Controller Synthesis for Linear Hybrid Systems

Part 4: Demo

Formal Methods for Cyber-Physical Systems
Verona, September 12-16, 2017

Marco Faella
Università di Napoli “Federico II”

Lesson Summary

- Symbolic polyhedra manipulation with PPL
- Controller synthesis with SpaceEx+

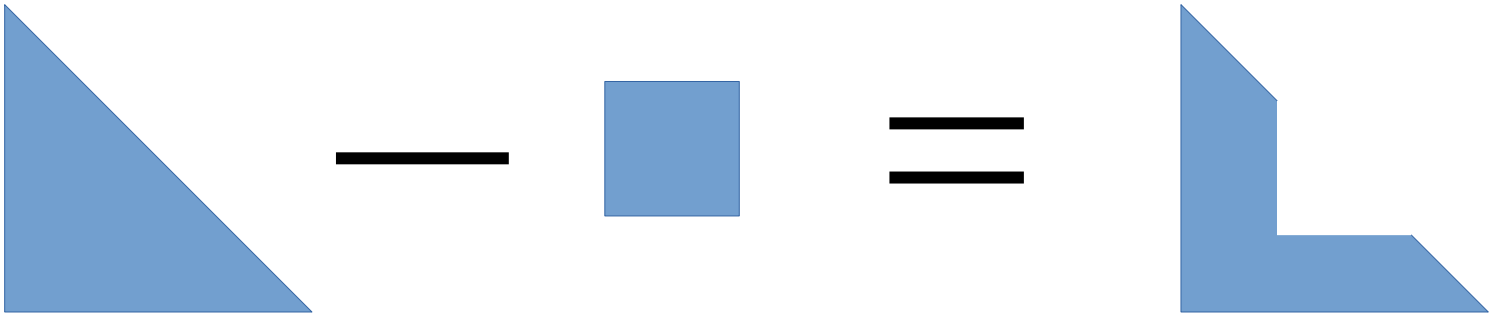
Why Polyhedra?

- Many applications!
  - Software static analysis
  - Software cost analysis
  - Software verification
  - Optimizing compilation (Graphite)
  - Stochastic games (PRISM)
  - Petri Nets (Romeo)

Parma Polyhedra Library

- Bagnara et al., 2002 - now
- Open source
- C++
- Supports several *domains*, including polyhedra

Example



Demo

`ppl-demo/basic.cpp`

Exercise

Companies A and B need raw materials x, y, z

Company A needs:

between 30 and 50 x, or

at least 100 y (not both);

also, between 10 and 20 z

Company B needs:

between 20 and 60 x,

any amount of y,

between 10 and 30 z

moreover, $x+z \geq 30$

Exercise (continued)

Raw material provider C wants to favor A over B

Can C make an offer of raw materials that satisfies A but not B?

(Optional) If it can, let the program print such an offer

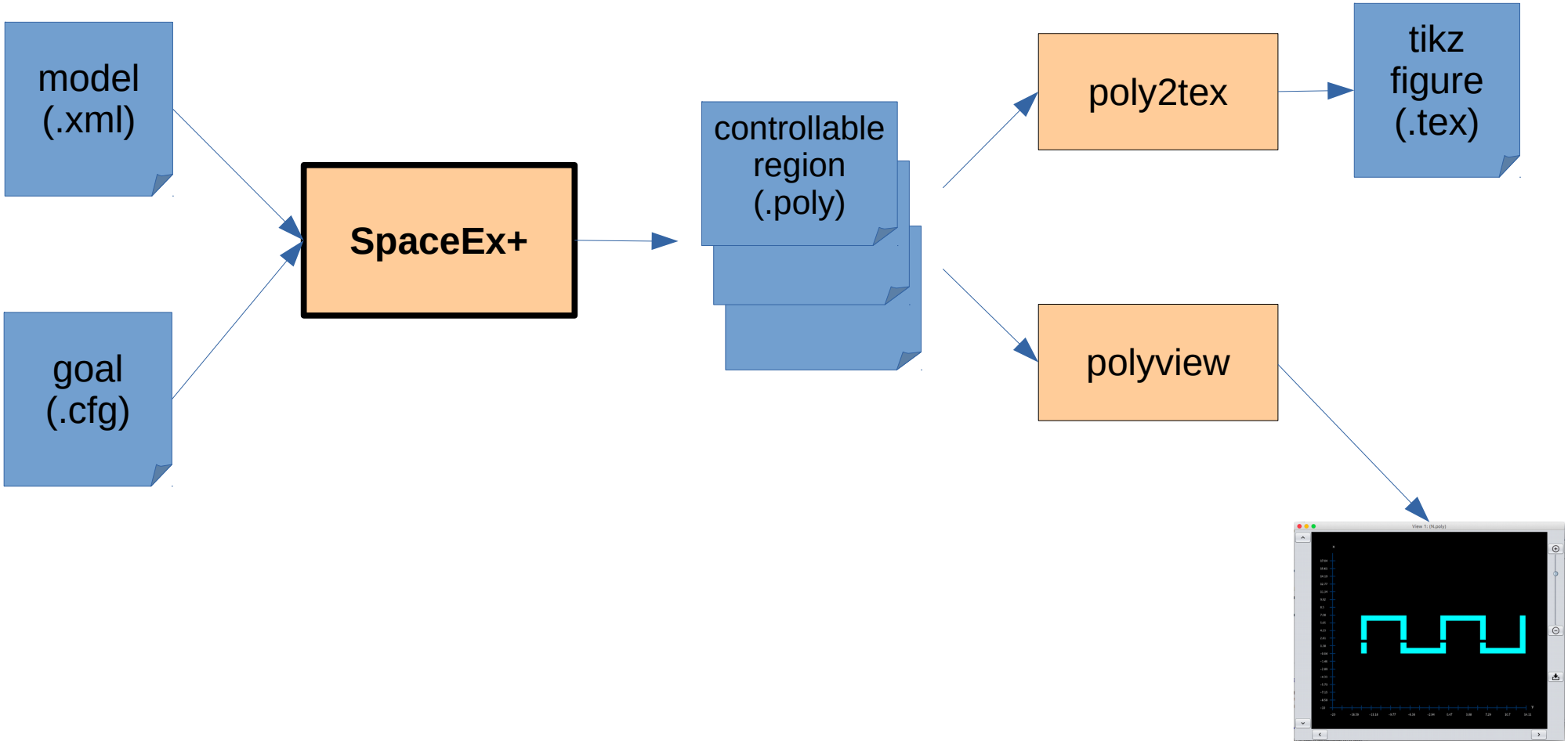
Controller Synthesis with SpaceEx+

Reachability

Instructions

- Launch the virtual machine:
  - `/opt/faella/faella`
- Login
  - username: spex
  - password: synthesis
- Open extra terminals
  - `ssh -X -p4422 spex@localhost`

Schematics


model
(.xml)
goal
(.cfg)
SpaceEx+
controllable
region
(.poly)
poly2tex
tikz
figure
(.tex)
polyview

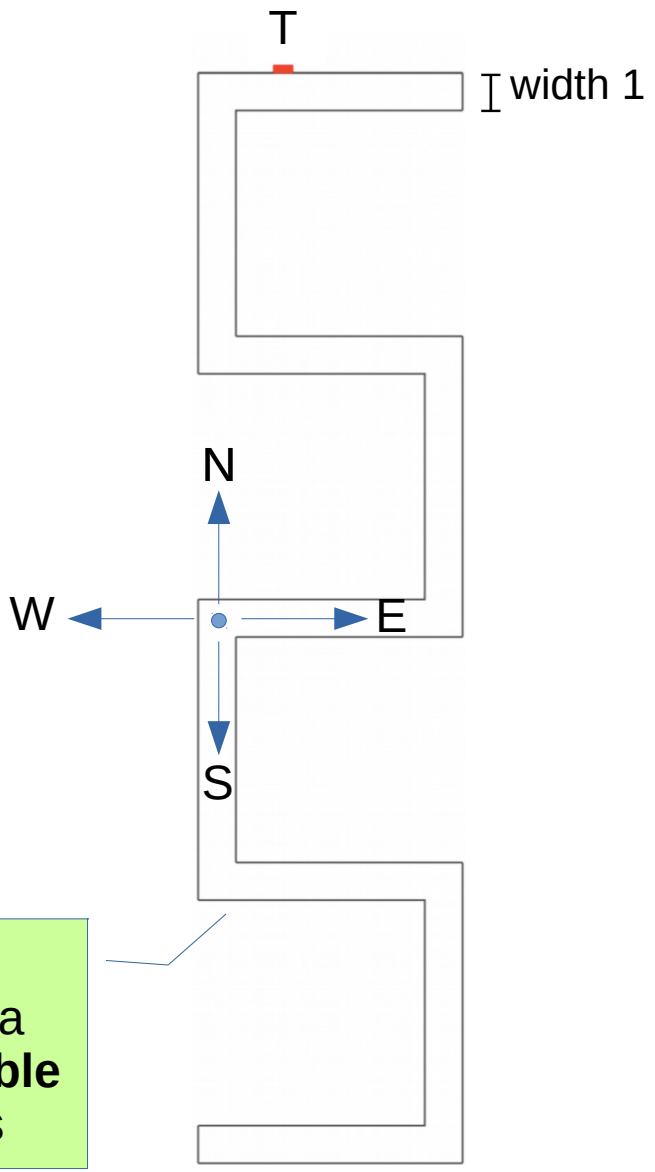
The “Maze” Example

Navigate a point vehicle in a maze

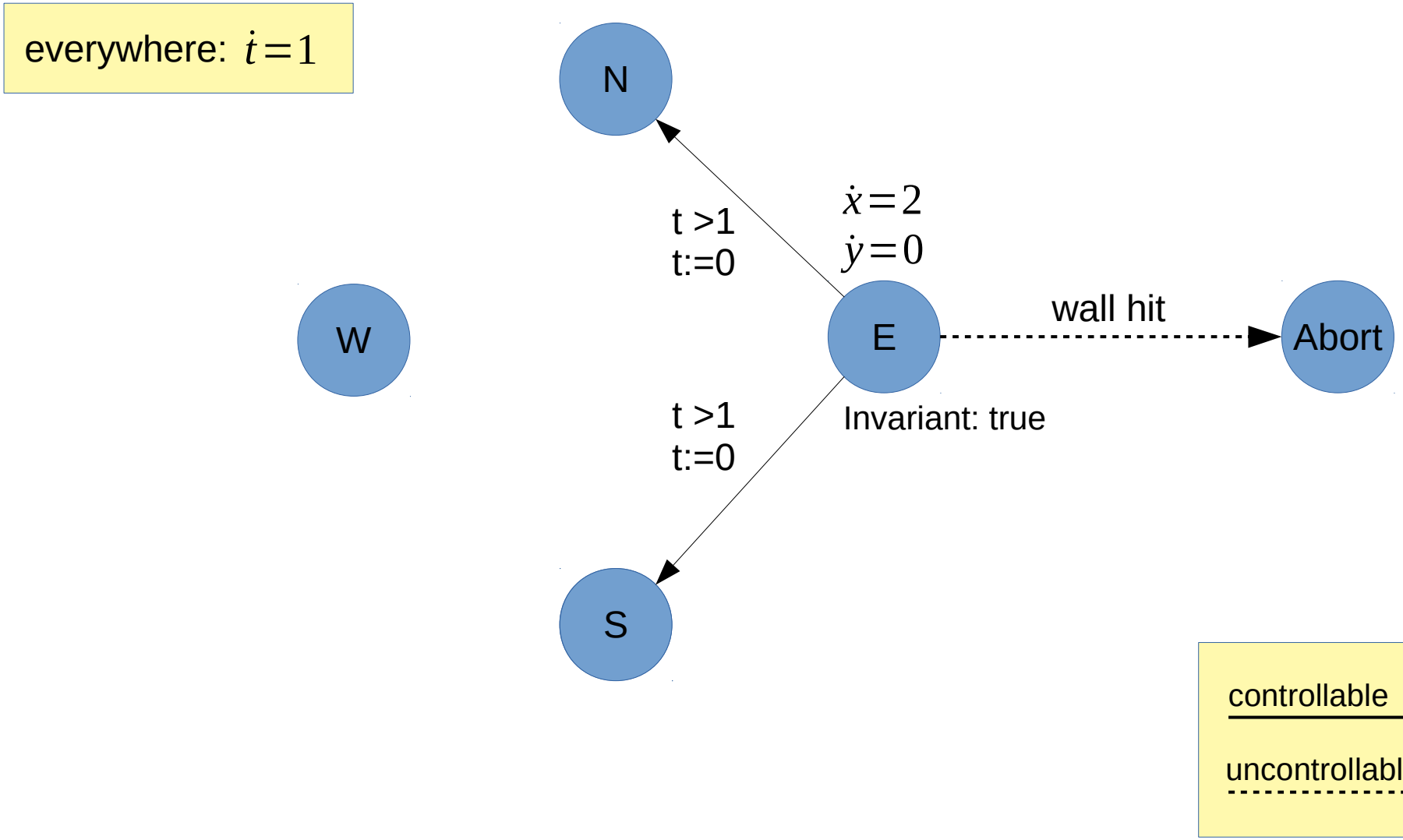
control goal: **reach T**

4 directions

1 time unit between two changes of dir. (non-Zeno)



The “Maze” Example



Demo

```
sspaceex -m maze.xml -g maze.cfg
```

Exercise 1

Plot location N when t=0

Can you explain the shape of the winning region in the topmost vertical section?

Why is it “thinner” than the middle vertical section?

Exercise 2

Project away t

Can you explain the enlargement of the winning region?

Why does it fill *most* of the topmost horizontal segment, but not *all* of it?

Tool Announcement

- A new tool, independent from SpaceEx
- Faster
- Fewer dependencies
- Easier to maintain/evolve

- October 2017

Bibliography

- M. Benerecetti, M. Faella. **Automatic Synthesis of Switching Controllers for Linear Hybrid Systems: Reachability Control**. *ACM Trans. on Embedded Computing Systems*, 16(4), 2017.
- M. Benerecetti, M. Faella. **Automatic Synthesis of Switching Controllers for Linear Hybrid Systems: Safety Control**. *Theoretical Computer Science*, 493. Elsevier, 2013.
- M. Benerecetti, M. Faella. **Tracking Differentiable Trajectories across Polyhedra Boundaries**. *HSCC 2013*.
- M. Benerecetti, M. Faella, S. Minopoli. **Reachability Games for Linear Hybrid Systems**. *HSCC 2012*.
- M. Benerecetti, M. Faella, S. Minopoli. **Revisiting Synthesis of Switching Controllers for Linear Hybrid Systems**. IEEE CDC 2011.