中国科学: 信息科学 2022 年 第 52 卷 第 10 期: 1853–1869
SCIENTIA SINICA Informationis
论文

非正障碍函数: 面向非线性系统状态安全控制的一类新颖障碍函数

朱哲人[1,2], 张新民[1,2], 柴毅[3*], 宋执环[1,2*]

1. 浙江大学控制科学与工程学院, 杭州 310027
2. 工业控制技术国家重点实验室, 杭州 310027
3. 重庆大学自动化学院, 重庆 400044
* 通信作者. E-mail: chaiyi@cqu.edu.cn, songzhihuan@zju.edu.cn

收稿日期: 2021–09–09; 修回日期: 2021–10–14; 接受日期: 2021–11–14; 网络出版日期: 2022–10–10

国家自然科学基金重点项目 (批准号: 61933013, 61633005) 资助

摘要 面向系统状态安全的分析与控制, 是目前控制领域内的热点研究之一. 针对一类具有可行状态集的动态系统, 本文深入讨论障碍函数与状态安全判据之间的相关性, 通过设计一种新颖的障碍函数, 提出了基于障碍函数的状态安全判据, 该状态安全判据可用于此类系统的安全分析、诊断与控制. 受启发于倒数障碍函数与零障碍函数, 本文设计了一类非正障碍函数, 并在此基础上提出了面向可行状态集的动态系统状态安全判据, 通过验证该可行状态集的前向不变性, 从而保证系统的安全性; 根据非正障碍函数, 建立了控制障碍函数, 以此设计面向动态控制系统的状态安全控制器, 保障系统的运行安全. 上述理论与方法在一类连续搅拌釜反应器的安全运行控制中得以应用, 通过仿真验证, 证明了理论与方法的有效性, 实现了基于障碍函数的安全控制理论在过程控制中的首次尝试.

关键词 非正障碍函数, 动态系统, 状态安全控制, 安全性判据, 控制障碍函数

1 引言

目前, 动态系统尤其是工业过程系统的安全研究大多集中在系统的宏观层面, 从业者可以通过分析事故或事件的原因, 利用统计方法计算、估计风险状态转移或事件发生概率, 以确定系统的安全风险等级, 并且已形成了面向系统安全风险的分析、评估和控制方法 [1~6], 状态监测方法 [7~9] 及其他安全分析评价方法等安全性研究体系. 基于上述宏观安全分析和评价方法的安全控制更侧重于决策, 往往会执行暂停运行指令以及相应的应急响应. 因此, 这样的安全控制模式可被称为安全被动防御控制.

实际上, 对于工业过程系统, 我们需要更精细化的、更微观的安全控制策略与手段, 期望可以依靠面向过程变量的底层控制器, 如温度、压力、流量、液位、浓度等控制器, 将安全控制直接作用于

引用格式: 朱哲人, 张新民, 柴毅, 等. 非正障碍函数: 面向非线性系统安全控制的一类新颖障碍函数. 中国科学: 信息科学, 2022, 52: 1853–1869, doi: 10.1360/SSI-2021-0313
Zhu Z R, Zhang X M, Chai Y, et al. Non-positive barrier function: a new notion of barrier function for state-safety control of nonlinear dynamical systems (in Chinese). Sci Sin Inform, 2022, 52: 1853–1869, doi: 10.1360/SSI-2021-0313

系统的运行状态, 实现 “主动安全控制 (active safety control, ASC)”. 我们所期望的主动安全控制, 应具有和稳定性控制类似的控制方式, 可以通过控制系统状态的动态变化轨迹, 将系统的状态运动约束在允许范围内; 且即使事件恶化使安全不可控, 也可以为系统宏观层面的安全决策赢得更多的可用时间. 因此, 主动安全控制的关键便是如何使状态 “安全化” 且保持 “安全化”. 类似于状态运动稳定性与 Lyapunov 函数的紧密联系, 障碍函数 (barrier function) 的提出便是为了建立状态与安全之间的纽带, 便于分析和诊断状态运动安全性、实现系统安全的安全化.

受启发于 Lyapunov 函数, Prajna 等 [10, 11] 最早提出障碍函数及其相应安全理论, 依靠初始状态集、不安全状态集等, 创造性地使用状态轨迹运动、微分方程等来注释系统安全问题. 自该项成果起, 状态安全分析、诊断与控制等方面的问题正逐渐转化为我们熟悉和擅长解决的问题. 之后, Kong 等 [12]、Dai 等 [13]、Sogokon 等 [14]、Wang 等 [15, 16]、Zhu 等 [17~19] 对基于障碍函数的安全性理论体系的壮大作出了大量贡献, 极大地丰富了可用安全判据的种类与数量. 此外, Wieland 等 [20] 将障碍函数拓展性地应用于安全控制, 并形成了控制障碍函数. Romdlony 等 [21~24] 也作出了重要贡献, 提出了一些具有重要意义的开创性理论成果, 这些成果涉及安全且稳定控制 (stabilization with guaranteed safety)、输入到状态安全 (input-to-state safety) 以及使用路径积分构建障碍函数等多个方面.

基于障碍函数的安全理论还存在另一个体系分支 [25~32]. Ames 等 [25, 31] 为该分支理论的奠基者, 他们设计了一种倒数障碍函数 (reciprocal barrier function), 该倒数障碍函数的构建仅取决于系统的安全状态集 $\mathcal{C}$, 并不需要参照不安全状态集. 且 Ames 创造性地提出了通过验证集合 $\mathcal{C}$ 的前向不变性来判定系统安全性的方法体系. 在此基础上, Xu 等 [26] 建立了零障碍函数 (zeroing barrier function), 并基于零障碍函数讨论了状态安全鲁棒性. 随后, 学者们 [27~30, 32] 将倒数障碍函数与零障碍函数应用于机器人及多机器人系统的安全控制.

如上所述, 目前障碍函数及其安全理论与应用方面的研究成果主要集中在安全控制方面的纯理论研究与机器人及多智能体系统的应用. 亟需拓展基于障碍函数的安全控制理论的新应用领域. 本文旨在探索将障碍函数应用于实现工业过程系统安全化的可能性. 然而, 相较于具有明显不可达或不可触及的实际物理区域或范围的 (多) 智能体运动控制场景, 对于大多数实际工业过程系统, 由于故障、性能退化等复杂机制, 难以获得过程系统完整且精确的不安全状态集. 但可以利用大量历史数据, 通过运用合适的学习算法, 构建出一个正常运行状态集, 且集合中的每一个状态都是已知能够保证系统良好运行的状态. 如果能通过控制将系统的运行状态束缚在此状态集内, 便能保证系统的长期安全运行.

显然, 在已知安全状态集的情况下, 倒数障碍函数 [25] 与零障碍函数 [26] 是当前的优选. 此外, 由于一般障碍函数 [13] 在设计用于系统安全性分析、诊断与控制的障碍函数时并不具有便捷性, 因此, 倒数障碍函数和零障碍函数是现存最兼顾可用性与通用性的障碍函数. 同时, 在 Ames 的理论框架下状态安全问题可直接转化为集合前向不变性的验证问题, 无需再计算系统可达集 (通常, 系统可达集的计算是一项较为艰巨的任务) [31], 并且还具有一种非常巧妙的设定即状态在集合边界时其对应障碍函数的单调性会发生反转. 因此, 本文试图在现有倒数障碍函数和零障碍函数的基础上, 探讨是否还存在一种具有更弱约束的障碍函数, 进一步松弛障碍函数对状态在集合 $\mathcal{C}$ 内部运动行为的约束, 并将其应用于安全控制. 本文的具体贡献如下.

(1) 借鉴于 $\mathcal{K}$ 类函数 (class $\mathcal{K}$ function), 构建了两种连续严格减函数 $\mathcal{D}_1$ 类函数与 $\mathcal{D}_2$ 类函数, 明确了函数的定义与一些基本函数性质, 为设计障碍函数奠定基础.

(2) 提出了一种非正障碍函数 (non-positive barrier function). 由于倒数障碍函数在集合边界上的取值趋于无穷且集合外的取值没有明确定义, 导致倒数障碍函数在边界附近对安全的监测性较弱; 零障碍函数对状态运动行为的约束仍具有弱化空间. 为弥补上述不足, 本文设计了一种新颖的障碍函数

并命名为非正障碍函数. 通过推理与分析, 非正障碍函数对状态在集合内部的运动约束比零障碍函数更松弛, 且对比零障碍函数和倒数障碍函数, 罗列了非正障碍函数的优势.

(3) 针对一类过程系统首次提出了基于障碍函数的安全控制方案. 根据非正障碍函数, 设计了相应的控制障碍函数, 并将其应用于连续搅拌釜反应器 (continuous stirred tank reactor, CSTR) 系统中, 将温度控制在非线性连续搅拌釜反应器的可用范围内, 保证 CSTR 系统反应器的温度安全.

本文共分为 7 节. 第 2 节主要陈列相关状态安全与数学方面的基础知识. 第 3 节为 $\mathcal{D}_1$ 类函数与 $\mathcal{D}_2$ 类函数的设计. 第 4 节为本文的核心章节: 构建非正障碍函数以及制定基于非正障碍函数的状态安全判据. 在此基础上, 在第 5 节中将非正障碍函数扩展为控制障碍函数, 并使用控制障碍函数设计相应的状态安全控制律以实现系统状态的安全化. 第 6 节为基于非正障碍函数在 CSTR 系统中的仿真应用. 而最后一节总结了现有工作并展望了未来的研究与发展.

2 基础知识

符号与注释: 假设 $\mathcal{C}$ 表示某个系统状态集合, 则 $\mathcal{C}$ 的内部与边界可分别被标记为 $\mathrm{Int}(\mathcal{C})$ 与 $\partial\mathcal{C}$. 如果连续函数 f 在点 x 是局部 Lipschitz 的, 则存在有限大正实常数 L 与 ϵ 使得对于任意 $\|x-x'\|\leqslant\epsilon$, $\|f(x)-f(x')\|\leqslant L\|x-x'\|$ 都成立. 根据文献 [25], 假设系统 $\dot{x}=f(x)$ 是局部 Lipschitz 的, 对于任意初始状态 $x_0\in\mathbb{R}^n$, 存在一个最大时间间隔 $I(x)=[0,\tau_{\max})$, 使得 $x(t)$ 是系统在 $I(x_0)$ 上的唯一状态解; 因此, 当 f 是前向完备的 (forward complete), 则有 $\tau_{\max}=\infty$. 而如果对于所有 $t\in I(x)$, 所有状态 x 都满足 $x\in\mathcal{C}$, $x(t)\in\mathcal{C}$, 则集合 $\mathcal{C}$ 是前向不变的 (forward invariant). 此外, 还有 3 个关于 $\mathcal{K}$ 类函数、$\mathcal{K}_\infty$ 类函数和 $\mathcal{KL}$ 类函数的重要定义 [33]: 如果一个连续函数 $\alpha:[0,a)\to[0,\infty)$ 是严格增函数且 $\alpha(0)=0$, 则可被称为属于 $\mathcal{K}$ 类函数; 如果当 $a=\infty$ 有 $r\to\infty$ 使得 $\alpha(r)\to\infty$, 则该函数可被称为属于 $\mathcal{K}_\infty$ 类函数. 如果一个连续函数 $\beta:[0,a)\times[0,\infty)\to[0,\infty)$, 当 s 固定时 $\beta(r,s)$ 是关于 r 的 $\mathcal{K}$ 类函数; 且当 r 固定时, $\beta(r,s)$ 是关于 s 的减函数且有 $s\to\infty$ 使得 $\beta(r,s)\to0$, 则可称该函数属于 $\mathcal{KL}$ 类. 另还有一种扩展 $\mathcal{K}$ 类函数 [26]: 对于 $a,b>0$, 如果一连续函数 $\beta:(-b,a)\to(-\infty,\infty)$ 是严格增函数且 $\beta(0)=0$, 则可称该函数属于扩展 $\mathcal{K}$ 类函数.

定义1 给定一个自治系统 $\dot{x}=f(x),x(t_0)=x_0\in\chi_0\subset\mathbb{R}^n$, 其中 $x(t)\in\mathbb{R}^n$. 该系统具有一个不安全状态 $\chi_u\subset\mathbb{R}^n$, 且满足 $\chi_0\cap\chi_u=\emptyset$. 则如果对于所有 $t\geqslant t_0$, 系统状态解 $x(t)$ 都满足 $x(t)\notin\chi_u$, 则系统是状态安全的 [21].

根据定义 1, 可以通过计算状态解到不安全状态集的可达性验证系统是否处于状态安全, 由此形成了始于 Prajna 的分支理论 [10~24]. 而在引言中提及的另一理论分支 [25~32], 根据如下定义 2, 另辟一条面向系统状态安全验证的求解思路, 并降低计算量.

定义2 给定一个自治系统 $\dot{x}=f(x),x(t_0)=x_0$ 具有一个可行安全状态集 $\mathcal{C}\subset\mathbb{R}^n$, 且满足 $x_0\in\mathcal{C}$. 如果可得证集合 $\mathcal{C}$ 是前向不变的, 则此自治系统是状态安全的 [25].

本文的研究内容是基于定义 2 展开的.

3 $\mathcal{D}_1$ 类和 $\mathcal{D}_2$ 类函数设计

为了便于第 3 节的障碍函数构建及对其属性的描述, 本文在 $\mathcal{K}$ 类和 $\mathcal{K}_\infty$ 类函数定义的基础上, 注释了几个新的函数定义及相应函数的基本性质、规则, 从而设计了两类新函数. 为了简便, 将本节中出现的常数 a 统一设定为 $a>0$.

定义3 如果一连续函数 $\alpha:[0,a)\to(-\infty,0]$ 是严格减函数且 $\alpha(0)=0$, 则可称该函数属于 $\mathcal{D}_1$ 类函数. 且如果 $a=\infty$ 有 $\theta\to\infty$ 使得 $\alpha(\theta)\to-\infty$, 则该函数可被认为属于 $\mathcal{D}_1^\infty$ 类函数.

定义4 如果一连续函数 $\alpha:(-a,0]\to[0,\infty)$ 是严格减函数且 $\alpha(0)=0$, 则可称该函数属于 $\mathcal{D}_2$ 类函数. 且如果 $a=\infty$ 有 $\theta\to-\infty$ 使得 $\alpha(\theta)\to\infty$, 则可称该函数属于 $\mathcal{D}_2^\infty$ 类函数.

例1 这里, 我们用以下几个小例子来解释上述定义 3 与 4.

• 现有一个 $\mathcal{K}$ 类函数 β, 其定义域为 $[0,a)$. 显然易见, 新函数 $-\beta$ 属于 $\mathcal{D}_1$ 类函数.

• 函数 $\alpha(\theta)=1-e^\theta$, 因为 $\alpha'(\theta)=-e^\theta<0$, 所以该函数严格减. 因此, 属于 $\mathcal{D}_1$ 类函数. 且由于 $\lim_{\theta\to\infty}\alpha(\theta)=-\infty$, 该函数还属于 $\mathcal{D}_1^\infty$ 类函数.

• 现有函数 $\alpha(\theta)=\frac{1}{1+\theta}-1$, 因为 $\alpha'(\theta)=-\frac{1}{(1+\theta)^2}<0$, 所以该函数是严格减的. 因此, 该函数属于 $\mathcal{D}_1$ 类函数. 然而, 由于 $\lim_{\theta\to\infty}\alpha(\theta)=-1$, 该函数不属于 $\mathcal{D}_1^\infty$ 类函数.

• 现有函数 $\alpha(\theta)=\sqrt{-\theta}-\theta$, 因为 $\alpha'(\theta)=-\frac{1}{2}(-\theta)^{-\frac{1}{2}}-1<0$, 所以该函数严格减. 因此, 属于 $\mathcal{D}_2$ 类函数. 并且由于 $\lim_{\theta\to\infty}\alpha(\theta)=\infty$, 该函数还属于 $\mathcal{D}_2^\infty$ 类函数.

引理1 设函数 α_1 是定义域在 $[0,a)$ 上的一个 $\mathcal{D}_1$ 类函数, 函数 α_2 是定义域在 $(-a,0]$ 上的一个 $\mathcal{D}_2$ 类函数, 函数 α_3 是定义域在 $[0,a)$ 上的一个 $\mathcal{D}_1^\infty$ 类函数, 函数 α_4 是定义域在 $(-a,0]$ 上的一个 $\mathcal{D}_2^\infty$ 类函数, 函数 β 是定义域在 $[0,a)$ 上的一个 $\mathcal{K}$ 类函数. 且将 α_i^{-1} 标记为 α_i 的反函数. 于是, 可得

- α_1^{-1} 被定义在 $(\alpha_1(a),0]$ 上, 属于 $\mathcal{D}_2$ 类函数; α_2^{-1} 被定义在 $[0,\alpha_2(-a))$ 上, 属于 $\mathcal{D}_1$ 类函数;
- α_3^{-1} 被定义在 $(-\infty,0]$ 上, 属于 $\mathcal{D}_2^\infty$ 类函数; α_4^{-1} 被定义在 $[0,\infty)$ 上, 属于 $\mathcal{D}_1^\infty$ 类函数;
- $\alpha_2\circ\alpha_1$ 属于 $\mathcal{K}$ 类函数; $\alpha_4\circ\alpha_3$ 属于 $\mathcal{K}_\infty$ 类函数;
- $\beta\circ\alpha_2$ 属于 $\mathcal{D}_2$ 类函数,

其中, $\alpha_i\circ\alpha_j$ 被标记为如下函数运算关系, $\alpha_i\circ\alpha_j(\theta)=\alpha_i(\alpha_j(\theta))$.

注释1 根据定义 3 与 4, 通过对函数的单调性、定义域与值域的变换计算, 便可轻易证得引理 1. 而引理 1 对非正障碍函数的行为约束设计至关重要.

4 非正障碍函数与安全判据

4.1 研究动机

现有一动态系统如式 (1) 所描述, 该系统已知一个唯一的状态集, 且状态集内的状态都为系统可安全运行的状态.

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

其中, $x(t)\in\mathbb{R}^n$, 且函数 f 是局部 Lipschitz 的. 系统 (1) 的唯一状态集可被记为 $\mathcal{C}\subseteq\mathbb{R}^n$. 此外, 由于对不安全状态集的未知, 根据 [17, Definition 5], 这里集合 $\mathcal{C}$ 的严格性是大于等于真实安全状态集 $\mathcal{S}$ 的, 即 $\mathcal{C}\subseteq\mathcal{S}$. 因此, 如果系统状态解 $x(t)$ 始终 "囚" 在集合 $\mathcal{C}$ 内, 则系统将持续保持安全.

所以, 本文的主要目的是探索能使系统保持安全的条件, 即此条件能保证系统 (1) 的状态集 $\mathcal{C}$ 是前向不变的. 本文将沿用倒数障碍函数 [25,31] 对集合 $\mathcal{C}$ 的基础设定. 集合 $\mathcal{C}$ 必须遵循:

$$\mathcal{C}=\{x\in\mathbb{R}^n:h(x)\geqslant 0\}, \tag{2}$$

$$\partial\mathcal{C}=\{x\in\mathbb{R}^n:h(x)=0\}, \tag{3}$$

$$\mathrm{Int}(\mathcal{C})=\{x\in\mathbb{R}^n:h(x)>0\}, \tag{4}$$

其中, 函数 $h:\mathbb{R}^n\to\mathbb{R}$ 是连续可微的, 也可称为是光滑的.

回顾倒数障碍函数 [25], 它必须满足两个重要的性质:

$$\inf_{x\in\mathrm{Int}(\mathcal{C})}B(x)>0,\quad \lim_{x\in\partial\mathcal{C}}B(x)=\infty.$$

然而, 倒数障碍函数的第 2 条性质 $\lim_{x\in\partial\mathcal{C}}B(x)=\infty$存在弱势之处. 根据文献 [25] 设定的条件, 可知 $B(x)$ 是标量函数, 当状态解 $x(t)$ 处于即将穿越 $\partial\mathcal{C}$ 并准备逃离集合 $\mathcal{C}$ 时, $B(x)=\infty$. 这导致在实际情景下使用倒数障碍函数来观测系统 (1) 的当前状态是否处于安全时, 无穷大的取值并不受人青睐, 容易产生安全员或操作员的安全焦虑.

当然, 上述情况并不会发生在系统稳态运行过程中. 但当系统处于退化过程或出现故障时, 系统性能退化或故障, 会导致系统状态描述发生改变, 这意味着系统 (1) 中的函数 f 更新为函数 $\bar{f}$ 后, $\bar{f}$ 不一定能继承原有函数的性质, 使得所设计的障碍函数不具有安全预警的作用. 因此, 必须使 $B(x)$ 在 $x\in\partial\mathcal{C}$ 时的取值设定为某个准确的数值, 如 0. 这一点是零障碍函数 [26] 的优势. 但零障碍函数由于考虑了安全鲁棒性, 构造了 $\dot{h}(x)\geqslant-\beta(h)$, 其中, 函数 β 是一个扩展 $\mathcal{K}$ 类函数. 根据扩展 $\mathcal{K}$ 类函数的性质, 可以发现零障碍函数至少无法包含 $\dot{h}(x)\geqslant-h^{2k}(x)$ (k 为正整数) 的情况. 显然, $h^{2k}(x)$ 是关于 h 的一个 $\mathcal{K}$ 类函数. 但根据条件 $\dot{h}(x)\geqslant-h^{2k}(x)$ (k 为正整数) 亦可证明集合 $\mathcal{C}$ 是前向不变的. 因此, 存在下述可能性, 即在零障碍函数的基础上进一步探索并获取使用范围更广且同时兼具易操作性的新的障碍函数.

新问题是如何设计这样的障碍函数, 从而能够保证系统状态解在初始状态满足 $x(t_0)\in\mathrm{Int}(\mathcal{C})$ 的前提下始终保持在集合 $\mathcal{C}$ 内. 本小节中, 系统仍可用 (1) 描述, 且集合 $\mathcal{C}$ 仍旧遵循 (2)∼(4), 其伴随函数 $h:\mathbb{R}^n\to\mathbb{R}$ 是连续可微的. 令

$$B(x)=H(h(x)),\tag{5}$$

但必须保证式 (5) 满足 $\sup_{x\in\mathrm{Int}(\mathcal{C})}B(x)<0$, $\lim_{x\in\partial\mathcal{C}}B(x)=0$. 本小节将障碍函数的值域设为 $(-\infty,0]$ 的目的为: 一是为区别于 Lyapunov 函数, 以防使用者将两类函数混淆; 二是对于从负增长到 0, 该增长过程更具有安全警示作用. 参照 $\dot{B}\leqslant-\gamma B$ [12, 17] 的基础形式, 本小节期望能设计出一个更为松弛的条件, 且该条件能够允许: 当状态解 $x(t)$ 离边界 $\partial\mathcal{C}$ 较远时障碍函数 B 的值能在一定范围内处于增长状态; 当状态解接近 $\partial\mathcal{C}$ 时, 障碍函数 B 的值趋近于零, 使得状态解不会穿越边界 $\partial\mathcal{C}$ 逃离由式 (2)∼(4) 定义的集合 $\mathcal{C}$. 具体形式如下:

$$\dot{B}\leqslant\gamma F(B),\quad \gamma>0.\tag{6}$$

为使由式 (5) 和 (6) 构成的障碍函数能够保证集合的不变性, 标量函数 $H:\mathbb{R}\to\mathbb{R}$ 和 $F:\mathbb{R}\to\mathbb{R}$ 应具有何种性质? 具体研究如 4.2 小节.

4.2 障碍函数与判据

根据定义 2, 可知系统的状态安全性等价于系统安全状态集的前向不变性. 如果能够找到 4.1 小节中标量函数 $H:\mathbb{R}\to\mathbb{R}$ 和 $F:\mathbb{R}\to\mathbb{R}$ 性质与集合前向不变性间的联系与内在机理规律, 便能保证当存在这样的障碍函数时集合便是前向不变的. 同时, 还需要所构建的障碍函数能兼顾一般性与易操作性.

定义5 现有一动态系统 (1), 该系统具有由式 (2)∼(4) 定义的安全状态集 $\mathcal{C}$ 且其伴随函数 $h:\mathbb{R}^n\to\mathbb{R}$ 连续可微. 如果存在局部 Lipschitz 的 $\mathcal{D}_1$ 类函数 α_1 和 α_2 (且 $-\frac{\partial\varphi(r)}{\partial r}$ 等于正实常数 m 或属

于 $\mathcal{D}_2$ 类函数, $\varphi=\alpha_i^{-1}, i=1,2$), 以及一个局部 Lipschitz 的 $\mathcal{K}$ 类函数 δ, 使得对于 $\forall x\in \mathrm{Int}(\mathcal{C})$, 都有不等式 (7) 与 (8), 那么函数 $B:\mathcal{C}\to\mathbb{R}$ 则可被认为是集合 $\mathcal{C}$ 的一个非正障碍函数:

$$\alpha_1(h(x))\leqslant B(x)\leqslant \alpha_2(h(x)), \tag{7}$$

$$\dot{B}\leqslant \lambda(t)\,\delta(h(x)), \tag{8}$$

其中, $\lambda(t)\in\mathbb{R}$ 是一个关于时间 t 的连续可微函数, 且函数 λ 有界满足 $|\lambda|\leqslant c$ ($c>0$ 为常数), 但单调性未知.

通过条件 (7) 可以使障碍函数 B 在行为上近似于满足如下基本性质的函数 α (α 为 $\mathcal{D}_1$ 类函数):

$$\sup_{x\in\mathrm{Int}(\mathcal{C})}\alpha(h(x))<0,\quad \lim_{x\in\partial\mathcal{C}}\alpha(h(x))=0.$$

并且条件 (8) 允许当状态解接近 $\partial\mathcal{C}$ 时障碍函数 B 趋于零, 当状态解远离 $\partial\mathcal{C}$ 时障碍函数 B 的值可以增大或减小.

定理1 给定系统 (1) 具有一个满足条件 (2)~(4) 的 $\mathcal{C}\subseteq\mathbb{R}^n$, 如果存在一个由定义 5 定义的非正障碍函数 $B:\mathcal{C}\to\mathbb{R}$, 则该集合 $\mathcal{C}$ 是前向不变的.

在开始定理 1 证明之前, 首先有必要建立如下引理.

引理2 有这样一个动态系统:

$$\dot{y}=\delta(\alpha(y)), \tag{9}$$

其中, $y_0=y(t_0)$, δ 是局部 Lipschitz 的 $\mathcal{K}$ 类函数, 以及 α 是局部 Lipschitz 的 $\mathcal{D}_2$ 类函数且满足 $-\frac{\partial\alpha(y)}{\partial y}$ 等于正实常数 m 或为一个 $\mathcal{D}_2$ 类函数 ϕ. 对于所有 $y_0\in(-\infty,0)$, $\forall t\in[t_0,\infty)$, 系统 (9) 只有一个唯一解, 且为

$$y(t)=\alpha^{-1}(\sigma(\alpha(y_0),t-t_0)), \tag{10}$$

其中, σ 是 $\mathcal{KL}$ 类函数, α^{-1} 是 α 的反函数.

证明 令 $z=\alpha(y)$, 则有 $\dot{z}=\frac{\partial\alpha(y)}{\partial y}\dot{y}=\frac{\partial\alpha(y)}{\partial y}\delta(\alpha(y))=\frac{\partial\alpha(y)}{\partial y}\delta(z)$. 已知 $-\frac{\partial\alpha(y)}{\partial y}$ 等于正实常数 m 或为一个 $\mathcal{D}_2$ 类函数 ϕ, 现分两类情况进行讨论.

(1) 当 $\frac{\partial\alpha(y)}{\partial y}=-m$ 时, 则可得

$$\dot{z}=-m\delta(z)\overset{\mathrm{def}}{=}-\bar{\delta}_1(z). \tag{11}$$

由于 δ 是 $\mathcal{K}$ 类函数, 则新定义函数 $\bar{\delta}_1$ 也为 $\mathcal{K}$ 类函数.

(2) 当 $\phi=-\frac{\partial\alpha(y)}{\partial y}$ 时, 则可得

$$\dot{z}=-\left[\phi\circ\alpha^{-1}(z)\right]\delta(z)\overset{\mathrm{def}}{=}-\bar{\delta}_2(z). \tag{12}$$

由于 ϕ 和 α 都属于 $\mathcal{D}_2$ 类函数, 根据引理 1, 可得 α^{-1} 属于 $\mathcal{D}_1$ 类函数, 则有 $\phi\circ\alpha^{-1}$ 是 $\mathcal{K}$ 类函数. 由于 $\delta(z)$ 是 $\mathcal{K}$ 类函数, 这使得 $\bar{\delta}_2(z)=\left[\phi\circ\alpha^{-1}(z)\right]\delta(z)$ 也是一个 $\mathcal{K}$ 类函数.

因此, 综合 (11) 与 (12), 最终可得一个统一表达式: $\dot{z}=-\bar{\delta}(z)$, 其中 $\bar{\delta}$ 属于 $\mathcal{K}$ 类函数. 根据 [33, Lemma 4.4], 可得 $z(t)=\sigma(z_0,t-t_0)$. 其中, σ 属于 $\mathcal{KL}$ 类函数. 通过代入 $y=\alpha^{-1}(z)$, 最终可得 $y(t)=\alpha^{-1}(\sigma(\alpha(y_0),t-t_0))$.

现在便可求证定理 1 是否能使非正障碍函数保证集合 $\mathcal{C}$ 具有前向不变性.

定理 1 的证明 由于 $\lambda(t)$ 取值不确定, 证明过程将分为 3 个部分.

(1) $\lambda(t)<0$. 因为 $\lambda(t)<0$, 由 (8), 可得 $\dot{B}\leqslant\lambda(t)\delta\circ\alpha_2^{-1}(-B)<0$. 因此, 对于所有 $t\geqslant t_0$, 都有 $B(x(t))<B(x(t_0))<0$. 由此, 根据 (7), 可推得 $\forall t\in I(x(t_0))$, $h(x(t))>h(x(t_0))>0$. 所以, $\forall t\in I(x(t_0))$, 有 $x(t)\in\mathcal{C}$. 因此, 集合 $\mathcal{C}$ 是前向不变的.

(2) $\lambda(t)>0$. 因为 $\lambda(t)>0$ 且 $|\lambda|\leqslant c$ ($c>0$ 为常数), 所以, 由不等式 (8), 可得, $\dot{B}\leqslant\lambda(t)\delta(h(x))\leqslant c\delta(h(x))$. 由于 δ 是一 $\mathcal{K}$ 类函数, 所以, $\bar{\delta}\overset{\text{def}}{=}c\delta$ 也属于 $\mathcal{K}$ 类函数. 重新整理不等式 (8), 可得, $\dot{B}\leqslant\bar{\delta}\left(\alpha_2^{-1}(B)\right)$. 其中, α_2^{-1} 是 α_2 的反函数. 根据引理 1, 可得 α_2^{-1} 是一 $\mathcal{D}_2$ 类函数. 令 $\alpha_3(B)=\alpha_2^{-1}(B)$, 因此 α_3 也是一个 $\mathcal{D}_2$ 类函数. 于是, 有 $\dot{B}\leqslant\bar{\delta}(\alpha_3(B))$. 根据比较引理 (comparison Lemma) [33] 以及引理 2, 对于所有 $t\in I(x(t_0))$, 都有 $B(x(t))\leqslant\alpha_3^{-1}(\sigma(\alpha_3(B(x(t_0))),t-t_0))$. 因此, 根据不等式 (7), 可得 $\alpha_1(h(x))\leqslant\alpha_3^{-1}(\sigma(\alpha_3(B(x(t_0))),t-t_0))$. 最终, 对于所有 $t\in I(x(t_0))$, 都可推得

$$h(x(t))\geqslant\alpha_1^{-1}\left(\alpha_3^{-1}(\sigma(\alpha_3(B(x(t_0))),t-t_0))\right). \tag{13}$$

因为 α_1^{-1} 与 α_3 属于 $\mathcal{D}_2$ 类函数, α_3^{-1} 属于 $\mathcal{D}_1$ 类函数, σ 属于 $\mathcal{KL}$ 类函数, 所以, 如果系统的初始状态满足 $x(t_0)\in\mathrm{Int}(\mathcal{C})$ with $B(x(t_0))<0$, 则不等式 (13) 表明 $\forall t\in I(x(t_0)),h(x(t))\geqslant 0$. 因此, $\forall t\in I(x(t_0)),x(t)\in\mathcal{C}$ 成立. 所以集合 $\mathcal{C}$ 是前向不变的.

(3) $\lambda(t)\in\mathbb{R}$. 由定义 5 可知, $|\lambda|\leqslant c(c>0)$. 因此, 在假设 (3) 下, 有 $-c\leqslant\lambda(t)\leqslant c$. 由于 $\lambda(t)$ 是连续可微函数, 存在一组时间 $t_1,t_2,\ldots$ 使得 $\forall i\in N_+$, 有 $\lambda(t_i)=0$ 并且 $\mathrm{sgn}(\lambda(p))\cdot\mathrm{sgn}(\lambda(q))=-1$, 其中 $p\in(t_i,t_{i+1})$, $q\in(t_{i+1},t_{i+2})$. 根据假设 (1) 和 (2) 的证明, 对于任意时间间隔 $[t_i,t_{i+1})$ 与 $[t_{i+1},t_{i+2})$, 集合 $\mathcal{C}$ 都能保持前向不变.

因此, 在 $\lambda(t)$ 是连续可微标量函数且满足 $|\lambda|\leqslant c$ (实常数 $c>0$ 有限大) 的假设下, 集合 $\mathcal{C}$ 始终是前向不变的. 因此, 定理 1 成立.

本质上, 非正障碍函数是在零障碍函数上的一种扩展. 两者之间的具体联系与区别, 将在 4.3 小节重点讨论. 下述例 2 示意了非正障碍函数在安全分析中的使用.

例2 考虑如下一个简单的一阶非线性系统:

$$\dot{x}=(1+x_u-x)\ln(x_u-x(t)),\quad x(t_0)=x_0, \tag{14}$$

其中, x_u 是一个正实数. 这里, 设集合 $\mathcal{C}$ 满足

$$\mathcal{C}=\{x\in\mathbb{R}:x\leqslant x_u\}, \tag{15}$$

$$\partial\mathcal{C}=\{x\in\mathbb{R}:x=x_u\}, \tag{16}$$

$$\mathrm{Int}(\mathcal{C})=\{x\in\mathbb{R}:x<x_u\}. \tag{17}$$

因此, $h(x)=x_u-x$. 假设 $x_0\in\mathrm{Int}(\mathcal{C})$, 于是, 构建 $B(x)$ 为

$$B(x)=-\ln(1+x_u-x). \tag{18}$$

因此有 $B(x)=-\ln(1+h(x))$, 而 $\alpha_1(r)=-\ln(1+r)$ 在定义域 $[0,a)$ 上是 $\mathcal{D}_1$ 类函数. 并且,

$$\dot{B}=\frac{\partial B}{\partial x}\dot{x}=\frac{\partial B}{\partial x}f(x)=\frac{f(x)}{1+x_u-x}=\ln(x_u-x). \tag{19}$$

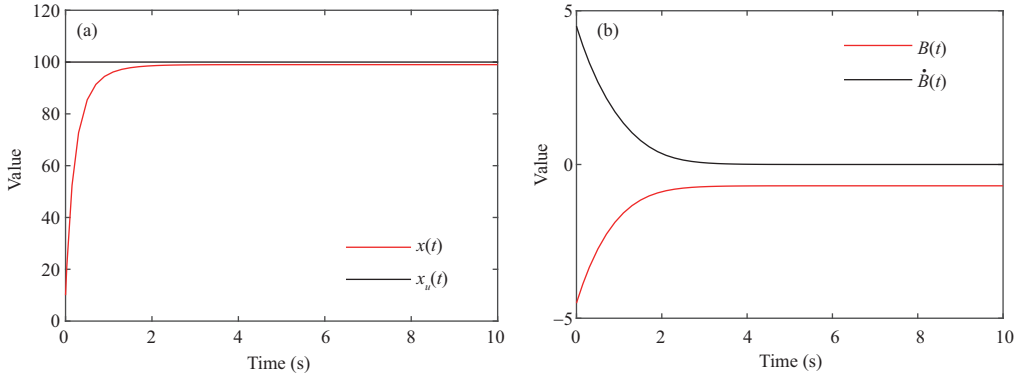

图 1 (网络版彩图) 状态 x 与其障碍函数仿真结果. (a) 状态的动态时变轨迹与状态和集合 $\mathcal{C}$ 的边界曲线; (b) 障碍函数 B 与其一阶导数 $\dot{B}$ 的动态变化曲线

Figure 1 (Color online) The results of the state x and the barrier function. (a) Dynamic time-varying trajectory and the relationship between x and set $\mathcal{C}$; (b) dynamic changes of B and $\dot{B}$

当 $x(t) \in \mathrm{Int}(\mathcal{C})$ 时, 有 $\ln(x_u - x) \leqslant \ln(1 + x_u - x)$. 因此,

$$\dot{B} \leqslant \ln(1 + h(x)). \tag{20}$$

因为 $\alpha_2(r) = \ln(1+r)$ 在定义域 $[0, a)$ 上是 $\mathcal{K}$ 类函数, 所以障碍函数满足定义 5. 因此, 所设计的障碍函数为非正障碍函数, 而集合 $\mathcal{C}$ 是前向不变的, 系统 (14) 是状态安全的. 该理论验证结果, 如图 1 所示, 设置 $x_u = 100$, 初始状态为 $x_0 = 10$, 因此 $\mathcal{C} = \{x \in \mathbb{R} : x \leqslant 100\}$. 图 1(a) 中黑线 $x = 100$ 的下方是安全域. 从图 1(a) 可发现, 状态解 $x(t)$ 最终会收敛到某个小于 $x_u = 100$ 的值. 而 $x_u = 100$ 正好是集合 $\mathcal{C}$ 的边界. 因此, 系统是状态安全的. 图 1(b) 佐证了状态解最终的收敛性, 且障碍函数 B 的值始终为负, 验证了仿真结果的有效性.

4.3 不同与优势对比

(1) 与倒数障碍函数的比较

非正障碍函数的松弛度高于倒数障碍函数 (在状态集闭合有界下倒数障碍函数可转化为零障碍函数), 其对于集合边界定义更便于读取与明确表达, 并且求导与计算过程相对简便.

非正障碍函数克服了倒数障碍函数的几点瑕疵: (i) 倒数障碍函数在集合边界的取值为无穷大, 对于实际系统, 无穷大的取值存在不可读的问题. 因为系统数据显示存在一个有限大的上界. 例如, 10000, 我们不能将超过 10000 的定义为边界值, 这样会造成事实上的误警. 因此, 非正障碍函数将集合边界的取值设定为 0, 便于读取与明确表达. (ii) 倒数障碍函数在使用时, 因为 $B_1(x) = \frac{1}{\alpha(h(x))}$ (α 是 $\mathcal{K}$ 类函数), 求导计算与推导过程相对复杂一些, 需要更细心与更好的高等数学技巧. 而由于非正障碍函数 $B_2(x) = \beta(h(x))$ (β 是 $\mathcal{D}_1$ 类函数), 一般可选择一个合适的 β, 因此, 其求导与推导计算比倒数障碍函数更便捷一些.

(2) 与零障碍函数的比较

非正障碍函数的松弛度高于零障碍函数, 并且实际应用时操作性更灵活.

(i) 当定义 5 中的 $\lambda(t) = 1$ 时, 非正障碍函数可由条件 (7) 与 (8) 推得, $\dot{h} \geqslant -m\delta(h)$ 或 $\dot{h} \geqslant -\bar{\delta}(h)\delta(h)$. 其中, $\bar{\delta} = \phi \circ \alpha_2$, $\phi = -\frac{\partial \varphi(r)}{\partial r}$. 根据定义 5, m 是正实常数, ϕ 是 $\mathcal{D}_2$ 类函数, α_2 是 $\mathcal{D}_1$ 类函数, $\bar{\delta}$ 与 δ 是 $\mathcal{K}$ 类函数. 当 δ 取扩展 $\mathcal{K}$ 类函数时, 前者等价于零障碍函数; 而后者 $\bar{\delta}$ 与 δ 都是扩展

$\mathcal{K}$ 类函数时, 函数 $\varpi(h)=\bar{\delta}(h)\delta(h)$ 不是扩展 $\mathcal{K}$ 类函数, 但也能保证集合的前向不变性. 非正障碍函数的松弛程度大于等于零障碍函数.

(ii) 当 $\lambda(t)$ 为某具体的有界时变函数时, 不等式 (8) 右侧引入 $\lambda(t)$ 有以下几个好处: (a) 弱化了零障碍函数、倒数障碍函数对障碍函数一阶导数的约束. 零障碍函数要求一阶导数满足 $\dot{h}\geqslant-\beta_1(h)$、倒数障碍函数要求一阶导数满足 $\dot{B}\leqslant\beta_2(h)$, 其中 β_1 为扩展 $\mathcal{K}$ 类函数、β_2 为 $\mathcal{K}$ 类函数. 其中根据扩展 $\mathcal{K}$ 类函数的性质, 可以发现零障碍函数至少无法包含 $\dot{h}(x)\geqslant-h^{2k}(x)$ (k 为正整数) 的情况. 显然, $h^{2k}(x)$ 是关于 h 的一个 $\mathcal{K}$ 类函数. 但根据条件 $\dot{h}(x)\geqslant-h^{2k}(x)$ (k 为正整数) 亦可证明集合 $\mathcal{C}$ 是前向不变的. 而本文提出的非正障碍函数为 $\dot{B}\leqslant\lambda(t)\beta_3(h)$ (β_3 为 $\mathcal{K}$ 类函数), 对不等式右侧的单调性没有前两种障碍函数这么强的行为约束, 只需满足条件: 可以分解成一个单调性可动态时变的有界函数和另一个 $\mathcal{K}$ 类函数的乘积形式. (b) 引入 $\lambda(t)$ 后, 可将部分对障碍函数求导时无法转换成 $h(x)$ 泛函形式的残余项转化为 $\lambda(t)$, 如 $x=(x_1,x_2)^{\mathrm{T}}$, 残余项里含有 x_1 或 x_2, 无法凑成 $h(x)$, 这时如果能转化为 $\lambda(t)$, 只需计算 $\lambda(t)$ 的有界性即可. 这一点对于非线性非自治系统可能更有优势.

综上, 本文所提出的非正障碍函数在某些方面相较零障碍函数与倒数障碍函数具有一定的优势.

5 控制障碍函数

对于如 (1) 描述的非线性自治系统, 仅在第 4 节设计的非正障碍函数可以应用于系统安全性的分析与判别以及保证部分自治系统实现安全化, 而缺少使系统安全化的能力. 如何能够通过控制使非线性动态系统实现安全化呢? Wieland 等 [20] 于 2007 年提出了安全控制中障碍函数的使用方法, 并命名为控制障碍函数 (control barrier function). 而文献 [25,31] 在此基础上提出了控制障碍函数的新用法. 本文继承该新用法, 将非正障碍函数转化成控制非正障碍函数, 用以设计状态安全控制器.

考虑一类非线性控制系统:

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

其中, $x\in\mathbb{R}^n$, $u\in U\subset\mathbb{R}^n$, U 为控制器的可行控制输出集, 函数 f 与 g 设定为是局部 Lipschitz 的.

我们希望能够使用控制律 u 来调节系统 (21) 的状态解 $x(t)$, 从而保证 $x(t)$ 能够始终处于由式 (2)$\sim$(4) 定义的集合 $\mathcal{C}$ 内. 例如, 我们希望控制律 u 能起到作用, 当系统 $\dot{x}=f(x)$ 在某一时刻发生故障导致系统描述函数改变如 $\dot{x}=f(x)+f_d(t)=\bar{f}(x)$ ($f_d(x,t)$ 是可观测的故障函数) 时, 无法保证状态解继续在 $\mathcal{C}$ 内运动. 因此, 有如下定义.

定义6 对于动态系统 (21), 该系统具有由式 (2)$\sim$(4) 定义的安全状态集 $\mathcal{C}$ 且其伴随函数 $h:\mathbb{R}^n\to\mathbb{R}$ 连续可微. 如果存在局部 Lipschitz 的 $\mathcal{D}_1$ 类函数 α_1 和 α_2 (且 $-\frac{\partial\varphi(r)}{\partial r}$ 等于正实常数 m 或属于 $\mathcal{D}_2$ 类函数, $\varphi=\alpha_i^{-1},i=1,2$), 以及一个局部 Lipschitz 的 $\mathcal{D}_2$ 类函数 α_3, 使得对于 $\forall x\in\mathrm{Int}(\mathcal{C})$, 都有不等式 (22) 与 (23), 那么函数 $B:\mathcal{C}\to\mathbb{R}$ 则可被认为是集合 $\mathcal{C}$ 的一个控制非正障碍函数:

$$\alpha_1(h(x))\leqslant B(x)\leqslant\alpha_2(h(x)), \tag{22}$$

$$\inf_{u\in U}\left[L_fB(x)+L_gB(x)u-\lambda(t)\alpha_3(B(x))\right]\leqslant 0, \tag{23}$$

其中, $\lambda(t)\in\mathbb{R}$ 是一个关于时间 t 的连续可微函数, 且函数 λ 有界满足 $|\lambda|\leqslant c$ ($c>0$ 为常数), 但单调性未知; $L_fB(x)=\frac{\partial B(x)}{\partial x}f(x)$, $L_gB(x)=\frac{\partial B(x)}{\partial x}g(x)$.

因此, 有

$$K_{\mathrm{cnpbf}}(x)=\{u\in U:L_fB(x)+L_gB(x)u\leqslant\lambda(t)\alpha_3(B(x))\}. \tag{24}$$

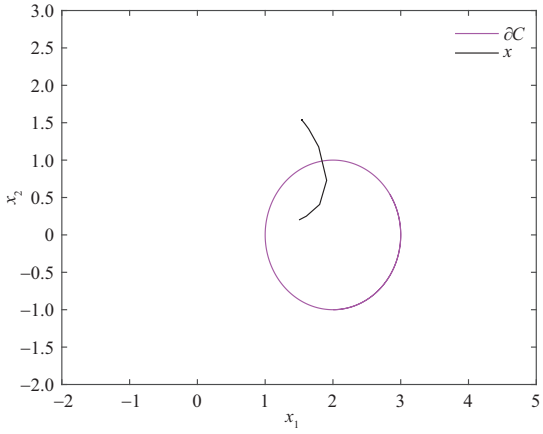

图 2 (网络版彩图) 无控制作用下的状态 x 与集合 $\mathcal{C}$ 的相对关系

Figure 2 (Color online) The relationship between the state x and the set $\mathcal{C}$ without control

控制律 u 可以通过二次型规划 (quadratic programming) 进行求解. 上述控制输出可依据推论 1 来保证集合 $\mathcal{C}$ 的前向不变性, 且推论 1 可由定理 1 推得.

推论1 给定系统 (21) 具有一个满足条件 (2)∼(4) 的 $\mathcal{C}\subseteq\mathbb{R}^n$, 如果存在一个由定义 6 定义的控制非正障碍函数 $B:\mathcal{C}\to\mathbb{R}$ 能使任意 Lipschitz 连续控制器有 $u(x)\in K_{\mathrm{cnpbf}}(x)$, 则该集合 $\mathcal{C}$ 是前向不变的.

证明 令 $u=K_{\mathrm{cnpbf}}(x)$, 系统 (21) 则可改写成 $\dot{x}=\bar{f}(x)$, 其中 $\bar{f}(x)=f(x)+g(x)K_{\mathrm{cnpbf}}(x)$. 根据条件 (22), 令 $B(x)=\alpha(h)$ (α 为 $\mathcal{D}_1$ 类函数), 于是, $\alpha_3(B)=\alpha_3\circ\alpha(h)$. 因为 α_3 为 $\mathcal{D}_2$ 类函数, 根据引理 1, $\alpha_3\circ\alpha$ 为 $\mathcal{K}$ 类函数. 因此, 条件 (23) 可由定义 5 的条件 (8) 转化. 因此, 根据定理 1, 可推得系统 (21) 是通过控制保持安全的.

例 3 验证了控制障碍函数与状态安全控制的明显效果.

例3 考虑一动态系统:

$$\dot{x}=-\frac{1}{2}\begin{pmatrix}x_1^5+3x_1^3x_2^2\\ x_2^5+3x_1^2x_2^3\end{pmatrix}+\frac{3r^2}{2}\begin{pmatrix}x_1^3+x_1x_2^2\\ x_2^3+x_1^2x_2\end{pmatrix}-\frac{3r^4}{2}\begin{pmatrix}x_1\\ x_2\end{pmatrix}+u, \tag{25}$$

其中, $x=(x_1,x_2)^{\mathrm{T}}$, $u=(u_1,u_2)^{\mathrm{T}}$. 令系统 (25) 的安全状态集 $\mathcal{C}$ 的伴随函数为 $h(x)=r^2-\|x-x_o\|_2^2$. 由此, 集合 $\mathcal{C}$ 是一个半径为 r, 圆心为 x_o 的圆. 所以, 如果状态 x 能始终处于该圆内, 则系统 (25) 是安全的. 设置 $x_o=(2r,0)^{\mathrm{T}}$. 设置仿真初始值为 $x_0=(1.5,0.2)^{\mathrm{T}}$, $r=1$, 则 $x_o=(2,0)^{\mathrm{T}}$. 如图 2 所示, 当系统 (25) 没有控制输入时, 即 $u\equiv 0$, 则系统将不能保持安全.

设障碍函数 $B(x)=-h(x)$. 这里将通过两组不同的障碍函数一阶导数不等式约束来充分展示控制效果.

(1) $\dot{B}(x)\leqslant h^2(x)$, 可得

$$\begin{aligned}&u=\arg\min u^{\mathrm{T}}u\\ &\text{s.t.}\ \ 2(x-x_o)^{\mathrm{T}}u\leqslant h(x)-2(x-x_o)^{\mathrm{T}}f(x),\end{aligned} \tag{26}$$

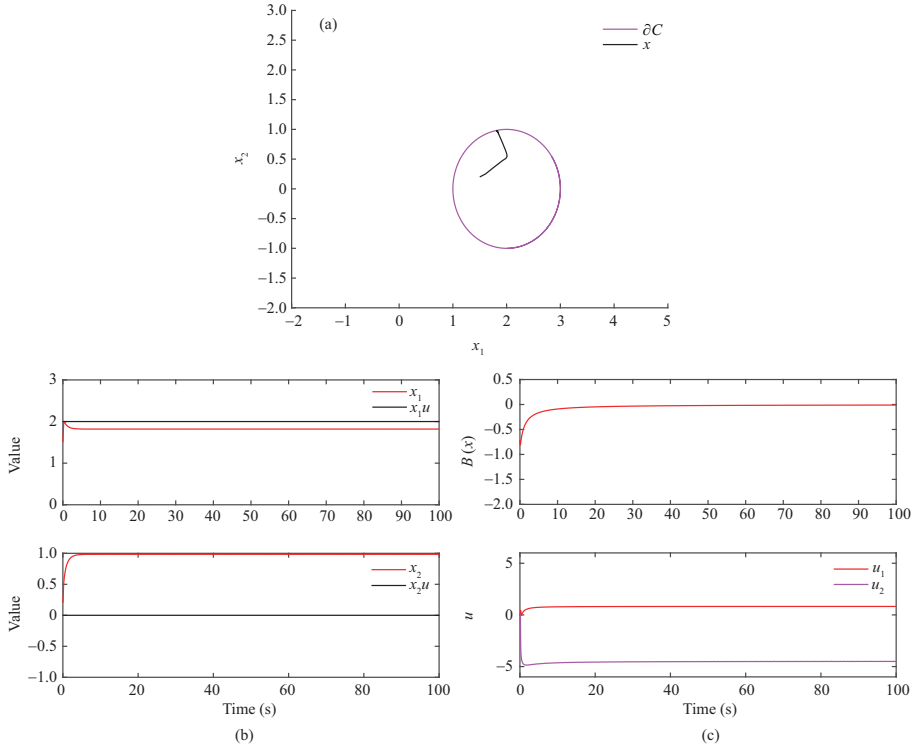

图 3 (网络版彩图) $\dot{B} \leqslant h^2(x)$ 下的状态 x、障碍函数与控制器仿真结果. (a) 状态 x 与集合 $\mathcal{C}$ 的相对关系; (b) 状态 x 的动态时变轨迹; (c) 障碍函数 B 与控制律 u 的动态变化曲线

Figure 3 (Color online) The curves of x, barrier function and controller u with $\dot{B} \leqslant h^2(x)$. (a) Relationship between state x and set $\mathcal{C}$; (b) dynamic time-varying trajectories of the state x; (c) dynamic changes of barrier function B and controller u

其中,

$$f(x) = -\frac{1}{2}\left(x_1^5 + 3x_1^3x_2^2, x_2^5 + 3x_1^2x_2^3\right)^{\mathrm{T}} + \frac{3r^2}{2}\left(x_1^3 + x_1x_2^2, x_2^3 + x_1^2x_2\right)^{\mathrm{T}} - \frac{3r^4}{2}(x_1, x_2)^{\mathrm{T}}.$$

(2) $\dot{B}(x) \leqslant h^4(x)$, 可得

$$\begin{aligned} &u = \arg\min u^{\mathrm{T}}u \\ &\text{s.t.}\ \ 2(x - x_o)^{\mathrm{T}}u \leqslant h^4(x) - 2(x - x_o)^{\mathrm{T}}f(x). \end{aligned} \tag{27}$$

通过 MATLAB 的 'quadprog' 可以求解 u, 其中仿真的停止时间设为100.

由图 3(c) 可知, B 在仿真时间结束前, 并未穿越 0, 这佐证了图 3(a) 中, 状态十分接近但并未到达集合的边界, 并未逃离集合. 由图 4(c) 可知, B 最终收敛到某个负值, 这佐证了图 4(a) 中, 状态始终保持在集合内, 并未逃离集合. 对比图 2, 在相同仿真时间下图 2 内有一半的状态在集合外, 因此, 控制效果极为明显. 从安全控制的整体效果出发, 图 4 的仿真结果表明基于控制障碍函数的控制律 u 的作用能有效控制系统状态, 保证系统的状态安全; 而图 3, 控制律能在状态向不安全恶化的情景下做到有效的延缓, 可以为系统安全连锁与安全停车争取更多可用时间.

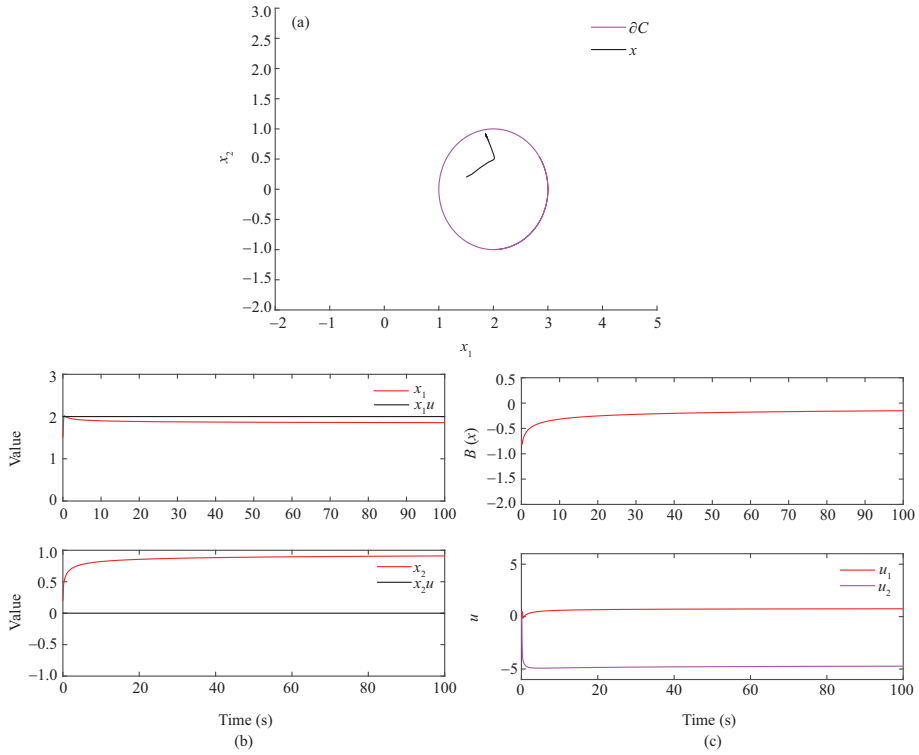

图 4 (网络版彩图) $\dot{B} \leqslant h^4(x)$ 下的状态 x、障碍函数与控制器仿真结果. (a) 状态 x 与集合 $\mathcal{C}$ 的相对关系; (b) 状态 x 的动态时变轨迹; (c) 障碍函数 B 与控制律 u 的动态变化曲线

Figure 4 (Color online) The curves of x, barrier function and controller u with $\dot{B} \leqslant h^4(x)$. (a) Relationship between state x and set $\mathcal{C}$; (b) dynamic time-varying trajectories of the state x; (c) dynamic changes of barrier function B and controller u

注释2 从仿真结果图 3 与 4 可以发现, 状态 $x(t)$ 都具有向集合 $\mathcal{C}$ 靠近的行为或趋势. 这是一种正常现象. 由于所提障碍函数对状态的约束力减弱 (即松弛化), 对于封闭的安全状态集, 不再需要状态最终收敛于集合内部的某一个点, 只需要状态一直属于集合即可. 因此, 状态靠近集合边界是可接受的结果, 只要不脱离集合.

6 障碍函数在 CSTR 中的应用

本节选用一种非线性连续搅拌釜反应器, 如图 5(a) 所示. CSTR 中的单一反应 $A \to B$ 是不可逆的. 到目前为止, 最近的相关工作开始聚焦于对 CSTR 的灾害研究 [34], 但控制问题仍然是稳定性问题 [35,36]. 控制过程集中在反应物浓度和反应器温度, 其中反应物温度需要控制在一个可用的范围内, 以保证温度不能太高或太低. 这意味着反应过程涉及一类安全问题: 温度安全. 本文采用的 CSTR 是文献 [37] 使用的非线性模型:

$$\dot{C}_A = \frac{q}{V}(C_{Af} - C_A) - k_0 \exp\left(-\frac{E}{RT}\right) C_A, \tag{28}$$

$$\dot{T} = \frac{q}{V}(C_{Af} - C_A) + \frac{-\Delta H}{\rho C_p} k_0 \exp\left(-\frac{E}{RT}\right) C_A + \frac{UA}{V\rho C_p}(T_c - T), \tag{29}$$

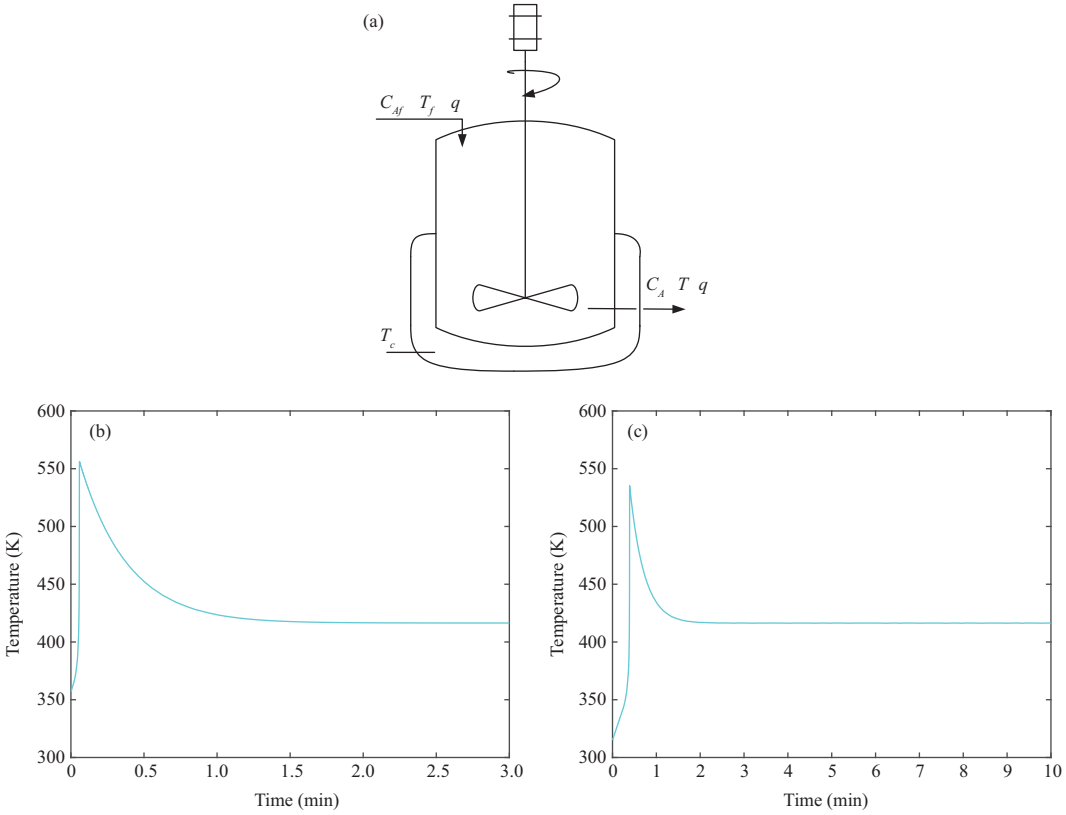

图 5 (网络版彩图) 连续搅拌釜反应器与无控制作用下的反应器温度 (即式 (30) 中 $u \equiv 0$). (a) 连续搅拌釜反应器示意图; (b) 初始温度为 $T_0 = 357$ K 的反应器温度 T; (c) 初始温度为 $T_0 = 315$ K 的反应器温度 T

Figure 5 (Color online) Continuously stirred tank reactor system and the temperatures of the reactor without control ($u \equiv 0$ in (30)). (a) Continuously stirred tank reactor system; (b) the temperature T of the reactor with the initial temperature $T_0 = 357$ K; (c) the temperature T of the reactor with the initial temperature $T_0 = 315$ K

其中, 有两个状态变量 (反应物浓度 C_A 与反应器温度 T), 一个可执行变量 (冷却液温度 T_c), 以及进料温度 T_f. 令

$$\alpha = \frac{q}{V}, \beta = \frac{UA}{V\rho C_p}, \mu = \frac{E}{RT_f},$$
$$b = \frac{(-\Delta H)\, C_{Af}}{\rho C_p T_f}, D_a = k_0 \mathrm{e}^{-\mu},$$
$$x_1 = \frac{C_{Af} - C_A}{C_{Af}}, x_2 = \frac{T - T_f}{T_f}, u = \frac{T_c - T_f}{T_f}.$$

该 CSTR 模型可改写成

$$\dot{x}_1 = -\alpha x_1 + D_a\,(1 - x_1)\,\mathrm{e}^{\frac{\mu x_2}{1+x_2}}, \tag{30}$$
$$\dot{x}_2 = -\,(\alpha + \beta)\, x_2 + bD_a\,(1 - x_1)\,\mathrm{e}^{\frac{\mu x_2}{1+x_2}} + \beta u. \tag{31}$$

根据文献 [37, Table 1] 的标称设定, 可得各参数值为 $T_f = 350$ K, $\alpha = 1\ \mathrm{min}^{-1}, \beta = 2.092\ \mathrm{min}^{-1}, \mu = 25, b = 0.5977, D_a = 0.9999\ \mathrm{min}^{-1}$. 这里, 假设反应器可容许的温度变化范围为 $|T - T_f| \leqslant 0.2T_f$. 设光滑函数 h 是集合 $\mathcal{C}$ 的伴随函数. 设 $x = (x_1, x_2)^{\mathrm{T}}$, $r = 0.2$, 定义 $\mathcal{C} = \left\{x \in \mathbb{R}^2 : r^2 - |x_2|^2 \leqslant 0\right\}$,

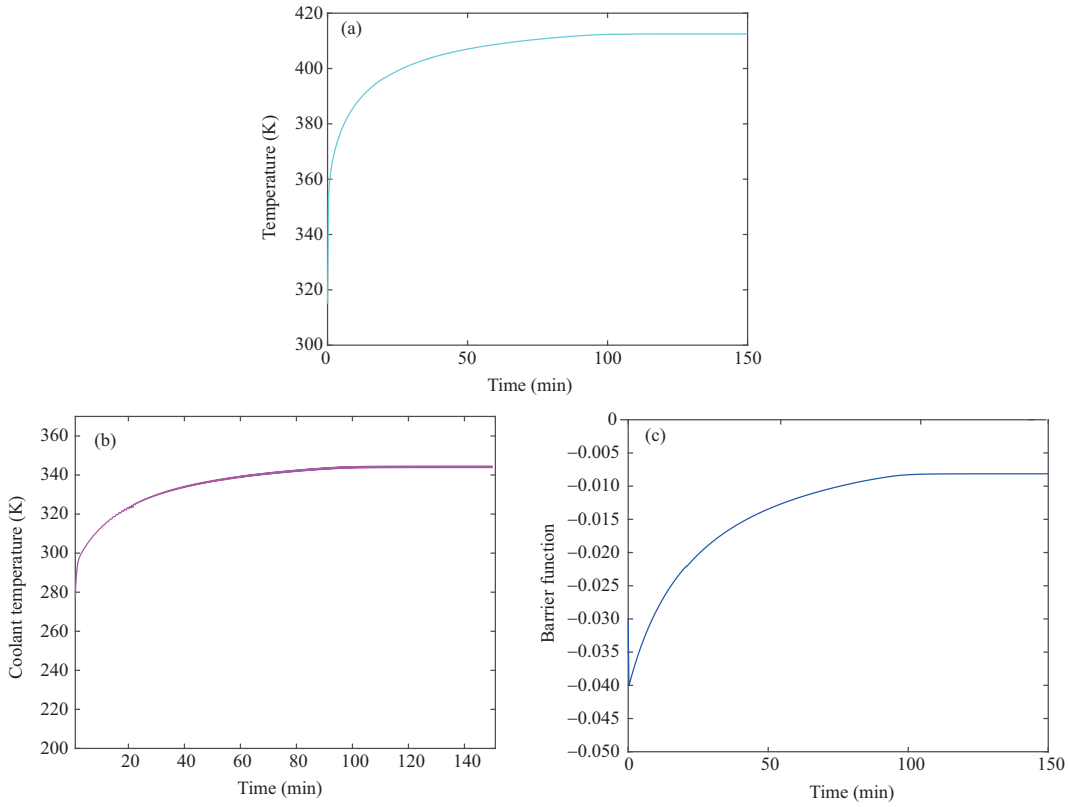

图 6 (网络版彩图) 反应器初始温度为 $T_0 = 357$ K 下的安全控制仿真结果. (a) 反应器的温度 T; (b) 控制器输出 T_c; (c) 障碍函数 $B(x)$

Figure 6 (Color online) Results for the simulation when $T_0 = 357$ K. (a) Temperature T of the reactor; (b) controller output T_c; (c) barrier function $B(x)$

可得安全范围为 $T \in [280\text{ K}, 420\text{ K}]$, $h(x) = r^2 - |x_2|^2$. 构建障碍函数 $B(x) = -h(x)$. 使用约束条件 $\dot{B} \leqslant h^2(x)$, 完成了两组仿真: 第 1 组的初始值为 $x_{10} = 0.03, x_{20} = 0.2$, 即 $T_0 = 357$ K; 第 2 组为 $x_{10} = 0.03, x_{20} = -0.1$, 即 $T_0 = 315$ K, 也如例 3 一样使用 'quadprog' 来实现 $\min u^{\mathrm{T}}u$ 的求解.

仿真结果图中的温度单位为 K, 时间单位为 min. 将图 6(a) 与 5(b) 对比, 将图 7(a) 与 5(c) 对比, 均可发现控制障碍函数与安全控制器的作用, 有效地将反应器的温度控制在 $T \in [280\text{ K}, 420\text{ K}]$. 由图 6(b) 与 7(b) 可以发现, 如果使用水作为冷却液, 则控制器可能无法找到合适的解 (当然这和障碍函数及其约束条件也具有一定的关系). 事实上, 我们对这样的情况在仿真软件中进行过实验, 并没有获得好的安全控制效果. 关于控制器饱和、系统参数与系统安全可控之间的关系, 我们将在未来进行深入的探讨与研究.

7 总结

本文主要解决一类动态系统的系统安全分析与控制的理论问题, 将有助于非自治系统实现安全化. 并且本文将系统安全分析和判断转化为验证系统安全状态集 $\mathcal{C}$ 的前向不变性. 通过创建 $\mathcal{D}_1$ 和 $\mathcal{D}_2$ 类函数, 设计了可约束状态运动行为的非正障碍函数, 并基于非正障碍函数提出了系统安全判据, 以及构建了相应的控制障碍函数, 设计了安全控制律, 为实现系统状态安全化提供理论与方法支撑. 最终

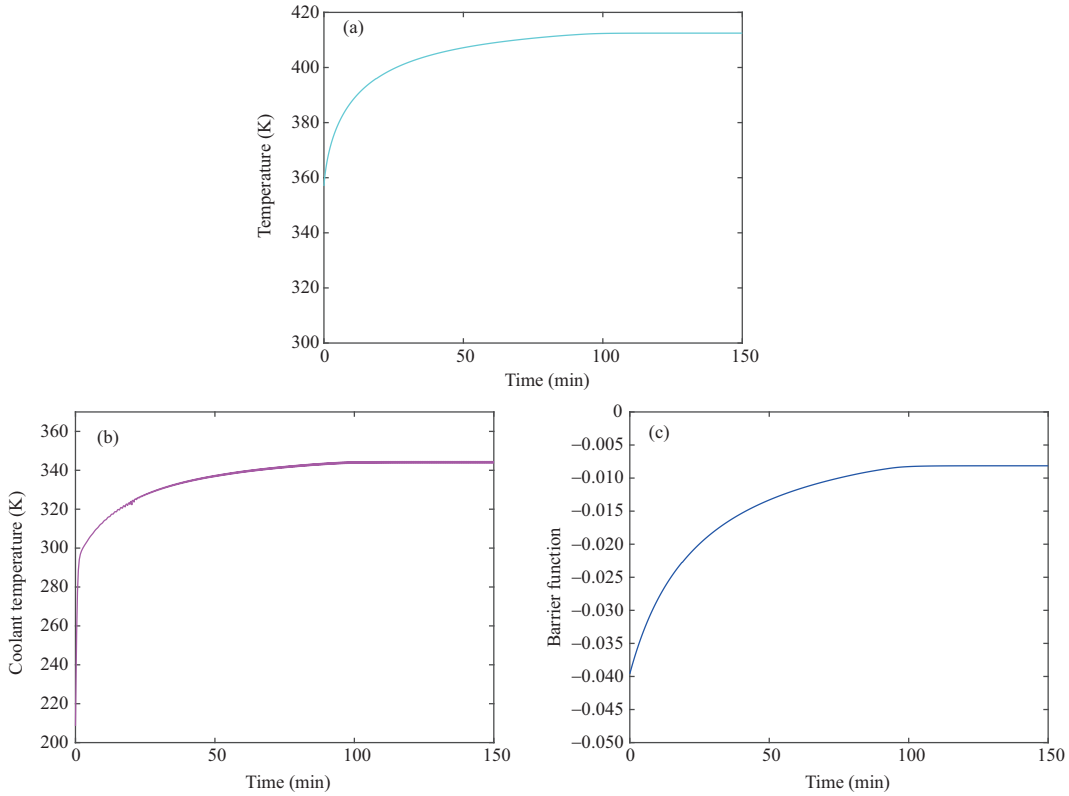

图 7 (网络版彩图) 反应器初始温度为 $T_0 = 315$ K 下的安全控制仿真结果. (a) 反应器的温度 T; (b) 控制器输出 T_c; (c) 障碍函数 $B(x)$

Figure 7 (Color online) Results for the simulation when $T_0 = 315$ K. (a) Temperature T of the reactor; (b) controller output T_c; (c) barrier function $B(x)$

通过对夹套连续搅拌釜反应器的仿真研究验证了所提出的理论和方法的有效性.

希望本文的研究工作能够帮助本领域的学者或工程师, 利用非正障碍函数这一框架性函数, 针对不同系统构建出方便实现且巧妙的障碍函数, 在计算量低、算法复杂度低的前提下实现状态安全控制.

参考文献

1 Chai Y, Zhang K, Mao Y, et al. Analysis and Technology of Dynamic System Operational Safety. Beijing: Chemical Industry Press, 2019

2 Villa V, Paltrinieri N, Khan F, et al. Towards dynamic risk analysis: a review of the risk assessment approach and its limitations in the chemical process industry. Saf Sci, 2016, 89: 77–93

3 Busby J S, Green B, Hutchison D. Analysis of affordance, time, and adaptation in the assessment of industrial control system cybersecurity risk. Risk Anal, 2017, 37: 1298–1314

4 Kriaa S, Pietre-Cambacedes L, Bouissou M, et al. A survey of approaches combining safety and security for industrial control systems. Reliability Eng Syst Saf, 2015, 139: 156–178

5 Talebberrouane M, Khan F, Lounis Z. Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms. J Loss Prevention Process Industries, 2016, 44: 193–203

6 Landucci G, Argenti F, Cozzani V, et al. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf Environ Protection, 2017, 110: 102–114

7 Ge Z, Song Z. Performance-driven ensemble learning ICA model for improved non-Gaussian process monitoring. Chemometr Intell Laboratory Syst, 2013, 123: 1–8

8 Liu Q, Chai T Y, Qin S Z, et al. Progress of data-driven and knowledge-driven process monitoring and fault diagnosis for industry process (in Chinese). Control and Decision, 2010, 25: 801–807 [刘强, 柴天佑, 秦泗钊, 等. 基于数据和知识的工业过程监视及故障诊断综述. 控制与决策, 2010, 25: 801–807]

9 Tan S, Chang Y Q, Wang F L, et al. Mode identification and process monitoring for multiple mode processes based on GMM (in Chinese). Control and Decision, 2015, 30: 53–58 [谭帅, 常玉清, 王福利, 等. 基于 GMM 的多模态过程模态识别与过程监测. 控制与决策, 2015, 30: 53–58]

10 Prajna S, Rantzer A. On the necessity of barrier certificates. In: Proceedings of the IFAC World Congress, Prague, 2005. 526–531

11 Prajna S, Jadbabaie A, Pappas G J. Stochastic safety verification using barrier certificates. In: Proceedings of IEEE Conference on Decision and Control, Nassau, 2004

12 Kong H, Song X, Han D, et al. A new barrier certificate for safety verification of hybrid systems. Comput J, 2014, 57: 1033–1045

13 Dai L, Gan T, Xia B, et al. Barrier certificates revisited. J Symbolic Computation, 2017, 80: 62–86

14 Sogokon A, Ghorbal K, Tan Y K, et al. Vector barrier certificates and comparison systems. In: Proceedings of International Symposium on Formal Methods, 2018. 10951: 418–437

15 Wang G, He J, Liu J, et al. Safety verification of interconnected hybrid systems using barrier certificates. Math Problems Eng, 2016, 2016: 1–10

16 Wang G, Jing L, Sun H, et al. Safety verification of state/time-driven hybrid systems using barrier certificates. In: Proceedings of the 35th Chinese Control Conference (CCC), Chengdu, 2016. 2483–2489

17 Zhu Z, Chai Y, Yang Z, et al. Exponential-alpha safety criteria of a class of dynamic systems with barrier functions. IEEE/CAA J Autom Sin, 2022, 9: 1939–1951

18 Zhu Z R, Chai Y, Yang Z M. A novel kind of sufficient conditions for safety judgement based on control barrier function. Sci China Inf Sci, 2021, 64: 199205

19 Zhu Z R, Chai Y, Yang Z M, et al. Safety criteria based on barrier function under the framework of boundedness for some dynamic systems. Sci China Inf Sci, 2022, 65: 122203

20 Wieland P, Allgöwer F. Constructive safety using control barrier functions. In: Proceedings of the 7th IFAC Symposium on Nonlinear Control System, Pretoria, 2007. 462–467

21 Romdlony M Z, Jayawardhana B. Stabilization with guaranteed safety using control Lyapunov-barrier function. Automatica, 2016, 66: 39–47

22 Romdlony M, Jayawardhana B. Passivity-based control with guaranteed safety via interconnection and damping assignment. In: Proceedings of the 5th IFAC Conference on Analysis and Design of Hybrid Systems, 2015. 48: 74–79

23 Romdlony M, Jayawardhana B. On the new notion of input-to-state safety. In: Proceedings of IEEE Conference on Decision Control (CDC), Las Vegas, 2016. 6403–6409

24 Romdlony M Z, Jayawardhana B. Robustness analysis of systems' safety through a new notion of input-to-state safety. Int J Robust Nonlin Control, 2019, 29: 2125–2136

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

26 Xu X, Tabuada P, Grizzle J W, et al. Robustness of control barrier functions for safety critical control. IFAC-PapersOnLine, 2015, 48: 54–61

27 Glotfelter P, Cortes J, Egerstedt M. Nonsmooth barrier functions with applications to multi-robot systems. IEEE Control Syst Lett, 2017, 1: 310–315

28 Borrmann U, Wang L, Ames A D, et al. Control barrier certificates for safe swarm behavior. IFAC-PapersOnLine, 2015, 48: 68–73

29 Wang L, Ames A D, Egerstedt M. Safety barrier certificates for collisions-free multirobot systems. IEEE Trans Robot, 2017, 33: 661–674

30 Wang L, Ames A, Egerstedt M. Safety barrier certificates for heterogeneous multi-robot systems. In: Proceedings of American Control Conference (ACC), Boston, 2016. 5213–5218

31 Ames A D, Xu X, Grizzle J W, et al. Control barrier function based quadratic programs for safety critical systems. IEEE Trans Automat Contr, 2017, 62: 3861–3876

32 Agrawal A, Sreenath K. Discrete control barrier functions for safety critical control of discrete systems with application

to bipedal robot navigation. In: Proceedings of Robotics: Science and Systems, Cambridge, 2017
33 Khalil H. Nonlinear Systems. 3rd ed. New Jersey: Prentice Hall, 2002
34 Xie Q, Zhang L, Yu X, et al. Thermal hazards for autocatalysis and stability in CSTR: decomposition of solution from nitrolysis of hexamethylenetetramine. Prop Explos Pyrotech, 2020, 45: 1859–1869
35 Stavrov D, Nadzinski G, Deskovski S, et al. Quadratic model-based dynamically updated PID control of CSTR system with varying parameters. Algorithms, 2021, 14: 31
36 Pipino H A, Cappelletti C A, Adam E J. Adaptive multi-model predictive control applied to continuous stirred tank reactor. Comput Chem Eng, 2021, 145: 107195
37 McLain R B, Henson M A. Nonlinear model reference adaptive control with embedded linear models. Ind Eng Chem Res, 2000, 39: 3007–3017

Non-positive barrier function: a new notion of barrier function for state-safety control of nonlinear dynamical systems

Zheren ZHU[1,2], Xinmin ZHANG[1,2], Yi CHAI[3*] & Zhihuan SONG[1,2*]

1. *College of Control Science and Engineering, Zhejiang University, Hangzhou* 310027*, China*;
2. *State Key Laboratory of Industrial Control Technology, Hangzhou* 310027*, China*;
3. *School of Automation, Chongqing University, Chongqing* 400044*, China*
* Corresponding author. E-mail: chaiyi@cqu.edu.cn, songzhihuan@zju.edu.cn

Abstract The analysis and control of system state safety are a research hotspot in the field of control. This article has thoroughly investigated some issues related to safety criteria with application to the safety analysis, diagnosis, and safety control of a class of dynamical systems with their unique set of available states via a new notion of barrier functions. Inspired by reciprocal barrier functions and zeroing barrier functions, a type of non-positive barrier function (NPBF) is designed and the safety criteria is proposed, guaranteeing that the unique set of available states is forward-invariant to ensure system safety at all times. Then, the control barrier function is established based on NPBFs for a class of dynamical control systems and used to design the safety controller. Conclusively, this is a first-of-its-kind study to apply safety criteria and control barrier functions to safeguard a class of continuously stirred tank reactors.

Keywords non-positive barrier function, dynamical systems, state-safety control, safety criteria, control barrier function