Safety filtering

(1) least restrictive safety filtering

$$u^*(x) = \begin{cases} u_{nom}(x) & \text{if } V^*(x) > 0 \\ u^*_{safe}(x) & \text{if } V^*(x) \leq 0 \end{cases}$$

(2) QP-based safety filtering

$$u^*(x) = \underset{u}{\operatorname{argmin}} \; \| u - u_{nom} \|_2^2$$

$$\text{s.t. } u \in U_{safe}$$

$$\Updownarrow$$

$$V^*(x(t+\delta)) \geq 0$$

} remain as close to u_{nom} as possible w/o violating safety

$$U_{safe} = \{ u : V^*(x(t+\delta)) \geq 0 \}$$

$$V^*(x(t+\delta)) = V^*(x) + \frac{\partial V^*}{\partial x}(x(t+\delta) - x(t))$$

$$= V^*(x) + \frac{\partial V^*}{\partial x} f(x,u) \cdot \delta$$

For control affine systems,

$$f(x,u) = f_1(x) + f_2(x)u$$

$$u^*(x) = \underset{u}{\operatorname{argmin}} \; \| u - u_{nom} \|_2^2$$

$$\text{s.t. } V^*(x) + \frac{\partial V^*}{\partial x} f_1(x)\delta + \left(\frac{\partial V^*}{\partial x} \cdot f_2(x)\delta\right) u \geq 0$$

$$\equiv Au + b \geq 0$$

$$A = \frac{\partial V^*}{\partial x} \cdot f_2(x)\delta$$

$$b = V^*(x) + \frac{\partial V^*}{\partial x} \cdot f_1(x)\delta$$

Ex. longitudinal quadrotor

$$f(x) = \begin{bmatrix} v \\ g \end{bmatrix} + \begin{bmatrix} 0 \\ k \end{bmatrix} u \qquad \frac{\partial V^*}{\partial x} = \begin{bmatrix} P_1(x) & P_2(x) \end{bmatrix}$$

$$A = \delta \begin{bmatrix} P_1(x) & P_2(x) \end{bmatrix} \begin{bmatrix} 0 \\ k \end{bmatrix} = \delta P_2(x) k$$

$$b = V^*(x) + \delta \begin{bmatrix} P_1(x) & P_2(x) \end{bmatrix} \begin{bmatrix} v \\ g \end{bmatrix}$$

$$= V^*(x) + \delta P_1(x) v + \delta P_2(x) g$$

$$u^*(x) = \underset{u}{\arg\min} \|u - u_{nom}\|_2^2$$

$$\text{s.t. } Au + b \geq 0$$

Ex. planar vehicle

$$f(x) = \begin{bmatrix} v\cos\theta \\ v\sin\theta \\ \omega \end{bmatrix} = \begin{bmatrix} v\cos\theta \\ v\sin\theta \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \omega$$

$$A = P_3(x)\delta$$

$$b = V^*(x) + \delta P_1(x) \cdot v\cos\theta + \delta P_2(x) \cdot v\sin\theta$$

$$f(x,u) = u^2$$

$$V^*(x(t+\delta)) \approx V^*(x) + \delta \cdot \frac{\partial V^*}{\partial x} \cdot u^2$$

QCQP - Quadratic constraint QP

$$\min_u J(x,u)$$

s.t. dynamics

$x_t \notin obs$

$$u^*_{safe}(x) = \arg\max_u \left(\min_d \frac{\partial V^*}{\partial x} \cdot f(x,u,d) \right)$$

control and disturbance affine dynamics:

$$f(x,u,d) = f_1(x) + f_2(x)u + f_3(x)d$$

$$\frac{\partial V^*}{\partial x} \cdot f(x,u,d) = \frac{\partial V^*}{\partial x} \cdot f_1(x) + \frac{\partial V^*}{\partial x} \cdot f_2(x)\, u + \frac{\partial V^*}{\partial x} \cdot f_3(x)\, d$$

$$u^*_{safe}(x) = \arg\max_u \frac{\partial V^*}{\partial x} \cdot f_2(x)\, u$$

Ex. $\dot{z} = v$ $\quad |u| \leq \bar{u}$

$\dot{v} = ku + g + d$ $\quad |d| \leq \bar{d}$

$$f(x,u,d) = \underbrace{\begin{bmatrix} v \\ g \end{bmatrix}}_{f_1(x)} + \underbrace{\begin{bmatrix} 0 \\ k \end{bmatrix}}_{f_2(x)} u + \underbrace{\begin{bmatrix} 0 \\ 1 \end{bmatrix}}_{f_3(x)} d$$

$$\frac{\partial V^*}{\partial x} = [\, P_1(x) \quad P_2(x) \,]$$

$$u^*_{safe}(x) = \arg\max_u \min_d \left([P_1(x)\ P_2(x)] \left(\begin{bmatrix} v \\ g \end{bmatrix} + \begin{bmatrix} 0 \\ k \end{bmatrix} u + \begin{bmatrix} 0 \\ 1 \end{bmatrix} d \right) \right)$$

$$= \arg\max_u \left(P_1(x) v + P_2(x) g + P_2(x) k u + \min_d P_2(x) d \right)$$

$$= \arg\max_u P_2(x) k u = \begin{cases} \bar{u} & \text{if } P_2(x) > 0 \\ -\bar{u} & \text{if } P_2(x) \leq 0 \end{cases}$$

Add disturbance

$$u^*(x) = \arg\min_u \| u - u_{nom} \|_2^2$$

$$\text{s.t.} \quad \min_d V^*(x(t+\delta)) \geq 0$$

$$\equiv \underbrace{V^*(x) + \delta \frac{\partial V^*}{\partial x} f_1(x) + \delta \frac{\partial V^*}{\partial x} f_2(x) u + \min_d \delta \frac{\partial V^*}{\partial x} f_3(x) d}_{Au + b \geq 0} \geq 0$$

$$A = \delta \frac{\partial V^*}{\partial x} \cdot f_2(x)$$

$$b = V^*(x) + \delta \frac{\partial V^*}{\partial x} f_1(x) + \min_d \delta \frac{\partial V^*}{\partial x} \cdot f_3(x) \cdot d$$

Ex. continued

$$A = \delta \frac{\partial V^*}{\partial x} \cdot f_2(x) = \delta P_2(x) k$$

$$b = V^*(x) + \delta P_1(x) v + \delta P_2(x) g + \min_d \delta P_2(x) d$$

$$\min_d \delta P_2(x) d = \begin{cases} \delta P_2(x) \bar{d} & \text{if } P_2(x) < 0 \\ -\delta P_2(x) \bar{d} & \text{if } P_2(x) \geq 0 \end{cases}$$

Pros	Cons
- "certified" safety guarantees	- not necessarily optimal performance
- can be used in real time	- could be hard to use on non-control affine systems
- irrespective of the nominal planner, we can ensure safety	- need to know the failure set beforehand