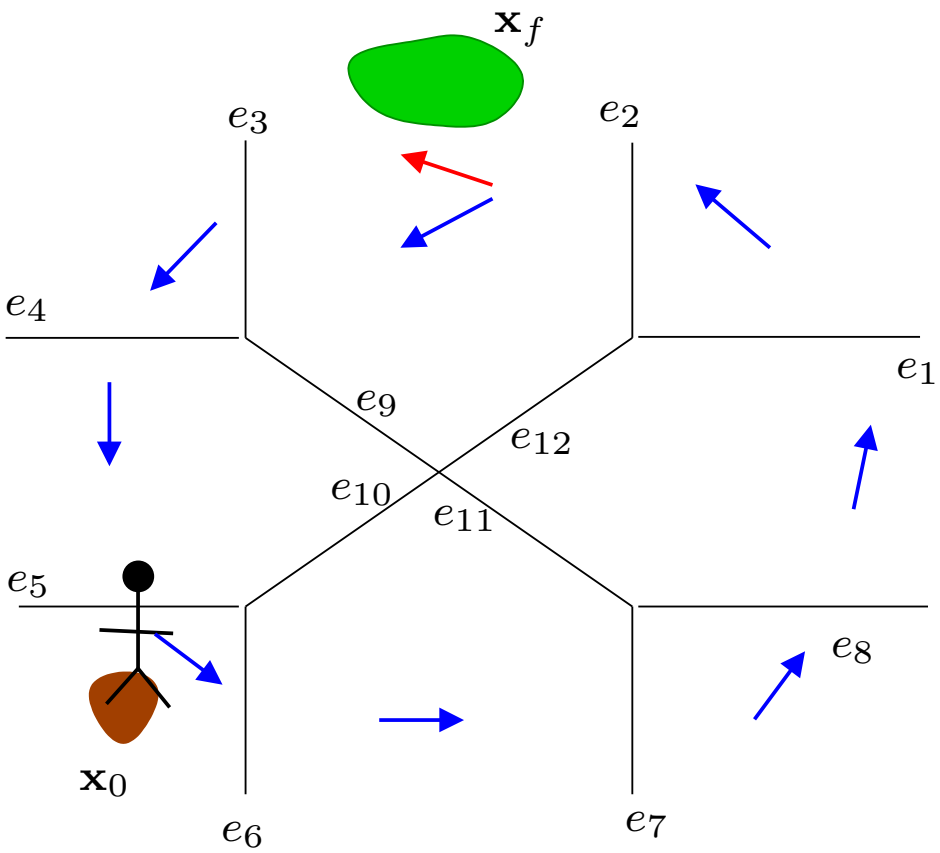
SPDIs are Hybrid Automata



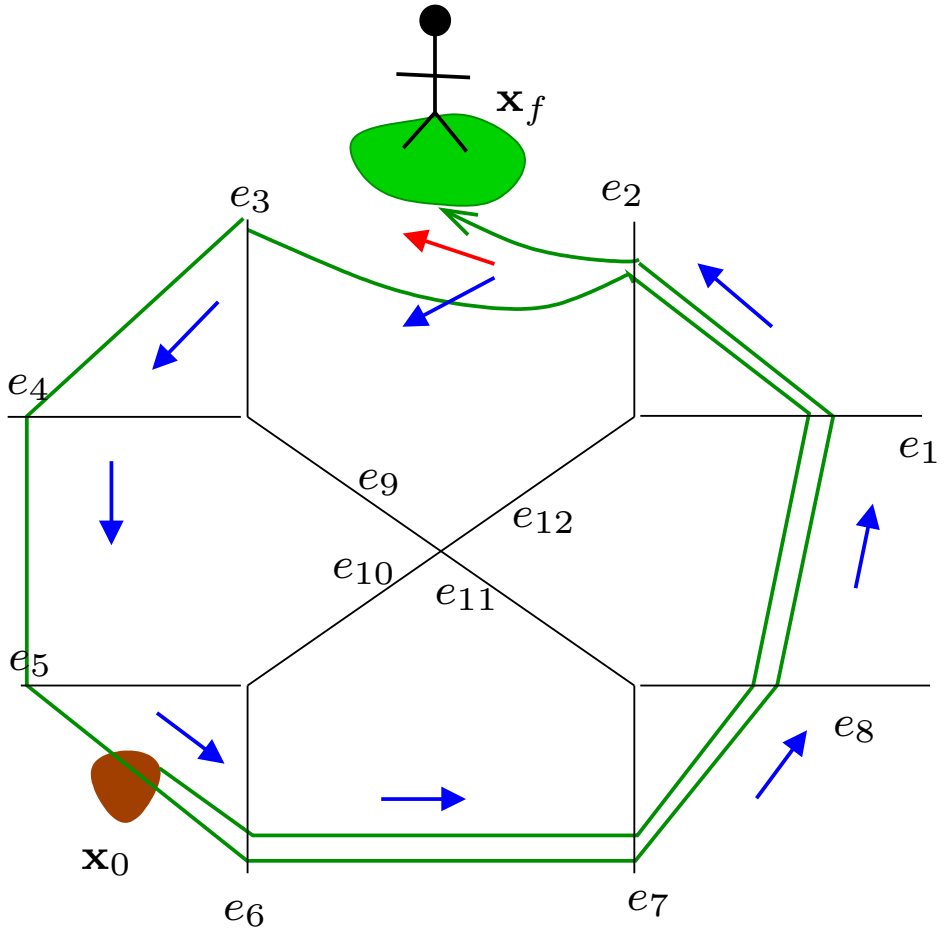
SPDIs are Hybrid Automata



The Reachability Problem for SPDIs



The Reachability Problem for SPDIs



Reachability problem: Is there a trajectory from $\mathbf{x}_0$ to $\mathbf{x}_f$?

The Reachability Algorithm

HSCC'2000

Planar Topology + Abstraction + Acceleration + a little bit of Linear Algebra

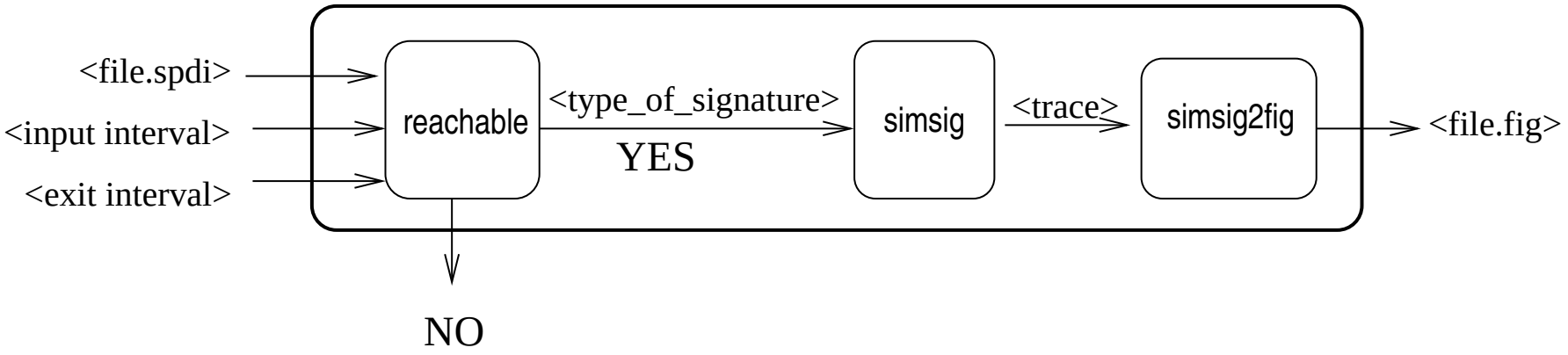
Our algorithm

Implementation: SPeeDI

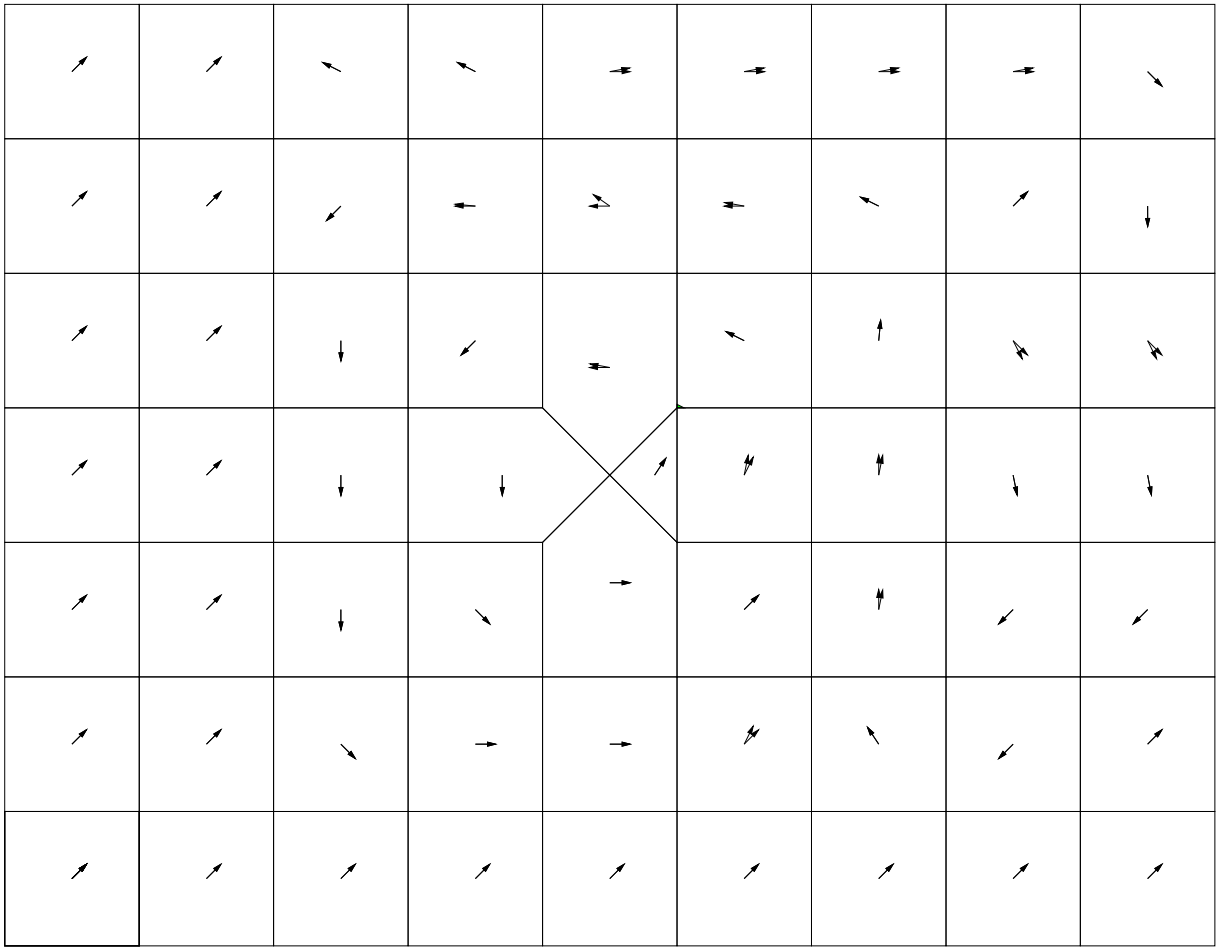
- We have implemented the reachability algorithm for SPDIs: SPeeDI
- 5000 lines of Haskell

Implementation: SPeeDI

- We have implemented the reachability algorithm for SPDIs: SPeeDI
- 5000 lines of Haskell



Example

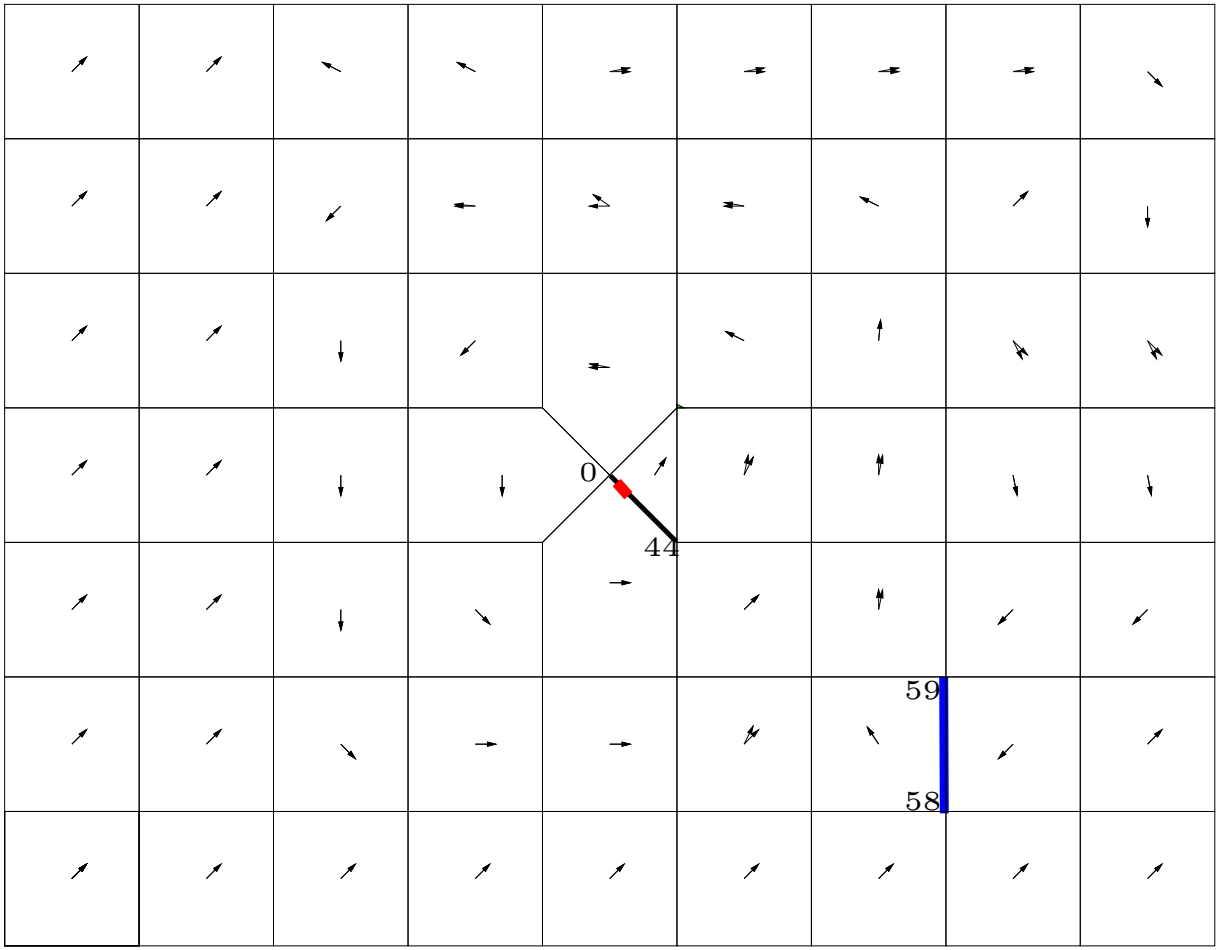


Example

Input file

Points:	Vectors:	Regions:
0. 0.0, 0.0	v3. -1,0.1833333333	* ...
* ...	* ...	* ...
33. -5.0, -35.0	v8. 1,0	33 ? 41 ! 42 ! 34 ? 33, v9, v9
34. -5.0, -25.0	v9. 1,1	34 ! 42 ! 43 ? 35 ? 34, v22, v22
35. -5.0, -15.0	v12. 1, 1.5	35 ? 36 ? 0 ! 44 ! 43 ! 35, v8, v8
36. -5.0, -5.0	v20. -1, 0.001	44 ! 45 ! 0 ? 44, v12, v12
37. -5.0, 5.0	v22. 1,-0.001	0 ? 45 ? 46 ! 38 ! 37 ! 0, v3, v20
38. -5.0, 15.0	v25. -1,0.7	38 ? 46 ? 47 ! 39 ! 38, v25, v20
39. -5.0, 25.0	v28. 1, 0.001	*...
* ...	*...	*...

Example



Is the blue interval on edge 58-59 reachable from the red one on edge 0-44?

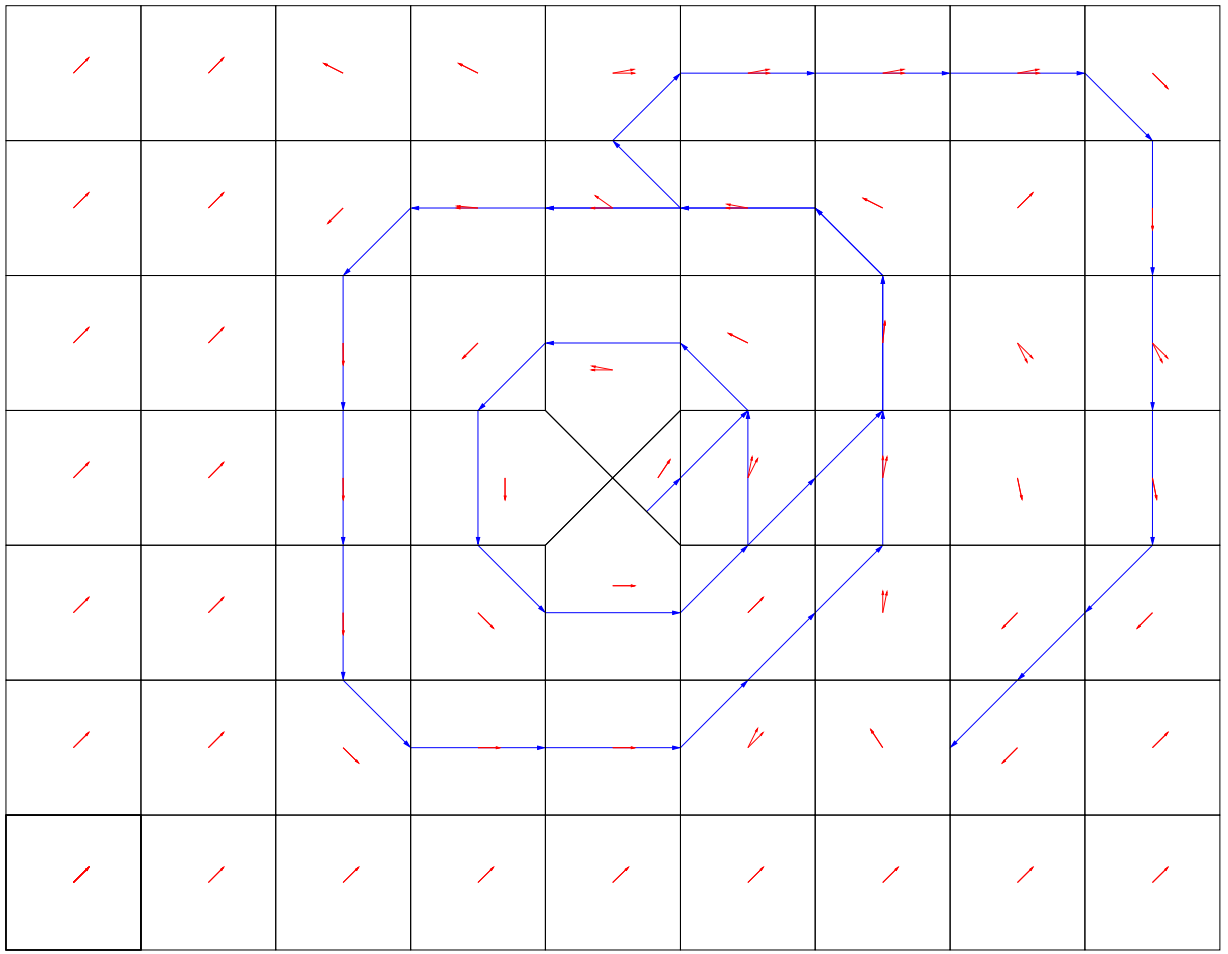
Example

Session log

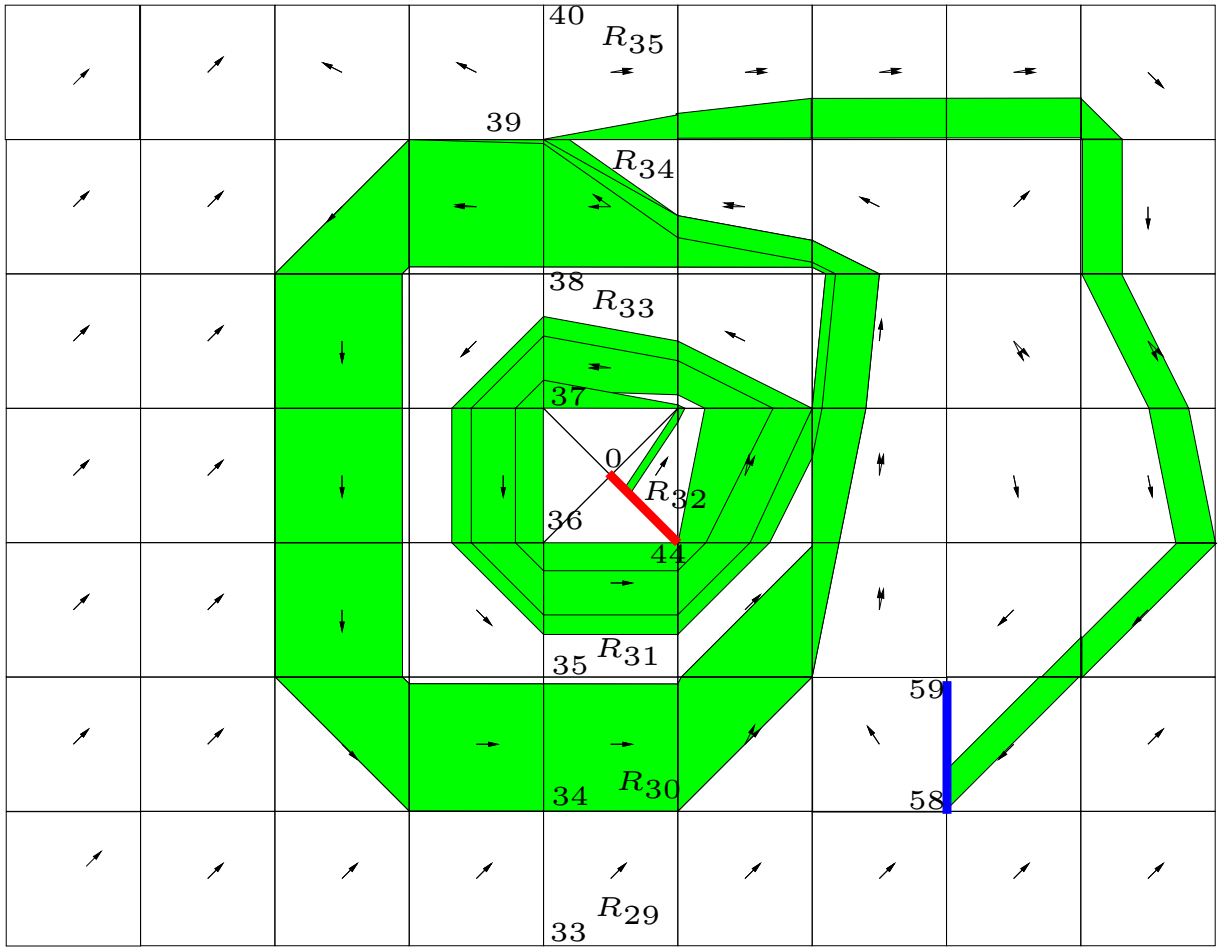
reachable example.spdi [1,2] [0,10] 0-44 58-59

Generating and trying signatures from edge 0-44 to 58-59
Starting interval: [1.0,2.0]
Finishing interval: [0.0,10.0]
(0-44,45-44) (45-53,45-46,37-38,...,36-35,44-43,44-52)*
(53-52,53-61,54-62,54-55,46-47) (38-39,..., 46-47)* (39-47,
...,67-59,58-59) <REACHABLE>

Example



Example



Conclusions

Implementation of the reachability algorithm for SPDIs: SPeeDI is based on a “geometric” method

– Restricted to 2 dimensional systems

\+ It is an exact decision algorithm

\+ It takes advantage of *abstraction* and *acceleration* techniques

\+ It performs better than HyTech for SPDIs

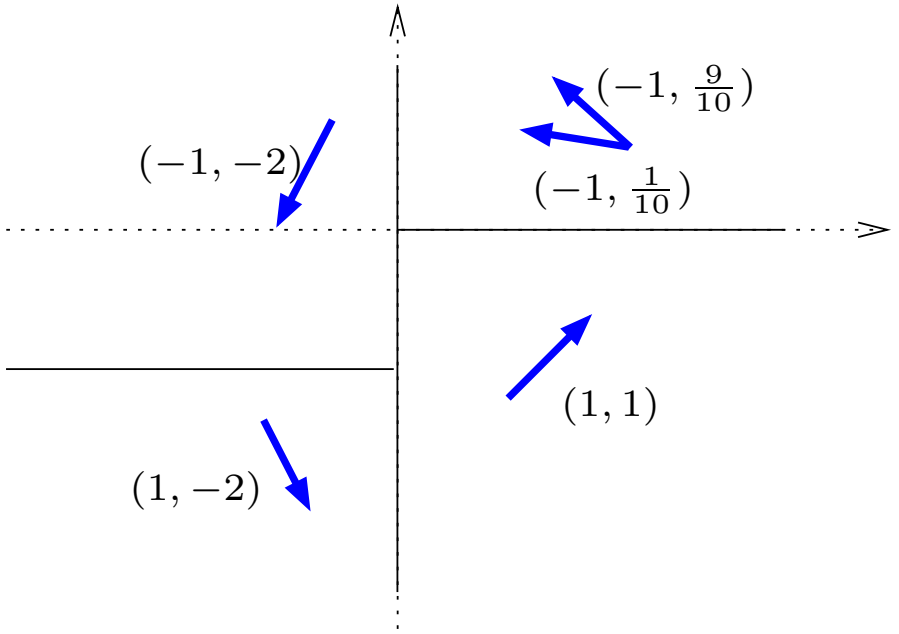
Perspectives

- Extensions beyond reachability: liveness, etc
- Application of the technique for more complex dynamics
- Extension to higher dimensional systems
- SPDI as an approximation of non-linear systems

Thank you!

Comparison with HyTech

Example:



Fixpoint: $I^* = (\frac{200}{9}; 200)$

Reachability question: Is $\frac{201}{9}$ reachable from $[3, 4]$?

Comparison with HyTech

Final Point	*HyTech*	*SPeeDI*	*Reachable*
199	`overflow`	`0.05 sec`	Yes
200	`overflow`	`0.05 sec`	No
210	`overflow`	`0.05 sec`	No
5	`0.04 sec`	`0.05 sec`	No
$\frac{200}{9}$	`0.10 sec`	`0.05 sec`	Yes
$\frac{201}{9}$	`overflow`	`0.03 sec`	Yes
$\frac{199}{9}$	`0.07 sec`	`0.04 sec`	Yes
$\frac{1}{2}$	`0.06 sec`	`0.05 sec`	No

Comparison with HyTech

Simulation of reachability for $x_f = \frac{201}{9}$