CONTROLLER DESIGN FOR SAFETY

Note Title 3/14/2006

Consider a transition system $T = (Q, U, \rightarrow, Q^0)$, where

Q is the set of states, U the set of input symbols, $\rightarrow$ the translation relation,

$(q, u, q') \in \rightarrow$ means from the state q, when given the input symbol u, the state jumps to q'.

Also written as $q \xrightarrow{u} q'$

Q^0 is the set of initial states.

Suppose that $F \subset Q$ is defined as the set of safe states.

Control goal: provide system with input such that the state remain safe.

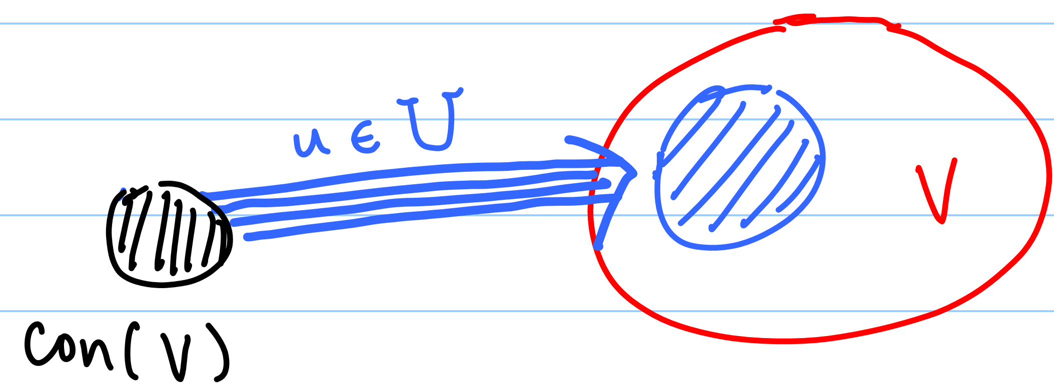
Define the next state function:

$$f(q,u) := \{ q' \in Q \mid q \xrightarrow{u} q' \}$$

The controlled Pre operator:

For any $V \subset Q$,

$$\mathrm{Con}(V) := \{ q \in Q \mid \exists u \in U \text{ s.t. } f(q,u) \subset V \}$$



Maximal controlled 'invariant subset of F

Consider the following iteration: $W_0 = F$

$$W_{i+1} = W_i \cap \mathrm{Con}(W_i)$$

Notice that : $W_{i+1} \subset W_i$ and

The fix point of the iteration satisfies:

$$W \subset F \quad \text{and}$$

$$W = W \cap \mathrm{Con}(W)$$

$$\Downarrow$$

$$W \subset \mathrm{con}(W)$$

- Meaning: from any state $q \in W$, we can choose a control input $u \in U$ such that the next state remains in W,
- W is controlled invariant
- W is the largest controlled invariant set contained in F

Starting in W, we can find a sequence that guarantees safety

If F and Q are finite, then the iteration is guaranteed to terminate after finitely many steps.

Linear systems with disturbance

Consider the linear system:

$$\dot{x} = Ax + Bu + Gd,$$

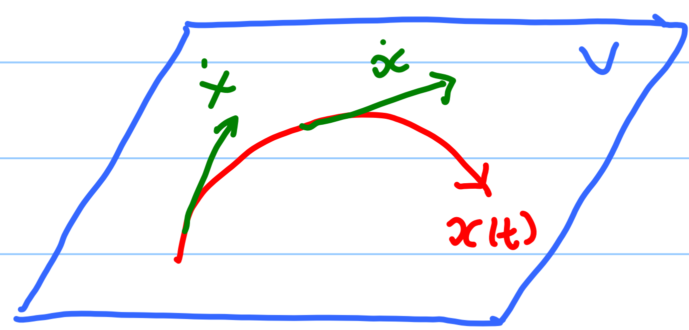
$$x \in \mathbb{R}^n, \quad u \in \mathbb{R}^m, \quad d \in \mathbb{R}^p$$

where u is the control input, and d is the disturbance.
Suppose that the safe set is a subspace $F \subset \mathbb{R}^n$
The control goal is to provide the system with an input $u(\cdot)$ that will make the system safe, despite of the disturbance.

A subspace $V \subset \mathbb{R}^n$ is controlled invariant under disturbance, if starting from any $x(0) \in V$ and given any disturbance, we can always construct an input u such that the state remains in V.

Geometrically: $\forall x \in V, d \in \mathbb{R}^p, \exists u \in \mathbb{R}^m$ such that

$$Ax + Bu + Gd \in V,$$



We are going to compute the largest controlled invariant subspace under disturbance.

Consider the iteration:

$$W_0 = F$$

$$W_{i+1} = \{ x \in W_i \mid Ax + \operatorname{im} G \subset W_i + \operatorname{im} B \}$$

Observe that:

- $W_{i+1} \subset W_i$
- W_i is a linear space (Prove that!)
- The fixpoint of the iteration satisfies

$$\boxed{AW + \operatorname{im} G \subset W + \operatorname{im} B}$$

$$\boxed{AW + \operatorname{im} G \subset W + \operatorname{im} B}$$

$\forall x \in W$ and $d \in \mathbb{R}^p$, there exist $w \in W$ and $u \in \mathbb{R}^m$ such that

$$Ax + Gd = w + Bu,$$

$$Ax - Bu + Gd = w \in W$$

W is controlled invariant!

Note: The iteration is guaranteed to terminate after finitely many steps (the dimension argument)

It is possible to design a linear feedback
$u = Kx + Ld$ such that:

$$\dot{x} = Ax + Bu + Gd = (A+BK)x + (G+BL)d$$

For any $x(0) \in W$, the trajectory remains in W for any disturbance d.

Special case: $\operatorname{im} G \subset \operatorname{im} B$, then L can be designed such that
$$G + BL = 0$$
The problem is reduced to finding the largest controlled invariant subspace without the presence of disturbance.

More general formulation:

* $u \in U$; $x \in \mathcal{X}$,
* $d \in D$,
* $F = \{ x \mid k(x) \geq 0 \}$

not necessarily linear spaces

$$\dot{x} = f(x, u, d)$$ → can be nonlinear

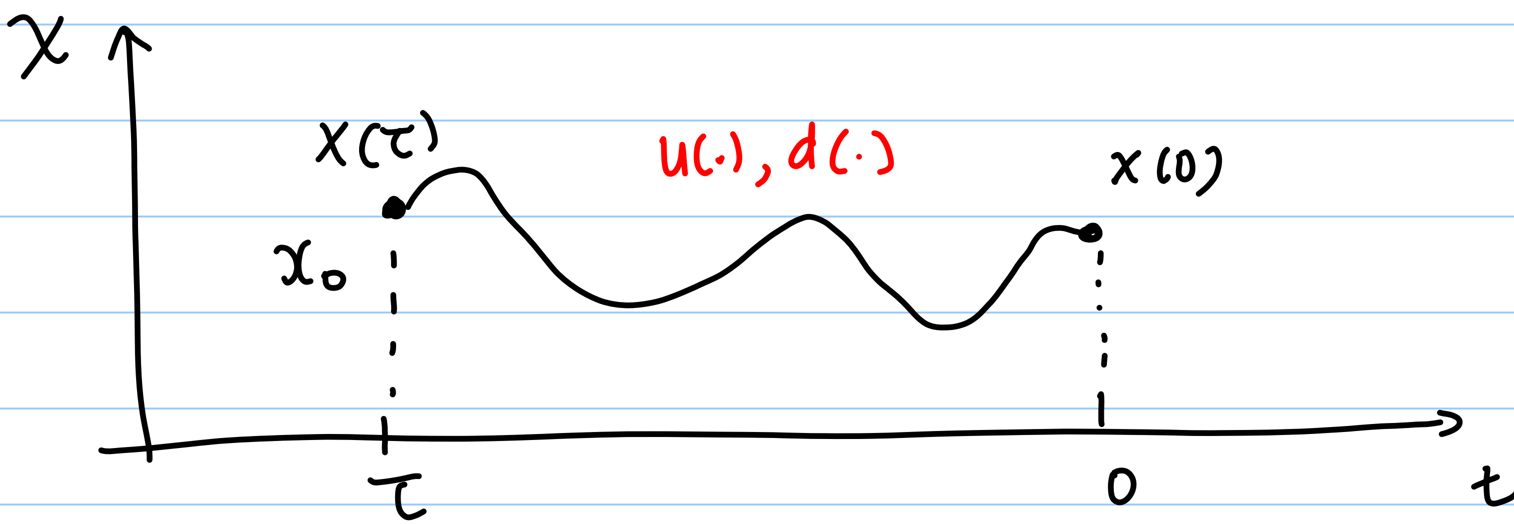
Controller design for safety can be formulated as a dynamic game.

The game: start at a time $\tau \leq 0$ with initial state $x(\tau) = x_0 \in \mathcal{X}$, the cost function is $K(x(0))$.

The input is selected such that $K(x(0))$ is as big as possible

The disturbance wants to make the cost function as small as possible

$$J(x_0, u(\cdot), d(\cdot), \tau) = K(x(0)) \begin{cases} \geq 0, & \text{safe} \\ < 0, & \text{unsafe} \end{cases}$$



The optimal cost function : $J^*(x,\tau) = \max_u \min_d J(x,u,d,\tau)$

Interpretation: $J^*(x_0,\tau) \geq 0$ means starting from $x(\tau) = x_0$, $\tau \leq 0$, the input u can make it such that the end state $x(0)$ is safe, despite of disturbance.

$J^*(x_0,\tau) \geq 0$, $\forall \tau \in [T,0]$, $T<0$, means starting from the initial condition x_0, the input can keep the state safe for at least $|T|$ time unit.

$T \to -\infty$ means the input u can keep the state safe all the time.

The value function can be computed using the Hamilton-Jacobi equation:

$$-\frac{\partial J^*}{\partial t} = H^*\left(x, \frac{\partial J^*}{\partial x}\right)$$

$$H^*\left(x, \frac{\partial J^*}{\partial x}\right) = \max_u \min_d \frac{\partial J^*}{\partial x} \cdot f(x,u,d)$$

$$J^*(x,0) = K(x)$$

$x_0 \in \mathcal{X}$ is always safe if $J^*(x_0, \tau) \geq 0, \forall \tau \leq 0$

An alternative formulation:

$$-\frac{\partial \tilde{J}}{\partial t} = \begin{cases} \min\left\{0, H^*\left(x, \frac{\partial \tilde{J}}{\partial x}\right)\right\} & \text{if } \tilde{J}(x,\tau) \le 0 \\ H^*\left(x, \frac{\partial \tilde{J}}{\partial x}\right), & \text{if } \tilde{J}(x,\tau) > 0 \end{cases}$$

$$H^*\left(x, \frac{\partial \tilde{J}}{\partial x}\right) = \max_u \min_d \frac{\partial \tilde{J}}{\partial x} \cdot f(x,u,d)$$

$$\tilde{J}(x,0) = K(x)$$

As we backward in time, $\tilde{J}$ cannot increase once it is negative.

For every $x \in \mathcal{X}$,

If $\tilde{J}(x,\tau) \le 0$, then $\tilde{J}(x,\tau') \le 0$ for all $\tau' \le \tau$

Interpretation: $\tilde{J}(x_0, \tau) \geq 0$ for $\tau \leq 0$ means starting from the initial condition x_0, the input can keep the state safe for at least $|\tau|$ time unit.

The set of states that are always safe is given by

$$\{x \mid \lim_{t \to -\infty} \tilde{J}(x, t) \geq 0\}$$

Computation : Level set toolbox (Mitchell, Tomlin)

The control input is given by

$$u^* = \arg\max_u \frac{\partial J}{\partial x} \cdot f(x, u, d)$$

Hybrid Systems

$$H = (Q, \mathcal{X}, \Sigma, V, Init, f, Inv, R)$$

Q = discrete state / location, $\mathcal{X}$ = continuous state,

Σ : discrete inputs, $\Sigma = \underbrace{\Sigma_1}_{\text{control input}} \cup \underbrace{\Sigma_2}_{\text{disturbance}}$

V : continuous input, $V = \underbrace{U}_{\text{control}} \cup \underbrace{D}_{\text{disturbance}}$

$Init \subset Q \times \mathcal{X}$ is the set of initial states

$f : Q \times X \times V \to X$ is a vector field describing the continuous dynamics of the system.

$Inv \subseteq Q \times X \times \Sigma \times V$ is the invariant

$R : Q \times X \times \Sigma \times V \to 2^{Q \times X}$ is the reset function.

Assume that the system does not have deadlock :

$$\text{If } (q, x, \sigma, v) \notin Inv \Rightarrow R(q, x, \sigma, v) \neq \emptyset$$

It's always possible to jump when the invariant is violated.

Suppose that the safe set is given as $F \subset Q \times X$, we aim to control the system such that it is always safe.

For any given $K \subset Q \times X$, define the two operators:

$$\begin{aligned} Pre_1(K) = \{ (q,x) \in K \mid\; & \exists (\sigma_1, u) \in \Sigma_1 \times U \text{ such that for all } \\ & (\sigma_2, d) \in \Sigma_2 \times D,\ (q,x,\sigma_1,\sigma_2,u,d) \notin Inv \text{ and } \\ & R(q,x,\sigma_1,\sigma_2,u,d) \subseteq K \} \end{aligned}$$

This is the set of states in K, where the input can force a jump back in K.

$$\mathrm{Pre}_2(K^c) = K^c \cup \{ (q,x) \in K \mid \forall (\sigma_1, u) \in \Sigma_1 \times U, \text{ there exists } (\sigma_2, d) \in \Sigma_2 \times D \text{ such that } R(q, x, \sigma_1, \sigma_2, u, d) \cap K^c \neq \emptyset \}$$

This is the set of states in K from where the disturbance can make the state jump out of K

Introduce the set valued function $\mathrm{Reach}(G, E)$, where

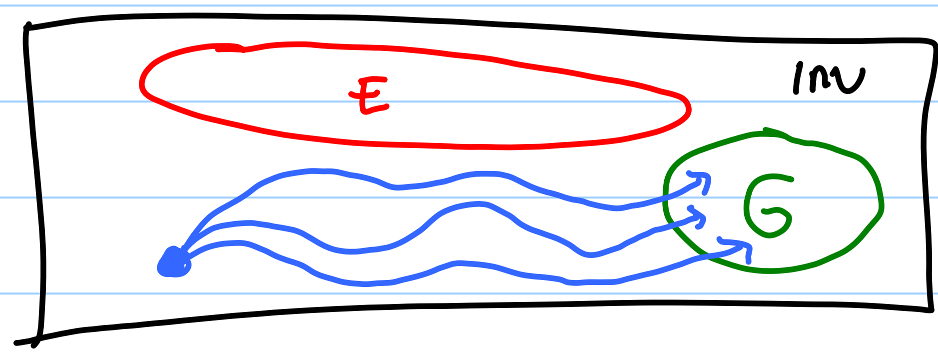
$G \subset Q \times X \rightarrow$ goal states

$E \subset Q \times X \rightarrow$ exit states

$$\mathrm{Reach}(G,E) = \{(q,x) \in Q \times X \mid \forall u, \exists d \text{ and } t \geq 0 \text{ such that } (q(t),x(t)) \in G \text{ and for all } s \in [0,t] \; (q(s),x(s)) \in \Pi(\mathrm{Inv}) \setminus E\}$$

$\Pi(\mathrm{Inv})$ is the state component of Inv.

Reach(G,E) is the set of states from where the disturbance can drive the state to the goal set, without entering the exit set or leaving the invariant.

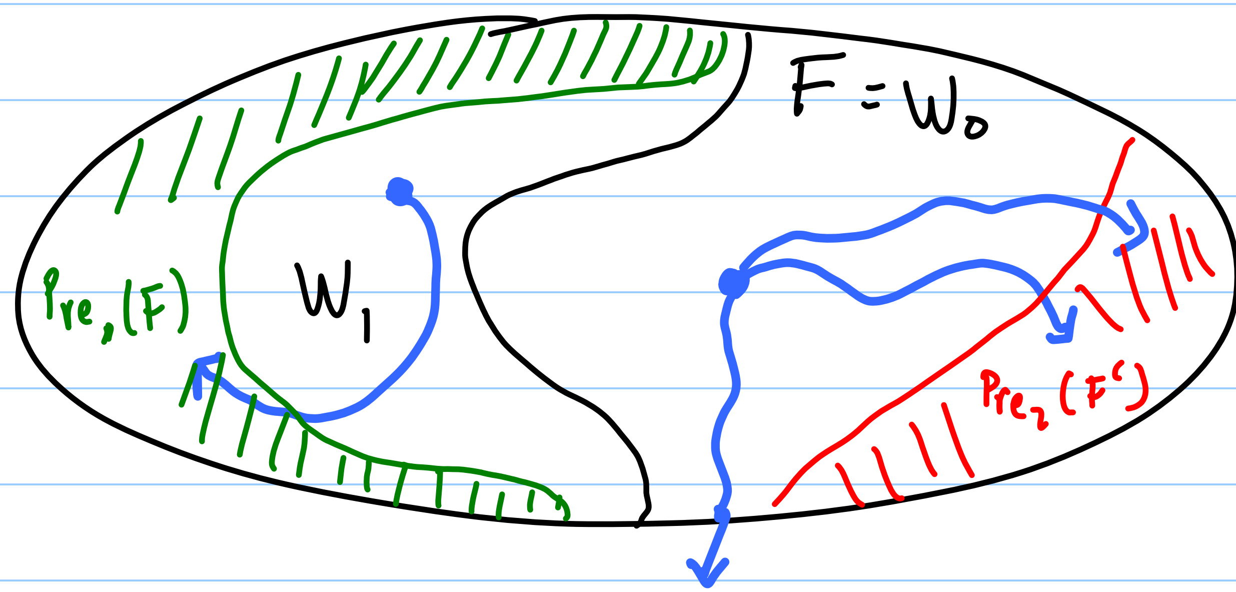


Consider the following iteration:

- $W_0 = F$, $W_1 = \emptyset$, $i = 0$
- While $W_{i+1} \neq W_i$ do
  - $W_{i+1} = W_i \setminus Reach(Pre_2((W_i)^c), Pre_1(W_i))$
  - $i = i+1$

  end while

Look at the first step: $W_0 \setminus W_1$ is the set of states from where the disturbance can drive the state to the unsafe set, or to a state where there can be a jump to the unsafe set, without touching the set where the input can force a safe jump.



Notice that: $W_{i+1} \subset W_i$

The fixpoint of the iteration satisfies:

$$W = W \setminus \mathrm{Reach}(\mathrm{Pre}_2(W^c), \mathrm{Pre}_1(W))$$

$$W \cap \mathrm{Reach}(\mathrm{Pre}_2(W^c), \mathrm{Pre}_1(W)) = \emptyset$$

Starting from W, the disturbance cannot win by driving the state out of W.

W is controlled invariant!

In fact, W is the largest controlled invariant set contained in F.

Computation of $\mathrm{Reach}(G, E)$ can be done a la dynamic game theory, with Hamilton-Jacobi equations

The computation is done per location.

Suppose that
$$\left.\begin{aligned} G_q &= \{x \in \mathcal{X} \mid \ell_G^q(x) \leq 0\} \\ E_q &= \{x \in \mathcal{X} \mid \ell_E^q(x) \leq 0\} \end{aligned}\right| \quad \forall q \in Q$$

Formulate the Hamilton-Jacobi equations

$$-\frac{\partial J_G^*}{\partial t} = \begin{cases} H_G^*\left(x, \frac{\partial J_G^*}{\partial x}\right), & J_G^*(x,t) > 0 \\ \min\left(0, H_G^*\left(x, \frac{\partial J_G^*}{\partial x}\right)\right), & \text{otherwise} \end{cases}$$

$$-\frac{\partial J_E^*}{\partial t} = \begin{cases} H_E^*\left(x, \frac{\partial J_E^*}{\partial x}\right), & J_E^*(x,t) > 0 \\ \min\left(0, H_E^*\left(x, \frac{\partial J_E^*}{\partial x}\right)\right), & \text{otherwise} \end{cases}$$

Initial condition: $J_G^*(x,0) = l_G^q(x)$; $J_E^*(x,0) = l_E^q(x)$

$$H_G^*\left(x, \frac{\partial J_G^*}{\partial x}\right) = \begin{cases} 0, \text{ if } J_E^*(x,t) \leq 0 & (*) \\ \max\limits_{u} \min\limits_{d} \dfrac{\partial J_G^*}{\partial x} \cdot f(x,u,d) & \text{otherwise} \end{cases}$$

$$H_E^*\left(x, \frac{\partial J_E^*}{\partial x}\right) = \begin{cases} 0, \text{ if } J_G^*(x,t) \leq 0 & (**) \\ \min\limits_{u} \max\limits_{d} \dfrac{\partial J_E^*}{\partial x} \cdot f(x,u,d) & \text{otherwise} \end{cases}$$

We formulate the problem as 2 games:
J_G^* is for the game where the disturbance tries to drive the state to G

J_G^* is for the game where the input tries to drive the state to E.

(*) and (**) mean : once the game is won by one side, the computation of the cost function is stopped (locally).

Reach(G, E) is then given by $\{x \mid \lim_{t \to -\infty} J_G^*(x,t) < 0\}$

The computation is done for every location.

The control input is then determined by:

In the interior of W (the largest controlled invariant set):

$(\sigma_1, u) \in \Sigma_1 \times U$ s.t. $\forall (\sigma_2, d) \in \Sigma_2 \times D$,

$$\boxed{R(q, x, \sigma_1, \sigma_2, v, d) \subset W}$$

At the boundary of W:

$(\sigma_1, u) \in \Sigma_1 \times U$ s.t. $\forall (\sigma_2, d) \in \Sigma_2 \times D$,

$$\frac{\partial J_G^*}{\partial x} f(q, x, u, d) \geq 0 \wedge (q, x, \sigma_1, \sigma_2, u, d) \in Inv \quad \text{or}$$

$$R(q, x, \sigma_1, \sigma_2, u, d) \subset W \wedge (q, x, \sigma_1, \sigma_2, u, d) \notin Inv.$$