非线性系统的安全分析与控制: 障碍函数方法

陈 杰 [1, 2, 3] 吕梓亮 [1, 2, 3] 黄鑫源 [1, 2, 3] 洪奕光 [1, 2, 3]

摘 要 近年来, 非线性系统的安全分析与控制已成为控制领域中的热门研究方向, 而障碍函数则是该方向的一种重要工具. 基于障碍函数的安全分析与控制方法具有计算效率高、鲁棒性强等优点. 本文首先从多个角度介绍了基于障碍函数的非线性系统安全性分析的理论成果, 并进一步综述了障碍函数方法在非线性系统安全控制中的最新进展. 最后, 简要地介绍了当前基于障碍函数的安全分析与控制理论中一系列尚未解决的问题, 并指出了未来可能发展的一些研究方向.

关键词 安全性分析, 安全控制, 障碍函数, 非线性系统

引用格式 陈杰, 吕梓亮, 黄鑫源, 洪奕光. 非线性系统的安全分析与控制: 障碍函数方法. 自动化学报, 2023, **49**(3): 567−579

DOI 10.16383/j.aas.c220888

Safety Analysis and Safety-critical Control of Nonlinear Systems: Barrier Function Approach

CHEN Jie[1, 2, 3] LYU Zi-Liang[1, 2, 3] HUANG Xin-Yuan[1, 2, 3] HONG Yi-Guang[1, 2, 3]

Abstract Safety analysis and safety-critical control of nonlinear systems have been important issues in the control society. The barrier function is a promising tool for the safety analysis and safety-critical control of nonlinear systems. This methodology has the advantages of high computation efficiency and strong robustness. In this paper, we first review the theoretical results on barrier function based safety analysis from different viewpoints, and then summarize some recent advances of the barrier function theory in the safety-critical control of nonlinear systems. Finally, we outline a series of open questions in the barrier function theory and point out some possible research directions.

Key words Safety analysis, safety-critical control, barrier functions, nonlinear systems

Citation Chen Jie, Lyu Zi-Liang, Huang Xin-Yuan, Hong Yi-Guang. Safety analysis and safety-critical control of nonlinear systems: Barrier function approach. *Acta Automatica Sinica*, 2023, **49**(3): 567−579

自上世纪 70 年代以来, 非线性控制系统理论获得了快速发展. 经过多年的努力, 控制学界已经在非线性控制系统的结构分析、稳定性分析、镇定设计以及非线性自适应和鲁棒控制等方面取得了突破性的研究成果[1−3]. 随着系统自主智能性的不断提高, 保证控制系统的安全性 (Safety) 变得越来越重要[4]. 现在, 非线性控制系统的安全分析与控制已经成为了当今控制领域的主流方向之一.

控制系统安全性的研究可以追溯到上世纪 40 年代日本学者 Nagumo 在不变集充要条件上的开拓性工作[5]. 如今, 安全性的研究已经从多个角度同时开展. 当前的安全分析与控制方法主要包括模型检测 (Model checking[6−7])、可达性分析 (Reachability analysis[8−10]) 以及障碍函数 (Barrier function[11−14]) 等.

模型检测通过穷举系统所有可能发生的动态行为以检测安全性. 值得注意, 现代控制系统往往同时包含连续和离散两种动态. 连续动态的存在导致系统具有无穷多种可能的动态行为, 从而造成模型检测方法在控制系统的安全分析与控制上受到巨大的限制. 可达性分析是另一种能够有效解决连续控制系统安全分析与控制的方法. 该方法具有成熟的计算工具包[15−16], 并已经被广泛地应用于现实中带有安全性约束的控制问题[17−19]. 然而, 可达集计算需要在状态空间上求解哈密顿−雅可比偏微分方程, 而这个过程对于非线性系统来说通常是比较困难的.

障碍函数最早应用于优化领域[20]. 与模型检测和可达性分析相比, 障碍函数方法可以高效地解决

收稿日期 2022-11-13 录用日期 2022-12-29
Manuscript received November 13, 2022; accepted December 29, 2022
国家自然科学基金 (61903027), 上海市重大专项 (2021SHZDZX0100), 上海市科技成果转化和产业化项目 (1951113210, 19511132101) 资助
Supported by National Natural Science Foundation of China (61903027), Shanghai Municipal Science and Technology Major Project (2021SHZDZX0100), and Shanghai Municipal Commission of Science and Technology (1951113210, 19511132101)
本文责任编委 杨涛
Recommended by Associate Editor YANG Tao
1. 同济大学电子与信息工程学院 上海 200092 2. 自主智能无人系统全国重点实验室 上海 201210 3. 同济大学上海自主智能无人系统科学中心 上海 201210
1. College of Electronic and Information Engineering, Tongji University, Shanghai 200092 2. National Key Laboratory of Autonomous Intelligent Unmanned Systems, Shanghai 201210 3. Shanghai Research Institute for Intelligent Autonomous Systems, Tongji University, Shanghai 201210

非线性控制系统的安全分析与控制问题, 并能够避免计算系统的状态轨迹或可达集. 在基于障碍函数的安全控制与分析框架下, 非线性系统的安全性分析可以通过障碍函数转化为凸优化问题[11], 能够有效降低安全性分析的计算复杂度和保守性; 而对于安全控制设计, 则可以通过控制障碍函数把安全性约束嵌入到反馈控制器[12−14], 能够有效地保证控制算法的实时性. 近年来, 在 Prajna、Ames 以及 Xu 等一批学者的共同努力下, 障碍函数已经成为了一种重要的安全分析与控制方法[11−14], 并被广泛地应用于生命维持系统[21]、集群机器人[22] 以及自动驾驶[23] 等实际问题的分析和设计.

本文将对障碍函数方法在非线性控制系统的安全分析与控制上的最新成果进行综述. 我们首先回顾了基于障碍函数的安全性分析理论. 随后介绍了基于障碍函数的安全控制设计方法. 最后简要地概括了现有障碍函数方法的不足之处, 浅析其未来的研究方向.

1 基于障碍函数的安全性分析

在这部分, 我们首先回顾基于障碍函数的非线性系统安全性分析的重要理论成果.

1.1 自治系统的安全性分析

考虑非线性自治系统

$$\dot{x} = f(x) \tag{1}$$

其中, $x \in \mathbf{R}^n$ 为系统状态, $f : \mathbf{R}^n \to \mathbf{R}^n$ 为局部利普希茨连续的向量场. 对于任意初始状态 $x_0 = x(t_0)$, 记 $x(t, x_0)$ 为系统 (1) 的解. 在不引起歧义的情况下, 本文将 $x(t, x_0)$ 简写成 $x(t)$.

假设系统 (1) 的安全性约束可以通过以下集合刻画:

$$\mathcal{S} = \{x \in \mathbf{R}^n : h(x) \geq 0\} \tag{2}$$

其中, $h : \mathbf{R}^n \to \mathbf{R}$ 是一个与系统安全性相关的连续标量函数. 该函数的零水平集将不安全区域 χ_u 隔开, 使得 $\mathcal{S} \subseteq \mathbf{R}^n \backslash \chi_u$. 在本文的随后部分, 我们把 $\mathcal{S}$ 称为系统 (1) 的安全集.

定义 1[12−14]**.** 对于系统 (1), 如果状态 $x(t, x_0)$ 从安全集 $\mathcal{S}$ 出发, 即 $x_0 \in \mathcal{S}$, 并始终停留在 $\mathcal{S}$ 中, 则称该系统是安全的.

基于障碍函数的安全性分析方法最早可见于文献 [24−25]. 其基本思想是根据系统的结构信息和安全性约束构造标量函数 $h(x)$, 以检测安全集 $\mathcal{S}$ 的不变性. 令 $B(x) = -h(x)$. 文献 [24−25] 指出, 如果

$$L_f B(x) \leq 0 \tag{3}$$

则 $\mathcal{S}$ 是一个不变集, 即系统 (1) 是安全的. 在这里, $L_f B(x)$ 表示 $B(x)$ 沿着向量场 f 的 Lie 导数. 本质上, 条件 (3) 等价于

$$L_f h(x) \geq 0 \tag{4}$$

定理 1[24−25]**.** 对于系统 (1), 如果存在连续可导函数 $h : \mathbf{R}^n \to \mathbf{R}$ 使得 (4) 成立, 则该系统是安全的.

满足 (4) 的障碍函数 $h(x)$ 也被称为障碍证书 (Barrier certificate, BC). 回顾经典的李雅普诺夫条件[2] 可知, $h(x)$ 本质上是一种不具有正定特性的类李雅普诺夫函数. 该方法不需要穷举系统的动态行为, 并且避免了显式计算系统的状态轨迹或可达集. 此外, 满足 (4) 的障碍函数集合是一个凸集, 即对于任意满足 (4) 的障碍函数 $h_1(x)$ 和 $h_2(x)$ 以及任意的常数 $a \in [0, 1]$, $h(x) = ah_1(x) + (1 - a)h_2(x)$ 仍然是一个满足 (4) 的障碍函数. 该特性意味着可以利用凸优化方法搜索障碍函数以验证系统的安全性, 能够为障碍函数的计算性综合带来巨大好处. 在文献 [26], Prajna 等进一步指出如果系统是安全的, 则必然存在满足 BC 条件 (4) 的标量函数 $h(x)$. 随后, 障碍函数方法获得了大量的关注. 例如, 文献 [27] 利用障碍函数方法验证复杂系统的时序逻辑属性, 而文献 [28−31] 则进一步对障碍函数的逆定理进行探索.

根据 BC 条件 (4) 可知, 状态轨迹 $x(t)$ 的运动方向始终指向安全集 $\mathcal{S}$ 的内部. 在该条件下, 即使 $x(t)$ 处于足够安全的位置 (离不安全区域足够远), 也不可以朝着安全集 $\mathcal{S}$ 边缘的方向移动. 这意味着定理 1 的分析方法是保守的, 同时也制约了该定理在安全控制上的应用. 为了降低 BC 条件的保守性, 国内外众多研究人员在过去十余年进行了大量的探索. 如今, 相关研究成果大致可以分为两类.

第一类障碍函数仅在安全集 $\mathcal{S}$ 内部具有定义, 并随着系统状态 $x(t)$ 靠近 $\mathcal{S}$ 的边缘而趋向于无穷大, 典型例子包括倒数障碍函数 (Reciprocal barrier function, RBF[12, 32])、障碍李雅普诺夫函数 (Barrier Lyapunov function, BLF[33−35]) 等. 此类障碍函数具有以下两点不足. 首先, 当 $h(x)$ 随着 $x(t)$ 靠近安全集边缘而趋向于无穷大时, 将不可避免地造成控制幅值过大. 其次, 在外部扰动的作用下, 系统实际的初始状态可能会偏离安全集. 例如, 给定预设的初始状态 $x_0^d \in \mathcal{S}$, 如果系统初始化时受到环境噪声的影响从而产生初始化偏差 δ, 那么实际的初始状态将变为 $x_0 = x_0^d + \delta$. 这可能会导致 $x_0 \notin \mathcal{S}$, 从而大大降低了此类障碍函数分析方法的适用性.

另一类障碍函数在状态空间具有全局定义, 并

且随着状态轨迹靠近安全集边缘而趋于零. 此类障碍函数又被称为零点障碍函数 (Zeroing barrier function, ZBF), 其定义最早由文献 [36] 提出. 随后, Xu 及其合作者提出非线性版本的 ZBF, 并从集合渐近稳定性的角度指出 ZBF 对初始状态的偏差具有鲁棒性[13]. 以上的这些优点使得 ZBF 成为当今安全分析与控制领域应用最广的障碍函数.

定义 2[13]**.** 对于系统 (1), 如果函数 $h:\mathbf{R}^n\to\mathbf{R}$ 连续可微并且满足

$$L_f h(x)\geq -\alpha(h(x)) \tag{5}$$

则称该函数为系统 (1) 的 ZBF. 这里, α 是一个局部利普希茨连续的扩展 K 类函数[1].

定理 2[13]**.** 如果系统 (1) 具有满足 (5) 的 ZBF, 则该系统是安全的.

由 (2) 可知, 当 $x(t)$ 处于 $\mathcal{S}$ 内部时, $\alpha(h(x))>0$. 因此, 在 ZBF 条件 (5) 下, $x(t)$ 可以朝安全集 $\mathcal{S}$ 边缘方向运动. 此外, 由 (5) 可知, 当 $x(t)$ 处于安全集 $\mathcal{S}$ 的内部并且运动方向指向 $\mathcal{S}$ 的边缘时, 其速度上限由 $\alpha(h(x))$ 决定; 当 $x(t)$ 运动至 $\mathcal{S}$ 边缘时, 该轨迹指向不安全区域方向的速度分量衰减至零, 即

$$x(t)\in\partial\mathcal{S}\Rightarrow\alpha(h(x))=0$$

这意味着状态轨迹 $x(t)$ 不能继续跨过安全集边缘进入不安全区域. 从这个角度上理解, ZBF 条件 (5) 对 $x(t)$ 的作用相当于汽车的刹车系统.

此外, 文献 [13] 从集合渐近稳定的角度指出 ZBF 对初始状态的偏差具有鲁棒性, 其具体分析过程如下. 考虑标量函数

$$V(x)=\begin{cases}0, & x\in\mathcal{S}\\ -h(x), & x\in\mathbf{R}^n\backslash\mathcal{S}\end{cases} \tag{6}$$

根据 (5) 可得: 1) 当 $x\in\mathcal{S}$, $V(x)=0$; 2) 当 $x\in\mathbf{R}^n\backslash\mathcal{S}$, $V(x)>0$; 3) 对于任意 $x\in\mathbf{R}^n\backslash\mathcal{S}$,

$$L_f V(x)=-L_f h(x)=\alpha(-V(x))$$

因此, $V(x)$ 是一个有效的李雅普诺夫函数. 由李雅普诺夫理论[37] 可知, 系统 (1) 相对于安全集 $\mathcal{S}$ 是渐近稳定的, 即:

$$|x(t,\,x_0)|_{\mathcal{S}}\leq\beta(|x_0|_{\mathcal{S}},\,t-t_0),\quad\forall x_0\in\mathbf{R}^n$$

其中, β 为 KL 类函数, $|x|_{\mathcal{S}}$ 表示欧几里德空间内一点 x 到集合 $\mathcal{S}$ 的距离. 由 KL 类函数性质可知: 1) 如果 $x_0\in\mathcal{S}$, 那么 $|x(t,\,x_0)|_{\mathcal{S}}=\beta(0,\,t-t_0)\equiv 0$, 系统状态 $x(t)$ 始终停留在安全集 $\mathcal{S}$ 的内部; 2) 如果 $x_0\notin\mathcal{S}$, 那么 $|x(t,\,x_0)|_{\mathcal{S}}$ 随着 t 增大而逐渐减小至零, 状态轨迹 $x(t,\,x_0)$ 最终会进入并始终保持在 $\mathcal{S}$ 内部. 上述性质表明 ZBF 对初始状态的偏差具有鲁棒性.

近年来, ZBF 方法被进一步推广. 例如, 文献 [38] 把有限时间稳定的思想应用到安全性分析, 提出了有限时间收敛 ZBF, 而文献 [39] 则通过引入非光滑分析技术把 ZBF 推广至微分包含, 去除了传统 ZBF 的连续可微限制. 此外, 文献 [40] 针对离散系统, 提出了离散时间 ZBF.

1.2　输入−状态安全系统的安全性分析

我们前面讨论了无输入非线性自治系统的安全性分析, 但是实际中的非线性系统常常会受到外部扰动的影响. 为此, 我们在这里进一步讨论带有外部输入的非线性系统的安全性分析. 这类方法有助于分析外部扰动带来的不确定性对系统安全的影响. 考虑

$$\dot{x}=f(x,\,u) \tag{7}$$

其中, $x\in\mathbf{R}^n$ 为系统状态, $u\in\mathbf{R}^m$ 为输入, $f:\mathbf{R}^n\times\mathbf{R}^m\to\mathbf{R}^n$ 为局部利普希茨连续函数. 在这里, $u:\mathbf{R}_{\geq 0}\to\mathbf{R}^m$ 可用于描述外部输入或扰动为系统所带来的不确定性. 根据惯例, 我们假设 $u(\cdot)$ 是可测且局部本质有界的, 并将此类函数记作 L_∞^m.

输入−状态安全 (Input-to-state safety, ISSf) 是刻画外部输入 u 对系统安全性影响的一种重要工具. ISSf 是输入−状态稳定性 (Input-to-state stability, ISS[41]) 在安全性分析上所对应的概念, 其定义最早由文献 [42−43] 给出. 该定义要求系统状态 $x(t)$ 到不安全区域的最小距离随着时间 t 的增大而增大, 存在较大保守性. 随后, 文献 [44] 首次从 ZBF 的角度重定义了 ISSf. 该定义继承了 ZBF 分析方法的鲁棒性强、保守性低等优点.

假设系统 (7) 的安全性约束可以由 (2) 所定义的集合 $\mathcal{S}$ 描述. 另外, 定义集合

$$\mathcal{C}=\{x\in\mathbf{R}^n:h(x)+\gamma(\|u\|)\geq 0\} \tag{8}$$

其中, $\|u\|=\sup\{|u(t)|,\,t\geq 0\}$ 表示 u 的 L_∞^m 范数, γ 为 K 类函数. 比较 (2) 和 (8) 可知, 对于任意 $u\in L_\infty^m$, $\mathcal{S}$ 是 $\mathcal{C}$ 的一个子集. 并且, 当 $u\equiv 0$ 时, $\mathcal{S}=\mathcal{C}$.

定义 3[44]**.** 对于非线性系统 (7), 如果状态轨迹 $x(t,\,x_0)$ 从安全集 $\mathcal{S}$ 出发, 即 $x_0\in\mathcal{S}$, 并始终停留在更大的集合 $\mathcal{C}$ 中, 则称该系统是输入−状态安全的. 这里, γ 被称为系统的 ISSf 增益.

根据定义 3 可知, ISSf 意味着对于任意从安全集 $\mathcal{S}$ 出发的状态轨迹 $x(t,\,x_0)$, 由于外部输入 u 带来的不确定性的存在, $x(t)$ 可能会离开 $\mathcal{S}$, 但是始终

[1] 扩展 K 类函数是传统 K 类函数[2] 在安全分析与控制上的推广. 对于任意函数 $\alpha:\mathbf{R}\to\mathbf{R}$, 我们说它是一个扩展 K 类函数, 如果该函数在 $\mathbf{R}$ 上连续、严格递增并满足 $\alpha(0)=0$; 特别地, 如果 $\alpha(s)$ 分别随着 s 趋于 $+\infty$ 和 $-\infty$ 而趋于 $+\infty$ 和 $-\infty$, 则该函数是一个扩展 K_∞ 类函数.

停留在一个包含 $\mathcal{S}$ 的大集合 $\mathcal{C}$ 内部, 并且 $\mathcal{S}$ 和 $\mathcal{C}$ 的最大边缘距离为 $\gamma(\|u\|)$. 因此, 在设计系统时, 必须预留 $\gamma(\|u\|)$ 的安全裕度. 当系统 ISSf 增益 γ 或外部输入的幅值 $|u|$ 减小时, $\mathcal{S}$ 和 $\mathcal{C}$ 的最大边缘距离随之减小. 因此, 外部输入 u 对系统安全性的影响就越小, 系统维持安全性的把握更大.

ISSf 障碍函数 (ISSf barrier function, ISSf-BF) 是分析系统 ISSf 的有效工具, 其定义最早由文献 [44] 给出.

定义 4[44]**.** 考虑系统 (7). 如果对于任意 $x \in \mathbf{R}^n$ 以及 $u \in L_\infty^m$, 函数 $h : \mathbf{R}^n \to \mathbf{R}$ 连续可微并且满足

$$\nabla h(x) f(x, u) \geq -\alpha(h(x)) - \phi(|u|) \tag{9}$$

则称该函数为系统 (1) 的 ISSf-BF. 这里, α 为局部利普希茨连续的扩展 K_∞ 类函数, ϕ 为 K 类函数.

最近, 文献 [45] 提出了另一种等价的 ISSf-BF 定义:

$$|h(x)| \geq \gamma(|u|) \Rightarrow \nabla h(x) f(x, u) \geq -\sigma(h(x)) \tag{10}$$

其中, σ 为扩展 K 类函数, γ 为 K 类函数. 不难看出, (9) 和 (10) 可以分别视为耗散型和增益裕度型 ISS 李雅普诺夫函数[41] 在安全性分析上所对应的概念.

定理 3[44−45]**.** 如果系统 (7) 具有满足 (9) 或 (10) 的 ISSf-BF, 则该系统是 ISSf 的, 即对于任意 $x_0 \in \mathcal{S}$, $x(t, x_0)$ 始终停留在 (8) 的集合 $\mathcal{C}$ 中.

近年来, ISSf-BF 已经在非线性系统的安全分析与控制上发挥着重要的作用. 例如, 著名学者 Krstic 利用 (10) 定义的 ISSf-BF 提出了一套逆最优安全控制设计方法[46]; 而文献 [47−49] 采用 ISSf-BF 分析事件触发采样机制对闭环系统安全性的影响.

注意到定理 3 要求安全约束的相对阶 (Relative degree) 等于 1. 也就是, 对 ISSf-BF 候选函数 $h(x)$ 进行一次微分即可获得外部输入 u 的信息[2]. 然而, 大多数复杂系统并不能满足这个要求, 典型的例子包括具有输出约束的欧拉−拉格朗日系统[50]、小车−弹簧−倒立摆系统[51] 等. 针对这个问题, 学术界已经从安全性分析[52] 和安全控制设计[53−56] 等不同的角度探索高阶约束下的外部输入 u 对系统安全性的影响. 在安全性分析方面, 文献 [52] 提出了高阶的 ISSf-BF. 为了给出高阶 ISSf-BF (相对阶为 r) 的定义, 令

$$\eta_0(x) = h(x) \tag{11a}$$

$$\eta_k(x) = \dot{\eta}_{k-1}(x) + \alpha_k(\eta_{k-1}(x)) \tag{11b}$$

其中, $1 \leq k \leq r$ 为整数, α_k 为扩展 K_∞ 类函数.

定义 5[52]**.** 如果 $h : \mathbf{R}^n \to \mathbf{R}$ 为 r 阶连续可微函数并且满足 (11) 及

$$\eta_r(x) \geq -\gamma(|u|) \tag{12}$$

则称该函数为系统 (7) 的 r 阶 ISSf-BF. 这里, γ 是一个 K 类函数.

定理 4[52]. 如果系统 (7) 具有满足 (11) 和 (12) 的 r 阶 ISSf-BF, 那么该系统是 ISSf 的.

1.3 障碍函数的计算方法

障碍函数安全性分析理论把系统的安全性验证问题转化为寻找障碍函数, 从而避免显式计算系统的状态轨迹或可达集. 但是, 对于一般化的非线性系统, 目前并没有普适的障碍函数构造方法.

受到非线性系统的李雅普诺夫函数计算方法[57] 的启发, Prajna 等在文献 [24−25] 中指出, 如果系统函数 $f(x)$ 具有多项式结构并且安全性约束可通过多项式结构的等式/不等式描述时, 则可以利用平方和 (Sum of squares, SOS) 规划[57] 自动搜索满足 BC 条件 (4) 的障碍函数. 随后, Xu 等进一步把 SOS 规划应用于自动搜索满足条件 (5) 的 ZBF[23]. SOS 规划是一种凸优化方法, 可以有效降低自动搜索障碍函数的保守性. 该过程相对于系统维数具有多项式复杂度, 并可以通过现有的成熟软件包 (如 SOSTOOLS[58−59]、SOSOPT[60] 等) 完成. 上述优势使得 SOS 规划成为了寻找非线性系统障碍函数的主流解决方案.

对于任意的多项式 $p(x)$, 如果存在一组多项式 $p_1(x), \cdots, p_m(x)$ 使得

$$p(x) = \sum_{i=1}^{m} (p_i(x))^2$$

则称 $p(x)$ 为一个具有 SOS 结构的多项式. 显然, 对于任意 SOS 多项式 $p(x)$, 其次数必定为偶数, 记为 $2d$. 令 $\Sigma[x]$ 表示具有 SOS 多项式的集合. 根据文献 [57], 检测多项式函数 $p(x)$ 是否具有 SOS 结构等价于寻找半正定实数矩阵 Q, 使得

$$p(x) = Z^{\mathrm{T}}(x) Q Z(x) \tag{13}$$

其中, $Z(x)$ 是由次数不大于 d 的单项式组成的向量. 显然, 约束 (13) 相对于待搜索参数矩阵 Q 具有凸性. 在控制领域, 参数矩阵 Q 的搜索可以通过半定规划 (Semidefinite program) 完成[57].

以下结果可通过文献 [23−25, 36] 的证明方法得到.

定理 5. 考虑系统 (1). 假设 $f(x)$ 具有多项式结构, 并且存在多项式函数 $\rho(x)$ 使得

$$\{x \in \mathbf{R}^n : \rho(x) \geq 0\} \subseteq \mathbf{R}^n \backslash \chi_u$$

其中, χ_u 为系统的不安全区域. 对于具有多项式结

[2] 这里的相对阶是把 $h(x)$ 当做某种意义下的输出.

构的连续可导函数 $h:\mathbf{R}^n\to\mathbf{R}$ 以及常数 $\lambda>0$, 如果

$$-h(x)+s_1^{\mathrm{T}}(x)\rho(x)\in\Sigma[x] \tag{14a}$$

$$L_fh(x)+\lambda h(x)-s_2(x)h(x)\in\Sigma[x] \tag{14b}$$

$$s_1(x),\, s_2(x)\in\Sigma[x] \tag{14c}$$

则 $h(x)$ 为系统 (1) 的 ZBF.

为保证本文的完整性, 我们简要概述 SOS 规划搜索 ZBF 的操作过程, 具体可分为以下三步.

第一步. 选定多项式 ZBF 候选函数的阶数 d, 并将 $h(x)$ 参数化为

$$h(x)=\sum_{j=1}^{m}a_jb_j(x)$$

其中, $b_1(x),\cdots,b_m(x)$ 是一组多项式基, m 为待设计的整数, $a_1,\cdots,a_m>0$ 是一组可以由 SOS 规划搜索得到的参数.

第二步. 根据 d 的取值确定 $s_1(x)$ 和 $s_2(x)$ 的阶数, 并利用第一步的方法将 $s_1(x)$ 和 $s_2(x)$ 参数化为

$$s_i(x)=\sum_{j=1}^{m}c_{i,\,j}s_{i,\,j}(x),\quad i=1,\,2$$

其中, $s_{i,\,1}(x),\cdots,\ s_{i,\,m}(x)$ 为一组与 $s_i(x)$ 维数相同的多项式向量, $c_{i,\,1},\cdots,\ c_{i,\,m}$ 是一组由 SOS 搜索得到的参数. 文献 [36] 指出, 为了保证 (14a) 和 (14b) 同时成立, $s_1^{\mathrm{T}}(x)\rho(x)$ 和 $s_2(x)h(x)$ 中至少有一项的阶数不小于 d.

第三步. 利用 SOS 规划搜索满足 (14a) ~ (14c) 的参数 a_j 和 $c_{i,\,j}$ $(i=1,\,2;\ j=1,\cdots,m)$.

1.4　组合系统的安全性分析

我们已经回顾了在系统具有多项式结构的情况下, 利用 SOS 规划计算障碍函数需要多项式复杂度. 这意味着随着系统的规模增大, 该计算方法将不可避免地陷入到 "维数灾难"中. 由于现实中的复杂系统通常是由多个相对独立模块或子系统相互连接而成的组合系统 (Compositional system)[3], 一个有效的解决思路是先利用障碍函数理论对较为简单的子系统进行单独的安全性分析, 然后通过组合系统分析工具 (如, 无源性理论[61]、小增益理论[62] 等) 从子系统的安全属性中推导出整体系统的安全性.

小增益理论是组合系统的有效分析工具. 早期小增益理论是从输入–输出角度提出的, 只针对系统增益具有线性或仿射形式的情况[62]. 随后, 文献 [63] 把小增益理论推广至非线性增益形式. 到了上世纪 90 年代, 小增益理论在 ISS 框架得到进一步发展[64–65]. 近年来, 文献 [45, 52, 66–67] 从 ISSf-BF 的角度出发, 建立了安全性分析的小增益理论. 考虑组合系统

$$\dot{x}_1=f_1(x_1,\,x_2,\,u_1) \tag{15a}$$

$$\dot{x}_2=f_2(x_1,\,x_2,\,u_2) \tag{15b}$$

其中, $x_i\in\mathbf{R}^{n_i}$, $u\in\mathbf{R}^{m_i}$ $(i=1,\,2)$. 假设 (15) 的每一个子系统均满足 ISSf-BF 条件

$$\begin{aligned}&\nabla h_i(x_i)f_i(x_i,\,x_{3-i},\,u_i)\geq\\&\quad-\alpha_i(h_i(x_i))+\phi_i(h_{3-i}(x_{3-i}))-\gamma_i(|u_i|)\end{aligned} \tag{16}$$

其中, $i=1,\,2$, α_i 和 ϕ_i 为扩展 K_∞ 类函数, γ_i 为 K 类函数. 根据 (16) 可知, x_i-子系统相对于输入 $(x_{3-i},\,u_i)$ 是 ISSf 的. 并且, 从 $h_{3-i}(x_{3-i})$ 到 $h_i(x_i)$ 的 ISSf 增益为

$$\hat{\phi}_i=\alpha_i^{-1}\circ(\mathrm{Id}+\rho)\circ\phi_i \tag{17}$$

其中, 记号 "$\circ$"表示函数复合运算符, Id 表示单位函数, ρ 为任意的扩展 K_∞ 类函数. 文献 [45] 指出, 在小增益条件下, 子系统的 ISSf 性质可以传递到组合系统 (15).

定理 6[45]**.** 假设系统 (15) 的子系统均满足 (16), 则该系统也是 ISSf 的, 如果以下小增益条件成立:

$$|\hat{\phi}_1\circ\hat{\phi}_2(s)|<|s|,\quad\forall s\in\mathbf{R}\backslash\{0\} \tag{18}$$

例 1. 考虑串联系统

$$\dot{x}_1=f_1(x_1,\,x_2,\,u_1),\ \dot{x}_2=f_2(x_1,\,u_2) \tag{19}$$

显然, (19) 是 (15) 的特例. 假设 x_1-子系统的 ISSf-BF 满足 (16), x_2-子系统的 ISSf-BF 满足

$$\begin{aligned}&\nabla h_2(x_2)f_1(x_1,\,x_2,\,u_2)\geq\\&\quad-\alpha_2(h_2(x_2))-\gamma_2(|u_2|)\end{aligned}$$

不难发现, 当 $\phi_2(s)\equiv0$ 时, 小增益条件 (18) 恒成立. 因此, 根据定理 6 可得, 串联系统 (19) 是 ISSf 的.

最近, 国内外研究人员从不同的角度对安全性分析的小增益定理进行了更深入的探索. 例如, 文献 [66] 针对更复杂网络化系统的安全性分析提出了回路小增益定理; 而文献 [67] 则利用离散小增益定理对具有复杂时序逻辑约束的大规模系统进行安全性验证, 以降低传统方法的计算复杂度. 另外, 定理 6 只针对于具有低阶安全性约束. 然而, 实际中的控制系统并不是总能满足该要求, 典型例子包括小车–弹簧–倒立摆系统[51] 等. 针对该问题, 文献 [52] 进一步提出高阶安全性约束的小增益定理, 并指出组合系统的 ISSf-BF 具有 ZBF 一样的鲁棒性. 假设系统 (15) 的安全性约束可以由以下高阶 ISSf-BF 刻画:

$$\eta_{i,\,0}(x_i)=h_i(x_i) \tag{20a}$$

[3] 在控制领域, 组合系统有时也被称作互联系统 (Interconnected system).

$$\eta_{i,\,k}(x_i) = \dot{\eta}_{i,\,k-1}(x_i) + \alpha_{i,\,k}(\eta_{i,\,k-1}(x_i)) \tag{20b}$$

$$\eta_{i,\,r}(x_i) \geq \phi_i(h_{3-i}(x_{3-i}) - \gamma_i(|u_i|) \tag{20c}$$

其中, $\alpha_{i,\,k}$ 和 ϕ_i 为扩展 K_∞ 类函数, γ_i 为 K 类函数. 在高阶 ISSf-BF 条件 (20) 的意义下, 我们可以确定 x_i-子系统的 ISSf 增益为

$$\hat{\phi}_i = (\mathrm{Id} + \sigma) \circ \alpha_{i,\,1}^{-1} \circ \cdots \circ (\mathrm{Id} + \sigma) \circ \alpha_{i,\,r}^{-1} \circ (\mathrm{Id} + \sigma) \circ \phi_i$$

其中, σ 为任意的扩展 K_∞ 类函数. 文献 [52] 指出, 如果系统 (15) 的 ISSf 增益 $\hat{\phi}_1$ 和 $\hat{\phi}_2$ 满足小增益条件 (18), 则该系统仍然是 ISSf.

1.5 时序逻辑约束下的安全性验证

上面介绍的安全性验证方法只考虑了底层物理动态的安全性约束. 为了提高对复杂系统分析和综合的效率, 人们会在系统设计中引入逻辑推理. 这时, 控制系统可以看作由上层逻辑和底层动力学两部分组成, 其安全性也需要在上述两个层面上得到保证. 也就是, 系统的安全运行需要在底层满足元器件的物理约束 (例如, 电机扭矩不能过大), 并且在上层也要满足预设的时序逻辑约束 (例如, 系统需要按照正确的顺序完成一系列任务)[68]. 在这种情况下, 控制系统将会表现出复杂的混杂行为, 对其安全性进行有效分析是当今学术界正在探索的重要方向之一.

线性时序逻辑 (Linear temporal logic, LTL[69]) 是一种能够描述控制系统动力学特性的形式化语言. LTL 语言由逻辑运算符和时序运算符组成, 其句法规则可以写成如下的形式:

$$\phi ::= \mathrm{TRUE} | p | \phi_1 \wedge \phi_2 | \neg\phi | \mathrm{O}\phi | \phi_1 \mathrm{U} \phi_2$$

这里, p 为原子命题, ϕ, ϕ_1 和 ϕ_2 为 LTL 公式, $\wedge$ 和 $\neg$ 分别表示逻辑运算符 "与"和 "非", O 和 U 分别表示时序运算符 "next"和 "until". 对于具有 LTL 约束的离散控制系统, 国内外学者已经借助模型检测技术建立了许多有效的安全性分析方法[70]; 而对于连续控制系统, 传统的解决思路是先对原系统进行抽象化处理得到离散的标签转移系统 (Labeled transition system, LTS), 然后利用模型检测工具验证这一个 LTS 是否满足预设的 LTL 约束, 以判断原系统是否能够安全运行. 值得注意, 上述抽象化得到的 LTS 大小随着原系统的维数增大而指数增长[6], 极大地制约了模型检测方法应用. 目前, 国内外学者正从多个方面对无抽象化的安全性分析技术进行探索.

障碍函数是一种具有广阔前景的无抽象化安全性分析技术. 文献 [26] 首先指出, 控制系统常见的 "always"和 "eventually"时序约束下的安全性验证问题均可分别通过障碍函数转化为凸优化问题. 随后, 文献 [27] 进一步针对 LTL 约束下的安全性分析问题, 结合自动机理论和障碍函数提出了一套无抽象的验证方法. 该方法首先利用自动机理论把复杂的 LTL 约束拆分成一系列简单的安全性约束, 并进一步利用障碍函数方法验证系统是否满足这些简单的安全性约束. 值得注意, 虽然该方法避免了抽象化过程, 但是其计算障碍函数过程的复杂度仍受限于系统维数以及 LTL 规约长度. 并且, 虽然该方法具有可靠性, 但却不具有完备性. 也就是, 如果该方法检测到系统满足 LTL 约束 ϕ, 则该结果为真; 但是, 如果没有检测到系统满足 LTL 约束 ϕ, 则不能说明系统一定不能满足此约束.

2 基于障碍函数的安全控制

我们在前面简要综述了基于障碍函数的安全性分析理论成果. 值得注意, 实际的自主智能控制系统并不是总能满足安全性约束. 在这种情况下, 借助反馈控制的手段来保证闭环系统的安全性就显得尤为重要. 在这里, 我们将介绍基于障碍函数的安全控制设计方法. 考虑非线性仿射控制系统

$$\dot{x} = f(x) + g(x)u \tag{21}$$

其中, $x \in \mathbf{R}^n$ 为系统状态, $u \in \mathbf{R}^m$ 为控制输入, $f: \mathbf{R}^n \to \mathbf{R}^n$ 和 $g: \mathbf{R}^n \to \mathbf{R}^n \times \mathbf{R}^m$ 为局部利普希茨连续的向量场. 假设系统 (21) 的安全性约束可由 (2) 中的集合 $\mathcal{S}$ 描述.

2.1 控制障碍函数

值得注意, 安全性分析中的障碍函数理论成果仅能用于无控制输入非线性系统的安全性分析, 并不能直接用于安全控制设计. 为此, 文献 [71] 受到控制李雅普诺夫函数 (Control Lyaupnov function, CLF[72−73]) 的启发, 提出了控制障碍函数 (Control barrier function, CBF). 这个概念是障碍函数安全控制理论的核心. 通过 CBF, 我们可以建立系统安全性约束和控制输入的直接联系. 基于文献 [13−14] 在障碍函数理论作出的突破性贡献, CBF 方法也被推广到 ZBF. 由于 ZBF 是当前应用最广泛的障碍函数, 所以在不引起歧义的情况下, CBF 通常指代的就是零点控制障碍函数 (Zeroing control barrier function).

定义 6[13−14]**.** 对于非线性控制系统 (21), 如果函

数 $h:\mathbf{R}^n\to\mathbf{R}$ 连续可微且满足

$$\sup_{u\in\mathbf{R}^m}[L_fh(x)+L_gh(x)u]\geq-\alpha(h(x)) \tag{22}$$

则称该函数为系统 (21) 的 CBF. 在这里, α 是一个局部利普希茨连续的扩展 K 类函数.

显然, 如果 $L_fh(x)\neq0$, 则 $h(x)$ 必然是一个有效的 CBF. 定义集合

$$K_{cbf}(x)=\{u\in\mathbf{R}^m:L_fh(x)+L_gh(x)u+\alpha(h(x))\geq0\} \tag{23}$$

不难发现, 如果 $h(x)$ 是开环系统 (21) 的 CBF, 则对于任意反馈律 $k(x)\in K_{cbf}(x)$, $h(x)$ 同时也是闭环系统 $\dot{x}=f(x)+g(x)k(x)$ 的 ZBF. CBF 的优势在于能够给出反馈控制 u 的可选范围, 而不需要求出 u 的显式表达式. 这个特点有利于将安全性约束通过 CBF 嵌入到反馈律中.

定理 7[13−14]**.** 对于控制系统 (21), 如果 $h(x)$ 是一个有效的 CBF, 则任意的局部利普希茨反馈律 $k(x)\in K_{cbf}(x)$ 均可保证由 (21) 和 $u=k(x)$ 组成的闭环系统是安全的.

可以看出, 上述 CBF 需要满足 $L_gh(x)\neq0$, 才能保证 $K_{cbf}(x)$ 是一个非空集合. 这类 CBF 又被称作具有相对阶 1.

由于控制系统本身的复杂性, 现实中的安全性约束通常不能被这种一阶 CBF 刻画. 近年来, 学术界对高阶 CBF 进行了深入的探索. 例如, 文献 [74] 受到非线性控制中著名的反步设计方法[75] 启发, 提出了一种高阶 CBF 的构造方法. 这种构造方法的实现难度较大, 并且容易造成系统状态在靠近安全集边缘的时候控制幅值过大. 针对上述方法的不足, 文献 [53] 从线性控制理论的角度出发, 提出了另一种指数型的高阶 CBF 构造方法. 随后, 文献 [54−56] 先后提出了时变版本和非线性版本的高阶 CBF. 由于篇幅有限, 本文仅介绍指数型的高阶 CBF. 为引入这个概念, 假设标量函数 $h:\mathbf{R}^n\to\mathbf{R}$ 具有相对阶 r, 即对于任意 $x\in\mathbf{R}^n$, $L_gh(x)=L_gL_fh(x)=\cdots=L_g^{r-2}h(x)=0$ 且 $L_gL_f^{r-1}h(x)\neq0$. 令

$$\nu(x)=\begin{bmatrix}h^{(r-1)}(x)\\h^{(r-2)}(x)\\\vdots\\\dot{h}(x)\\h(x)\end{bmatrix}=\begin{bmatrix}L_f^{r-1}h(x)\\L_f^{r-2}h(x)\\\vdots\\L_fh(x)\\h(x)\end{bmatrix}$$

定义 7[53]**.** 对于控制系统 (21), 如果存在常数 $a_1,\cdots,a_r$ 使得

$$\sup_{u\in\mathbf{R}^m}[L_f^rh(x)+L_gL_f^{r-1}h(x)u]\geq-\lambda^{\mathrm{T}}\nu(x) \tag{24}$$

并且特征方程

$$s^r+a_1s^{r-1}+\cdots+a_{r-1}s+a_r=0 \tag{25}$$

的所有特征根均小于零, 则称 $h(x)$ 为具有相对阶 r 的 CBF. 这里, $\lambda=[a_1,\cdots,a_r]^{\mathrm{T}}$.

令 $p_1,\cdots,p_r$ 为特征方程 (25) 的根. 定义

$$\eta_0(x)=h(x)$$
$$\eta_k(x)=\dot{\eta}_{k-1}+p_k\eta_{k-1}(x)$$

以及集合

$$\mathcal{S}_0=\{x\in\mathbf{R}^n:\eta_0(x)\geq0\}$$
$$\mathcal{S}_k=\{x\in\mathbf{R}^n:\eta_k(x)\geq0\}$$

这里, $k=1,\cdots,r$. 显然, $\mathcal{S}_0=\mathcal{S}$, 并且 $\bigcap_{k=0}^r\mathcal{S}_k\subseteq\mathcal{S}$. 令

$$K_{hocbf}(x)=\{u\in\mathbf{R}^m:L_f^rh(x)+L_gL_f^{r-1}h(x)u+\lambda^{\mathrm{T}}\nu(x)\geq0\} \tag{26}$$

该集合可以理解为在 r 阶 CBF 意义下的控制信号可选范围. 由于 $L_gL_f^{r-1}h(x)\neq0$, $K_{hocbf}(x)$ 必然是一个非空集合.

定理 8[53]**.** 对于控制系统 (21), 如果 $h(x)$ 是一个有效的 r 阶 CBF 并且初始状态满足 $x_0\in\bigcap_{k=0}^r\mathcal{S}_k$, 则任意局部利普希茨 $k(x)\in K_{hocbf}(x)$ 均可保证由 (21) 和 $u=k(x)$ 组成的闭环系统是安全的.

2.2　CLF 和 CBF 的统一设计方案

值得注意, CBF 方法只能保证系统不违反安全性约束, 而实际中的控制系统往往还需要在不违反安全性约束的前提下实现控制目标 (如镇定、跟踪等). 在 CBF 的安全控制框架中, 系统的控制目标通常由 CLF 刻画. 然而, 在实际应用中, 由于系统控制通道往往是给定的, 如何将 CLF 和 CBF 所刻画的反馈信息统一整合到同一个控制器是安全控制的关键, 并且也是一直困扰着障碍函数安全控制方法的难题. 到目前为止, 学术界所采用的统一设计方案可大致分为三种.

第一种是文献 [33−35] 所采用的 BLF 方法. 在该方法中, CLF 和 CBF 被整合到同一个名为 BLF 的标量函数中. BLF 继承了李雅普诺夫函数的正定性质, 能够结合非线性控制中著名的反步设计技术[75] 以解决复杂高阶系统的安全控制问题. 但是, BLF 方法需要被控对象同时具有 CLF 和 CBF. 这一个要求对于某些控制问题来说是苛刻的. 例如, 在自适应巡航问题[12−14] 中, 如果后方车辆所需要调节到

的目标速度大于前方车辆的速度, CLF 和 CBF 约束将无法同时满足.

第二种是文献 [71, 76] 所采用的切换控制方案. 该方法通过监控系统状态到不安全区域的距离, 对 CLF 和 CBF 所确定的候选控制器进行切换. 值得注意, 两个不同的控制器切换会引起控制信号跳变、控制输入幅值过大等现象. 控制信号的跳变将会降低闭环系统的控制品质. 并且, 由于控制系统的执行部件往往具有饱和约束, 控制幅值过大将会导致执行器无法将等量的控制信号传递到被控对象, 从而造成系统违反安全性约束.

第三种是文献 [12] 提出的二次规划 (Quadratic program, QP) 方案. 该方法可以将 CLF 和 CBF 所刻画的反馈信息进行有效整合, 得到一个局部利普希茨连续的反馈控制器, 能够解决控制目标和安全性约束存在冲突时的矛盾关系, 并且可以避免控制信号跳变. 此外, 与传统的模型预测控制方法[77−78] 相比, CLF-CBF-QP 具有更高的实时性, 近年来已经被广泛地应用于机器人控制[22, 79−80]、无人机控制[81−83] 以及自动驾驶[12, 23, 84] 等领域.

由于第三种方法具有众多优点, 并且是当前障碍函数安全控制领域研究最多的方法, 我们在这里将详细地介绍其基本思路. 假设系统 (21) 的控制目标可以由以下 CLF 描述:

$$\inf_{u\in\mathbf{R}^m}\left[L_fV(x)+L_gV(x)u\right]\leq-\sigma(V(x)) \tag{27}$$

其中, $V:\mathbf{R}^n\to\mathbf{R}_{\geq0}$ 为正定、连续可微且径向无界的标量函数, σ 为 K 类函数. 文献 [12] 指出, 可通过以下 QP 把 CLF 和 CBF 描述的反馈信息整合到同一个控制器:

$$v^*(x)=\arg\min_{v=[u^{\mathrm{T}},\,\delta]^{\mathrm{T}}\in\mathbf{R}^{m+1}}v^{\mathrm{T}}v\quad(\mathrm{CLF}-\mathrm{CBF}-\mathrm{QP})$$

$$\text{s.t.}\quad L_fV(x)+L_gV(x)u\leq-\sigma(V(x))+\delta,$$

$$L_fh(x)+L_gh(x)u\geq-\alpha(h(x))$$

在该 QP 问题中, CLF 和 CBF 分别被当作软约束和硬约束. 当 $x(t)$ 在安全集 $\mathcal{S}$ 内部时, $L_gh(x)\neq0$, 因此总存在 u 满足 CLF-CBF-QP 中的 CBF 约束. 并且, 由于松弛变量 δ 的存在, CLF 约束始终能够满足. 综上所述, CLF-CBF-QP 始终存在可行解. 如果 CLF 描述的控制目标和 CBF 描述的安全性约束不冲突, 那么闭环系统将会在不违反安全性约束的情况下, 实现控制目标; 否则, 闭环系统将牺牲控制目标以保证系统不违反安全性约束. 根据文献 [13], 如果 $L_gh(x)\neq0$, 则 CLF-CBF-QP 具有闭式解

$$u^*(x)=-\lambda_1(x)L_gV^{\mathrm{T}}(x)+\lambda_2(x)L_gh^{\mathrm{T}}(x)$$

$$\delta^*(x)=\lambda_1(x)$$

其中,

$$\lambda_1(x)=\begin{cases}0, & G_{12}c_2-G_{22}c_1<0\\ \dfrac{G_{12}c_1-G_{22}c_1}{G_{11}G_{22}-G_{12}G_{21}}, & G_{12}c_2-G_{22}c_1\geq0\end{cases}$$

$$\lambda_2(x)=\begin{cases}0, & G_{21}c_1-G_{11}c_2<0\\ \dfrac{G_{21}c_1-G_{11}c_2}{G_{11}G_{22}-G_{12}G_{21}}, & G_{21}c_1-G_{11}c_2\geq0\end{cases}$$

在这里,

$$c_1(x)=-L_fV(x)$$

$$c_2(x)=L_fh(x)+\alpha(h(x))$$

$$G_{11}(x)=L_gV(x)L_gV^{\mathrm{T}}(x)+1$$

$$G_{12}(x)=-L_gV(x)L_gh^{\mathrm{T}}(x)$$

$$G_{22}(x)=L_gh(x)L_gh^{\mathrm{T}}(x)$$

定理 9[13]**.** 对于非线性控制系统 (21), 如果 $V:\mathbf{R}^n\to\mathbf{R}_{\geq0}$ 是一个局部利普希茨连续的 CLF, $h:\mathbf{R}^n\to\mathbf{R}$ 是一个局部利普希茨连续的 CBF 并满足 $L_gh(x)\neq0$, 则 $u^*(x)$ 和 $\delta^*(x)$ 也是局部利普希茨连续的.

特别地, 如果反馈律 $u=k(x)$ 具有显式表达式, 则可以通过以下 QP 将 CBF 描述的安全性约束嵌入到闭环系统:

$$u^*(x)=\arg\min_{u\in\mathbf{R}^m}\|u-k(x)\|\qquad(\mathrm{CBF}-\mathrm{QP})$$

$$\text{s.t.}\ \ L_fh(x)+L_gh(x)u\geq-\alpha(h(x))$$

在这个意义下, CBF 可看作是一个能够将违反安全性的控制输入过滤掉的 “滤波器”, 而 $u^*(x)$ 则是被 CBF 筛选后最接近 $k(x)$ 的安全控制输入.

现在, 我们以自适应巡航控制为例简要介绍 CLF-CBF-QP 安全控制框架的应用.

例 2[12−14]**.** 假设汽车的动态可以由以下微分方程描述:

$$m\frac{\mathrm{d}v}{\mathrm{d}t}=u-F_r \tag{28}$$

这里, m 为汽车的质量 (kg), v 为汽车的速度 (m/s), u 为车轮的牵引力 (N), F_r 为空气阻力 (N) 并满足

$$F_r=f_0+f_1v+f_2v^2$$

其中, f_0, f_1 及 f_2 为实验测得的常数. 假设汽车在行驶的过程中, 前方有另一辆汽车以 v_0 的速度匀速行驶. 此时, 两车之间的距离可描述为

$$\frac{\mathrm{d}}{\mathrm{d}t}D = v_0 - v$$

自适应巡航控制的目标是控制 u 从而将车速 v 调节至预设的速度 v_d, 并且避免与前方车辆发生碰撞. 显然, (28) 是一个能控的系统. 因此, 在不考虑安全性约束的情况下, 必然存在反馈律 $u = k(x)$ 使得 $v(t) \to v_d$. 注意到安全性约束 $D \geq 0$ 的相对阶为 2, 即需要对 $D(t)$ 进行二阶微分才能得到控制输入 u. 为了解决这个问题, 引入以下约束:

$$D(t) \geq 1.8v(t), \quad \forall t \geq 0 \tag{29}$$

根据文献 [12], (29) 成立意味着 $D(t) \geq 0$. 考虑 CBF 候选函数 $h = D - 1.8v$. 不难发现, $h(x)$ 是一个有效的 CBF. 因此, 如果

$$u^*(x) = \arg\min_{u \in \mathbf{R}^m} \|u - k(x)\|^2 \ \text{ s.t. } \psi_1 + \psi_0 u \geq 0$$

具有可行解, 则 $u = u^*$ 可以解决上述自适应巡航控制问题. 这里, $\psi_1 = v_0 - v + F_r/(2m) + \lambda h$, $\psi_1 = 1/(2m)$, 其中 $\lambda > 0$是待设计参数.

2.3　多约束下的 QP 可行性

上面讨论的 CLF-CBF-QP 只含有单个 CBF 约束. 然而, 现实中的控制系统常常需要同时满足多个安全性约束, 例如无人驾驶汽车需要同时满足不超速、车道间距保持、避障等安全约束. 在这种情况下, 通常需要引入多个 CBF 才能完整地刻画所有安全性约束. 然而, 当多个 CBF 同时耦合在同一个 CLF-CBF-QP 的时候, 将可能导致该 QP 问题不存在可行解.

通过布尔逻辑运算符把多个 CBF 进行组合是一个有效的思路. 例如, 文献 [85] 通过 max/min 运算符对多机器人系统的安全性约束进行布尔组合, 使得机器人编队能够完成预设的协同任务. 针对布尔逻辑组合带来的非光滑特性, 文献 [86] 进一步提出了一套非光滑障碍函数的分析方法. 然而, 非光滑分析是一个较为复杂的过程. 为了解决这个问题, 文献 [87] 利用 max/min 函数的光滑逼近, 提出了另一种组合 CBF 构造方法, 以避免复杂的非光滑分析过程.

分析多个 CBF 的控制共享属性 (Control-sharing property) 是另一种保证 QP 可行性的有效方法[54]. 这种方法的本质思想是检测多个 CBF 所划定的控制输入可选范围是否存在交集. 考虑 CBF

$$\sup_{u \in \mathbf{R}^m} [L_f h_i(x) + L_g h_i(x) u] \geq -\alpha_i(h_i(x))$$

及其划定的控制输入可选范围

$$K_{cbf_i}(x) = \{u \in \mathbf{R}^m : L_f h_i(x) + L_g h_i(x) u + \alpha_i(h_i(x)) \geq 0\}$$

其中, $i = 1, \cdots, q$. 文献 [54] 指出, 如果 $\bigcap_{i=1}^{q} K_{cbf_i}(x)$ 不为空集, 则以下 QP 问题具有可行解:

$$\begin{aligned} u^*(x) = \arg\min_{u \in \mathbf{R}^m} \ & \|u - k(x)\| \\ \text{s.t. } \ & L_f h_1(x) + L_g h_1(x) u \geq -\alpha_1(h_1(x)) \\ & \cdots \\ & L_f h_q(x) + L_g h_q(x) u \geq -\alpha_q(h_q(x)) \end{aligned}$$

特别地, 对于两个 CBF 的特殊情况, 文献 [54] 给出了以下控制共享的充要条件, 并指出相关结果可以推广至多个 CBF.

定理 10[54]**.** 假设系统 (21) 具有 CBF $h_1 : \mathbf{R}^n \to \mathbf{R}$ 和 $h_2 : \mathbf{R}^n \to \mathbf{R}$. 如果以下任意一个条件成立, 则 $K_{cbf_1}(x) \bigcap K_{cbf_2}(x) \neq \emptyset$:

1) $\mathrm{sign}(L_g h_1(x))\mathrm{sign}(L_g h_2(x)) = 1$;
2) 当 $L_g h_1(x) > 0$ 且 $L_g h_2(x) < 0$ 时,
$$L_g h_1(x)[L_f h_2(x) + \alpha_2(h_2(x))] \geq L_g h_2(x)[L_f h_1(x) + \alpha_1(h_1(x))]$$
3) 当 $L_g h_1(x) < 0$ 且 $L_g h_2(x) > 0$ 时,
$$L_g h_1(x)[L_f h_2(x) + \alpha_2(h_2(x))] \leq L_g h_2(x)[L_f h_1(x) + \alpha_1(h_1(x))]$$

值得注意, 上述方法牺牲了安全集的范围以换取 CLF-CBF-QP 的可行性, 在某种程度上具有保守性. 尽管学术界对 CLF-CBF-QP 可行性问题已经进行了相当多的探索, 但目前仍未出现突破性的进展.

2.4　复杂时序逻辑规约下的安全控制

随着系统结构和任务要求的复杂性提高, 利用上层逻辑和下层动力学相结合的系统设计思想正得到越来越多的认可. 时序逻辑是刻画控制系统复杂动态行为的有效工具, 并已经被广泛应用于控制系统安全性的研究上[88]. 然而, 上层时序逻辑约束与底层动力学特性的耦合使得系统成为了混杂系统, 相关的分析和设计理论至今还很欠缺. 因此, 基于该思路的非线性系统安全控制设计仍处于探索阶段, 亟待进一步发展.

近年来, 控制领域的研究者已经开始从模型预测控制[77−78]、非线性优化[89] 以及 CBF-QP[87, 90−91] 等不同的角度进行了许多的研究. CBF-QP 方法的主要思路是利用 CBF 建立上层的时序逻辑约束以及控制系统的动力学特性和反馈控制器的联系, 并通过 QP 确定最终的控制输入. 对于现实中广泛存在的非线性仿射控制系统, CBF 施加在控制器的约束

是线性的. 因此, CBF-QP 拥有比模型预测控制和非线性优化方法更高的求解效率和实时性, 并逐渐获得越来越多学者的关注.

在 CBF-QP 角度, 目前刻画系统动态行为的工具主要包括 LTL 语言和信号时序逻辑语言 (Signal temporal logic, STL[92]) 两种. 在 LTL 方面, 由于障碍函数方法已经在 LTL 约束下的安全性分析取得重大突破[27], 相关的理论成果已经被用于大规模网络化系统[67]、多智能体系统[93]、随机系统[94] 以及机器人[95] 等带有 LTL 约束的非线性系统安全控制设计. 与 LTL 相比, 由于 STL 句法规则带有时间变量, 其结构更加复杂, 相关的安全控制研究进展也较为缓慢. 文献 [87] 指出, STL 中的时序运算符 "always"、"eventually"以及 "until"所刻画的约束信息均可以通过 CBF-QP 传递到控制器, 并给出了对应的 CBF 构造方法. 随后, 文献 [91] 进一步引入事件触发机制, 给出了 STL 约束下机器人集群的安全控制方法.

3 总结与展望

本文简要介绍了基于障碍函数方法的非线性系统安全分析与控制的理论成果. 与现有的安全分析与控制技术相比, 障碍函数方法具有计算高效、鲁棒性强、无需穷举系统行为、能够有效地兼顾控制目标和安全性等优点.

虽然障碍函数已被广泛研究, 但是由于该方法在非线性系统安全分析与控制中起步相对较晚, 目前仍有许多尚待解决的问题. 首先, 构造障碍函数依旧是一个难题. 虽然某些特殊结构的系统 (如多项式系统等) 已经有了解决方案, 但是对于更一般化的非线性系统, 如何寻找最优的障碍函数仍需要进一步探索. 其次, CLF-CBF-QP 可行性是障碍函数安全控制方法的关键. 虽然在单个 CBF 约束的情况下可以引入松弛变量保证其可行性, 但是在多个 CBF 约束下, 不同的 CBF 可能存在冲突从而导致 CLF-CBF-QP 不存在可行解. 在这种情况下, 如何权衡不同 CBF 的优先级以保证 CLF-CBF-QP 的可行性依旧是一个难题. 另外, 为了实现闭环系统的自主性和智能性, 现代控制系统有时需要满足上层单元给定的时序逻辑约束, 而传统控制理论往往只关注鲁棒性、稳定性等底层的动力学或者控制特性. 到目前为止, 对逻辑和物理动态混杂的非线性控制系统的安全分析与控制研究还比较欠缺. 如何将时序逻辑与障碍函数进行多方位融合以提高实际非线性系统的安全控制效率也是未来系统安全性研究的关键.

References

1 Isidori A. *Nonlinear Control Systems*. London: Springer-Verlag, 1995.

2 Khalil H K. *Nonlinear Systems*. Upper Saddle River: Prentice Hall, 2002.

3 Hong Yi-Guang, Cheng Dai-Zhan. *Analysis and Design of Nonlinear Systems*. Beijing: Science Press, 2005.
(洪奕光, 程代展. 非线性系统的分析与控制. 北京: 科学出版社, 2005.)

4 Aubin J P. *Viability Theory*. Boston: Birkhäuser, 1991.

5 Nagumo M. Über die lage der integralkurven gewöhnlicher differentialgleichungen. *Proceedings of the Physico-Mathematical Society of Japan*, 1942, **24**(6): 551–559

6 Clarke E M, Grumberg O, Peleg D. *Model Checking*. Cambridge: MIT Press, 1999.

7 Baier C, Katoen J P. *Principles of Model Checking*. Cambridge: MIT Press, 2008.

8 Tomlin C, Pappas G J, Sastry S. Conflict resolution for air traffic management: A study in multiagent hybrid systems. *IEEE Transactions on Automatic Control*, 1998, **43**(4): 509–521

9 Mitchell I M, Bayen A M, Tomlin C J. A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on Automatic Control*, 2005, **50**(7): 947–957

10 Gao Y, Johansson K H, Xie L. Computing probabilistic controlled invariant sets. *IEEE Transactions on Automatic Control*, 2021, **66**(7): 3138–3151

11 Prajna S. Optimization-based Methods for Nonlinear and Hybrid Systems Verification [Ph.D. dissertation], California Institute of Technology, USA, 2005

12 Ames A D, Grizzle J W, Tabuada P. Control barrier function based quadratic programs with application to adaptive cruise control. In: Proceedings of the 53rd IEEE Conference on Decision and Control (CDC). Los Angeles, CA, USA: IEEE, 2014. 6271–6278

13 Xu X, Tabuada P, Grizzle J W, Ames A D. Robustness of control barrier functions for safety-critical control. *IFAC-PapersOnLine*, 2015, **48**(27): 54–61

14 Ames A D, Xu X, Grizzle J W, Tabuada P. Control barrier function based quadratic programs for safety critical systems. *IEEE Transactions on Automatic Control*, 2017, **62**(8): 3861–3876

15 Annichini A, Bouajjani A, Sighireanu M. TReX: A tool for reachability analysis of the complex systems. In: Proceedings of the International Conference on Computer Aided Verification (CAV). Paris, France: Springer, 2001. 368–372

16 Mitchell I M. A toolbox of level set methods [Online], available: https://www.cs.ubc.ca/~mitchell/ToolboxLS, September 3, 2019

17 Fisac J F, Chen M, Tomlin C J, Sastry S S. Reach-avoid problems with time-varying dynamics, targets and constraints. In: Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control (HSCC). New York, USA: ACM, 2015. 11–20

18 Herbert S L, Chen M, Han S, Bansal S, Fisac J F, Tomlin C J. FaSTrack: A modular framework for fast and guaranteed safe motion planning. In: Proceedings of the 56th IEEE Conference on Decision and Control (CDC). Melbourne, Australia: IEEE, 2017. 1517–1522

19 Bajcsy A, Bansal S, Bronstein E, Tolani V, Tomlin C J. An efficient reachability-based framework for provably safe autonomous navigation in unknown environments. In: Proceedings of the 58th IEEE Conference on Decision and Control (CDC). Nice,

France: IEEE, 2019. 1758−1765

20 Boyd S, Vandenberghe L. *Convex Optimization*. Cambridge: Cambridge University Press, 2004.

21 Glavaski S, Papachristodoulou A, Ariyur K. Safety verification of controlled advanced life support system using barrier certificates. In: Proceedings of the International Workshop on Hybrid Systems: Computation and Control (HSCC). Zurich, Switzerland: Springer, 2005. 306−321

22 Wang L, Ames A D, Egerstedt M. Safety barrier certificates for collisions-free multirobot systems. *IEEE Transactions on Robotics*, 2017, **33**(3): 661−674

23 Xu X, Grizzle J W, Tabuada P, Ames A D. Correctness guarantees for the composition of lane keeping and adaptive cruise control. *IEEE Transactions on Automation Science and Engineering*, 2017, **15**(3): 1216−1229

24 Prajna S, Jadbabaie A. Safety verification of hybrid systems using barrier certificates. In: Proceedings of the International Workshop on Hybrid Systems: Computation and Control (HSCC). Philadelphia, PA, USA: Springer, 2004. 477−492

25 Prajna S, Jadbabaie A, Pappas G J. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 2007, **52**(8): 1415−1428

26 Prajna S, Rantzer A. Convex programs for temporal verification of nonlinear dynamical systems. *SIAM Journal on Control and Optimization*, 2007, **46**(3): 999−1021

27 Wongpiromsarn T, Topcu U, Lamperski A. Automata theory meets barrier certificates: Temporal logic verification of nonlinear systems. *IEEE Transactions on Automatic Control*, 2015, **61**(11): 3344−3355

28 Wisniewski R, Sloth C. Converse barrier certificate theorems. *IEEE Transactions on Automatic Control*, 2015, **61**(5): 1356−1361

29 Ratschan S. Converse theorems for safety and barrier certificates. *IEEE Transactions on Automatic Control*, 2018, **63**(8): 2628−2632

30 Liu J. Converse barrier functions via lyapunov functions. *IEEE Transactions on Automatic Control*, 2021, **67**(1): 497−503

31 Maghenem M A, Sanfelice R G. On the converse safety problem for differential inclusions: Solutions, regularity, and time-varying barrier functions. *IEEE Transactions on Automatic Control*, 2022: 1−16

32 Jankovic M. Robust control barrier functions for constrained stabilization of nonlinear systems. *Automatica*, 2021, **96**: 359−367

33 Ngo K B, Mahony R, Jiang Z P. Integrator backstepping using barrier functions for systems with multiple state constraints. In: Proceedings of the 44th IEEE Conference on Decision and Control (CDC). Seville, Spain: IEEE, 2005. 8306−8312

34 Tee K P, Ge S S, Tay E H. Barrier Lyapunov functions for the control of output-constrained nonlinear systems. *Automatica*, 2009, **45**(4): 918−927

35 Wang X, Lyu Z, Dong Y. A unified approach for safety critical control problem via output regulation theory and barrier function. In: Proceedings of the 41st Chinese Control Conference (CCC). Hefei, China: IEEE, 2022. 833−837

36 Kong H, He F, Song X, Hung W N, Gu M. Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In: Proceedings of the International Conference on Computer Aided Verification (CAV). Saint Petersburg, Russia: Springer, 2013. 242−257

37 Lin Y, Sontag E D, Wang Y. A smooth converse Lyapunov theorem for robust stability. *SIAM Journal on Control and Optimization*, 1996, **34**(1): 124−160

38 Li A, Wang L, Pierpaoli P, Egerstedt M. Formally correct composition of coordinated behaviors using control barrier certificates. In: Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS). Madrid, Spain: IEEE, 2018. 3723−3729

39 Glotfelter P, Cortés J, Egerstedt M. Nonsmooth barrier functions with applications to multi-robot systems. *IEEE Control Systems Letters*, 2017, **1**(2): 310−315

40 Ahmadi M, Singletary A, Burdick J W, Ames A D. Safe policy synthesis in multi-agent pomdps via discrete-time barrier functions. In: Proceedings of the 58th IEEE Conference on Decision and Control (CDC). Nice, France: IEEE, 2019. 4797−4803

41 Sontag E D, Wang Y. On characterizations of the input-to-state stability property. *Systems & Control Letters*, 1995, **24**(5): 351−359

42 Romdlony M Z, Jayawardhana B. On the new notion of input-to-state safety. In: Proceedings of the 55th IEEE Conference on Decision and Control (CDC). Las Vegas, NV, USA: IEEE, 2016. 6403−6409

43 Romdlony M Z, Jayawardhana B. Robustness analysis of systems′ safety through a new notion of input-to-state safety. *International Journal of Robust and Nonlinear Control*, 2019, **29**(7): 2125−2136

44 Kolathaya S, Ames A D. Input-to-state safety with control barrier functions. *IEEE Control Systems Letters*, 2018, **3**(1): 108−113

45 Lyu Z, Xu X, Hong Y. Small-gain theorem for safety verification of interconnected systems. *Automatica*, 2022, **139**: Article No. 110178

46 Krstic M. Inverse optimal safety filters [Online], available: https://arxiv.org/abs/2112.08225, February 20, 2023

47 Taylor A J, Ong P, Cortés J, Ames A D. Safety-critical event triggered control via input-to-state safe barrier functions. *IEEE Control Systems Letters*, 2020, **5**(3): 749−754

48 Long L, Wang J. Safety-critical dynamic event-triggered control of nonlinear systems. *Systems & Control Letters*, 2022, **162**: Article No. 105176

49 Li X, Yin X, Li S. Cooperative event triggered control for multi-robot systems with collision avoidance. In: Proceedings of the 40th Chinese Control Conference (CCC). Shanghai, China: IEEE, 2021. 5460−5465

50 Cortez W S, Dimarogonas D V. Correct-by-design control barrier functions for Euler-Lagrange systems with input constraints. In: Proceedings of the American Control Conference (ACC). Denver, CO, USA: IEEE, 2020. 950−955

51 Shi L, Singh S K. Decentralized adaptive controller design for large-scale systems with higher order interconnections. *IEEE Transactions on Automatic Control*, 1992, **37**(8): 1106−1118

52 Lyu Z, Xu X, Hong Y. Small-gain theorem for safety verification under high-relative-degree constraints [Online], available: https://arxiv.org/abs/2204.04376, February 20, 2023

53 Nguyen Q, Sreenath K. Exponential control barrier functions for enforcing high relative-degree safety-critical constraints. In: Proceedings of the American Control Conference (ACC). Boston, MA, USA: IEEE, 2016. 322−328

54 Xu X. Constrained control of input-output linearizable systems using control sharing barrier functions. *Automatica*, 2018, **87**: 195−201

55 Xiao W, Belta C. High order control barrier functions. *IEEE Transactions on Automatic Control*, 2021: 1−8

56 Tan X, Cortez W S, Dimarogonas D V. High-order barrier functions: Robustness, safety, and performance-critical control. *IEEE Transactions on Automatic Control*, 2021, **67**(6): 3021−3028

57 Parrilo P A. Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization [Ph.D. dissertation], California Institute of Technology, USA, 2000

58 Prajna S, Papachristodoulou A, Parrilo P A. Introducing SOSTOOLS: A general purpose sum of squares programming solver. In: Proceedings of the 41st IEEE Conference on Decision and Control (CDC). Las Vegas, NV, USA: IEEE, 2002. 741–746

59 Papachristodoulou A, Prajna S. A tutorial on sum of squares techniques for systems analysis. In: Proceedings of the American Control Conference (ACC). Portland, OR, USA: IEEE, 2005. 2686−2700

60 Seiler P. SOSOPT: A toolbox for polynomial optimization [Online], available: https://arxiv.org/abs/1308.1889, February 20, 2023

61 Willems J C. Dissipative dynamical systems part I: General theory. *Archive for Rational Mechanics and Analysis*, 1972, **45**(5): 321−351

62 Desoer C A, Vidyasagar M. *Feedback Systems: Input-Output Properties*. New York: Academic Press, 1975.

63 Hill D J. A generalization of the small-gain theorem for nonlinear feedback systems. *Automatica*, 1991, **27**(6): 1043−1045

64 Jiang Z P, Teel A R, Praly L. Small-gain theorem for ISS systems and applications. *Mathematics of Control, Signals and Systems*, 1994, **7**(2): 95−120

65 Teel A R. A nonlinear small gain theorem for the analysis of control systems with saturation. *IEEE Transactions on Automatic Control*, 1996, **41**(9): 1256−1270

66 Huang X, Lyu Z, Hong Y. Safety verification of large-scale nonlinear systems: A cyclic-small-gain approach. In: Proceedings of the 17th International Conference on Control & Automation (ICCA). Naples, Italy: IEEE, 2022. 459−462

67 Jagtap P, Swikir A, Zamani M. Compositional construction of control barrier functions for interconnected control systems. In: Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control (HSCC). New York, USA: ACM, 2000. 1−11

68 Yin X, Li S. Recent advances on formal methods for safety and security of cyber-physical systems. *Control Theory and Technology*, 2020, **18**(4): 459−461

69 Belta C, Yordanov B, Gol E A. *Formal Methods for Discrete-Time Dynamical Systems*. Berlin: Springer, 2017.

70 Tian D, Fang H, Yang Q, Wei Y. Decentralized motion planning for multiagent collaboration under coupled LTL task specifications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2022, **52**(6): 3602−3611

71 Wieland P, Allgöwer F. Constructive safety using control barrier functions. *IFAC Proceedings Volumes*, 2007, **40**(12): 462−467

72 Artstein Z. Stabilization with relaxed controls. *Nonlinear Analysis: Theory, Methods & Applications*, 1983, **7**(11): 1163−1173

73 Sontag E D. A ùniversal′ construction of Artstein′s theorem on nonlinear stabilization. *Systems & Sontrol Letters*, 1989, **13**(2): 117−123

74 Hsu S C, Xu X, Ames A D. Control barrier function based quadratic programs with application to bipedal robotic walking. In: Proceedings of the American Control Conference (ACC). Chicago, IL, USA: IEEE, 2015. 4542−4548

75 Krstic M, Kokotovic P V, Kanellakopoulos I. *Nonlinear and Adaptive Control Design*. New York: Wiley and Sons, 1995.

76 Romdlony M Z, Jayawardhana B. Uniting control Lyapunov and control barrier functions. In: Proceedings of the 53rd IEEE Conference on Decision and Control (CDC). Los Angeles, CA, USA: IEEE, 2014. 2293−2298

77 Wu C, Fang H, Yang Q, Zeng X, Wei Y, Chen J. Distributed cooperative control of redundant mobile manipulators with safety constraints. *IEEE Transactions on Cybernetics*, 2022: 1−13

78 Raman V, Donzé A, Maasoumy M, Murray R M. Model predictive control with signal temporal logic specifications. In: Proceedings of the 53rd IEEE Conference on Decision and Control (CDC). Los Angeles, CA, USA: IEEE, 2014. 81−87

79 Wu S, Liu T, Jiang Z P. Continuous safety control of mobile robots in cluttered environments. *IEEE Robotics and Automation Letters*, 2022, **7**(3): 8012−8019

80 Nguyen Q, Sreenath K. Safety-critical control for dynamical bipedal walking with precise footstep placement. *IFAC-PapersOnLine*, 2015, **48**(27): 147−154

81 Khan M, Zafar M, Chatterjee A. Barrier functions in cascaded controller: Safe quadrotor control. In: Proceedings of the American Control Conference (ACC). Denver, CO, USA: IEEE, 2020. 1737−1742

82 Wang L, Theodorou E A, Egerstedt M. Safe learning of quadrotor dynamics using barrier certificates. In: Proceedings of the IEEE International Conference on Robotics and Automation (ICRA). Brisbane, Australia: IEEE, 2018. 2460−2465

83 Wu G, Sreenath K. Safety-critical control of a 3D quadrotor with range-limited sensing. In: Proceedings of the ASME Dynamic Systems and Control Conference (DSCC). Minneapolis, MN, USA: ASME, 2016. 1−11

84 Xiao W, Mehdipour N, Collin A, Bin-Nun A Y, Frazzoli E, Tebbens R D, et al. Rule-based optimal control for autonomous driving. In: Proceedings of the ACM/IEEE 12th International Conference on Cyber-Physical Systems (ICCPS). New York, NY, USA: ACM/IEEE, 2021. 143−154

85 Glotfelter P, Cortés J, Egerstedt M. Boolean composability of constraints and control synthesis for multi-robot systems via nonsmooth control barrier functions. In: Proceedings of the IEEE Conference on Control Technology and Applications (CCTA). Copenhagen, Denmark: IEEE, 2018. 897−902

86 Glotfelter P, Cortés J, Egerstedt M. A nonsmooth approach to controller synthesis for boolean specifications. *IEEE Transactions on Automatic Control*, 2020, **66**(11): 5160−5174

87 Lindemann L, Dimarogonas D V. Control barrier functions for signal temporal logic tasks. *IEEE Control Systems Letters*, 2018, **3**(1): 96−101

88 Manna Z, Pnueli A. *Temporal Verification of Reactive Systems: Safety*. New York: Springer Verlag, 1995.

89 Tian D, Fang H, Yang Q, Guo Z, Cui J, Liang W, et al. Two-phase motion planning under signal temporal logic specifications in partially unknown environments. *IEEE Transactions on Industrial Electronics*, 2022: 1−10

90 Li X, Serlin Z, Yang G, Belta C. A formal methods approach to interpretable reinforcement learning for robotic planning. *Science Robotics*, 2019, **4**(37): 1−15

91 Gundana D, Kress-Gazit H. Event-based signal temporal logic synthesis for single and multi-robot tasks. *IEEE Robotics and Automation Letters*, 2021, **6**(2): 3687−3694

92 Maler O, Nickovic D. Monitoring temporal properties of continuous signals. *Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems*, 2004: 152−166

93 Huang X, Li L, Chen J. Multi-agent system motion planning under temporal logic specifications and control barrier function. *Control Theory and Technology*, 2020, **18**(3): 269−278

94 Jagtap P, Soudjani S, Zamani M. Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*, 2020, **66**(7): 3097−3110

95 Srinivasan M, Coogan S. Control of mobile robots using barrier functions under temporal logic specifications. *IEEE Transactions on Robotics*, 2020, **37**(2): 363−374

陈 杰 中国工程院院士, 同济大学教授, 北京理工大学自动化学院教授, 自主智能无人系统全国重点实验室教授. 1986 年、1996 年和 2001 年分别获得北京理工大学控制理论与应用专业学士学位、硕士学位和博士学位. 主要研究方向为复杂系统智能控制与优化, 多智能体协同控制.
E-mail: chenjie@bit.edu.cn
(**CHEN Jie** Academician of Chinese Academy of Engineering, professor at Tongji University, School of Automation, Beijing Institute of Technology, and National Key Laboratory of Autonomous Intelligent Unmanned Systems. He received his bachelor, master, and Ph.D. degrees in control science and application from Beijing Institute of Technology in 1986, 1996, and 2001, respectively. His research interest covers intelligent control and optimization of complex systems, and cooperative control of multi-agent systems.)

吕梓亮 同济大学电子与信息工程学院博士研究生. 2017 年和 2020 年分别获得广东工业大学学士和硕士学位. 主要研究方向为非线性系统安全分析与控制.
E-mail: zlyu@tongji.edu.cn
(**LYU Zi-Liang** Ph.D. candidate at the College of Electronic and Information Engineering, Tongji University. He received his bachelor and master degrees from Guangdong University of Technology in 2017 and 2020, respectively. His research interest covers safety analysis and safety-critical control of nonlinear systems.)

黄鑫源 同济大学电子与信息工程学院博士研究生. 2019 年获得同济大学控制科学与工程专业学士学位. 主要研究方向为安全控制和基于形式化方法的控制.
E-mail: xy_huang@tongji.edu.cn
(**HUANG Xin-Yuan** Ph.D. candidate at the College of Electronic and Information Engineering, Tongji University. He received his bachelor degree in control science and engineering from Tongji University in 2019. His research interest covers safety control and formal methods-based control.)

洪奕光 同济大学电子与信息工程学院教授, 自主智能无人系统全国重点实验室教授. 1987 年和 1990 年分别获得北京大学力学系学士和硕士学位, 1993 年获得中科院系统所博士学位. 主要研究方向为复杂系统, 控制理论, 人工智能. 本文通信作者.
E-mail: yghong@tongji.edu.cn
(**HONG Yi-Guang** Professor at College of Electronic and Information Engineering, Tongji University and National Key Laboratory of Autonomous Intelligent Unmanned Systems. He received his bachelor and master degrees from Department of Mechanics of Peking University in 1987 and 1990, respectively, and his Ph.D. degree from Institute of Systems Science of Chinese Academy of Sciences in 1993. His research interest covers complex systems, control theory, and artificial intelligence. Corresponding author of this paper.)