Safety Analysis of Hybrid Systems with SpaceEx

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

Colas Le Guernic
New York University CIMS

Antoine Girard
Laboratoire Jean Kuntzmann, France

CMACS Seminar, Pittsburgh, PA, July 20, 2011

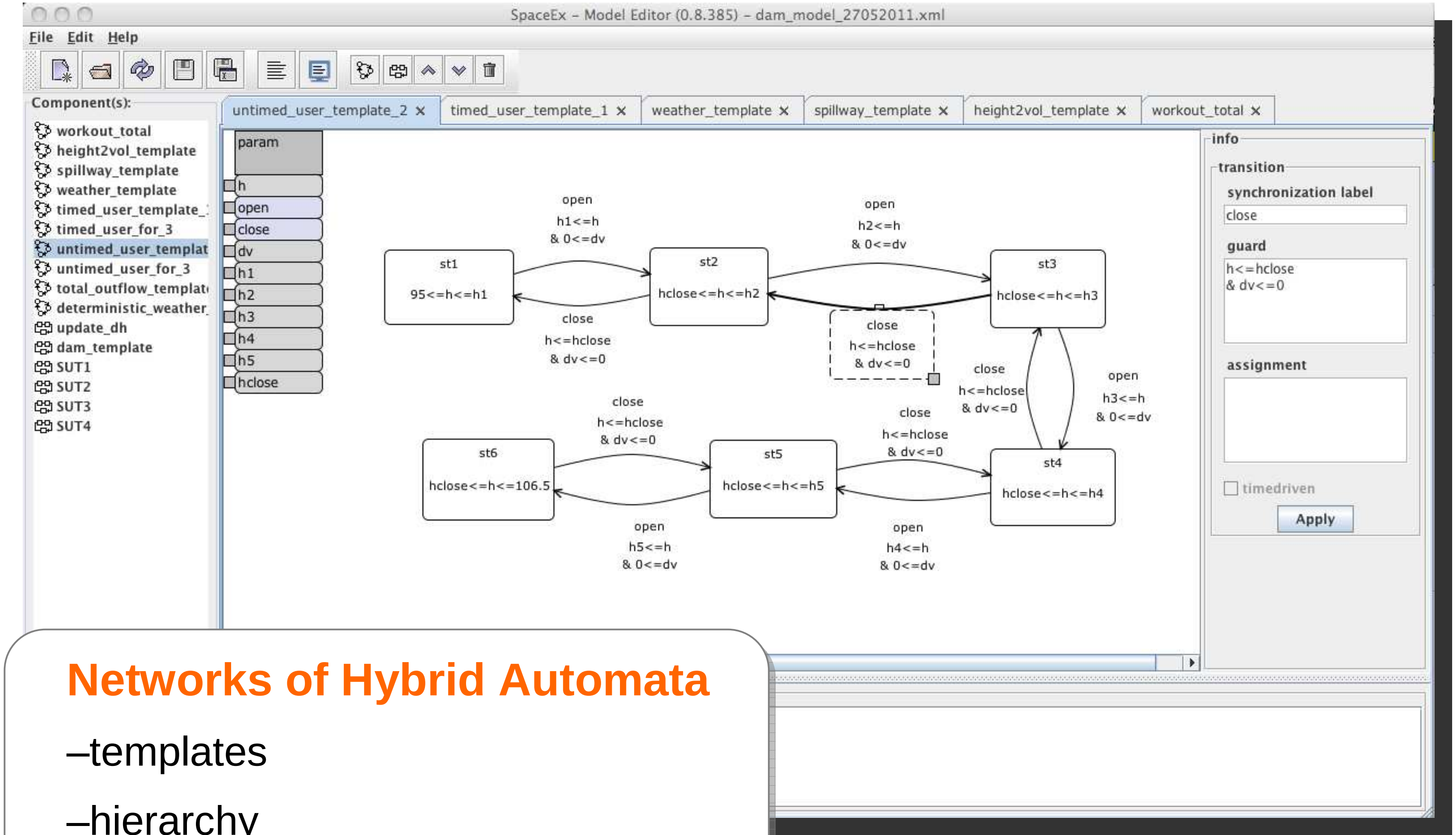
Outline

- **SpaceEx Verification Platform**
- **SpaceEx Reachability Algorithm**
  – Time Elapse Computation with Support Functions
  – Transition Successors Mixing Support Functions and Polyhedra
  – Fixpoint Algorithm: Clustering & Containment
- **Examples**

SpaceEx Verification Platform

- **Platform for developing verification algorithms**
  - Analysis Core (90kloc C++)
  - Model Editor
  - Web Interface
- **Provides data structures, operators, infrastructure**
  - proprietary polyhedra library
  - number type is templated (substitute your own)
  - interfaces to linear programming solvers (GLPK,PPL), Parma Polyhedra Library, ode solvers (CVODES)
- **Open Source: spaceex.imag.fr**

SpaceEx Model Editor

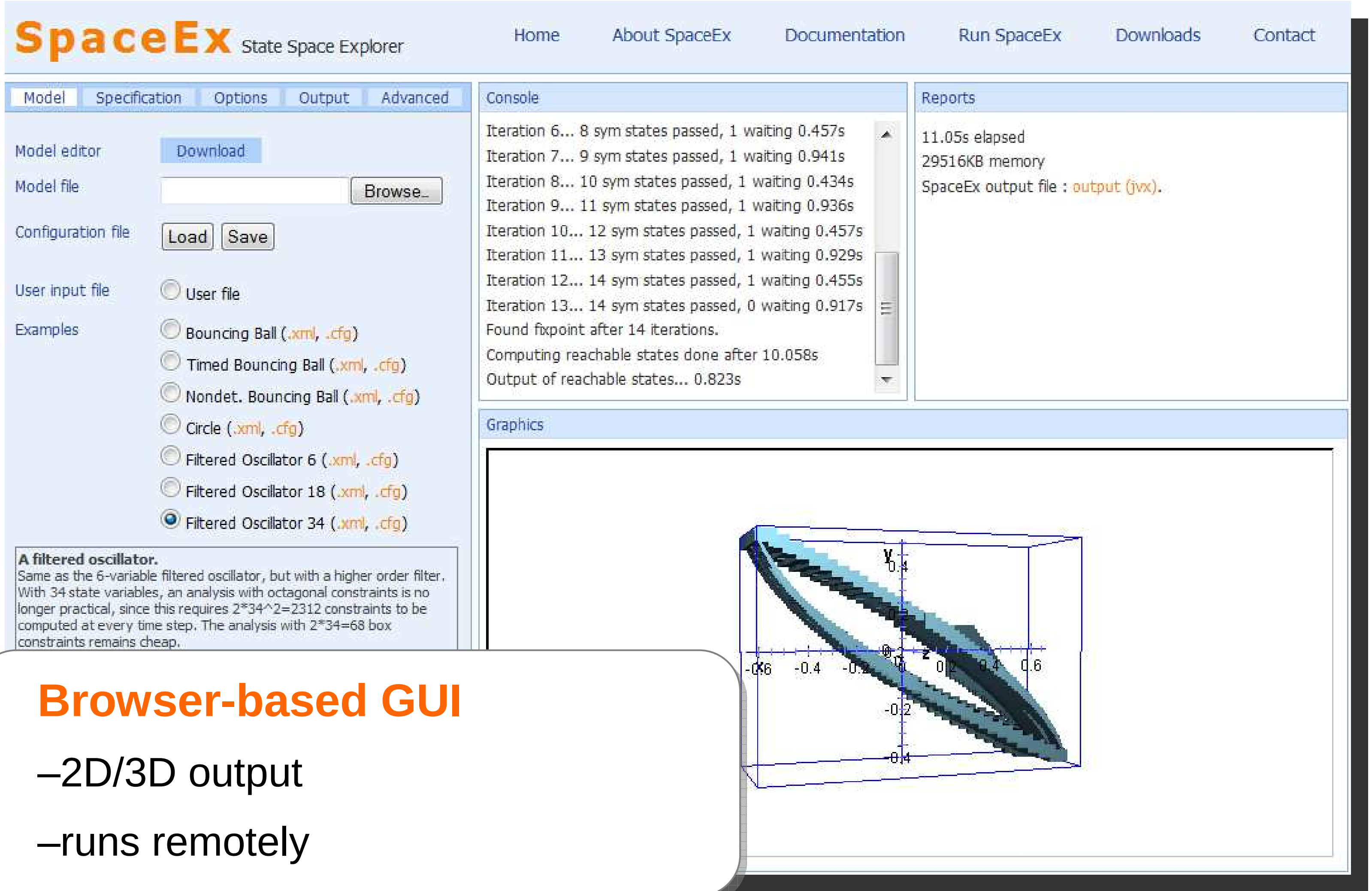


Networks of Hybrid Automata

–templates

–hierarchy

SpaceEx Web Interface

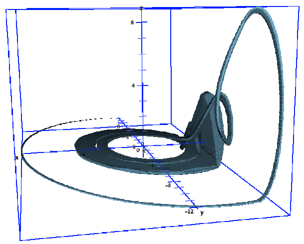


Browser-based GUI

– 2D/3D output

– runs remotely

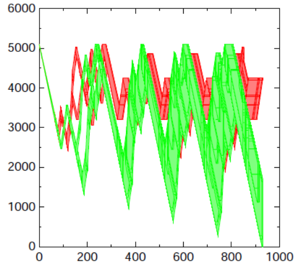
SpaceEx Reachability Algorithms



Support Function Algo

–many continuous variables

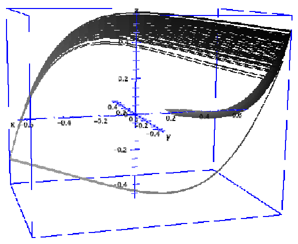
–low discrete complexity



PHAVer

–constant dynamics (LHA)

–formally sound and exact

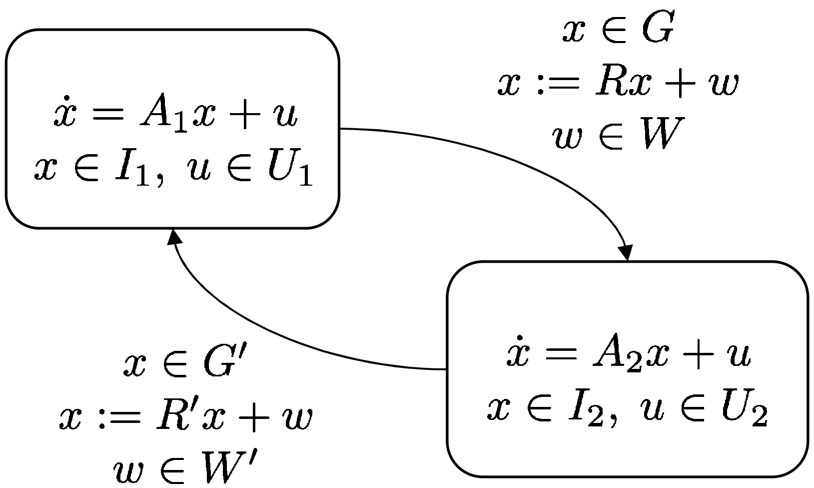


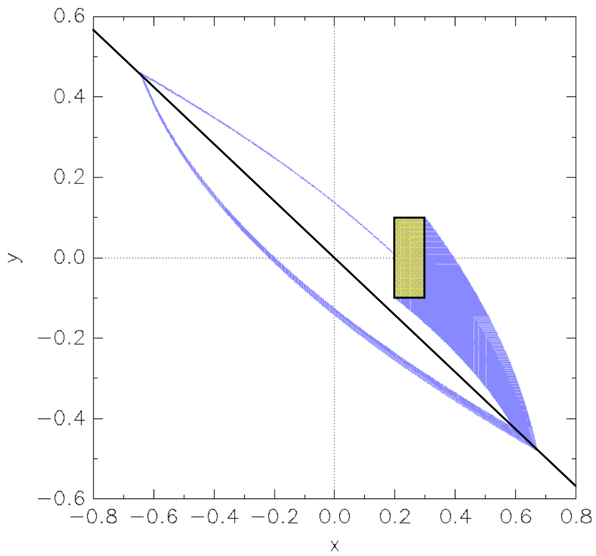
Simulation

–nonlinear dynamics

–based on CVODE

Hybrid Automata with Affine Dynamics





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

Reachability of Hybrid Automata

- **reachability is hard for continuous dynamics**
  - complex, nonconvex sets
- **even harder for hybrid dynamics**
  - involves reachability of continuous dynamics
  - plus event detection over a dense domain
- **approximations needed**

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

Outline

- **SpaceEx Verification Platform**
- **SpaceEx Approximation Algorithm**
  - Time Elapse Computation with Support Functions
  - Transition Successors Mixing Support Functions and Polyhedra
  - Fixpoint Algorithm: Clustering & Containment
- **Examples**

Time Elapse with Affine Dynamics

- **Affine Flow**
  - nondeterministic affine differential equation:

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

- **Solve with superposition principle**
  - disregard inputs: “autonomous dynamics”
  - add inputs afterwards

Linear Dynamics

- **"Autonomous" part of the dynamics:**

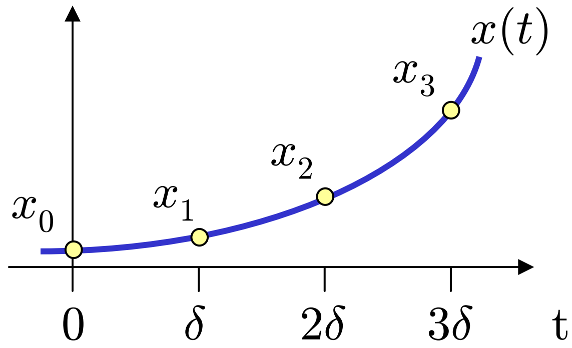
$$\dot{x} = Ax, \quad x \in \mathbb{R}^n$$

- **Known solutions:**
  - analytic solution in continuous time
  - explicit solution at discrete points in time (up to arbitrary accuracy)
- **Approach for Reachability:**
  - Compute reachable states over finite time: $Reach_{[0,\mathrm{T}]}(X_{Ini})$
  - Use time-discretization, but with care!

Time-Discretization for an Initial Point

- **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):**

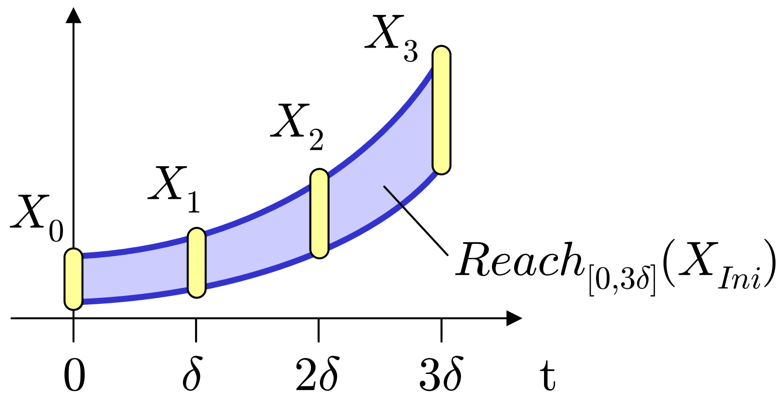
$$\begin{aligned} x_0 &= x_{Ini} \\ x_{k+1} &= e^{A\delta} x_k \end{aligned}$$

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

Time-Discretization for an Initial Set

- **Explicit solution in discretized time**

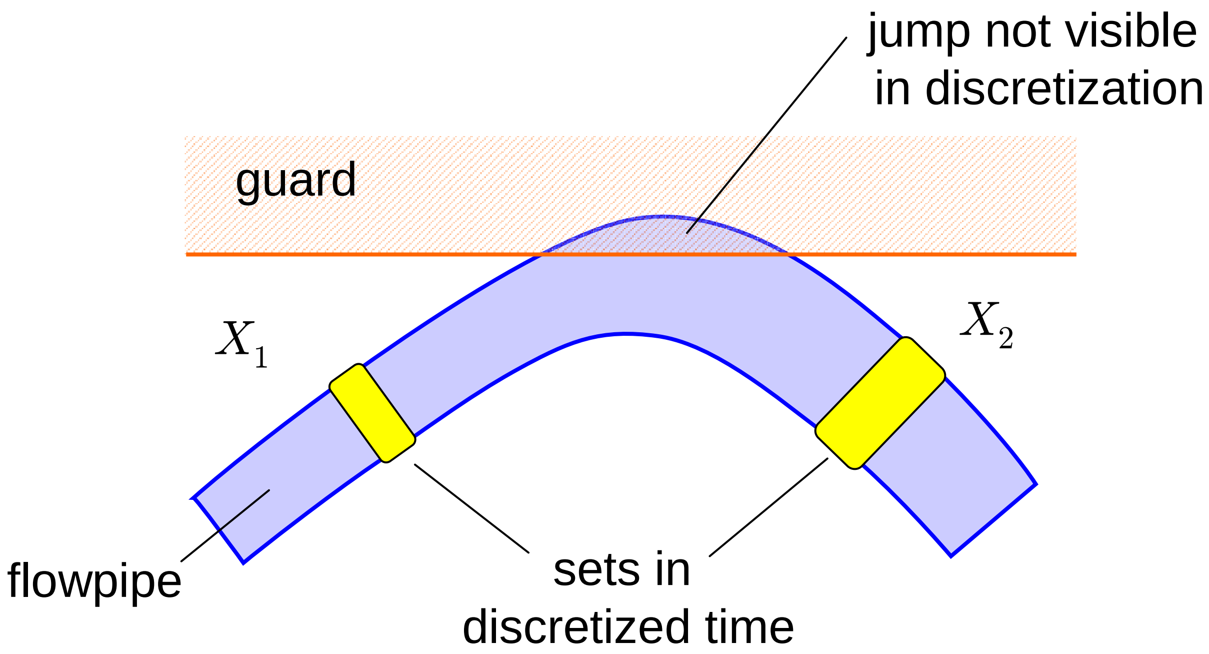
$$\begin{aligned} X_0 &= X_{Ini} \\ X_{k+1} &= e^{A\delta} X_k \end{aligned}$$



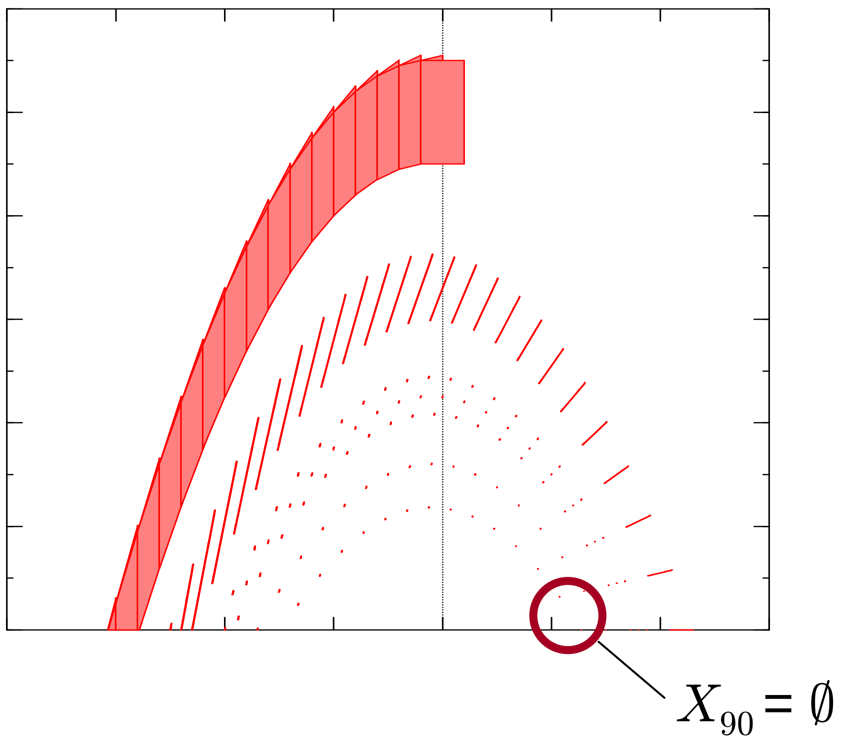
- **Acceptable solution for purely continuous systems**
  – $x(t)$ is in $\epsilon(\delta)$-neighborhood of some X_k
- **Unacceptable for hybrid systems**
  – discrete transitions might “fire” between sampling times
  – if transitions are “missed,” $x(t)$ not in $\epsilon(\delta)$-neighborhood

Time Discretization for Hybrid Systems

- **One can miss jumps**
  - intersection with guard set



Bouncing Ball



– In other examples this error might not be as obvious…

Reachability by Time-Discretization

- **Goal:**
  - Compute sequence Ω_k over bounded time $[0, N\delta]$ such that:

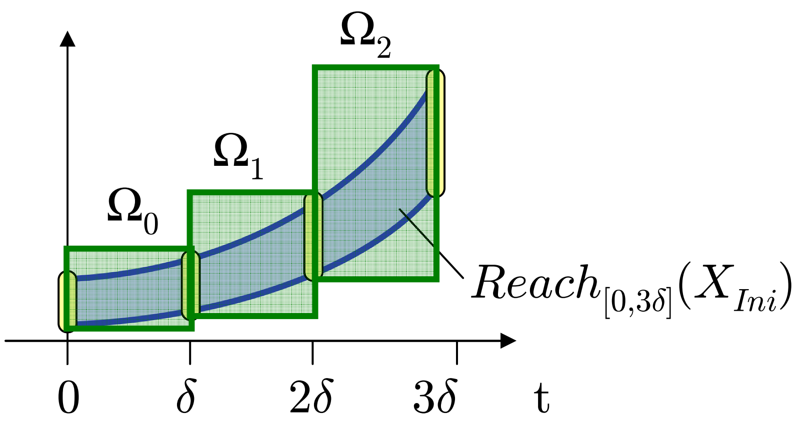
$$\mathrm{Reach}_{[0,N\delta]}(X_{Ini}) \subseteq \Omega_0 \cup \Omega_1 \cup \ldots \cup \Omega_N$$

- **Approach:**
  - Refine Ω_k by recurrence:

$$\Omega_{k+1} = e^{A\delta}\Omega_k$$

  - Condition for Ω_0:

$$\mathrm{Reach}_{[0,\delta]}(X_{Ini}) \subseteq \Omega_0$$



Nondeterministic Affine Dynamics

- **Let's include the effect of inputs:**

$$\dot{x} = Ax + u, \quad x \in \mathbb{R}^n, u \in U$$

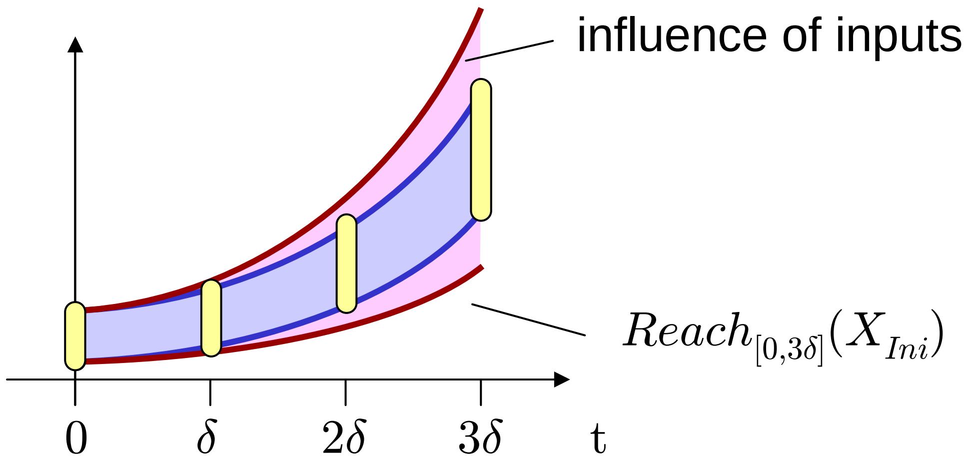
  – variables $x_1,\ldots,x_n$, inputs $u_1,\ldots,u_p$

- **Input u models nondeterminism**
  – disturbances etc.
  – can be used for overapproximating nonlinear dynamics ($U =$ bounds of approximation error)

Nondeterministic Affine Dynamics

- **Superposition Principle**

$$x(t) = \underbrace{e^{A\delta}x(0)}_{\text{autonomous dynamics}} + \underbrace{\int_0^t e^{A(\delta-\tau)}u(\tau)d\tau}_{\text{influence of inputs}}$$



Nondeterministic Affine Dynamics

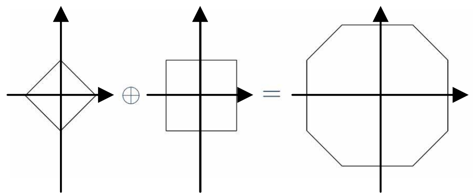
- **Set overapproximation of input influence**
  - How far can the input "push" the system in δ time?
  - from Taylor series expansion

$$\Psi = \delta U \oplus \mathcal{E}_\Psi \qquad \text{(input influence set)}$$

$$\mathcal{E}_\Psi = \boxdot\left(\Phi_\Psi \boxdot (A\mathcal{U})\right) \qquad \text{(error bound)}$$

$$\Phi_\Psi = |A|^{-2}\left(e^{\delta|A|} - I - \delta|A|\right) \qquad \text{(matrix)}$$

- **Operators:**
  - Minkowski Sum: $A \oplus B = \{a + b \mid a \in A,\ b \in B\}$
  - Symmetric Bounding Box: $\boxdot(\cdot)$
  - Linear Transform

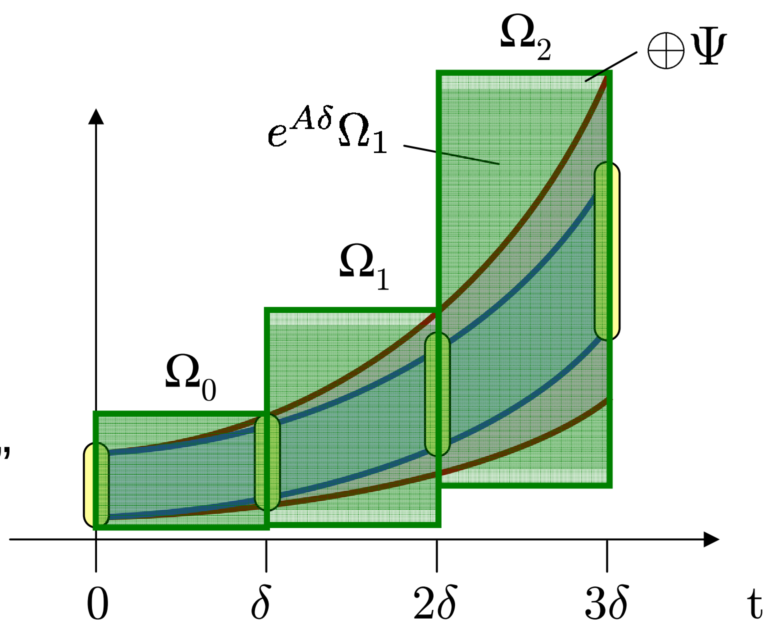


Nondeterministic Affine Dynamics

- **Recurrence equation with influence of inputs**

$$\Omega_{k+1} \quad = \quad e^{A\delta}\Omega_k \oplus \Psi$$

- **Still needed:**
  - approximation of the initial time step with Ω_0
  - called “approximation model”



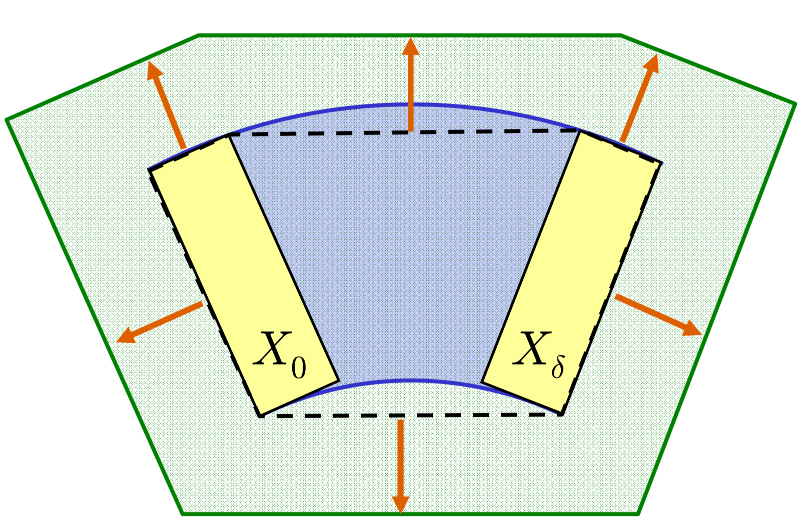
Approximation Models – Prev. Work

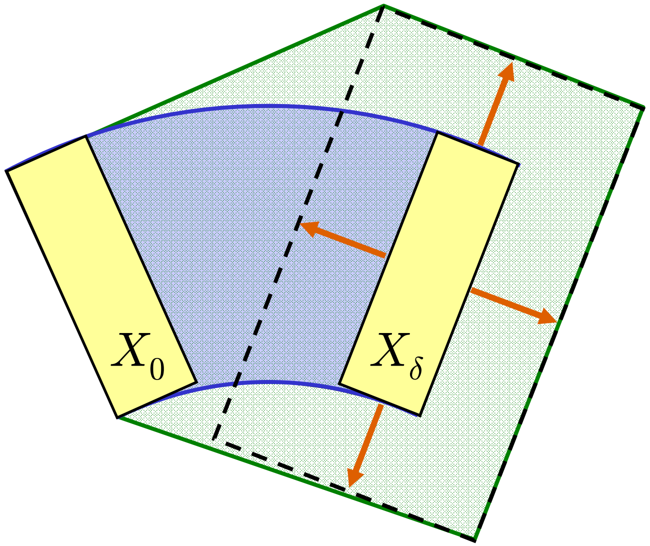
- **convex hull constraints + bloat with** $\sim e^{\|A\|\delta}$

  Asarin, Dang et al., HSCC 2000

- **bloat last set with** $\sim e^{\|A\|\delta}$ **+ convex hull**

  Le Guernic, Girard, CAV 2009



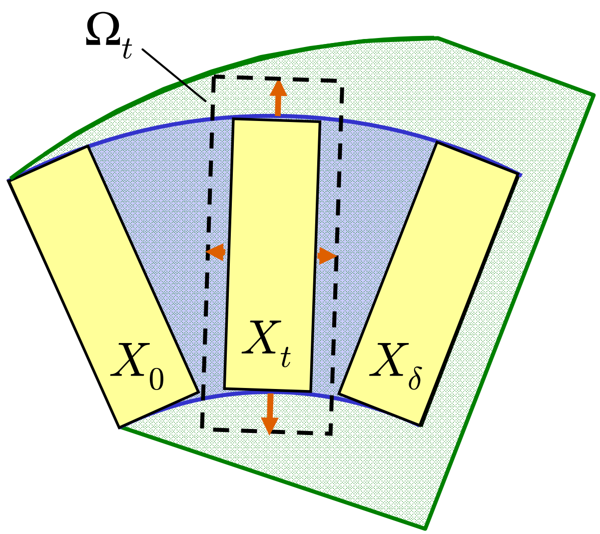


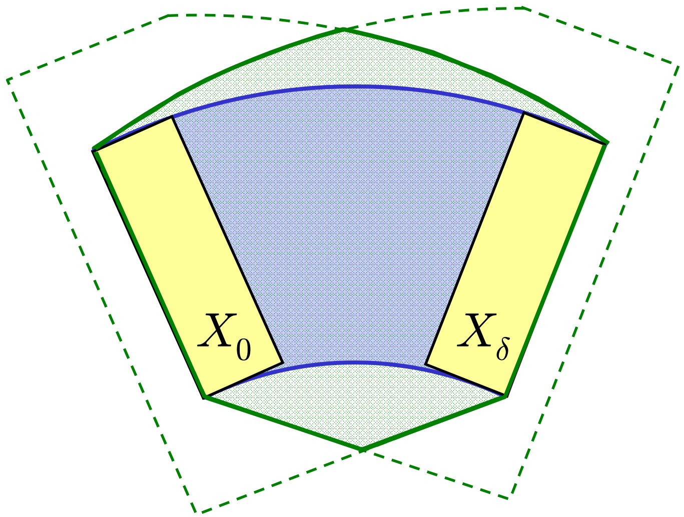
- **error large and uniform**
- **exponential cost**

- **error large and uniform**
- **efficient for high dimensions**

New Approximation Model

- **approximate set for each t + bloat with $\sim e^{\mathrm{abs}(A)\delta} A X_0$**
- **intersect forward and backward approximations**





- **error small and non-uniform thanks to math tricks**
- **without inputs: exact at t=0 and t=δ**

New Approximation Model

- **for each t: overapproximate** Reach$_{[t,t]}$ **with Ω_t**

$$\Omega_t = \underbrace{(1-\tfrac{t}{\delta})\mathcal{X}_0 \oplus \tfrac{t}{\delta}e^{\delta A}\mathcal{X}_0}_{\text{linear interpolation between } X_0 \text{ and } X_\delta = e^{A\delta} X_0}$$

$$\oplus \underbrace{\left(\tfrac{t}{\delta}\mathcal{E}_\Omega^+ \cap (1-\tfrac{t}{\delta})\mathcal{E}_\Omega^-\right)}_{\text{error bound from Taylor approximation around } t=0 \text{ and around } t=\delta}$$

$$\underbrace{\oplus t\mathcal{U} \oplus \tfrac{t^2}{\delta^2}\mathcal{E}_\Psi}_{\text{Taylor approximation of inputs with error bound}}$$

New Approximation Model

- **overapproximate** Reach$_{[0,\,\delta]}$ **with convex hull of time instant approximations**

$$\Omega_{[0,\delta]} = \mathrm{chull}\left(\bigcup_{0\le t\le\delta} \Omega_t\right)$$

- **error terms: symmetric bounding boxes**

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

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

$$\mathcal{E}_\Psi(\mathcal{U},\delta) = \boxdot\left(\Phi_2(|A|,\delta)\,\boxdot\left(A\mathcal{U}\right)\right).$$

$$\Phi_2(A,\delta) = A^{-2}\left(e^{\delta A} - I - \delta A\right)$$

New Approximation Model

- **overapproximate** Reach$_{[0,\,\delta]}$ **with convex hull of time instant approximations**

$$\Omega_{[0,\delta]} = \mathrm{chull}\left(\bigcup_{0\leq t\leq\delta} \Omega_t\right)$$

- **smaller overall error with math tricks**
  - Taylor approx. of interpolation error
  - bound remainder with absolute value sum instead of matrix norm

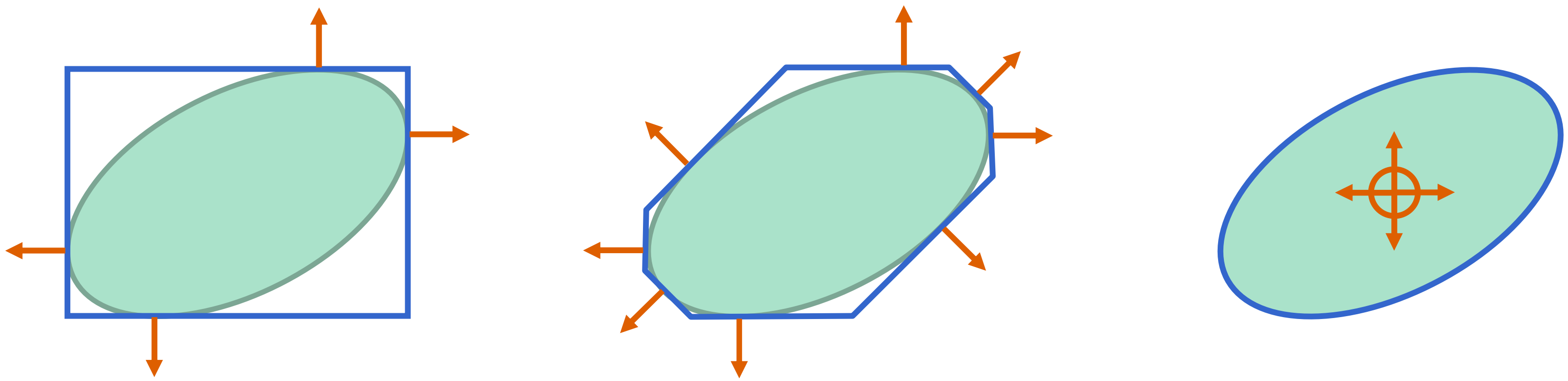
New Approximation Model

- **What Set Representation to Use?**

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

Representing of Convex Sets

- **Approximation with Supporting Halfspaces**
  - given template directions = **outer polyhedral approximation**



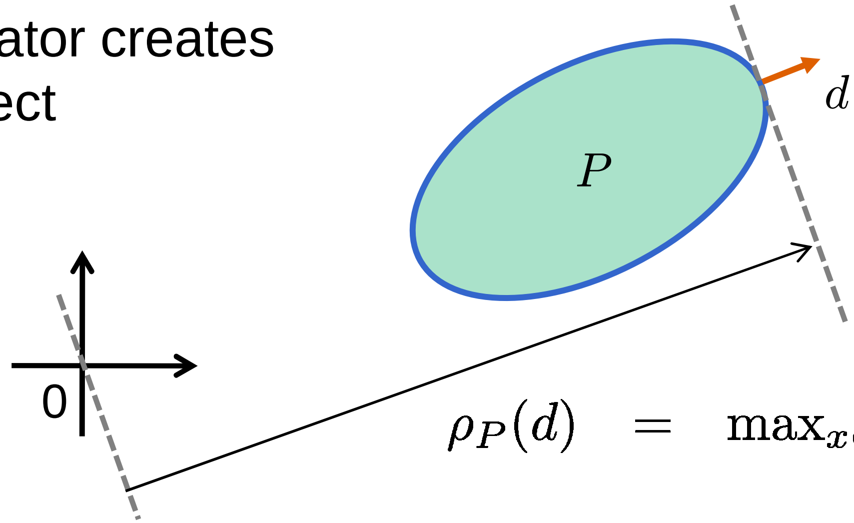
axis ($\pm x_i$)
$\Downarrow$
bounding box
2n facets

octagonal ($\pm x_i \pm x_j$)
$\Downarrow$
bounding polytope
$2n^2$ facets

all directions
$\Downarrow$
exact set

Representation of Convex Sets

- **Support Function**
  - direction $\rightarrow$ position of supporting halfspace
  - exact set representation
- **Implemented as function objects**
  - applying an operator creates new function object



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

Computing with Support Functions

- **Needed operations are simple**
  - Linear Transform: $\rho_{AP}(d) = \rho_P(A^T d)$
  - Minkowski sum: $\rho_{P \oplus Q}(d) = \rho_P(d) + \rho_Q(d)$
  - Convex hull: $\rho_{chull(P,Q)}(d) = \max(\rho_P(d), \rho_Q(d))$
- **Implement as function objects**
  - can add more directions at any time

C. Le Guernic, A.Girard. Reachability analysis of hybrid systems using support functions. CAV'09

New Approximation Model

- **Efficiently computable with support functions**

$$\Omega_{[0,\delta]} = \text{chull} \bigcup_{0\le t\le\delta} \Big((1-\tfrac{t}{\delta})\mathcal{X}_0 \oplus \tfrac{t}{\delta} e^{\delta A}\mathcal{X}_0$$

chull of union $\Rightarrow$ max

$$\oplus \left(\tfrac{t}{\delta}\mathcal{E}_\Omega^+ \cap (1-\tfrac{t}{\delta})\mathcal{E}_\Omega^-\right)$$

intersection of
axis aligned boxes
$\Rightarrow$ solution of pw linear function

$$\oplus t\mathcal{U} \oplus \tfrac{t^2}{\delta^2}\mathcal{E}_\Psi \Big)$$

New Approximation Model

- **Efficiently computable with support functions**

$$\rho_{\Omega_{[0,\delta]}}(d) = \max_{t\in[0,\delta]} \Big\{ (1-\tfrac{t}{\delta})\rho_{\mathcal{X}_0}(d) + \tfrac{t}{\delta}\rho_{\mathcal{X}_0}(e^{\delta A^T} d)$$

$$+ \textstyle\sum_{i=1}^{n} \min(\tfrac{t}{\delta} e_i^+, (1-\tfrac{t}{\delta}) e_i^-)|d_i|$$

solution for intersection of
axis aligned boxes

$$+ t\rho_{\mathcal{U}}(d) + \tfrac{t^2}{\delta^2}\rho_{\mathcal{E}_\Psi}(d) \Big\}$$

quadratic term

- maximize piecewise quadratic scalar function
  for each template direction

New Approximation Model

- **Error bounds for each template direction d**

$$\varepsilon_{\Psi_\delta(\mathcal{U})}(d) \le \rho_{\mathcal{E}_\Psi}(d) + \rho_{-A\Phi_2\mathcal{U}}(d)$$

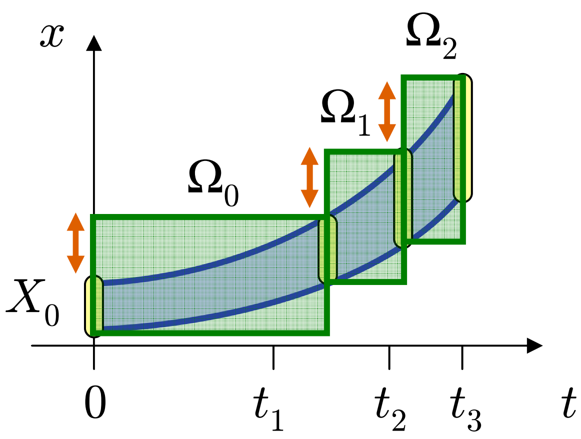
$$\varepsilon_{\Omega_{[0,\delta]}(\mathcal{X}_0,\mathcal{U})}(\ell) \le \max_{\lambda\in[0,1]} \Big\{\rho_{\left(\lambda\mathcal{E}_\Omega^+ \cap (1-\lambda)\mathcal{E}_\Omega^-\right)}(d) + \lambda^2 \rho_{\mathcal{E}_\Psi(\mathcal{U},\delta)}(d) + \lambda\rho_{-A\Phi_2\mathcal{U}}(d)\Big\}.$$

  - used to choose time steps

- **Error incurred with each application of time elapse operator**
  - transition successor computation will void this bound for subsequent steps

Extension to Variable Time Steps

- **adapt to error**



- **different time scale for each direction**
  - new approximation model can interpolate
- **cost: recompute matrix** $e^{A\delta}$
  - cache matrix

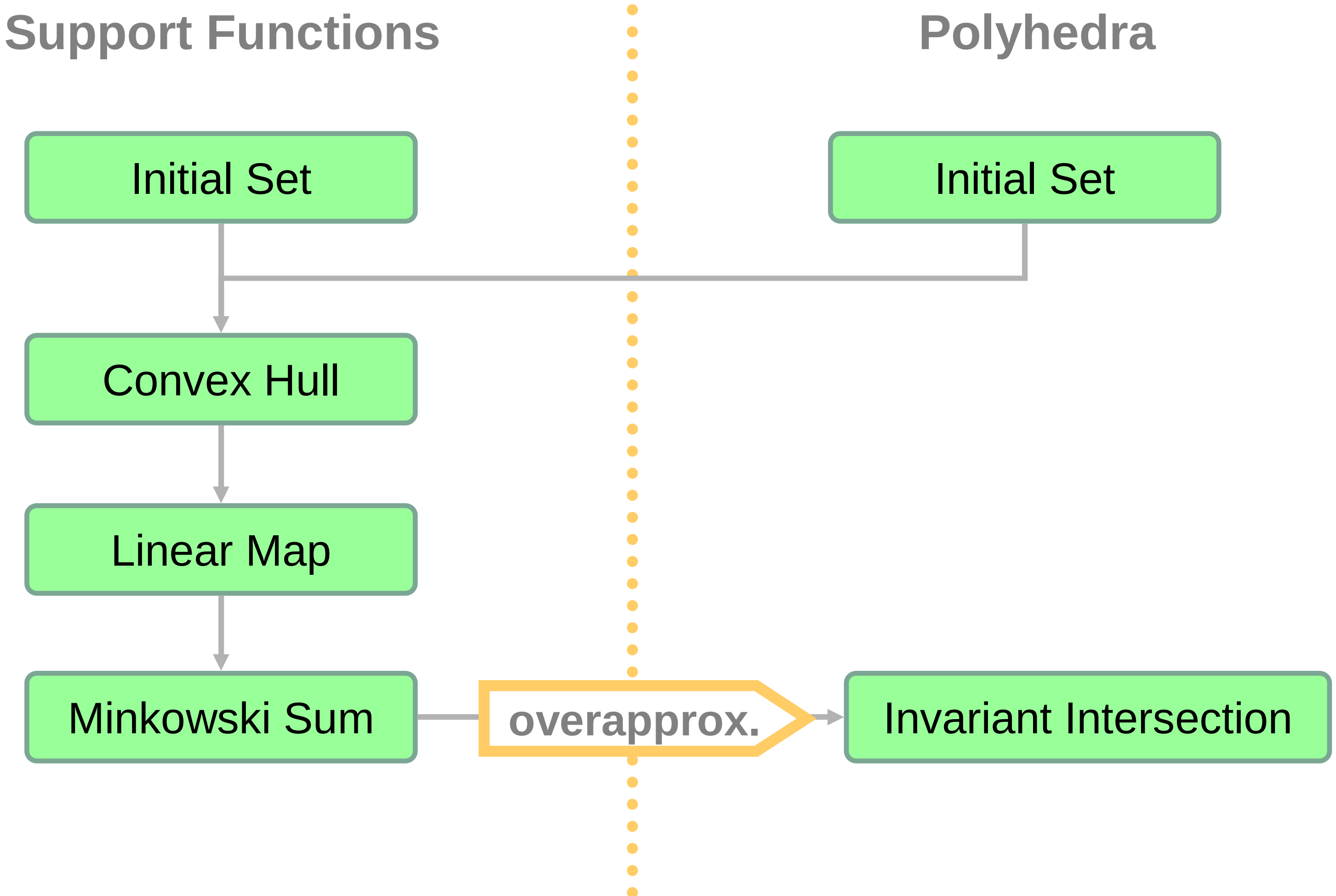
Intersection with Invariant

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

Switching Set Representations

- **Classic example:**
  Convex hull of polyhedra in constraint form
  - constraint form $\rightarrow$ vertex form: exponential cost
  - compute convex hull in vertex form (union of vertices)
  - vertex form $\rightarrow$ constraint form: exponential cost
- **Polyhedron $\rightarrow$ Support Function**
  - cheap & exact: solve a linear program
- **Support function $\rightarrow$ Polyhedron**
  - cheap, but overapproximative
  - to bound Hausdorff distance: exponential # of template directions

Computing Time Elapse

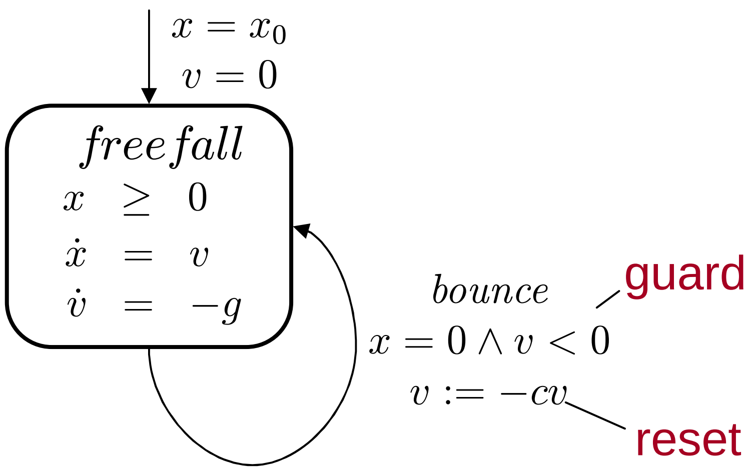


Outline

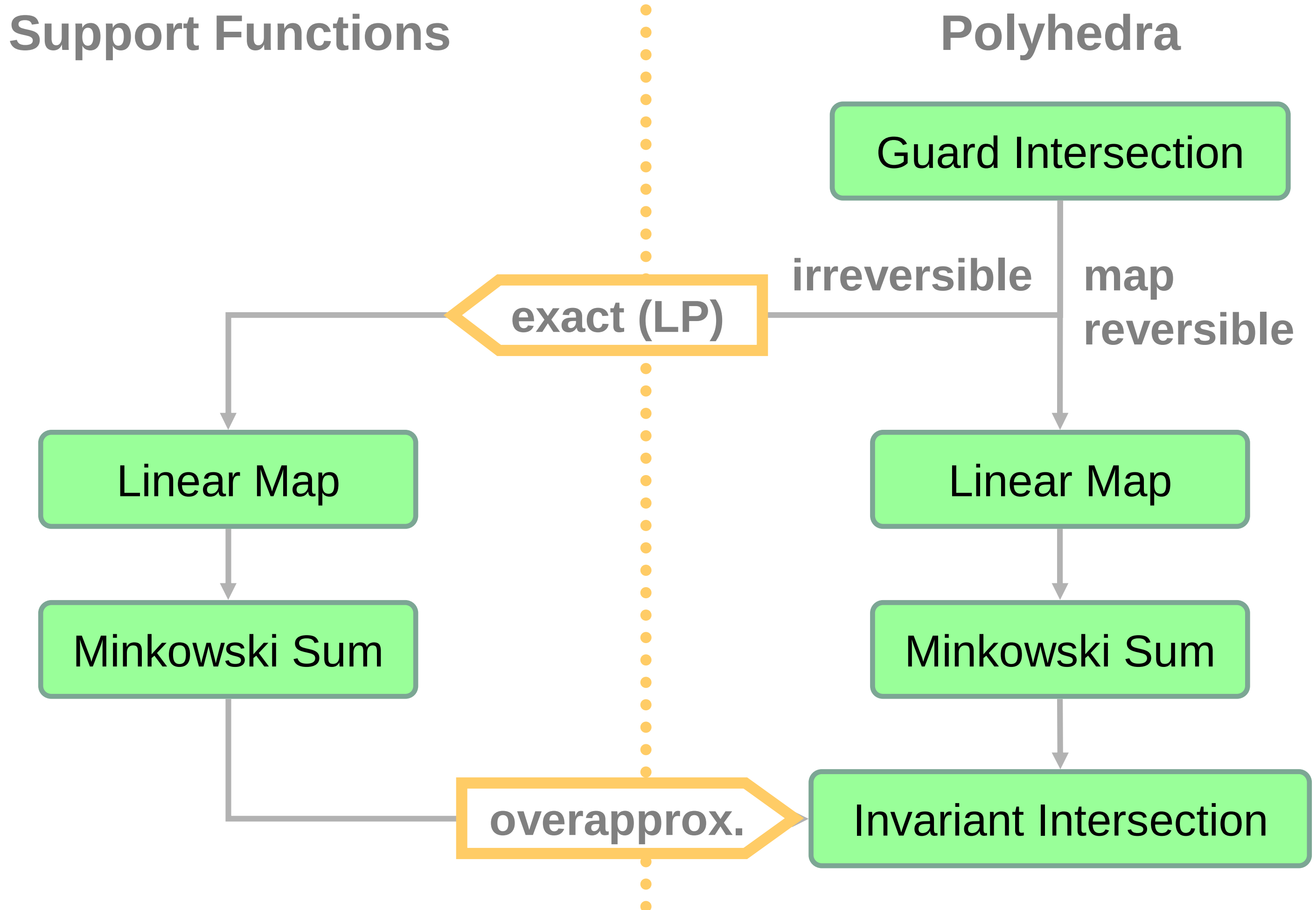
- **SpaceEx Verification Platform**
- **SpaceEx Approximation Algorithm**
  - Time Elapse Computation with Support Functions
  - Transition Successors Mixing Support Functions and Polyhedra
  - Fixpoint Algorithm: Clustering & Containment
- **Examples**

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



Outline

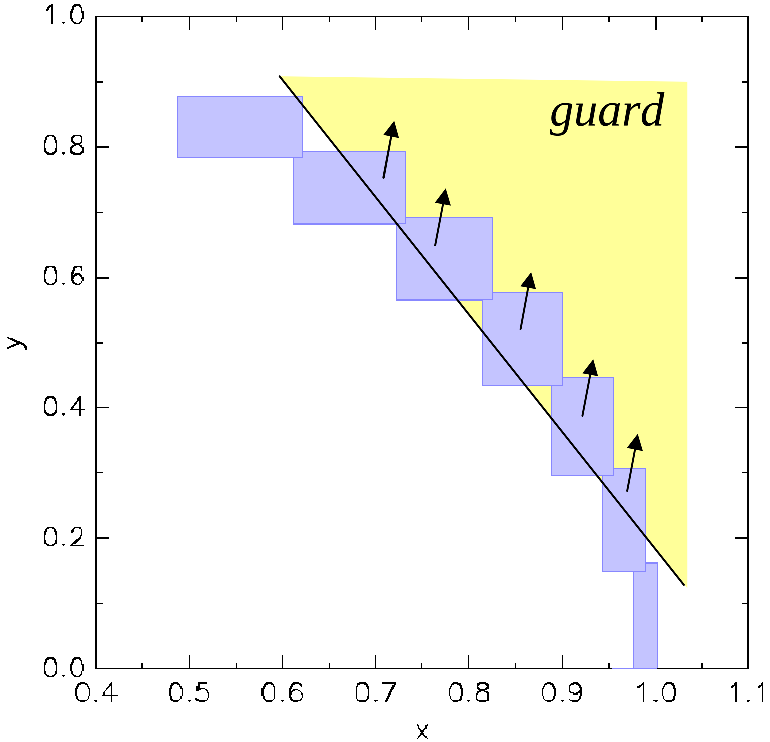
- SpaceEx Verification Platform
- SpaceEx Approximation Algorithm
  - Time Elapse Computation with Support Functions
  - Transition Successors Mixing Support Functions and Polyhedra
  - Fixpoint Algorithm: Clustering & Containment
- Examples

Fixpoint Computation

- **Standard fixpoint algorithm**
  - Alternate time elapse and transition successor computation
  - Stop if new states are **contained** in old states
- **Problem: flowpipe = union of many sets**
  - number of flowpipes may explode with exploration depth
  - containment very difficult on unions
- **Solution:**
  - reduce number after jump through **clustering**
  - use **sufficient conditions for containment**
  - nested depth of support function calls is limited due to outer poly.

Clustering

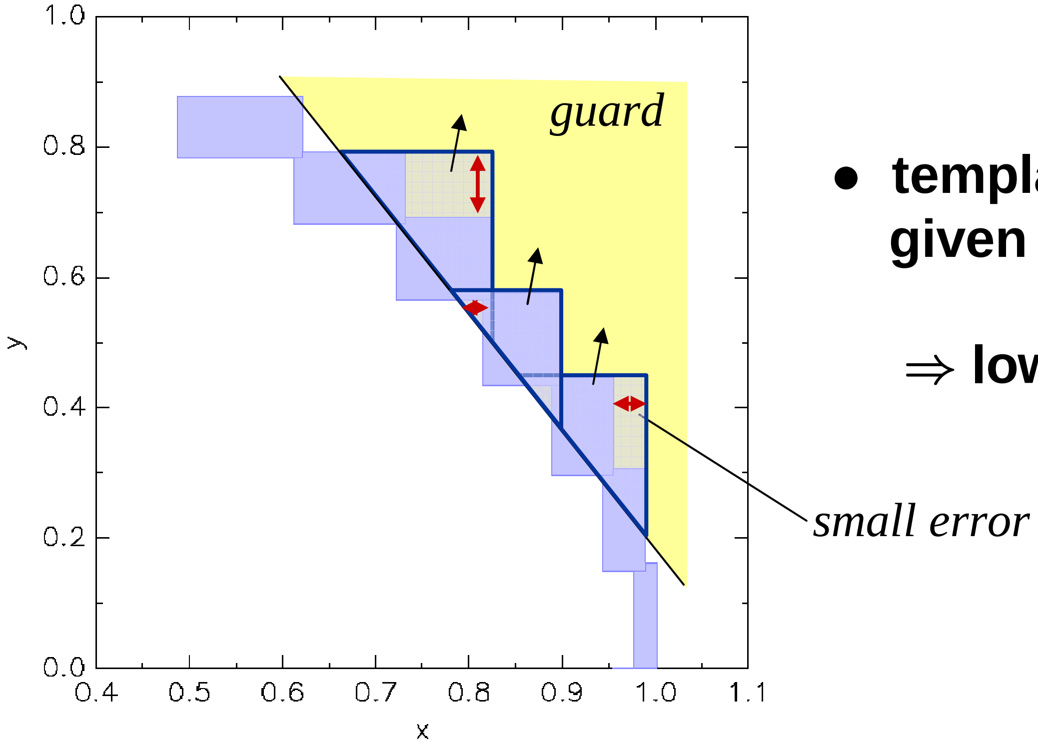
- **After discrete jump, every convex set spawns a new flowpipe**



- **Reduce number to avoid explosion**
- **How many sets?**
- **Bound approximation error**

Clustering – Template Hull

- **Template Hull**
  = Outer polyhedron for template directoins

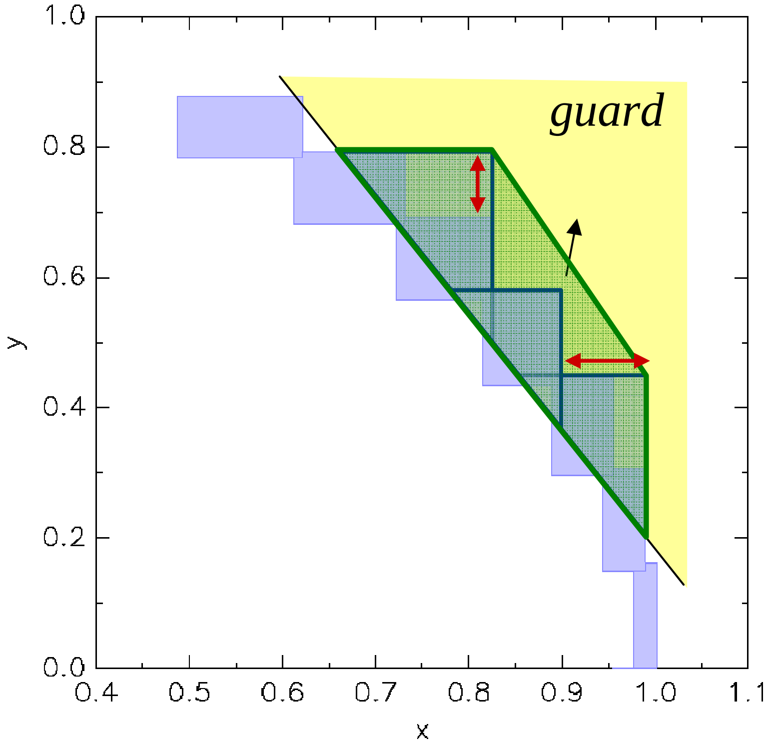


- **template hull up to given error bound**

  ⇒ low number of sets

Clustering

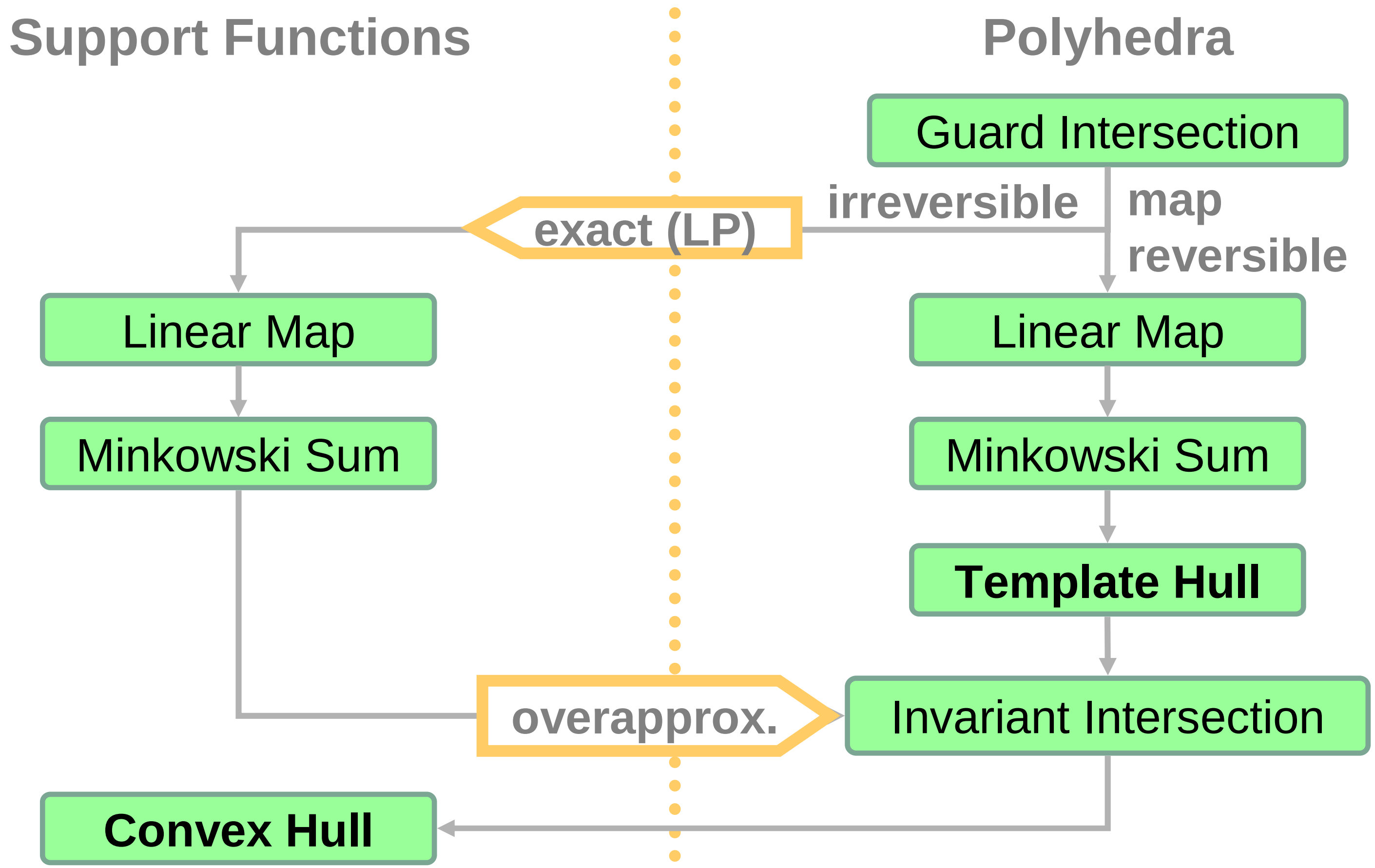
- **Even a low number of sets might be still too much**



- **2 sets $\Rightarrow$ possibly 2^k sets at iteration k**
- **cluster again using convex hull**

$\Rightarrow$ 1 set, good accuracy

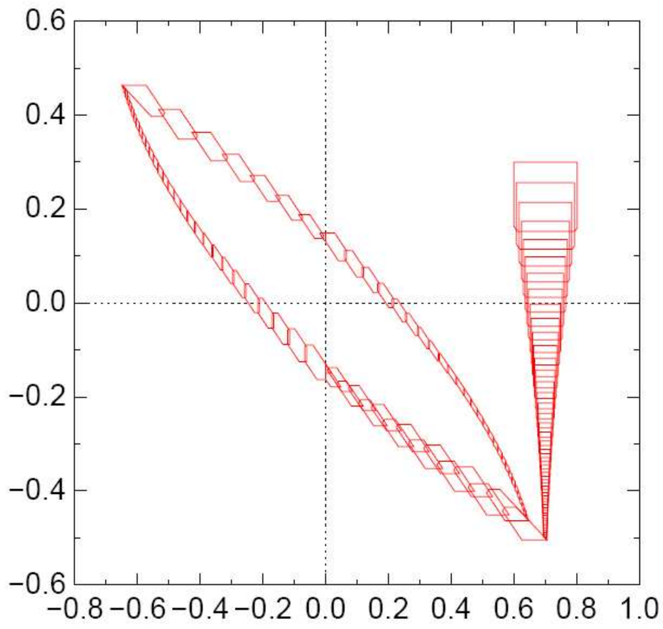
Transition Successors with Clustering



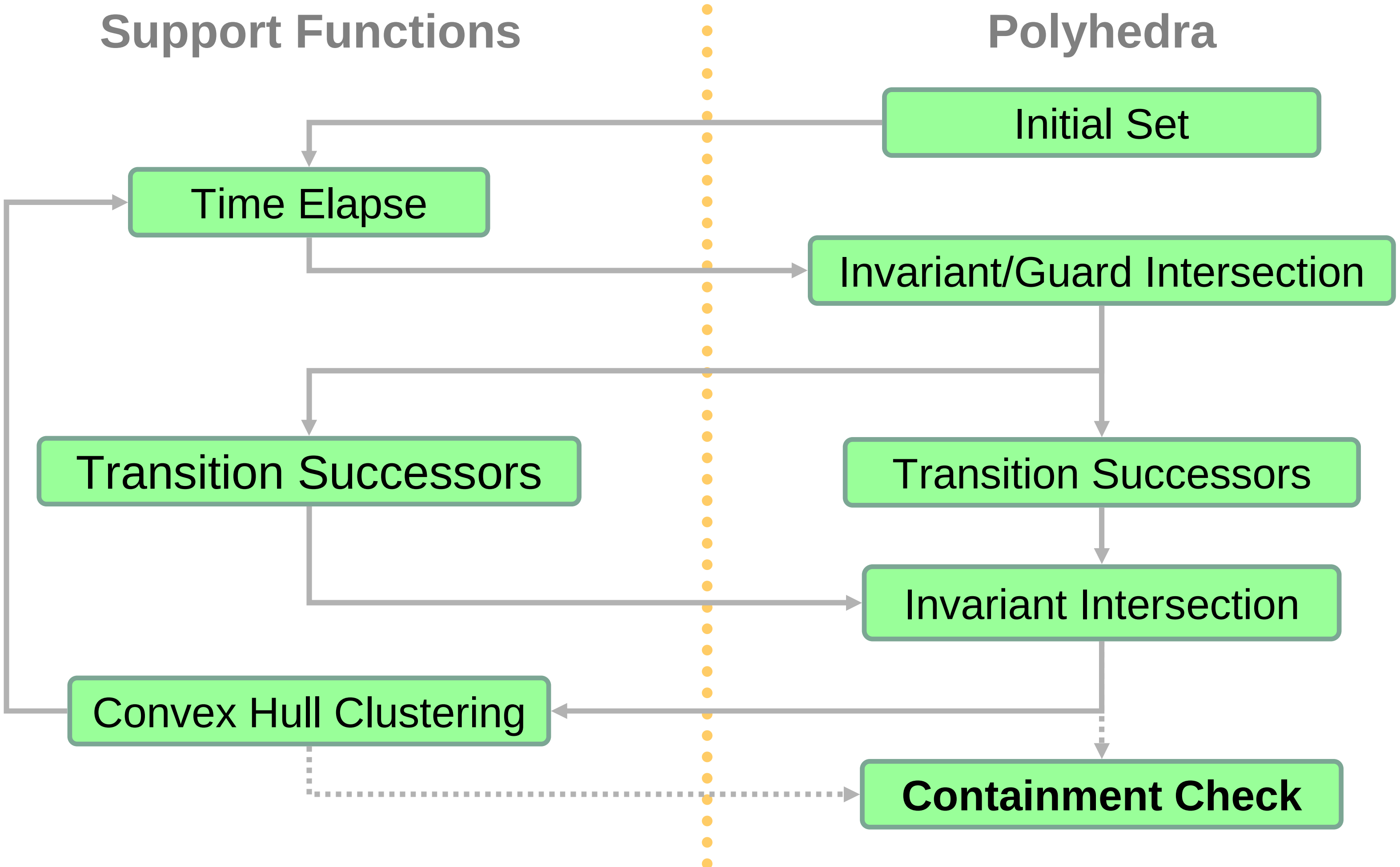
after intersection because
contained in convex invariant

Sufficient Conditions for Containment

- **“Cheap” containment**
  - pairwise comparison
  - comparison only with initial set of flowpipe
- **Clustering helps**
  - delays containment one iteration if clustering to a single set



Summary:
Reachability Fixpoint Algorithm

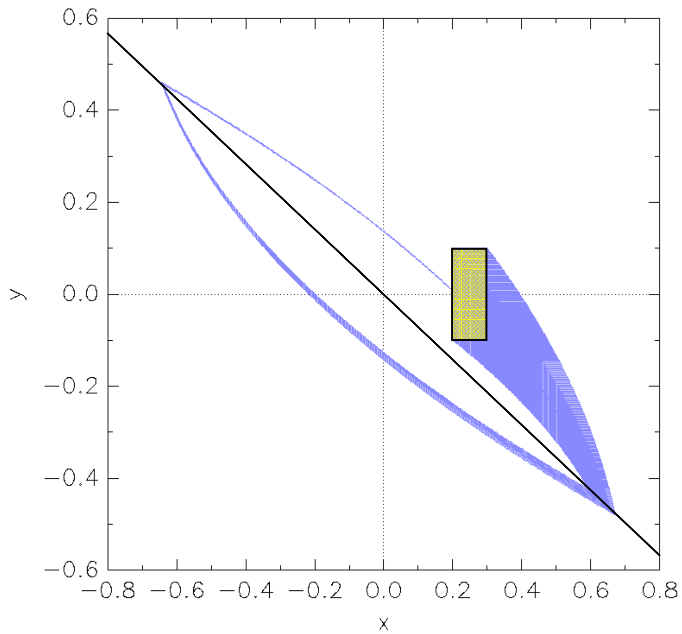


Outline

- **SpaceEx Verification Platform**
- **SpaceEx Approximation Algorithm**
  - Time Elapse Computation with Support Functions
  - Transition Successors Mixing Support Functions and Polyhedra
  - Fixpoint Algorithm: Clustering & Containment
- **Examples**

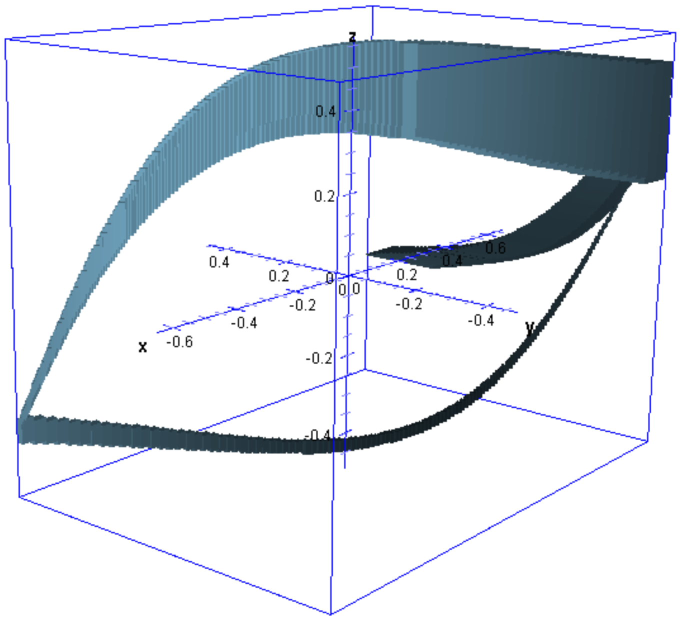
Example 1: Filtered Switched Oscillator

- **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

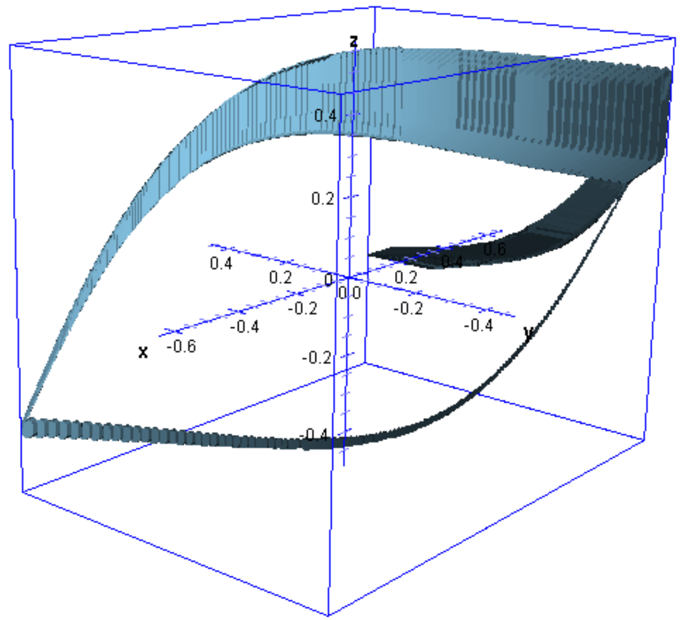


Filtered Switched Oscillator

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



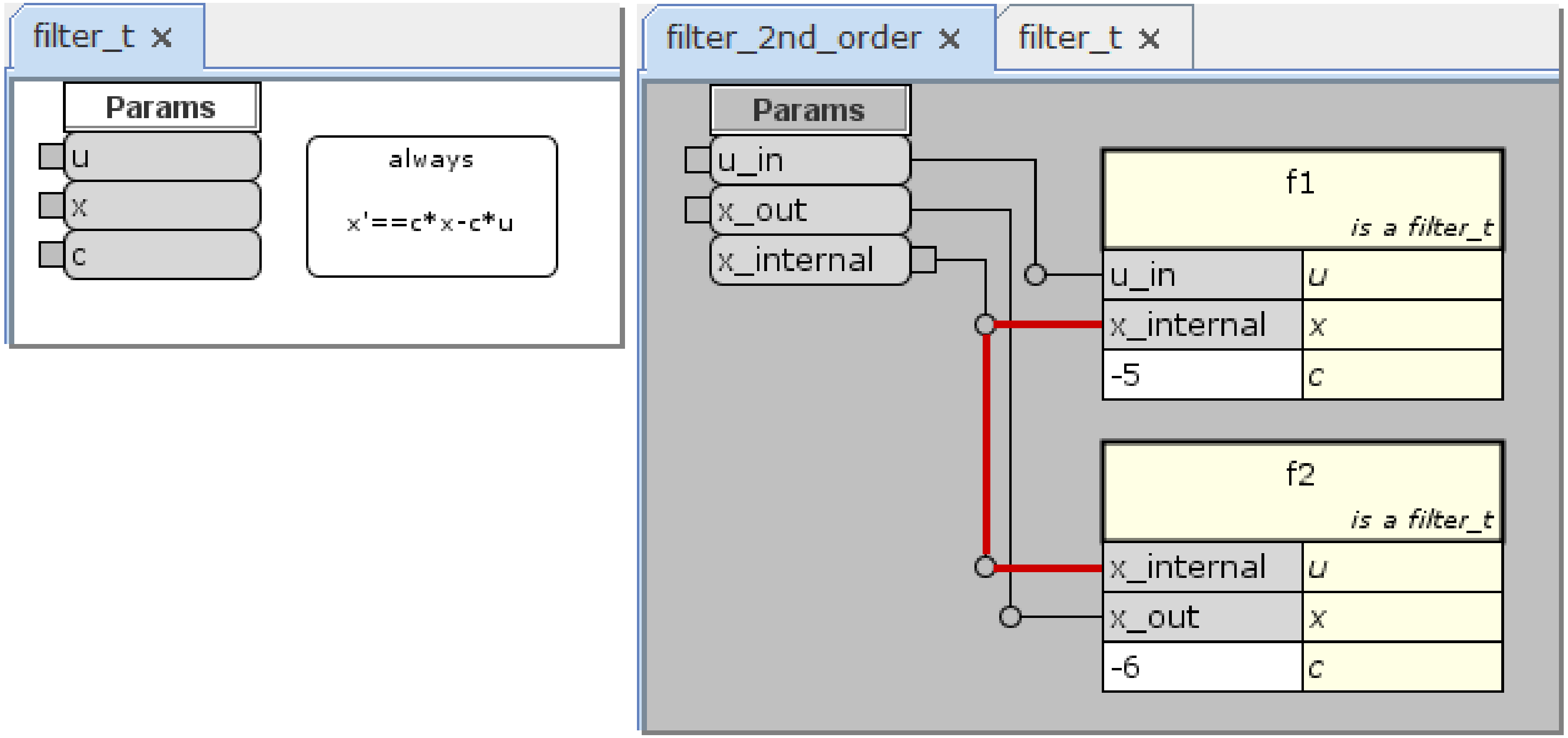
12 box constraints
(axis directions)



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

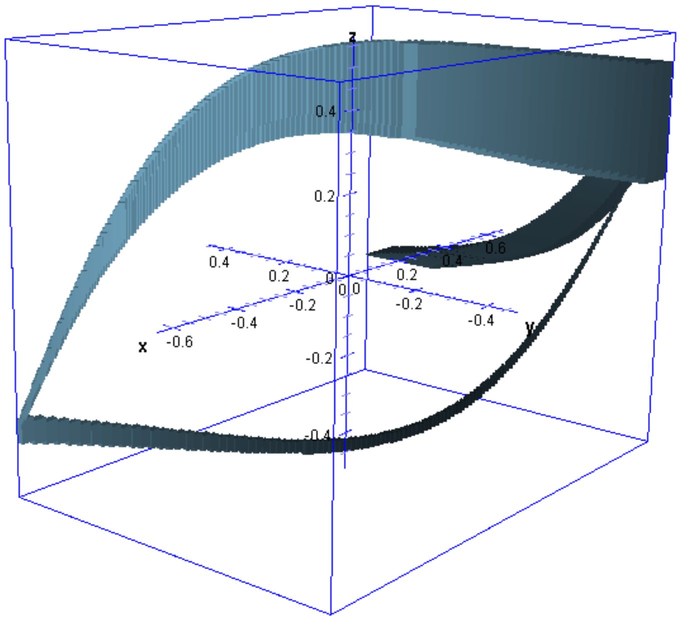
Example 1: Switched Oscillator

- **Connecting Filter Components**

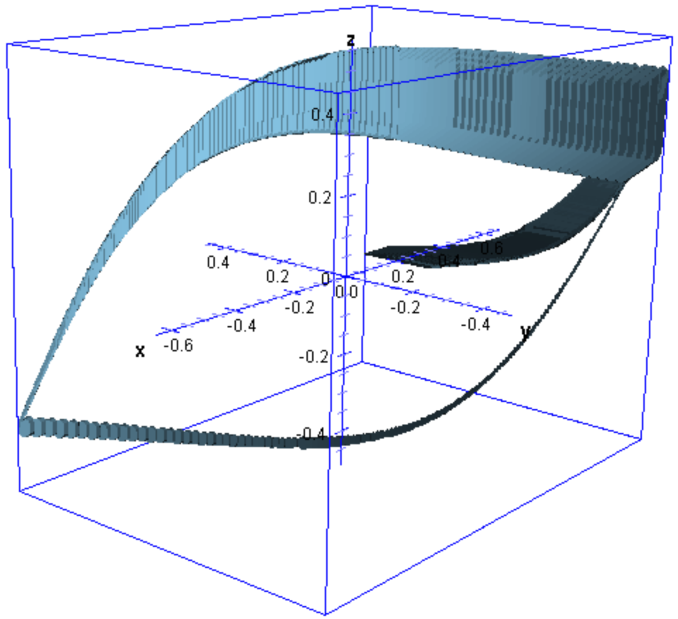


Example 1: Switched Oscillator

- **Low number of direction sufficent**
  - here: 6 state variables



12 box constraints
(axis directions)

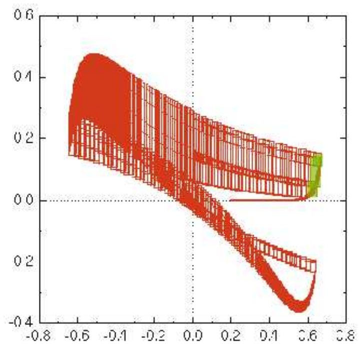


72 octagonal constraints
$(\pm x_i \pm x_j)$

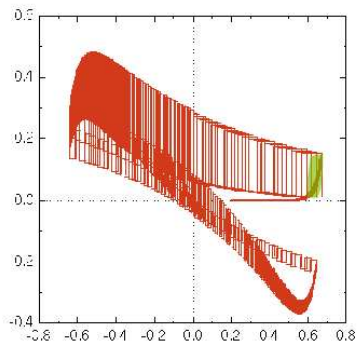
Template Hull and Convex Hull Clustering

- **first jump has 57 sets $\Rightarrow$ impossible w/o clustering**

11.5 sec



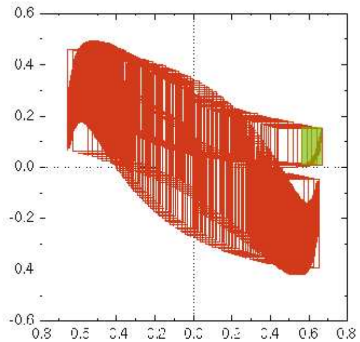
(a) 30% clustering (3 flowpipes)



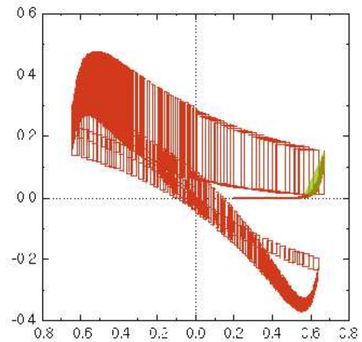
(b) 30% clustering, then convex hull aggregation

3.6 sec

3.4 sec



(c) Constraint hull aggregation

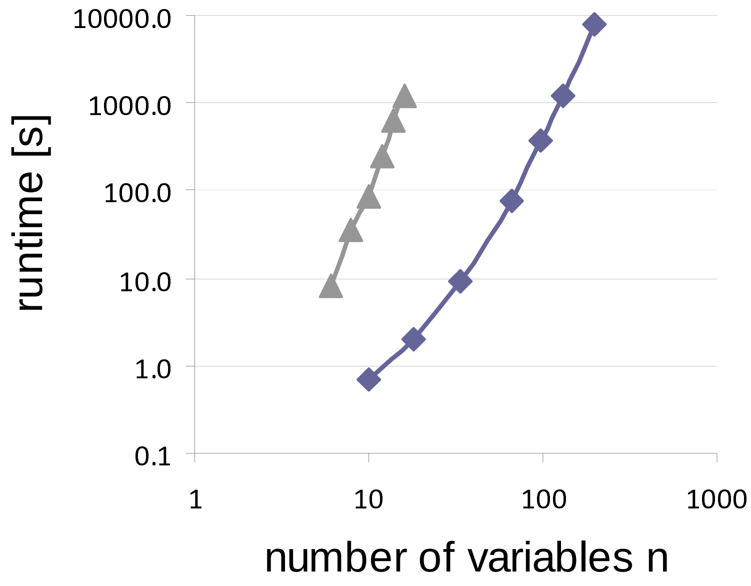


(d) Convex hull aggregation

8.2 sec

Example 1: Switched Oscillator

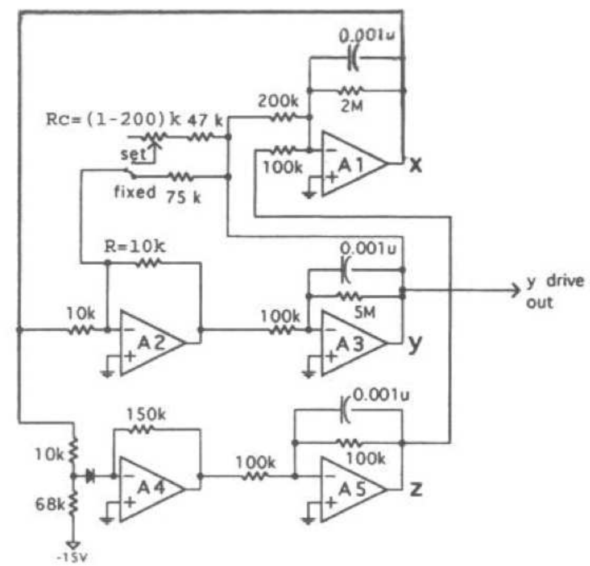
- **Scalable:**
  - fixpoint reached in $\mathrm{O}(nm^2)$ time
  - box constraints: $\mathrm{O}(n^3)$
  - octagonal constraints: $\mathrm{O}(n^5)$

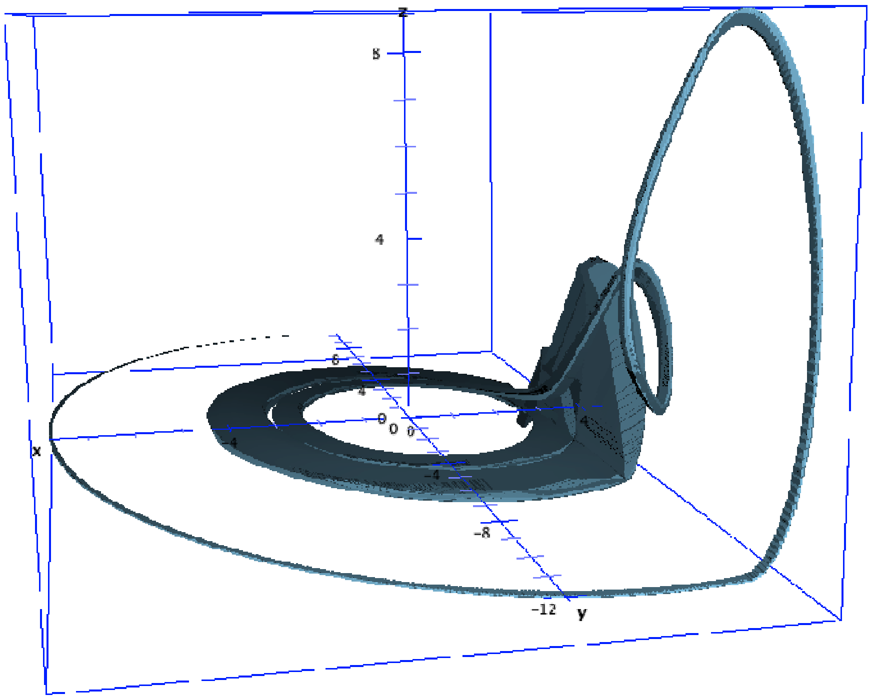


- **Clustering necessary**
  - 57 sets take first jump
  - combination of template and convex hull: compromise in speed and accuracy

Example 2: Chaotic Circuit

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





Example 2: Controlled Helicopter


Photo by Andrew P Clarke

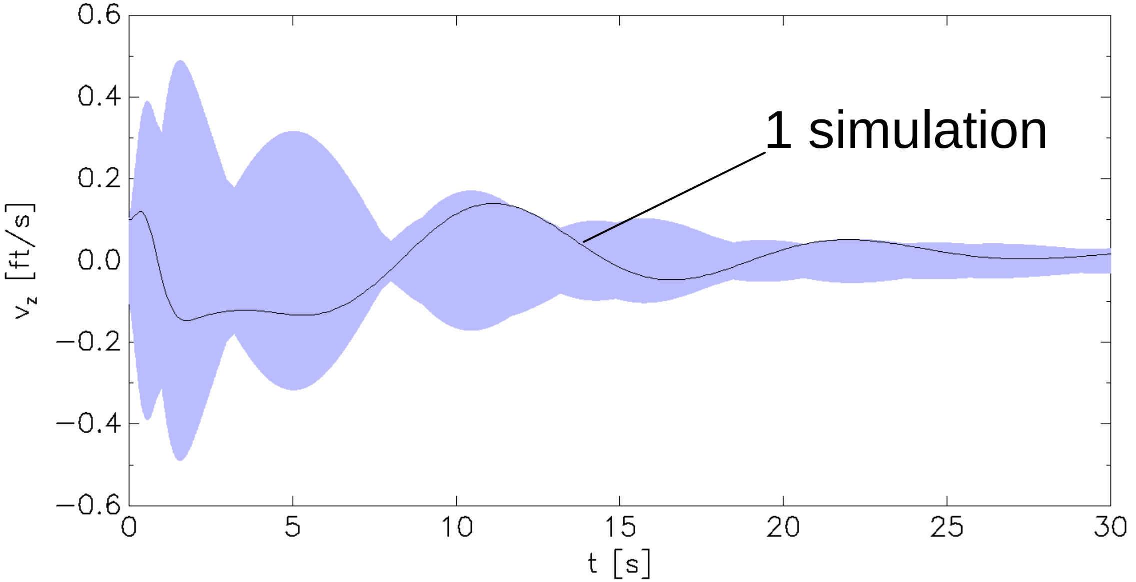
- **28-dim model of a Westland Lynx helicopter**
  - 8-dim model of flight dynamics
  - 20-dim continuous H_∞ controller for disturbance rejection
  - stiff, highly coupled dynamics

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

Example 2: Controlled Helicopter

- **Reachability for uncertain initial states:**
  - old approx.: 200s error large
  - new approx.: 24s error < 0.025
  - variable time step: 14s error < 0.025
    (without interpolation)

vertical speed

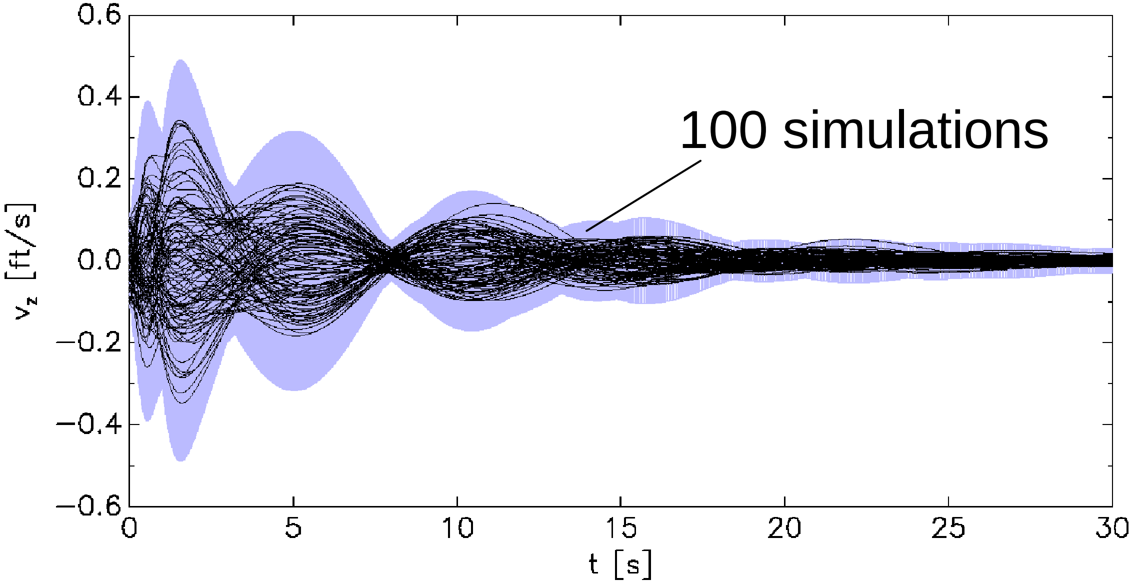


S. Skogestad and I. Postlethwaite, Multivariable Feedback Control: Analysis and Design. John Wiley & Sons, 2005.

Example 2: Controlled Helicopter

- **Reachability for uncertain initial states:**
  - old approx.: 200s error large
  - new approx.: 24s error < 0.025
  - variable time step: 14s error < 0.025
    (without interpolation)

vertical speed

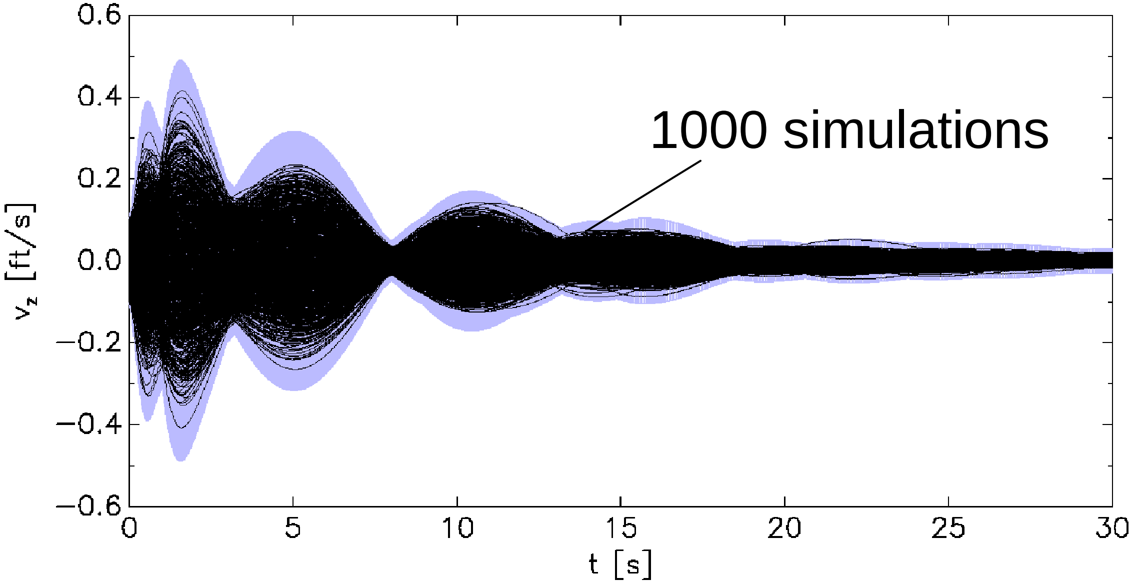


S. Skogestad and I. Postlethwaite, Multivariable Feedback Control: Analysis and Design. John Wiley & Sons, 2005.

Example 2: Controlled Helicopter

- **Reachability for uncertain initial states:**
  - old approx.: 200s error large
  - new approx.: 24s error < 0.025
  - variable time step: 14s error < 0.025
    (without interpolation)

vertical speed

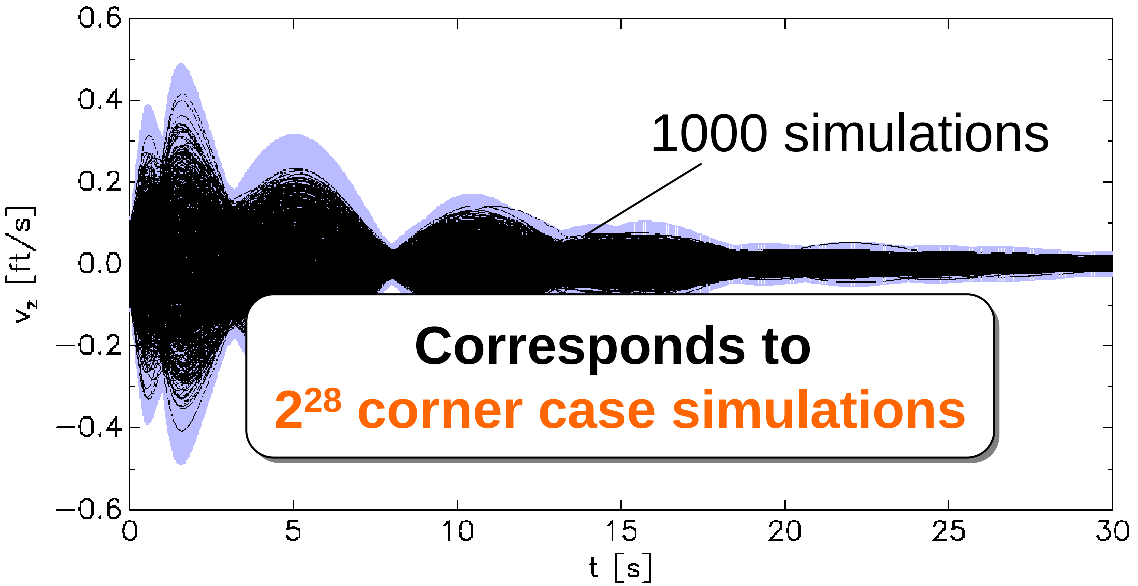


S. Skogestad and I. Postlethwaite, Multivariable Feedback Control: Analysis and Design. John Wiley & Sons, 2005.

Example 2: Controlled Helicopter

- **Reachability for uncertain initial states:**
  - old approx.: 200s error large
  - new approx.: 24s error < 0.025
  - variable time step: 14s error < 0.025
    (without interpolation)

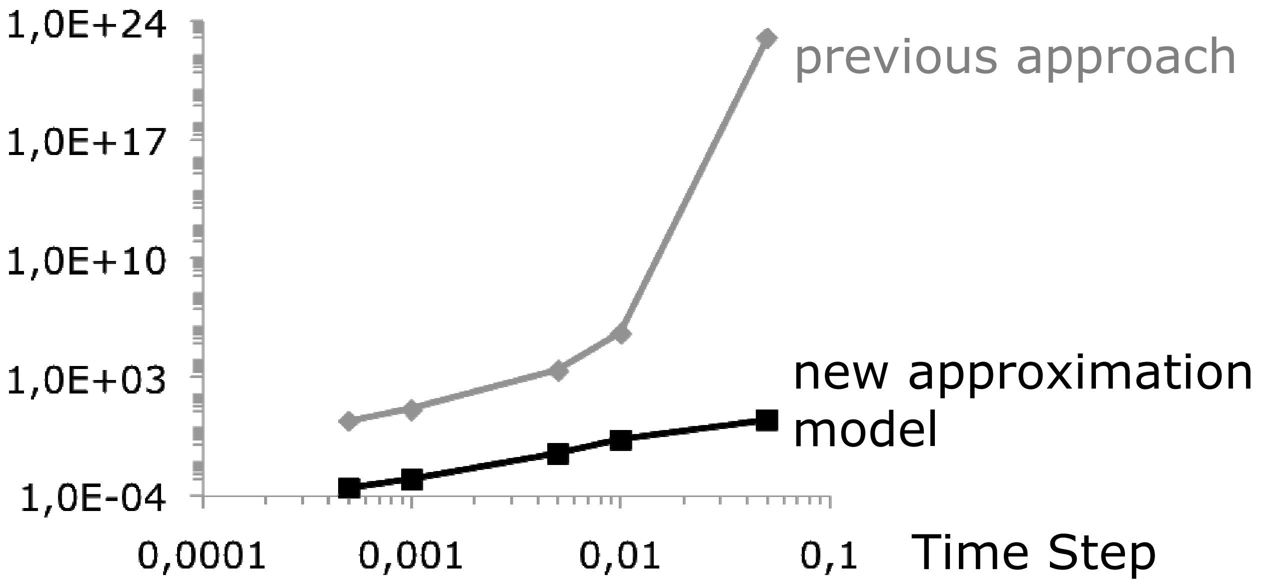
vertical speed



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

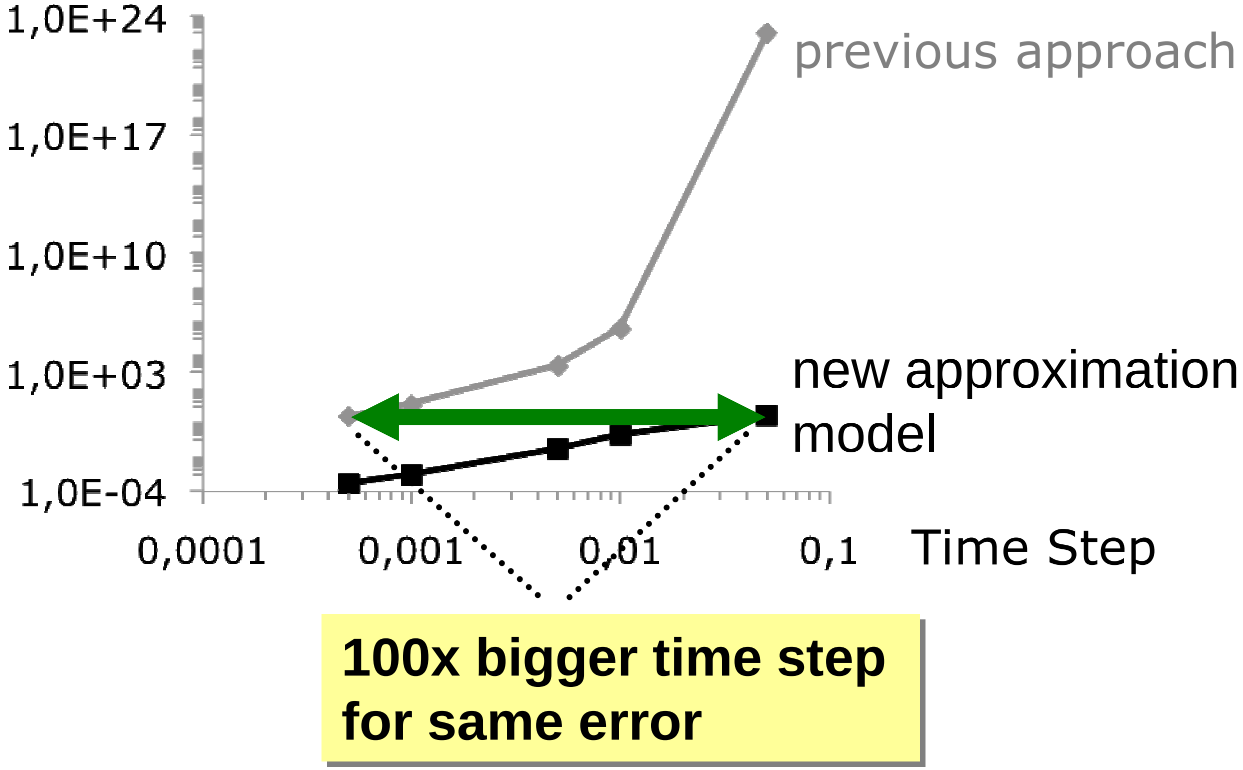
Example 2: Controlled Helicopter

- **Max error per template direction per time elapse:**



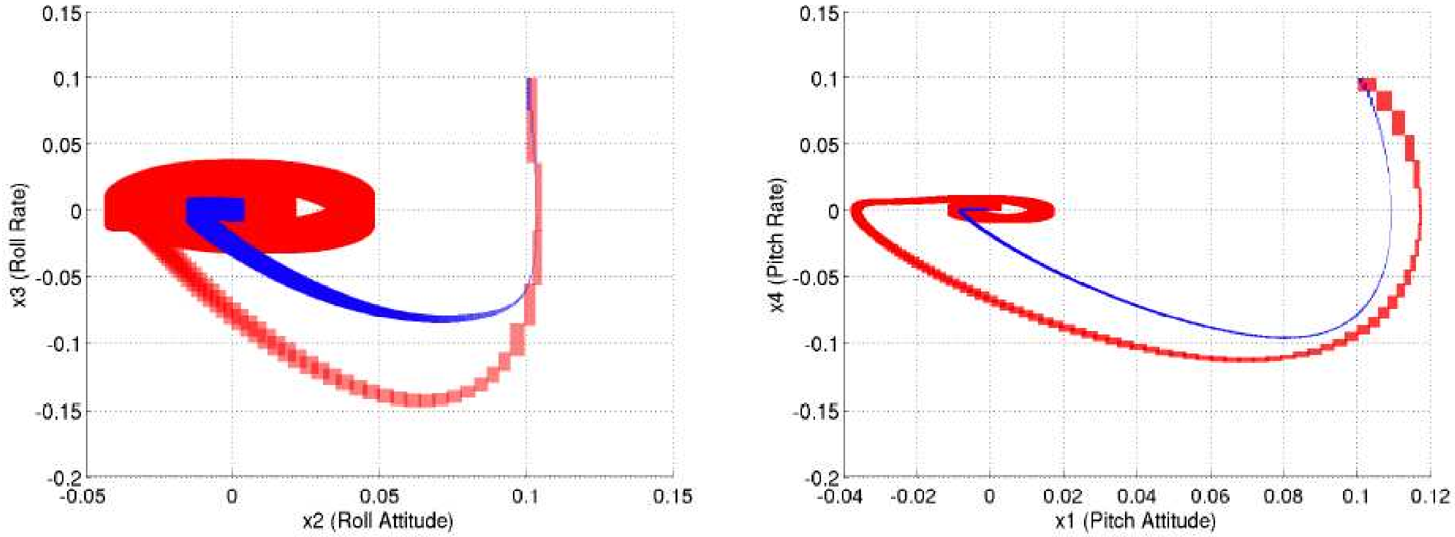
Example 2: Controlled Helicopter

- **Max error per template direction:**



Example 2: Controlled Helicopter

- **Comparing two controllers under nondeterministic disturbances**

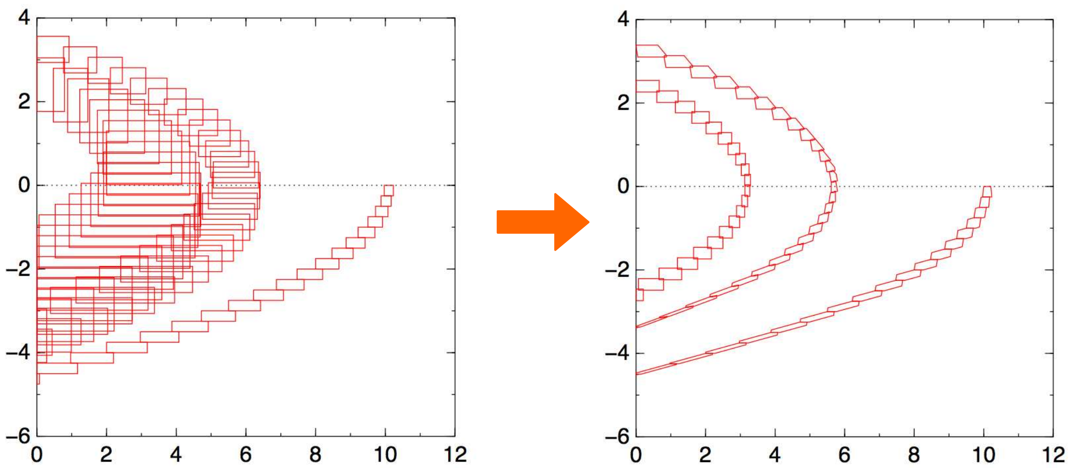


(a) Roll stabilization   (b) Pitch stabilization

Conclusions

- **SpaceEx Verification Platform**
  - available at **spaceex.imag.fr**
  - tutorial with solutions for course work
- **Scalable reachability for piecewise affine dynamics**
  - fixpoint computation with 200+ variables
- **Algorithmic improvements**
  - approximation improved significantly
  - switching set representations for best efficiency
  - variable time step with error bounds

Ongoing Work



- **Precise Intersection**
  - reduce error by finding template directions
- **Nonlinear Systems**
  - linearize with sliding window

Tool Download:
spaceex.imag.fr

Bibliography

- **Affine Dynamics**
  - E. Asarin, O. Bournez, T. Dang, and O. Maler. Approximate Reachability Analysis of Piecewise-Linear Dynamical Systems. HSCC'00
  - A. Girard, C. Le Guernic, and O. Maler. Efficient computation of reachable sets of linear time-invariant systems with inputs. HSCC'06
- **Support Function Reachability**
  - C. Le Guernic, A.Girard. Reachability analysis of hybrid systems using support functions. CAV'09
  - G. Frehse et al. SpaceEx: Scalable Verification of Hybrid Systems. CAV'11