CSE 591: Theoretical Aspects of CPS

Computation of reachable sets: Tabuada Ch 7.6, References in the slides

Instructor: Georgios E. Fainekos

Slides adapted and mixed by A. Girard, A. A. Julius and G. Pappas

School of Computing, Informatics and Decision System Engineering

Arizona State University

fainekos at asu edu

http://www.public.asu.edu/~gfaineko

Reachability Problem

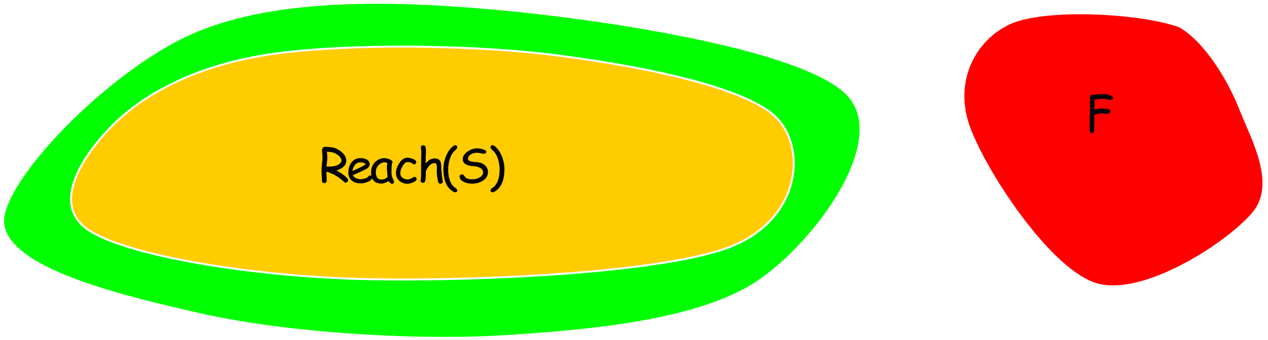
- Given a set $F \subseteq R^n$, evaluate the expressions

$$Reach_{[0,T]}(S) \cap F = \emptyset$$

$$Reach(S) \cap F = \emptyset$$

- Safety verification (F is an unsafe set)

- Exact computation difficult (impossible for most systems):
  -> Compute over-approximations the reachable set



-> S is safe

Reachability Analysis Using Numerical Techniques

- Level Sets Methods,
  [Mitchell, Tomlin and other contributors]
- CheckMate,
  [Chutinan, Krogh and other contributors]
- d/dt,
  [Dang]
- Ellipsoidal Toolbox,
  [Kurzhanski and Varaiya]
- MATISSE,
  [Girard]

Flow Pipe Approximation

- Main observation:

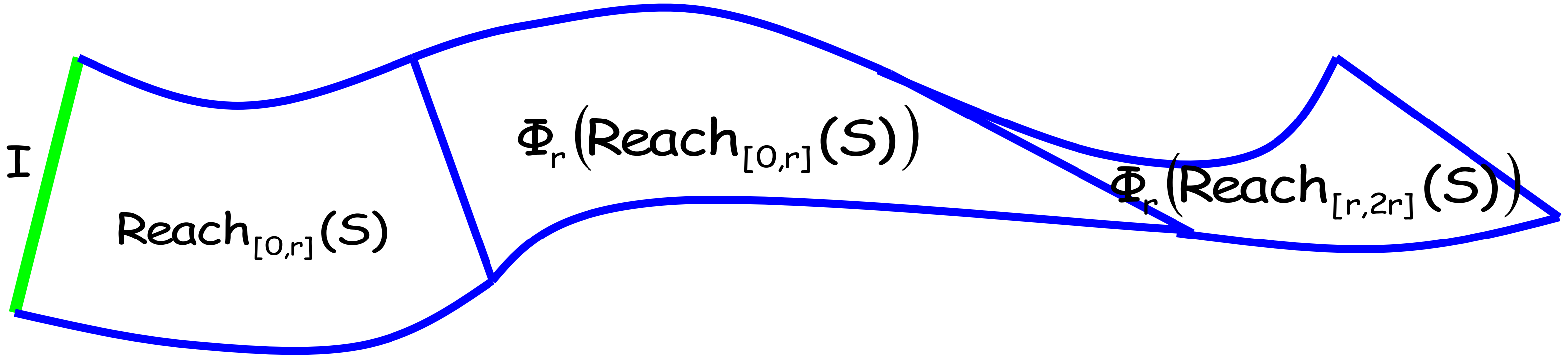
Given a time step r and T = Nr,

$$Reach_{[0,T]}(S) = \bigcup_{k=0}^{k=N-1} Reach_{[kr,(k+1)r]}(S).$$

and

$$Reach_{[kr,(k+1)r]}(S) = \Phi_r\left(Reach_{[(k-1)r,kr]}(S)\right)$$

where $\Phi_r(X)$ is the set of points reachable at time r from X.



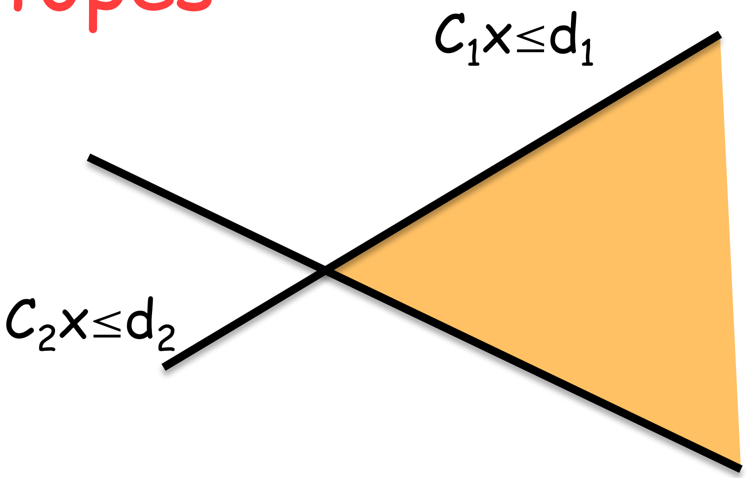
Flow Pipe Approximation

- Algorithm:
  - Over-approximate $Reach_{[0,r]}(S)$
  - Propagate the reachable set using Φ_r
- For linear systems ($f(x,u)=Ax+Bu$):

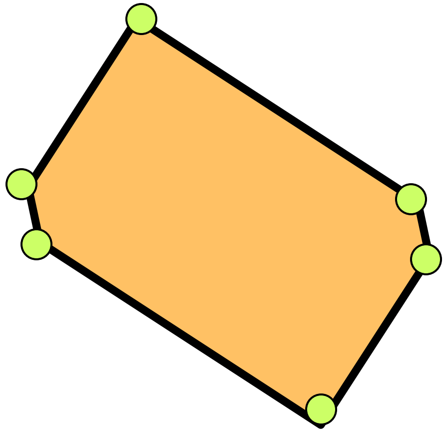
$$\Phi_r(X) = e^{rA}X \oplus V$$

- After initialization, only requires
  - linear transformations
  - Minkowski sums

Polytopes



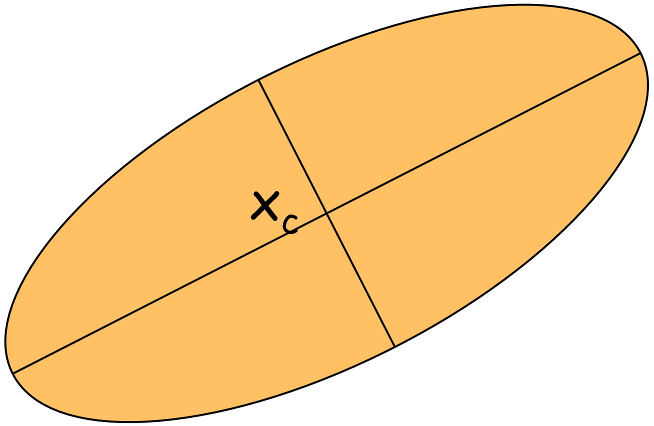
- H-Polyhedron
  - $P = \cap_{i\in\{1,p\}} \{ x\in\mathbb{R}^n \mid C_i x\leq d_i \}$
- V-Polytope
  - Convex hull of finite set of points



- H-Polyhedron vs V-Polytope
  - d-cube: 2d halfspaces vs 2^d vertices
- Matlab Toolbox for manipulating polytopes
  - MPT

Ellipsoids

- $E = \{ x \mid (x-x_c)^T A^{-1} (x-x_c) \leq 1\}$
  - A is symmetric
  - The lengths of the semi axis are given by $(\lambda_i)^{1/2}$
    λ_i are the eigenvalues of A

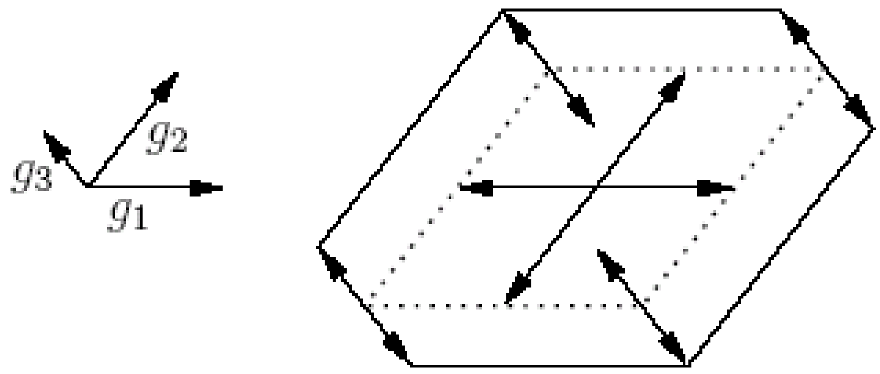


Zonotopes

- Zonotope: Minkowski sum of a finite number of segments.

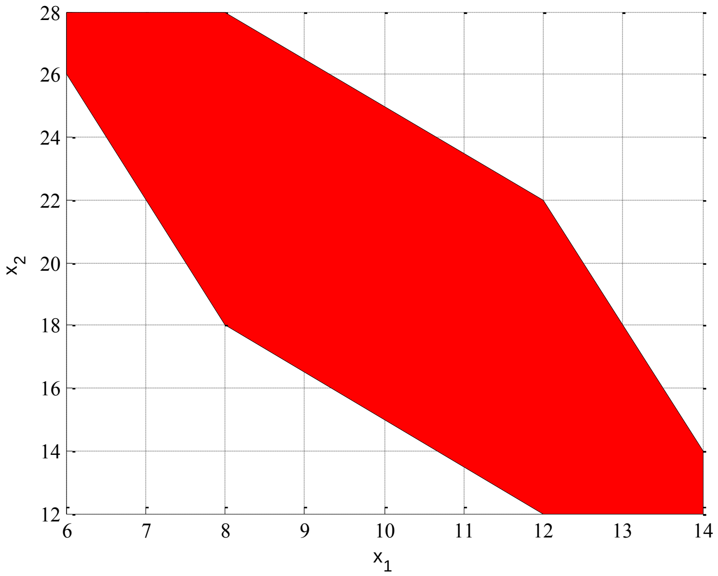
$$Z = \left\{ x \in R^n, x = c + \sum_{i=1}^{i=p} x_i g_i, -1 \le x_i \le 1 \right\}.$$

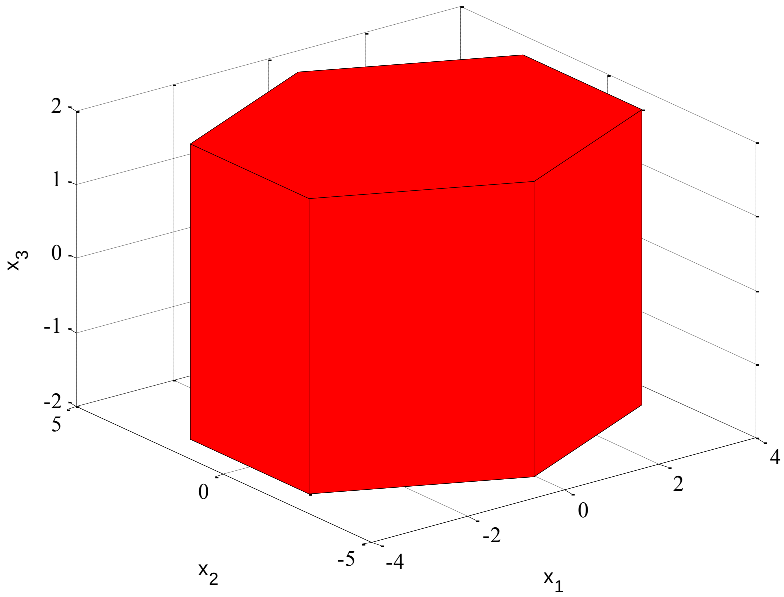
- c is the center of the zonotope, $\{g_1,\ldots,g_p\}$ are the generators. The ratio p/n is the order of the zonotope.



Two dimensional zonotope with 3 generators

Examples





$c = [10, 20]^T$

$g_1 = [2,-3]^T$

$g_2 = [1,0]^T$

$g_3 = [0,1]^T$

$g_4 = [-1,4]^T$

$c = [0, 0, 0]^T$

$g_1 = [3^{1/2},1,0]^T$

$g_2 = [3^{1/2},-1,0]^T$

$g_3 = [0,2,0]^T$

$g_4 = [0,0,2]^T$

Some Properties of Zonotopes

- The encoding of a zonotope has a polynomial complexity with the dimension.

- The set of zonotopes is closed under linear transformation

$$Z = (c, < g_1, \ldots, g_p >), LZ = (Lc, < Lg_1, \ldots, Lg_p >).$$

- The set of zonotopes is closed under the Minkowski sum

$$Z_1 = (c_1, < g_1, \ldots, g_p >), Z_2 = (c_2, < h_1, \ldots, h_q >).$$

$$Z_1 \oplus Z_2 = (c_1 + c_2, < g_1, \ldots, g_p, h_1, \ldots, h_q >).$$

- Exactly what we need for our reachability algorithm

Flow Pipe Approximation

- Choice of the representation of the reachable set:
  - closed under linear maps and Minkowski sums
    - -> Polytopes [Krogh; Dang]
    - -> Accurate
    - -> Not scalable (exponential complexity)
  - scalable representations
    - -> Ellipsoids [Kurzhanski and Varaiya]
    - -> Oriented rectangular hull [Krogh]
    - -> Not closed under linear maps and Minkowski sums
    - -> Additional computations and approximations
  - Zonotopes [Girard]
    - -> Closed under linear maps and Minkowski sums
    - -> Accurate
    - -> Scalable (polynomial complexity/dimension)

Linear Systems

Linear systems: $\dot{x} = Ax + Bu$.

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

If $u(t) \in \mathbb{R}^m$: $\mathrm{im}[B \; AB \; \cdots \; A^{n-1}B]$

If $\|u(t)\|_\infty \leq \mu$,

$$\left\| \int_0^t e^{(t-\tau)A}Bu(\tau)d\tau \right\|_\infty \leq \int_0^t \left\| e^{(t-\tau)A}Bu(\tau) \right\|_\infty d\tau$$

Linear Systems

$$\int_0^t \left\| e^{(t-\tau)A} B u(\tau) \right\|_\infty d\tau \leq \int_0^t \left\| e^{(t-\tau)A} B \right\|_\infty \| u(\tau) \|_\infty d\tau$$

$$\leq \int_0^t \left\| e^{(t-\tau)A} B \right\|_\infty \mu d\tau$$

$$= \mu \int_0^t \left\| e^{(t-\tau)A} B \right\|_\infty d\tau$$

$$= \mu \cdot \beta$$

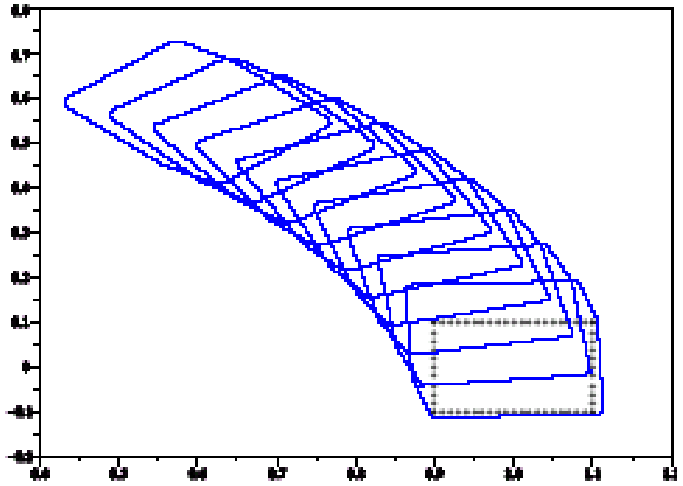
Thus $\int_0^t e^{A(t-\tau)} B u(\tau) d\tau$ is approximated with a rectangle.

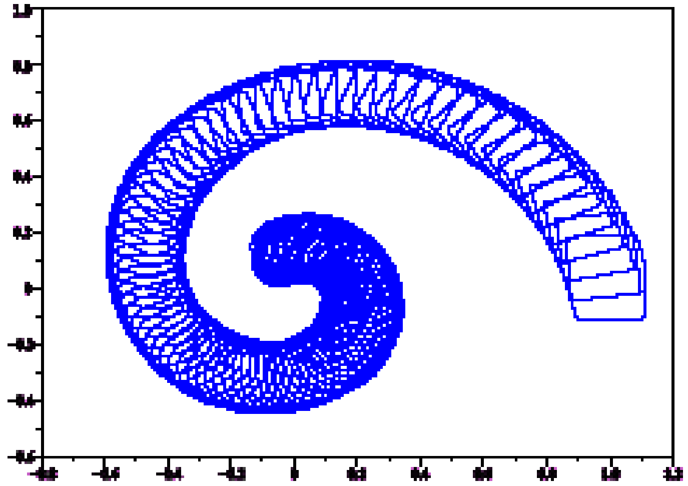
Reachability Algorithm with Zonotopes

APPROXIMATE $\text{Reach}_{[0,T]}(S)$

1. $r = \frac{T}{N}$
2. Obtain a zonotope Q_0 as an over approximation of $\text{Reach}_{[0,r]}(S)$.
3. $R_0 = Q_0$.
4. $Q_{i+1} = e^{Ar} Q_i \oplus \square$.
5. $R_{i+1} = R_i \cup Q_{i+1}$.
6. $\text{Reach}_{[0,T]}(S) \approx R_N$

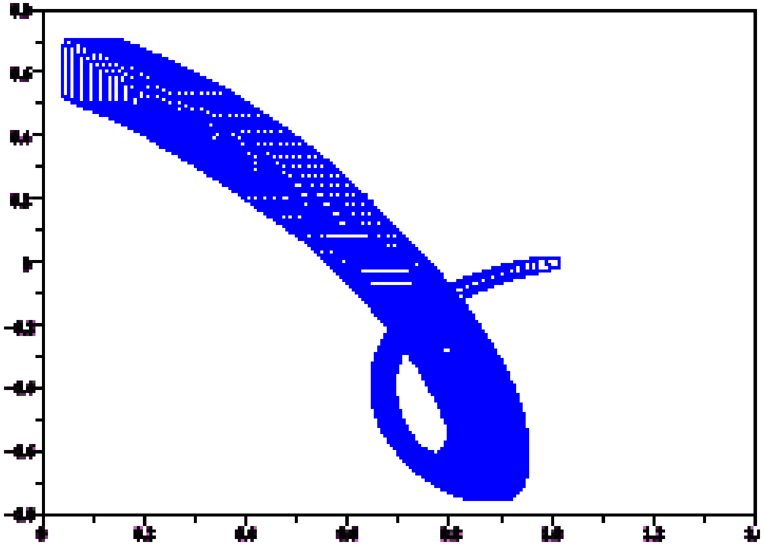
Two dimensional example

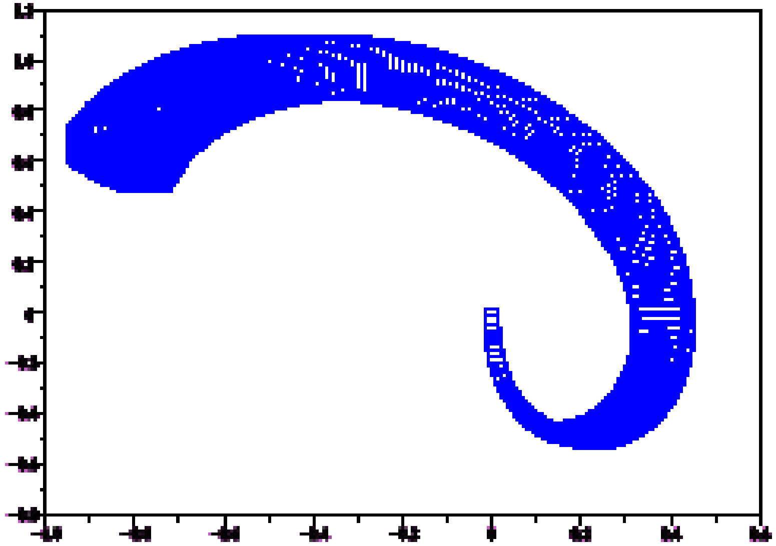




Reachable set on the interval [0,2],
100 iterations.

Five dimensional example





Projections of the reachable set on the interval [0,1], 200 iterations.

Hybrid Systems

We consider the class of hybrid systems that consists of:

1. A finite set Q of modes.
2. In each mode q, the continuous dynamics is given by a linear system:

$$\dot{x}(t) = A_q x(t) + B_q u(t),\ u(t) \in U_q$$

3. Switching conditions (Guards) are given by linear inequalities:

$$q \to q' \Leftrightarrow x(t) \in S_{q,q'} = \left\{ m_{q,q'} \le h_{q,q'} \cdot x \le M_{q,q'} \right\}$$

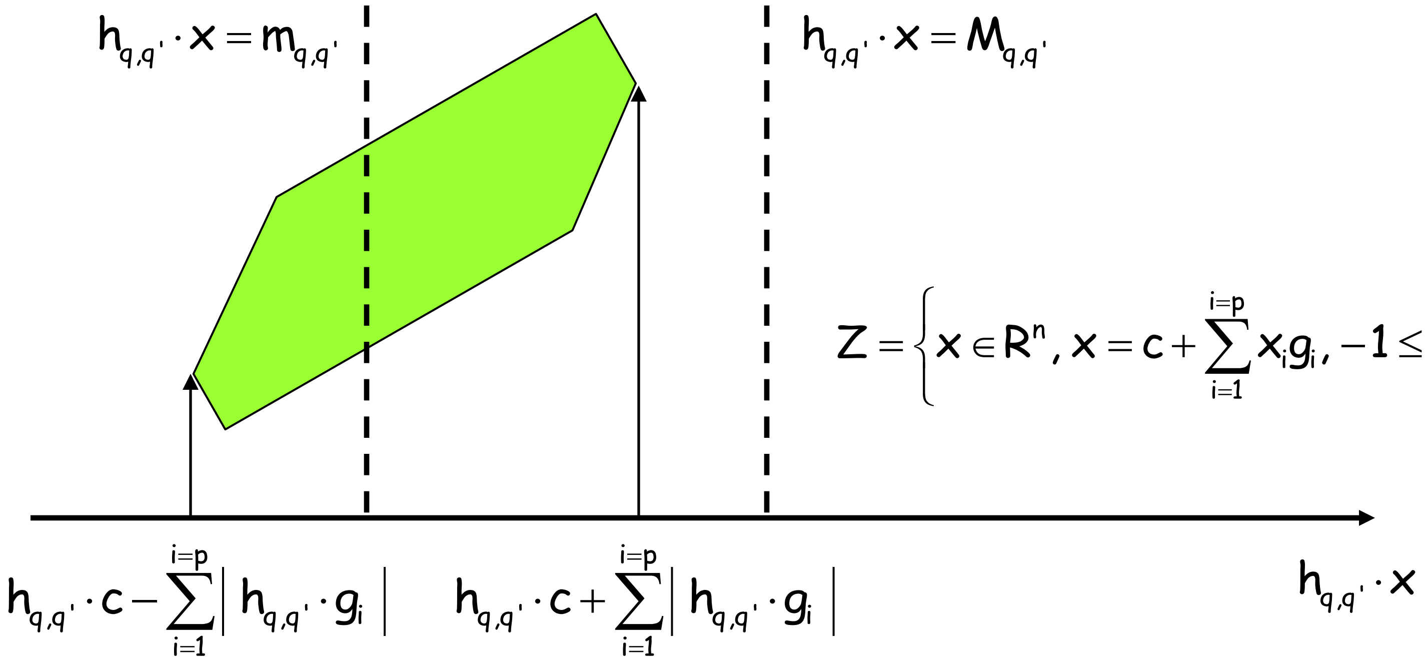
Reachability of Hybrid Systems

Following the classical scheme for reachability of hybrid systems:

- In each mode, the reachability analysis of the continuous dynamics is handled by our algorithm.
- Processing of discrete transitions requires:
  1. Detection of the intersection of a zonotope with a guard.
  2. Computation of this intersection
     - The intersection of zonotope with a band is not a zonotope.
     - Over-approximation algorithms.

Event Detection

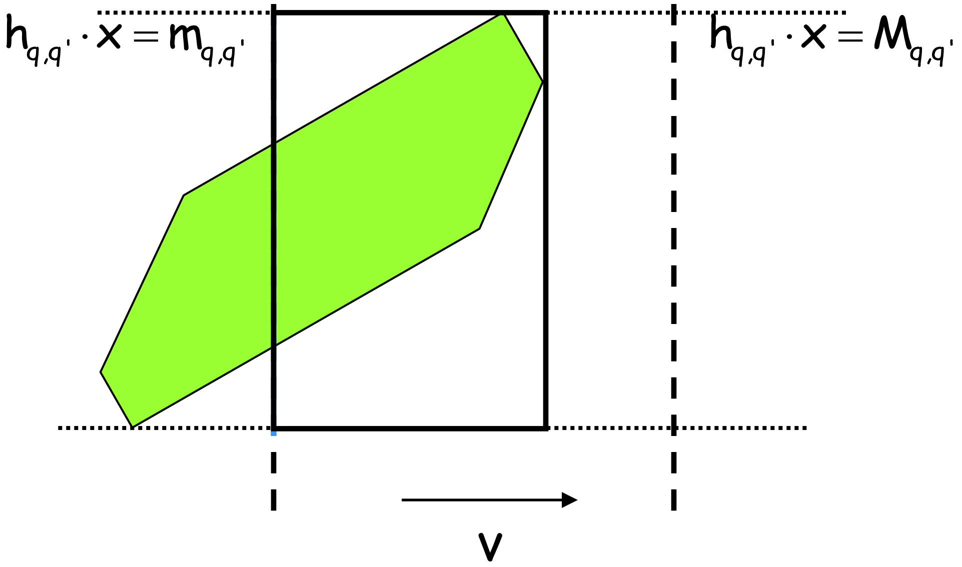
- Detection of the intersection of a zonotope with a guard.



$$\text{Intersection} \Leftrightarrow \left[h_{q,q'} \cdot c - \sum_{i=1}^{i=p} \left| h_{q,q'} \cdot g_i \right|, h_{q,q'} \cdot c + \sum_{i=1}^{i=p} \left| h_{q,q'} \cdot g_i \right| \right] \cap \left[m_{q,q'}, M_{q,q'} \right] \neq \varnothing$$

Computing the Intersection

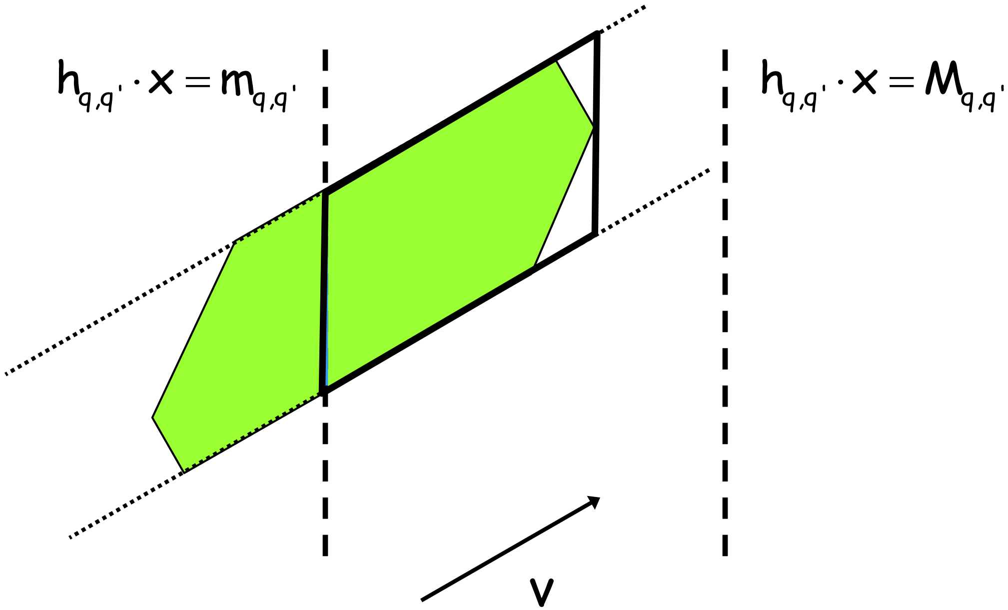
- Over-approximation by projection and bloating:



- The over-approximation I is
  - a zonotope: $I = P_v Z \oplus [\alpha, \beta] v.$
  - included in the guard

Computing the Intersection

- You can project in an other direction:



- Find the direction which results in the *best* over-approximation.

Direction of Projection

- Computation of the best direction is feasible but difficult
- Heuristics:
  - direction as weighted sum of generators (C. Le Guernic):

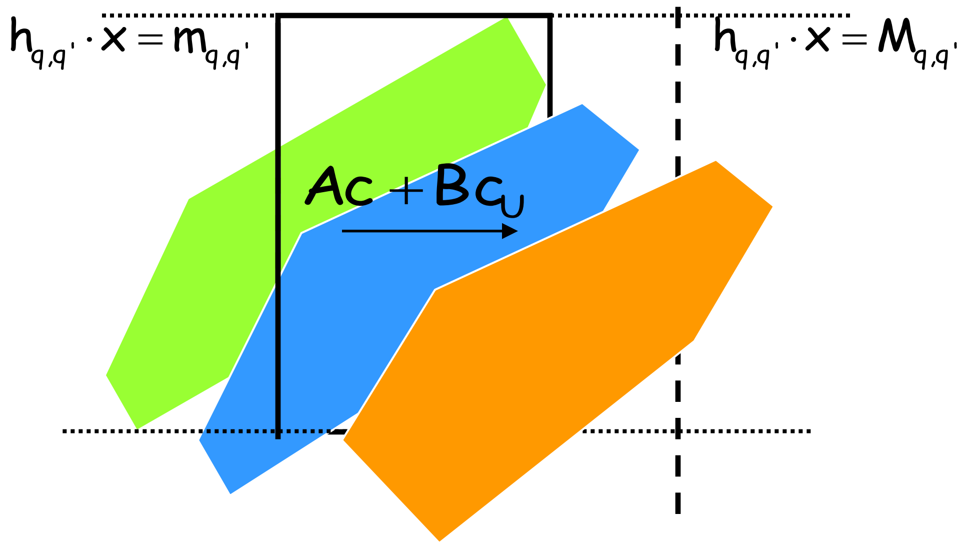
$$v = \sum_{i=1}^{i=p} \frac{|g_i \cdot h_{q,q'}|}{\|g_i\|} g_i.$$

  - use the dynamics of the system:

$$v = Ac + Bc_U.$$

Direction of Projection

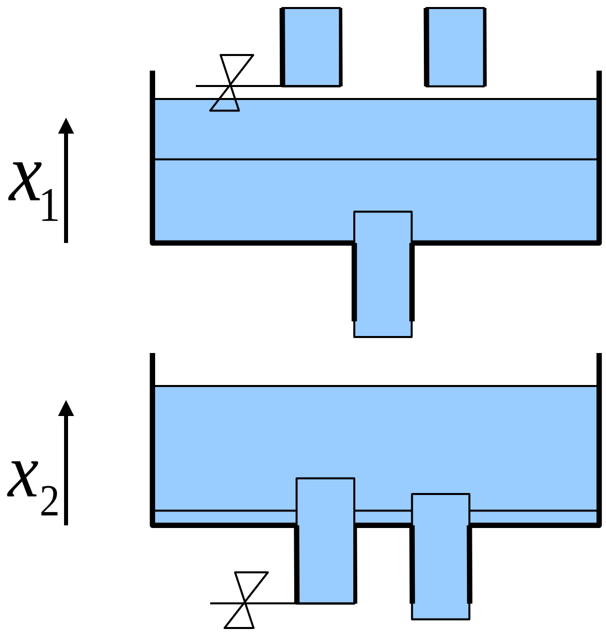
- *Dynamic* heuristic:

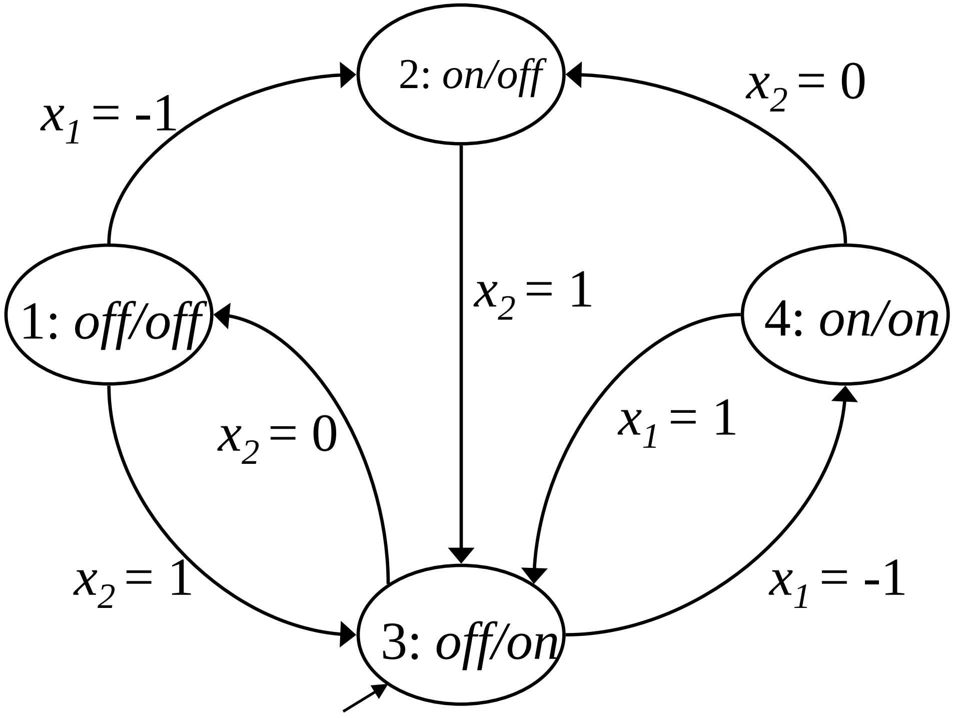


- A large part of the over-approximation at step k is actually reachable at steps k+1, k+2…

Example

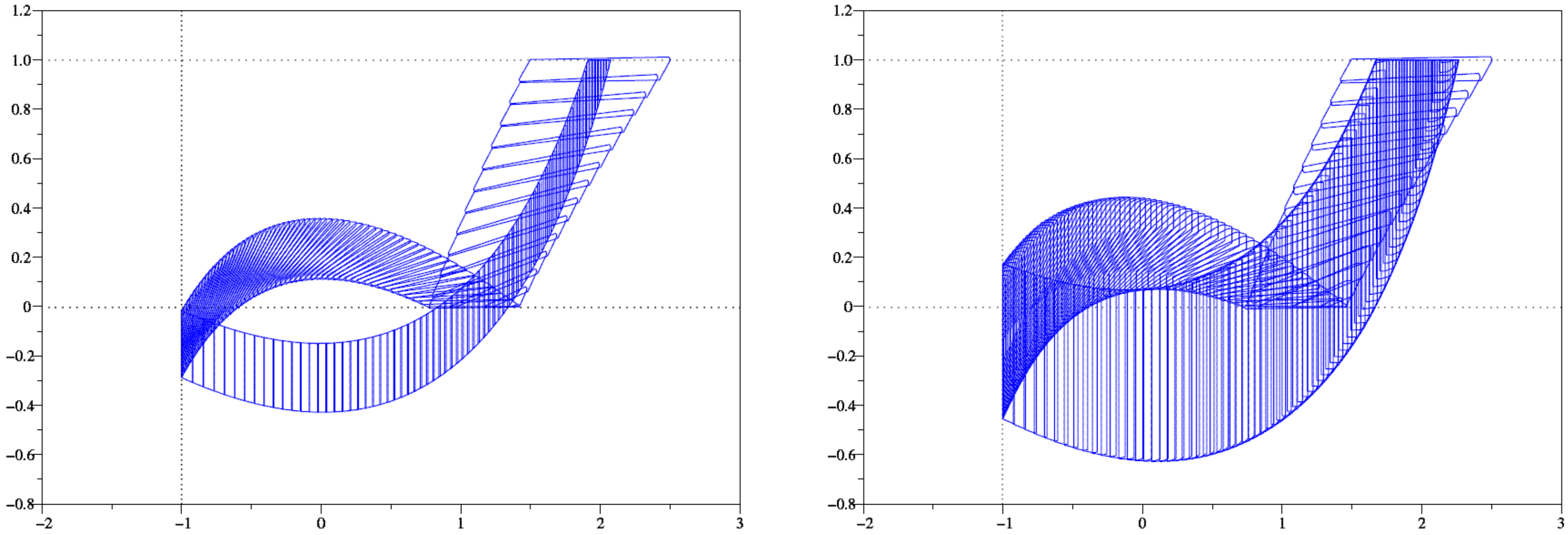
Two tank system:





Want to check robustness of periodic behavior.

Example



Reachable set of the two tank system for $\mu = 0.01$ and $\mu = 0.1$

Hybrid reachability needs to be tested for large scale examples.

Reachability of Nonlinear Systems

Two approaches for reachability analysis of nonlinear systems:

- Hybridization approach [Asarin, Dang, Girard]:
  - state space is partitioned
  - in each region, linear conservative approximation of the nonlinear vector field
  - accurate approximation
- Trajectory piecewise linearization [Han, Krogh]:
  - at each time step, vector field linearized around the center of the zonotope
  - efficient computations

MATISSE

- MATISSE is a MATLAB toolbox.
- Developed by Antoine Girard and George Pappas at UPenn.
- Main purpose is to compute abstraction/reduction of constrained linear systems, based on approximate bisimulation.
- Contains a functionality to compute the reachable set of a constrained linear system.

Constrained Linear Systems

- Constraints and reachable set are expressed as zonotopes.

- Constrained linear systems are systems of the form:

$$\begin{aligned}\dot{x} &= Ax + Bu,\\ y &= Cx,\\ x(0) \in I&, u(t) \in U.\end{aligned}$$

- The set I and U are zonotopes.

Usage

- A constrained linear system (CLS) is defined as a 5-tuple, (A,B,C,U,I).

```
S = cls(A,B,C,U,I);
```

- Example:

```
A=[0 1 0;-1 0 0; 0 0 -1];B=[1;0;1];
C=[1 0 0;0 1 1];
U=inhull(-1,1);
I=inhull([9 9 9]',[10 10 10]');
S=cls(A,B,C,U,I);
```

Reachable set

- Reachable set is computed using the function reach_set. The function returns two arrays of zonotopes.

```
[Rx,Ru]=reach_set(S,dt,N);
```

- S is a CLS, dt is the time step, N is the number of intervals. The end time of the reachability algorithm is thus N x dt.
- Then, a 2-dimensional cross-section of the reachability set can be plotted using:

```
plot_reach(Rx,Ru,P,'b');
```

Plotting the reachable set

- Plotting the reachability set in 2D:

```
plot_reach(Rx,Ru,P,'b');
```

- P is a 2xm matrix that defines the projection from output space to $\mathbb{R}^2$.

- The color of the plot is defined by the last option. In this case 'b' means blue, 'r' means red, etc

Example