Set-Based Simulation with SpaceEx

Goran Frehse, Olivier Lebeltel, Thao Dang, Oded Maler
Univ. Grenoble Alpes / CNRS – Verimag, France

Alexandre Donzé
UC Berkeley, USA

Colas Le Guernic
DGA, France

Antoine Girard
Laboratoire Jean Kuntzmann, France

CPSoS Workshop, Vienna, April 11, 2016

Example: Tunnel Diode Oscillator

Tunnel Diode

V_d

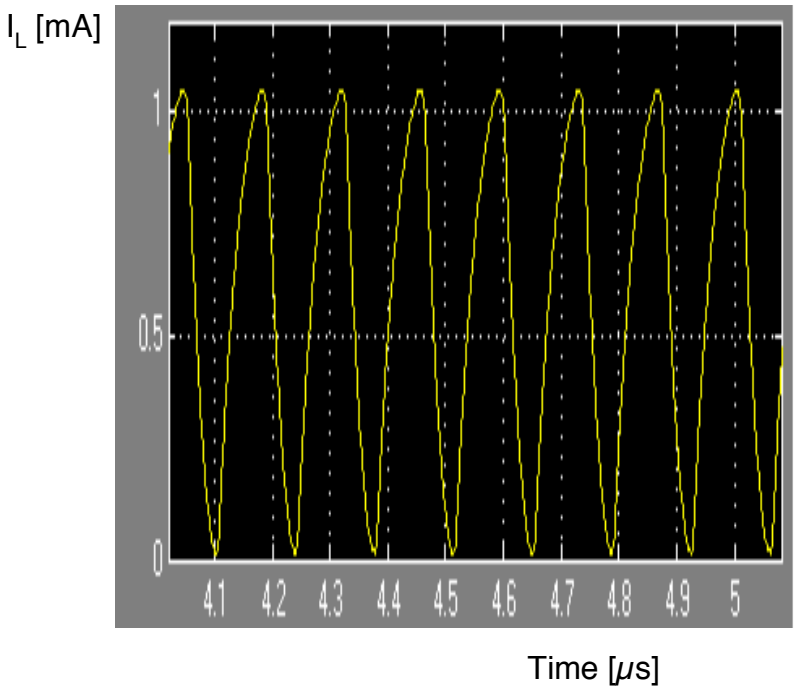
$$\dot{V}_C = \tfrac{1}{C}\left(-I_d(V_C) + I_L\right)$$
$$\dot{I}_L = \tfrac{1}{L}\left(-V_C - RI_L + V_{in}\right)$$

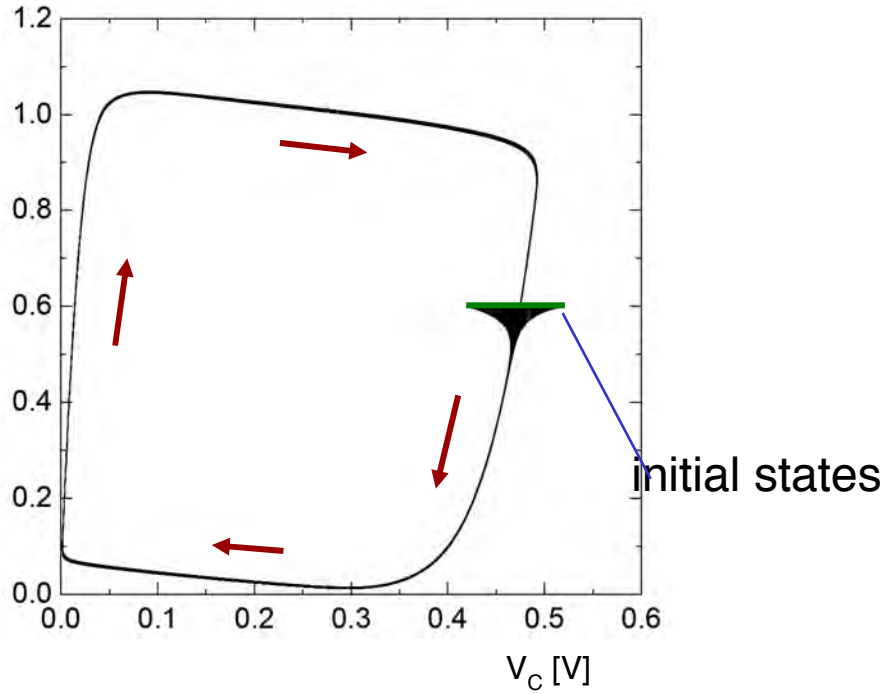
Dang, Donze, Maler, FMCAD' 04

- **What are good parameters?**
  - startup conditions
  - parameter variations
  - disturbances

Example: Tunnel Diode Oscillator

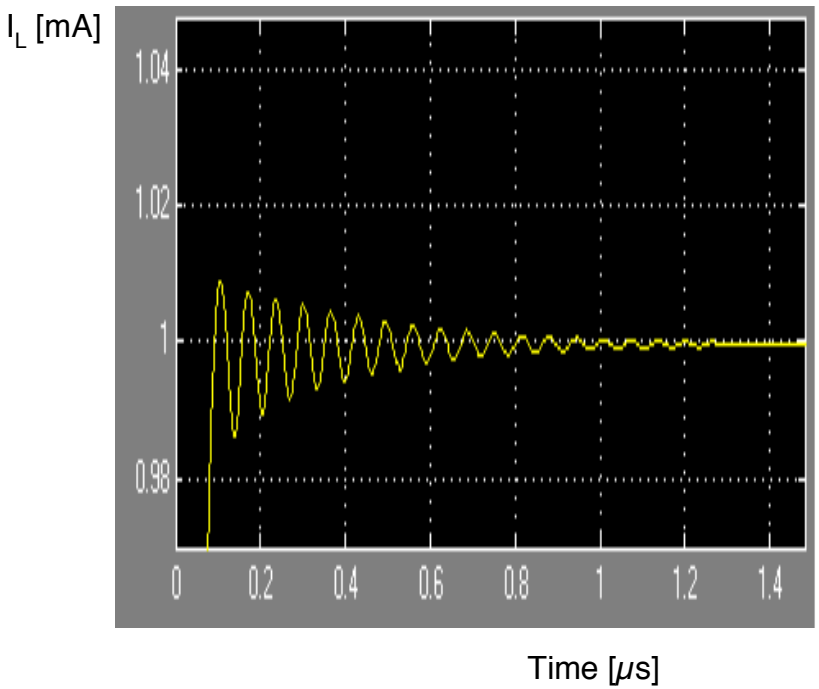
R=0.20Ω ⇒ Oscillation

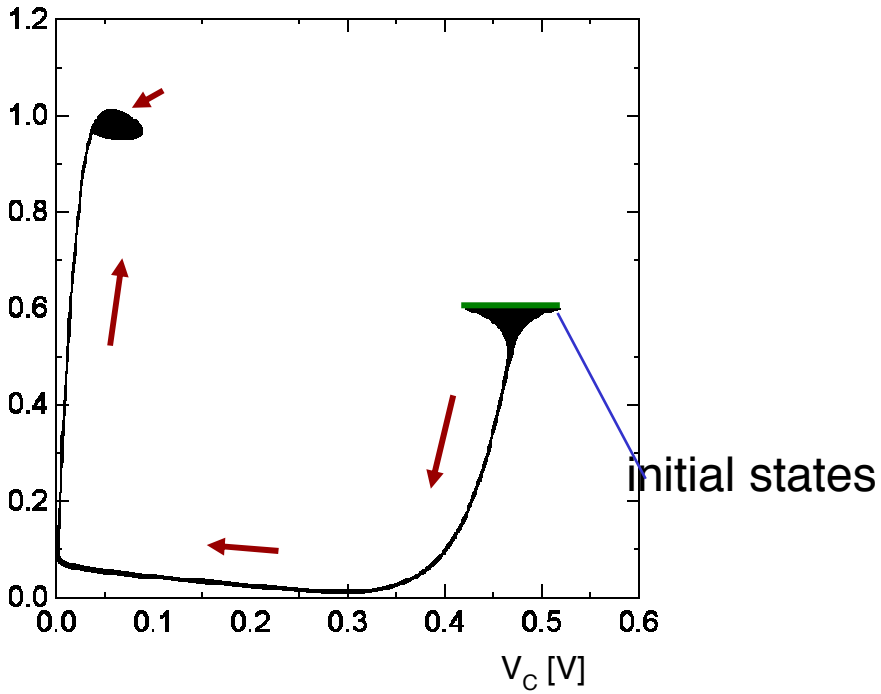




Example: Tunnel Diode Oscillator

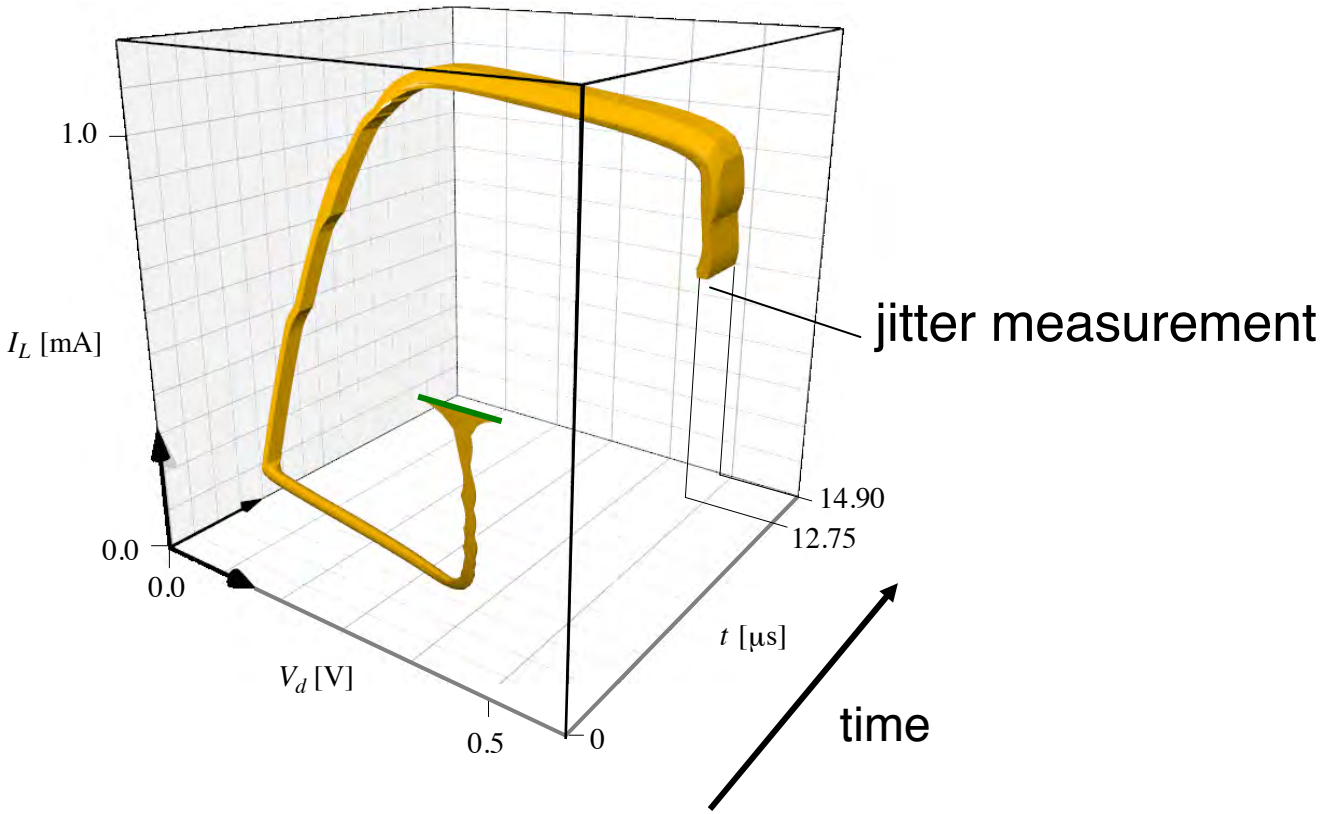
R=0.24Ω ⇒ Stable equilibrium





Example: Tunnel Diode Oscillator

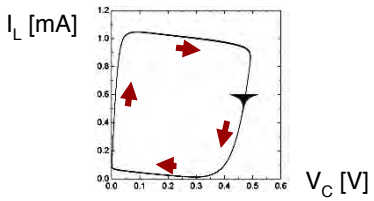
- **Jitter measurement**
  - add clock that is reset at zero crossing



Example: Tunnel Diode Oscillator

Tunnel Diode

$$\dot{V}_C = \tfrac{1}{C}\left(-I_d(V_C) + I_L\right)$$
$$\dot{I}_L = \tfrac{1}{L}\left(-V_C - RI_L + V_{in}\right)$$



- Oscillation
- Jitter
- …

Analog/Mixed Signal Circuit

↓

Formal Model

↓

Reachability Analysis

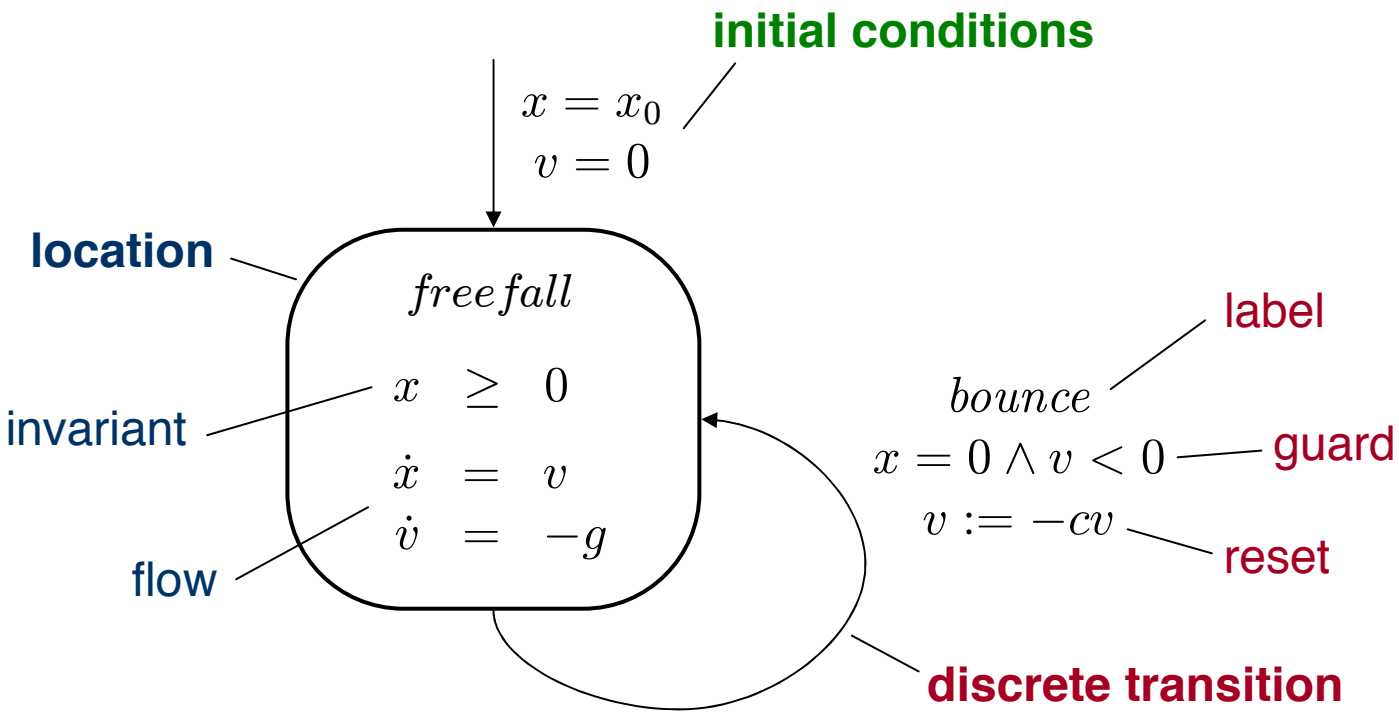
↓

Guaranteed Safety Property

Outline

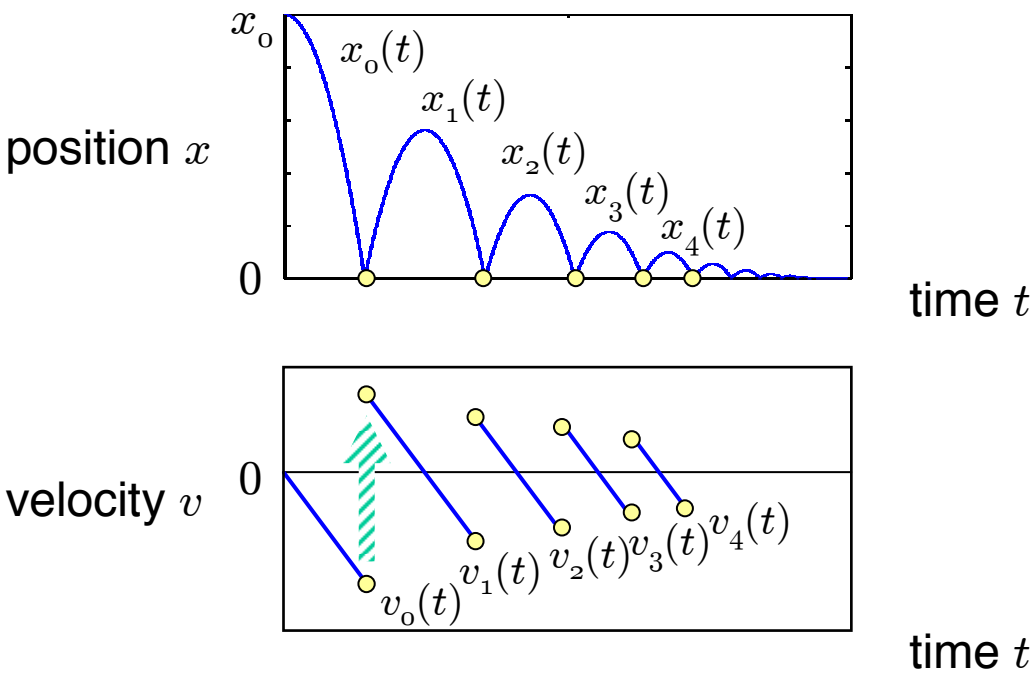
- Modeling with Hybrid Automata
- Reachability versus Simulation
- Computing with High-Dimensional Sets
- SpaceEx Verification Platform

Hybrid Automaton Model



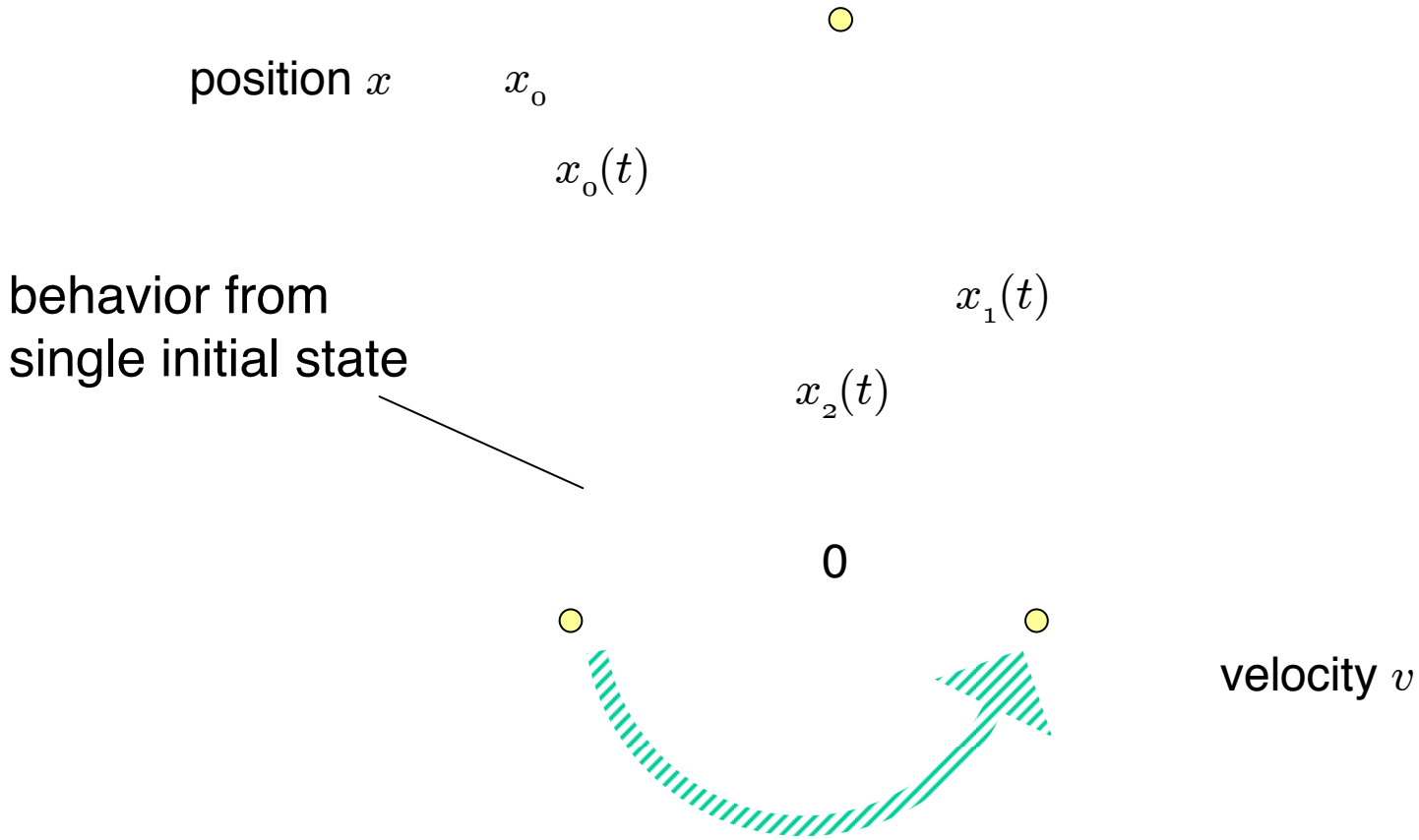
Semantics

- **alternating sequence**
  - time elapse (ODEs)
  - jumps (intersection with guard, affine map)



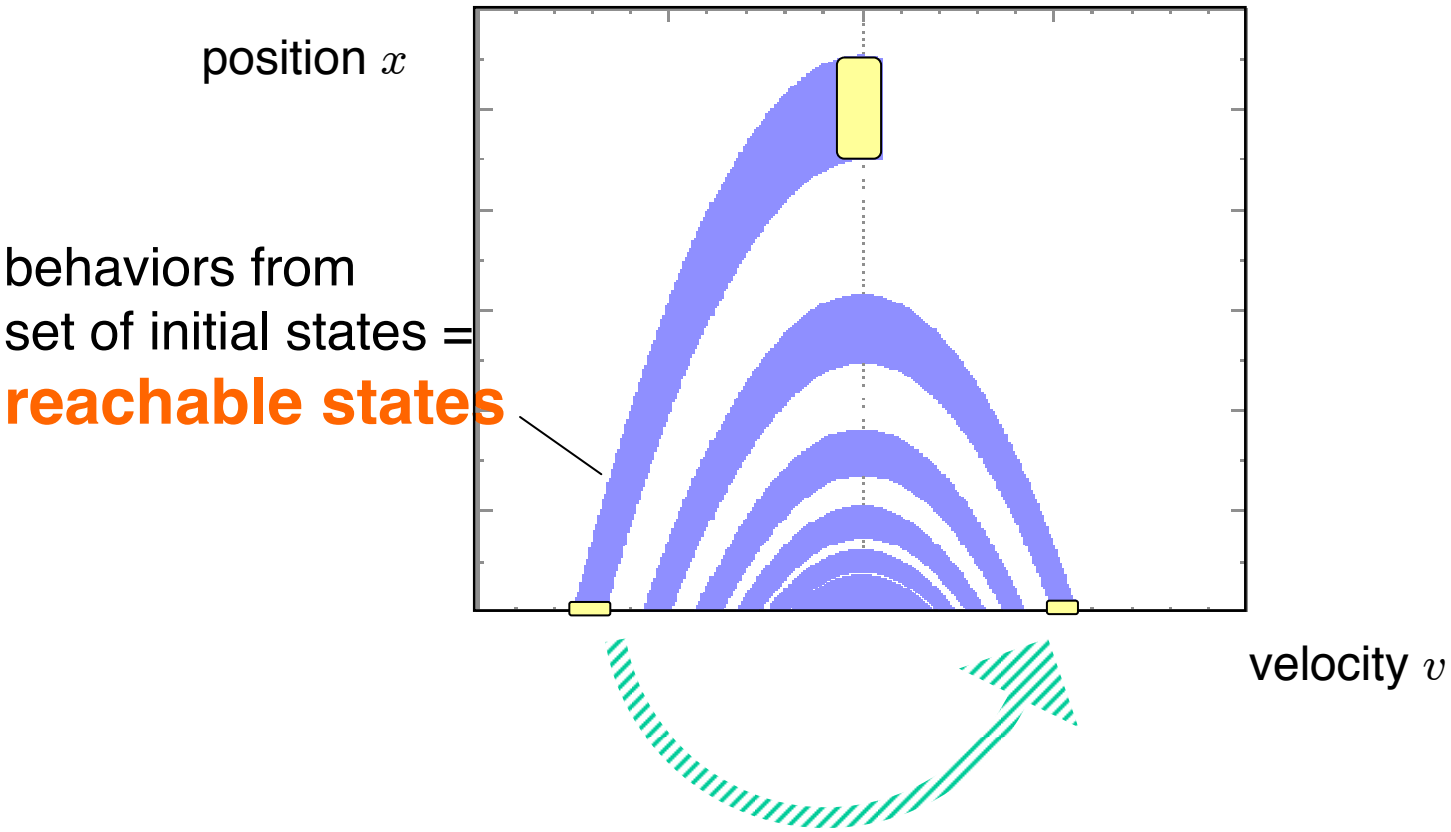
Example: Bouncing Ball

- **States over States = State-Space View**



Example: Bouncing Ball

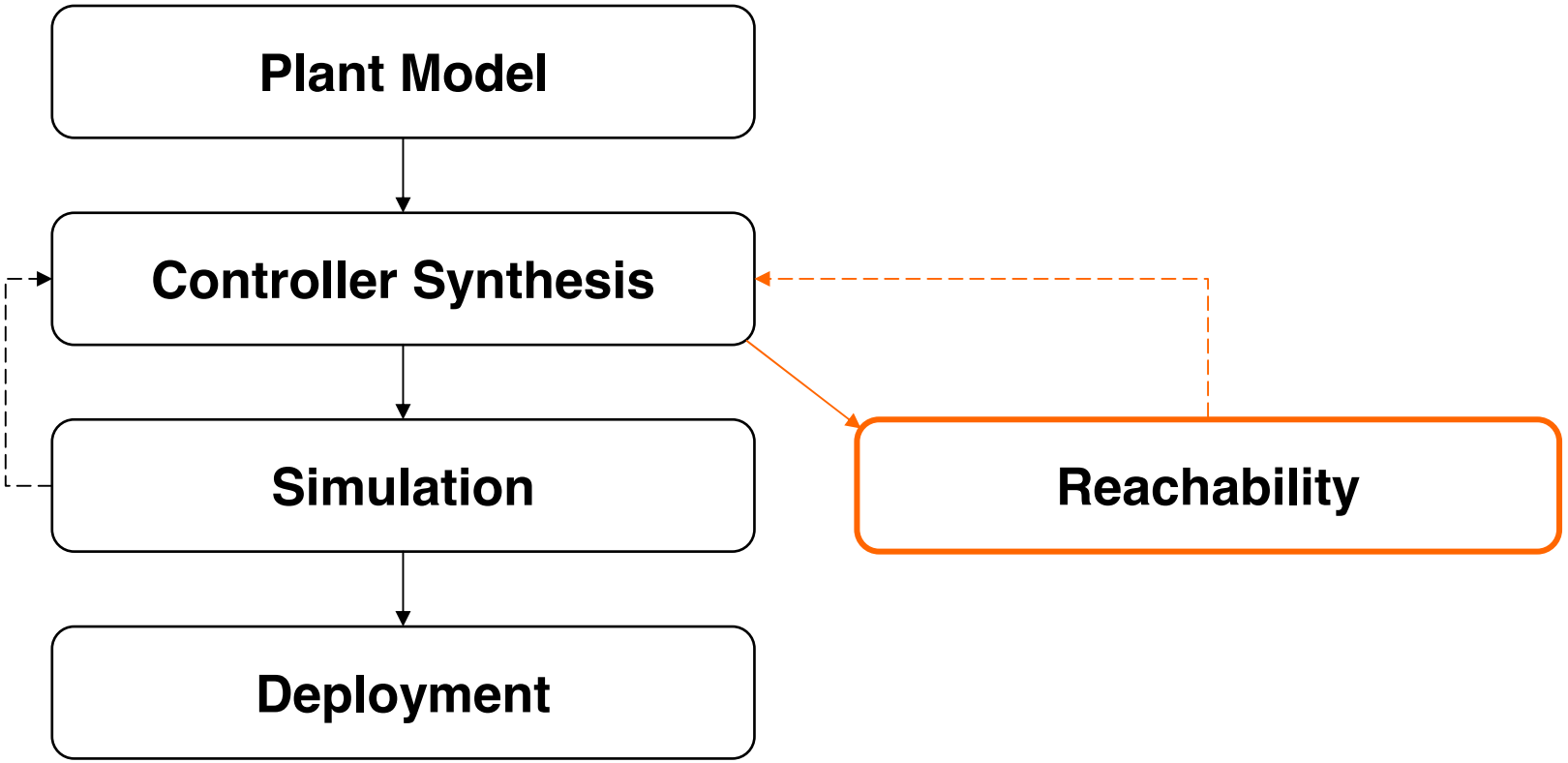
- **Reachability in State-Space**



Outline

- Modeling with Hybrid Automata
- **Reachability versus Simulation**
- Computing with High-Dimensional Sets
- SpaceEx Verification Platform

Reachability in Model Based Design



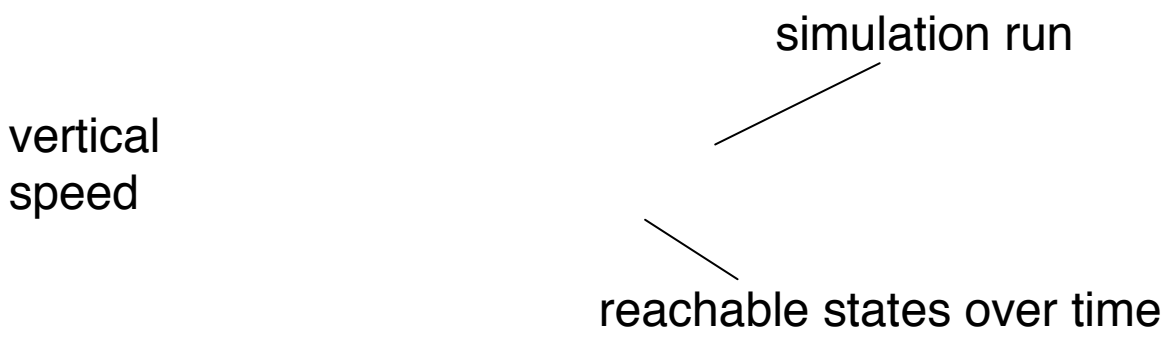
Example: Controlled Helicopter

- **28-dim model of a Westland Lynx helicopter**
  - 8-dim model of flight dynamics
  - 20-dim continuous H∞ controller for disturbance rejection
  - stiff, highly coupled dynamics

S. Skogestad and I. Postlethwaite, Multivariable Feedback Control: Analysis and Design. John Wiley & Sons, 2005.

Simulation vs Reachability

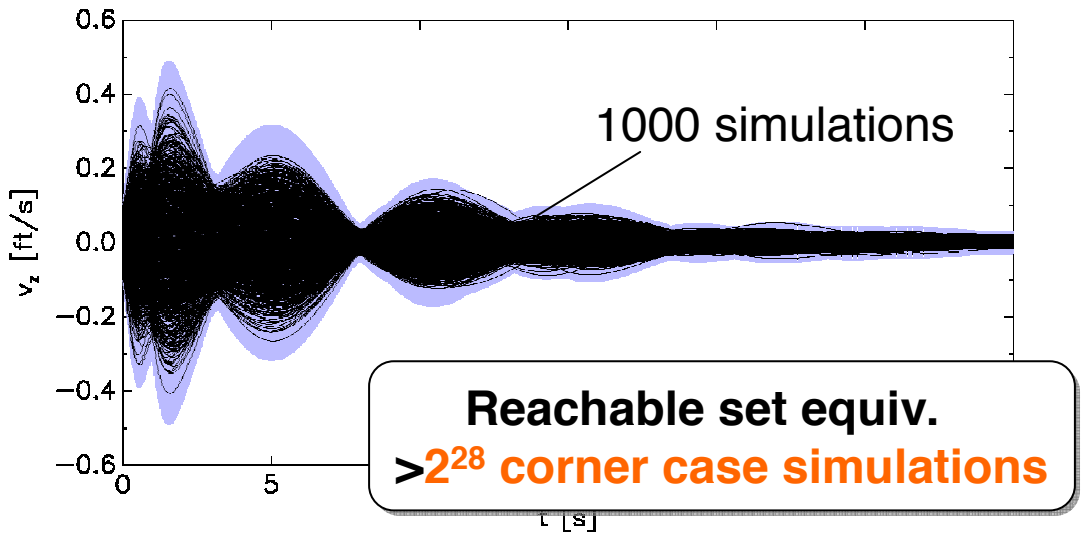
- **Simulation**
  - approximative sample of **single** behavior
  - over finite time
- **Reachability**
  - over-approximative set-valued cover of **all** behaviors
  - over finite or infinite time



Simulation vs Reachability

- **Simulation**
  - deterministic
    - resolve nondet. using Monte Carlo etc.
  - scalable for nonlinear dyn.
- **Reachability**
  - **nondeterministic**
    - continuous disturbances...
    - implementation tolerances...
  - scalable for linear dynamics

vertical speed



Outline

- Modeling with Hybrid Automata
- Reachability versus Simulation
- **Computing with High-Dimensional Sets**
- SpaceEx Verification Platform

Computing Reachable States

- **Set-based integration can answer many interesting questions about a system**
  - safety, bounded liveness,…
- **Problems**
  - in general termination not guaranteed
  - set-based integration of ODEs is hard
- **Solution**
  - piecewise linear approximations
  - algorithmic & math tricks (implicit set representations,...)

Time Elapse Computation

- **Continuous time elapse for affine dynamics**
  - efficient, scalable
  - approximation without accumulation of approximation error (wrapping effect)
- **Much heritage from prior work**
  - Chutinan, Krogh. HSCC'99
  - Asarin, Bournez, Dang, Maler. HSCC'00
  - Girard. HSCC'05
  - **Le Guernic, Girard.** HSCC'06, **CAV'09**

Affine Dynamics

- **linear terms plus inputs U:**

$$\dot{x} = Ax + u,\ u \in U$$

- **solution:**

$$x(t) = e^{At}x(0) + \int_0^t e^{A(t-\tau)}u(\tau)d\tau$$

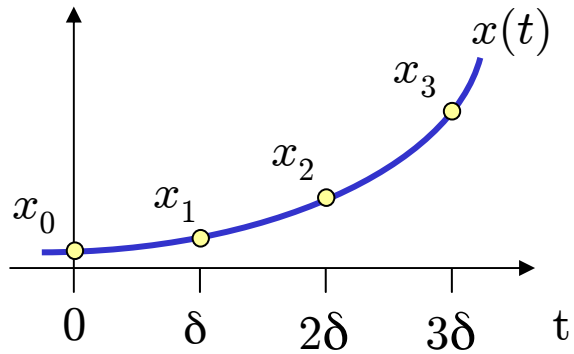
matrix exponential

factors influence of inputs
(stable system forgets the past)

Time-Discretization (no inputs)

- **Analytic solution:** $x(t) \quad = \quad e^{At} x_{Ini}$
  - with $t = \delta k$:

$$x(\delta(k+1)) \quad = \quad e^{A\delta} x(\delta k)$$



- **Explicit solution in discretized time (recursive):**

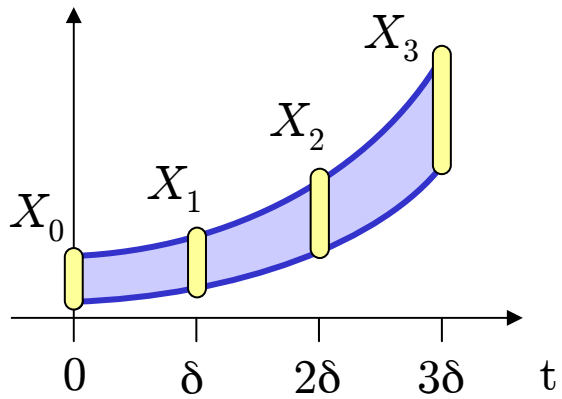
$$\begin{aligned} x_0 &= x_{Ini} \\ x_{k+1} &= e^{A\delta} x_k \end{aligned}$$

multiplication with const. matrix $e^{A\delta}$
= linear transform

Time-Discretization for an Initial Set

- **Explicit solution in discretized time**

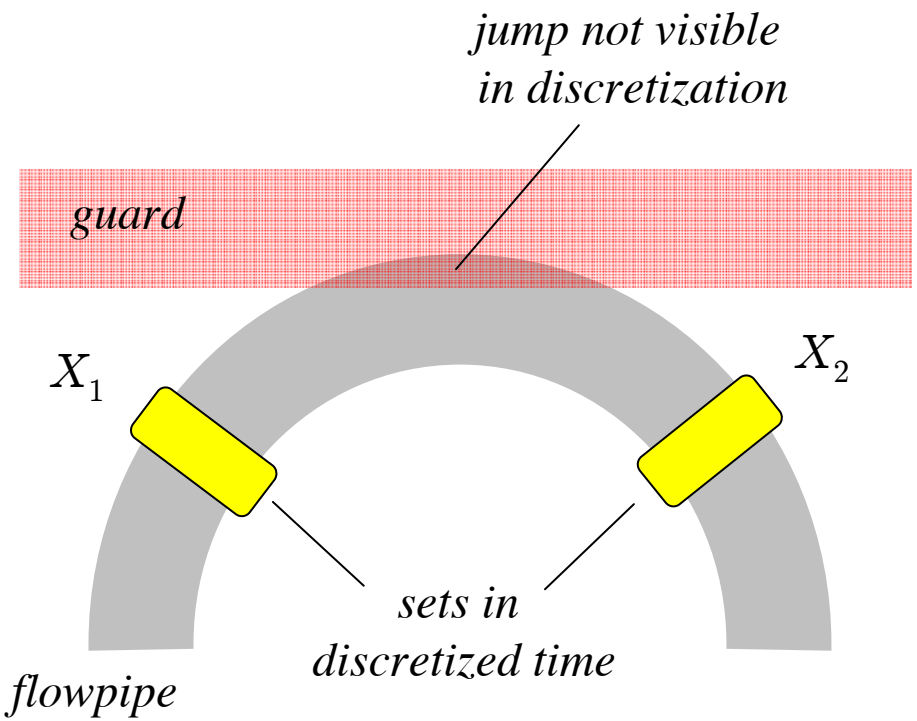
$$\begin{aligned} X_0 &= X_{Ini} \\ X_{k+1} &= e^{A\delta} X_k \end{aligned}$$



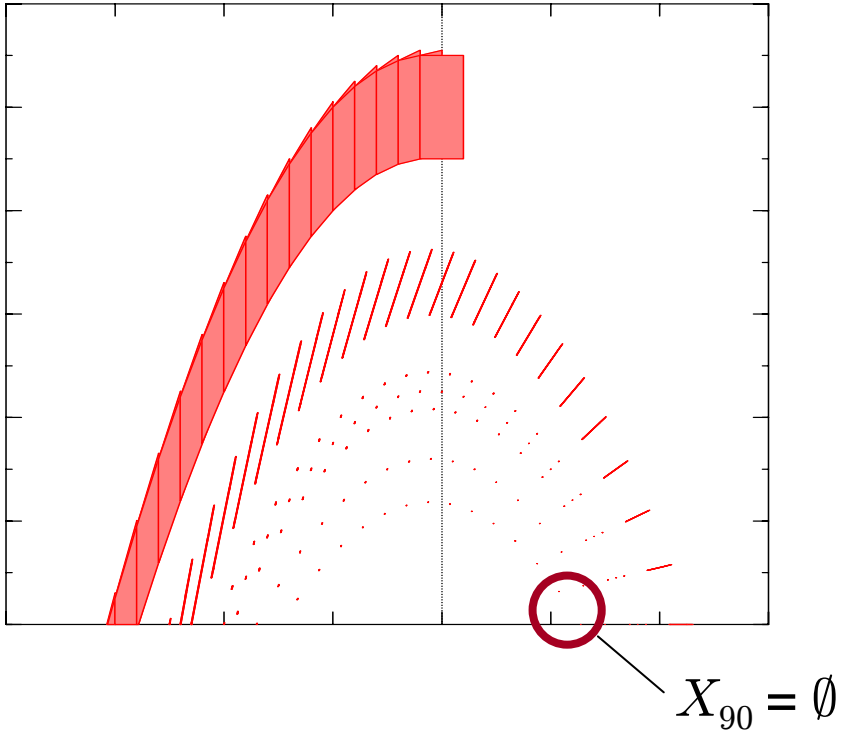
- **Acceptable solution for purely continuous systems**
  - $x(t)$ is in $\epsilon(\delta)$-neighborhood of some X_k
- **Unacceptable for hybrid systems**
  - discrete transitions might "fire" between sampling times
  - if transitions are "missed," $x(t)$ not in $\epsilon(\delta)$-neighborhood

Time Discretization for Hybrid Systems

- **One can miss jumps (guard)**



Bouncing Ball



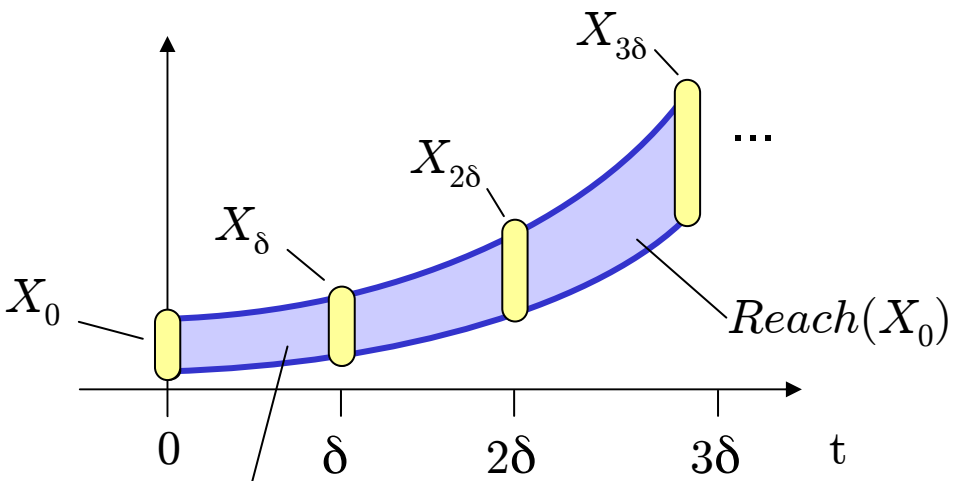
- Note: Computed in exact arithmetic, no numerical errors
- In other examples this error might not be as obvious…

From Time-Discretization to Reach

- **States in discrete time:**

$$X_{k\delta} \quad = \quad (e^{A\delta})^k X_0 \oplus S_{k\delta}$$

integral over inputs

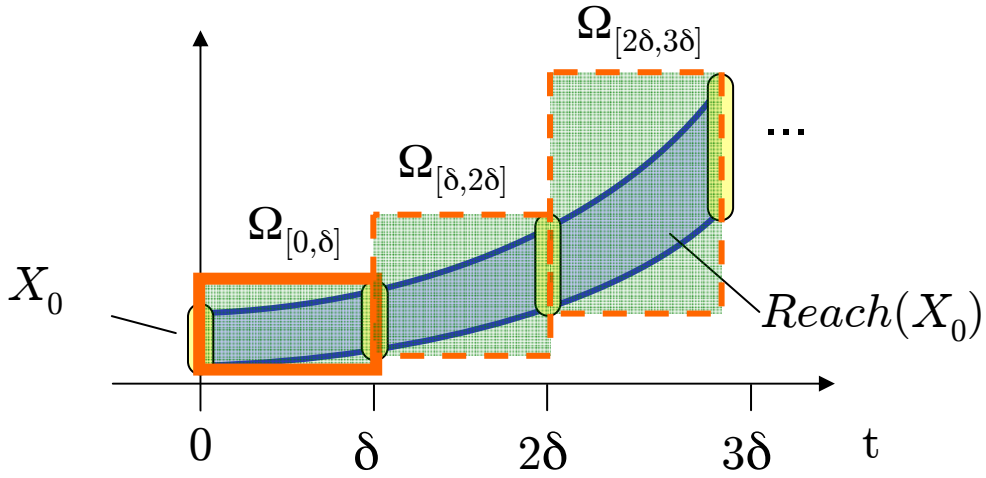


need to cover also states in between!

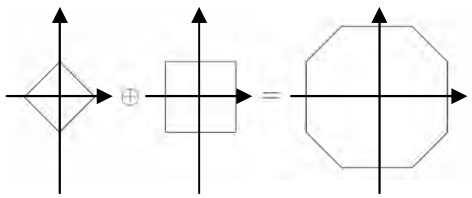
From Time-Discretization to Reach

- **Cover in discrete time:**

$$\Omega_{[k\delta,(k+1)\delta]} \quad = \quad (e^{A\delta})^k \Omega_{[0,\delta]} \oplus \Psi_{k\delta}$$



$\oplus$ Minkowski sum = pointwise sum of sets



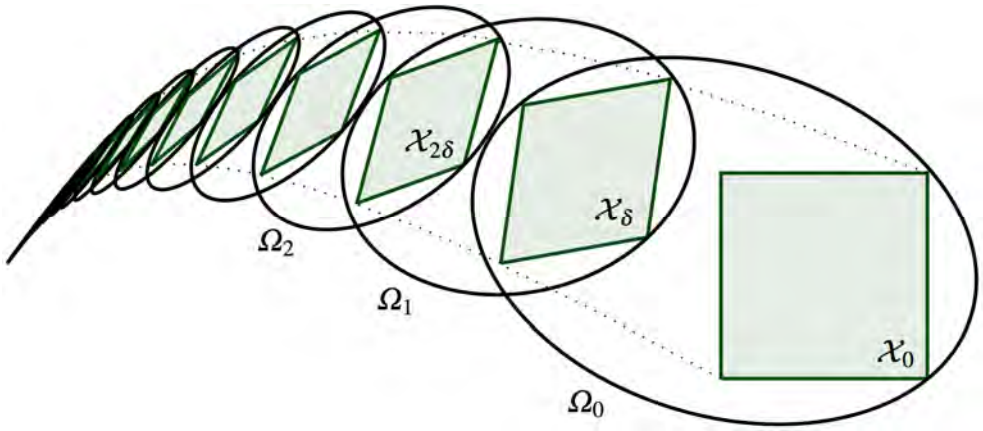
Reachability in High Dimensions

- **Scalability Trick 1:**

  Use data structures adapted to operations

Scalable Set Representations

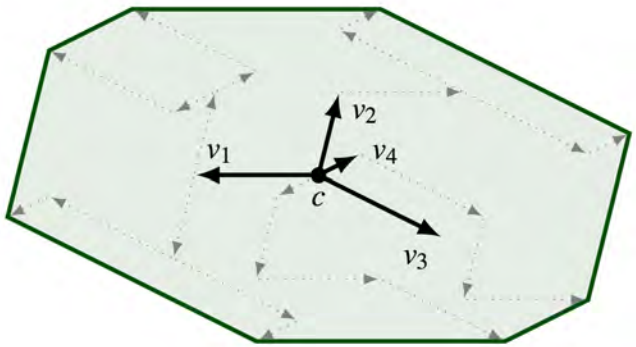
- **Ellipsoids** **[Kurzhansky, Varaiya 2006]**
  - bad representation of intersection, convex hull, flat sets

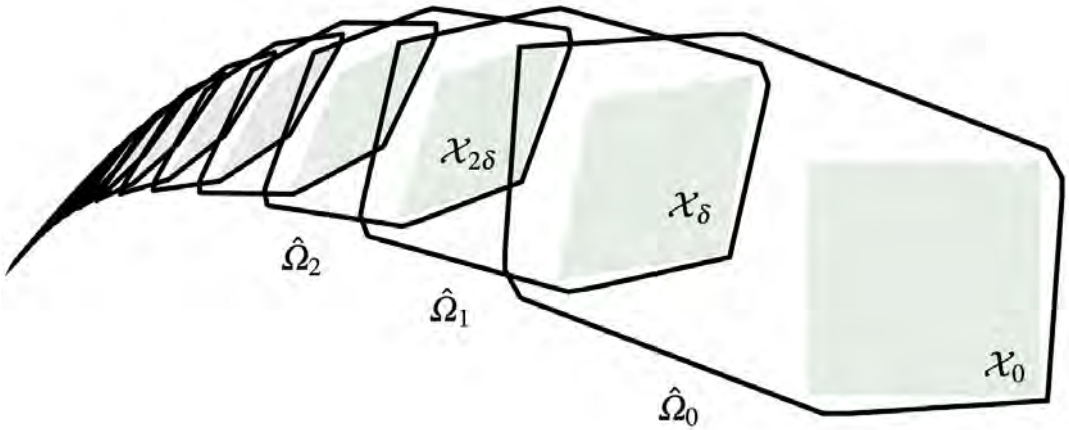


(this is an illustration, not actual computation)

Scalable Set Representations

- **Zonotopes** **[Girard 2005]**
  - symmetric polytope spanned by set of generator vectors
  - bad representation of intersection, convex hull, asymmetric sets

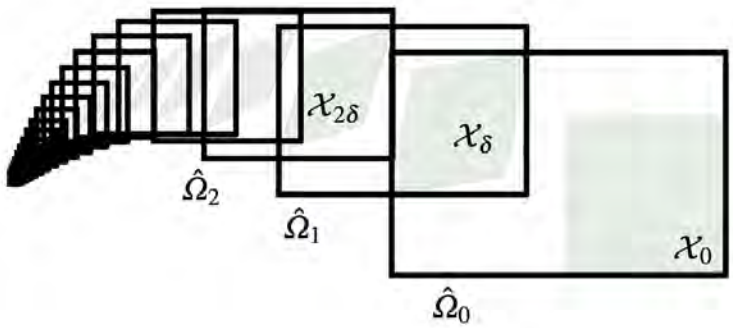




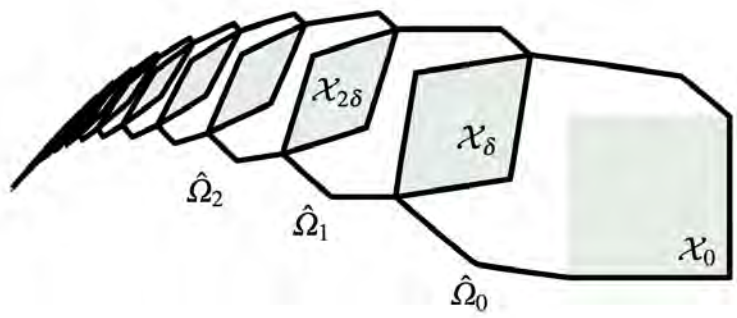
(computed with Zonotope toolbox of M. Althoff)

Scalable Set Representations

- **Support Functions** **[Le Guernic, Girard 2009]**
  - lazy representation of any convex set
  - gives outer polyhedral approximation that can be refined
  - scalable except for intersection



low accuracy



high accuracy

(computed with SpaceEx)

Operations on Convex Sets

Operators	Polyhedra		Zonotopes	Support F.
	Constraints	Vertices		
Convex hull	--	+	--	++
Affine transform	+/-	++	++	++
Minkowski sum	--	--	++	++
Intersection	+	--	--	-

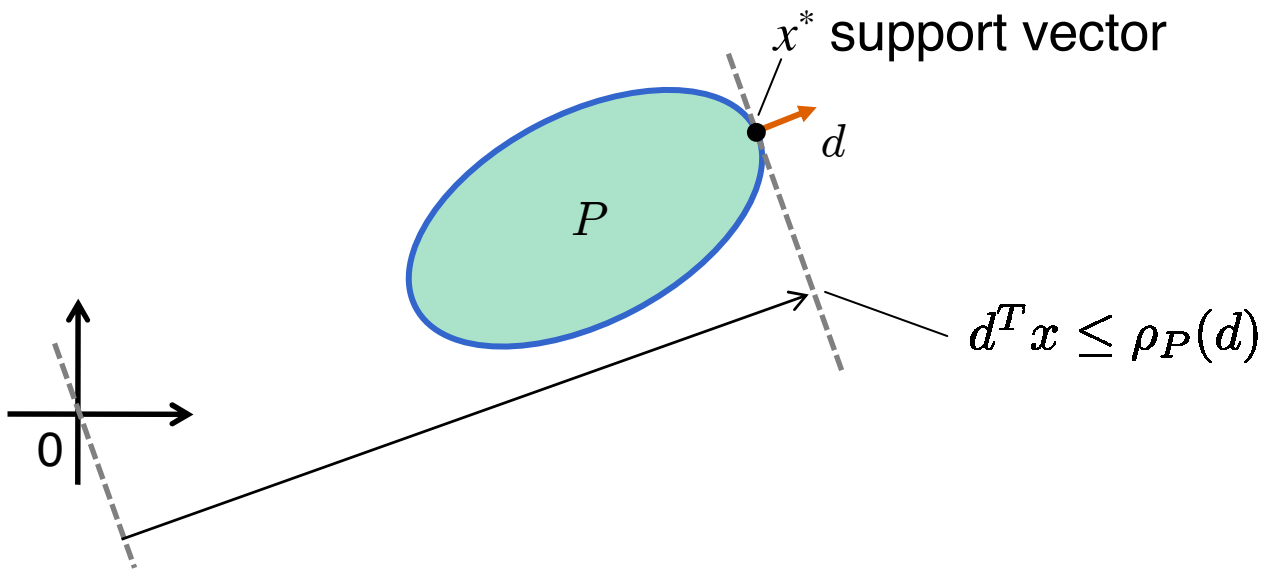
Le Guernic, Girard. CAV'09

Support Functions

- **Support Function** $R^n \rightarrow R$
  - direction d → position of supporting halfspace

$$\rho_P(d) \quad = \quad \max_{x \in P} d^T x$$

  - exact set representation

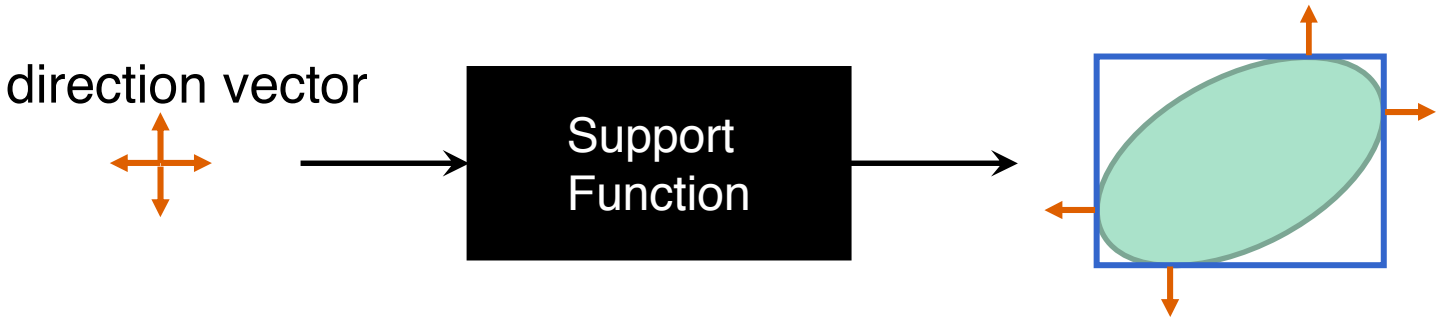


Support Functions

- **black box representation of a convex set**
- **implementation: function objects**

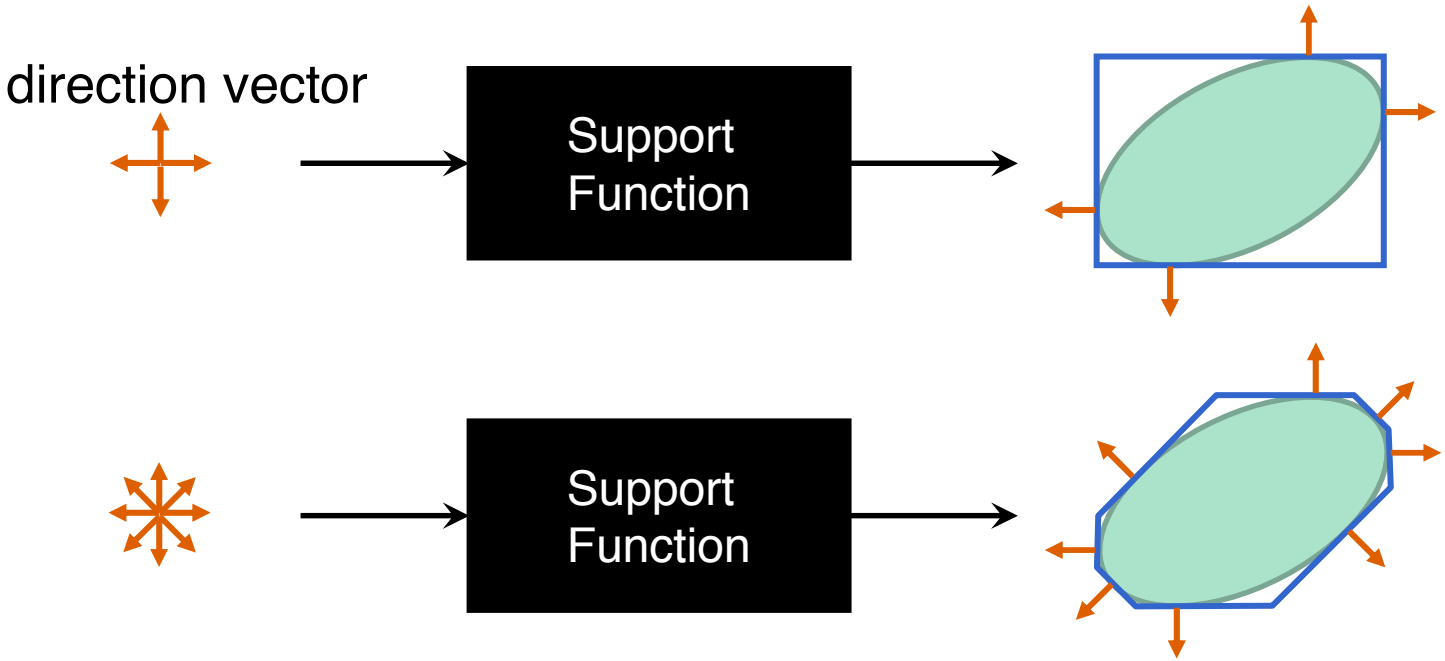
Support Functions

- **black box representation of a convex set**
- **implementation: function objects**



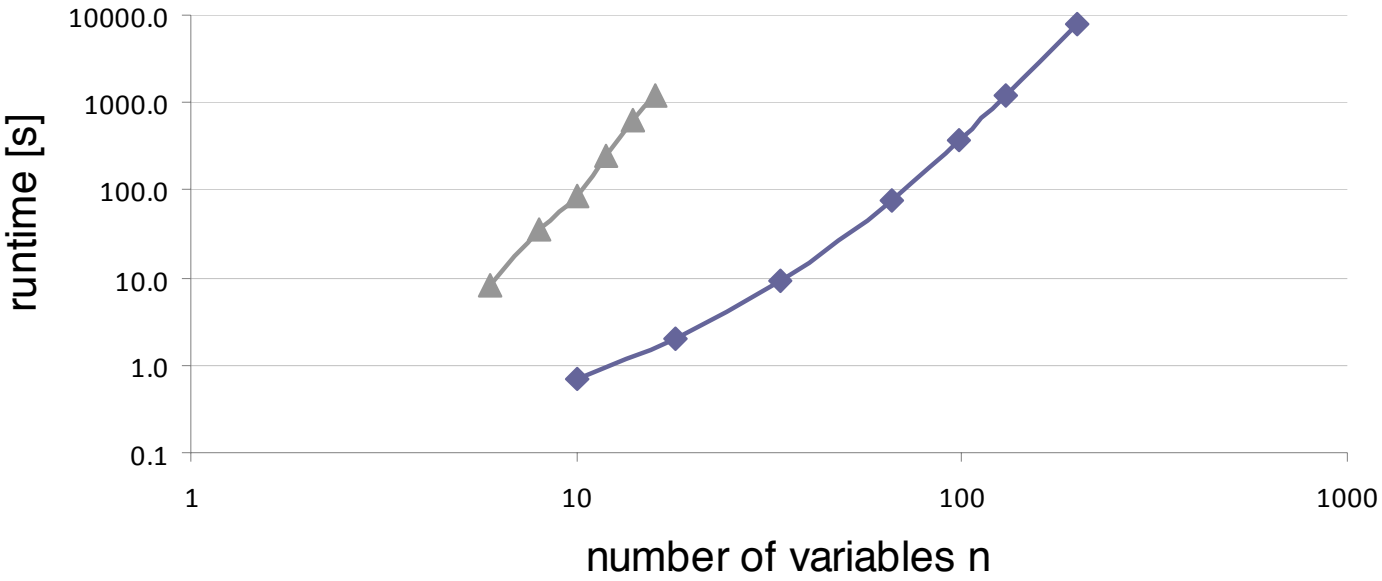
Support Functions

- **black box representation of a convex set**
- **implementation: function objects**



Example: Switched Oscillator

- **Scalability Measurements:**
  - fixpoint reached in $\mathrm{O}(nm^2)$ time
  - box constraints: $\mathrm{O}(n^3)$
  - octagonal constraints: $\mathrm{O}(n^5)$

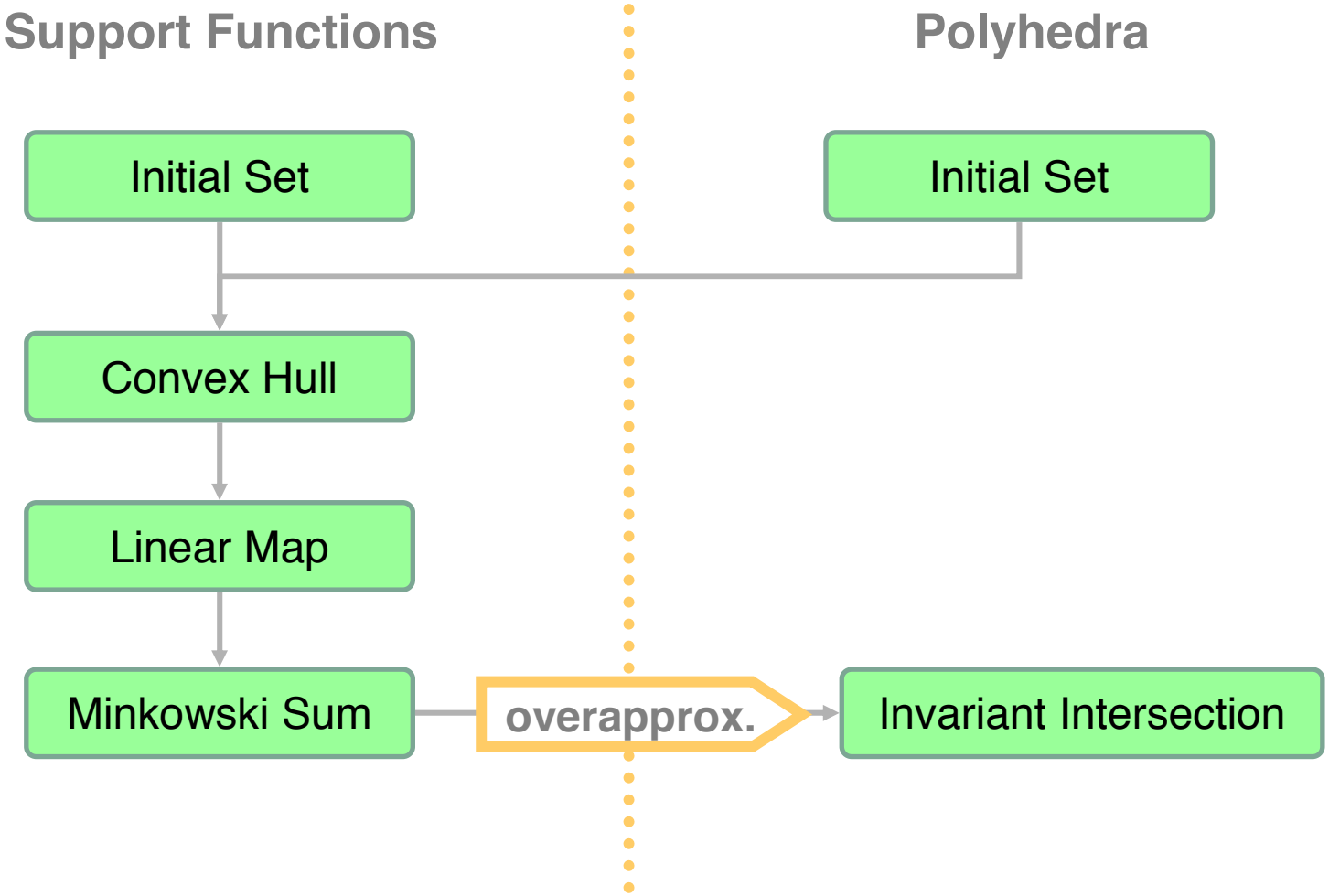


Reachability in High Dimensions

- **Scalability Trick 2:**

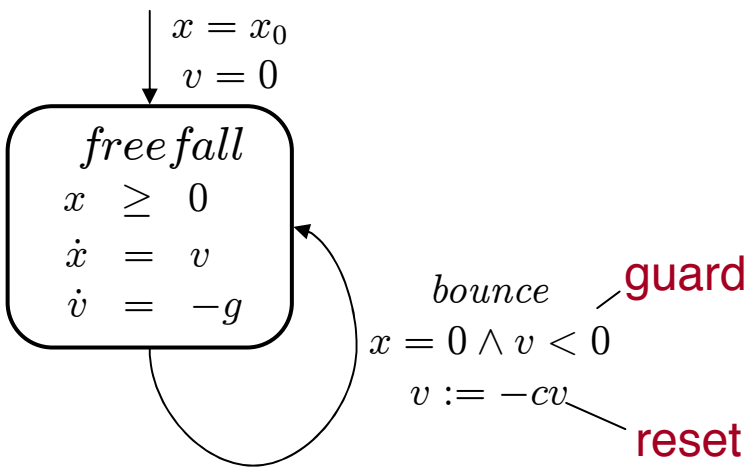
  Change data structures (data-dependent)

Computing Time Elapse

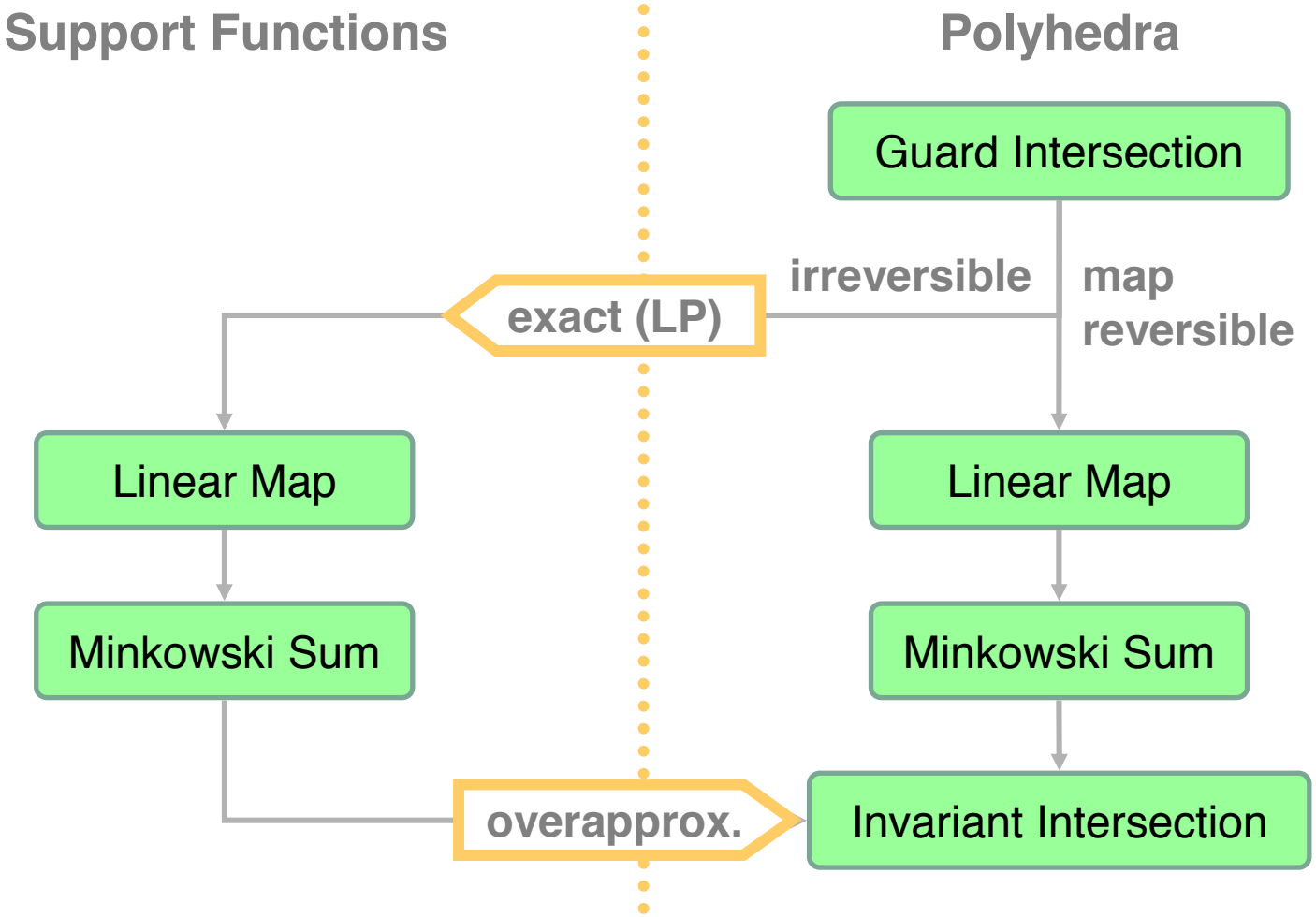


Computing Transition Successors

- **Intersection with guard**
  - use outer poly approximation
- **Linear map & Minkowski sum**
  - with polyhedra if invertible (map regular, input set a point)
  - otherwise use support functions
- **Intersection with target invariant**
  - use outer poly approximation



Computing Transition Successors

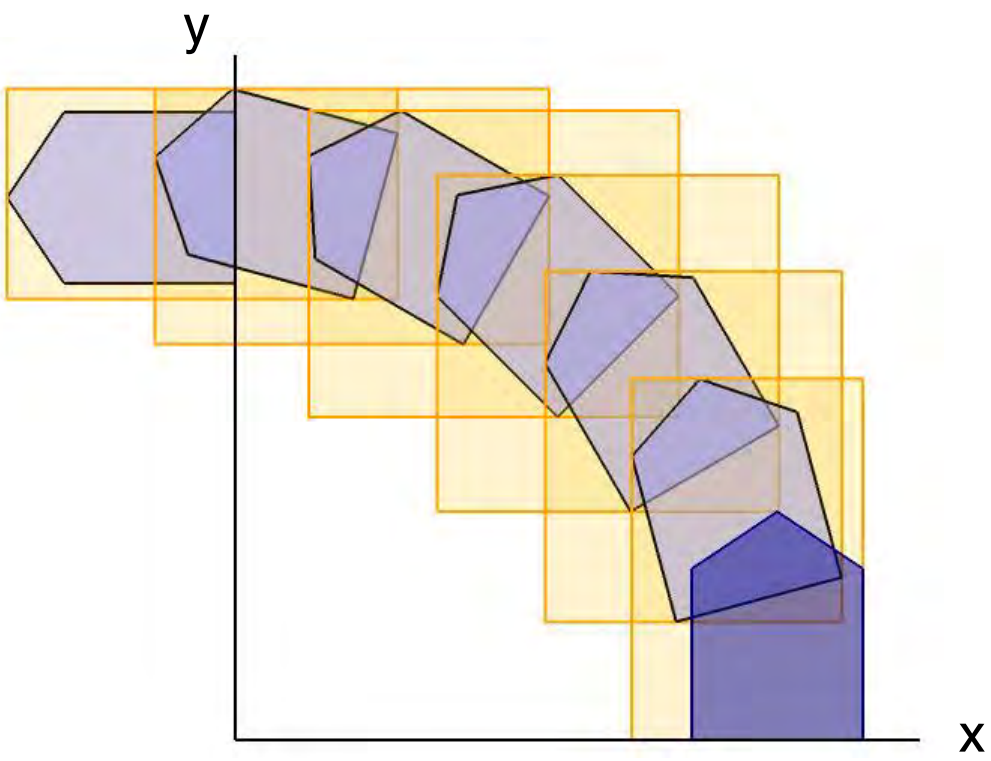


Reachability in High Dimensions

- **Scalability Trick 3:**

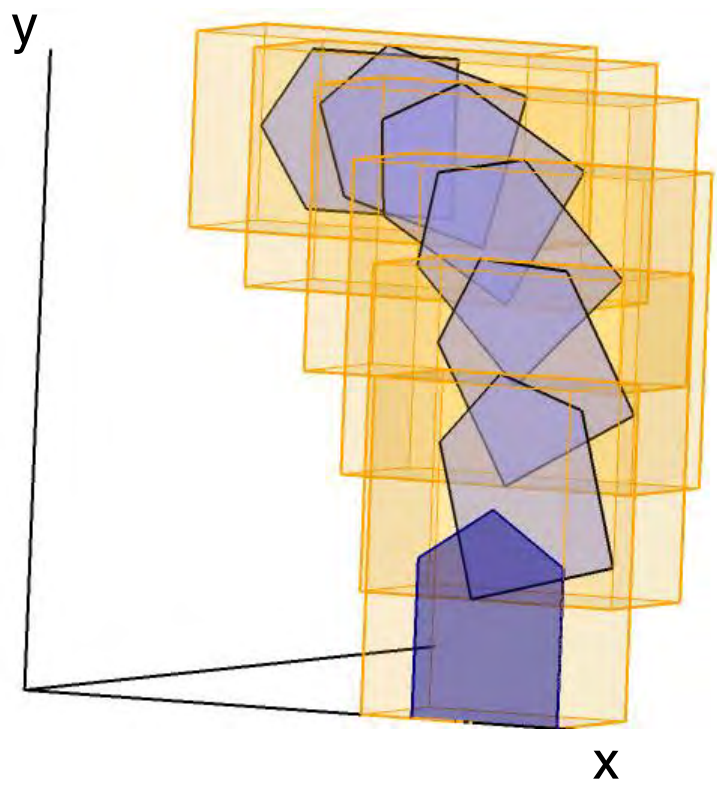
  Clustering and containment (in Space-Time)

Approximation in Space-Time

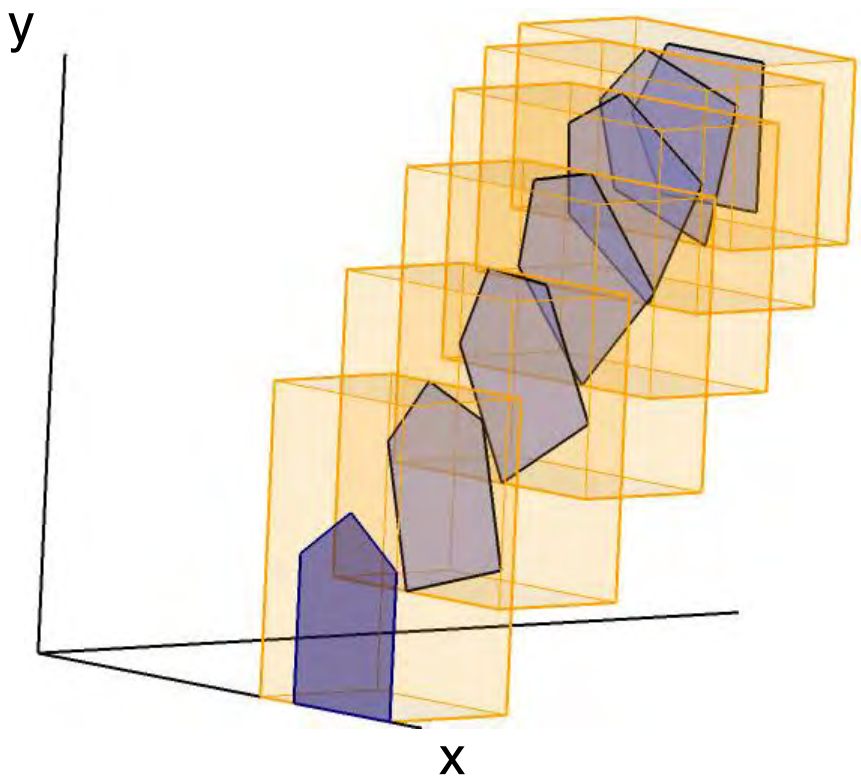


Improve the approximation by adding time...

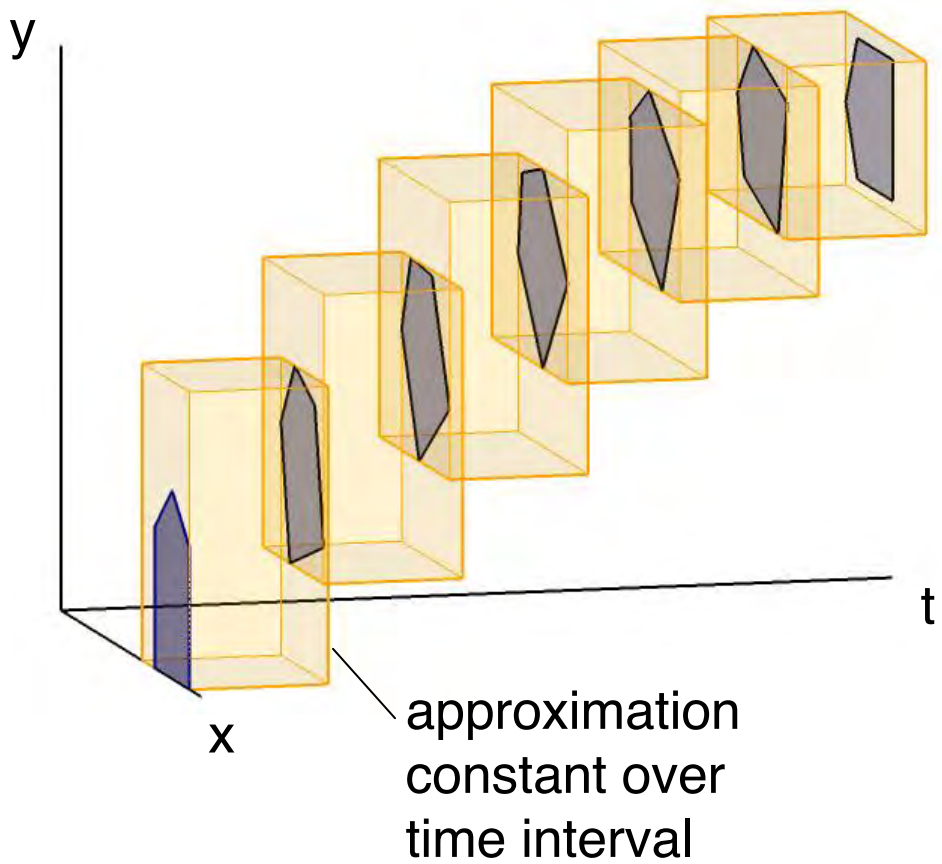
Approximation in Space-Time



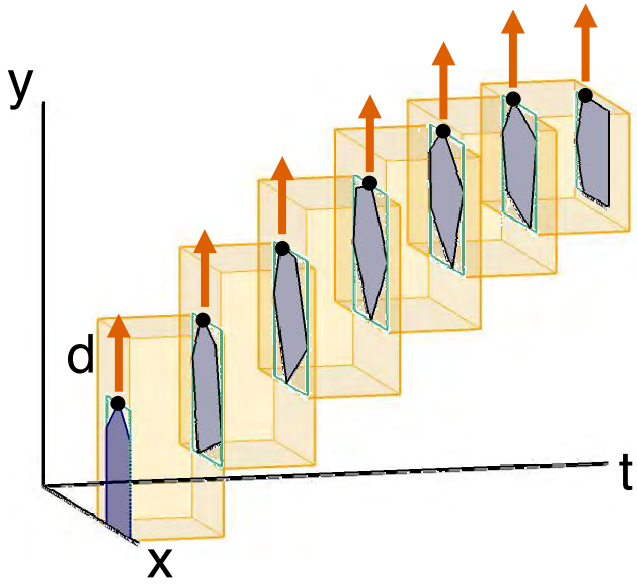
Approximation in Space-Time

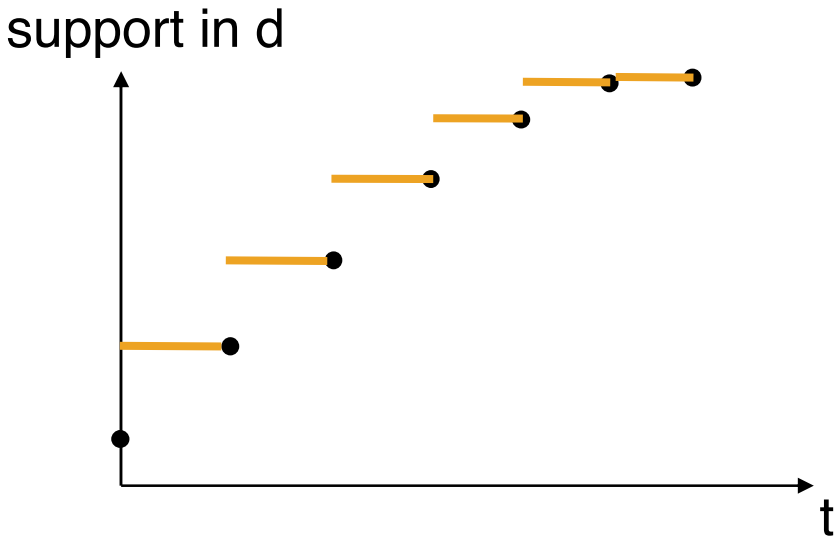


Approximation in Space-Time



Support Function over Time





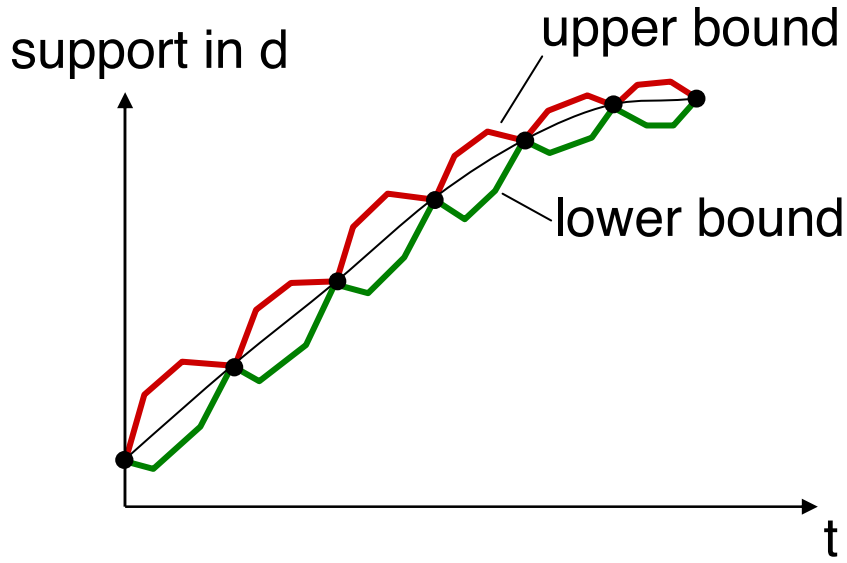
convex set per time interval =
piecewise constant scalar functions

Support Function over Time

- **1st order Taylor approx.**
  CAV'11

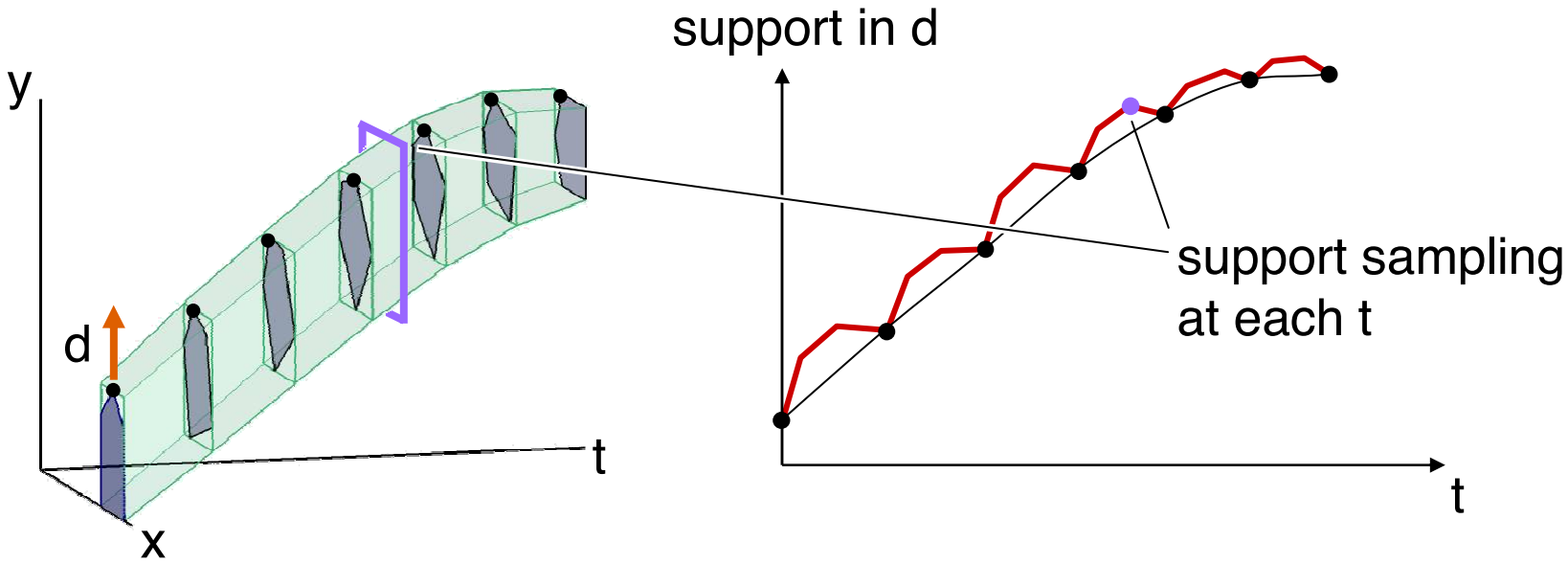
$$\begin{aligned}\Omega_t = (1-\tfrac{t}{\delta})\mathcal{X}_0 \oplus \tfrac{t}{\delta}e^{\delta A}\mathcal{X}_0 \\ \oplus\left(\tfrac{t}{\delta}\mathcal{E}_\Omega^+ \cap (1-\tfrac{t}{\delta})\mathcal{E}_\Omega^-\right) \\ \oplus t\mathcal{U} \oplus \tfrac{t^2}{\delta^2}\mathcal{E}_\Psi\end{aligned}$$

$$\begin{aligned}\Phi_2(A,\delta) &= A^{-2}\left(e^{\delta A} - I - \delta A\right) \\ \mathcal{E}_\Omega^+(\mathcal{X}_0,\delta) &= \boxdot\left(\Phi_2(|A|,\delta)\boxdot\left(A^2\mathcal{X}_0\right)\right), \\ \mathcal{E}_\Omega^-(\mathcal{X}_0,\delta) &= \boxdot\left(\Phi_2(|A|,\delta)\boxdot\left(A^2e^{\delta A}\mathcal{X}_0\right)\right), \\ \mathcal{E}_\Psi(\mathcal{U},\delta) &= \boxdot\left(\Phi_2(|A|,\delta)\boxdot\left(A\mathcal{U}\right)\right).\end{aligned}$$



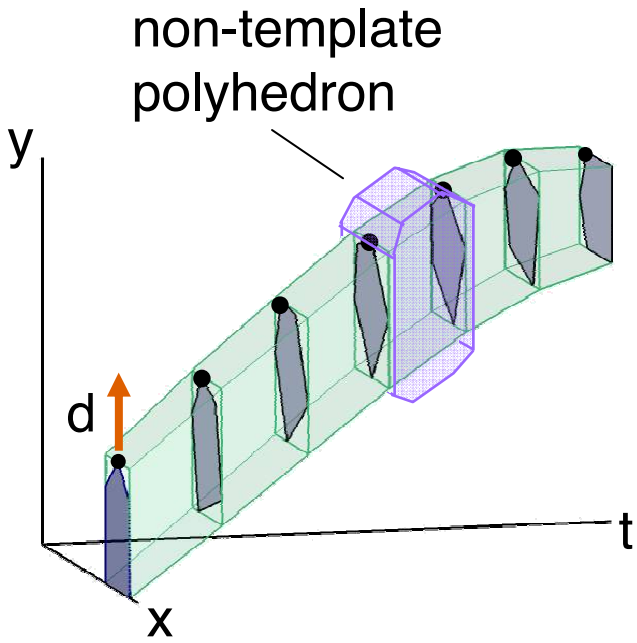
interpolation with
piecewise linear scalar functions

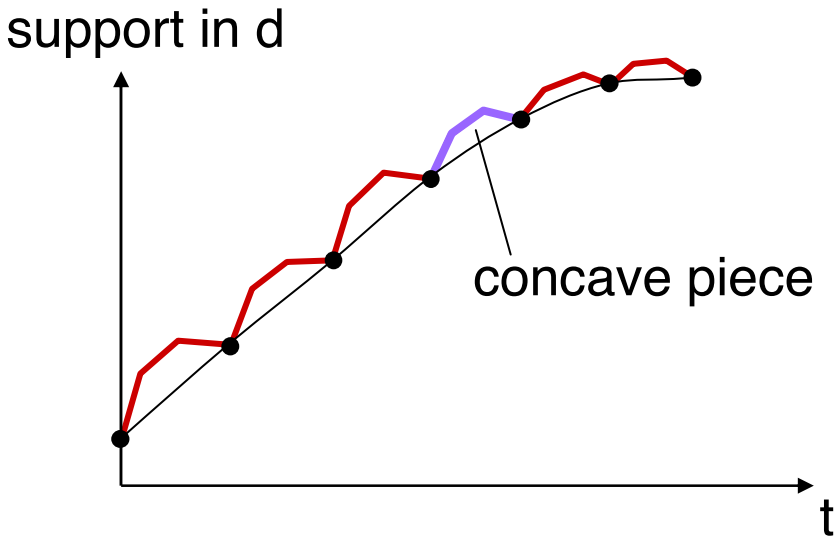
Support Function over Time



infinite union of template polyhedra
(one for each t)

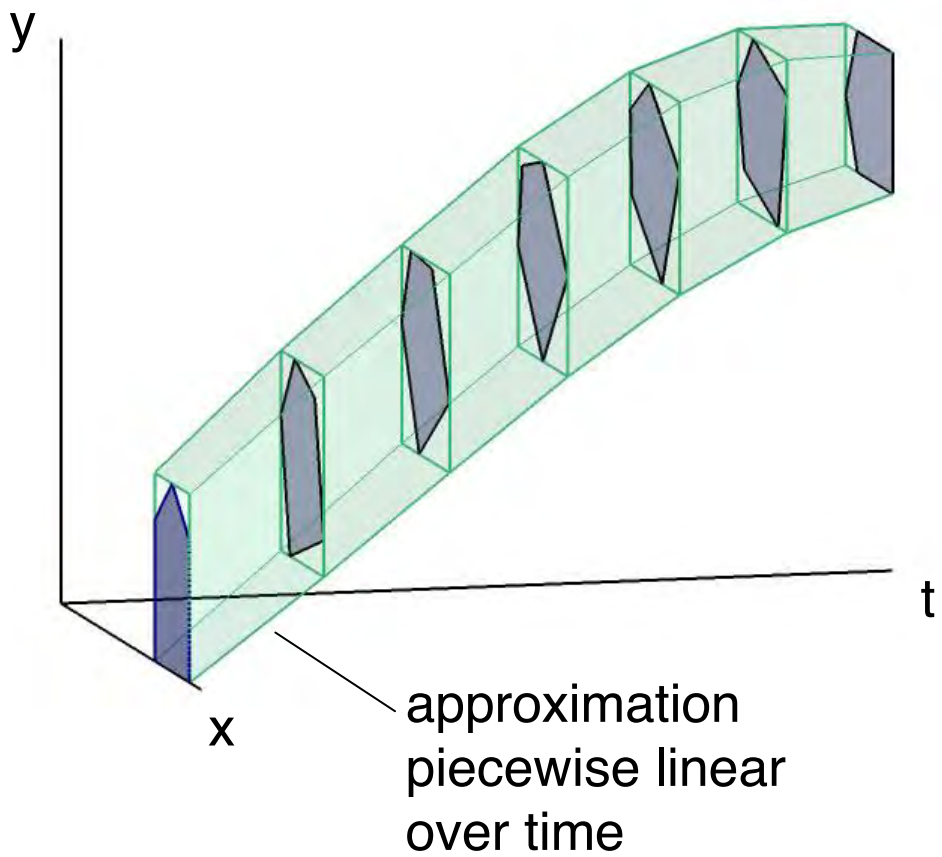
Convexification



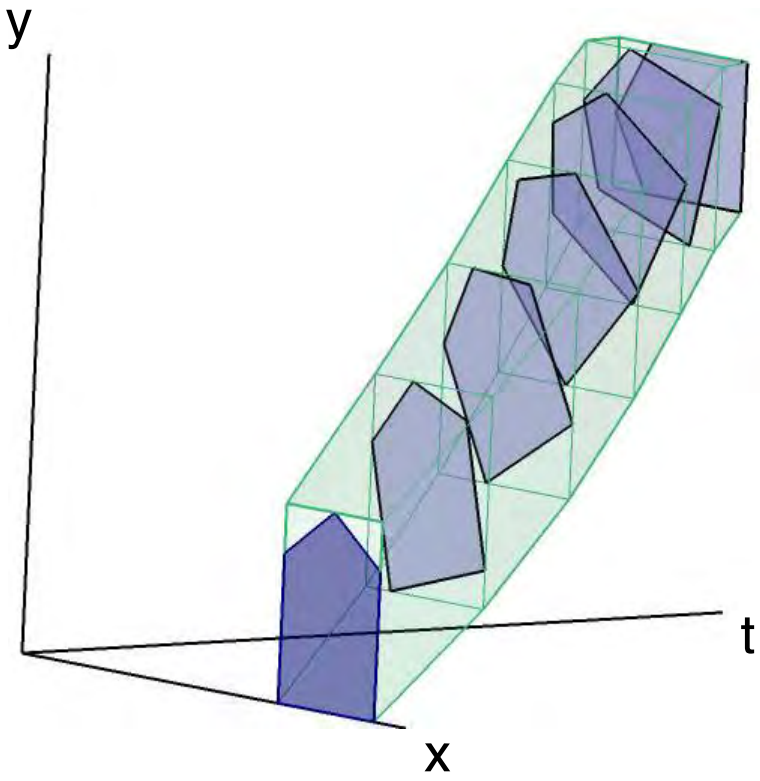


finite union of non-template polyhedra
(one for each concave piece)

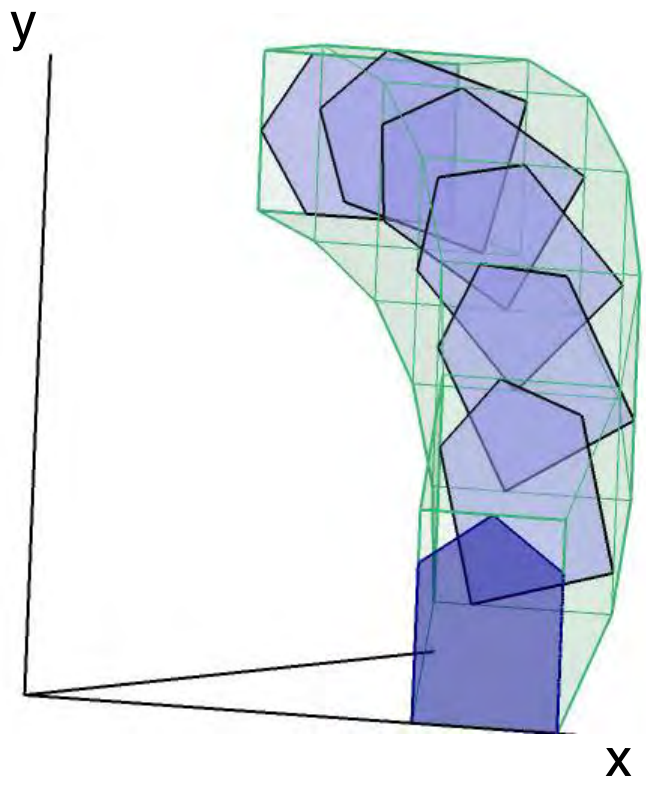
Approximation in Space-Time



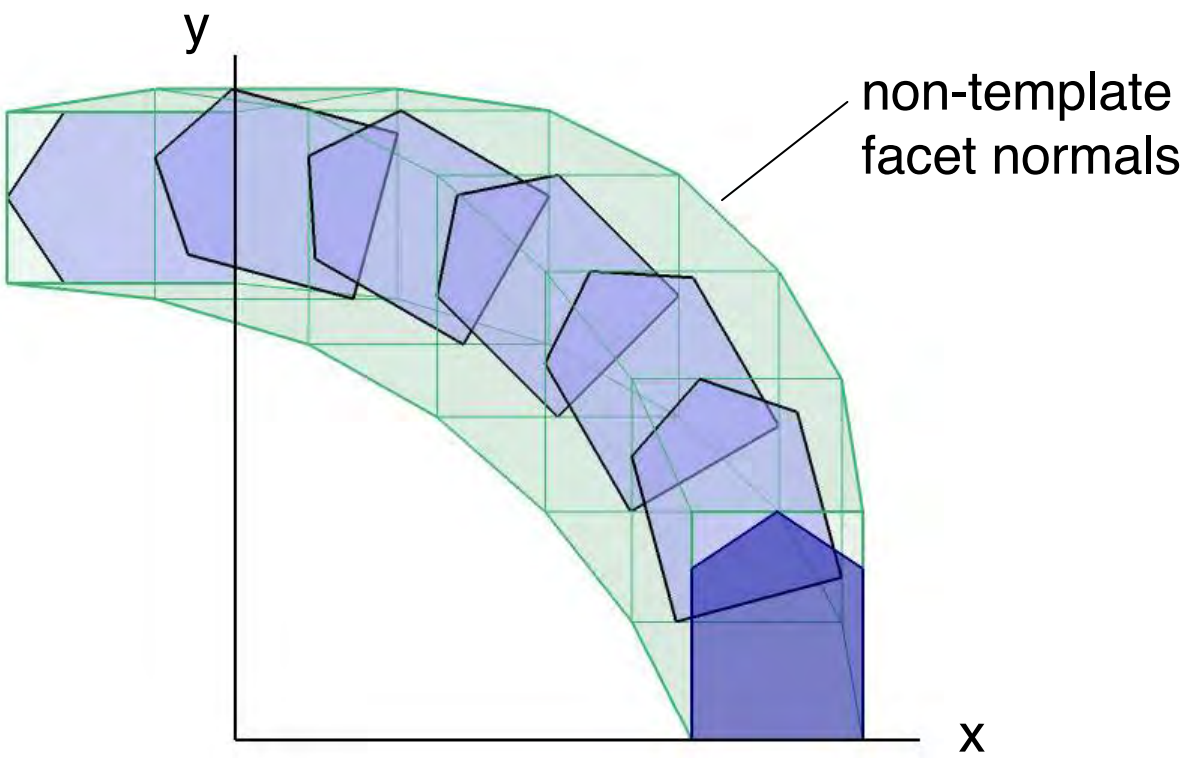
Approximation in Space-Time



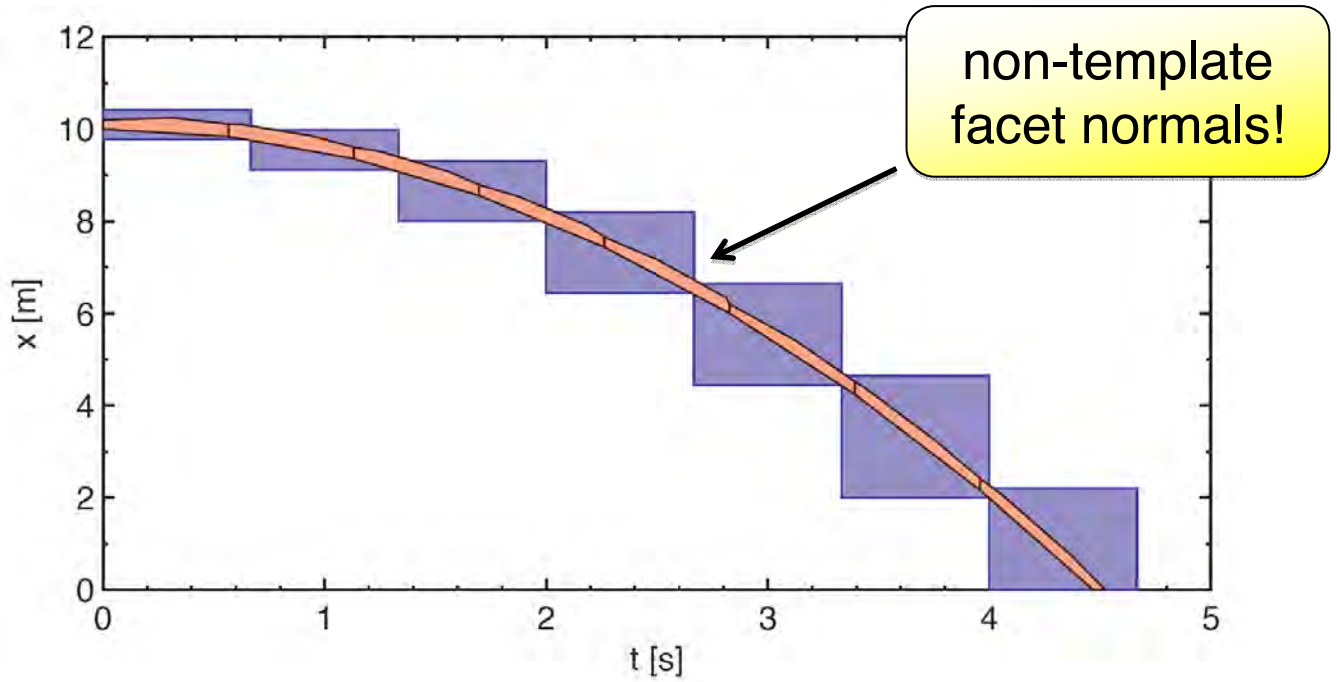
Approximation in Space-Time



Approximation in Space-Time

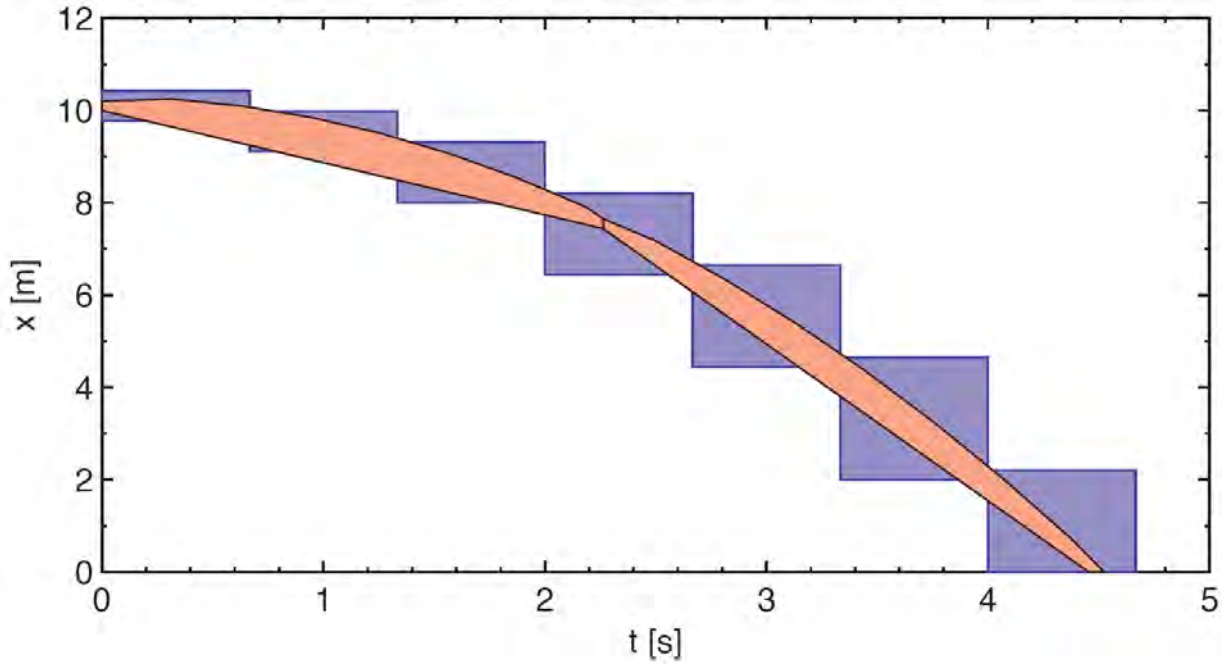


Example: Bouncing Ball



Clustering up to total error 0.1 = 8 pieces

Example: Bouncing Ball



Clustering up to total error 1.0 = 2 pieces

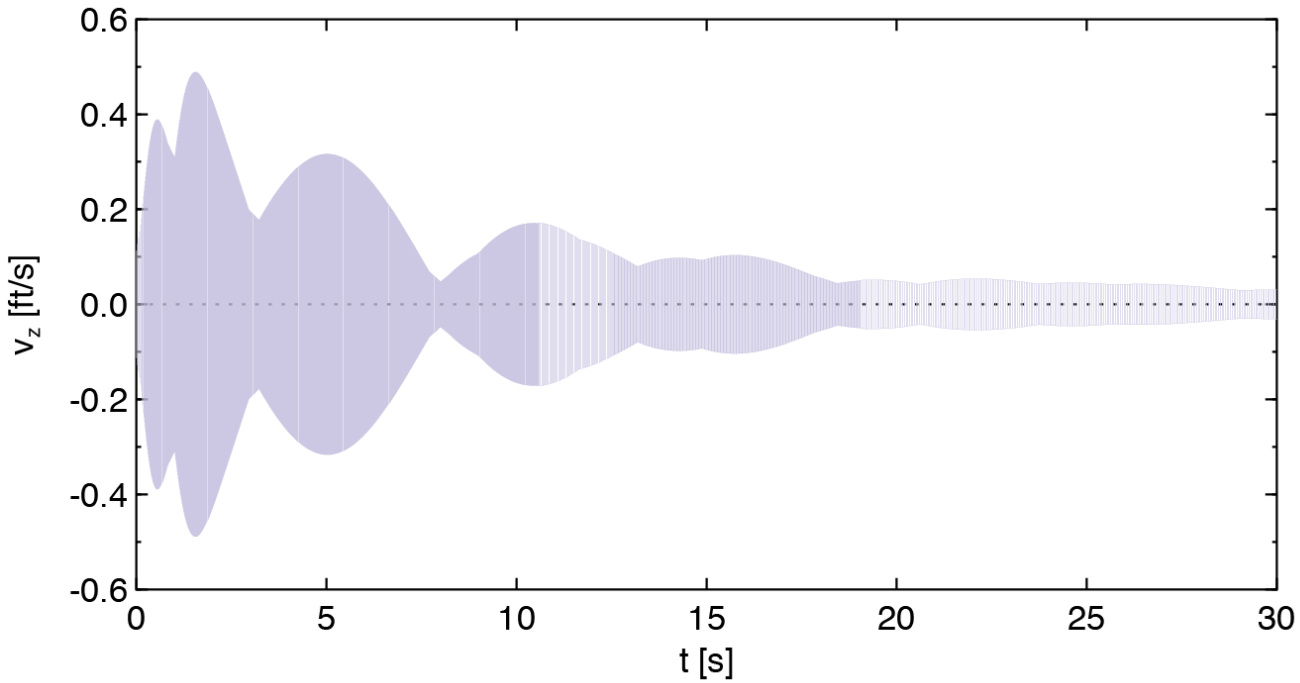
Example: Controlled Helicopter

- **28-dim model of a Westland Lynx helicopter**
  - 8-dim model of flight dynamics
  - 20-dim continuous H∞ controller for disturbance rejection
  - stiff, highly coupled dynamics

S. Skogestad and I. Postlethwaite, Multivariable Feedback Control: Analysis and Design. John Wiley & Sons, 2005.

Example: Helicopter

- **28 state variables + clock**

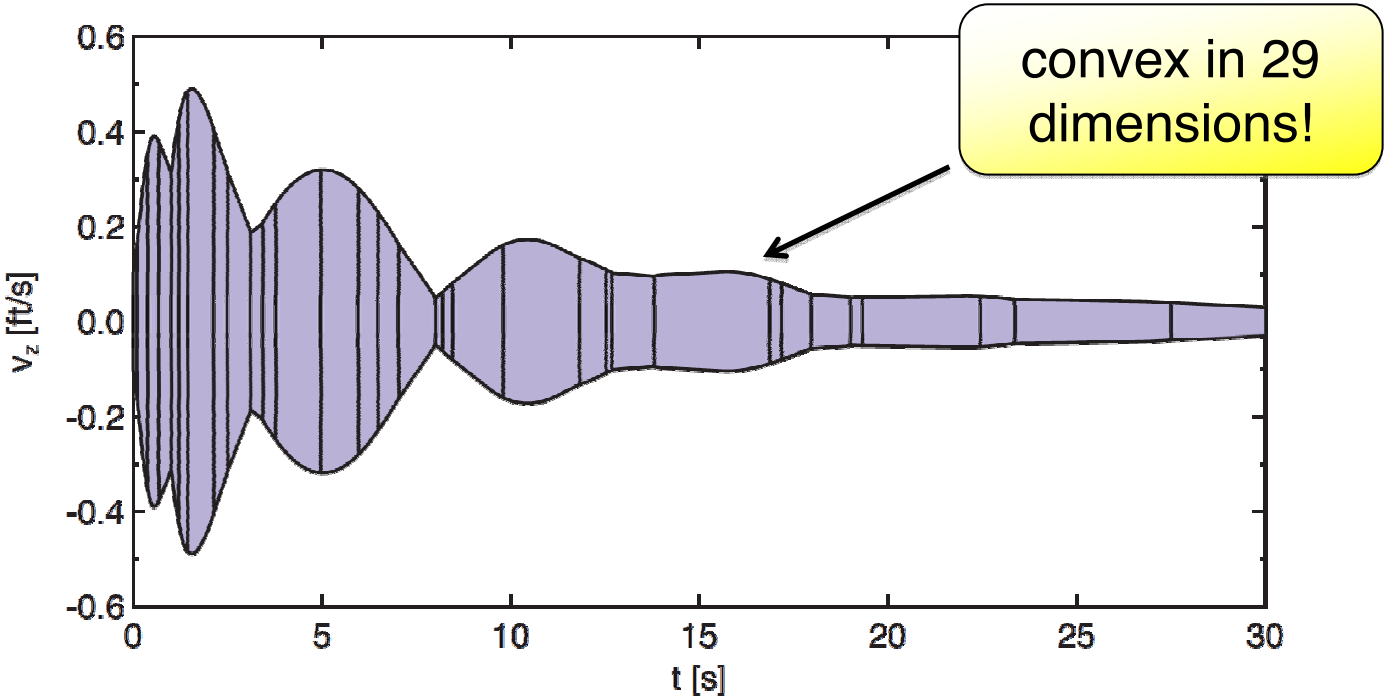


CAV'11: 1440 sets in 5.9s

1440 time steps

Example: Helicopter

- **28 state variables + clock**

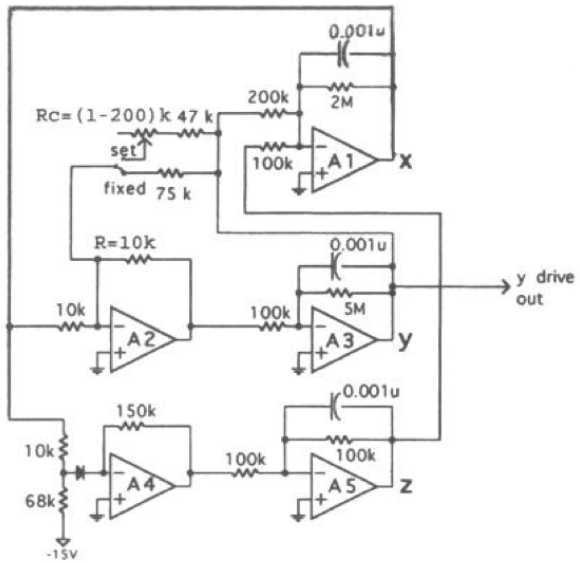


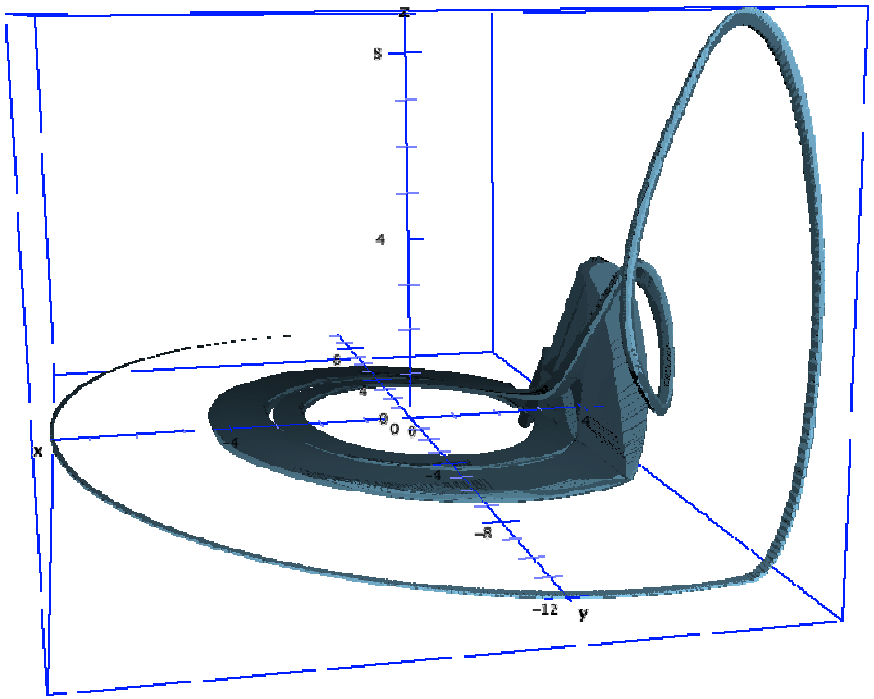
HSCC'13: **32** sets in 15.2s (4.8s clustering)

2 -- 3300 time steps, median 360

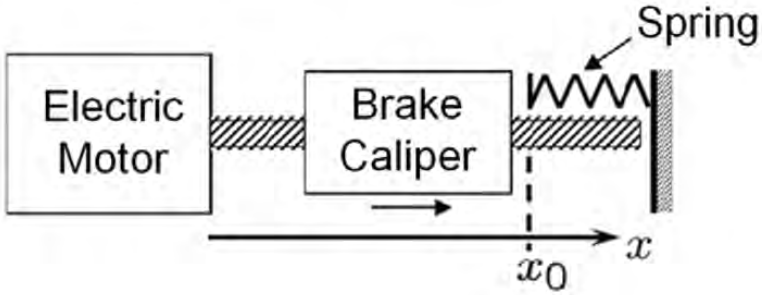
Example: Chaotic Circuit

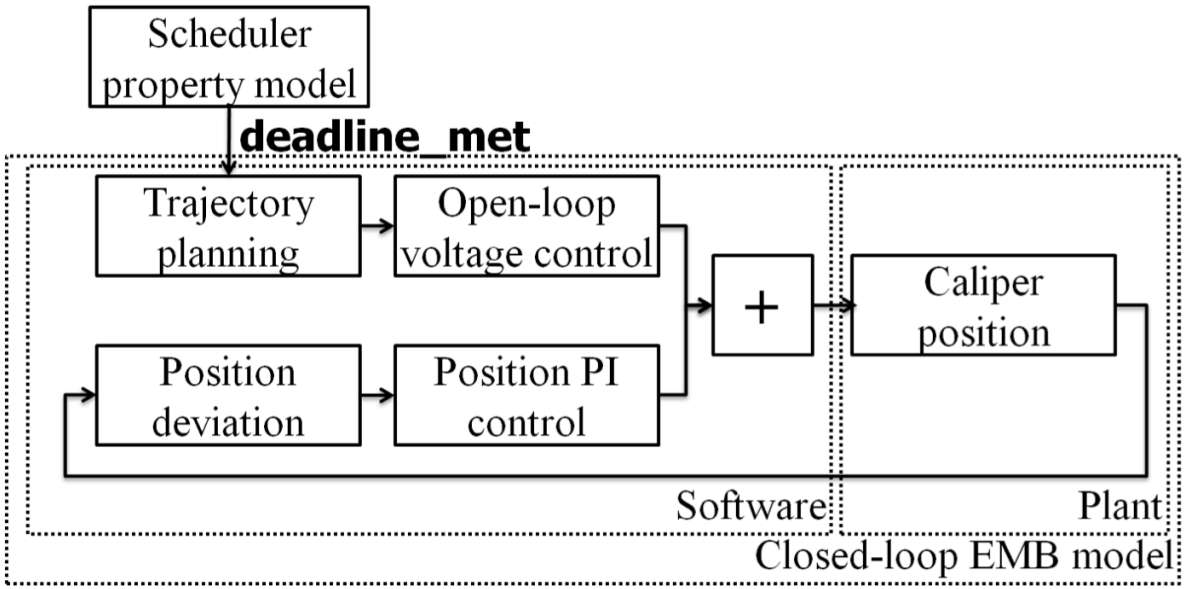
- **piecewise linear Rössler-like circuit**
  Pisarchik, Jaimes-Reátegui. ICCSDS'05
- **added nondet. disturbances**
- **3 variables, hard!**





Case Study: Electro-Mechanical Brake

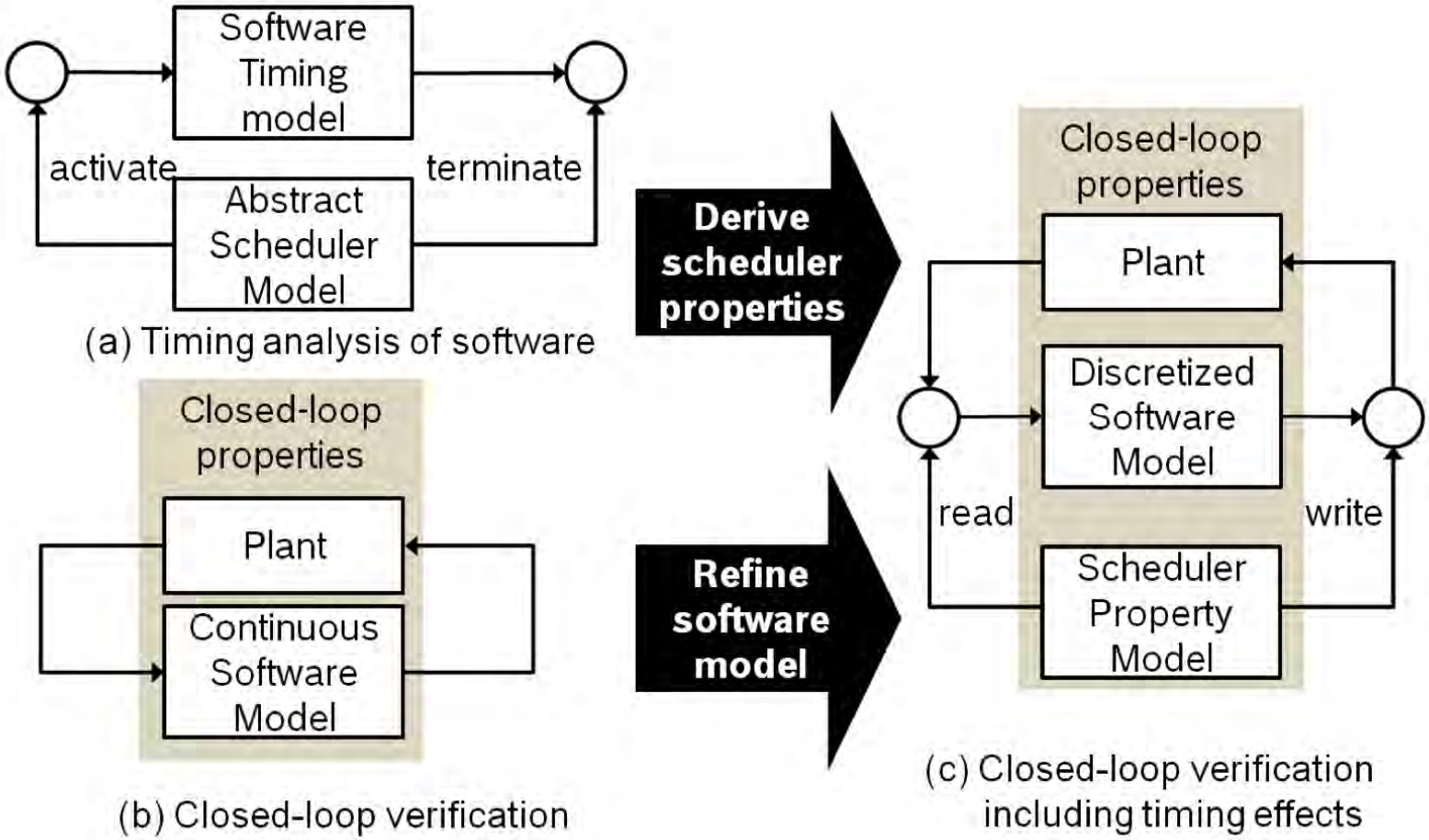




Case Study: Electro-Mechanical Brake

- **Controller Implementation**
  - discrete time
  - fixed-point arithmetic
  - multi-tasking processor: **scheduling with uncertain frequency**
  - worst-case analysis too conservative

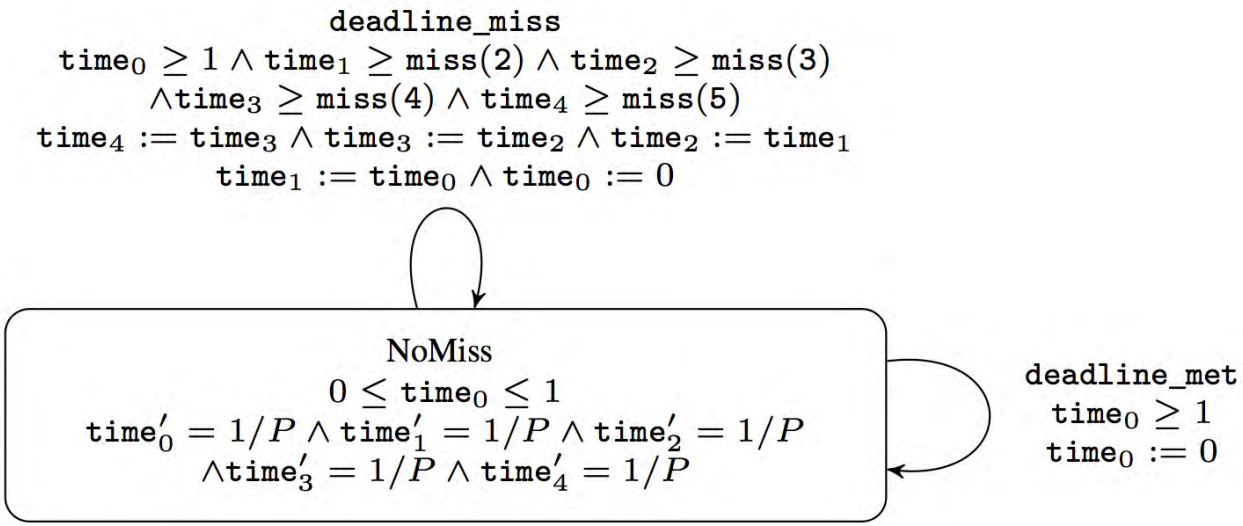
Case Study: Electro-Mechanical Brake



Case Study: Electro-Mechanical Brake

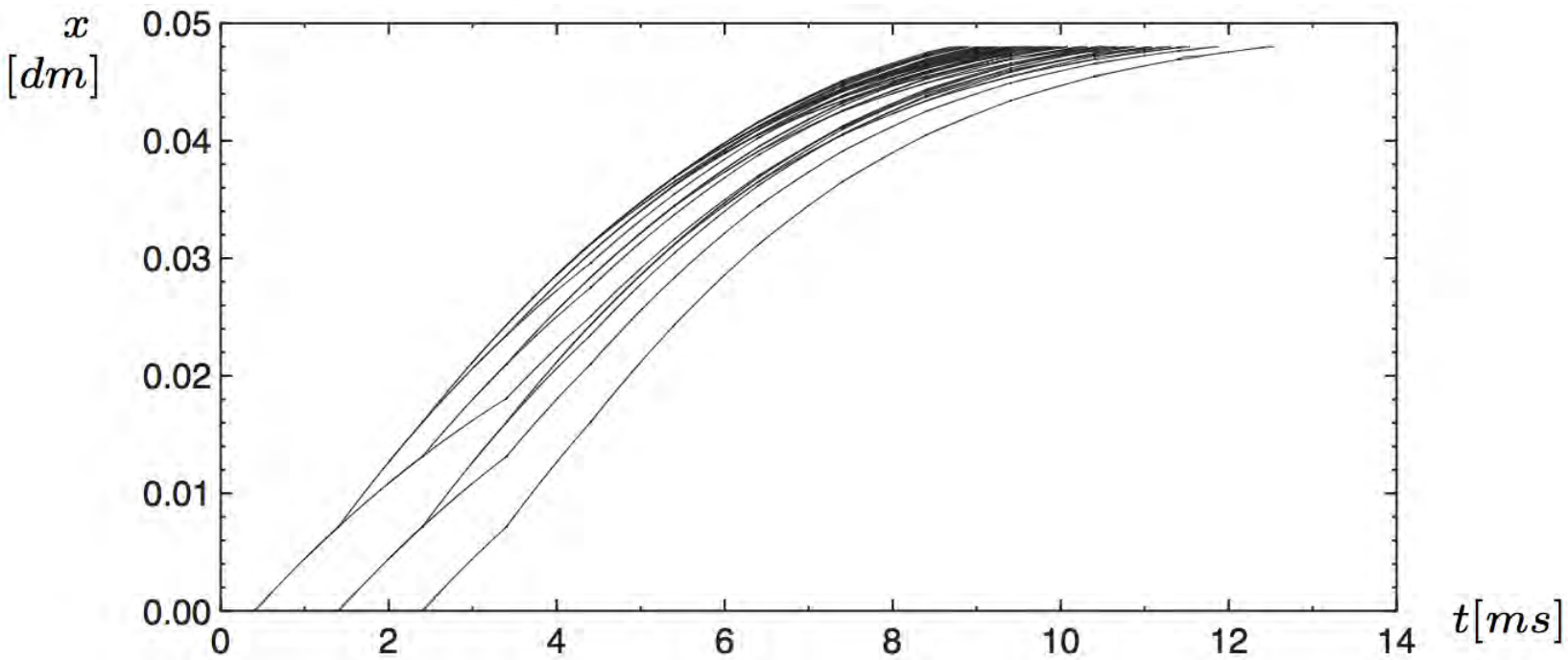
- **Typical Worst-Case Execution Time**
  - limit missed schedules per time interval

# deadline misses	consecutive executions
2	2
3	18
4	20
5	56



Case Study: Electro-Mechanical Brake

caliper position

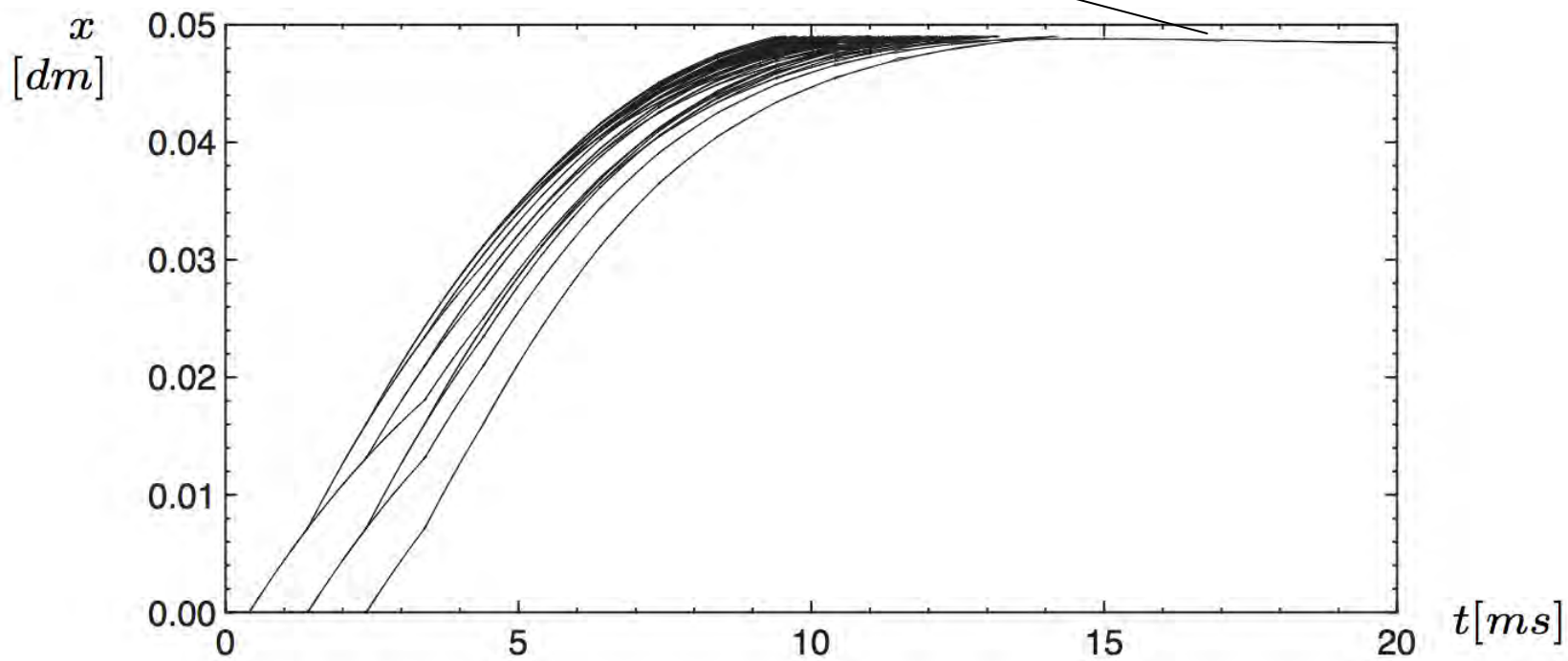


time

Case Study: Electro-Mechanical Brake

caliper position

only failure – hard to detect

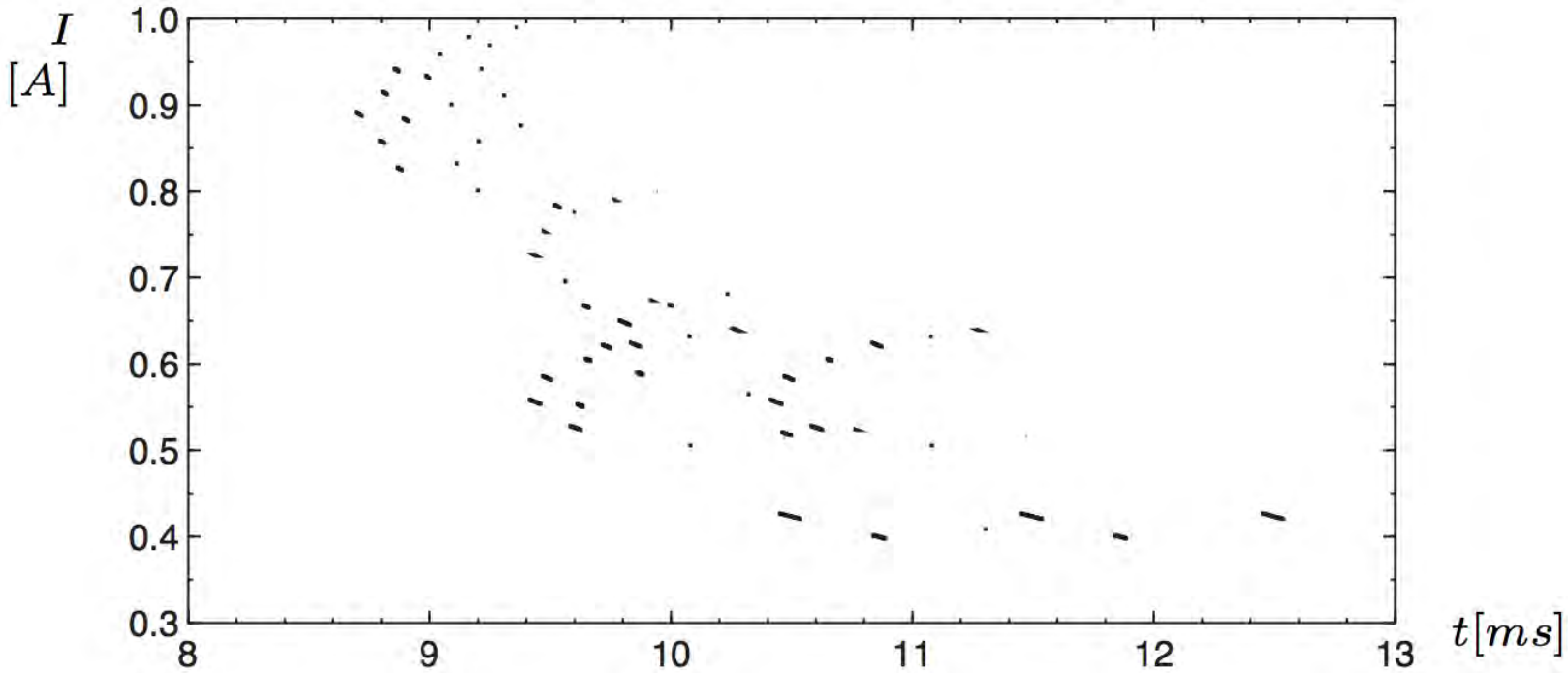


time

artificial failure case
(inconsistent with classical theory)

Case Study: Electro-Mechanical Brake

current



time

physical properties: maximum impulse on contact (measured via current)

Outline

- Modeling with Hybrid Automata
- Reachability versus Simulation
- Computing with High-Dimensional Sets
- **SpaceEx Verification Platform**

SpaceEx Verification Platform

SpaceEx State Space Explorer

Home | About SpaceEx | Documentation | Run SpaceEx | Downloads | Contact

Model | Specification | Options | Output | Advanced

Model editor: Download

Model file: Browse...

Configuration file: Load Save

User input file: User file

Examples:
- Bouncing Ball (.xml, .cfg)
- Timed Bouncing Ball (.xml, .cfg)
- Nondet. Bouncing Ball (.xml, .cfg)
- Circle (.xml, .cfg)
- Filtered Oscillator 6 (.xml, .cfg)
- Filtered Oscillator 18 (.xml, .cfg)
- Filtered Oscillator 34 (.xml, .cfg)

A filtered oscillator.
Same as the 6-variable filtered oscillator, but with a higher order filter. With 34 state variables, an analysis with octagonal constraints is no longer practical, since this requires 2*34^2=2312 constraints to be computed at every time step. The analysis with 2*34=68 box constraints remains cheap.

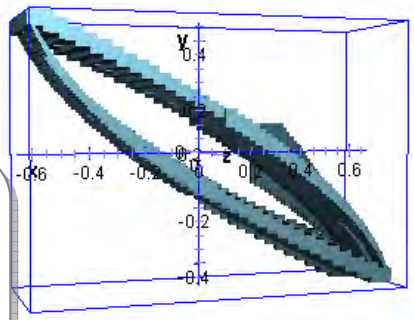
Console

```
Iteration 6... 8 sym states passed, 1 waiting 0.457s
Iteration 7... 9 sym states passed, 1 waiting 0.941s
Iteration 8... 10 sym states passed, 1 waiting 0.434s
Iteration 9... 11 sym states passed, 1 waiting 0.936s
Iteration 10... 12 sym states passed, 1 waiting 0.457s
Iteration 11... 13 sym states passed, 1 waiting 0.929s
Iteration 12... 14 sym states passed, 1 waiting 0.455s
Iteration 13... 14 sym states passed, 0 waiting 0.917s
Found fixpoint after 14 iterations.
Computing reachable states done after 10.058s
Output of reachable states... 0.823s
```

Reports

11.05s elapsed
29516KB memory
SpaceEx output file : output (jvx).

Graphics

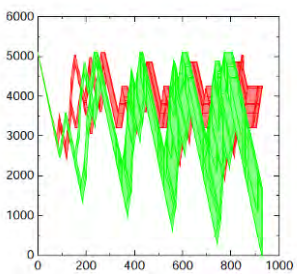


Browser-based GUI

–2D/3D output

–runs remotely

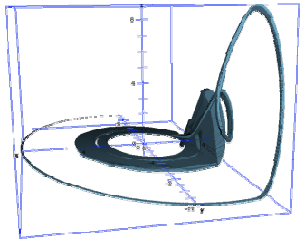
SpaceEx Reachability Algorithms



PHAVer

–constant dynamics (LHA)

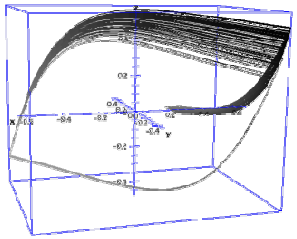
–formally sound and exact



Support Function Algo

–many continuous variables

–low discrete complexity

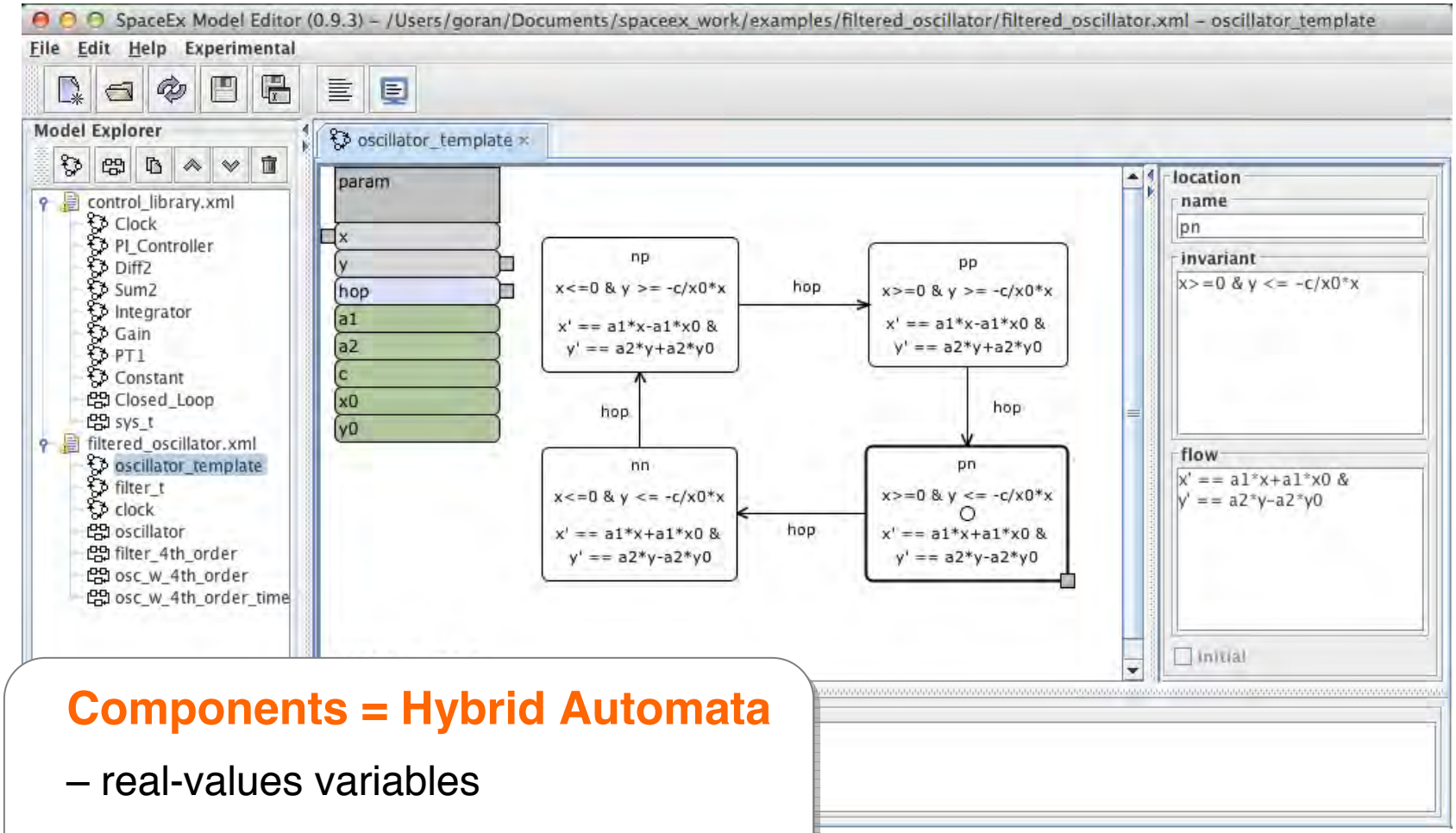


Simulation

–nonlinear dynamics

–based on CVODE

SpaceEx Model Editor

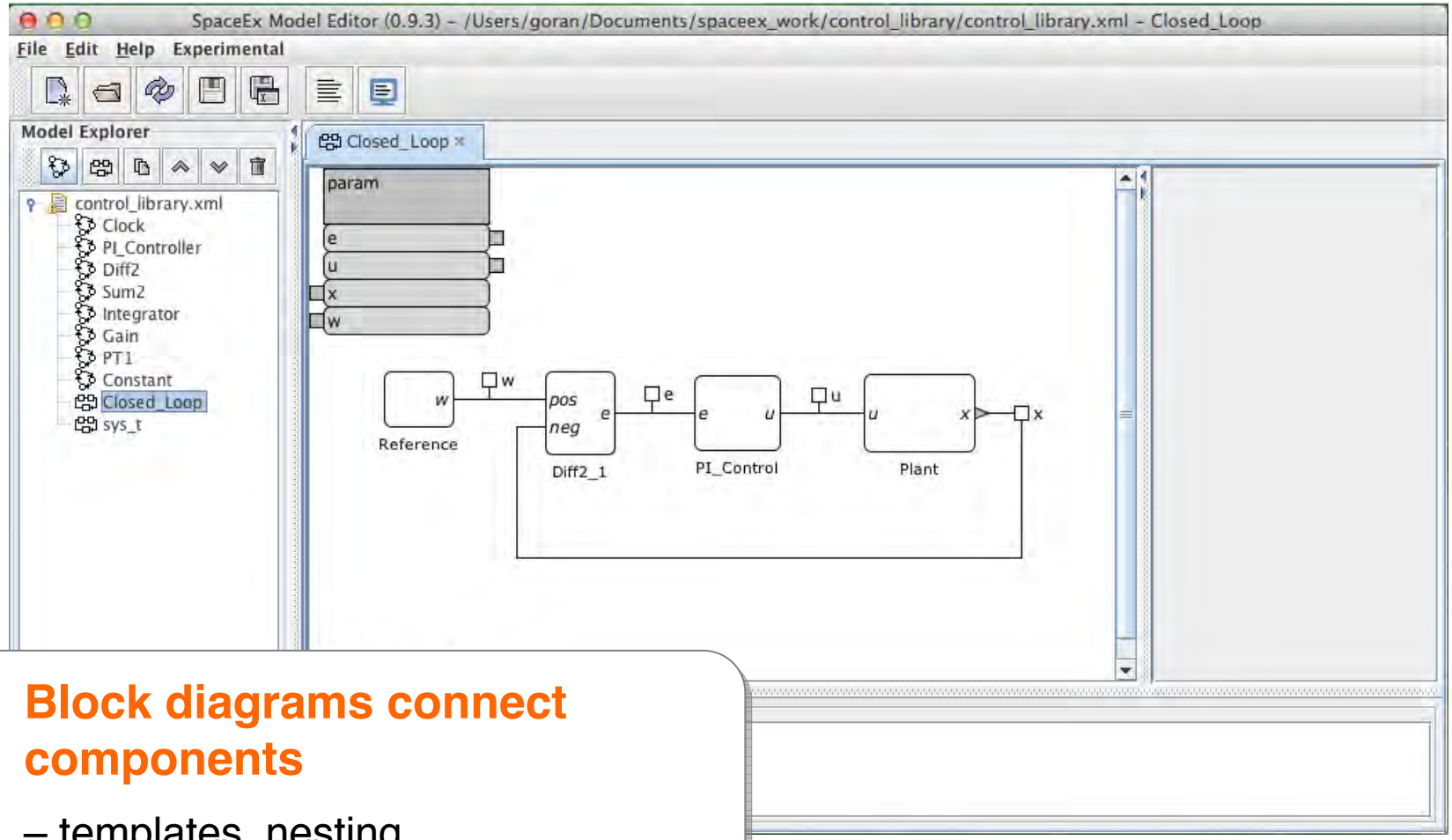


Components = Hybrid Automata

– real-values variables

– ODE, linear DAE

SpaceEx Model Editor



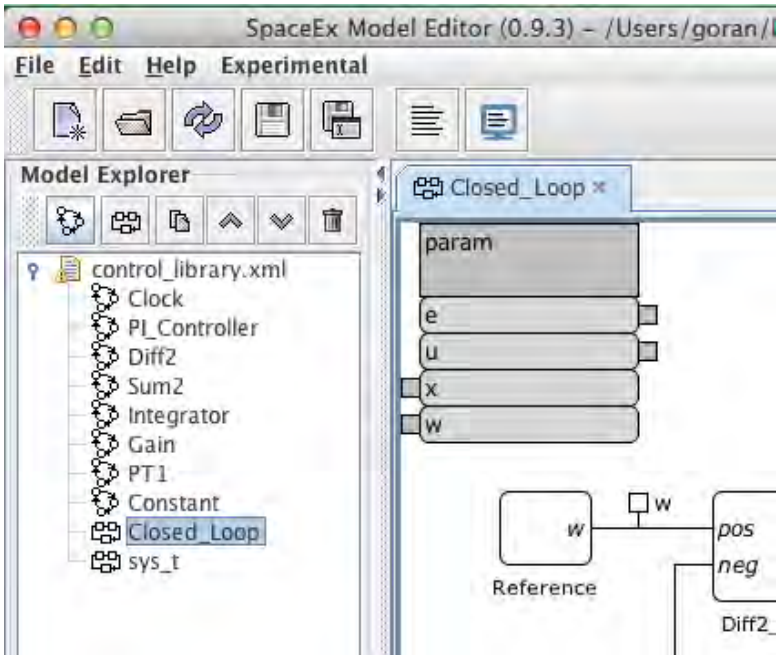
Block diagrams connect components

– templates, nesting

Control System Models

- **1-to-1 correspondence with standard block diagrams**
- **library of standard control system blocks**

- **Carnot Project 2014: semi-automatic translation from Matlab/Simulink to SpaceEx**



Conclusions

- **Reachability with 100+ variables**
  - convex sets as support functions
- **Convexification with semi-template data structures**
  - total approximation error measurable

- **Ongoing Work**
  - abstraction refinement (directions) - HSCC'15
  - extension to nonlinear dynamics

spaceex.imag.fr