Note Title 2/21/2006

Reachability and safety analysis

Goal: To verify if the set of reachable states intersect the set of unsafe states.

Methods :

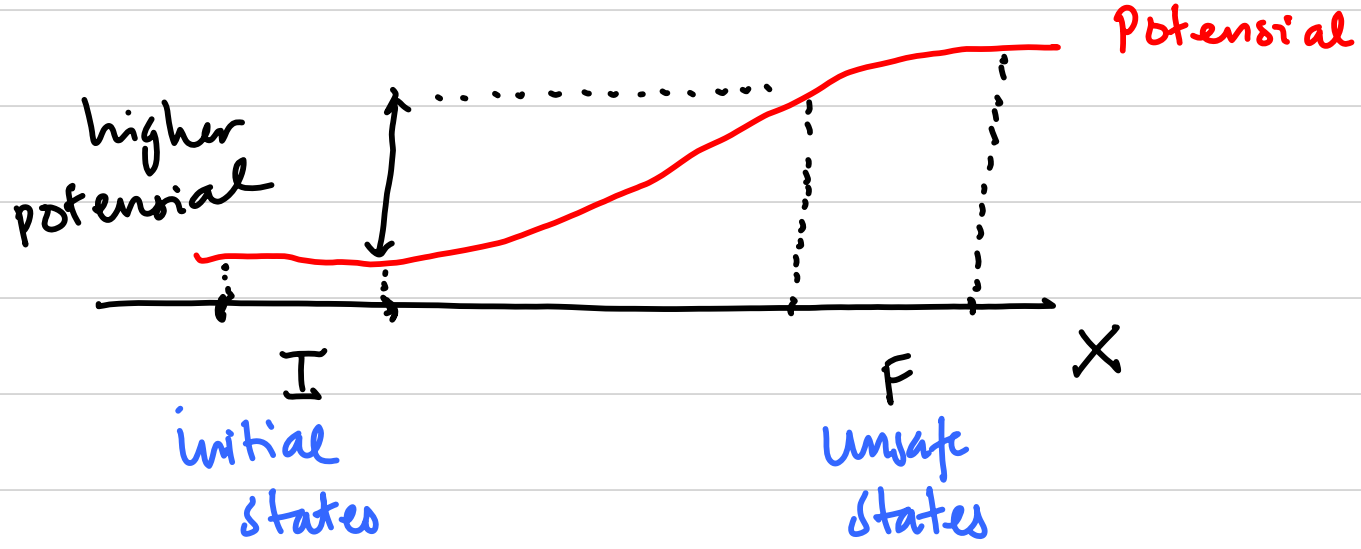
- Flowpipe ✓
- Barrier certificate
- Level sets
- Predicate abstraction

Tools :

- d/dt, Hytech, UPPAAL, KRONOS, SOSTOOL, Level set toolbox.

Barrier Certificate (R22)

Basic idea: create a potential like barrier between the set of initial states and the unsafe set.



We guarantee that there is no trajectory going from I to F.

Remarks:

- Similar to Lyapunov theory for stability
- there is no need to compute the flow of the system.

Given a dynamical system:

$$\dot{x} = f(x, d)$$

state, input

$$x \in X, \quad d \in D$$

Set of initial states X_0

Set of unsafe states X_u

A barrier certificate $B(x)$ satisfies:

$B(x) > 0, \quad \forall x \in \mathcal{X}_u$

$B(x) < 0, \quad \forall x \in \mathcal{X}_0$

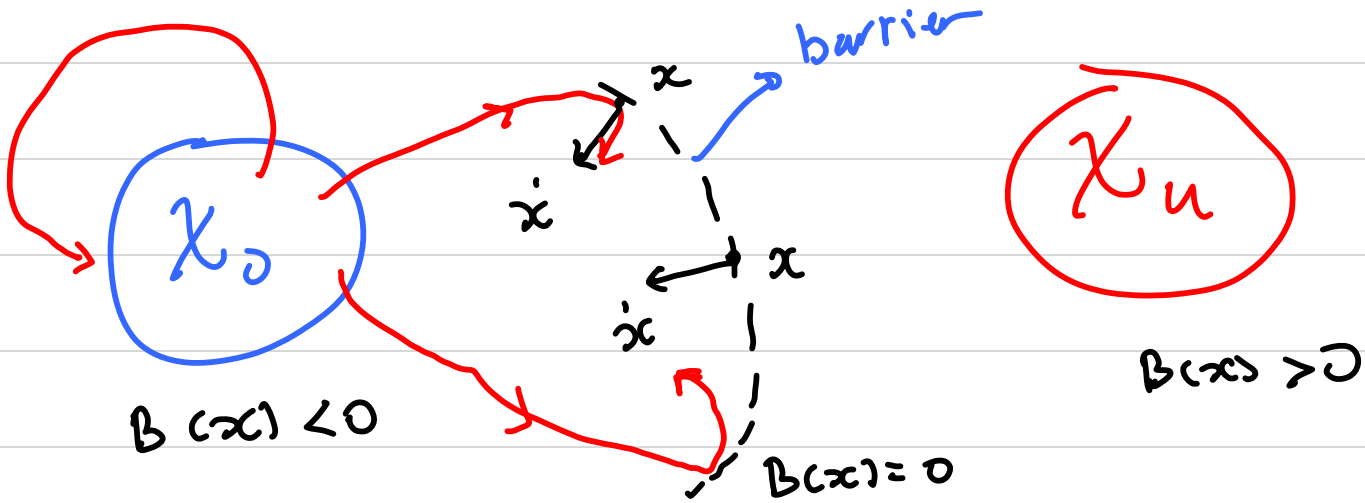
$\underbrace{\frac{\partial B}{\partial x} f(x,d)}_{\frac{d}{dt}B} \leq 0, \quad \forall x \in \mathcal{X}$, and $d \in D$ such that $B(x) = 0$

$\frac{d}{dt}B = \frac{\partial B}{\partial x} \cdot \frac{dx}{dt}$

$= \frac{\partial B}{\partial x} f(x,d)$

→ the rate of change of $B(x)$ at $B(x) = 0$

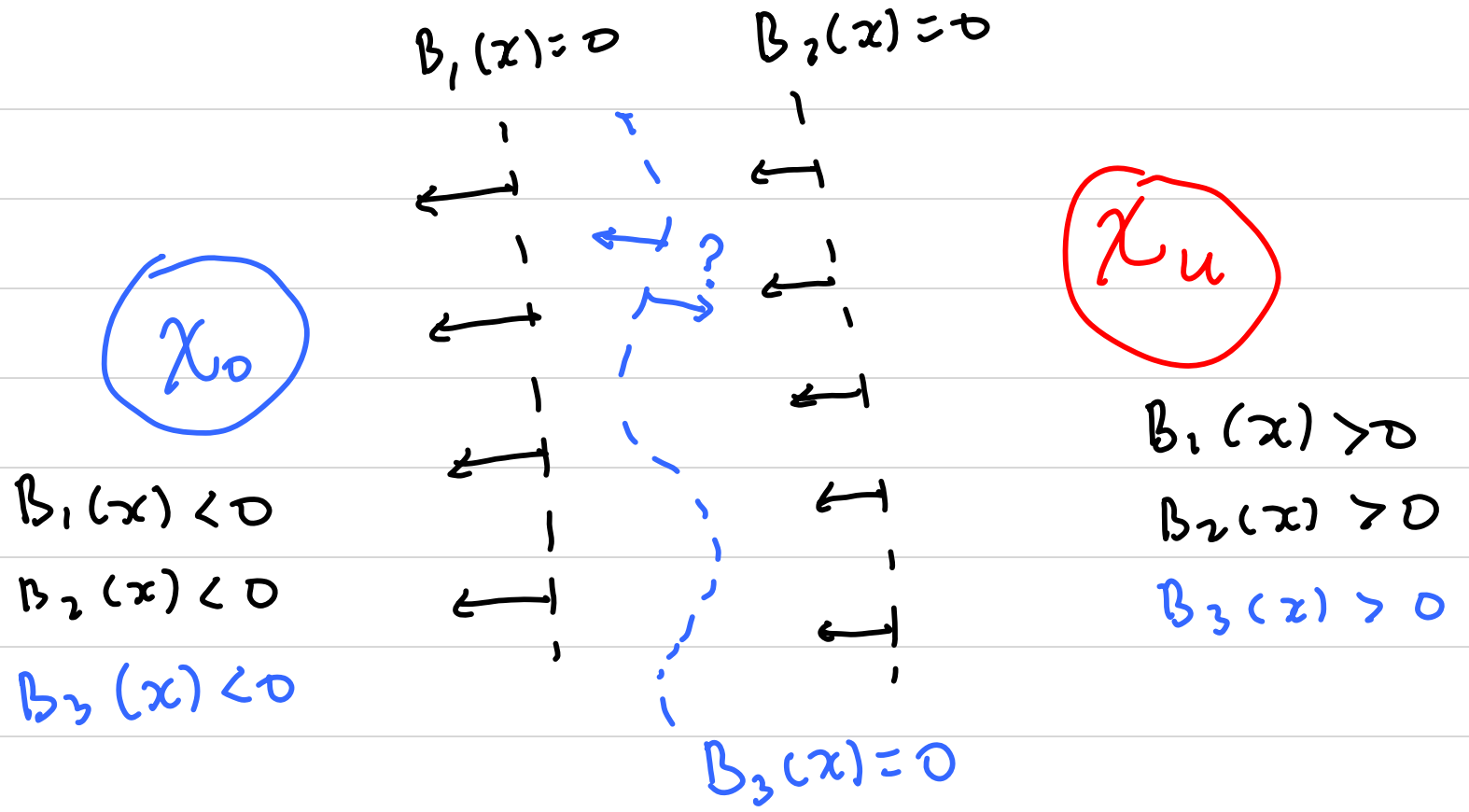
Existence of B implies the system is safe.



The set of such barrier functions is not convex, i.e:
If B_1 and B_2 are barrier functions, then for any $0 \leq \lambda \leq 1$,

$$B_3 := (\lambda B_1 + (1-\lambda) B_2)$$

is generally not a barrier function.



Non convexity means we cannot apply methods from convex optimization to construct a barrier.

The set of barrier functions can be made convex by requiring that:

$$\frac{\partial B}{\partial x} f(x,d) \leq 0 \quad \text{for all } x \in X, d \in D$$

instead of

$$\frac{\partial B}{\partial x} f(x,d) \leq 0 \quad \text{for all } x \in X, d \in D \text{ s.t } B(x)=0$$

Construction of barrier certificate, under the assumption that

- $f(x,d)$ is a polynomial
- X_0 and X_u are semi algebraic sets
- the barrier itself is a polynomial,

can be posed as a semidefinite optimization problem. There is a MATLAB Toolbox for this purpose, SOSTOOL.

Application to hybrid systems

Consider a hybrid system

$$H = (X, L, X_0, I, F, T)$$

X is the continuous state space

L is the set of locations, $L \times X$ is the hybrid state space

$X_0 \subseteq L \times X$ is the set of initial states

$I : L \to 2^X$, is the invariant. $I(l)$ is the invariant of location $l \in L$

$F : L \times \mathcal{X} \to 2^{\mathbb{R}^n}$ is a set of vector fields.

$\dot{x} \in F(\ell, x)$

is the continuous dynamics of location $\ell \in L$

Assume: $F(\ell, x) = \{ z \mid z = f_\ell(x, d), \text{ for some } d \in D(\ell) \}$

$T \subseteq (L \times \mathcal{X}) \times (L \times \mathcal{X})$ is the transition relation

Guard and reset are encoded in T.

$\text{Guard}(\ell, \ell') = \{ x \in \mathcal{X} \mid \exists x' \in \mathcal{X}. ((\ell, x), (\ell', x')) \in T \}$

$\text{Reset}(\ell, \ell')(x) = \{ x' \in \mathcal{X} \mid ((\ell, x), (\ell', x')) \in T \}$

Given an unsafe set $X_u \subseteq L \times X$, define

$$\text{Init}(l) = \{x \in X \mid (l,x) \in X_0\}$$

$$\text{Unsafe}(l) = \{x \in X \mid (l,x) \in X_u\}$$

A family of barrier certificates $\{B_l\}_{l \in L}$ satisfies:

$$B_l(x) > 0 \quad , \forall x \in \text{Unsafe}(l)$$

$$B_l(x) < 0 \quad , \forall x \in \text{Init}(l)$$

$$(*) \quad \frac{\partial B_l}{\partial x} f_l(x,d) \quad , \forall x \in I(l), d \in D(l) \text{ s.t. } B_l(x) = 0$$

$$(**) \quad B_{l'}(x') \leq 0 \quad , \forall x' \in \text{Reset}(l,l')(x), x \in \text{Guard}(l,l')$$

$$B_l(x) \leq 0$$

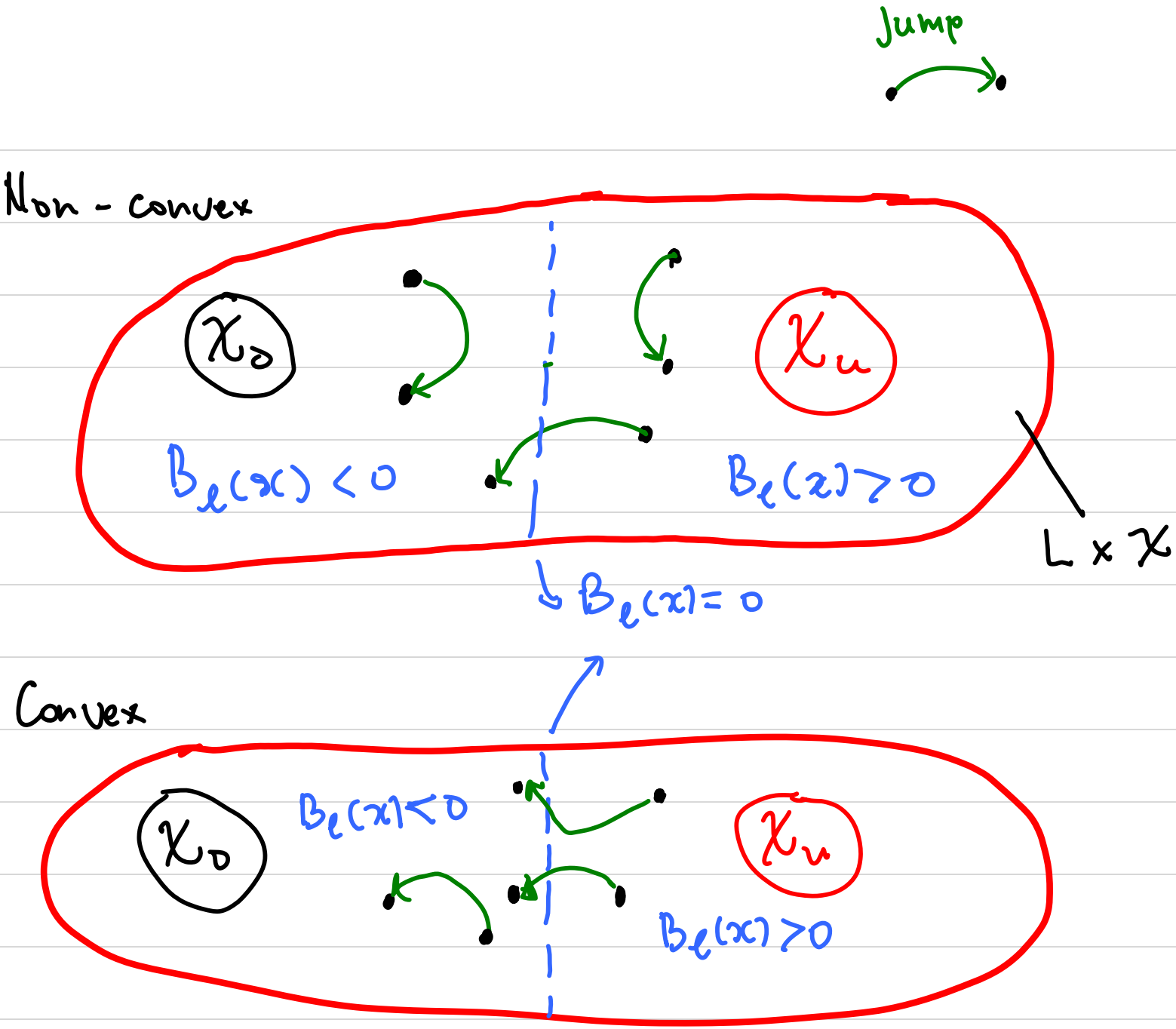
Existence of $\{B_\ell\}_{\ell \in L}$ implies the system is safe

The set of barrier certificates characterized in the previous page is **not convex.**

To get a convex set, we replace (*) and (**) with

$$\frac{\partial B_\ell}{\partial x} f_\ell(x, d) \leq 0, \quad \forall x \in I(\ell), d \in D(\ell)$$

$$B_{\ell'}(x') \leq 0, \quad \forall x' \in \text{Reset}(\ell, \ell')(x), x \in \text{Guard}(\ell, \ell')$$


Jump
Non - convex
χ_o
χ_u
$B_\ell(x) < 0$
$B_\ell(x) > 0$
$L \times \chi$
$B_\ell(x) = 0$
Convex
χ_o
$B_\ell(x) < 0$
χ_u
$B_\ell(x) > 0$

Under several assumptions:

- $f_q(x,d)$ is a polynomial,
- K_0 and K_u are semi algebraic sets,
- the barrier itself is a polynomial,
- the reset and guards are semialgebraic sets,

The construction of the barrier can be posed as a semidefinite programming, and can be solved using SOSTOOL.

Level sets (R23) (R24)

Consider a dynamical system

$$\dot{x} = f(x, u, d)$$

state, input, disturbance

The dynamics of the system can be thought of as a game between the input and the disturbance.

The game interpretation plays role, e.g. in controller design.

The game: The input makes a decision first, and then the disturbance does. The disturbance wins if the state is steered to unsafe set. Otherwise the input wins.

E.g. in designing a controller that guarantees safety regardless of the action of the disturbance.

Let $G_0 \subset X$ be the unsafe set.

Let $G(\tau)$ be the set of states such that

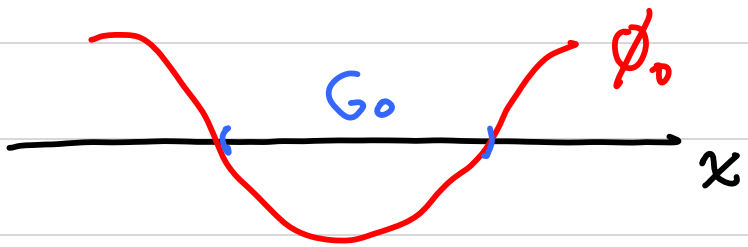
$x_0 \in G(\tau) \implies \exists\ 0 \le s \le \tau$ such that for any $u(\cdot)$, there exists a $d(\cdot)$ that steers the state from initial state $x(0) = x_0$ to $x(s) \in G_0$

$G(\tau)$ is the set of states from where the disturbance can win within τ time units.

In this method, sets are represented as level sets of a function.

$$G_0 \subseteq X \longrightarrow \quad \phi_0 : X \to \mathbb{R}$$

$$G_0 = \{ x \mid \phi_0(x) \leq 0 \}$$



The set $G(\tau)$ is represented by $\phi(\cdot, \tau)$, with

$$\phi(\cdot,\cdot) : \mathcal{X} \times \mathbb{R}_+ \to \mathbb{R}$$

From optimal control theory, it can be proven that

$$\frac{\partial \phi}{\partial t} - \min\left[0, H\left(x, \frac{\partial \phi}{\partial x}\right)\right] = 0,$$

$$H\left(x, \frac{\partial \phi}{\partial x}\right) = \max_{u \in \mathcal{U}} \min_{d \in \mathcal{D}} \frac{\partial \phi}{\partial x} \cdot f(x, u, d)$$

with initial condition $\phi(\cdot, 0) = \phi_0$

Interpretation: $\tau \leq \tau' \Longrightarrow G(\tau) \subseteq G(\tau')$

If the input wins: $H(x, \frac{\partial \phi}{\partial x}) \geq 0$, $G(\tau)$ does not become bigger.

If the disturbance wins: $H(x, \frac{\partial \phi}{\partial x}) < 0$, $G(\tau)$ becomes bigger.

If we are interested in reachability without 2-player game interpretation, the formulation can be adopted to:

$$\dot{x} = f(x, d)$$

The set of initial condition $\underline{I} \subset K$ is represented by $I := \{ x \mid \phi_0 \leq 0 \}$

The forward reachable set $\text{Reach}_{[0,\tau]}$ is represented by $\phi(\cdot, \tau)$

$$\frac{\partial \phi}{\partial t} + \max\left[0, H\left(x, \frac{\partial \phi}{\partial x}\right)\right] = 0$$

$$H\left(x, \frac{\partial \phi}{\partial x}\right) = \max_{d \in D} \frac{\partial \phi}{\partial x} \cdot f(x, d)$$

$$\phi(\cdot, 0) = \phi_0$$

The PDE is solved numerically by gridding the state space.

This method is powerful for nonlinear dynamics

Caveat: because of gridding technique, complexity increases exponentially w.r.t system dimension.

Available tool: Level sets toolbox for MATLAB.

Predicate Abstraction (R25)

Idea: create a finite abstraction from the original system.

Given a hybrid automaton

$$H = (\mathcal{X}, L, X_0, I, f, T)$$

Suppose that the invariant and guards are given by linear predicates, i.e. they are given as a set of linear equations.

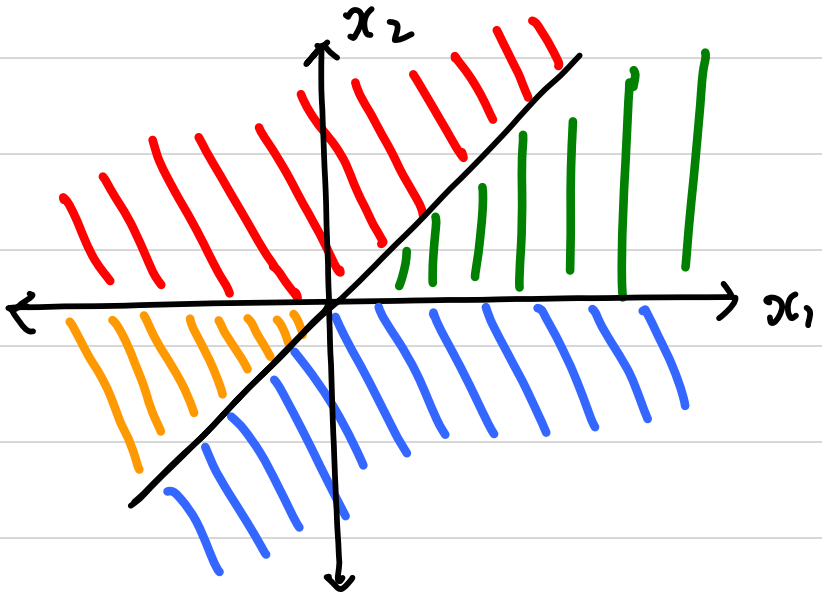
Suppose that there are k linear predicates in the system.

The continuous state space is divided into at most 2^k partition, corresponding to the truth values of the predicates

E.g.: $x_1 - x_2 \leq 0$

$x_2 \leq 0$

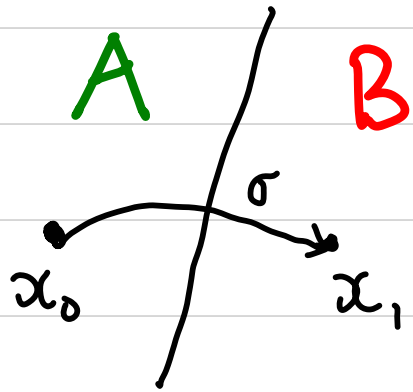
$X = \mathbb{R}^2$



Thus, the hybrid state space $L \times \mathcal{X}$ is partitioned into at most $|L| \cdot 2^k$ partitions (finite)

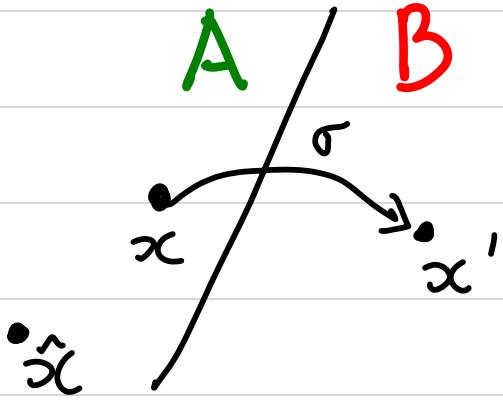
The partitions defined discrete states of a transition system that acts as an abstraction to the original system.

There is a transition from a partition A to partition B if there is a transition from a state in A to a state in B



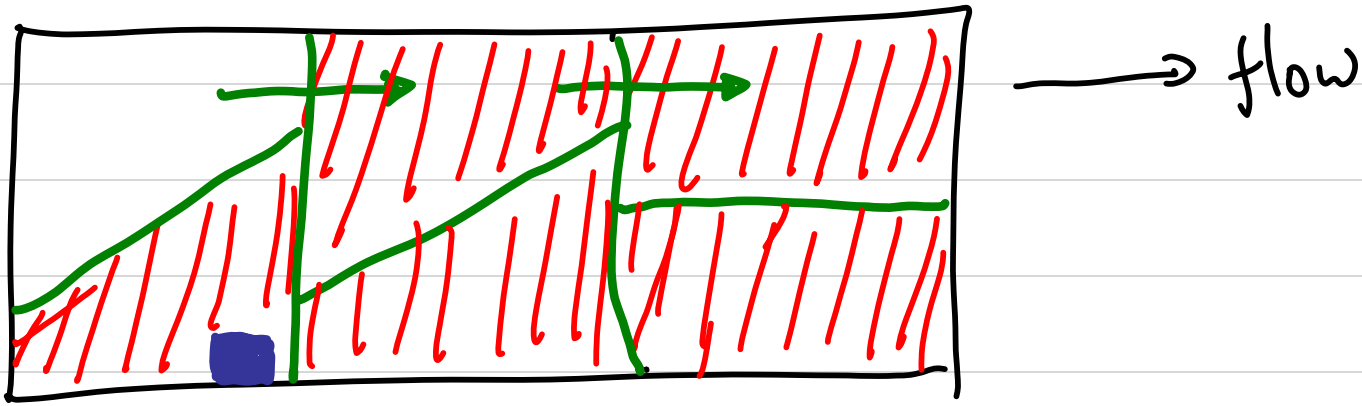
$A \xrightarrow{\sigma} B$

Approximation of the reachable set using predicate abstraction is clearly an over approximation.



$A \xrightarrow{\sigma} B$

$\not\exists \hat{x}' \in B,\ \hat{x} \xrightarrow{\sigma} \hat{x}'$



Good news: If the abstraction proves safety, then the real system is safe. Otherwise, cannot infer anything (yet).

If the partition is consistent (bisimulation), then safety of the abstraction is equivalent to safety of the real system.