Reachability of Hybrid Systems in Space-Time

Goran Frehse, Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel, Rajat Kateja, Manish Goyal, Rodolfo Ripado, Thao Dang, Oded Maler
Université Grenoble 1 Joseph Fourier / CNRS – Verimag, France

Colas Le Guernic
DGA, France

Antoine Girard
Laboratoire Jean Kuntzmann, France

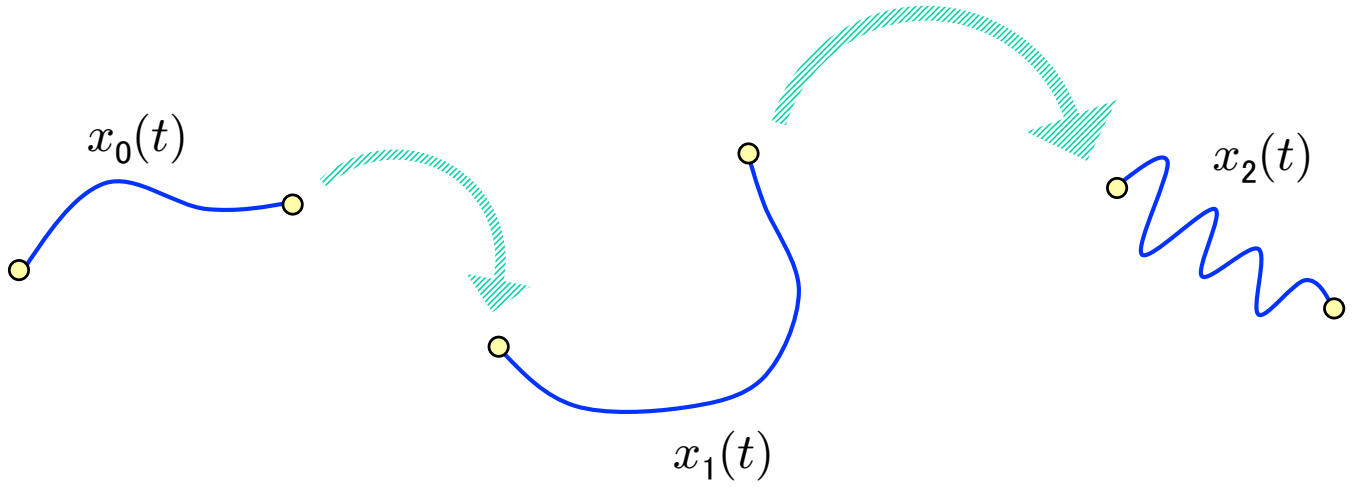
DREAM Seminar, Berkeley, May 7, 2013

Outline

- **Hybrid Systems and Reachability**
- **Reachability with Support Functions**
  - Computing with High-Dimensional Sets
- **Approximation in Space-Time**
  - Reducing the Number of Sets
  - Measuring the Approximation Error
- **SpaceEx Development Platform**

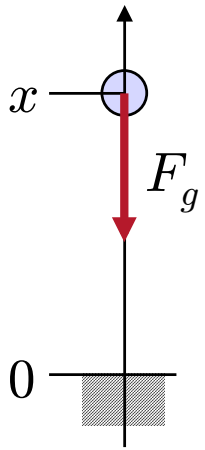
Hybrid Systems - Semantics

- **Continous/Discrete Behaviour**
  - evolution with time according to ODE dynamics
  - dynamics can switch (instantaneous)
  - state can jump (instantaneous)

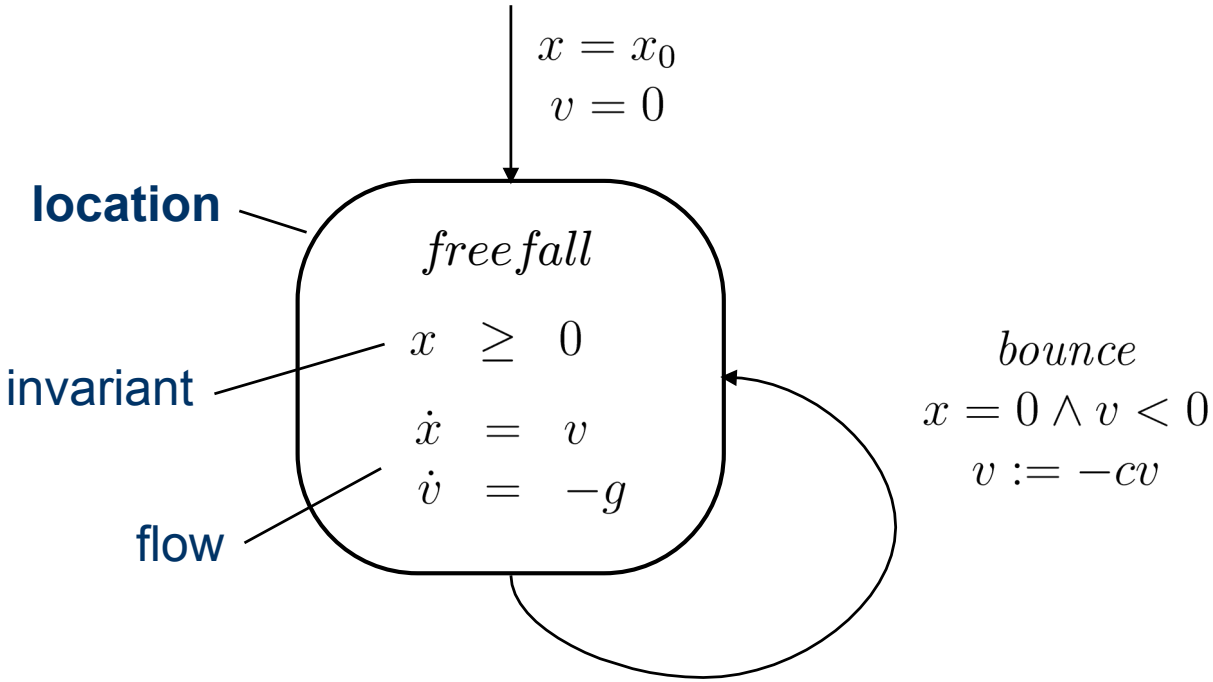


Modeling Hybrid Systems

- **Example: Bouncing Ball**
  - ball with mass m and position x in free fall
  - bounces when it hits the ground at $x = 0$
  - initially at position x_0 and at rest

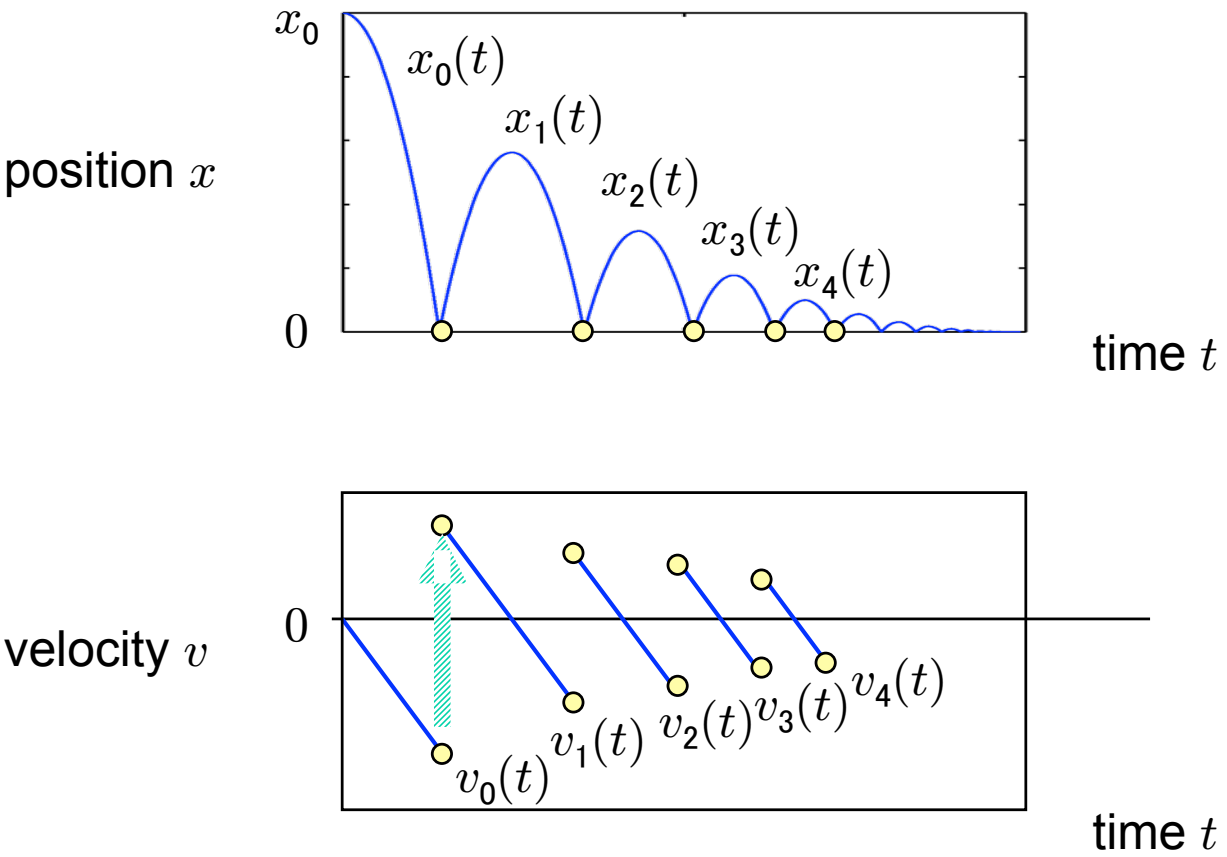


Hybrid Automaton Model



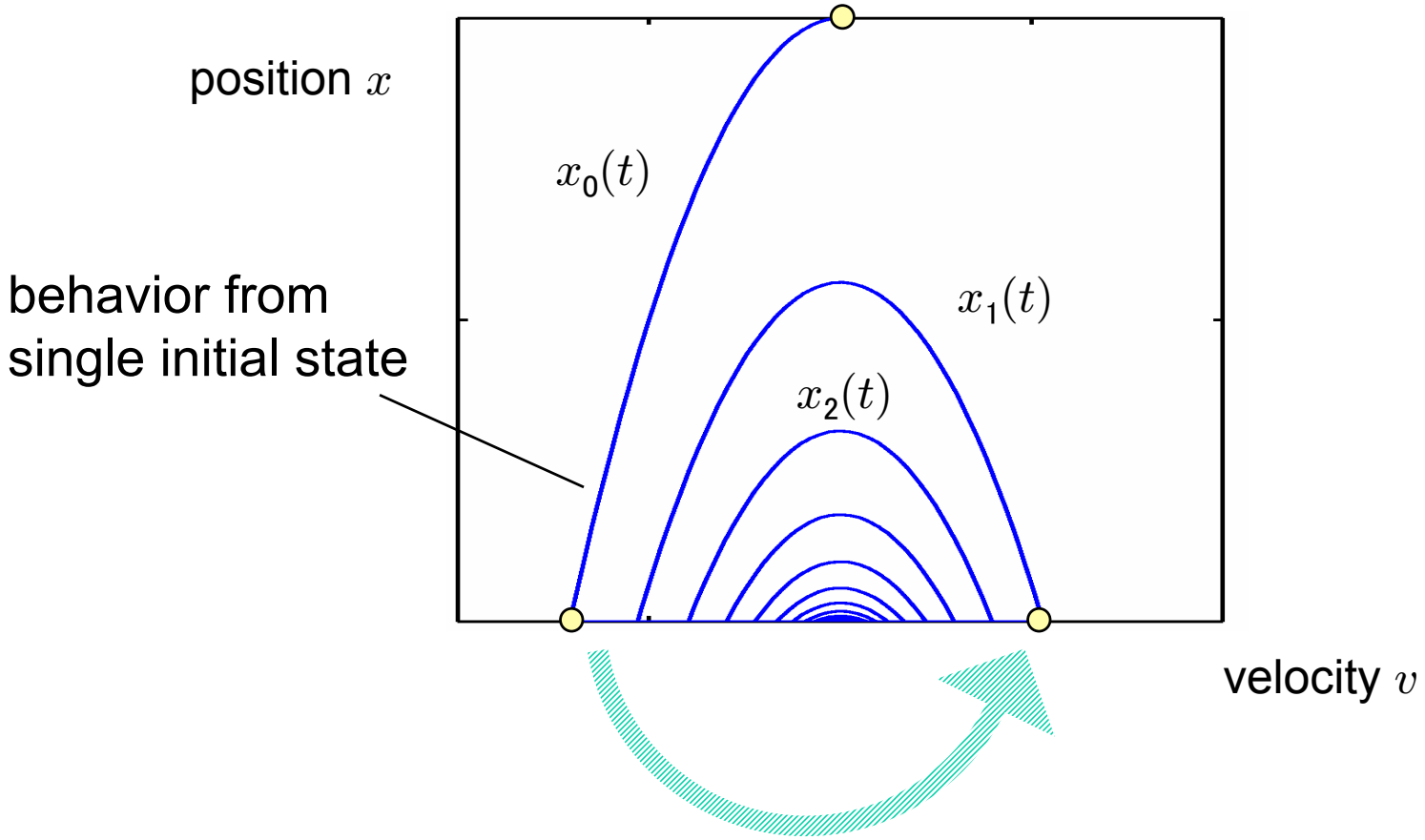
Example: Bouncing Ball

- **States over Time**



Example: Bouncing Ball

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

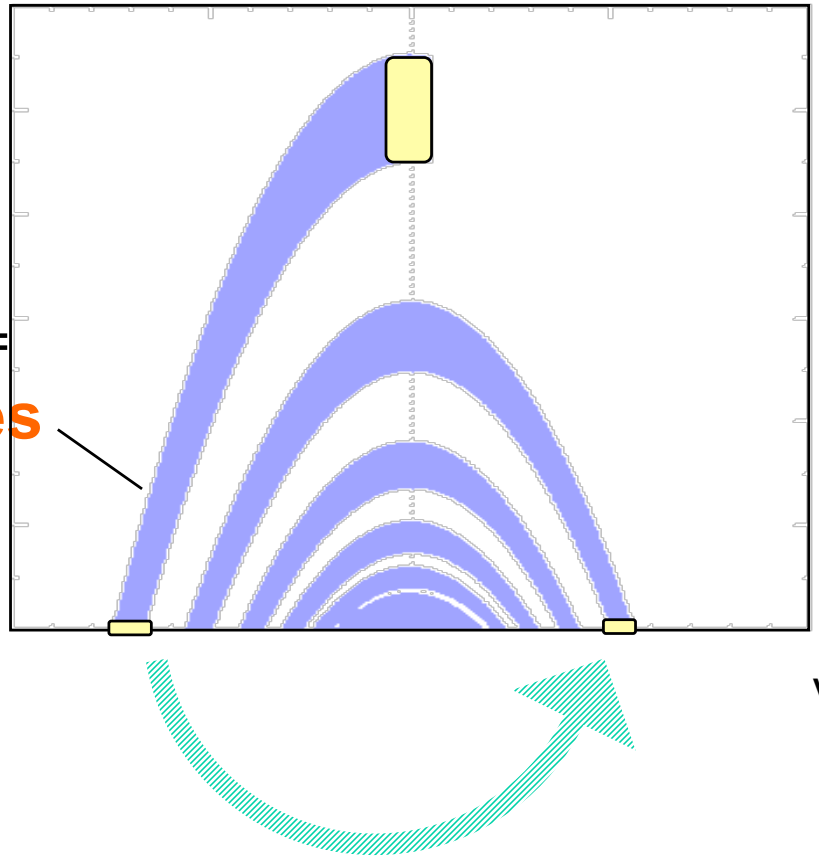


Example: Bouncing Ball

- **Reachability in State-Space**

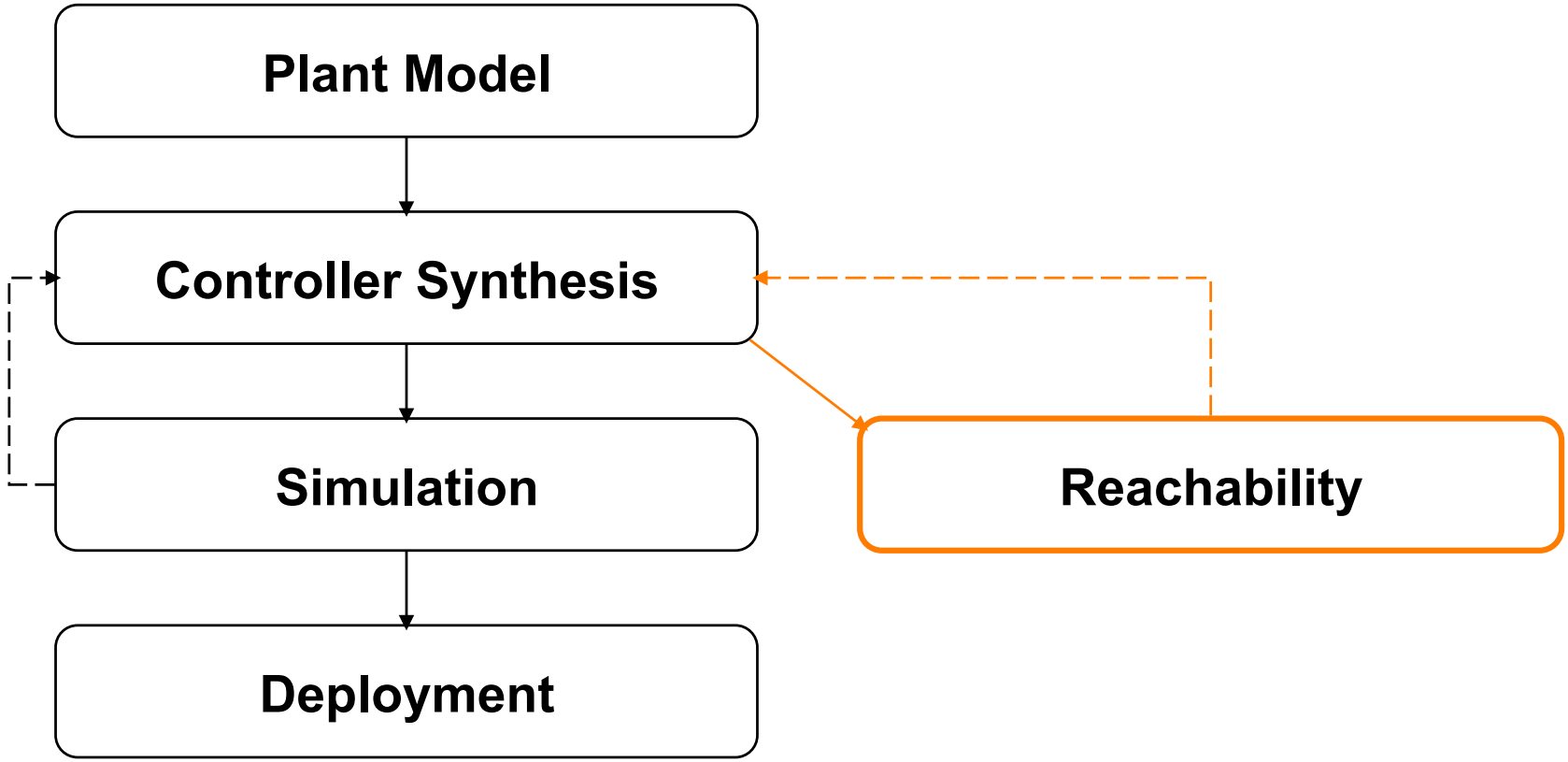
position x

behaviors from
set of initial states =
reachable states



velocity v

Application:
Reachability in Model Based Design



Example: Controlled Helicopter

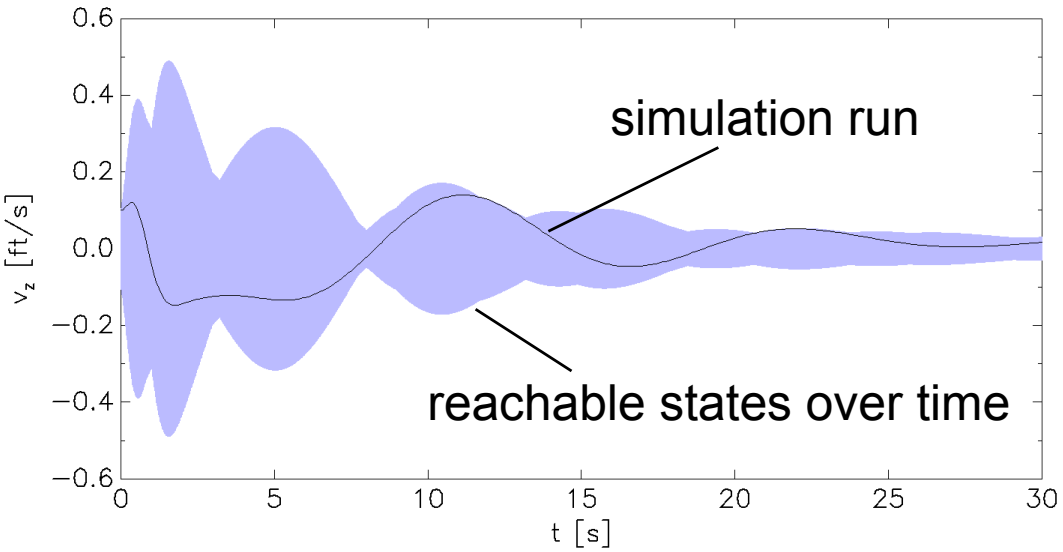
- **28-dim model of a Westland Lynx helicopter**
  - 8-dim model of flight dynamics
  - 20-dim continuous H∞ controller for disturbance rejection
  - stiff, highly coupled dynamics

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

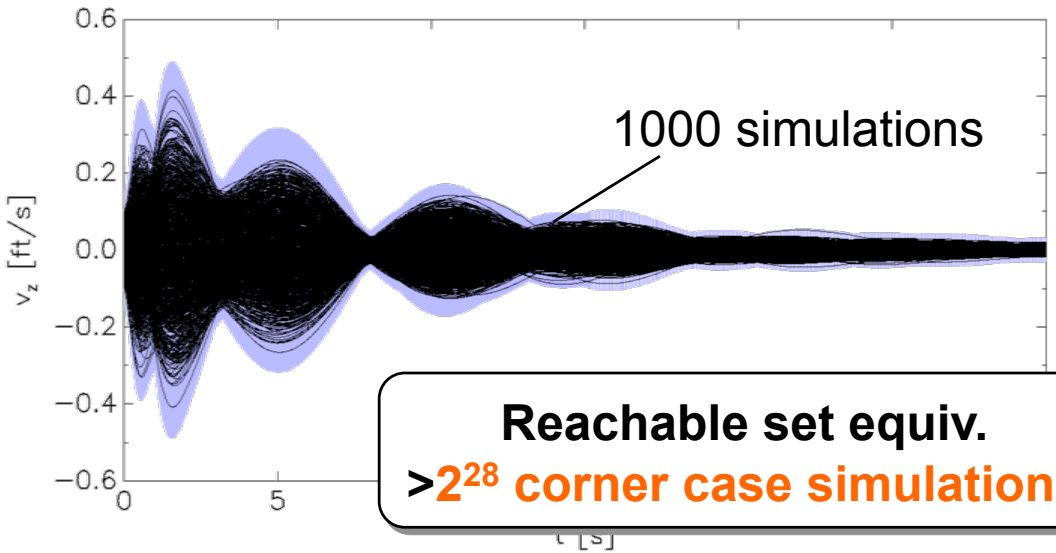
vertical speed



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

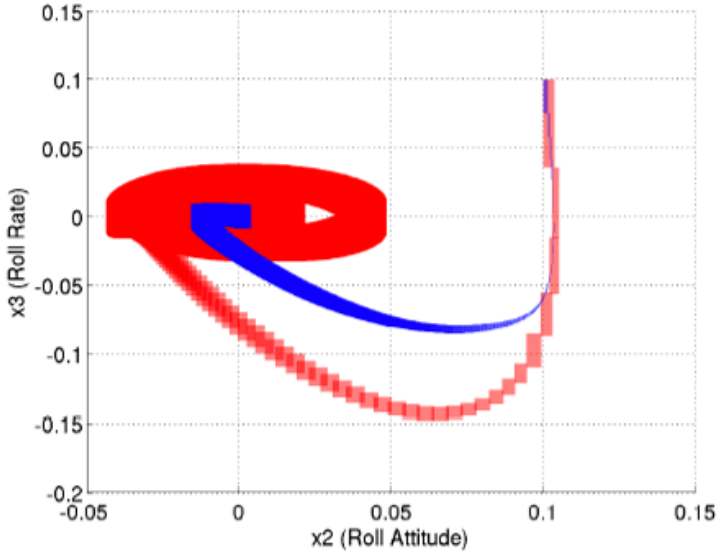
vertical speed



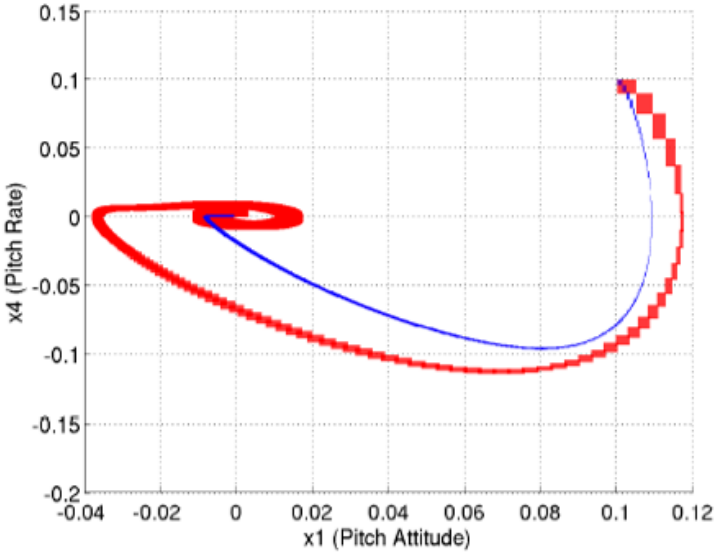
Reachable set equiv.
>2^{28} corner case simulations

Example: Controlled Helicopter

- **Comparing two controllers subject to continuous disturbance**



(a) Roll stabilization

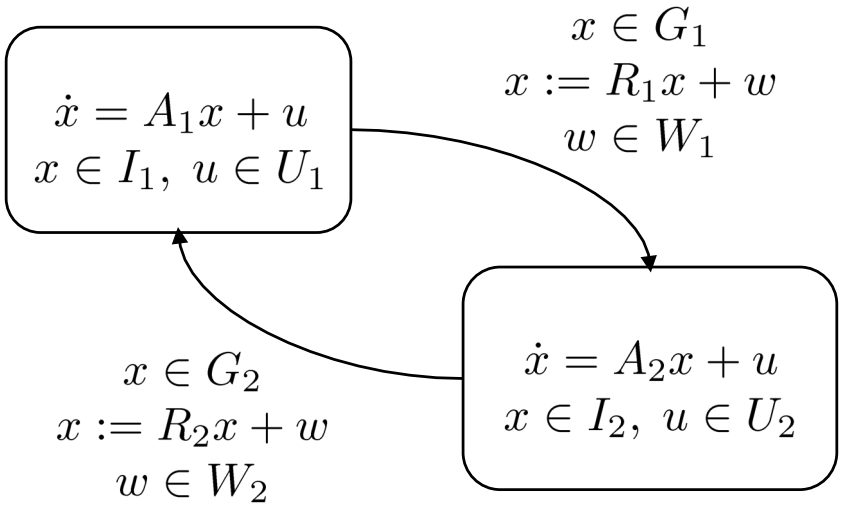


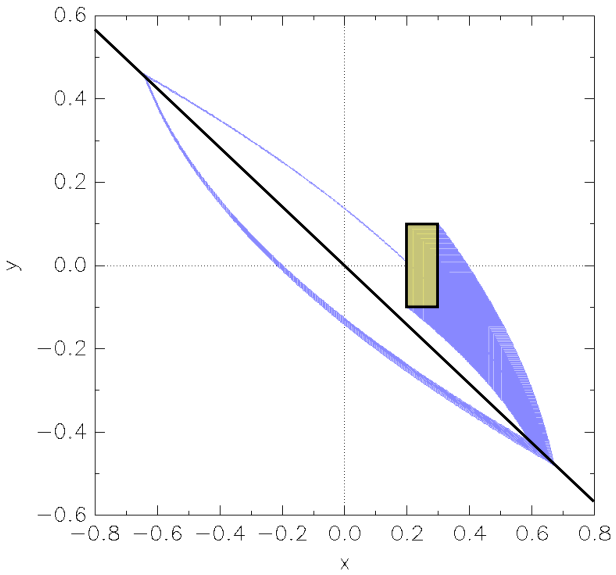
(b) Pitch stabilization

Outline

- Hybrid Systems and Reachability
- **Reachability with Support Functions**
- Approximation in Space-Time
- SpaceEx Development Platform

Hybrid Automata with Affine Dynamics





- **linear differential equations**
- **can be highly nondeterministic:**
  - additive “inputs” u,$w$model continuous disturbances (noise etc.)

Key: find approximation that is efficient but accurate for a large number of continuous variables

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

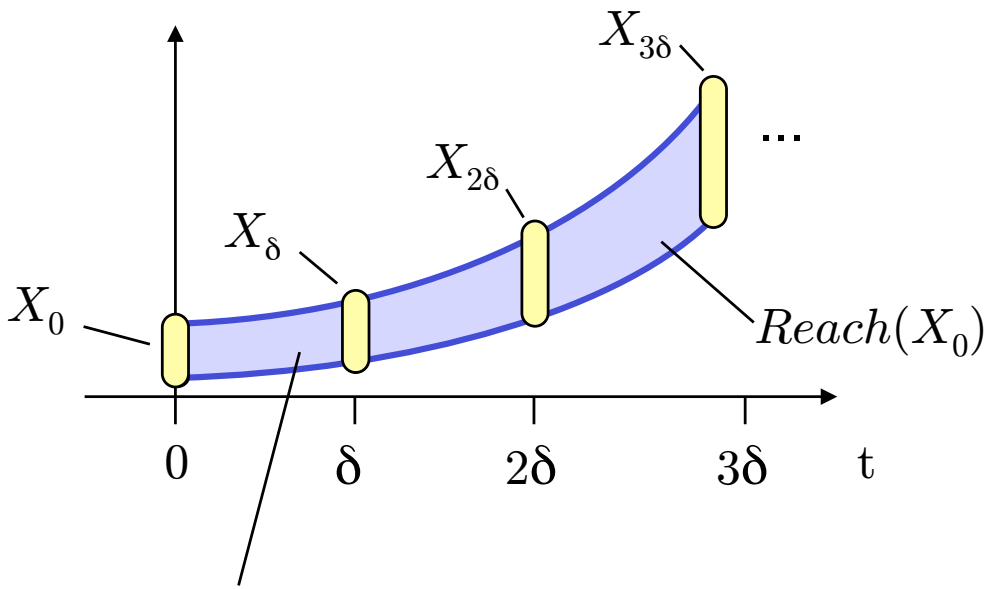
factors influence of inputs
(stable system forgets the past)

From Time-Discretization to Reach

- **States in discrete time:**

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

integral over inputs

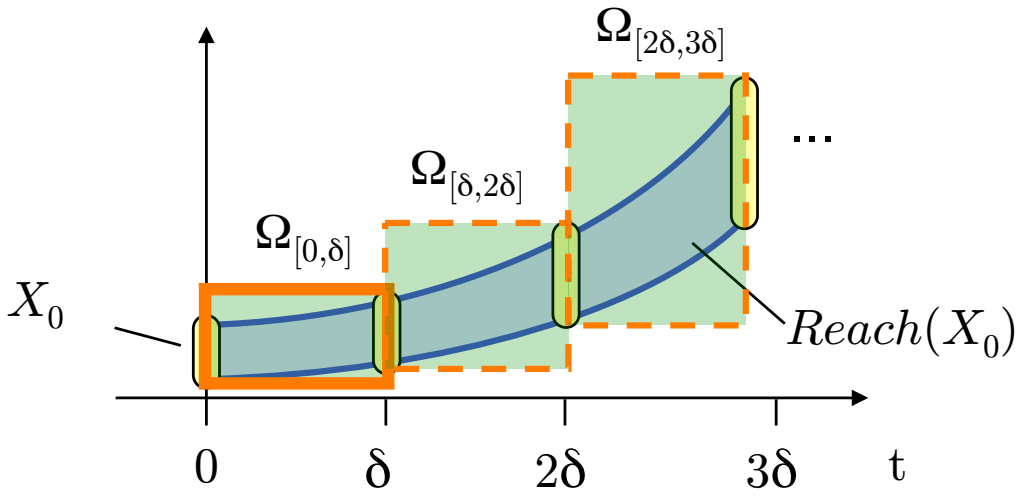


need to cover also states in between!

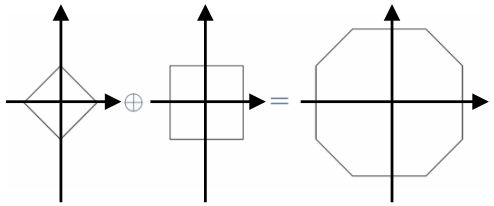
From Time-Discretization to Reach

- **Cover in discrete time:**

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

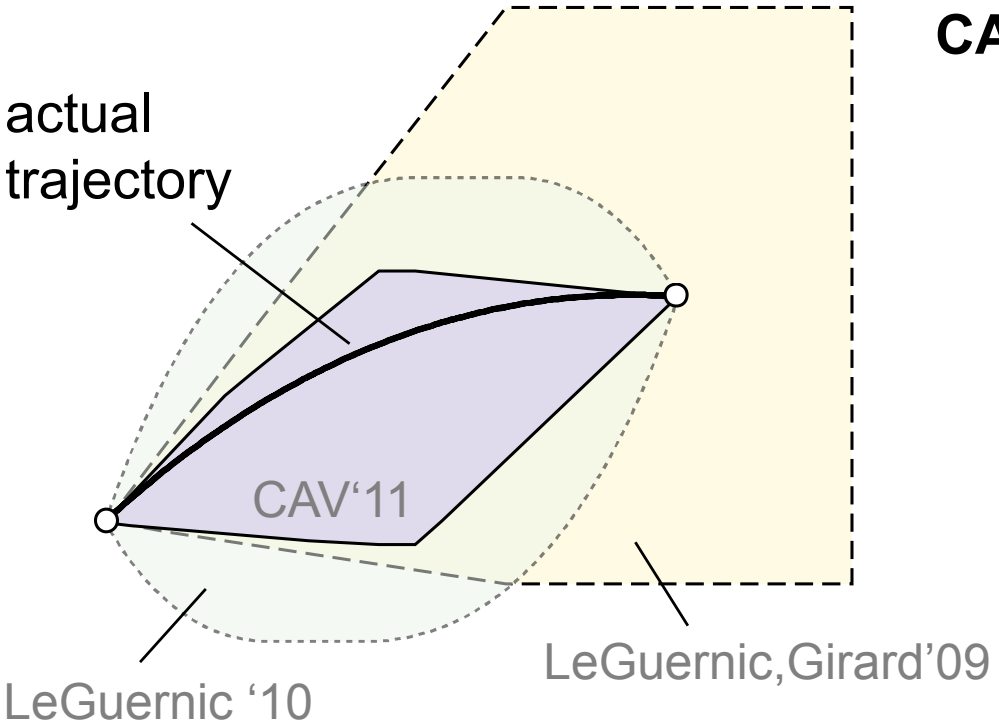


© Minkowski sum = pointwise sum of sets



From Time-Discretization to Reach

- **1st order Taylor approximation**
- **different bounds on the remainder**



CAV’11: Complex Polytope

$$
\begin{aligned}
\Omega_{[0,\delta]} &= \mathrm{chull}(\textstyle\bigcup_{0\le t\le\delta}\Omega_t)\\
\Omega_t &= (1-\tfrac{t}{\delta})\mathcal{X}_0 \oplus \tfrac{t}{\delta}e^{\delta A}\mathcal{X}_0\\
&\quad \oplus \left(\tfrac{t}{\delta}\mathcal{E}^+_\Omega \cap (1-\tfrac{t}{\delta})\mathcal{E}^-_\Omega\right)\\
&\quad \oplus t\mathcal{U} \oplus \tfrac{t^2}{\delta^2}\mathcal{E}_\Psi\\
\Phi_2(A,\delta) &= A^{-2}\left(e^{\delta A} - I - \delta A\right)\\
\mathcal{E}^+_\Omega(\mathcal{X}_0,\delta) &= \boxdot\left(\Phi_2(|A|,\delta)\boxdot\left(A^2\mathcal{X}_0\right)\right),\\
\mathcal{E}^-_\Omega(\mathcal{X}_0,\delta) &= \boxdot\left(\Phi_2(|A|,\delta)\boxdot\left(A^2e^{\delta A}\mathcal{X}_0\right)\right),\\
\mathcal{E}_\Psi(\mathcal{U},\delta) &= \boxdot\left(\Phi_2(|A|,\delta)\boxdot\left(A\mathcal{U}\right)\right).
\end{aligned}
$$

Operations on Convex Sets

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

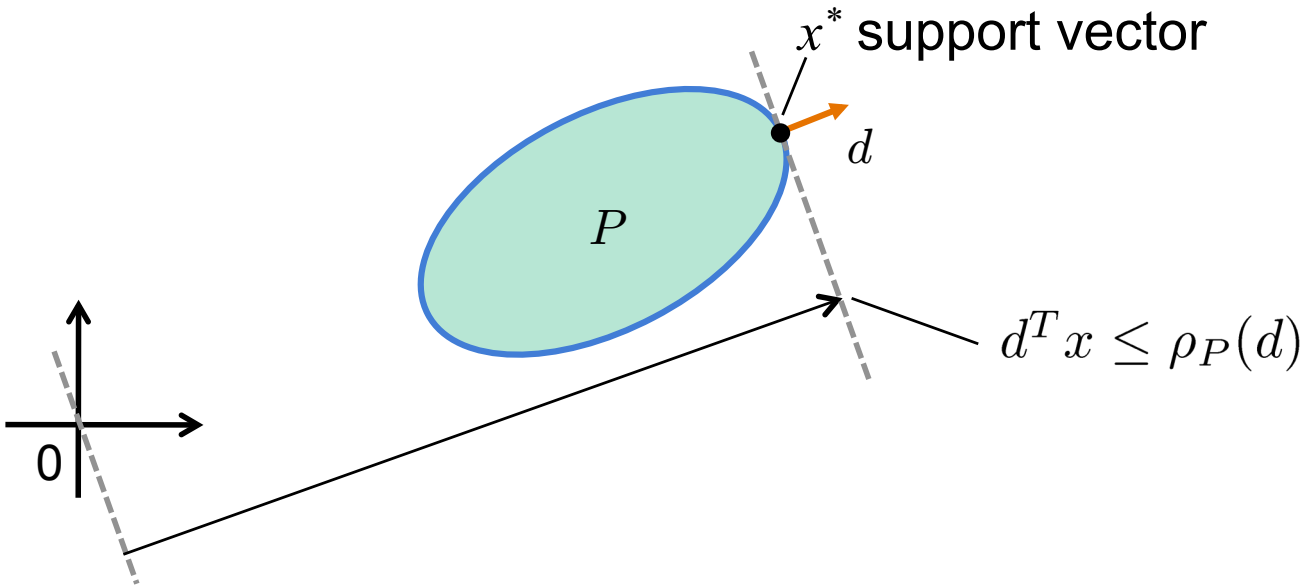
Le Guernic, Girard. CAV'09

Support Functions

- **Support Function R^n ! R**
  - direction d ! position of supporting halfspace

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

  - exact set representation

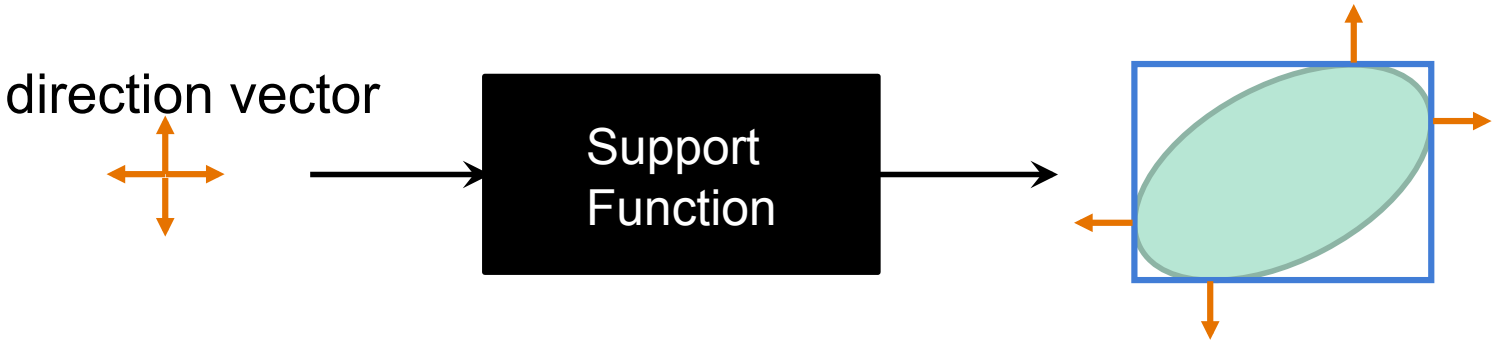


Support Functions

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

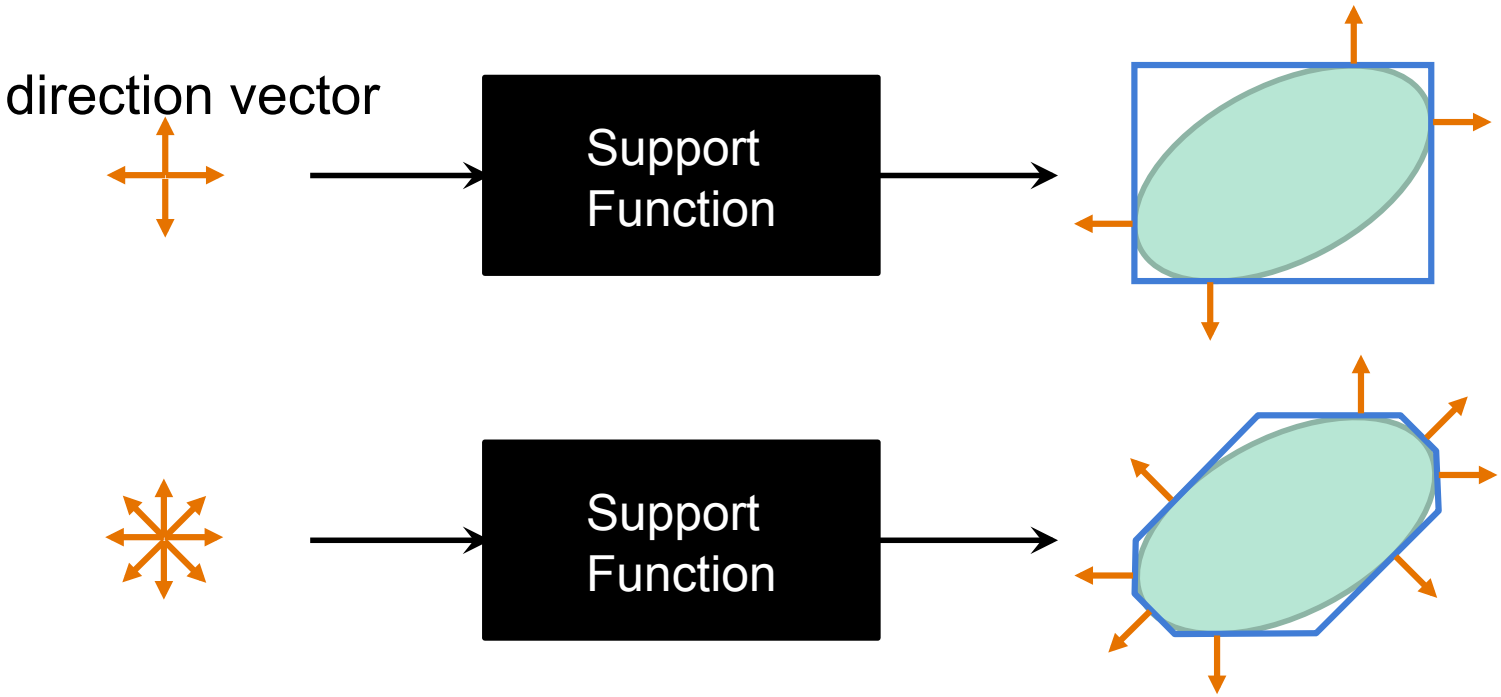
Support Functions

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



Support Functions

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

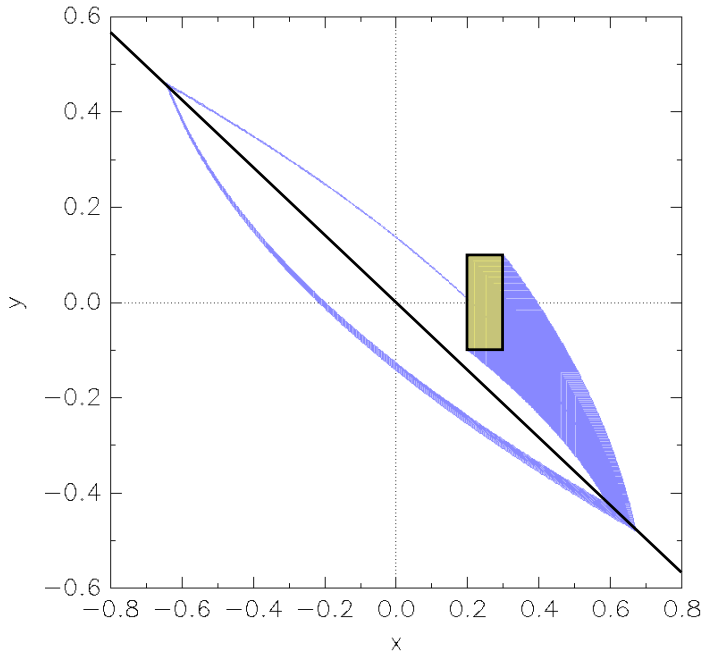


Computing with Support Functions

- **Simple Operations** (Le Guernic, Girard. CAV'09)
  - Linear Transform: $\rho_{AP}(d) = \rho_P(A^T d)$
    - O(n^2) incl. existential quantification
  - Minkowski sum: $\rho_{P \oplus Q}(d) = \rho_P(d) + \rho_Q(d)$
    - O(1)
  - Convex hull: $\rho_{chull(P,Q)}(d) = \max(\rho_P(d), \rho_Q(d))$
    - O(1)

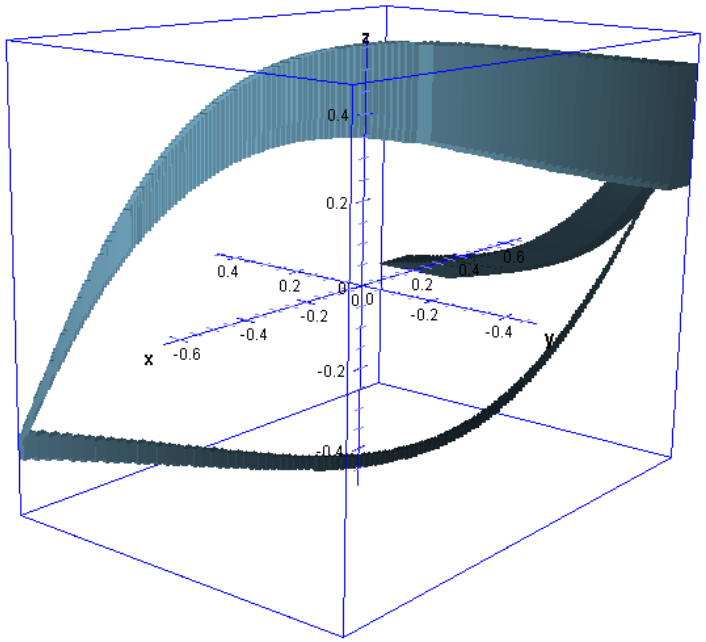
Example: Switched Oscillator

- **Switched oscillator**
  - 2 continuous variables
  - 4 discrete states
  - similar to many circuits (Buck converters,…)
- **plus linear filter**
  - m continuous variables
  - dampens output signal
- **affine dynamics**
  - total $2 + m$ continuous variables

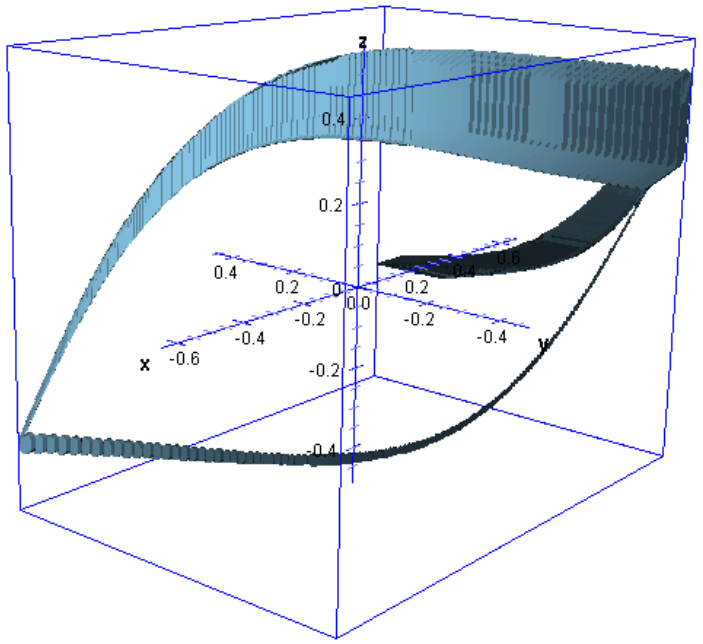


Example: Switched Oscillator

- **Low number of directions sufficient?**
  - here: 6 state variables



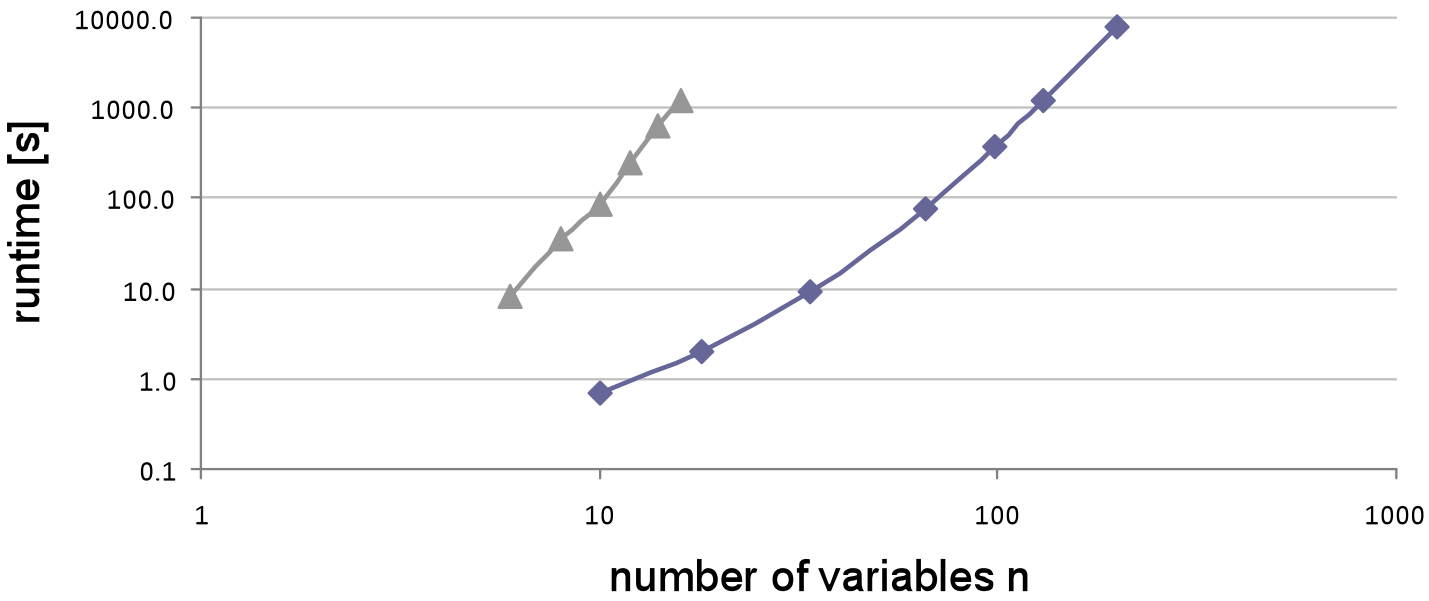
12 box constraints
(axis directions)



72 octagonal constraints
$(\pm x_i \pm x_j)$

Example: Switched Oscillator

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

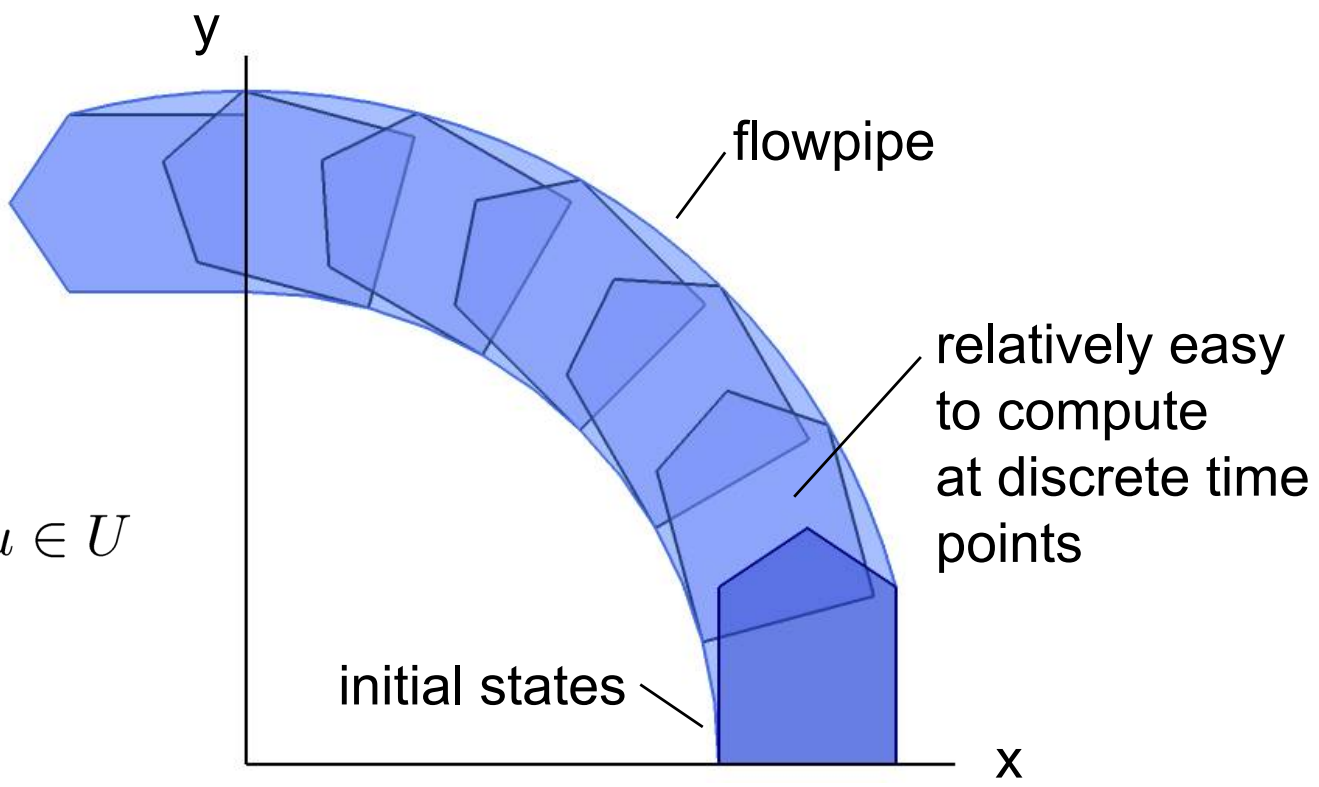


Outline

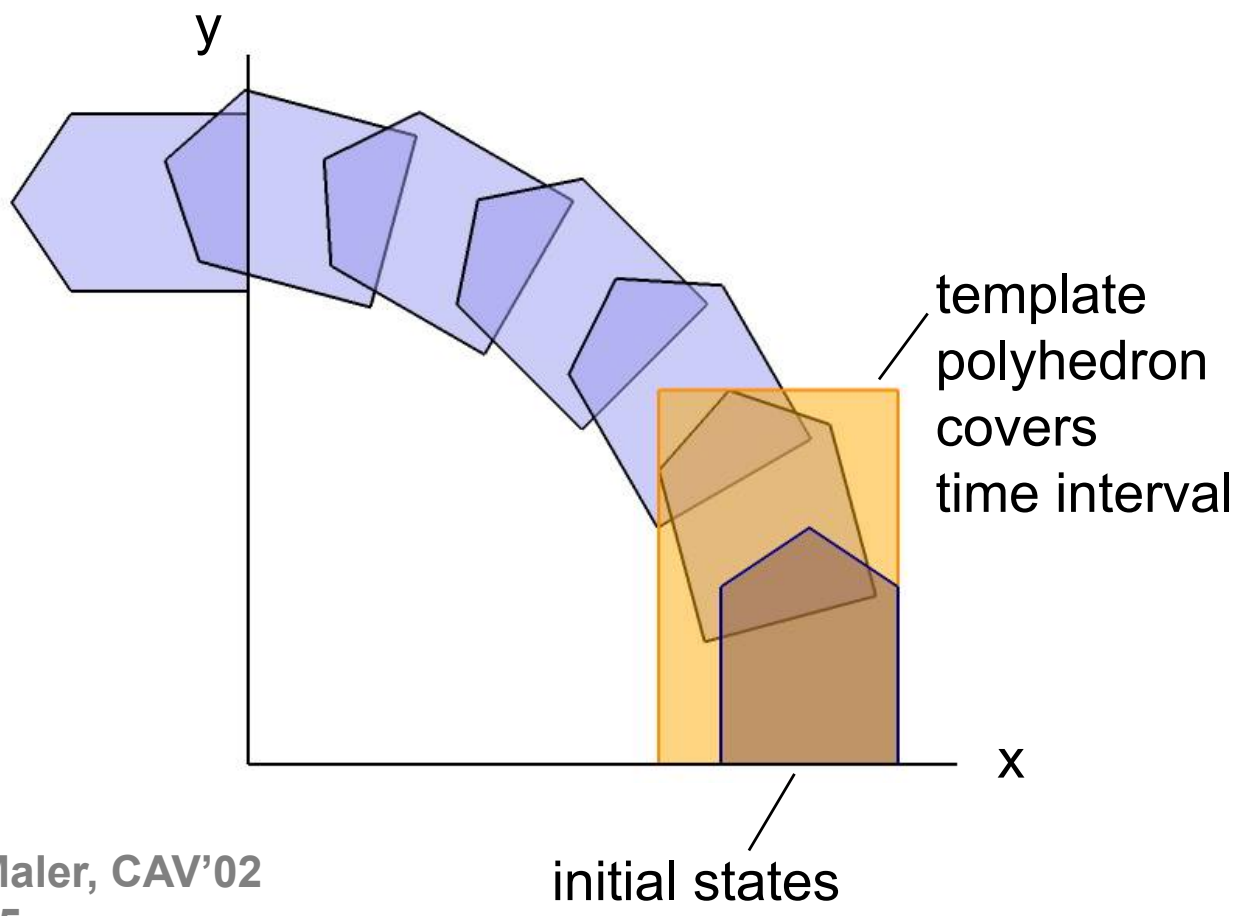
- Hybrid Systems and Reachability
- Reachability with Support Functions
- **Approximation in Space-Time**
- SpaceEx Development Platform

Flowpipe – Reachable States over Time

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

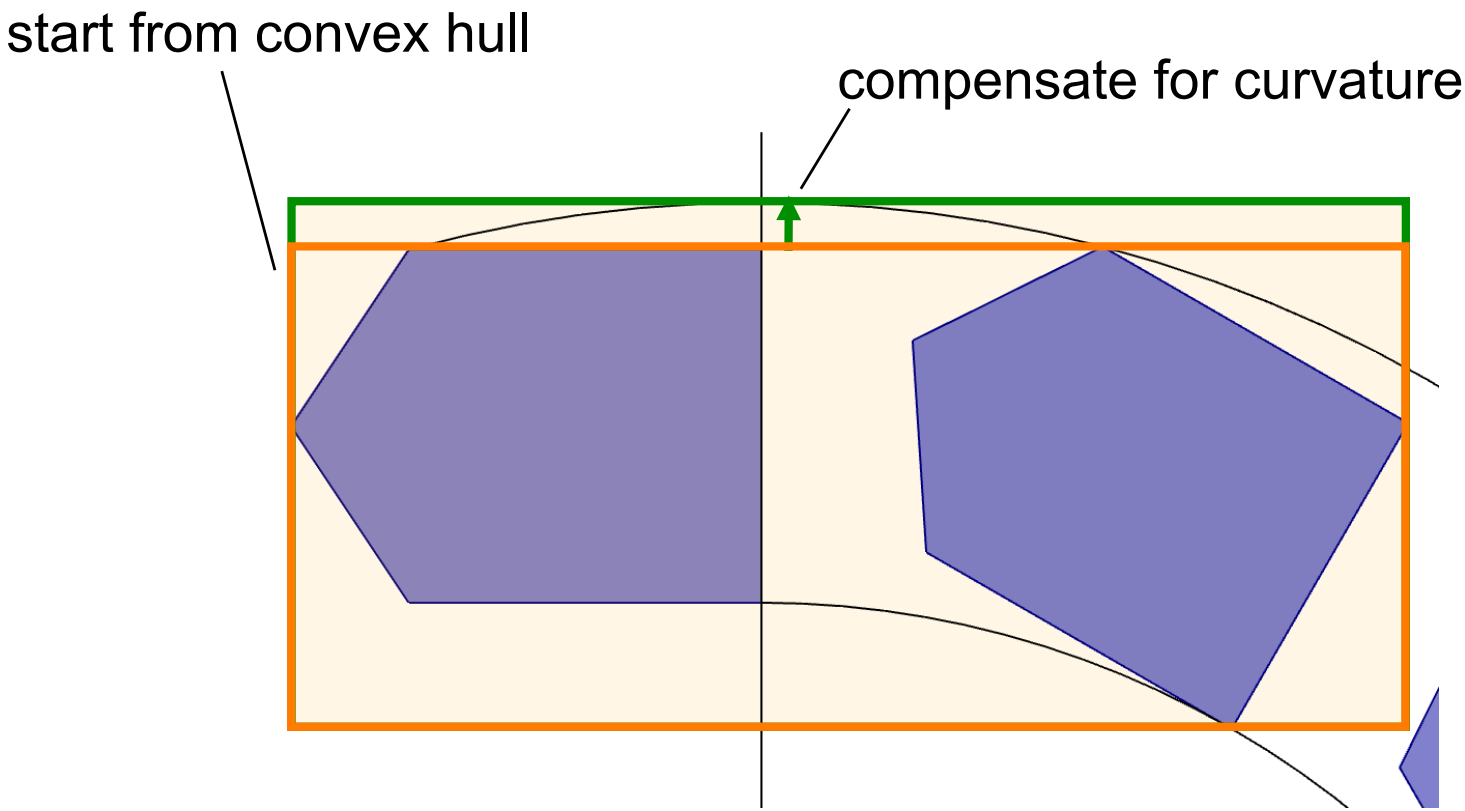


Approximation with Template Polyhedra

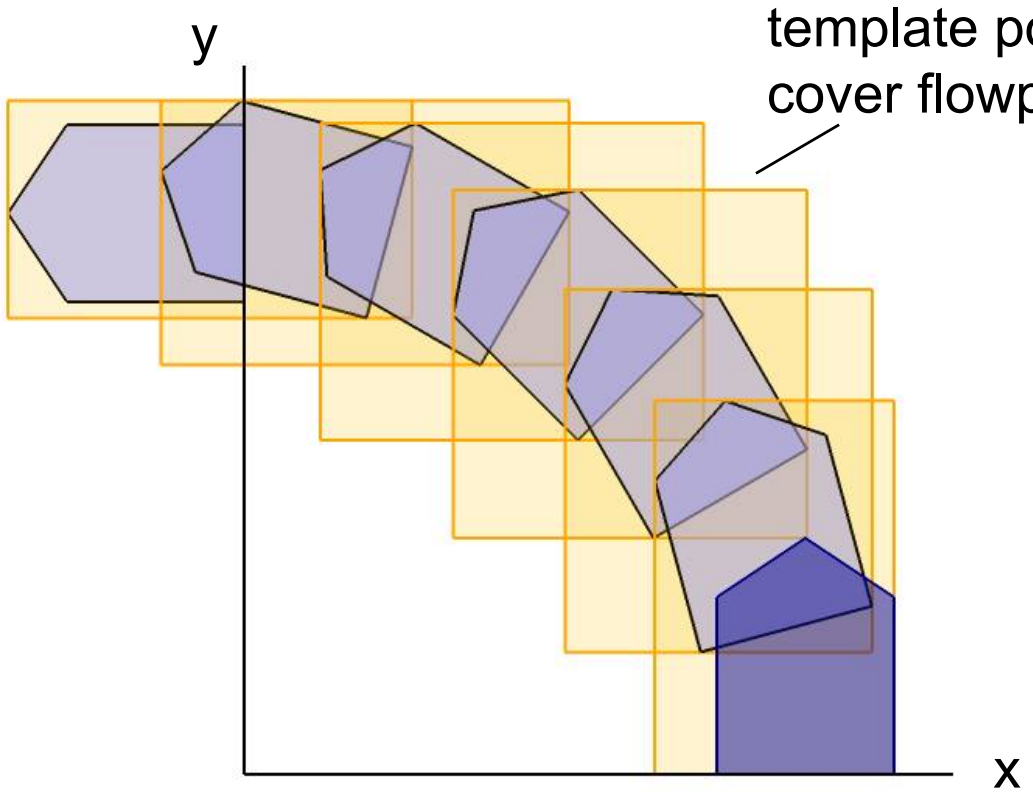


- Asarin, Dang, Maler, CAV'02
- Girard, HSCC'05
- Le Guernic, Girard, CAV'09
- Frehse et al. CAV'11

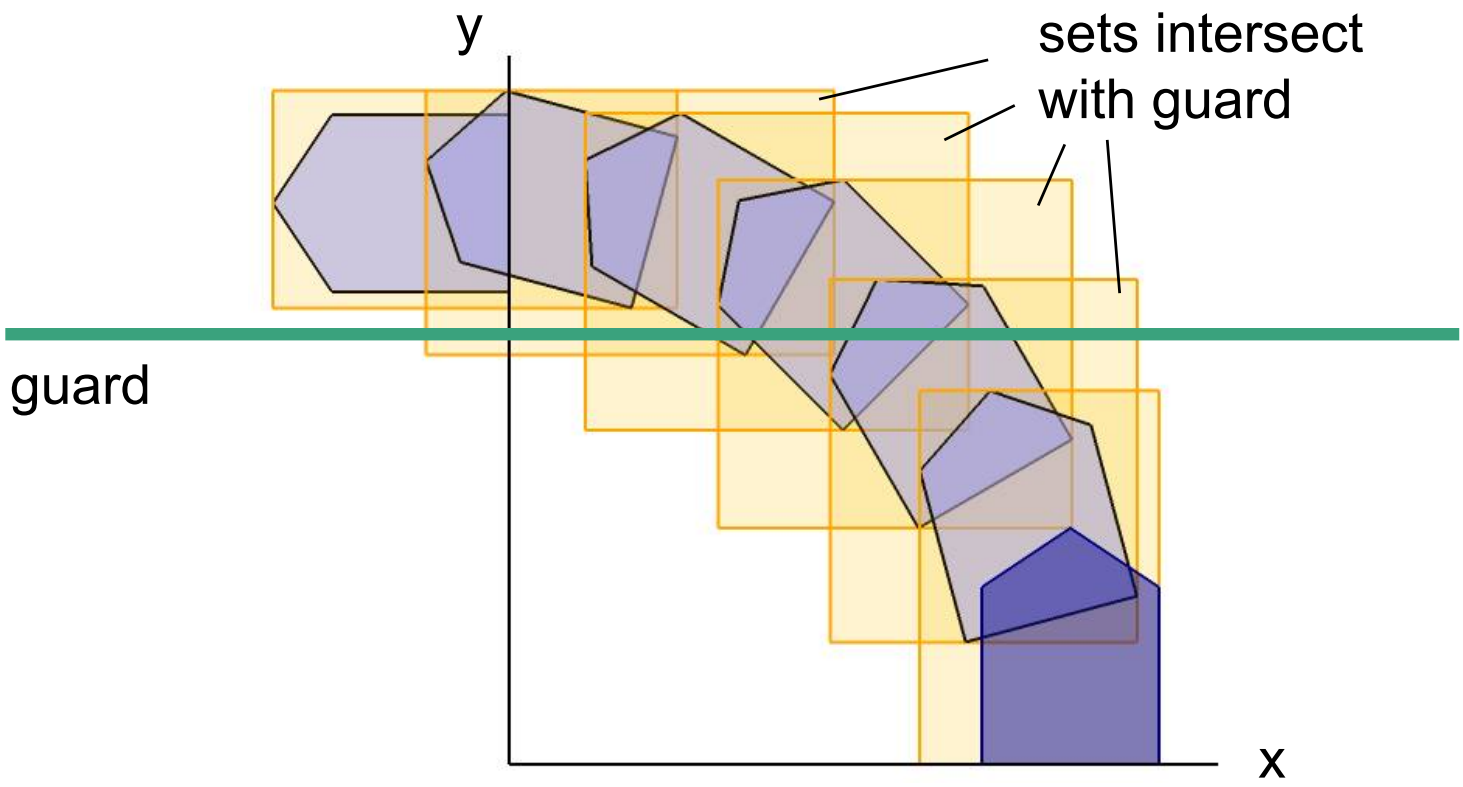
Approximation with Template Polyhedra



Approximation with Template Polyhedra

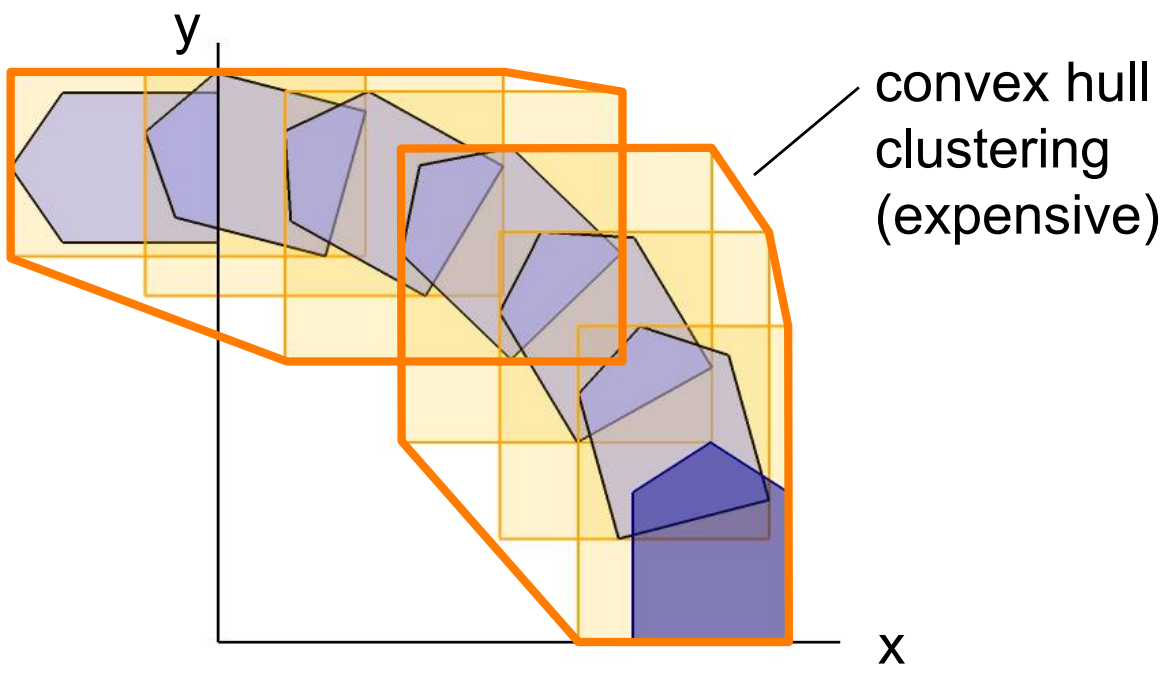


Problem 1: Too many sets

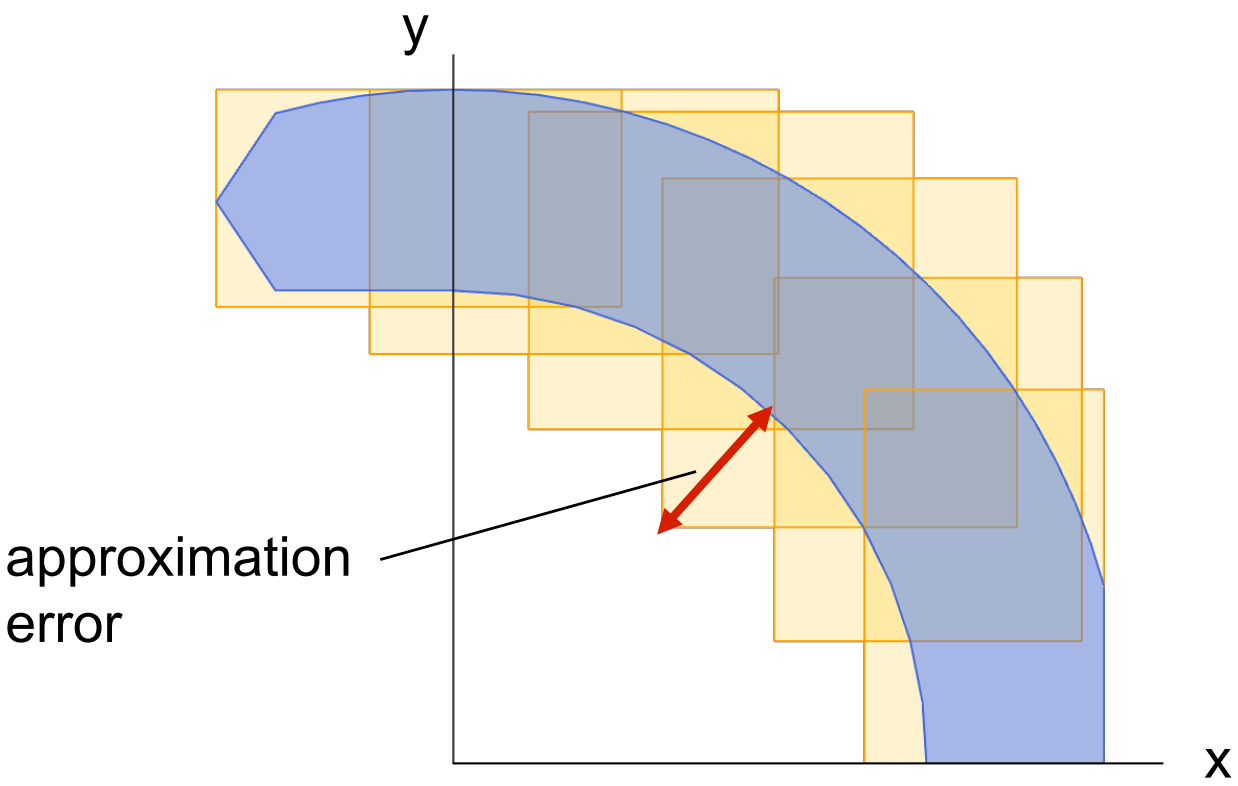


Problem 1: Too many sets

- **Jumps: Exponential increase in the number of sets**
  - case studies: 10x – 100x per jump



Problem 2: Quantify error

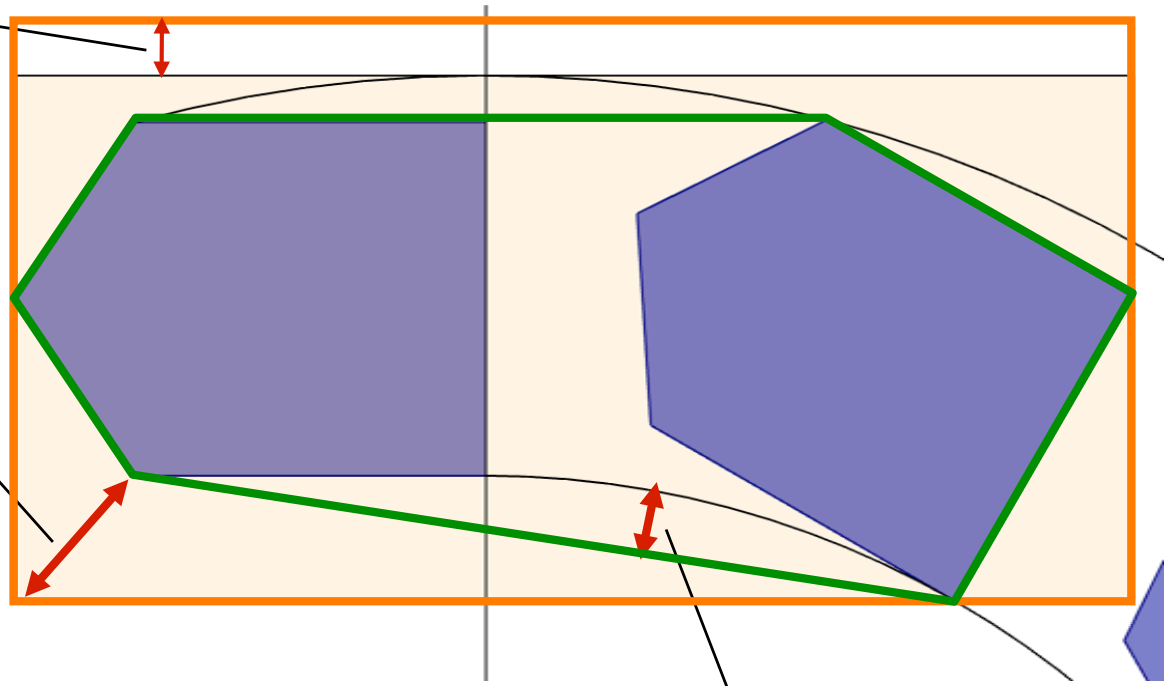


four sources of error...

Problem 2: Quantify error

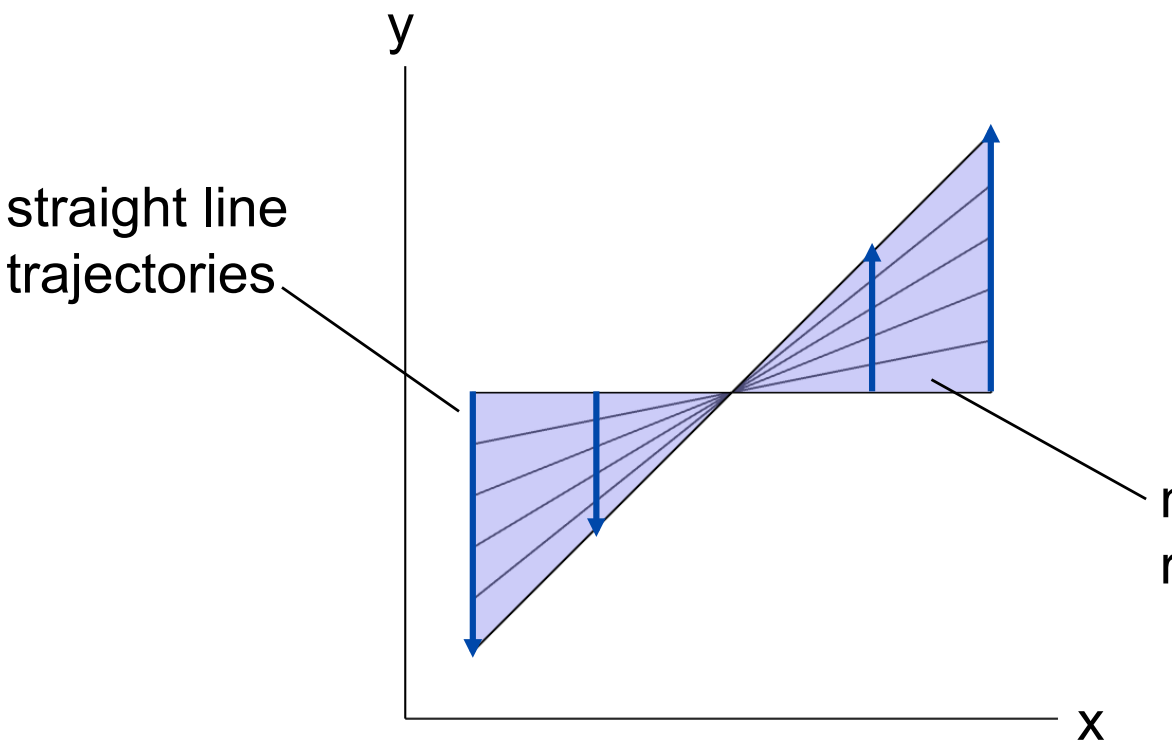
(2) bloating error (curvature estimation)

(1) template error (distance to convex hull)



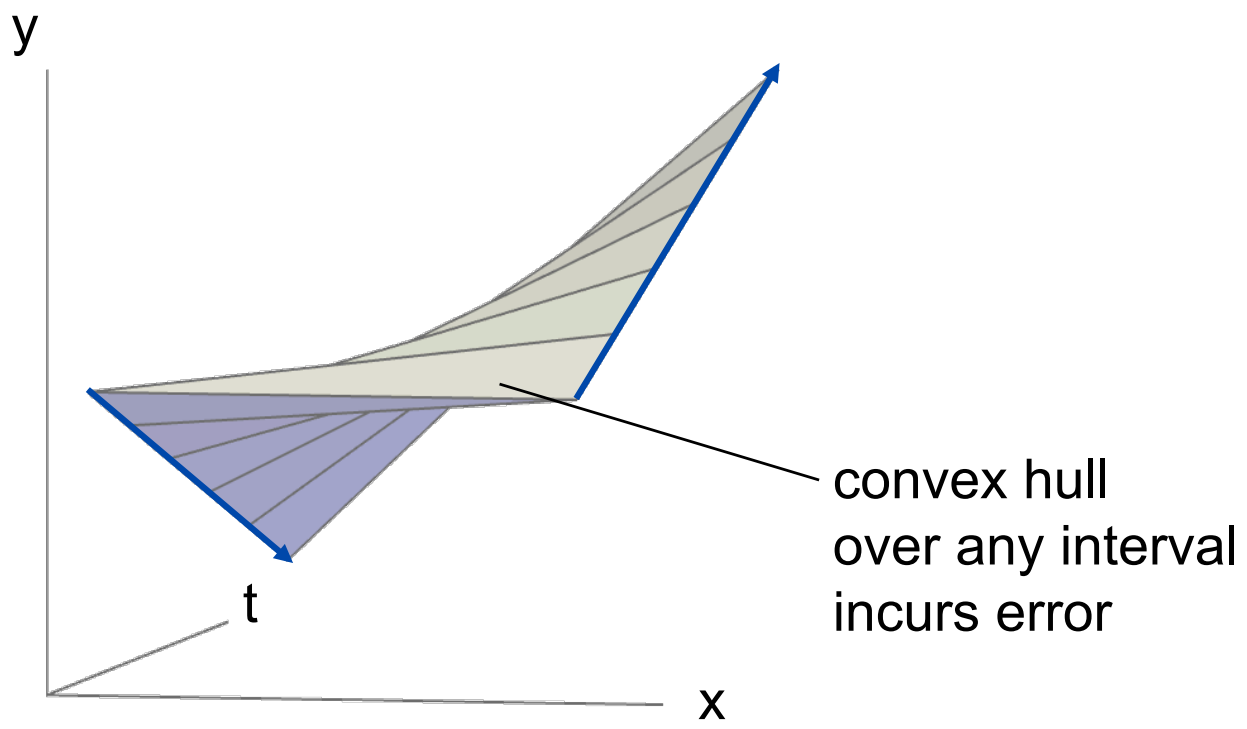
(3) convexity error **(unknown)**

Problem 2: Quantify error

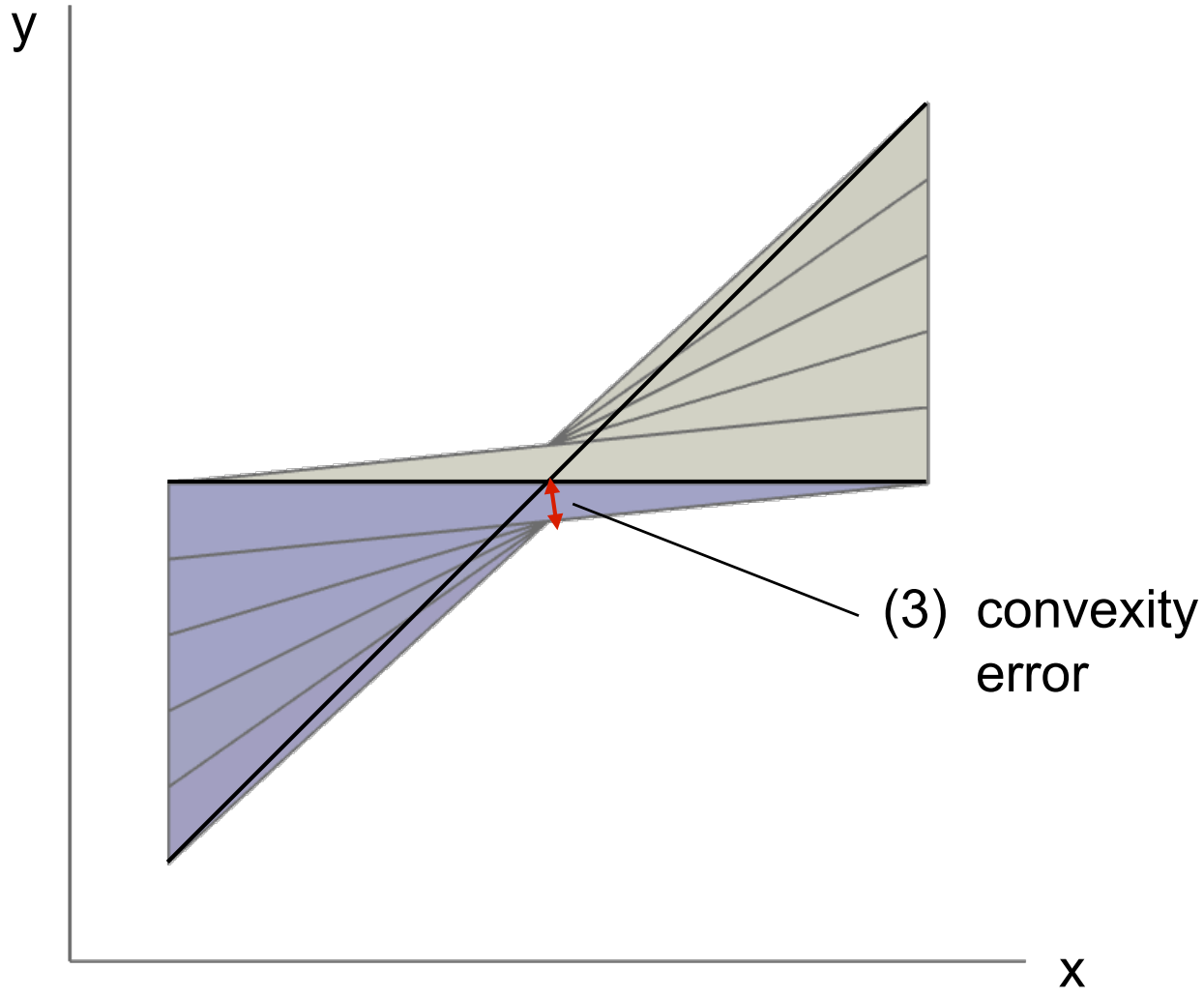


It’s not just curvature...

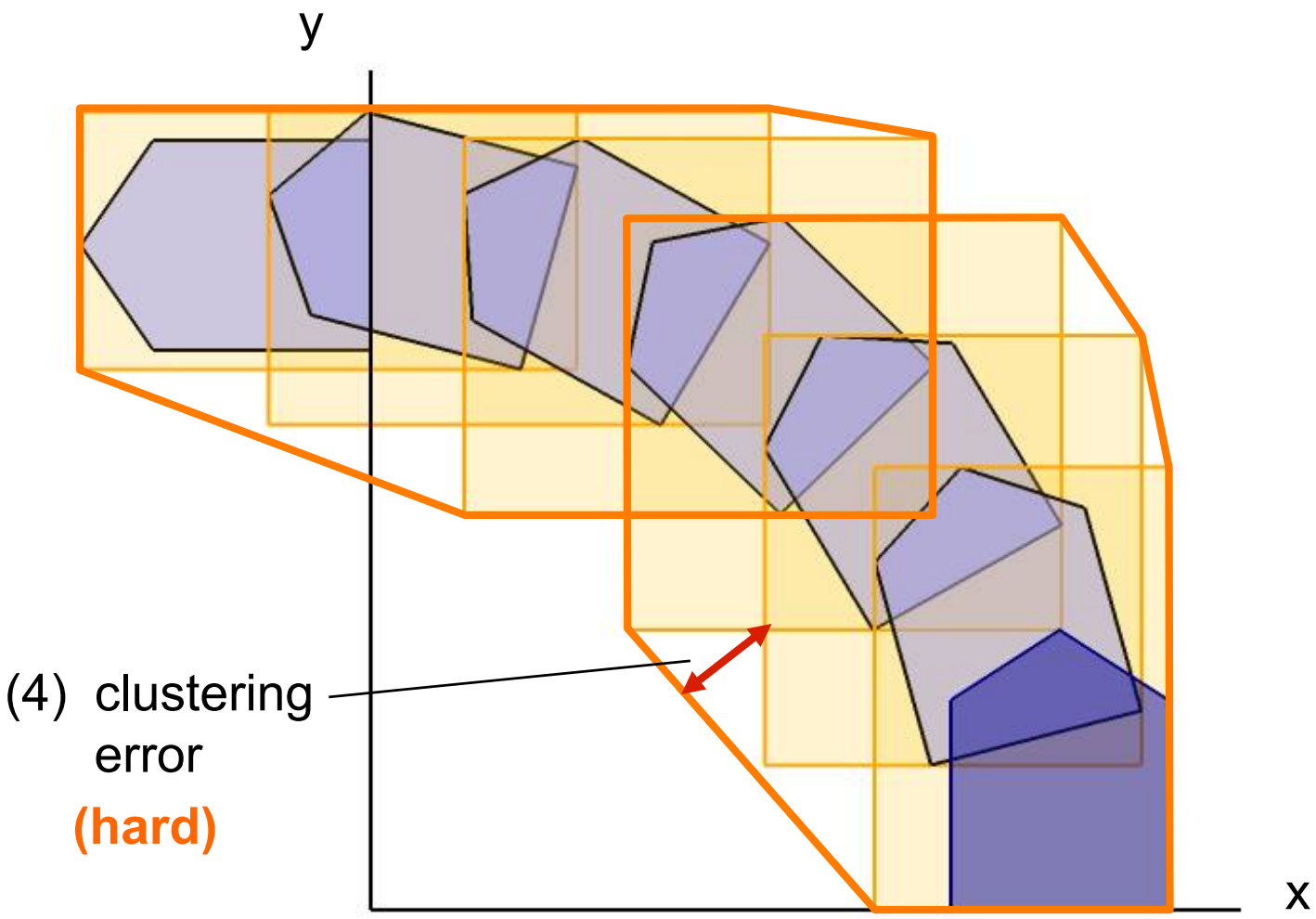
Problem 2: Quantify error



Problem 2: Quantify error



Problem 2: Quantify error

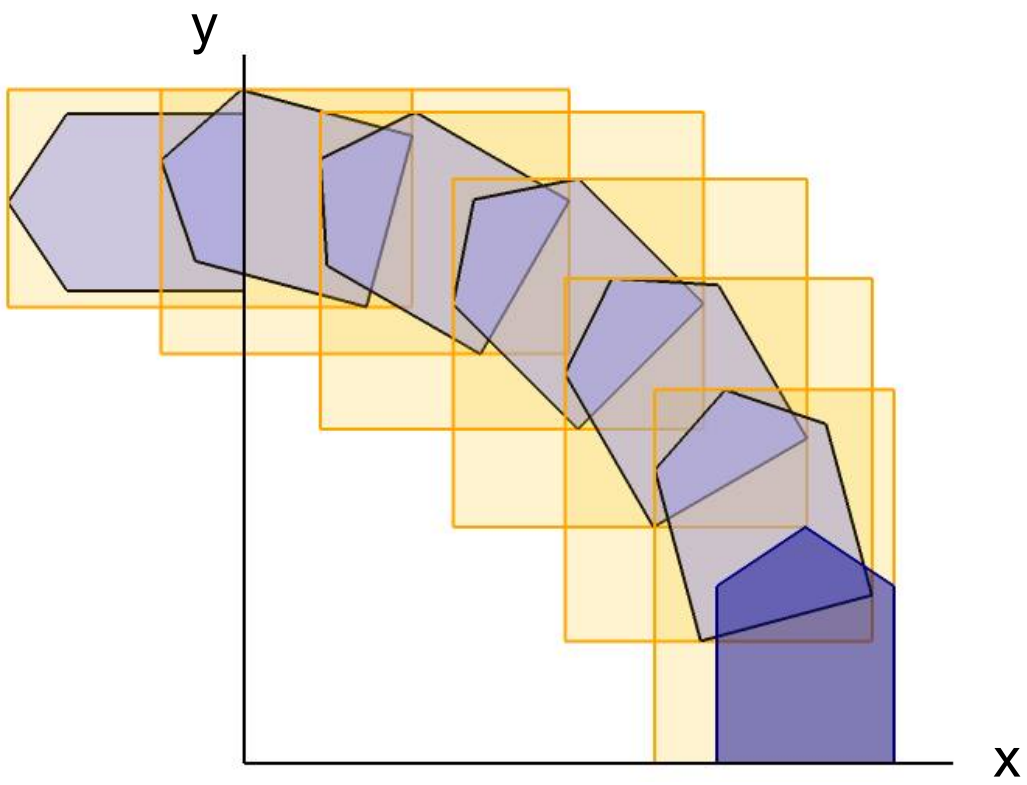


Goals

- **Reduce the number of convex sets**
- **Measure the total error**
  1) template error
  2) bloating error
  3) **convexity error**
  4) **clustering error**

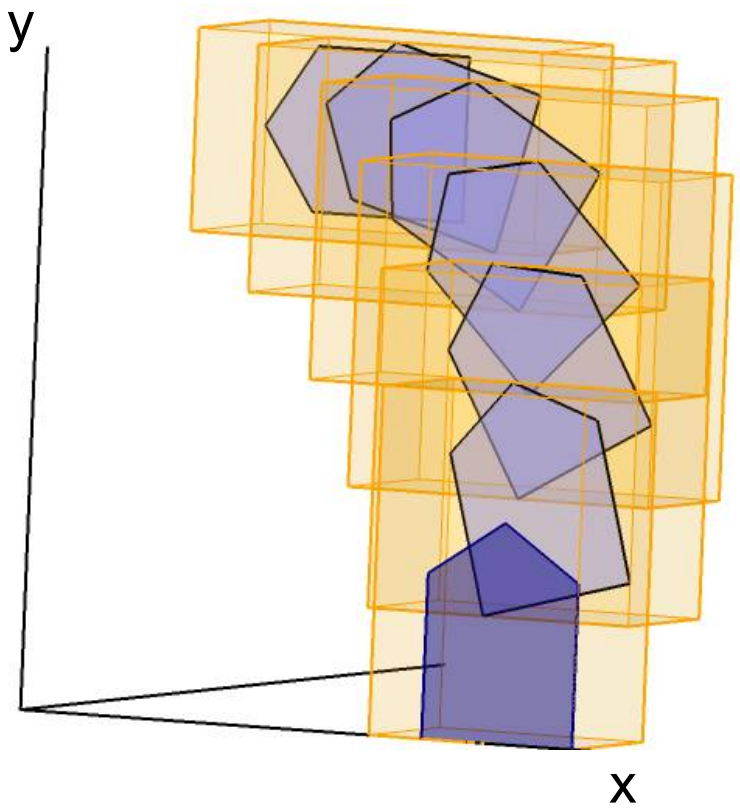
} ***directional error***

Approximation in Space-Time

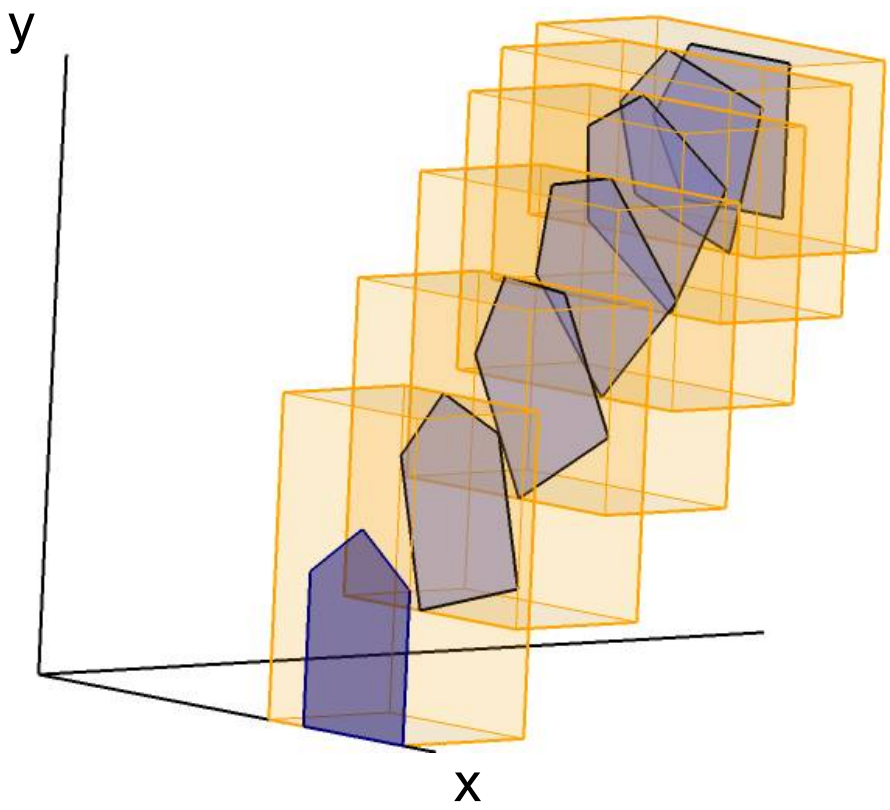


Improve the approximation by adding time...

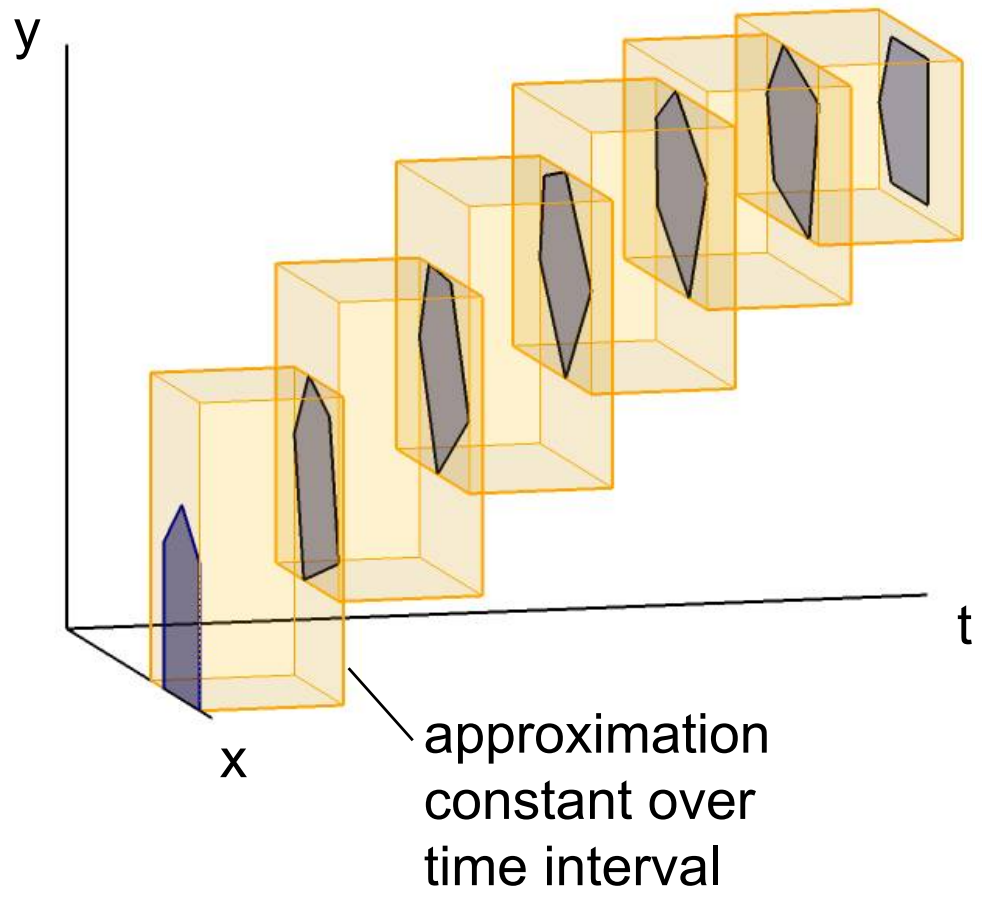
Approximation in Space-Time



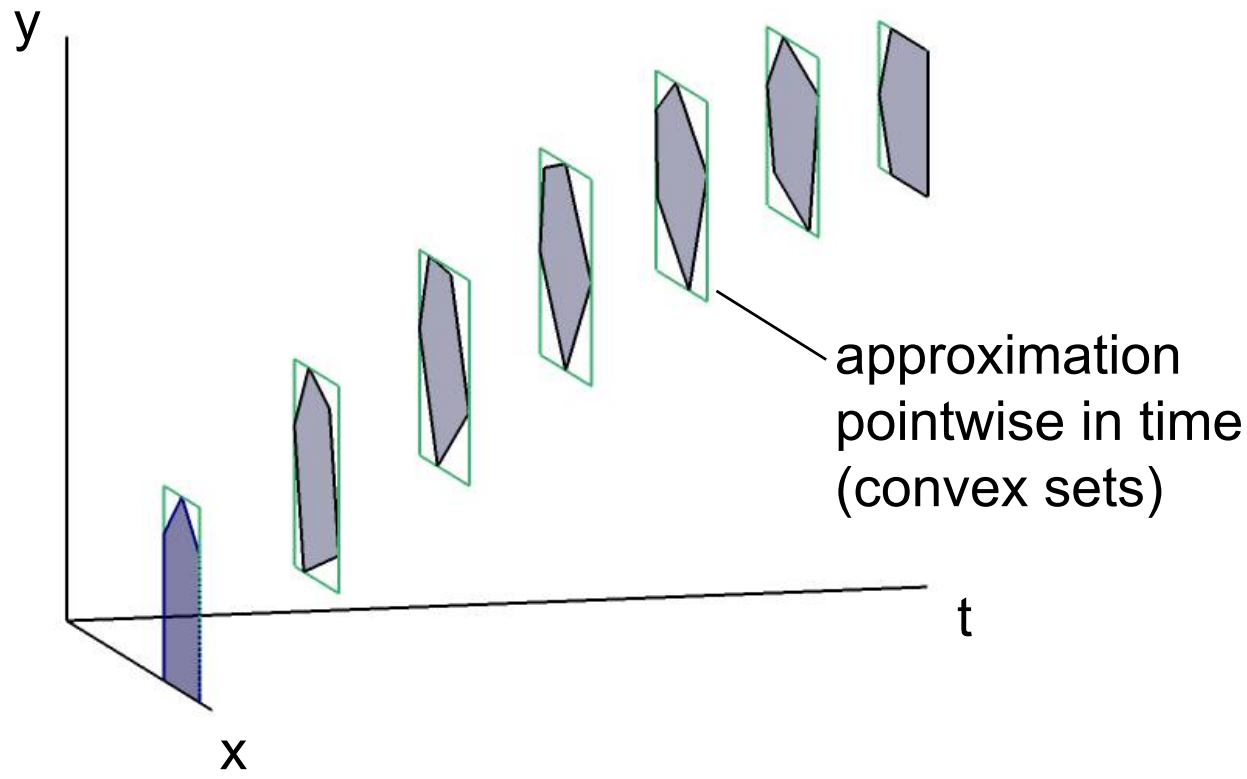
Approximation in Space-Time



Approximation in Space-Time

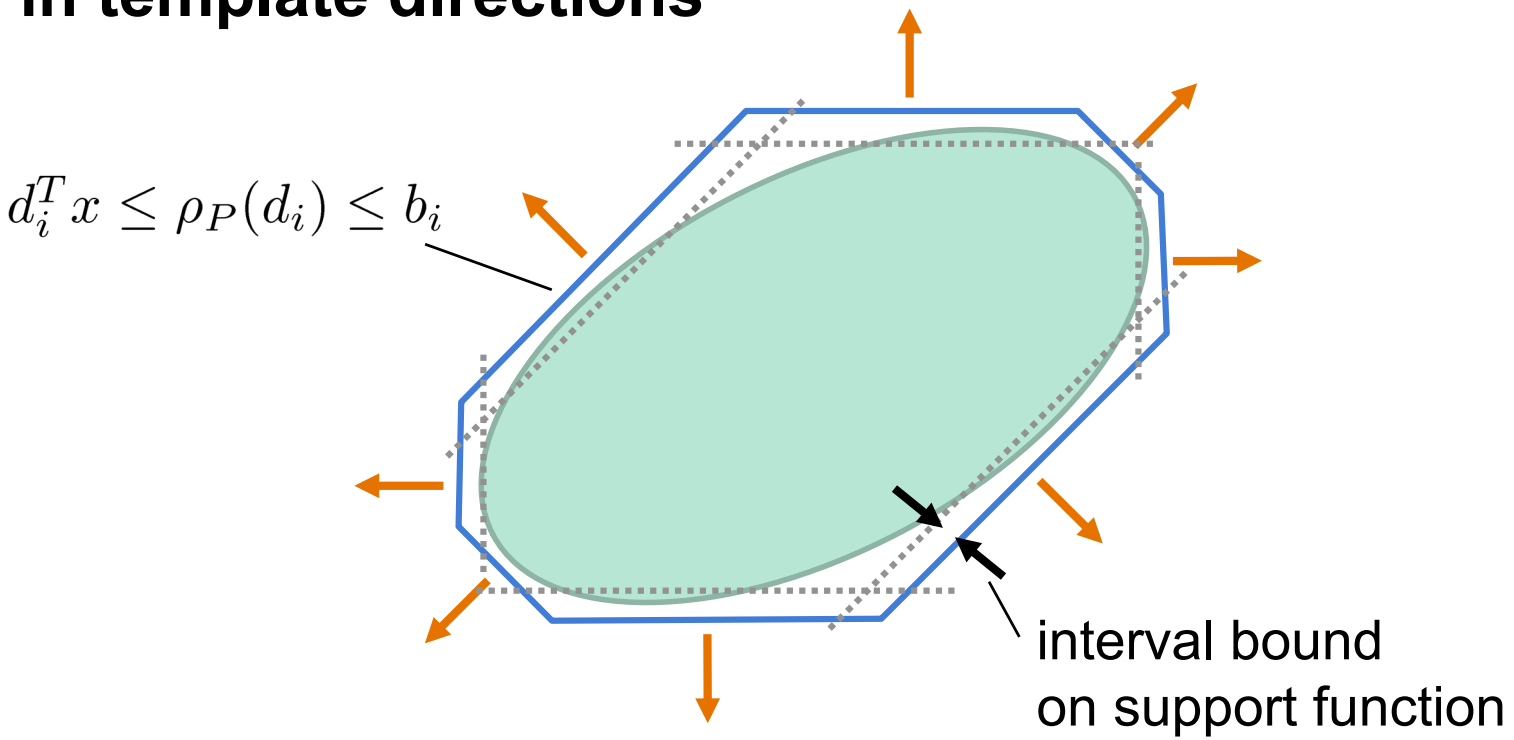


Approximation in Space-Time



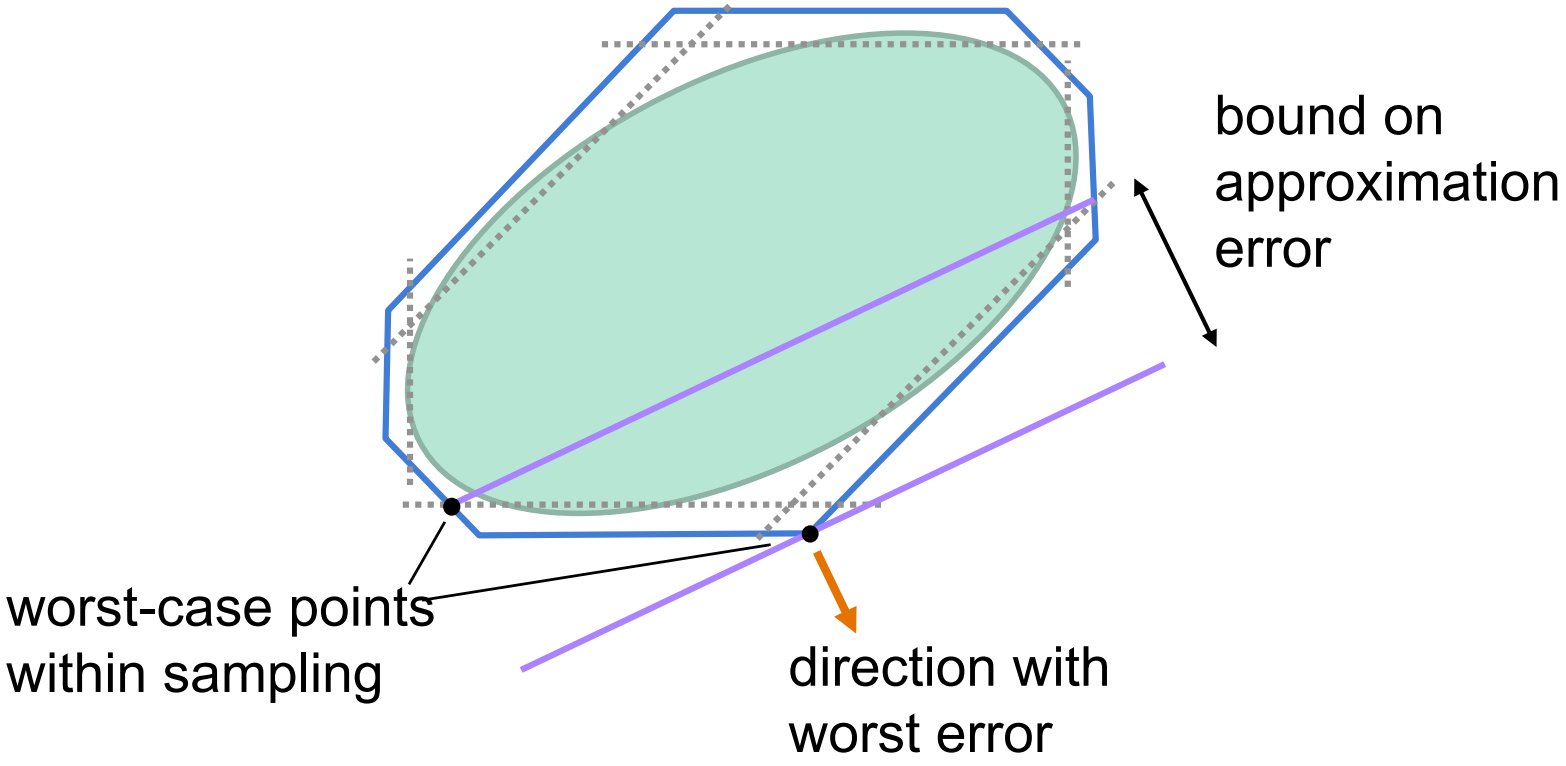
Support Sampling

- **interval bound on support function in template directions**

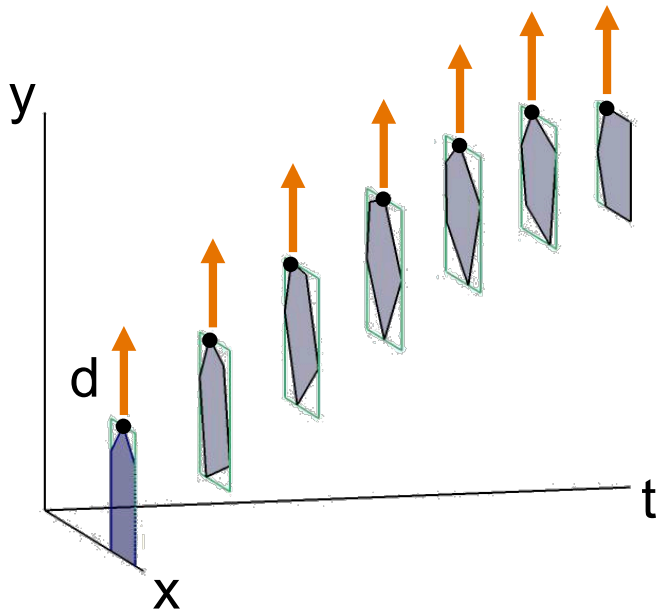


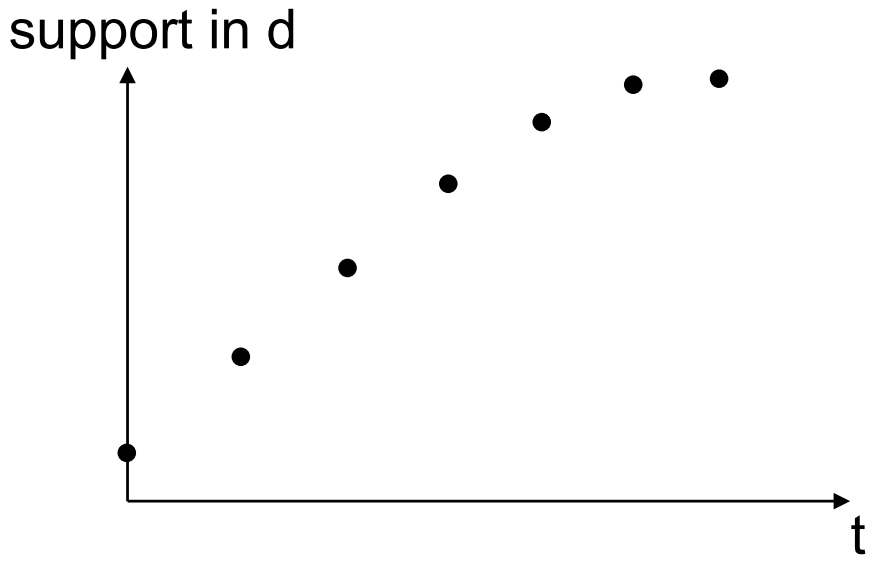
Support Sampling

- **bounds support function in all directions**
- **bounds Hausdorff distance**



Flowpipe Sampling





compute support at discrete time points

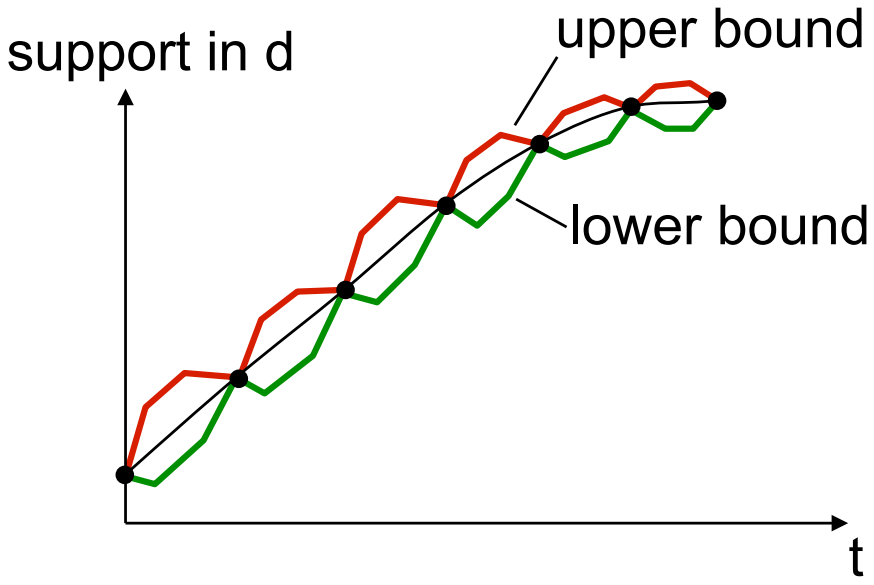
$$X_{k\delta} = (e^{A\delta})^k X_0 \oplus S_{k\delta}$$

Flowpipe Sampling - Interpolation

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

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

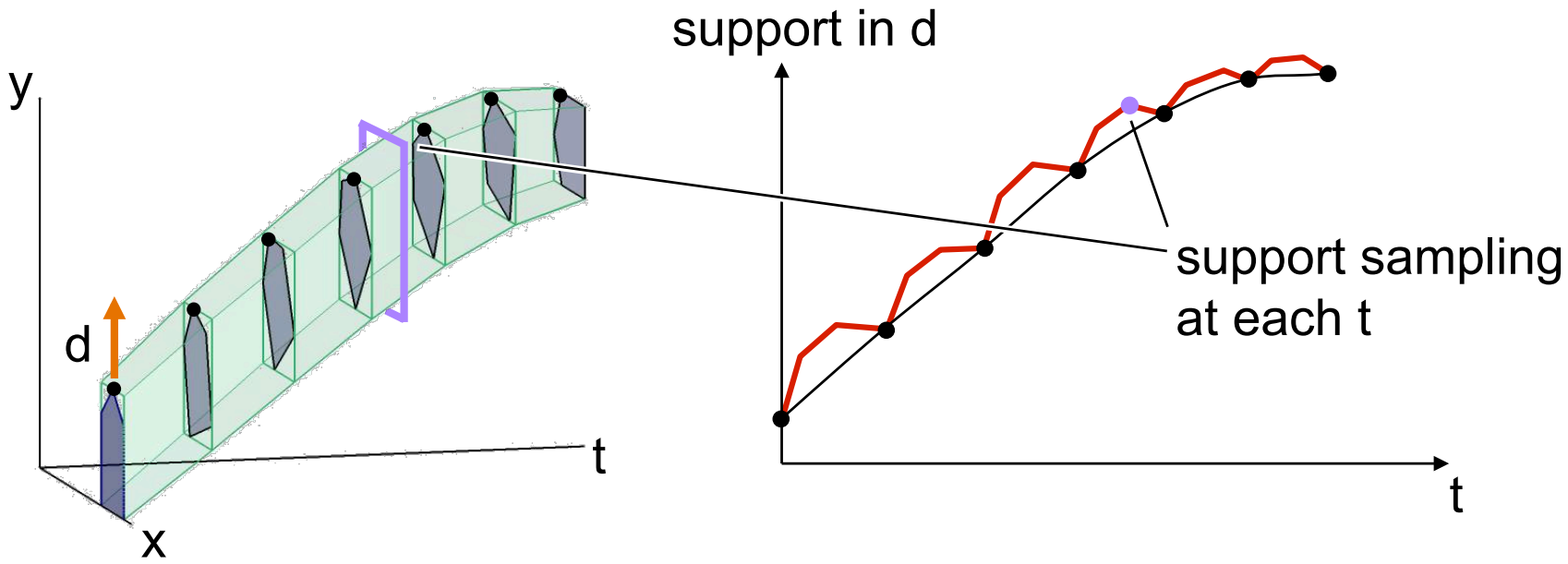
$$\Phi_2(A,\delta) = A^{-2}\left(e^{\delta A} - I - \delta A\right)$$
$$\mathcal{E}^+_\Omega(\mathcal{X}_0,\delta) = \boxdot\left(\Phi_2(|A|,\delta) \boxdot \left(A^2\mathcal{X}_0\right)\right),$$
$$\mathcal{E}^-_\Omega(\mathcal{X}_0,\delta) = \boxdot\left(\Phi_2(|A|,\delta) \boxdot \left(A^2e^{\delta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



- **independent time scales**
  - per direction
- **parallelizeable**

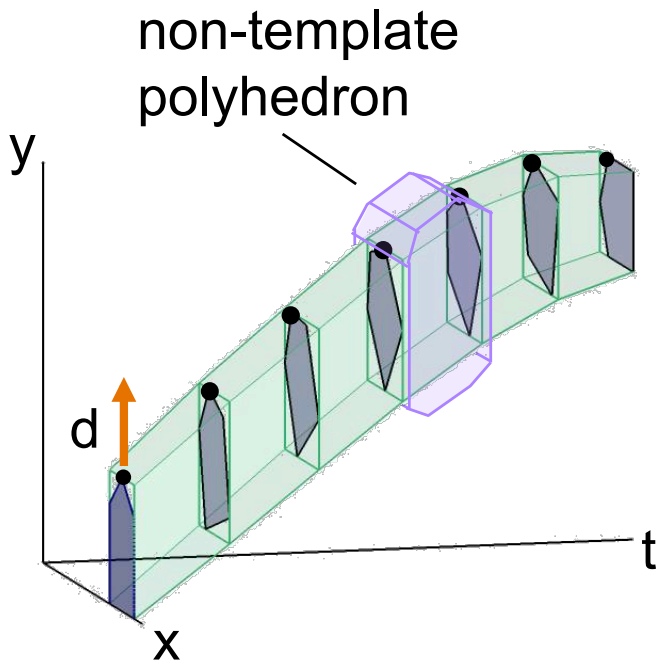
piecewise linear scalar functions

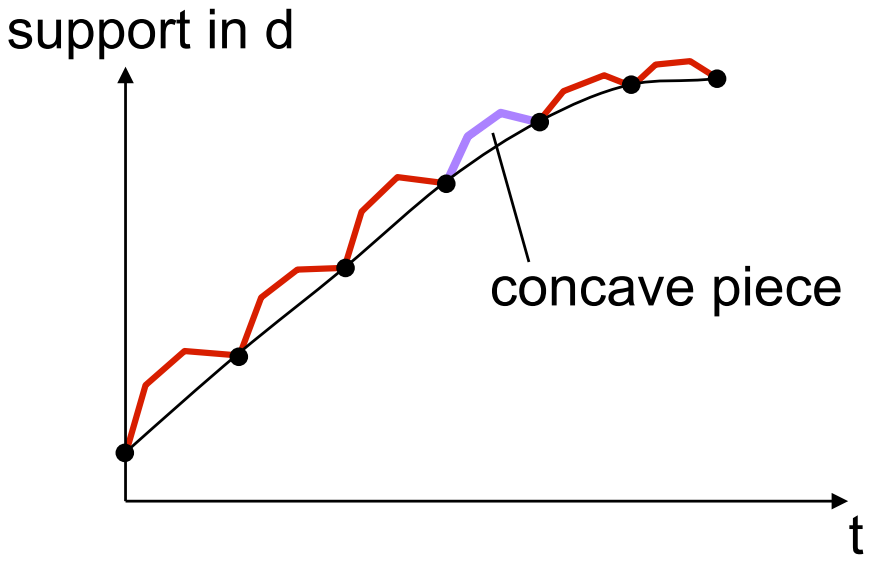
Flowpipe Sampling - Convexification



infinite union of template polyhedra
(one for each t)

Flowpipe Sampling - Convexification

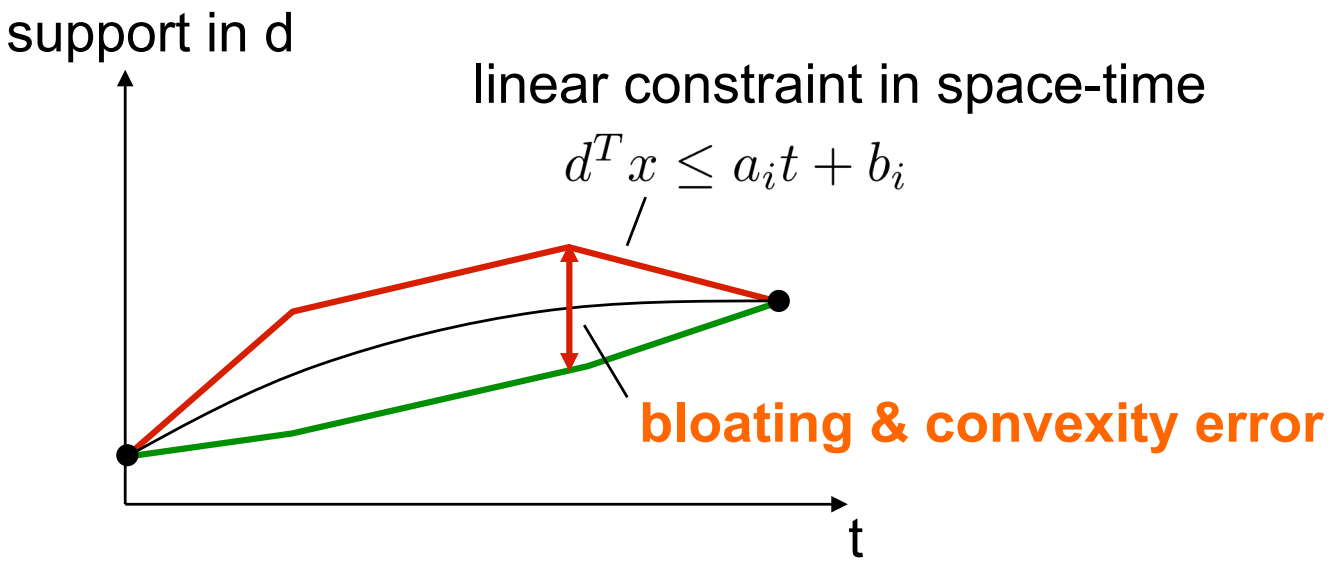




finite union of non-template polyhedra
(one for each concave piece)

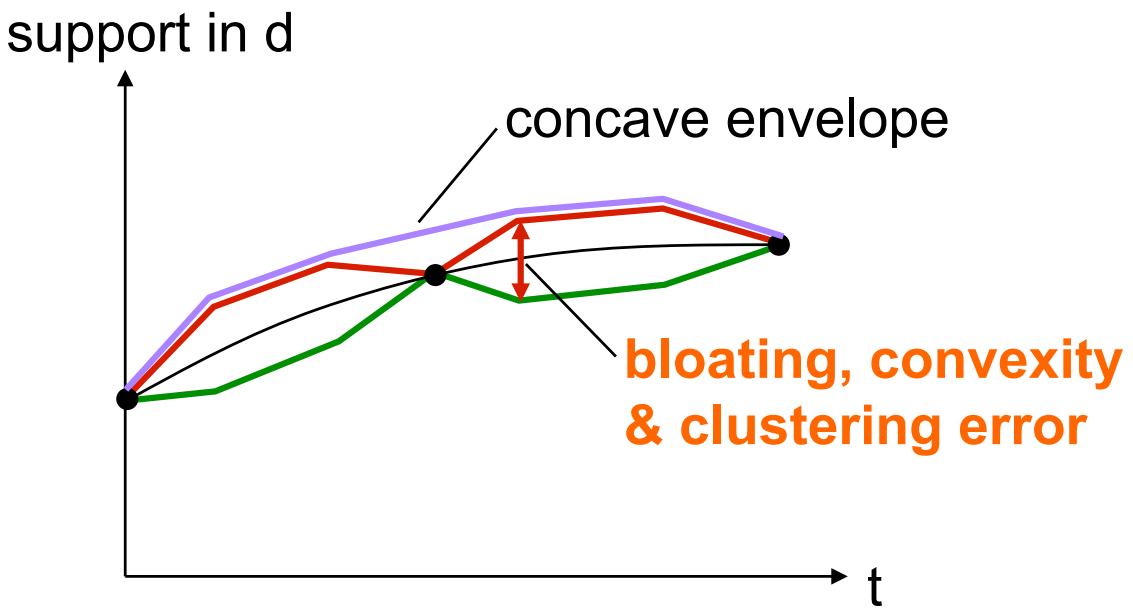
template, bloating & convexity error measurable

Flowpipe Sampling - Convexification



flowpipe samplings need to be concave
for every direction

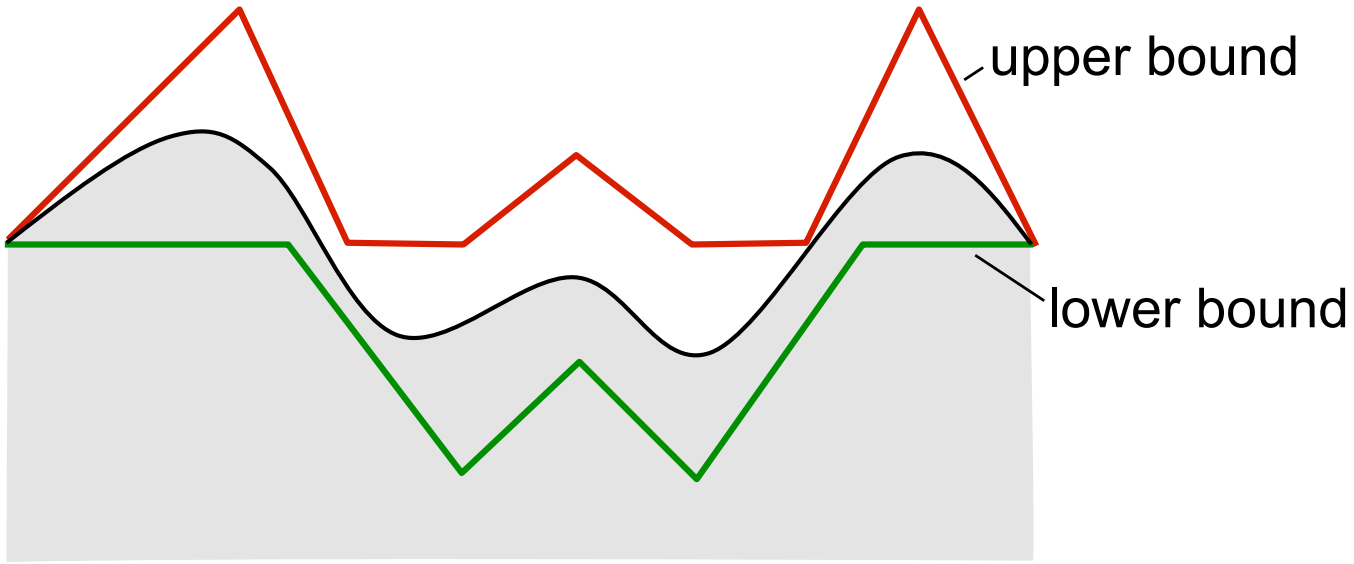
Flowpipe Sampling - Clustering



convex hull = concave envelope
(efficient for pwl functions)

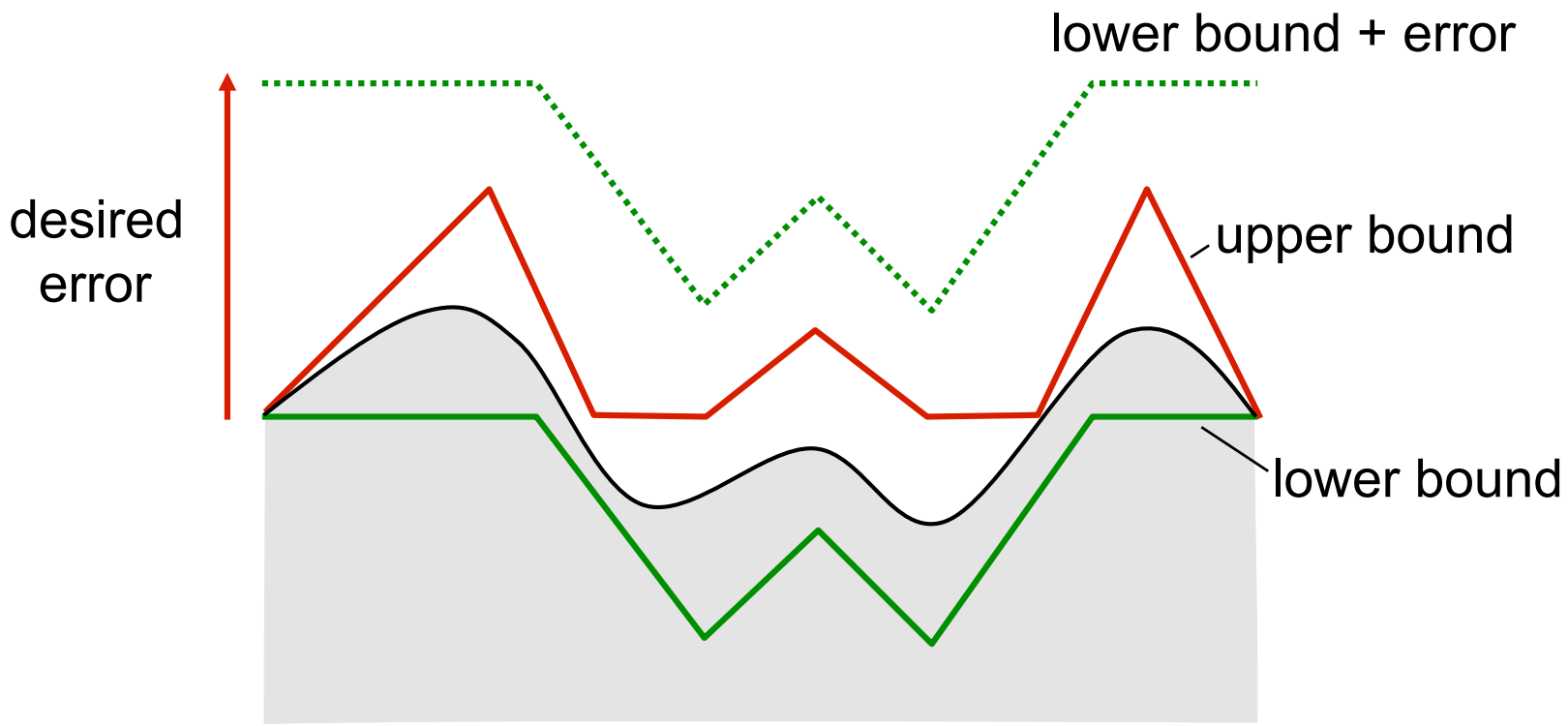
Flowpipe Sampling - Clustering

- **for given error, minimize number of convex sets**
  - equiv. number of concave pieces

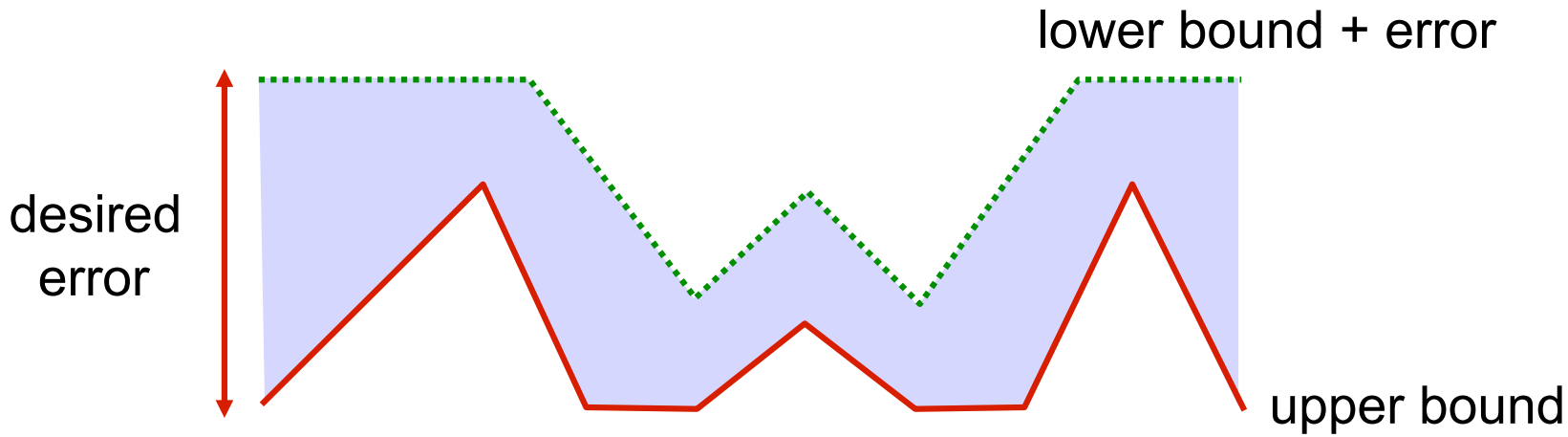


Flowpipe Sampling - Clustering

- **for given error, minimize number of convex sets**
  - equiv. number of concave pieces

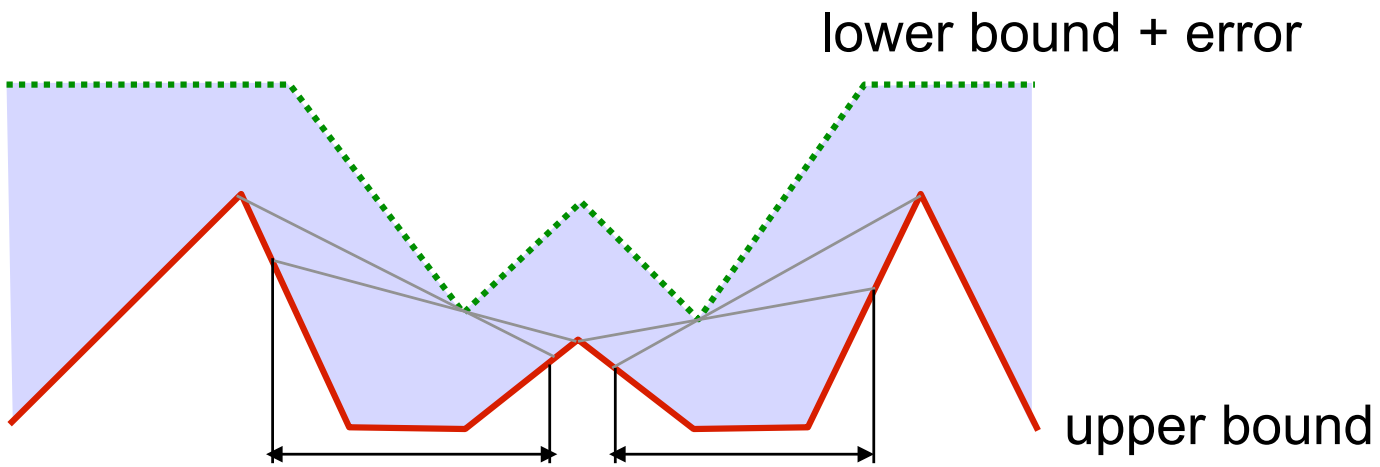


Flowpipe Sampling - Clustering



any function inside gap is
- conservative upper bound
- within desired error

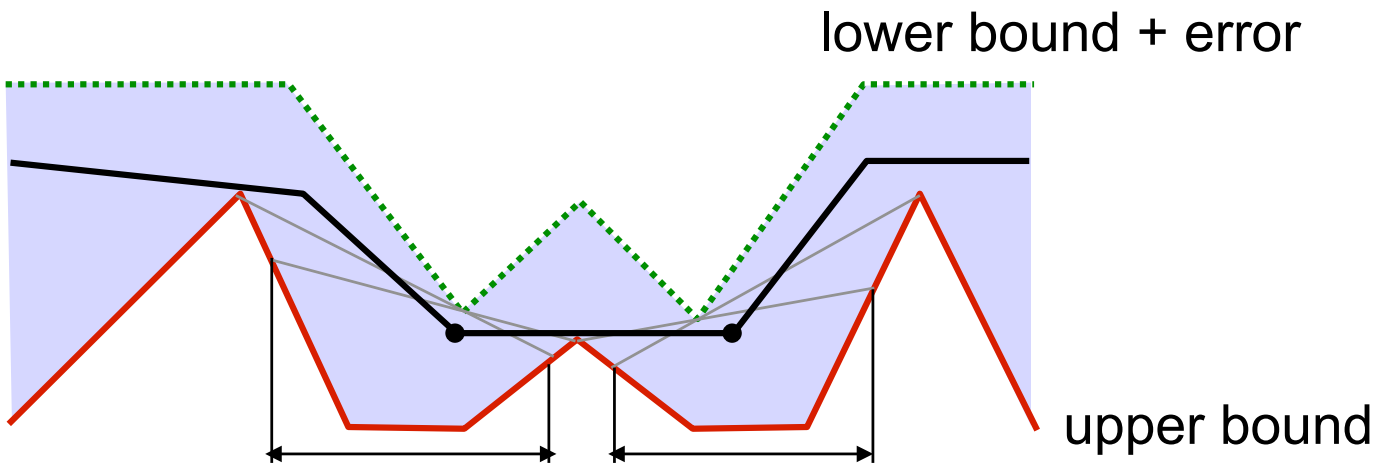
Flowpipe Sampling - Clustering



find inflection intervals:
every pw concave function must cut pieces here

(cannot drive a car from left to right without making two left turns)

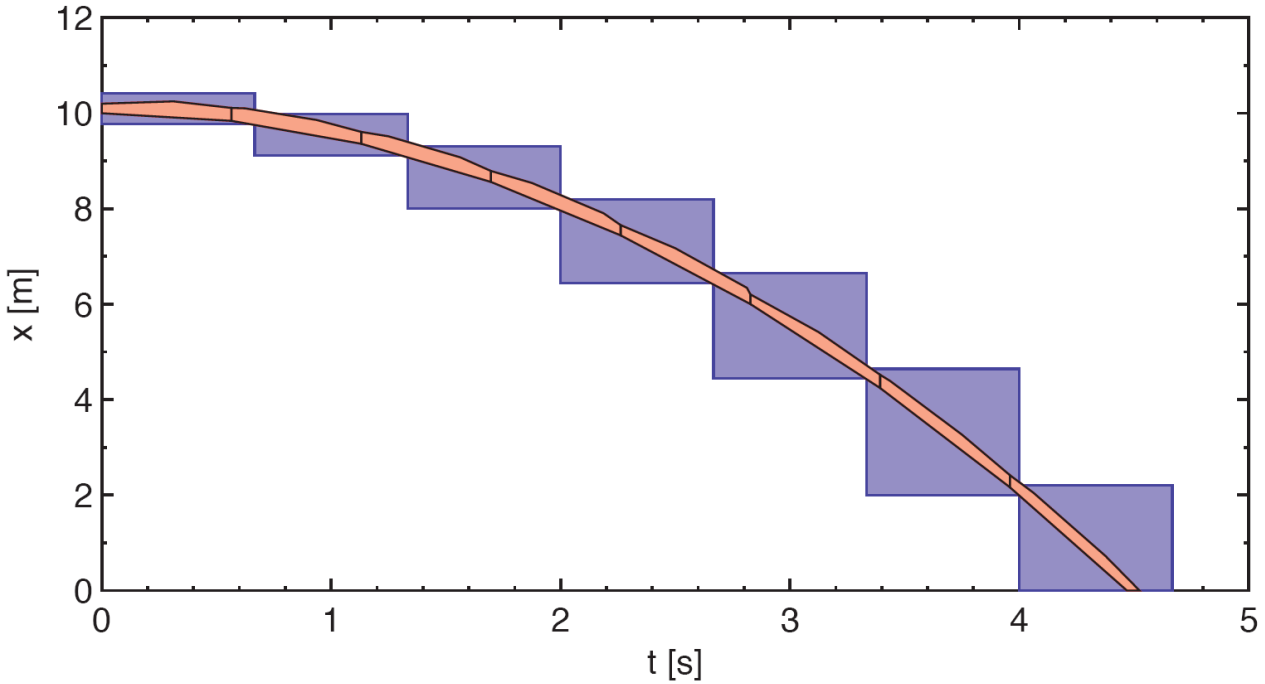
Flowpipe Sampling - Clustering



2 inflection intervals: at least 3 concave pieces

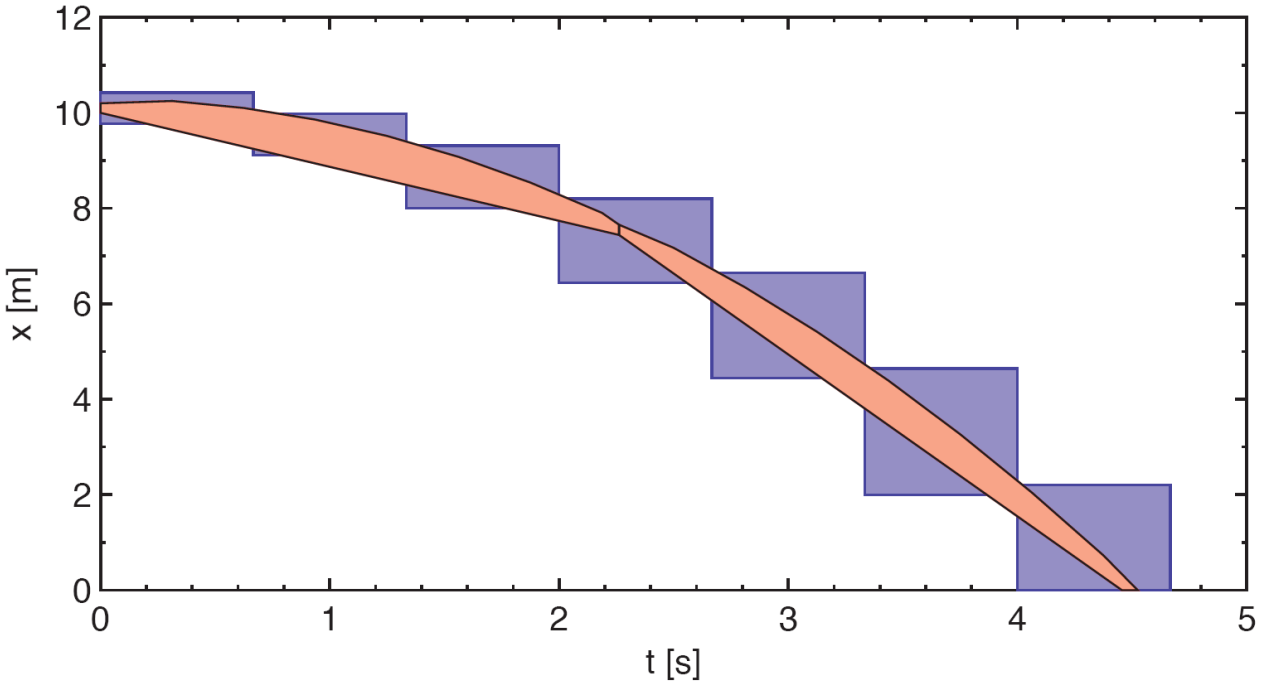
combining inflection intervals over all directions
= graph coloring problem

Example: Bouncing Ball



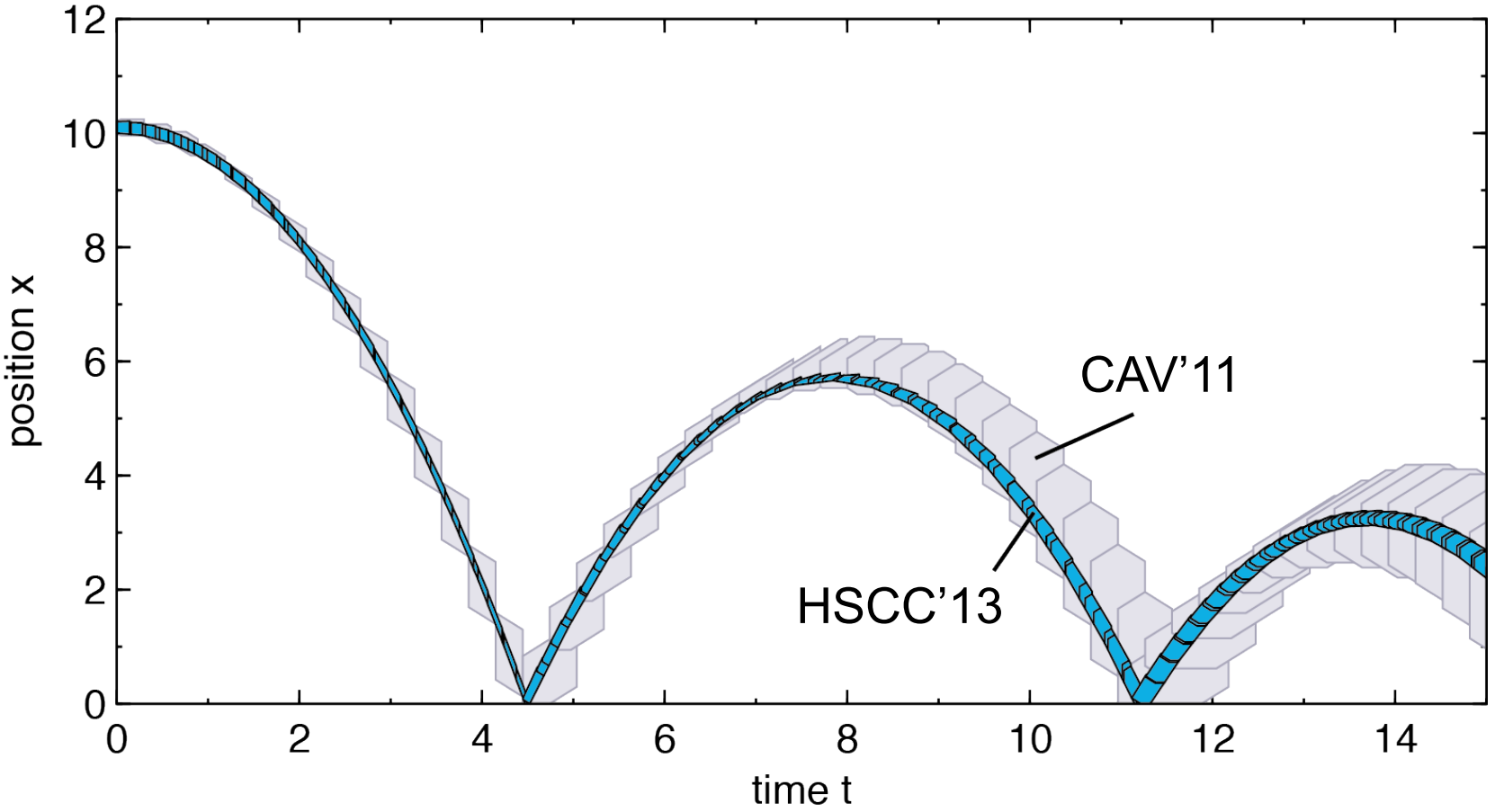
Clustering up to total error 0.1 = 8 pieces

Example: Bouncing Ball



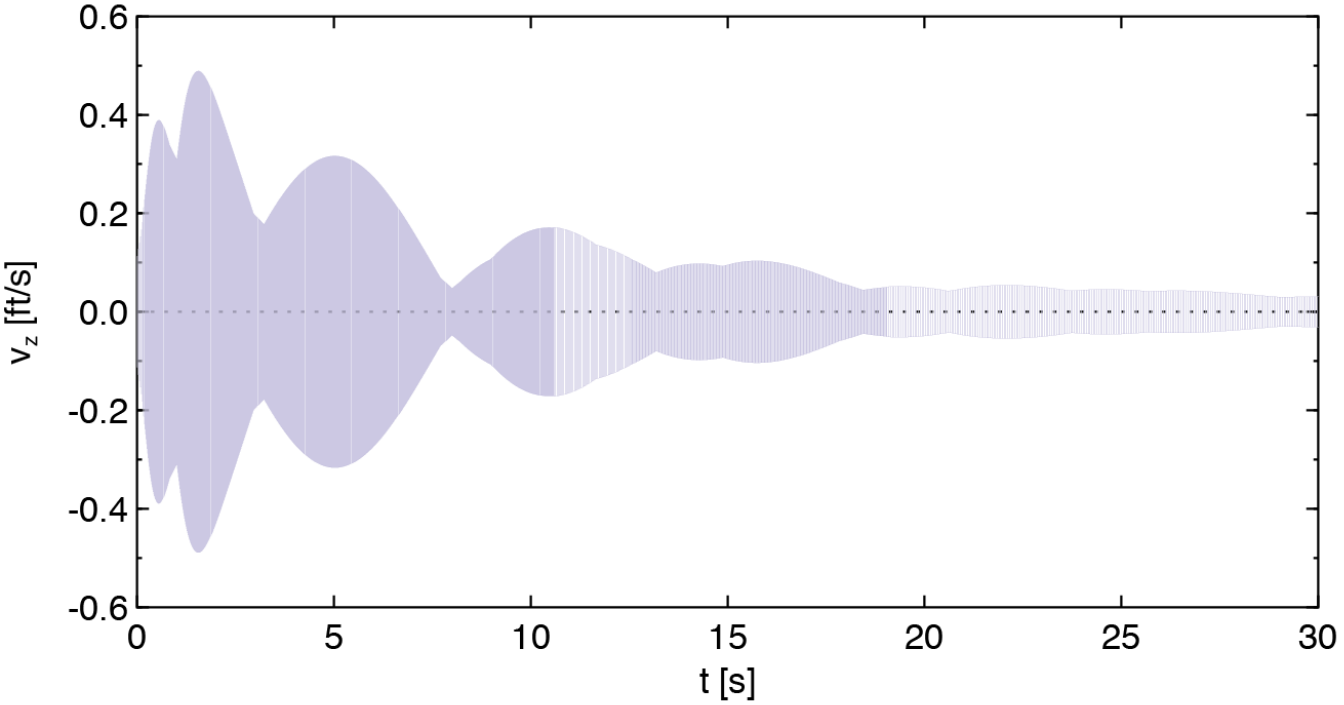
Clustering up to total error 1.0 = 2 pieces

Example: Bouncing Ball



Example: Helicopter

- **28 state variables + clock**

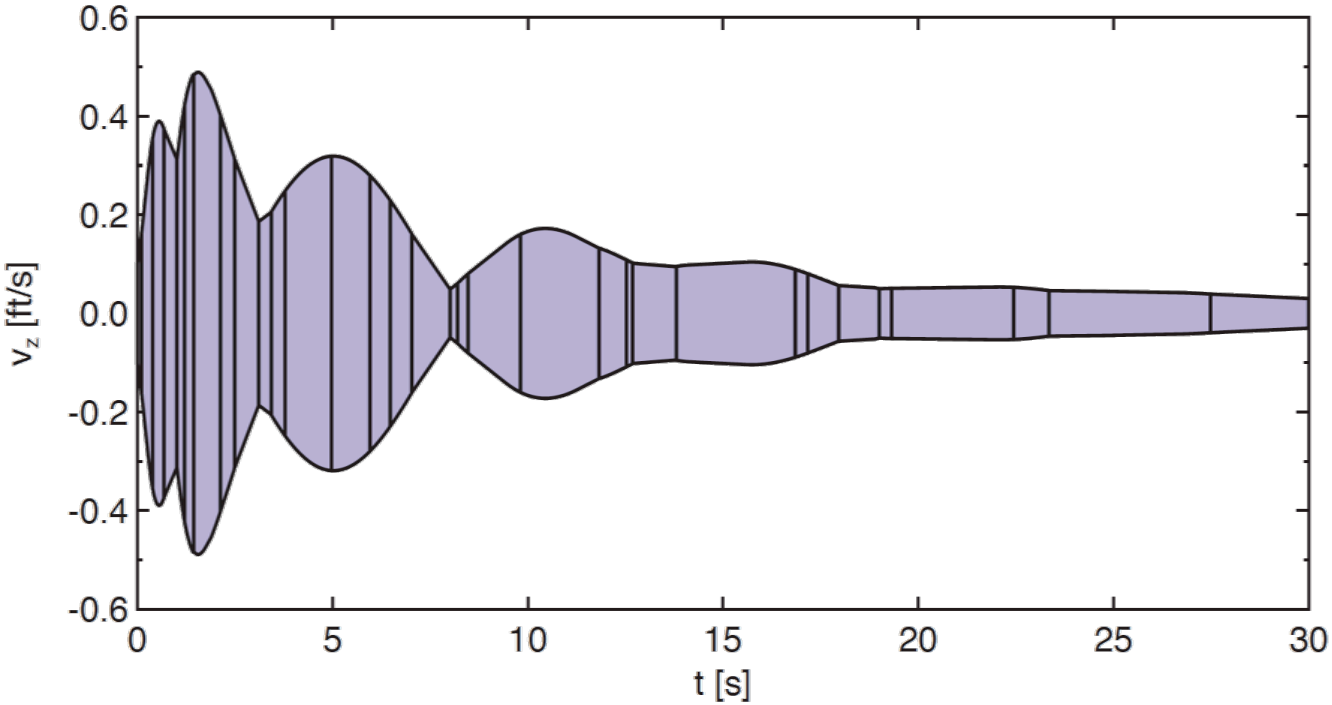


CAV'11: 1440 sets in 5.9s

1440 time steps

Example: Helicopter

- **28 state variables + clock**

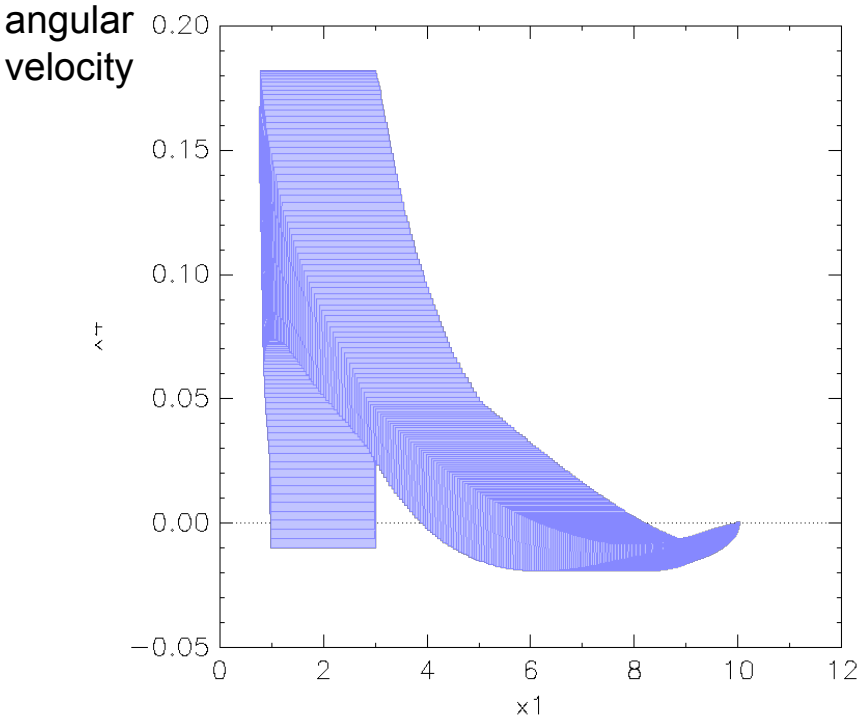


CAV'11: **32** sets in 15.2s (4.8s clustering)

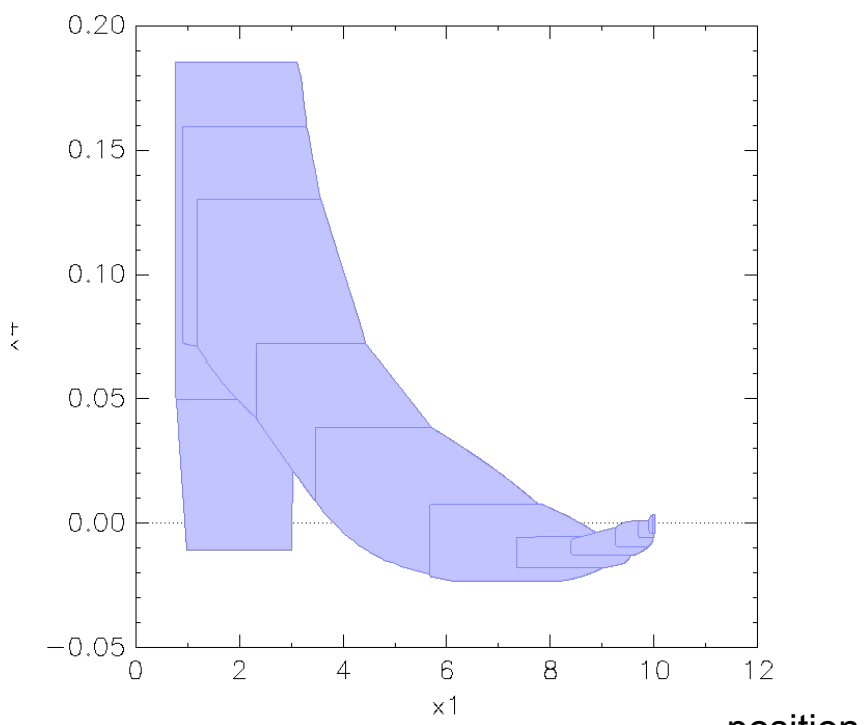
2 -- 3300 time steps, median 360

Example: Overhead Crane

- **4 state variables, error < 0.05**



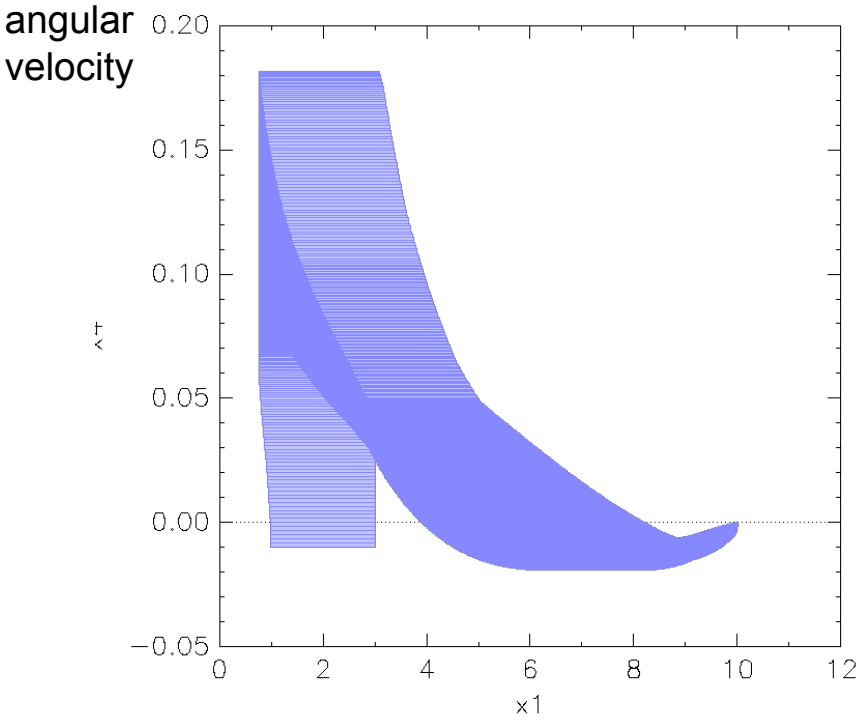
369 sets, 0.15s



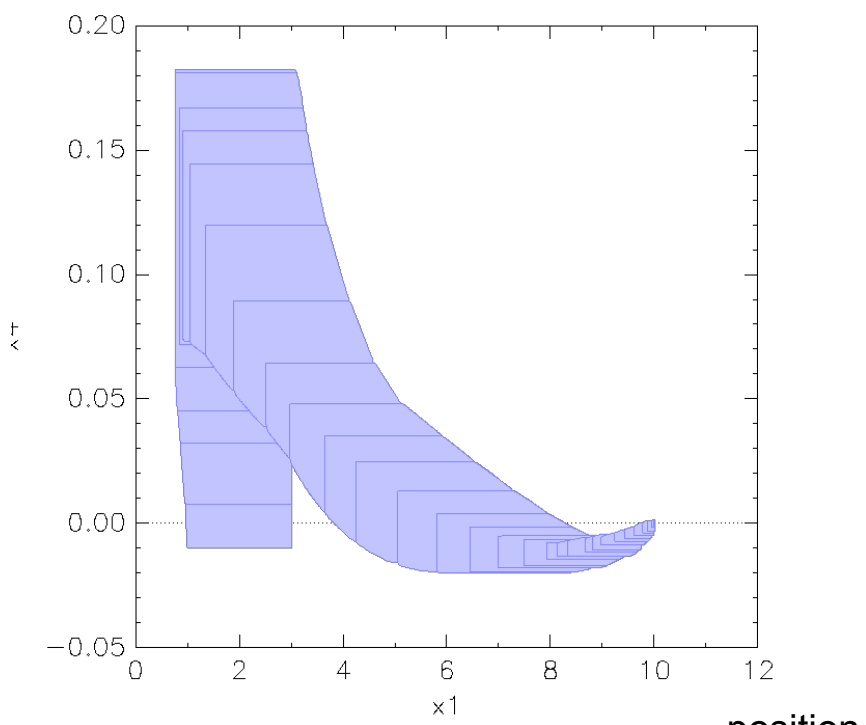
15 sets, 0.28s

Example: Overhead Crane

- **4 state variables, error < 0.005**



1108 sets, 0.36s



32 sets, 0.46s

Performance Comparison

	CAV'11		HSCC'13	
	Time	Sets	Time	Sets
Helicopter (29)	5.90	1440	15.20	**32**
Helicopter 2 (29)	10.40	2563	14.30	**10**
Bouncing Ball (3)	0.04	261	0.02	**56**
Bouncing Ball w. Inputs (3)	6.30	17208	29.90	**64**
Three-Tank (3)	0.03	105	0.03	**9**
Overhead Crane (4)	0.12	369	0.17	**15**

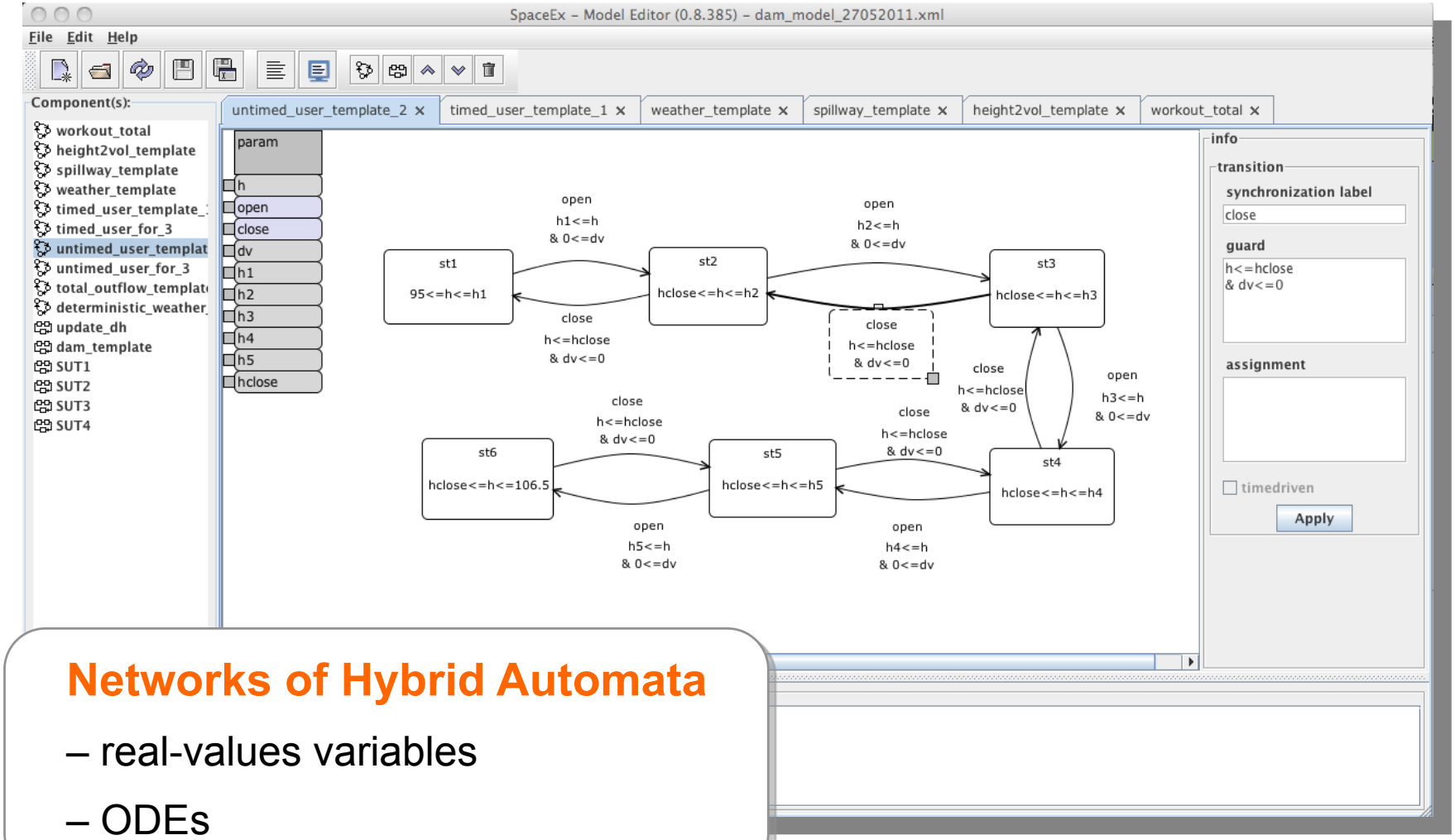
Outline

- Hybrid Systems and Reachability
- Reachability with Support Functions
- Approximation in Space-Time
- **SpaceEx Development Platform**

SpaceEx Verification Platform

- **Analysis of Hybrid Systems**
  - Reachability
  - Monitoring
  - Simulation
- **Open Source: spaceex.imag.fr**
  - proprietary polyhedra library
  - number type is templated (substitute your own)
  - interfaces to linear programming solvers (GLPK,PPL), Parma Polyhedra Library, ode solvers (CVODES)

SpaceEx Model Editor

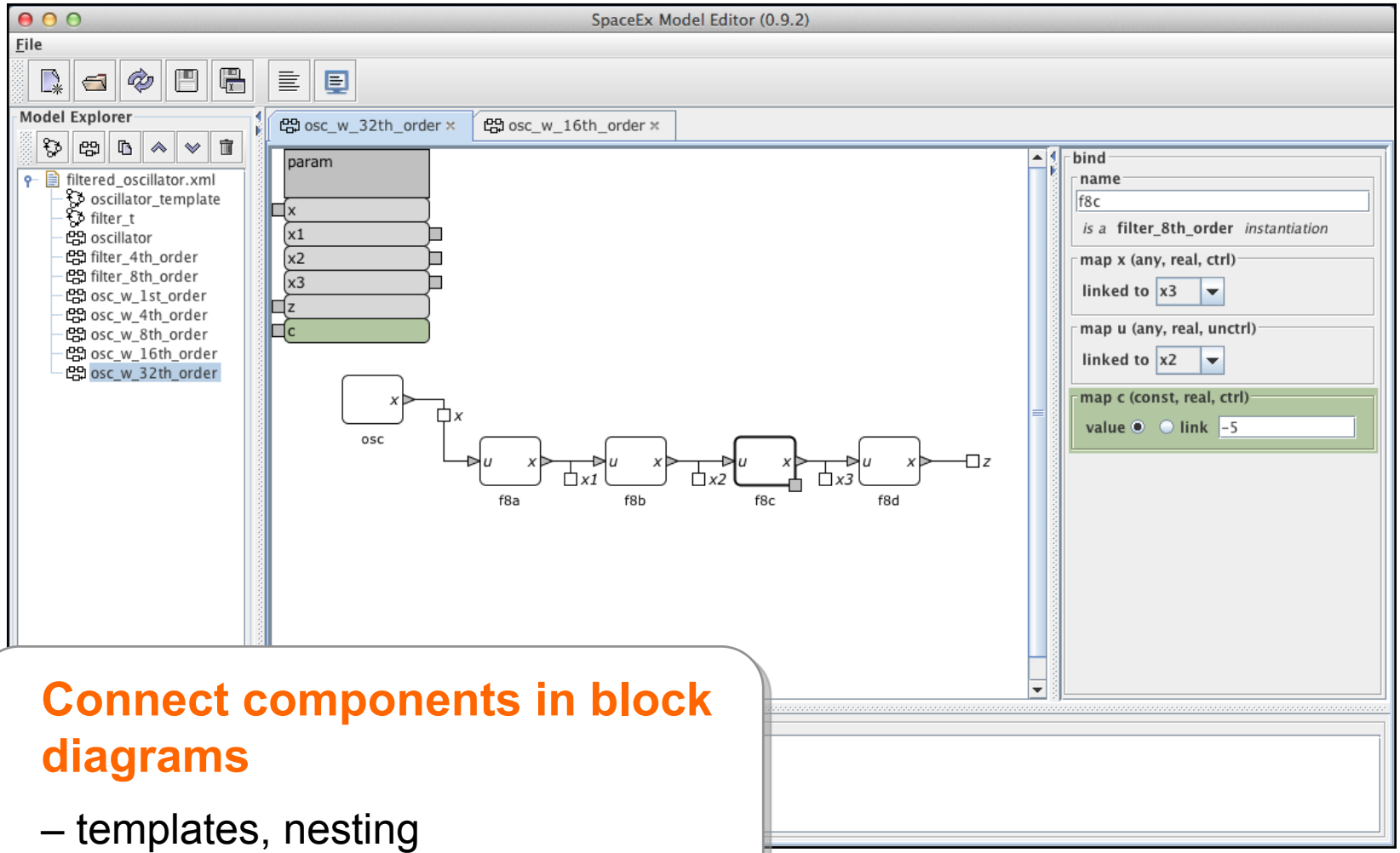


Networks of Hybrid Automata

– real-values variables

– ODEs

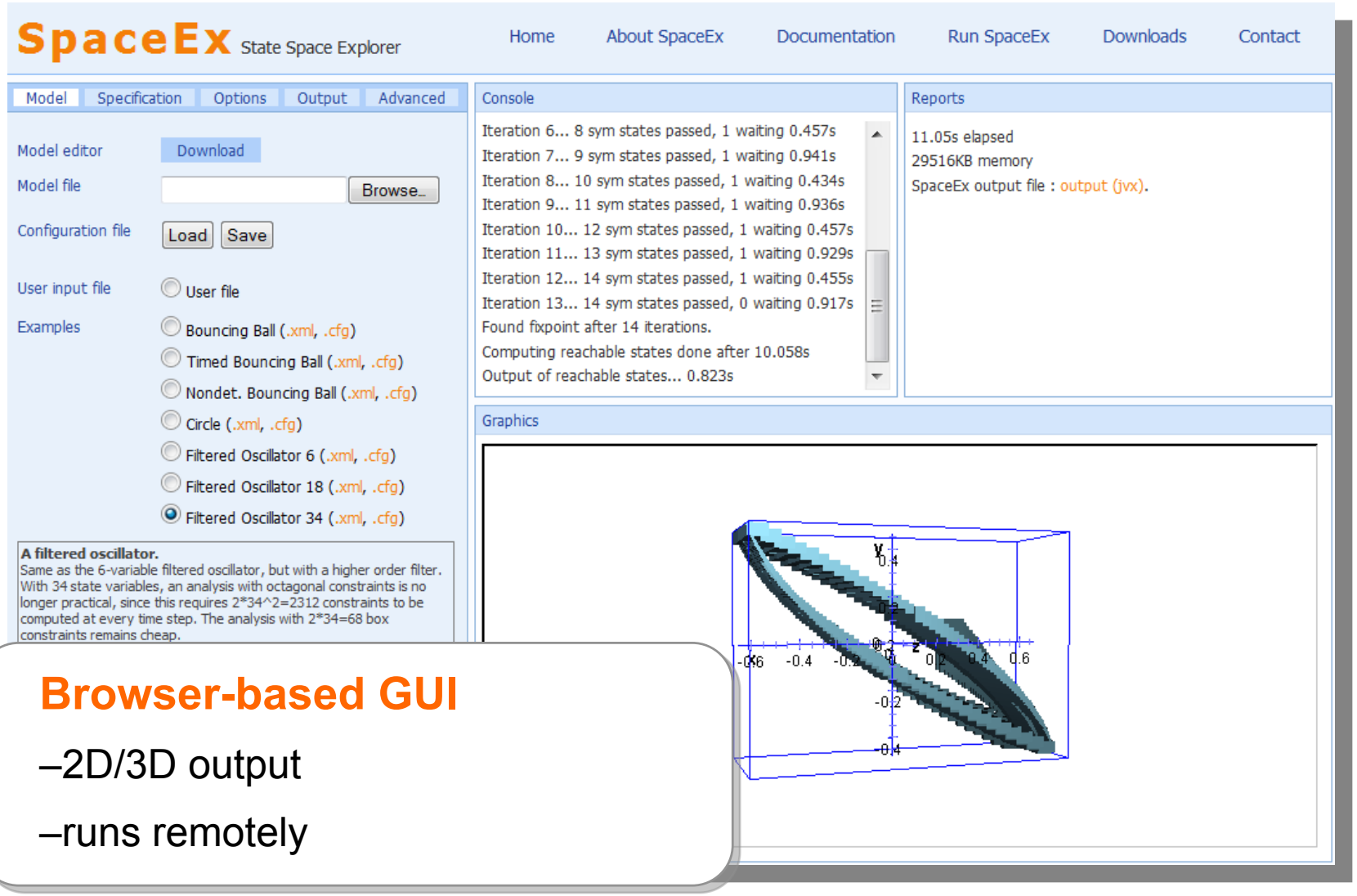
SpaceEx Model Editor



Connect components in block diagrams

– templates, nesting

SpaceEx Web Interface

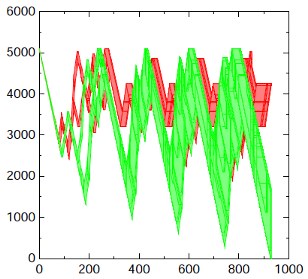


Browser-based GUI

–2D/3D output

–runs remotely

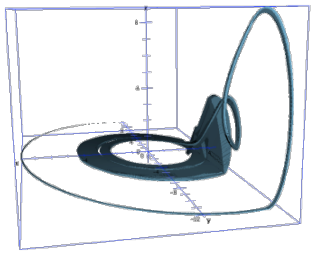
SpaceEx Reachability Algorithms



PHAVer

–constant dynamics (LHA)

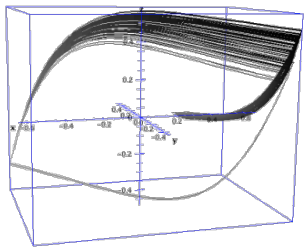
–formally sound and exact



Support Function Algo

–many continuous variables

–low discrete complexity



Simulation

–nonlinear dynamics

–based on CVODE

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)
  - extension to nonlinear dynamics

spaceex.imag.fr