CHAPTER 5

Safety-Critical System

In this chapter, we revisit preliminaries for safety based on Control Barrier Functions (CBFs) and provide solutions to **Problem 3**, **4**, and **5** with the papers proposed by this thesis [4][5][6].

5.1 Preliminaries

Set Invariance

The core concept of set invariance [83] is to ensure that the state of a system is contained in a desired set at all times; thus set invariance is one promising way to design safe controllers or filters. Consider the following nonlinear control system:

$$\dot{x} = f(x), \tag{5.1}$$

where $x \in \mathcal{X} \subset \mathbb{R}^n$ is the system state. And we assume that f is a continuously differentiable function. Then, the following definition of set invariance is constructed [84]:

Definition 1. Let $\mathcal{S} \subset \mathcal{X}$. Then, $\mathcal{S}$ is forward invariant for the system (5.1) if for any $x(0) \in \mathcal{S}$, there exists $x(t) \in \mathcal{S}$ for all $t \geq 0$.

Furthermore, we define set invariance in terms of the control input, $u(t) \in \mathcal{U} \subset \mathbb{R}^m$ as follows:

Definition 2. Let $\mathcal{S} \subset \mathcal{X}$. Then $\mathcal{S}$ is control invariant for the system (5.1) if for any $x(0) \in \mathcal{S}$, there exists a point-wise continuous control input signal $u(t) \in \mathcal{U}$ such that $x(t) \in \mathcal{S}$ for all $t \geq 0$.

From **Definition 1**, the first and simple switching safety filter is established based on *Nagumo's Theorem*. Consider the following closed-loop system with a feedback controller:

$$\dot{x} = f(x, u_f), \tag{5.2}$$

where $u_f : \mathcal{X} \rightarrow \mathcal{U}$ is the feedback controller, and a set $\mathcal{S}$ is defined as the zero superlevel set of a continuously differentiable function $h : \mathcal{X} \rightarrow \mathbb{R}$ as:

$$\mathcal{S} = \{x \in \mathbb{R}^n \mid h(x) \geq 0\} \tag{5.3}$$
$$\text{Int}(\mathcal{S}) = \{x \in \mathbb{R}^n \mid h(x) > 0\} \tag{5.4}$$
$$\partial\mathcal{S} = \{x \in \mathbb{R}^n \mid h(x) = 0\}. \tag{5.5}$$

Theorem 1 (*Nagumo's Theorem*)**.** Consider the system (5.2) and a set $\mathcal{S}$ from (5.3) with $\text{Int}(\mathcal{S}) \neq \emptyset$ and a continuously differentiable function h satisfying $\frac{\partial h(x)}{\partial x} \neq 0$. Then $\mathcal{S}$ is forward invariant for the system (5.2) if and only if

$$\dot{h}(x) = \frac{\partial h}{\partial x} f(x, u_f(x)) \geq 0, \quad \forall x \in \partial\mathcal{S}. \tag{5.6}$$

From (5.6), the following switching control scheme is obtained:

$$u_{\text{safe}} = \begin{cases} u_f(x), & x \in \partial\mathcal{S} \text{ or } u_{\text{nominal}} \notin \mathcal{U} \\ u_{\text{nominal}}, & \text{otherwise}, \end{cases} \tag{5.7}$$

where $u_{\text{safe}} : \mathcal{X} \rightarrow \mathcal{U}$, and $u_{\text{nominal}} : \mathcal{X} \rightarrow \mathcal{U}$ is the nominal control input. Instead of switching the control input signal at the boundary of the set, $\mathcal{S}$, the desired control input can be smoothly corrected as the system state approaches the boundary by using Barrier Function [84] defined as:

Definition 3. Consider the following control affine system:

$$\dot{x} = f(x) + g(x)u, \tag{5.8}$$

and let a set $\mathcal{S} \subset \mathcal{X}$ be the zero superlevel set of a continuously differentiable function $h : \mathcal{X} \rightarrow \mathbb{R}$. Then, h is a *Barrier Function* (BF) on $\mathcal{S}$ if there exists an extended class $\mathcal{K}_\infty$ function, α and a feedback controller $k : \mathcal{X} \rightarrow \mathcal{U}$ such that for all $x \in \mathcal{S}$:

$$\dot{h} = \frac{\partial h}{\partial x}(f(x) + g(x)k(x)) \geq -\alpha(h(x)). \tag{5.9}$$

And a BF can be leveraged to ensure set variance based on the following theorem:

Theorem 2 ([85])**.** If h is a BF for the system (5.8) on $\mathcal{S}$, then $\mathcal{S}$ is forward invariant for (5.8).

Control Barrier Function

To synthesize a safe controller with a convex optimization problem in an efficient way, the following *Control Barrier Function* (CBF) is defined:

Definition 4. A continuously differentiable function $h : \mathcal{X} \to \mathbb{R}$ is a *Control Barrier Function* for the system (5.8) on the set, $\mathcal{S}$, if there exists an extended class $\mathcal{K}_\infty$ function α such that for all $x \in \mathcal{S}$:

$$\sup_{u \in \mathcal{U}} \left[\frac{\partial h}{\partial x}(f(x) + g(x)u) \right] \geq -\alpha(h(x)). \tag{5.10}$$

Then the following theorem is obtained:

Theorem 3 ([47])**.** If h is a CBF for the system (5.8), any locally Lipschitz continuous controller u_{safe} satisfying

$$u_{\mathsf{safe}}(x) \in \left\{ u \in \mathcal{U} \;\middle|\; \frac{\partial h}{\partial x}(f(x) + g(x)u) \geq -\alpha(h(x)) \right\}, \tag{5.11}$$

makes $\mathcal{S}$ forward invariant and thus u_{safe} renders the system (5.8) safe.

The concept of CBF (5.10) has the following benefits. First, using an extended class $\mathcal{K}_\infty$ function allows for reducing the conservatism of the original CBF-based controller [86]. Secondly, Theorem 3 is easily implemented through a convex optimization problem such as quadratic programming, which leads to the increase of scalability of the method. For example, the synthesizing with a nominal control input in minimally invasive way can be formulated [87] as:

$$\begin{aligned} u_{\mathsf{safe}} = \quad & \min_{u \in \mathcal{U}} \frac{1}{2}||u - u_{\mathsf{nominal}}||^2 \quad \textbf{(CBF-QP)} \\ \text{s.t.}\ & \frac{\partial h}{\partial x}(f(x) + g(x)u) \geq -\alpha(h(x)). \end{aligned}$$

Example 1. In this example, a simple safe contact force controller designed with CBF is presented. Consider the following system based on Kelvin-Voigt contact model [88]:

$$\begin{aligned} F &= F_{\mathrm{c}} + u \\ M\ddot{x} &= -D\dot{x} - Kx + u \end{aligned} \tag{5.12}$$

where F is the sum of all forces applied to the mass, F_{c} is the contact force, u is the control input, and $\ddot{x}, \dot{x}, x$ are acceleration, velocity and position, respectively, and $M > 0, D > 0, K > 0$ are the parameters of mass, damper and spring respectively. The system (5.12) is rewritten as the control affine form of (5.8):

$$\begin{bmatrix} \dot{x} \\ \ddot{x} \end{bmatrix} = \underbrace{\begin{bmatrix} \dot{x} \\ \frac{1}{M}(-D\dot{x} - Kx) \end{bmatrix}}_{f(x)} + \underbrace{\begin{bmatrix} 0 \\ \frac{1}{M} \end{bmatrix}}_{g(x)} u. \tag{5.13}$$

The structure of a safe contact force controller is shown in Figure 5.1. There exists a nominal feedback controller (e.g. P or an admittance controller) to track the desired force F_{d} when given

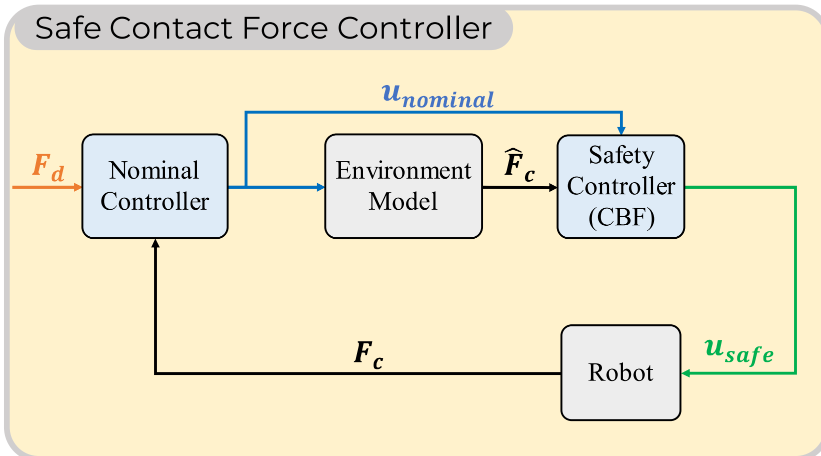


FIGURE 5.1 Illustration of a safe contact force controller.

the current contact force F_c, and the environment contact model is defined from (5.12). The contact model provides the estimated contact force, $\hat{F}_c$ and is used to calculate Lie derivatives with h in the safety controller based on CBF. Then, the CBF-based controller generates a safe control input signal, u_{safe} while minimizing the deviation from the nominal control input. As a result, the safety controller alters the nominal control output to enforce safety constraints. The following presents how the safety controller based on CBF is designed. The condition that the contact force controller should satisfy is formulated as:

$$F_c \geq F_{\min}, \tag{5.14}$$

where the contact force should be greater than the minimum contact force. Then, the candidate barrier function $h(x)$ is chosen as:

$$h(x) = F_c - F_{\min} = -D\dot{x} - Kx - F_{\min}. \tag{5.15}$$

And then the safety condition from (5.11) is formulated with the contact model (5.12) as:

$$\begin{aligned} L_f h(x) + L_g h(x)u &\geq -\alpha(h(x)), \\ L_f h(x) &= \begin{bmatrix} -K & -D \end{bmatrix} \begin{bmatrix} \dot{x} \\ \frac{1}{M}(-D\dot{x} - Kx) \end{bmatrix} = -K\dot{x} - \frac{D}{M}(-D\dot{x} - Kx), \\ L_g h(x)u &= \begin{bmatrix} -K & -D \end{bmatrix} \begin{bmatrix} 0 \\ \frac{1}{M} \end{bmatrix} u = -\frac{D}{M}u. \end{aligned} \tag{5.16}$$

The following quadratic programming generates a safe control input signal that satisfies (5.11):

$$u_{\text{safe}} = \min_{u \in \mathcal{U}} \quad \frac{1}{2}||u - u_{\text{nominal}}||^2 \quad \textbf{(CBF-QP)} \tag{5.17}$$
$$\text{s.t. } L_f h(x) + L_g h(x) u \geq -\alpha(h(x))$$

For practical implementation, the constraint (5.16) is rewritten with the form, $Au \leq b$ as:

$$-K\dot{x} - \frac{D}{M}(-D\dot{x} - Kx) - \frac{D}{M}u + \alpha(h(x)) \geq 0$$
$$\underbrace{\frac{D}{M}}_{A} u \leq \underbrace{-K\dot{x} - \frac{D}{M}(-D\dot{x} - Kx) + \alpha(h(x))}_{b}. \tag{5.18}$$

Figure 5.2 shows the simulation results of the CBF-based contact force controller. As shown in Figure 5.2.(A), P controller is used as the nominal controller to track the desired force profile. And the safety limit is set to $-8.5N$ in this scenario. CBF-based controller with (5.17) ensures the safety guarantees from (5.14), which satisfies $h \geq 0$ for all times as shown in Figure 5.2.(B).

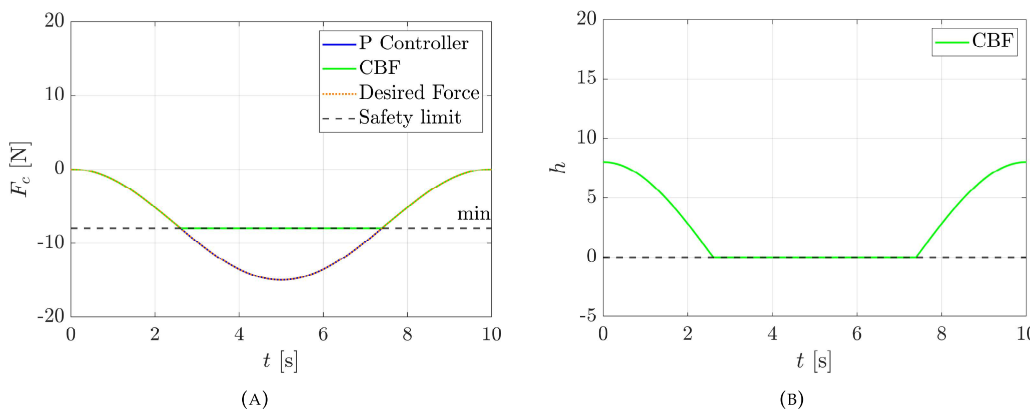


FIGURE 5.2 Simulation results of a safe contact force controller based on CBF. (A) Contact force and (B) h function.

Model Uncertainty

Inherent model uncertainty deteriorates the performance of the CBF-based controller, which is a common challenge in CBF-based schemes since the uncertainty causes a discrepancy between the true Lie derivative, $\dot{h}$ and the estimated one, and this prevents the controllers from satisfying the forward invariant condition (5.10). Adaptive and robust techniques are required to ensure safety guarantees when uncertainty is present. This can be done in the two following ways: Adaptive Control Barrier Function and Robust adaptive Control Barrier Function.

Adaptive Control Barrier Functions

To reduce the model uncertainty, we introduce a parametric model structure that is linear with respect to the parameters in the system. Consider the following control affine system that includes parametric uncertainty:

$$\dot{x} = f(x) + F(x)\theta^* + g(x)u \tag{5.19}$$

where $\theta^* \in \Theta \subset \mathbb{R}^k$ is an unknown parameter, and $F : \mathcal{X} \to \mathbb{R}^{m\times k}$ is smooth on $\mathcal{X}$ and $F(0) = 0$. To estimate θ^* adaptively and achieve the safety guarantees, the following adaptive controller with update rule is used:

$$\begin{bmatrix} \dot{x} \\ \dot{\hat{\theta}} \end{bmatrix} = \begin{bmatrix} f(x) + F(x)\theta^* + g(x)u \\ \Gamma\tau(x, \hat{\theta}) \end{bmatrix} \tag{5.20}$$

where $\hat{\theta} \in \Theta$ is the estimated parameter, and τ is an update law that is locally Lipschitz continous on $\mathcal{X} \times \Theta$. In terms of the safety, the parameterized safe set is defined as:

$$\mathcal{S}_\theta \triangleq \{x \in \mathcal{X} \mid h_a(x, \theta) \geq 0\} \tag{5.21}$$

with 0-superlevel set of a continuously differentiable function $h_a : \mathcal{X} \times \Theta \to \mathbb{R}$. Then, an adaptive control barrier function can be defined as follows [57]:

Definition 5. Let $\mathcal{S}_\theta$ be 0-superlevel set of a continuously differentiable function $h_a : \mathcal{X} \times \Theta \to \mathbb{R}$ where $\frac{\partial h_a}{\partial x}$ is Lipschitz continuous. Then, h_a is an *adaptive Control Barrier Function* (aCBF) on $\mathcal{S}_\theta$ for the system (5.19), for any $\theta \in \Theta$, and for all $x \in \mathcal{S}_\theta$:

$$\sup_{u\in\mathcal{U}} \left[\frac{\partial h_a}{\partial x}(x, \theta)\Big(\mathcal{F}_{cbf}(x, \theta) + g(x)u\Big)\right] \geq 0 \tag{5.22}$$

with

$$\mathcal{F}_{cbf}(x, \theta) = f(x) + F(x)\lambda_{cbf}(x, \theta), \quad \lambda_{cbf}(x, \theta) \triangleq \theta - \Gamma\left(\frac{\partial h_a}{\partial \theta}(x, \theta)\right)^\top,$$

where $\Gamma \in \mathbb{R}^{k\times k}$ is a symmetric and positive-definite adaptive gain.

The existence of an aCBF implies adaptively safety to the unknown parameters in the system; thus, the safety is achieved with the following theorem [57]:

Theorem 4. Let h_a be an adaptive control barrier function on $\mathcal{S}_\theta$ and assume that the initial estimate error, $\theta^* - \hat{\theta}(0)$ is bounded as $||\theta^* - \hat{\theta}(0)||_2 \leq c, c > 0$ and $x(0) \in \mathcal{S}_\theta$. If there exists a positive definite adaptive gain satisfying:

$$\lambda_{\text{min}}(\Gamma) \geq \frac{c^2}{2h_a(x(0), \hat{\theta}(0))}, \tag{5.23}$$

and an update law:

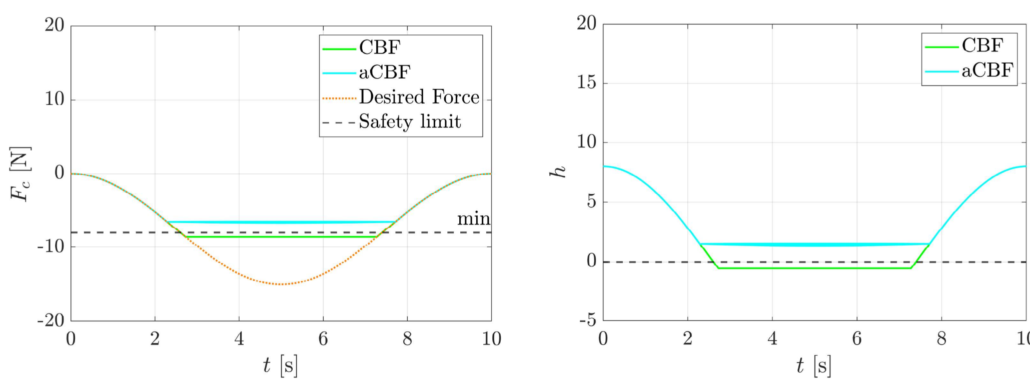
$$\tau(x,\hat{\theta}) = -\left(\frac{\partial h_a}{\partial x}(x,\hat{\theta})F(x)\right)^{\top}, \tag{5.24}$$

then any locally Lipschitz continuous controller satisfying (5.22) makes $\mathcal{S}_\theta$ forward invariant, i.e. the system is adaptively safe.

Similar to (5.17), the control input that renders the system safe is generated based on a QP formulation [57] as:

$$\begin{aligned} u_{\mathsf{safe}} = \quad & \min_{u\in\mathcal{U}} \frac{1}{2}||u-u_{\mathsf{nominal}}||^2 \quad \textbf{(aCBF-QP)} \\ \text{s.t. } & \frac{\partial h_a}{\partial x}(x,\hat{\theta})\left(\mathcal{F}_{cbf}(x,\hat{\theta})+g(x)u\right) \geq 0. \end{aligned} \tag{5.25}$$

The QP formulation, (5.25) is applied to the same safe contact force controller design scenario, but we introduce model uncertainty on K, D in (5.13). As shown in Figure 5.3.(A), aCBF adapts to the parametric uncertainty while CBF violates the safety limit. However, aCBF shows the conservative performance and chattering behavior on the boundary of the safe set due to the strict safety condition from (5.22), which is confirmed with h function as shown in Figure 5.3.(B).



(A) (B)

FIGURE 5.3 Simulation results of aCBF and CBF. (A) Contact forces and (B) h functions of each controller.

Robust Adaptive Control Barrier Function

Due to the stricter condition of aCBF (5.22) than (5.10), the state stays more inside of the safe set, which leads to more conservative behavior of the designed controller as we showed in the previous simulation. To remedy this, Robust adaptive Control Barrier Function (RaCBF) [58] is proposed to tighten the subset, $\mathcal{S}_\theta$ by introducing a maximum possible error, and the tightened safety subset is defined as:

$$\mathcal{S}_\theta^r = \left\{ x \in \mathcal{X} : h_r(x,\theta) \geq \frac{1}{2}\tilde{\vartheta}^\top \Gamma^{-1} \tilde{\vartheta} \right\}, \tag{5.26}$$

where $\mathcal{S}_\theta^r \subset \mathcal{S}_\theta$ is the tightened set, and $\tilde{\vartheta} \in \mathbb{R}^k$ is the maximum possible element-wise error between θ^* and $\hat{\theta}$. Then, the following definition allows h_r to establish a robust aCBF [58]:

Definition 6. Let $\mathcal{S}_\theta^r$ be a superlevel set of a continuously differentiable function $h_r : \mathcal{X} \times \Theta \to \mathbb{R}$. Then, h_r is a *Robust adaptive Control Barrier Function* (RaCBF) if there exists an extended class $\mathcal{K}_\infty$ function α such that for the system (5.20), any $\theta \in \Theta$, and for all $x \in \mathcal{S}_\theta^r$:

$$\sup_{u \in \mathcal{U}} \left[\frac{\partial h_r}{\partial x}(x,\theta)\Big(\mathcal{F}_{racbf}(x,\theta) + g(x)u\Big)\right] \geq -\alpha\left(h_r(x,\theta) - \frac{1}{2}\tilde{\vartheta}^\top \Gamma^{-1}\tilde{\vartheta}\right) \tag{5.27}$$

with

$$\mathcal{F}_{racbf}(x,\theta) = f(x) + F(x)\lambda_{racbf}(x,\theta), \quad \lambda_{racbf}(x,\theta) \triangleq \theta - \Gamma\left(\frac{\partial h_r}{\partial \theta}(x,\theta)\right)^\top.$$

The set invariance condition (5.27) behaves less conservative than (5.22) since the condition enables the system state to get close to the boundary of $\mathcal{S}_\theta^r$. The following theorem provides a sufficient condition for forward invariance of $\mathcal{S}_\theta^r$ [58].

Theorem 5. If h_r is a Robust adaptive Control Barrier Function on $\mathcal{S}_\theta^r$, and there exists a positively definite adaptive gain satisfying:

$$\lambda_{\min}(\Gamma) \geq \frac{||\tilde{\vartheta}||^2}{2h_r(x(0),\theta(0))}, \tag{5.28}$$

and an update law:

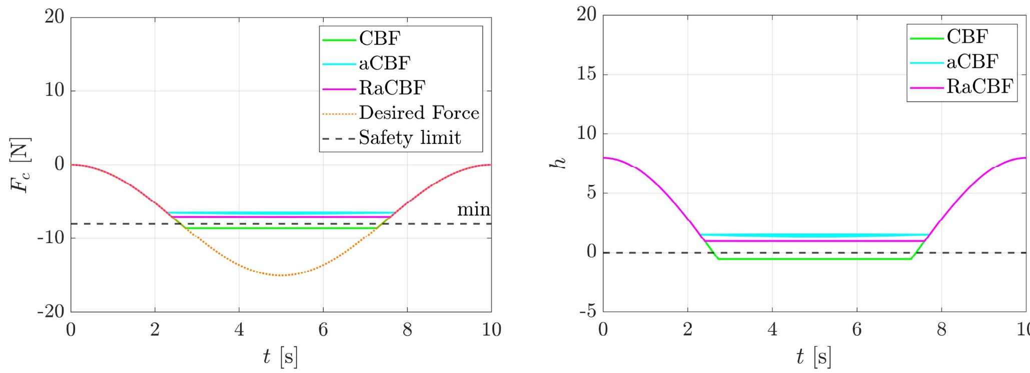
$$\tau(x,\hat{\theta}) = -\left(\frac{\partial h_r}{\partial x}(x,\hat{\theta})F(x)\right)^\top, \tag{5.29}$$

then any locally Lipschitz continuous controller satisfying (5.27) makes $\mathcal{S}_\theta^r$ is forward invariant, i.e. the system (5.19) is safe for $x \in \mathcal{S}_\theta^r$.

Like aCBF-QP, an optimization problem with RaCBF to generate a safe control input is formulated by [58] as:

$$\begin{aligned} u_{\mathsf{safe}} = \quad & \min_{u \in \mathcal{U}} \frac{1}{2}||u - u_{\mathsf{nominal}}||^2 \quad \textbf{(RaCBF-QP)} \\ \text{s.t. } & \frac{\partial h_r}{\partial x}(x,\hat{\theta})\Big(\mathcal{F}_{rcbf}(x,\hat{\theta}) + g(x)u\Big) \geq -\alpha\left(h_r(x,\hat{\theta}) - \frac{1}{2}\tilde{\vartheta}^\top\Gamma^{-1}\tilde{\vartheta}\right). \end{aligned} \tag{5.30}$$

As shown in Figure 5.4.(A), RaCBF shows less conservative behavior than aCBF since we use the maximum possible error in the formulation to achieve the tightened safe set, which allows for the system to approach the boundary of $\mathcal{S}_{\theta}^{r}$. It is worth noting that using the tightened set in RaCBF also removes the chattering behavior of aCBF controller as shown in Figure 5.4.(B).



(A) (B)

FIGURE 5.4 Simulation results of RaCBF and other safe contact force controllers. (A) Contact forces and (B) h functions of each controller.

Set Membership Identification (SMID)

Using the maximum possible error still leads to some conservatism in the RaCBF controller as shown in Figure 5.4.(A). To reduce the conservatism, a data-driven approach, Set Membership IDentification (SMID) [89] can be leveraged to decrease the maximum possible error by using the pair of two linear programmings (LPs) that search for a set intersection of minimum and maximum values of the parameters. We consider the following assumption on the unknown parameters [90]:

Assumption 1. There exists bounds of the unknown parameters with minimum and maximum values, $\underline{\theta}_i, \overline{\theta}_i \in \mathbb{R}$ for all $i \in \{1, \dots, k\}$ and a hyper-rectangle $\Theta := [\underline{\theta}_1, \overline{\theta}_1] \times [\underline{\theta}_2, \overline{\theta}_2] \cdots \times [\underline{\theta}_k, \overline{\theta}_k] \subset \mathbb{R}^k$ such that $\theta \in \Theta$.

To calculate each bound of the maximum possible error of each parameter, input-output data of the system (5.19) is first collected online. Let $\mathcal{H} = \{\mathcal{Y}_j, \mathcal{D}_j\}_{j=1}^{M}$ be a stack data with size, $M \in \mathbb{N}$ where $\mathcal{Y}_j = \dot{x}(t_j) - f(x(t_j)) - g(x(t_j))u(t_j)$ and $\mathcal{D}_j = F(x(t_j))$. Define the following set for all strictly increasing time sequences, t_j and $\Xi_0 = \Theta$:

$$\Xi_{t_j} = \{\theta \in \Xi_{t_j - 1} | -\varepsilon 1_n \leq \mathcal{Y}_j - \mathcal{D}_j \theta \leq \varepsilon 1_n\} \quad \forall j \in M, \tag{5.31}$$

where 1_n is $n-$dimensional vector of ones, and $\varepsilon \in \mathbb{R}$ is the tunable precision variable that can be treated as a parameter governing the conservatism of SMID, which can be used as a bound of the disturbance or noise in the system. Then, the following LPs' iterations are leveraged to find the set intersection that the true parameters belong to [90]:

$$\begin{aligned} \underline{\theta}_i^j &= \arg\min_{\theta} \quad \theta_i \\ \text{s.t. } & \mathcal{Y}_j - \mathcal{D}_j\theta \le \varepsilon 1_n \forall j \\ & \mathcal{Y}_j - \mathcal{D}_j\theta \ge -\varepsilon 1_n \forall j \\ & A_{j-1}\theta \le b_{j-1} \end{aligned} \tag{5.32}$$

$$\begin{aligned} \overline{\theta}_i^j &= \arg\max_{\theta} \quad \theta_i \\ \text{s.t. } & \mathcal{Y}_j - \mathcal{D}_j\theta \le \varepsilon 1_n \forall j \\ & \mathcal{Y}_j - \mathcal{D}_j\theta \ge -\varepsilon 1_n \forall j \\ & A_{j-1}\theta \le b_{j-1}, \end{aligned} \tag{5.33}$$

where A_{j-1}, b_{j-1} are the obtained bounds of θ from the previous iteration. And the iterations of (5.32) and (5.33) imply the following Lemma:

Lemma 1 ([90])**.** If *Assumption* 1 holds, the set, Ξ_{t_j} found by the iterations of LPs (5.32) and (5.33) satisfies the following:

$$\Xi_{t_j} \subset \Xi_{t_j - 1} \subset \Theta, \tag{5.34}$$

such that $\theta \in \Xi_{t_j}$ for all $j \in \mathbb{N}$.

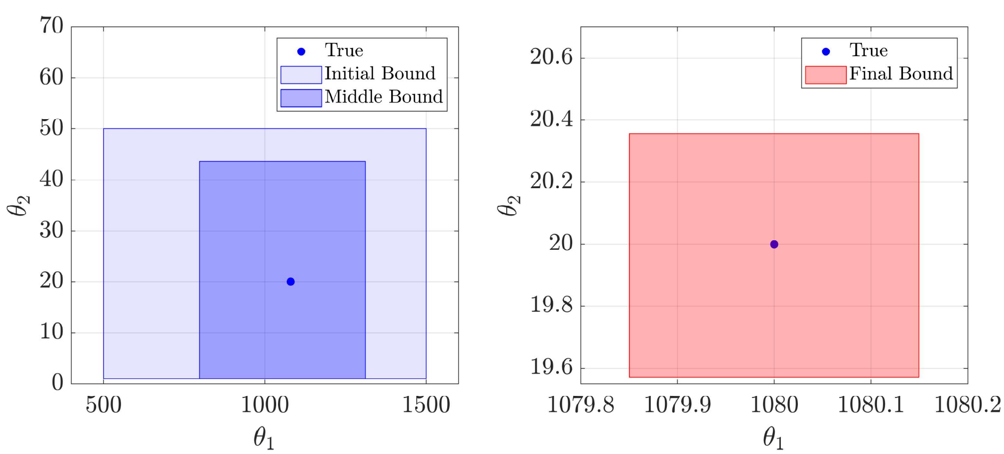
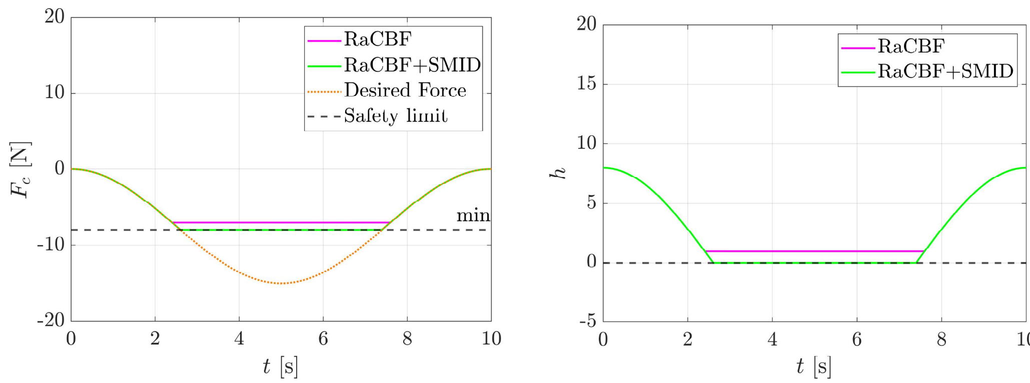


FIGURE 5.5 The results of set intersection estimate from SMID for the system (5.20). The pale blue shows the initial bound and the dark one is in the middle of the estimate. Lastly, the dark red rectangle represents the final estimate of the bounds of each parameter. The blue dot is the ground truth of the parameters.

SMID is directly applied to the same scenario on the top of RaCBF while searching for the bound of the parameters θ_1 and θ_2. The results of the bound approximation are shown in Figure 5.5, and the updated maximum possible errors of each parameter are used to reduce $\tilde{\vartheta}$ in the formulation (5.30). It is observed that the data-driven SMID scheme considerably decreases the conservatism of the nature of RaCBF as shown in Figure 5.6.



(A) (B)

FIGURE 5.6 (A) Contact forces of RaCBF with and without SMID and (B) h functions of each controller.

Input-to-State Safety

Input disturbances might exist in the system (5.8) and deteriorate the performance of the safe controller; thus, we consider the following system with input disturbances when designing the safe controller:

$$\dot{x} = f(x) + g(x)(u + d). \tag{5.35}$$

To this end, we use the notion of *input-to-state-safety* (ISSf) that allows minimal safety violation in the presence of input disturbances. We first define the following extended safe set $\mathcal{S}_\delta \supset \mathcal{S}$ provided a continuously differentiable function $h : \mathcal{X} \to \mathbb{R}$:

$$\mathcal{S}_\delta := \{x \in \mathbb{R}^n \mid h(x) + \gamma(\delta) \geq 0\}, \tag{5.36}$$

where $\gamma(\cdot)$ is an extended class $\mathcal{K}_\infty$ function. Note that the size of the extension is proportional to the magnitude of the input disturbance, $\delta \geq 0$. $\delta = 0$ implies the set, $\mathcal{S}_\delta$ is equivalent to the original safe set, $\mathcal{S}$. Based on the extended safe set, we have the following definition.

Definition 7 (*Input-to-state-safety* [90])**.** Consider the system (5.35) with input disturbances and an original safe set, $\mathcal{S}$. Then, we say that the system is *Input-to-State-Safety* if there exist an extended class $\mathcal{K}_\infty$ function γ and δ such that for all $||d||_\infty \leq \delta$ and $\mathcal{S}_\delta$ is forward invariant.

ISSf for the system is achieved by using the following control barrier function:

Definition 8 ([91])**.** A continuously differentiable function h is a *Input-to-State Safe Control Barrier Function* (ISSf-CBF) if there exist an extended class $\mathcal{K}_\infty$ function α and $\iota \in \mathcal{K}_{[0,a)}$ such that for all $x \in \mathcal{S}_\delta$:

$$\sup_{u\in\mathcal{U}}\{L_f h(x) + L_g h(x)(u+d)\} \geq -\alpha(h(x)) - \iota(||d||_\infty). \tag{5.37}$$

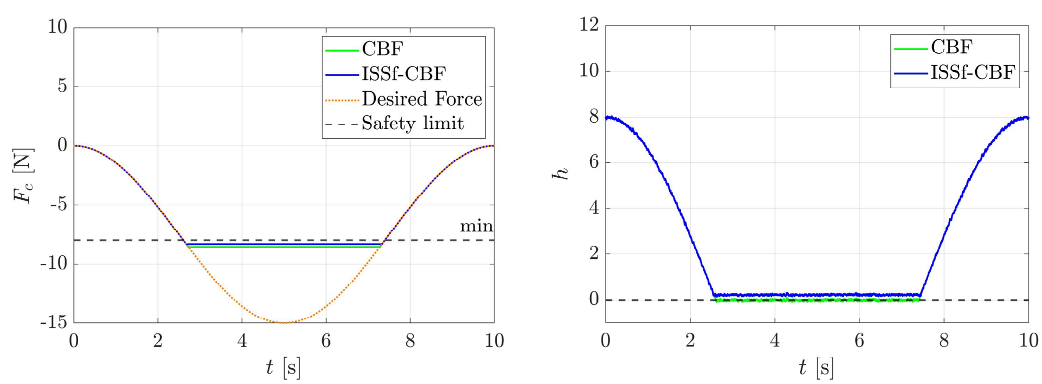
Then, the following theorem is obtained to render the system ISSf.

Theorem 6 ([91])**.** Let h be an ISSf-CBF, then any locally Lipschitz controller u satisfying (5.37) renders the system (5.35) ISSf with respect to $\mathcal{S}_\delta$.

In the same example, we introduce normally distributed input disturbances, $d \sim \mathcal{N}(0, \sigma^2)$ with standard deviation, σ and provide the following point-wise control input with QP:

$$\begin{aligned} u_{\text{safe}} = \min_{u\in\mathcal{U}} \quad & \frac{1}{2}||u - u_{\text{nominal}}||^2 \quad \textbf{(ISSf-CBF-QP)} \\ \text{s.t. } & L_f h(x) + L_g h(x) u \geq -\alpha(h(x)) + ||L_g h(x)||\delta - \frac{\epsilon\delta^2}{4} \end{aligned} \tag{5.38}$$

where $\gamma(\alpha)$ is chosen as $-\alpha^{-1}\left(-\frac{\epsilon_0\delta^2}{4}\right)$ from [75], and $\epsilon = 0.1$. Fig. 5.7 shows the simulation results of ISSf-CBF in the presence of input disturbances. Since we make the controller robust with the second term against the disturbances and select the small ϵ value, ISSf-CBF ensures the safety guarantees as shown in Fig. 5.7(B) compared to the normal CBF.



(A) (B)

FIGURE 5.7 Simulation results of safe contact force controllers. (A) Contact forces and (B) h functions of each controller.