d/dt: A Tool for Reachability Analysis of Continuous and Hybrid Systems

E. Asarin, T. Dang, and O. Maler
VERIMAG

Outline

1. Introduction
2. Reachability problem and our approach
3. Reachability technique for non-linear continuous systems
4. Reachability technique for linear continuous systems
5. Analysis of hybrid systems: verification and controller synthesis
6. The tool d/dt

Reachability Problem for Continuous Systems

The basic problem

$\dot{\mathbf{x}} = f(\mathbf{x})$; $\mathbf{x} \in \mathcal{X}$, bounded subset of R^n

$\mathbf{x}(0) \in F$, set of initial states

- Characterizing *the set of states reachable* from the *set F*
- Representation of reachable sets that can *be tested for intersection with other sets*

• Exact symbolic computation: applicable for restricted classes $\Rightarrow$ **Numerical approximation** of the reachable set

Reachability operators

For a given set $F \subseteq \mathcal{X}$ and a time interval $I = [t_1, t_2]$

$\delta_I(F)$: set of states reachable from F in time $t \in I$

$\delta_t(F)$: set of states reachable after exact amount of time t

$\delta(F) = \delta_{[0,\propto)}(F)$: reachable set

Semi-group property: $\delta_{[0,\, t_1+t_2]}(F) = \delta_{[0,\, t_2]}(\delta_{[0,\, t_1]}(F))$

Abstract Algorithm for Computing $\delta(F)$

$P^0 := F; \quad k := 0;$

repeat

  $k := k + 1;$

  $P^k := P^{k-1} \cup \delta_{[0,t]}(P^{k-1});$

until $(P^k = P^{k-1})$

Problems

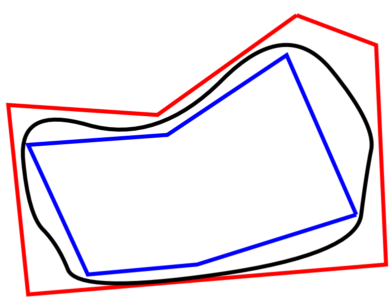
- Compute $\delta_{[0,t]}$ of a set
- Perform set *union*, *equivalence testing*

Approximation by Orthogonal Polyhedra

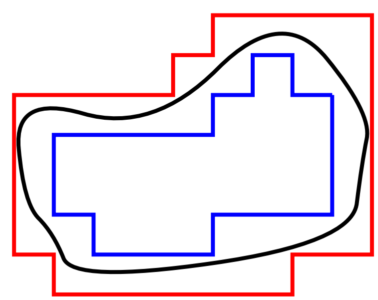
- Reachable sets are often *non-convex* $\Rightarrow$ difficulty in representing and manipulating arbitrary non-convex polyhedra

$\Rightarrow$ *Orthogonal Polyhedra*

- Canonical representation, relatively efficient manipulation
- Easy termination checking
- *Over*-approximation (*verification*), *under*-approximation (*synthesis*)



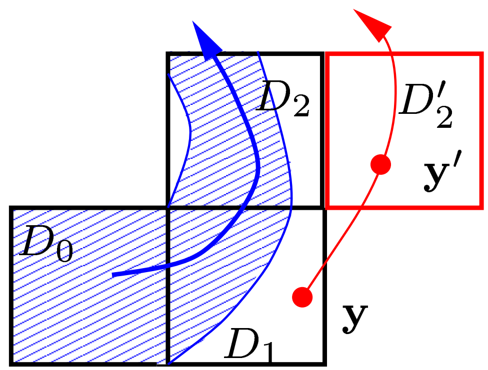
Arbitrary polyhedra



Orthogonal polyhedra

Approximation by Orthogonal Polyhedra (cont'd)

Accumulation of **over-approximation** *errors*

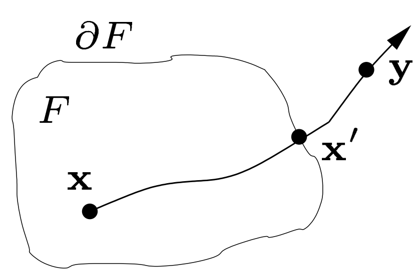


Reachability Technique for Non-Linear Continuous Systems

A non-linear continuous system: $\dot{\mathbf{x}} = f(\mathbf{x})$; F is the set of initial states

Face-lifting technique, inspired by [Greenstreet 96]

– Continuity of trajectories $\Rightarrow$ *computing from the boundary*



The set F is *polyhedral* $\Rightarrow$ boundary of F is the union of its *faces*

– Consider the evolution in the *outward normal direction of each face* of F

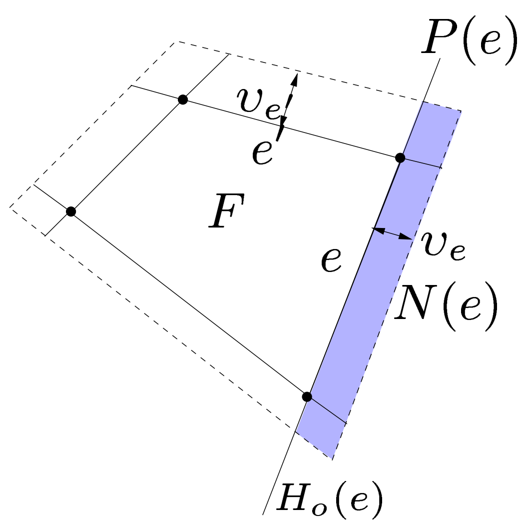
Face Lifting Technique

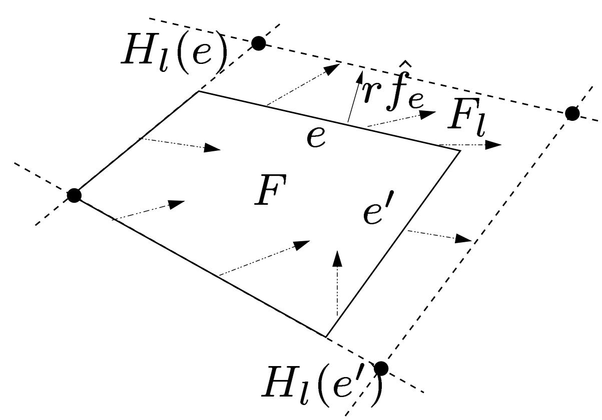
Step 1 - Rough approximation: neighborhood $N(F)$ such that all trajectories starting from F stay in $N(F)$ for at least r time.

Step 2 - More precise approximation

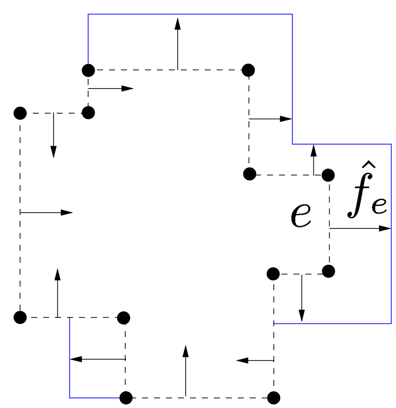
$f_e(\mathbf{x})$: projection of $f(\mathbf{x})$ on the outward normal vector $\mathbf{n}(e)$ of face e

$\hat{f}_e$: maximum of f_e over $N(e)$





Face Lifting using Orthogonal Polyhedra



Using orthogonal polyhedra:

- Faces can be systematically enumerated
- Orthogonal polyhedra are closed under the lifting operation

Reachability of Linear Continuous Systems

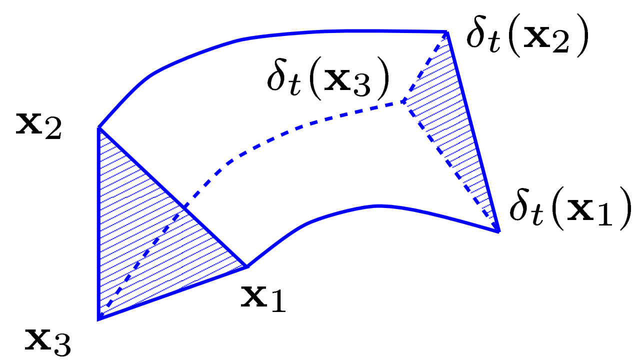
A linear continuous system: $\dot{\mathbf{x}} = A\mathbf{x}$, F is the set of initial states

$\delta_t(F) = e^{At}F$

Property: *Convexity is preserved*

$F = conv\{\mathbf{x}_1, \ \ldots \ , \mathbf{x}_m\}$; $\mathbf{x}_i$ are vertices of F

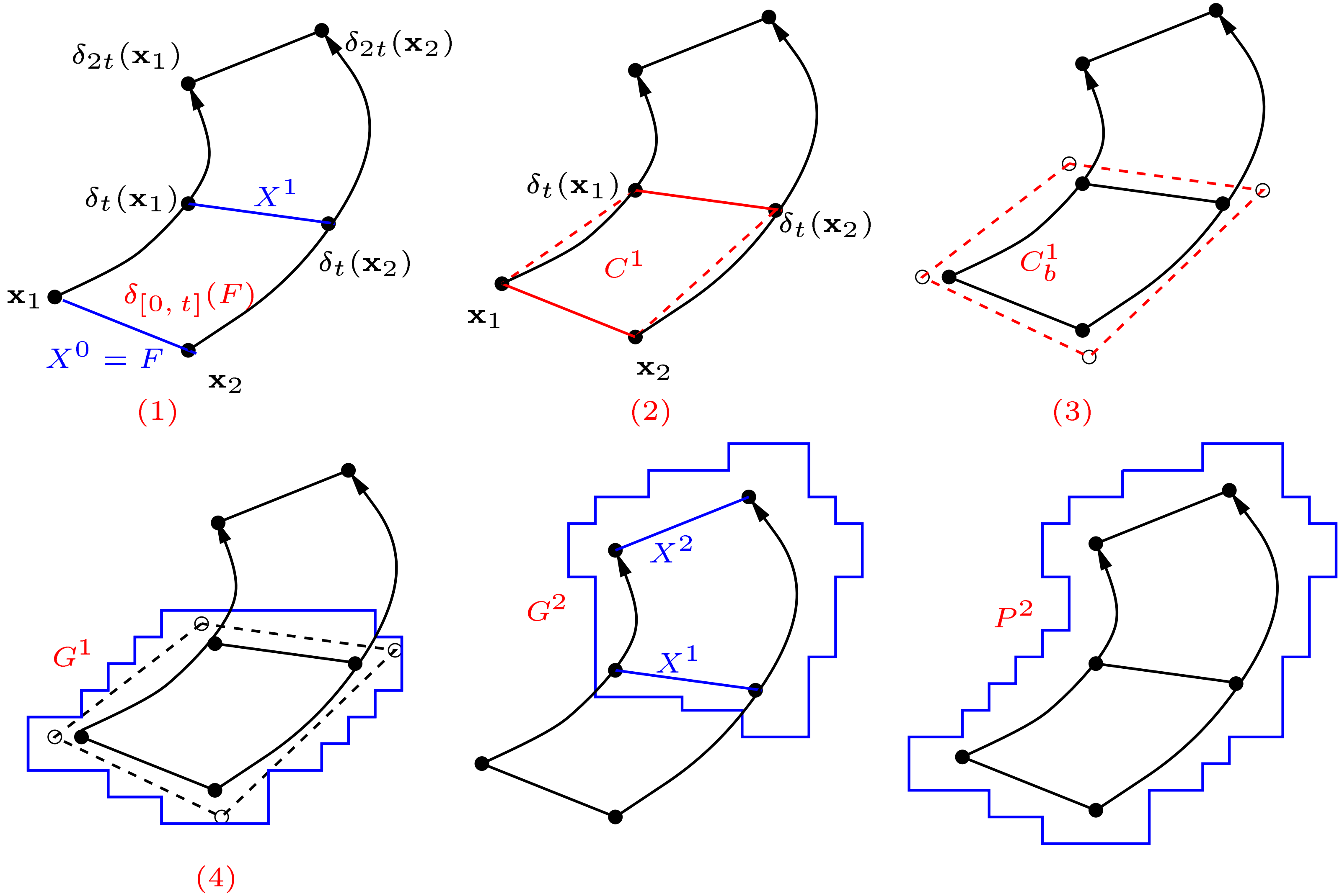
$\delta_t(F) = conv\{\delta_t(\mathbf{x}_1), \ \ldots \ , \delta_t(\mathbf{x}_m)\}$ with $\delta_t(\mathbf{x}_i) = e^{At}\mathbf{x}_i$



$\delta_t(F)$ can be computed by a finite number of integrations.

$\Rightarrow$ We exploit this property to approximate $\delta(F)$

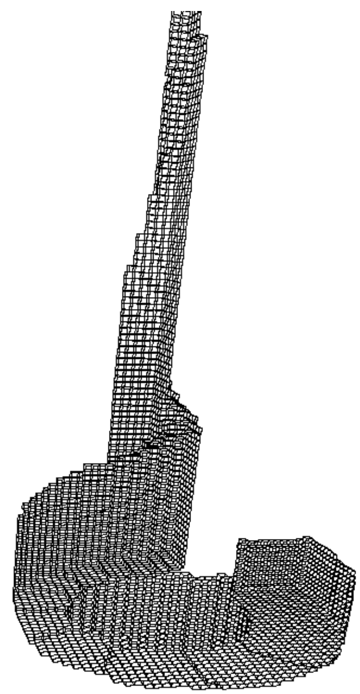
Approximate Computation of $\delta(F)$



Example

$\dot{\mathbf{x}} = A\mathbf{x}$, initial set $F = [0.025, 0.05] \times [0.1, 0.15] \times [0.05, 0.1]$

$$A = \begin{pmatrix} -1.0 & -4.0 & 0.0 \\ 4.0 & -1.0 & 0.0 \\ 0.0 & 0.0 & 0.5 \end{pmatrix}$$



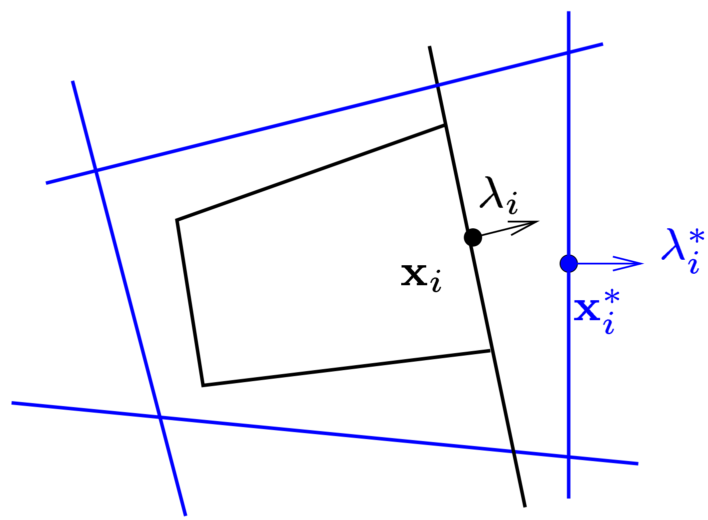
Linear Systems with Uncertain Input

$\dot{\mathbf{x}} = A\mathbf{x} + \mathbf{u}$, where $\mathbf{u} \in U$ (convex set)

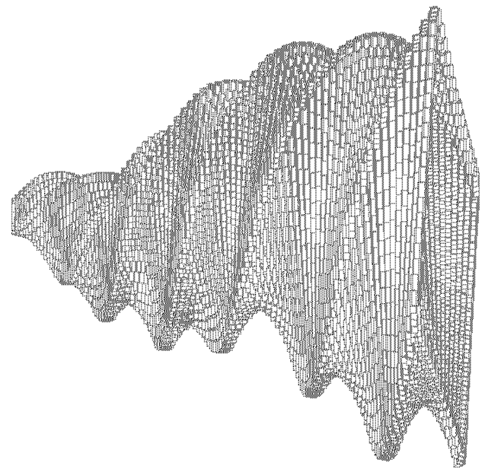
Approach: inspired by [Varaiya 98] using the Maximum Principle

Convex polyhedron $F = \bigcap\{\langle \lambda_i, \mathbf{x}\rangle \leq \gamma_i\}$ (*intersection of halfspaces*)

Face i: $\langle \lambda_i, \mathbf{x}\rangle = \gamma_i$ $\quad \mathbf{u}_i{}^* = argmax\{\ \langle \lambda_i, A\mathbf{x} + \mathbf{u}\rangle \mid \mathbf{u} \in U\ \}$



Example of Linear Continuous Systems with Input



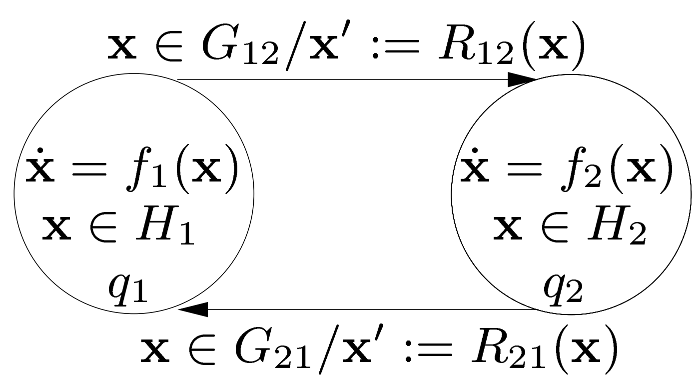
$$\dot{\mathbf{x}} = A\mathbf{x} + \mathbf{u}, \quad \mathbf{u} \in U; \qquad A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -8 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -4 & 0 \end{pmatrix}$$

Input set $U = [-0.5, 0.5] \times [-0.005, 0.005] \times [-0.5, 0.5] \times [-0.005, 0.005]$;

Initial set $F = [0, 2] \times [-1, 1] \times [0, 2] \times [-1, 1]$; [Kurzhanski and Valyi 97]

Hybrid Dynamical Systems

- several *modes* (*discrete states*, *locations*)
- continuous dynamics of the modes are defined by *differential equations*
- *staying* conditions (*'invariants'*) of each mode: convex polyhedra
- *switching* conditions (*'guards'*): convex polyhedra
- *reset functions* associated with transitions: affine of the form $R_{qq'}(\mathbf{x}) = D_{qq'}\mathbf{x} + J_{qq'}$



Reachability Analysis of Hybrid Systems

The state $(q, \mathbf{x})$ of the system can change in two ways:

- by **continuous dynamics**: location q remains constant, and $\mathbf{x}$ changes continuously according to the differential equation of location q
- by **discrete transitions**: location q changes, and $\mathbf{x}$ can be changed according to the reset function

Reachability procedure requires the computation of

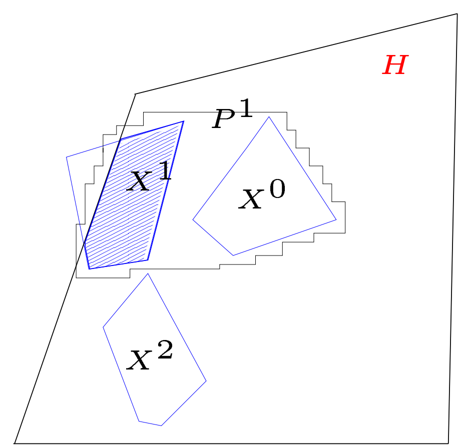
⋆ reachable sets by continuous dynamics (**continuous-successors**)

⋆ reachable sets by discrete transitions (**discrete-successors**)

Reachability Technique for Hybrid Systems

Computation of continuous-successors

- based on the computation of *reachable sets of continuous systems*
- takes into account the *staying condition* of the current location



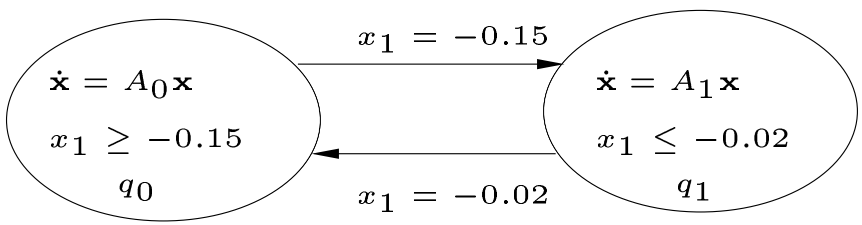
Computation of discrete-successors

- Set of discrete-successors of set F by transition from q to q':

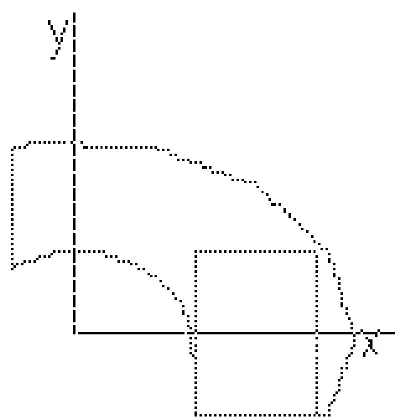
$$R_{qq'}(F \cap G_{qq'} \cap H_{q'})$$

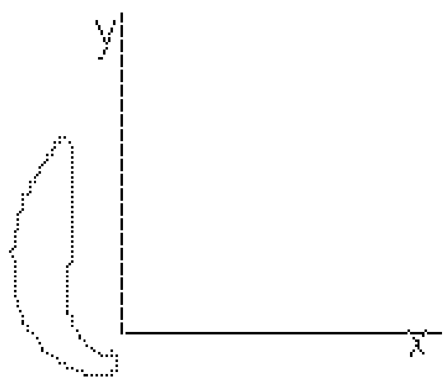
- *Boolean* and *geometric* operations on polyhedra

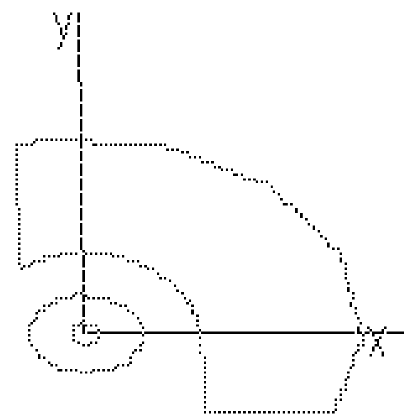
Example



$$A_0 = \begin{bmatrix} 0 & -0.6 \\ 3 & 0 \end{bmatrix} \quad A_1 = \begin{bmatrix} -2 & -3 \\ 3 & -2 \end{bmatrix}$$



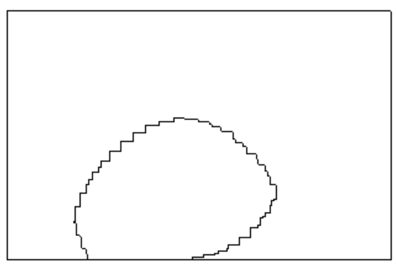




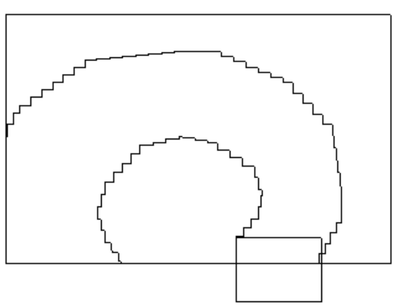
q_0 q_1 q_0

Example: $F\ Until\ G$

Given two subsets F and G. Calculate $F\ Until\ G$?



The states which can **stay in** F **forever**



The states which can **stay in** F and **reach** G

$A = \begin{pmatrix} -0.5 & 4.0 \\ -3.0 & -0.5 \end{pmatrix}$; $F = [-0.1, 0.1] \times [-0.03, 0.1]$;
$G = [0.02, 0.06] \times [-0.05, -0.02]$

The tool d/dt

Three functionalities

- **Reachability Analysis**
  - Linear continuous systems
  - Non-linear continuous systems
  - Hybrid systems
- **Safety verification of hybrid systems**
- **Safety switching controller synthesis** for hybrid systems with linear continuous dynamics

Future work

⋆ More efficient polyhedral approximation algorithms

⋆ Verification and controller synthesis for more general properties

Some Related Works

- Integrating Projection [Greenstreet 96]
- Ellipsoidal Techniques [Kurzhanski and Valyi 97; Kurzhanski and Varaiya 00]
- Flow-pipe Approximation [Chutinan and Krogh 99]
- Symbolic Method [Pappas, Lafferier and Yovine 99; Anai and Weipsfenning 01]
- Verification via mathematical programming [Bemporad and Morari 99]