CBF Verification

Motivation

- The problem of verifying whether the CBF constraints can always be satisfied has received less attention. The work propose a framework for verifying that a CBF guarantees safety for all time and synthesizing CBFs with verifiable safety in polynomial control systems.
- The approach is based on the fact that the safety guarantees rely on two properties.
  - There should be no point on the boundary of the CBF for which the Lie derivative of the CBF is always negative
  - The safe region of the CBF should be contained within the overall safe region.

Contribution

- The paper develop a SOS program for verifying that a given CBF construction ensures safety. We extend this approach to high-order CBFs and systems with multiple CBF constraints.
- The paper propose an alternating-descent heuristic for synthesizing CBFs using the proposed conditions.
- Considering special cases of the approach, including compact safe regions and constraints where the unsafe region is a union of non-overlapping convex sets.

CBF Verification

- Consider a nonlinear dynamic control system with dynamic:

$$\dot{x}(t) = f\big(x(t)\big) + g\big(x(t)\big)u(t) \qquad (1)$$

- where $x(t) \in \mathbb{R}^n$ denotes the state, $u(t) \in \mathbb{R}^m$ is a control input, and $f: \mathbb{R}^n \to \mathbb{R}$ and $g: \mathbb{R}^n \to \mathbb{R}$ are polynomials. The *safe region* is defined as $\mathcal{C} = \{x: h(x) \geq 0\}$, where $h: \mathbb{R}^n \to \mathbb{R}$ is a polynomial. The boundary of the safe region, denoted $\partial\mathcal{C}$, is defined by $\partial\mathcal{C} = \{x: h(x) = 0\}$. The *viability kernel* is defined as:
- Definition 1: The viability kernel is a set $\Omega \subseteq \mathcal{C}$ such that, for any $x_0 \in \Omega$, there is a control input signal $\{u(t): t \in [0, \infty)\}$ that guarantees $x(t) \in \Omega$ for all time t when the initial state is $x(0) = x_0$.

CBF Verification

- *Problem 1:* Given a system (1) and a safety constraint set $\mathcal{C}$, (i) verify whether a set $\widetilde{\omega}$ is contained in the viability kernel, and (ii) verify that a given control policy ensures that the system state remains in the viability kernel.
- Note that we do not consider any constraints on the control input $u(t)$ (e.g., limits on actuation).
- *Definition 2:* A function b is a control barrier function for system (1) if there is a class-K function α such that, for all x with $b(x) \geq 0$, there exist u satisfying

$$\frac{\partial b}{\partial x}(f(x) + g(x)u) \geq -\alpha\big(b(x)\big) \quad (2)$$

CBF Verification

- *Theorem 1:* A polynomial $b(x)$ is a CBF for (1) if and only if there exist polynomials $\eta(x), \theta_1(x), \dots, \theta_m(x)$, SOS polynomials $\alpha_0(x)$ and $\alpha_1(x)$, and an integer r such that:

$$\eta(x)b(x) + \sum_{i=1}^{m} \theta_i(x) \left[\frac{\partial b}{\partial x} g(x)\right]_i - \alpha_0(x) - \alpha_1(x) \frac{\partial b}{\partial x} f(x) + \left(\frac{\partial b}{\partial x} f(x)\right)^{2r} = 0 \quad (3)$$

- Moreover, the set $\{b(x) \geq 0\}$ is a subset of the viability kernel of $\mathcal{C}$ if (3) holds and there exist SOS polynomials $\beta_0(x)$ and $\beta_1(x)$ and a polynomial $\omega(x)$ such that

$$\beta_0(x) + \beta_1(x)b(x) + \omega(x)h(x) + 1 = 0$$

Control Barrier Function Construction

- *Problem 2:* Given a system (1) and a safety constraint set $\mathcal{C}$, construct a CBF b that verifiably guarantees positive invariance of $\mathcal{C}$.
- We initialize $b^0(x)$ arbitrarily and parameters ρ_0 and ρ' to be infinite. At step k, we solve the following SOS program with variable $\rho, \alpha^k(x), \eta^k(x), \theta_1^k(x), \dots, \theta_m^k(x), \omega(x)$,and $\beta^k(x)$

$$\min \ \rho$$

$$\textbf{s.t.} \quad \alpha^k(x)\frac{\partial b^{k-1}}{\partial x} f(x) + \sum_{i=1}^{m} \theta_i^k(x) \left[\frac{\partial b^{k-1}}{\partial x} g(x)\right]_i + \eta^k(x) b^{k-1}(x) + \rho\Lambda(x) - 1 \in SOS$$

$$-\beta^k(x) b^{k-1}(x) + \omega(x) h(x) - 1 \in SOS$$

$$\beta^k(x), \alpha^k(x) \in SOS$$

Control Barrier Function Construction

- $\Lambda(x)$ is a fixed SOS polynomial of sufficiently large degree to ensure that the first constraint is SOS for sufficiently large ρ. We let ρ_k denote the value of ρ returned by the optimization. The procedure terminates if $\rho \leq 0$ or if $|\rho_k - \rho'_{k-1}| < \epsilon$. Otherwise, we solve the SOS problem with variables ρ and b^k given by

$$\min \ \rho$$

$$\textbf{s.t.} \quad \alpha^k(x)\frac{\partial b^k}{\partial x} f(x) + \sum_{i=1}^{m} \theta_i^k(x) \left[\frac{\partial b^k}{\partial x} g(x)\right]_i + \eta^k(x) b^k(x) + \rho\Lambda(x) - 1 \in SOS$$

$$-\beta^k(x) b^k(x) + \omega(x) h(x) - 1 \in SOS$$

$$\beta^k(x), \alpha^k(x) \in SOS$$

- ρ'_k denote the value of ρ returned by the optimization. The procedure terminates if $\rho \leq 0$ or if $\left|\rho_k - \rho'_{k-1}\right| < \epsilon$.

Compact Safe Region

- Theorem 9: Suppose that (x^*, u^*) is a fixed point of (1), P is a solution to the Lyapunov equation corresponding to a stabilizing controller of the linearized system, and the SOS constraints

$$\alpha(x)\left(-2(x-x^*)^T P f(x)\right) + \sum_{i=1}^{m} \theta_i(x)[-2(x-x^*)^T P g(x)]_i + \eta(x)\left(\delta - (x-x^*)^T P (x-x^*)\right) \in SOS$$

- and

$$h(x) - \beta(x)\left(\delta - (x-x^*)^T P (x-x^*)\right) \in SOS$$

- hold for some polynomials $\theta_1, \ldots, \theta_m, \eta(x)$ and SOS polynomials $\alpha(x)$ and $\beta(x)$. Then $b_0(x; x^*) = \delta - (x-x^*)^T P (x-x^*)$ is a CBF and $\{b_0(x; x^*) \geq 0\}$ is in the viability kernel.

Compact Safe Region

- Let (x^*, u^*) satisfy $f(x^*) + g(x^*)u^* = 0$ and $x^* \in int(\mathcal{C})$. Then there exist a positive definite matrix P and $\delta > 0$ such that the function

$$b_0(x; x^*) = \delta - (x - x^*)^T P (x - x^*)$$

- is a CBF with $\{b_0(x; x^*) \geq 0\} \subseteq \mathcal{C}$

Compact Unsafe Region

- We consider a special case where the viability kernel and $\mathcal{C}$ are identical. This is the case of controllable linear systems $\dot{x}(t) = Fx(t) + Gu(t)$ where the safe region is given by $\mathcal{C} = \mathbb{R}^n \setminus \bigcup_{i=1}^{m} \{h_i(x) \leq 0\}$, where each h_i is a convex function, and the distance $d\left(\{h_i(x) \leq 0\}, \{h_j(x) \leq 0\}\right) > \delta$ for all i, j and $\delta > 0$.
- Theorem 10: Under the conditions described above, the viability kernel is equal to $\mathcal{C}$, and there exists a CBF-based policy that ensures safety.