EE C222/ME C237 - Spring'18 - Lecture 15 Notes[1]

Murat Arcak

March 12 2018

Reachable Sets and Safety Certification

Reachable sets with unit peak inputs

$$\boxed{R_T \triangleq \{x(T) \mid \dot{x} = f(x,u),\ x(0) = 0,\ |u| \le 1\}} \tag{1}$$

The set of points that can be reached from $x(0) = 0$ with inputs not exceeding unit magnitude. Difficult to find exactly, but methods exist to find overapproximations.

ISS gives a very conservative bound:

$$|x(T)| \le \underbrace{\beta(|x(0)|, T)}_{=0} + \gamma\left(\sup_{0\le t\le T} \underbrace{|u(t)|}_{\le 1}\right) \le \gamma(1).$$

A less conservative estimate with level sets:

Find positive definite $V(\cdot)$ and a constant $c > 0$ such that

$$|u| \le 1 \quad \text{and} \quad V(x) \ge c \quad \Rightarrow \quad \nabla V(x) \cdot f(x,u) \le 0.$$

Then, the level set $\Omega_c \triangleq \{x : V(x) \le c\}$ contains the reachable set:

$$R_T \subset \Omega_c \quad \forall T \ge 0.$$

<u>Example:</u> Linear system $\dot{x} = Ax + Bu$. Use $V(x) = x^T P x$. If there exists $P = P^T > 0$ such that

$$\boxed{u^T u \le 1 \text{ and } x^T P x \ge 1 \quad \Rightarrow \quad x^T(A^T P + PA)x + x^T PBu + u^T B^T P x \le 0}$$

then the ellipsoid $\{x : x^T P x \le 1\}$ is an overapproximation of R_T.

Rewrite the above implication as:

$$\left\{ \begin{bmatrix} x \\ u \end{bmatrix}^T \begin{bmatrix} 0 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix} + 1 \ge 0 \right\} \wedge \left\{ \begin{bmatrix} x \\ u \end{bmatrix}^T \begin{bmatrix} P & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix} - 1 \ge 0 \right\}$$

$$\Longrightarrow \begin{bmatrix} x \\ u \end{bmatrix}^T \begin{bmatrix} A^T P + PA & PB \\ B^T P & 0 \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix} \le 0.$$

Note that this statement is verified if we can find $\alpha \ge 0$, $\beta \ge 0$ such that, for all x and u,

$$\begin{bmatrix} x \\ u \end{bmatrix}^T \begin{bmatrix} A^TP + PA & PB \\ B^TP & 0 \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix} + \alpha \left(\begin{bmatrix} x \\ u \end{bmatrix}^T \begin{bmatrix} P & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix} - 1 \right)$$
$$+\beta \left(\begin{bmatrix} x \\ u \end{bmatrix}^T \begin{bmatrix} 0 & 0 \\ 0 & -I \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix} + 1 \right) \leq 0 \qquad (2)$$

or, equivalently:

$$\begin{bmatrix} x \\ u \end{bmatrix}^T \begin{bmatrix} A^TP + PA + \alpha P & PB \\ B^TP & -\beta I \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix} \leq \alpha - \beta.$$

This inequality holds for all x and u if and only if

$$\begin{bmatrix} A^TP + PA + \alpha P & PB \\ B^TP & -\beta I \end{bmatrix} \leq 0 \qquad (3)$$
$$\beta - \alpha \leq 0. \qquad (4)$$

Let $\beta = \alpha$ which is the best choice to satisfy (3) without violating (4):

$$\begin{bmatrix} A^TP + PA + \alpha P & PB \\ B^TP & -\alpha I \end{bmatrix} \leq 0. \qquad (5)$$

Summary: procedure to overapproximate the reachable set

Look for $P = P^T > 0$ and $\alpha > 0$ satisfying the matrix inequality (5). This in not a linear matrix inequality (LMI) in α and P, but it is an LMI in P if α is fixed. The resulting ellipsoid $\{x : x^TPx \leq 1\}$ is a superset of R_T.

Additional objectives can be incorporated, such as minimizing the volume of the ellipsoid, which is proportional to $\sqrt{\det P^{-1}}$:

$$\text{minimize} \log(\det P^{-1}) \text{ which is convex in } P.$$

S-procedure

The principle used to obtain (2) is known as the S-procedure in control theory. To show that:

$$q_0(\xi) \geq 0 \quad \text{whenever} \quad q_i(\xi) \geq 0 \quad i = 1, 2, \ldots, p$$

look for $\tau_1, \tau_2, \ldots, \tau_p \geq 0$ such that

$$q_0(\xi) - \sum_{i=1}^{p} \tau_i q_i(\xi) \geq 0.$$

In (2), $q_i(\cdot)$, $i = 0, 1, 2$, are quadratic functions of $\xi = \begin{bmatrix} x \\ u \end{bmatrix}$.

Reachable sets with unit energy inputs

$$\boxed{R_T \triangleq \{x(T) \mid \dot{x} = f(x,u),\ x(0) = 0,\ \int_0^T u^T(t)u(t)dt \leq 1\}} \qquad (6)$$

For an overapproximation, find positive definite $V(\cdot)$ such that

$$\nabla V(x) \cdot f(x,u) \leq u^T u.$$

$$\frac{d}{dt}V(x(t)) \leq u^T u \ \Rightarrow\ V(x(T)) - V(x(0)) \leq \int_0^T u^T(t)u(t)dt \leq 1$$
$$\Rightarrow\ V(x(T)) \leq 1.$$

Therefore, $x \in R_T$ implies $V(x) \leq 1$, *i.e.*, the level set contains the reachable set:

$$R_T \subset \{x : V(x) \leq 1\}.$$

Example:

$$\dot{x} = Ax + Bu \quad V(x) = x^T P x.$$

Find $P = P^T > 0$ such that

$$x^T(A^T P + PA)x + x^T PBu + u^T B^T Px \leq u^T u$$

or, written more compactly:

$$\begin{bmatrix} x \\ u \end{bmatrix}^T \begin{bmatrix} A^T P + PA & PB \\ B^T P & 0 \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix} \leq \begin{bmatrix} x \\ u \end{bmatrix}^T \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} \begin{bmatrix} x \\ u \end{bmatrix}.$$

This means

$$\begin{bmatrix} A^T P + PA & PB \\ B^T P & -I \end{bmatrix} \leq 0$$

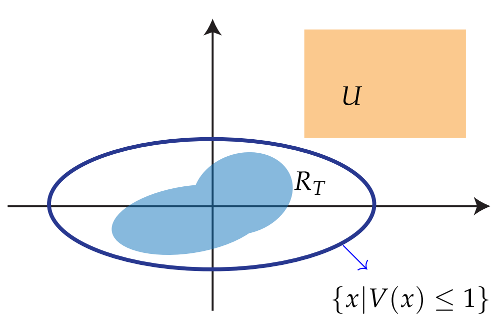
which is a LMI in P.

Safety Certification

Given an "unsafe" set U, show that

$$R_T \cap U = \emptyset.$$

The level set overapproximations above can be used to prove safety:



Look for a V with the additional property that $x \in U \Rightarrow V(x) > 1$. Such functions V are sometimes called "barrier functions."

Example: Suppose the unsafe set is the half-space:

$$U = \{x : a^T x > 1\}.$$

Let $V(x) = x^T P x$. From the S-procedure, if there exists $\tau > 0$ such that

$$(x^T P x - 1) - \tau(a^T x - 1) \geq 0, \tag{7}$$

then $x \in U \Rightarrow V(x) > 1$.

Exercise: Show that (7) is equivalent to: $P \geq aa^T$.

Thus, the LMIs in the previous examples can be augmented with this additional constraint to certify safety.