arXiv:2303.03247v1 [eess.SY] 6 Mar 2023

通过降阶模型实现具有有界输入的安全关键控制

Tamas G. Molnar 和 Aaron D. Ames

摘要——由于这些系统本质上具有高维特性，并且相应的复杂模型在实践中可能难以确定，因此在从汽车到行走机器人的复杂自主系统上保证安全行为是一项挑战。基于这一动机，本文提出了一种安全关键控制框架，该框架利用降阶模型确保全阶动力学的安全性，即使这些模型受到扰动并具有有界输入（例如驱动限制）。为处理输入约束，本文在降阶模型的背景下重新 formulates 备份集方法，并推导出保证全阶系统安全行为的条件。随后，本文引入输入到状态安全备份集方法，以增强针对降阶模型与实际系统之间差异的鲁棒性。最后，通过高保真仿真验证了所提出的框架：借助独轮车模型，四足机器人通过腿式运动安全地绕过了障碍物。

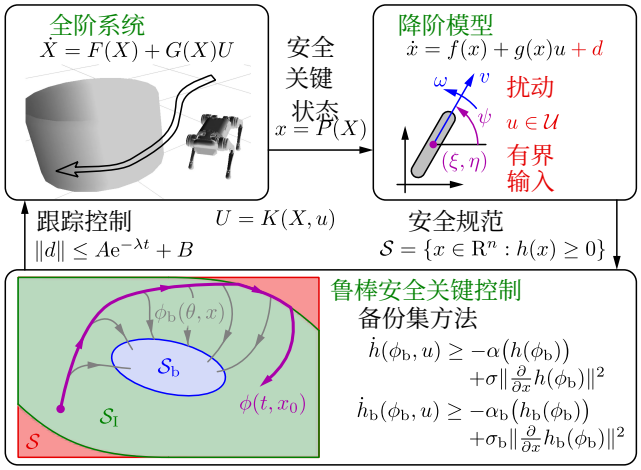


图 1. 所提出的安全关键控制框架概览。

I. 引言

现实中的工程系统往往具有复杂、非线性且高维的动态行为。自主（机器人）系统尤其如此，其动力学在实现预期行为方面发挥着关键作用。这使得控制这类系统颇具挑战，也使得难以为闭合控制回路的稳定或安全演化提供形式化保证。为应对这类复杂的控制问题，控制器综合过程中常使用动态行为的简化降阶模型（ROM），并取得了显著的实际成效 [1], [2]。然而，基于降阶模型可认证的行为与全阶系统（FOS）上实际观察到的行为之间，往往存在理论上的差距。

本文聚焦于降阶模型在安全关键控制中的作用。给定准确的动力学模型，可以借助相关工具综合出能够提供安全性形式化保证的控制器。例如，控制障碍函数（*CBF*） [3] 已被提出用于实现这一目标，并已在多种应用中证明有效，从多机器人系统 [4] 到航天器对接 [5]。在许多应用中，一个重大挑战是如何在驱动受限的情况下维持安全性：大多数物理系统的驱动能力有限，这种限制表现为

在底层模型中将其作为控制输入的约束。针对输入受限的安全关键控制，人们提出了多种方法，包括备份集方法 [6],输入受限控制屏障函数 [7], 和神经网络控制屏障函数 [8]。尽管这些方法已在各个领域取得成功，但一种通用方法仍然难以实现。

安全关键控制中的另一个重要挑战是，降阶模型（ROM）始终无法完全准确：降阶模型与实际全阶系统（FOS）之间总是存在偏差。因此，鲁棒性至关重要，必须确保即使存在此类偏差且驱动受限，安全性仍能得到保障。已有一些控制障碍函数（CBF）方法能够抵御扰动，例如输入到状态安全 [9], [10] 和鲁棒控制障碍函数 [11]。然而，这些方法尚未考虑输入约束。与此同时，前述处理输入约束的方法尚未具备鲁棒性。另一方面，也有鲁棒可达性方法能够同时处理输入约束和扰动 [12], [13], [14], [15], ，但这些方法通常会遭遇维数灾难，对于维度较高的降阶模型而言难以计算。

本文提出了一种鲁棒的安全关键控制框架，如图 1 所示。该框架利用输入受限的降阶模型和 CBF，实现对具有复杂全阶动力学的系统的形式化安全保证。为此，我们作出以下三项主要贡献。首先，我们在降阶模型的背景下重新表述了备份集方法，并给出了可证明安全行为的条件，同时考虑了降阶模型与其所跟踪的全阶系统之间的偏差。其次，我们提出了输入到状态安全备份集方法，以限制较少的条件来增强对偏差的鲁棒性。第三，我们在避障问题中实现了该方法，并通过高保真仿真展示了使用独轮车降阶模型实现四足机器人安全行走的效果。

*本研究部分由美国国家科学基金会（CPS奖项 #1932091）、陶氏公司（#227027AT）和 AeroVironment 资助。作者供职于加州理工学院机械与土木工程系，美国加利福尼亚州帕萨迪纳，邮编 91125。{tmolnar, ames}@caltech.edu

II. 输入约束下的安全性

考虑如下控制仿射系统:

$$\dot{x} = f(x) + g(x)u, \tag{1}$$

其中状态为 $x \in \mathbb{R}^n$，输入为 $u \in \mathcal{U}$，凸可行输入集为 $\mathcal{U} \subseteq \mathbb{R}^m$，局部 Lipschitz 连续函数为 $f: \mathbb{R}^n \to \mathbb{R}^n$, $g: \mathbb{R}^n \to \mathbb{R}^{n\times m}$。考虑控制器 $k: \mathbb{R}^n \to \mathcal{U}$, $u = k(x)$，它产生如下闭合控制回路:

$$\dot{x} = f(x) + g(x)k(x), \tag{2}$$

与初始条件 $x(0) = x_0 \in \mathbb{R}^n$ 相关联。若 k 局部 Lipschitz 连续，则闭环系统在一个存在区间上有唯一解 $\phi(t,\ x_0)$。为简单起见，我们假设该解对所有 $t \geq 0$ 均存在。

我们的目标是设计控制器 k，使闭环系统安全。具体而言，若系统状态 x 位于安全集 $\mathcal{S} \subset \mathbb{R}^n$ 内，我们就认为该系统是安全的。为确保闭合控制回路的安全演化，我们要求安全集 $\mathcal{S}$ 沿式 (2) 正向不变。

定义 1. 给定 $k: \mathbb{R}^n \to \mathcal{U}$，集合 $\mathcal{S} \subset \mathbb{R}^n$ 沿着 (2) 正向不变，如果 $x_0 \in \mathcal{S} \implies \phi(t,\ x_0) \in \mathcal{S}, \forall t \geq 0$。只有当 $\mathcal{S}$ 是控制不变的，这一要求才能得到满足。

定义 2. 如果存在$k: \mathbb{R}^n \to \mathcal{U}$使得 $\mathcal{S}$ 沿着 (2) 正向不变，则集合 $\mathcal{S} \subset \mathbb{R}^n$ 是控制不变的。

A. 控制障碍函数

控制障碍函数 [3] 为安全控制设计提供了强有力的工具，因此我们简要回顾这一方法。本文中，我们考虑将函数 h: $\mathbb{R}^n \to \mathbb{R}$的零上水平集定义为安全集:

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

使得 h 连续可微，且零是 h的正则值，即 $h(x) = 0 \implies \nabla h(x) \neq 0$。

定义3。 如果存在 $\alpha \in \mathcal{K}_\infty$ 使得[1]成立，则函数 h 在 $\mathcal{S}$ 上是系统(1)的控制屏障函数 *(CBF)*:

$$\sup_{u\in\mathcal{U}} \dot{h}(x,u) > -\alpha\big(h(x)\big) \tag{4}$$

对于 $\forall x \in \mathcal{S}$成立，其中:

$$\dot{h}(x,u) = \nabla h(x)(f(x) + g(x)u). \tag{5}$$

给定一个CBF， [3]建立了以下安全性结果。

定理1 ([3])。 如果 h 是 $\mathcal{S}$上系统*(1)*的*CBF*，那么任何满足以下条件的局部利普希茨连续控制器 k： $\mathbb{R}^n \to \mathcal{U}$

$$\dot{h}\big(x,k(x)\big) \geq -\alpha\big(h(x)\big) \tag{6}$$

$\forall x \in \mathcal{S}$ 使 $\mathcal{S}$ 沿系统*(2)*正向不变。

条件 (6) 可用作合成安全控制器时的约束。例如，给定一个期望控制器 $k_\mathrm{d}: \mathbb{R}^n \to \mathcal{U}$，可使用以下基于二次规划的控制器进行安全关键控制:

$$\begin{aligned} k(x) = \underset{u\in\mathcal{U}}{\operatorname{argmin}} \quad & \|u - k_\mathrm{d}(x)\|_\Gamma^2 \\ \text{s.t.} \quad & \dot{h}(x,u) \geq -\alpha\big(h(x)\big), \end{aligned} \tag{7}$$

其中， $\|u\|_\Gamma^2 = u^\top \Gamma u$ 和 $\Gamma \in \mathbb{R}^{m\times m}$ 是可调的正定权重矩阵。

B. 备份集方法

虽然控制障碍函数可以确保行为安全，但要验证某个特定的 h 确实是满足（4）的 CBF 并非易事，尤其是在存在有界输入（$\mathcal{U} \subset \mathbb{R}^m$）时。任意的 h都可能不具有控制不变的零上水平集，也可能不是 CBF，并且可能不存在满足（6）的安全输入。因此，在输入约束下，（7）这类优化问题可能不可行。提出备份集方法 [6]，通过 CBF 框架合成控制不变集及相应的安全控制器，以解决这一问题。

备份集方法描述如下；下文及 [6], [16]中给出了示例。首先，必须指定 $\mathcal{S}$的一个控制不变子集，称为备份集:

$$\mathcal{S}_\mathrm{b} = \{x \in \mathbb{R}^n : h_\mathrm{b}(x) \geq 0\}, \tag{8}$$

使得 $h_\mathrm{b}: \mathbb{R}^n \to \mathbb{R}$ 连续可微，零是 h_b的正则值，即 $h_\mathrm{b}(x) = 0 \implies \nabla h_\mathrm{b}(x) \neq 0$，且$\mathcal{S}_\mathrm{b} \subseteq \mathcal{S}$。此外，还必须定义一个备份控制器$k_\mathrm{b}: \mathbb{R}^n \to \mathcal{U}$，使备份集沿闭环系统正向不变:

$$\dot{x} = f(x) + g(x)k_\mathrm{b}(x) \triangleq f_\mathrm{b}(x). \tag{9}$$

我们将满足 $x(0) = x_0 \in \mathbb{R}^n$ 的式 (9) 的解记为$\phi_\mathrm{b}(t, x_0)$。总之，备份集和备份控制器的选择必须满足以下假设。

假设1。 备份集 $\mathcal{S}_\mathrm{b} \subseteq \mathcal{S}$ 是控制不变的，且备份控制器 k_b 使 $\mathcal{S}_\mathrm{b}$ 沿式 (9) 正向不变，同时满足输入约束:

$$x \in \mathcal{S}_\mathrm{b} \implies \phi_\mathrm{b}(\theta, x) \in \mathcal{S}_\mathrm{b} \subseteq \mathcal{S},\ \forall \theta \geq 0, \tag{10}$$

且 $k_\mathrm{b}(x) \in \mathcal{U}, \forall x \in \mathcal{S}$。

寻找控制不变子集 $\mathcal{S}_\mathrm{b}$，远比验证给定的 $\mathcal{S}$ 是否为控制不变集容易得多。由此，通过构造，我们得到了一个控制不变集 $\mathcal{S}_\mathrm{b}$和一个可用的安全控制器 k_b。然而，构造 $\mathcal{S}_\mathrm{b}$ 的方法（示例见 [6], [16]）可能会得到一个很小的集合，因此直接在$\mathcal{S}_\mathrm{b}$ 内运行系统可能导致行为过于保守。为降低这种保守性，我们将 $\mathcal{S}_\mathrm{b}$ 扩展为集合 $\mathcal{S}_\mathrm{I} \subseteq \mathcal{S}$:

$$\mathcal{S}_\mathrm{I} = \left\{ x \in \mathbb{R}^n : \begin{array}{l} \phi_\mathrm{b}(\theta, x) \in \mathcal{S},\ \forall \theta \in [0, T], \\ \phi_\mathrm{b}(T, x) \in \mathcal{S}_\mathrm{b} \end{array} \right\}, \tag{11}$$

使用 $T \geq 0$; 参见图 1。注意， T 是一个设计参数， $\mathcal{S}_\mathrm{I}$ 的大小随 T 增大，而 $T = 0$ 得出 $\mathcal{S}_\mathrm{I} = \mathcal{S}_\mathrm{b}$。

引理 1 ([6])。 集合 $\mathcal{S}_\mathrm{I}$ 是控制不变的，且备份控制器 k_b 使 $\mathcal{S}_\mathrm{I}$ 沿着 *(9)* 正向不变:

$$x \in \mathcal{S}_\mathrm{I} \implies \phi_\mathrm{b}(\vartheta, x) \in \mathcal{S}_\mathrm{I},\ \forall \vartheta \geq 0. \tag{12}$$

[1]函数 $\alpha:\ \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ 若连续，且$\alpha(0) = 0$ 并且$\lim_{r\to\infty} \alpha(r) = \infty$，则属于-$\mathcal{K}_\infty$ ($\alpha \in \mathcal{K}_\infty$)类。注意，定义在 $\mathbb{R}$ 上的扩展-$\mathcal{K}_\infty$ 类函数也用于确保安全集的吸引性。

引理1和引理2的证明见附录。

因此，(11) 得到的控制不变集 $\mathcal{S}_{\mathrm{I}}$ 比备份集 $\mathcal{S}_{\mathrm{b}}$ 更大，在实际应用中也更有用；关于 $\mathcal{S}_{\mathrm{I}}$ 的大小分析，参见 [16]。我们基于 CBF 的框架，使用 $\mathcal{S}_{\mathrm{I}}$ 来保证安全性。我们依赖以下导数:

$$\begin{aligned}\dot{h}\big(\phi_{\mathrm{b}}(\theta,x),u\big) &= \frac{\partial h\big(\phi_{\mathrm{b}}(\theta,x)\big)}{\partial x}\big(f(x)+g(x)u\big),\\ \dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T,x),u\big) &= \frac{\partial h_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T,x)\big)}{\partial x}\big(f(x)+g(x)u\big).\end{aligned} \tag{13}$$

因此，我们可以断定，备份控制器 k_{b} 满足与 (6) 类似的安全条件。

引理 2 ([6])。 存在 α、$\alpha_{\mathrm{b}} \in \mathcal{K}_\infty$，使得 $\forall x \in \mathcal{S}_{\mathrm{I}}$:

$$\begin{aligned}\dot{h}\big(\phi_{\mathrm{b}}(\theta,x),k_{\mathrm{b}}(x)\big) &\geq -\alpha\big(h(\phi_{\mathrm{b}}(\theta,x))\big),\ \forall\theta\in[0,T],\\ \dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T,x),k_{\mathrm{b}}(x)\big) &\geq -\alpha_{\mathrm{b}}\big(h_{\mathrm{b}}(\phi_{\mathrm{b}}(T,x))\big).\end{aligned} \tag{14}$$

由此得到备份集方法的主要结果。

定理2 ([6])。 考虑系统 *(1)*、*(3)* 中的集合 $\mathcal{S}$、*(8)* 中的集合 $\mathcal{S}_{\mathrm{b}}$、假设*1*，以及 *(11)* 中的集合 $\mathcal{S}_{\mathrm{I}}$。那么，存在 α、$\alpha_{\mathrm{b}} \in \mathcal{K}_\infty$，使得控制器 $k\colon \mathbb{R}^n \to \mathcal{U}$ 满足:

$$\begin{aligned}\dot{h}\big(\phi_{\mathrm{b}}(\theta,x),k(x)\big) &\geq -\alpha\big(h(\phi_{\mathrm{b}}(\theta,x))\big),\ \forall\theta\in[0,T],\\ \dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T,x),k(x)\big) &\geq -\alpha_{\mathrm{b}}\big(h_{\mathrm{b}}(\phi_{\mathrm{b}}(T,x))\big).\end{aligned} \tag{15}$$

保证 $\forall x \in \mathcal{S}_{\mathrm{I}}$ 存在。此外，任何满足 *(15)* 的局部 *Lipschitz* 连续控制器 $k\colon\ \mathbb{R}^n \to \mathcal{U}$ 都会使 $\mathcal{S}_{\mathrm{I}} \subseteq \mathcal{S}$ 沿着 *(2)* 正向不变。

证明。 根据引理 2，满足 (15) 的控制器 k 存在，因为 k_{b} 就是这样的控制器。 $\mathcal{S}_{\mathrm{I}}$ 的正向不变性由定理1保证。□

C. 优化问题中的实现

定理2 可直接用于控制器综合，例如在优化问题（如 (7)）中使用 (15):

$$\begin{aligned}k(x)=\underset{u\in\mathcal{U}}{\operatorname{argmin}}\ &\|u-k_{\mathrm{d}}(x)\|_\Gamma^2\\ \text{s.t. }&\dot{h}\big(\phi_{\mathrm{b}}(\theta,x),u\big)\geq-\alpha\big(h(\phi_{\mathrm{b}}(\theta,x))\big),\forall\theta\in[0,T],\\ &\dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T,x),u\big)\geq-\alpha_{\mathrm{b}}\big(h_{\mathrm{b}}(\phi_{\mathrm{b}}(T,x))\big).\end{aligned} \tag{16}$$

注意，约束关于 u 是仿射的，参见 (13)，因此该优化问题是凸的；如果 $u \in \mathcal{U}$ 也由仿射约束描述，则该问题可转化为二次规划。此外，与 (7) 不同，即使未验证 h 是 CBF，优化问题 (16) 仍保证可行。

(16) 的约束包含 (13) 中的项，其中:

$$\begin{aligned}\frac{\partial h\big(\phi_{\mathrm{b}}(\theta,x)\big)}{\partial x} &= \nabla h\big(\phi_{\mathrm{b}}(\theta,x)\big)\frac{\partial\phi_{\mathrm{b}}(\theta,x)}{\partial x},\\ \frac{\partial h_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T,x)\big)}{\partial x} &= \nabla h_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T,x)\big)\frac{\partial\phi_{\mathrm{b}}(T,x)}{\partial x}.\end{aligned} \tag{17}$$

这里，$Q(\theta,\ x) \triangleq \partial\phi_{\mathrm{b}}(\theta,\ x)/\partial x$ 是流$\phi_{\mathrm{b}}(\theta,\ x)$ 对其初始条件 x 的灵敏度。$\phi_{\mathrm{b}}(\theta,\ x)$ 和 $Q(\theta,\ x)$ 可以通过求解以下初值问题同时计算:

$$\begin{aligned}\phi_{\mathrm{b}}'(\theta,x) &= f_{\mathrm{b}}\big(\phi_{\mathrm{b}}(\theta,x)\big), &\phi_{\mathrm{b}}(0,x) &= x,\\ Q'(\theta,x) &= \frac{\partial f_{\mathrm{b}}}{\partial x}\big(\phi_{\mathrm{b}}(\theta,x)\big)Q(\theta,x), &Q(0,x) &= I,\end{aligned} \tag{18}$$

其中，撇号表示相对于 θ 的导数，f_{b} 与（9）中相同，I 是 $n\times n$ 单位矩阵。

优化问题 (16) 包含由 $\theta \in [0,T]$ 参数化的无限多个约束。为便于计算，通常将其离散化为有限个在 $\theta_i = iT/N_{\mathrm{c}}$、$i \in \mathcal{I} = \{0,1,\dots,N_{\mathrm{c}}\}$ 处的 N_{c} 约束，从而得到:

$$\begin{aligned}k(x)=\underset{u\in\mathcal{U}}{\operatorname{argmin}}\ &\|u-k_{\mathrm{d}}(x)\|_\Gamma^2\\ \text{s.t. }&\dot{\bar{h}}_i(x,u)\geq-\alpha\big(\bar{h}_i(x)\big),\ \forall i\in\mathcal{I},\\ &\dot{\bar{h}}_{\mathrm{b}}(x,u)\geq-\alpha_{\mathrm{b}}\big(\bar{h}_{\mathrm{b}}(x)\big).\end{aligned} \tag{19}$$

这里采用简写记号 $\bar{h}_i(x) = h(\phi_{\mathrm{b}}(\theta_i,\ x))$ 以及 $\bar{h}_{\mathrm{b}}(x) = h_{\mathrm{b}}(\phi_{\mathrm{b}}(T,\ x))$。下文中，我们将在一个示例中实现控制器 (19)。

示例1 （独轮车模型）。考虑如下独轮车模型:

$$\begin{aligned}\dot{\xi} &= v\cos\psi,\\ \dot{\eta} &= v\sin\psi,\\ \dot{\psi} &= \omega,\end{aligned} \tag{20}$$

其中，平面位置 $p = \begin{bmatrix}\xi & \eta\end{bmatrix}^\top \in \mathbb{R}^2$ 和偏航角 $\psi \in \mathbb{R}$ 构成状态 $x = \begin{bmatrix}p^\top & \psi\end{bmatrix}^\top$，而速度$v \in [v_{\min}, v_{\max}] \subset \mathbb{R}$ 和偏航角速度 $\omega \in [-\omega_{\max}, \omega_{\max}] \subset \mathbb{R}$ 构成控制输入 $u = \begin{bmatrix}v & \omega\end{bmatrix}^\top$。我们的目标是在目标位置 η_{g} 处以速度v_{g}沿 ξ 方向驱动独轮车，同时避开位于位置 p_{O}、半径为 $R_{\mathrm{O}} > 0$ 的圆形障碍物。首先考虑静止障碍物，然后考虑速度为 $\dot{p}_{\mathrm{O}}$、加速度为 $\ddot{p}_{\mathrm{O}}$的移动障碍物。请注意，后一问题已得到充分研究 [17], ，并且控制不变集的闭式表达式存在 [18]。

我们通过期望控制器实现目标运动:

$$k_{\mathrm{d}}(x) = \begin{bmatrix} v_{\mathrm{g}} \\ K_\eta(\eta_{\mathrm{g}}-\eta) - K_\psi\sin\psi\end{bmatrix}, \tag{21}$$

需要对其进行修改，以获得安全控制器 $k(x)$。为刻画安全性，我们首先引入到障碍物中心的欧几里得距离D 、指向远离障碍物方向的法向量 n ，以及相关的投影矩阵 P:

$$D = \|p-p_{\mathrm{O}}\|,\quad n = \frac{p-p_{\mathrm{O}}}{\|p-p_{\mathrm{O}}\|},\quad P = I-nn^\top. \tag{22}$$

注意，$\partial D/\partial p = n^\top$ 和 $\partial n/\partial p = P/D$ 成立。此外，我们将航向方向描述为:

$$q = \begin{bmatrix}\cos\psi\\ \sin\psi\end{bmatrix},\quad r = \begin{bmatrix}-\sin\psi\\ \cos\psi\end{bmatrix}. \tag{23}$$

有了这些准备，我们引入以下从 [19]到用于刻画安全性的函数:

$$h(x,t) = D - R_{\mathrm{O}} + \delta n^\top q, \tag{24}$$

其中，可调参数 $\delta \geq 0$ 会对朝向障碍物的航向施加惩罚。相应的导数为:

$$\begin{aligned}\nabla h(x,t) &= \begin{bmatrix}n^\top + \delta q^\top P/D & \delta n^\top r\end{bmatrix},\\ \frac{\partial h}{\partial t}(x,t) &= -n^\top\dot{p}_{\mathrm{O}} - \delta q^\top P\dot{p}_{\mathrm{O}}/D.\end{aligned} \tag{25}$$

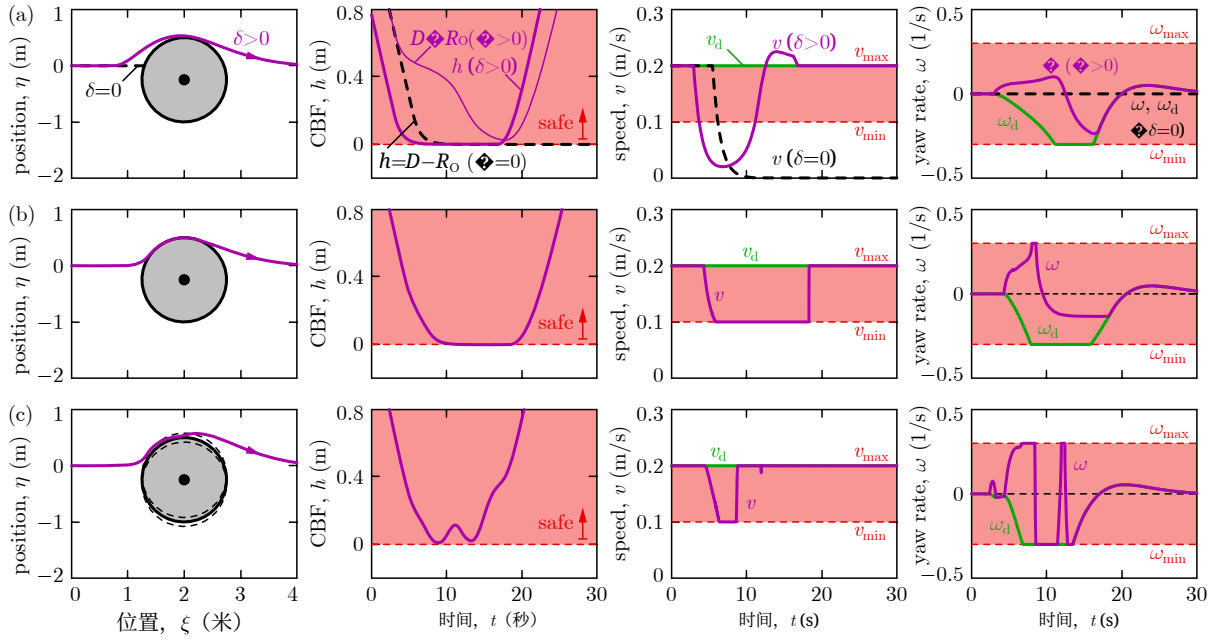


图 2. 独轮车模型的避障安全关键控制。(a) 基于控制屏障函数的控制器 (7) 可在不限制输入（速度和偏航角速度）的情况下保持安全。(b) 基于备份集方法的控制器 (19) 在输入约束下确保安全。(c) 控制器 (19) 可处理移动障碍物。

请注意，如果障碍物正在移动，则 h 会通过 p_{O} 显式依赖于时间，因此必须将 $\partial h/\partial t$ 纳入 h_{b}。对于静止障碍物，可以省略这种对 t 的依赖。

如果没有输入约束，h 可用作 CBF，控制器 (7) 将确保行为安全。图 2(a) 展示了针对表 I 中的参数以及 $x_0 = 0$，执行 (7) 并排除输入约束（即取$\mathcal{U} = \mathbb{R}^2$）时的结果。对于 $\delta = 0$，即 CBF 不对航向方向进行惩罚时，独轮车会在障碍物前停下（虚线），这样虽然安全，但过于保守。对于 $\delta > 0$，独轮车能够安全地执行任务（实线）。然而，由于优化问题中未纳入输入约束，速度上下限均被违反。另一方面，在存在输入约束时，h 不一定是有效的 CBF。

为处理输入约束，我们采用备份控制器：

$$k_{\mathrm{b}}(x,t) = \begin{bmatrix} v_{\max} \\ \omega_{\max}\tanh(n^{\top}r/\varepsilon) \end{bmatrix}, \tag{26}$$

该控制器旨在尽可能快速地使独轮车转向远离障碍物，并以最大速度驶离。参数ε 用于调节转向激进程度，偏航角速度$\pm\omega_{\max}$ 通过 $\varepsilon \to 0$实现。因此，该控制器能够确保我们避开速度低于$v_{\max}$ 且转向速率低于 $\omega_{\max}$的障碍物。

备份控制器与以下内容相关：

$$h_{\mathrm{b}}(x,t) = n^{\top}(qv_{\max} - \dot{p}_{\mathrm{O}}), \tag{27}$$

其导数为：

$$\begin{aligned} \nabla h_{\mathrm{b}}(x,t) &= \begin{bmatrix} (qv_{\max} - \dot{p}_{\mathrm{O}})^{\top}P/D & n^{\top}rv_{\max} \end{bmatrix}, \\ \frac{\partial h_{\mathrm{b}}}{\partial t}(x,t) &= -(qv_{\max} - \dot{p}_{\mathrm{O}})^{\top}P\dot{p}_{\mathrm{O}}/D - n^{\top}\ddot{p}_{\mathrm{O}}. \end{aligned} \tag{28}$$

数值示例的参数值（表 I）

参数	值	Unit	参数	值	Unit
$v_{\max}$	0.2	m/s	δ (例 1)	0, 0.5	m
$v_{\min}$	0.1	m/s	δ (例 2)	0	m
$\omega_{\max}$	0.3	弧度/秒	ε	0.01	1
η_{g}	0	m	γ	1	1/s
v_{g}	0.2	m/s	γ_{b}	1	1/s
K_η	0.5	1/(毫秒)	Γ	diag$\{1, 0.25\}$	$\{1, \mathrm{m}^2\}$
K_ψ	0.5	1/s	T	4	s
R_{O}	0.75	m	N_{c} (例 1)	80	1
ξ_{O}	2	m	N_{c} (例 2)	400	1
$\bar{\eta}_{\mathrm{O}}$	-0.25	m	σ	0.1	m/s
A_η	0.1	m/s	σ_{b}	0.1	m
Ω	$2\pi/5$	弧度/秒	p	10^{18}	1
			p_{b}	10^{18}	s^2

我们指出，由k_{b} 保持不变的备份集实际上由 $h_{\mathrm{b}}(x,\ t) \geq 0$和 $h(x,\ t) \geq 0$共同给出（而不只是 $h_{\mathrm{b}}(x,\ t) \geq 0$），但这两个函数都涉及式（15）。

参数如表 I 和 $\delta = 0$ 所示时，图 2(b) 展示了带控制器 (19) 的备份集方法的效果。该控制器在满足输入约束的同时保持安全性；值得注意的是，即使 $\delta = 0$，也能实现预期行为。图 2(c) 则测试了同一控制器在存在移动障碍物时的表现。障碍物沿 η 方向作正弦运动，其运动为 $p_{\mathrm{O}}(t) = \begin{bmatrix} \xi_{\mathrm{O}} & \eta_{\mathrm{O}}(t) \end{bmatrix}^{\top}$，$\eta_{\mathrm{O}}(t) = \bar{\eta}_{\mathrm{O}} - A_\eta \sin(\Omega t)/\Omega$。最终结果仍然是在有界输入下保持安全性。

III. 降阶模型

模型 (1) 通常是对真实控制系统的简化表示。实际动力学可能更加复杂、维度更高，且包含未建模现象，因此

我们称 (1) 为降阶模型 *(ROM)*。备份集方法能够在遵守输入约束的同时控制 ROM，并提供形式化安全保证。然而，实际全阶系统 *(FOS)*的安全性未必得到保证。接下来，我们研究未建模动力学对安全性的影响，并沿用先前的工作 [19]，推导保证 FOS 安全性的条件。随后，我们提出一种鲁棒化的备份集方法。本文假定 ROM 已知，而构建 ROM 的方法不在讨论范围内。最后，我们通过一个示例展示该框架：控制四足机器人的运动（FOS），使其跟随独轮车模型（ROM）。

考虑一个全阶系统，其状态为 $X \in \mathbb{R}^N$、输入为 $U \in \mathbb{R}^M$，局部利普希茨连续函数为 $F\colon \mathbb{R}^N \to \mathbb{R}^N$ 和$G\colon \mathbb{R}^N \to \mathbb{R}^{N\times M}$，其动力学为：

$$\dot{X} = F(X) + G(X)U. \tag{29}$$

此外，令降阶状态 $x \in \mathbb{R}^n$ 由连续可微映射 $P\colon \mathbb{R}^N \to \mathbb{R}^n$ 定义：

$$x = P(X). \tag{30}$$

选择降阶状态，使其能够描述安全关键行为。具体而言，考虑以下安全集：

$$\mathcal{C} = \{X \in \mathbb{R}^N : h(P(X)) \geq 0\} \tag{31}$$

对于具有 $h\colon \mathbb{R}^n \to \mathbb{R}$ （如前所述）的全阶系统。

为实现全阶系统的安全行为，可以构建类似于式（1）的降阶模型，设计安全关键降阶模型控制器 $u = k(x)$，并使用跟踪控制器 $K\colon \mathbb{R}^N \times \mathbb{R}^m \to \mathbb{R}^M$,$U = K(X,\ u)$，使闭环全阶系统：

$$\dot{X} = F(X) + G(X)K(X,u) \tag{32}$$

跟踪降阶模型。通过选择适当的降阶模型和跟踪控制器，降阶状态的真实动力学 x 能够准确跟踪降阶模型。真实的降阶动力学为：

$$\dot{x} = f(x) + g(x)u + d, \tag{33}$$

其中， $d \in \mathbb{R}^n$ 是相对于降阶模型的偏差，定义如下：

$$d = \nabla P(X)\big(F(X)+G(X)K(X,u)\big)-f(P(X))-g(P(X))u. \tag{34}$$

请注意，尽管 d 对降阶模型起扰动作用，但也可以将其视为全阶系统试图消除的跟踪误差。

如果偏差 d 为零，降阶模型就能准确捕捉全阶系统的安全关键行为，此时可直接将备份集方法与控制不变集结合使用：

$$\mathcal{C}_{\mathrm{I}} = \left\{ X \in \mathbb{R}^N : \begin{array}{l} h\big(\phi_{\mathrm{b}}(\theta, P(X))\big) \geq 0,\ \forall \theta \in [0,T], \\ h_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T, P(X))\big) \geq 0 \end{array} \right\}, \tag{35}$$

对于该控制器 $X \in \mathcal{C}_{\mathrm{I}} \iff x \in \mathcal{S}_{\mathrm{I}}$。随后，根据定理2，存在一个控制器 k，其满足（15），并使 $\mathcal{C}_{\mathrm{I}} \subseteq \mathcal{C}$ 沿（29）正向不变。然而，非零偏差 d 可能导致安全违规。下面我们将讨论在何种条件下能够保持安全性，并研究如何针对 d 提供鲁棒性。在鲁棒化过程中，考虑（33），同时将偏差 d 视为一个代表与降阶模型相关的建模误差和扰动的未知但有界项（见下述假设）。

A. 理想跟踪下的安全性

如果降阶模型和跟踪控制器设计良好，真实降阶动力学将收敛于降阶模型，且偏差 d 将消失。首先，我们考虑以下假设所反映的这一理想情形。

假设 2. 跟踪控制器 $U = K(x,u)$ 使真实降阶动力学与降阶模型之间的偏差指数收敛至零。也就是说，存在 $A \geq 0$和 $\lambda > 0$，使得 $\forall t \geq 0$:

$$\|d\| \leq A\mathrm{e}^{-\lambda t}. \tag{36}$$

为简便起见，我们假设指数收敛，不过也可以考虑右侧带有类-$\mathcal{KL}$ 函数的渐近稳定性。同样，为简化讨论，我们选用线性类-$\mathcal{K}_\infty$函数：$\alpha(r) = \gamma r$， $\alpha_{\mathrm{b}}(r) = \gamma_{\mathrm{b}} r$，其中 $\gamma, \gamma_{\mathrm{b}} > 0$。此外，我们假设 $h(\phi_{\mathrm{b}}(\theta,x))$和 $h_{\mathrm{b}}(\phi_{\mathrm{b}}(\theta,x))$的梯度有界，即存在 $D, D_{\mathrm{b}} \geq 0$，使得$\|\partial h\big(\phi_{\mathrm{b}}(\theta,x)\big)/\partial x\| \leq D$， $\forall \theta \in [0,T]$ 以及$\|\partial h_{\mathrm{b}}\big(\phi_{\mathrm{b}}(\theta,x)\big)/\partial x\| \leq D_{\mathrm{b}}$均成立，其中采用欧几里得范数 $\|.\|$。下一节将放宽这些假设。

在这些假设下，我们证明 $\mathcal{C}_{\mathrm{I}}$ 的一个时变子集是控制不变的。我们将该集合 $\mathcal{C}_{\mathrm{d}}(t)$定义为：

$$\mathcal{C}_{\mathrm{d}}(t) = \left\{ X \in \mathbb{R}^N : \begin{array}{l} H(\theta,X,t) \geq 0,\ \forall \theta \in [0,T], \\ H_{\mathrm{b}}(T,X,t) \geq 0 \end{array} \right\}, \tag{37}$$

其中：

$$\begin{aligned} H(\theta,X,t) &= h\big(\phi_{\mathrm{b}}(\theta, P(X))\big) - \frac{DA\mathrm{e}^{-\lambda t}}{\lambda - \gamma}, \\ H_{\mathrm{b}}(T,X,t) &= h_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T, P(X))\big) - \frac{D_{\mathrm{b}}A\mathrm{e}^{-\lambda t}}{\lambda - \gamma_{\mathrm{b}}}. \end{aligned} \tag{38}$$

定理3。 考虑降阶模型*(1)*、*(11)*中的集合 $\mathcal{S}_{\mathrm{I}}$ 以及满足*(15)*的局部利普希茨连续控制器 k： $\mathbb{R}^n \to \mathcal{U}$，其中 $\alpha(r) = \gamma r$、$\alpha_{\mathrm{b}}(r) = \gamma_{\mathrm{b}} r$、 $\forall x \in \mathcal{S}_{\mathrm{I}}$。此外，考虑全阶系统*(29)*、降阶状态*(30)*、*(31)*中的集合 $\mathcal{C}$ 、*(37)-(38)*中的集合 $\mathcal{C}_{\mathrm{d}}(t)$ 以及假设*2*。若γ、 $\gamma_{\mathrm{b}} < \lambda$，则 $\mathcal{C}_{\mathrm{d}}(t) \subseteq \mathcal{C}$ 沿*(32)*正向不变。

证明。 对于 γ， $\gamma_{\mathrm{b}} < \lambda$，式（38）中的项 $DA/(\lambda-\gamma)\mathrm{e}^{-\lambda t}$ 和 $D_{\mathrm{b}}A/(\lambda-\gamma_{\mathrm{b}})\mathrm{e}^{-\lambda t}$ 均为非负 $\forall t \geq 0$。因此，$\mathcal{C}_{\mathrm{d}}(t) \subseteq \mathcal{C}_{\mathrm{I}}$， $\forall t \geq 0$，且 $X \in \mathcal{C}_{\mathrm{d}}(t)$意味着 $x \in \mathcal{S}_{\mathrm{I}}$。于是，可以应用定理2，并保证存在满足式（15）的控制器 k，对于所有 $X \in \mathcal{C}_{\mathrm{d}}(t)$均成立，因为 $x \in \mathcal{S}_{\mathrm{I}}$。根据式（38）和式（15），沿着式（32）的 H 的导数满足：

$$\begin{aligned} &\dot{H}(\theta,X,t,k(P(X)),d) \\ &= \dot{h}\big(\phi_{\mathrm{b}}(\theta,x),k(x)\big) + \frac{\partial h\big(\phi_{\mathrm{b}}(\theta,x)\big)}{\partial x} d + \frac{\lambda DA\mathrm{e}^{-\lambda t}}{\lambda - \gamma} \\ &\geq -\gamma h(\phi_{\mathrm{b}}(\theta,x)) - \left\| \frac{\partial h\big(\phi_{\mathrm{b}}(\theta,x)\big)}{\partial x} \right\| \|d\| + \frac{\lambda DA\mathrm{e}^{-\lambda t}}{\lambda - \gamma} \\ &\geq -\gamma h(\phi_{\mathrm{b}}(\theta,x)) - DA\mathrm{e}^{-\lambda t} + \frac{\lambda DA\mathrm{e}^{-\lambda t}}{\lambda - \gamma} \\ &\geq -\gamma H(\theta,X,t). \end{aligned} \tag{39}$$

类似地，可以证明 $H_{\mathrm{b}}(T,\ X,\ t,\ k(P(X))\ d) \geq -\gamma_{\mathrm{b}} H_{\mathrm{b}}(T,\ X,\ t)$。因此，根据定理1，我们可以得出 $\mathcal{C}_{\mathrm{d}}(t) \subseteq \mathcal{C}_{\mathrm{I}}$具有正向不变性，这意味着全阶系统是安全的。 □

备注1. 定理3指出，只要对降阶模型的跟踪足够快，全阶系统就能保持安全，并在一个保证存在基于备份集方法的控制器的区域内演化。不过，该结果以理想的指数跟踪（以及关于 h 和 h_{b}的有界梯度的技术性假设）为前提。接下来，我们将放宽这些限制。

B. 输入到状态安全备份集方法

我们采用以下较弱的跟踪假设。

假设3. 跟踪控制器 $U = K(x,u)$使真实降阶动力学与降阶模型之间的偏差指数收敛到零的一个邻域。也就是说，存在 $A, B \geq 0$ 和 $\lambda > 0$，使得 $\forall t \geq 0$:

$$\|d\|^2 \leq A\mathrm{e}^{-\lambda t} + B. \tag{40}$$

请注意，该假设包含情形 $A = 0$，即偏差不一定衰减，而是保持在 B以下。我们还要指出，在 d的范数后面加上平方仅仅是为了代数运算方便。下面的四足机器人示例将说明该假设成立。

当偏差无法衰减至零（$B \neq 0$）时，式（15）便无法再形式化地保证安全性。为解决这一问题，一些控制障碍函数方法会在其安全约束中添加额外的鲁棒化项 [9], [11]。例如，输入到状态安全控制障碍函数方法会将（6）修改为$\dot{h}(x,\ k(x)) \geq -\alpha(h(x)) + \sigma\|\nabla h(x)\|^2$ 其中 $\sigma > 0$（当$\nabla h(x)$可被 $\nabla h(x) g(x)$替代时，适用于匹配扰动）[10]。我们提出将这一方法扩展到输入到状态安全备份集方法，将（15）修改为:

$$\begin{aligned}
\dot{h}\big(\phi_{\mathrm{b}}(\theta,x),k(x)\big) &\geq -\alpha\big(h(\phi_{\mathrm{b}}(\theta,x))\big) \\
&\quad + \sigma\left\|\frac{\partial h(\phi_{\mathrm{b}}(\theta,x))}{\partial x}\right\|^2,\ \forall\theta\in[0,T], \\
\dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T,x),k(x)\big) &\geq -\alpha_{\mathrm{b}}\big(h_{\mathrm{b}}(\phi_{\mathrm{b}}(T,x))\big) \\
&\quad + \sigma_{\mathrm{b}}\left\|\frac{\partial h_{\mathrm{b}}(\phi_{\mathrm{b}}(T,x))}{\partial x}\right\|^2,
\end{aligned} \tag{41}$$

其中可调参数为 $\sigma,\ \sigma_{\mathrm{b}} > 0$。

输入到状态安全控制障碍函数方法能够在存在扰动的情况下，使安全集的一个邻域保持不变，并且通过参数 σ 可以将该邻域调节到任意小。我们希望利用备份集方法，在存在输入约束的情况下实现相同的结果。因此，我们考虑控制不变集 $\mathcal{S}_{\mathrm{I}}$的一个邻域 $\mathcal{S}_{\mathrm{d}}$：

$$\mathcal{S}_{\mathrm{d}} = \left\{x\in\mathbb{R}^n:\ \begin{matrix} h(\phi_{\mathrm{b}}(\theta,x)) \geq -B/(4\sigma\gamma),\ \forall\theta\in[0,T], \\ h_{\mathrm{b}}(\phi_{\mathrm{b}}(T,x)) \geq -B/(4\sigma_{\mathrm{b}}\gamma_{\mathrm{b}}) \end{matrix}\right\}, \tag{42}$$

由 σ、σ_{b} 确定，并将式 (37) 中的集合 $\mathcal{C}_{\mathrm{d}}(t)$ 重新定义为:

$$\begin{aligned}
H(\theta,X,t) &= h\big(\phi_{\mathrm{b}}(\theta,P(X))\big) - \frac{A\mathrm{e}^{-\lambda t}}{4\sigma(\lambda-\gamma)} + \frac{B}{4\sigma\gamma}, \\
H_{\mathrm{b}}(T,X,t) &= h_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T,P(X))\big) - \frac{A\mathrm{e}^{-\lambda t}}{4\sigma_{\mathrm{b}}(\lambda-\gamma_{\mathrm{b}})} + \frac{B}{4\sigma_{\mathrm{b}}\gamma_{\mathrm{b}}}.
\end{aligned} \tag{43}$$

然后，我们说明集合 $\mathcal{C}_{\mathrm{d}}(t)$ 的不变性；通过增大 σ、σ_{b}，可以使该集合任意接近安全集 $\mathcal{C}$。

定理 4。 考虑 *ROM (1)*，将 $\mathcal{S}_{\mathrm{d}}$ 设为 *(42)* 中的集合，并考虑满足 *(41)* 且具有 $\alpha(r) = \gamma r$, $\alpha_{\mathrm{b}}(r) = \gamma_{\mathrm{b}} r$, $\forall x \in \mathcal{S}_{\mathrm{d}}$ 的局部利普希茨连续控制器 k：$\mathbb{R}^n \to \mathcal{U}$。此外，考虑 *FOS (29)*、降阶状态 *(30)*、*(37)–(43)* 中的集合 $\mathcal{C}_{\mathrm{d}}(t)$ 以及假设 *3*。若 $\gamma, \gamma_{\mathrm{b}} < \lambda$，则 $\mathcal{C}_{\mathrm{d}}(t)$沿着 *(32)* 正向不变。

证明。 首先，我们证明以下不等式成立:

$$\begin{aligned}
&\sigma\left\|\frac{\partial h(\phi_{\mathrm{b}}(\theta,x))}{\partial x}\right\|^2 - \left\|\frac{\partial h(\phi_{\mathrm{b}}(\theta,x))}{\partial x}\right\|\|d\| \\
&\quad\geq \left(\sqrt{\sigma}\left\|\frac{\partial h(\phi_{\mathrm{b}}(\theta,x))}{\partial x}\right\| - \frac{\|d\|}{2\sqrt{\sigma}}\right)^2 - \frac{\|d\|^2}{4\sigma} \\
&\quad\geq -\frac{A\mathrm{e}^{-\lambda t}+B}{4\sigma}.
\end{aligned} \tag{44}$$

然后，证明的其余部分可按照定理3进行:

$$\begin{aligned}
&\dot{H}(\theta,X,t,k(P(X)),d) \\
&\quad= \dot{h}\big(\phi_{\mathrm{b}}(\theta,x),k(x)\big) + \frac{\partial h\big(\phi_{\mathrm{b}}(\theta,x)\big)}{\partial x} d + \frac{\lambda A\mathrm{e}^{-\lambda t}}{4\sigma(\lambda-\gamma)} \\
&\quad\geq -\gamma h(\phi_{\mathrm{b}}(\theta,x)) - \frac{A\mathrm{e}^{-\lambda t}+B}{4\sigma} + \frac{\lambda A\mathrm{e}^{-\lambda t}}{4\sigma(\lambda-\gamma)} \\
&\quad\geq -\gamma H(\theta,X,t),
\end{aligned} \tag{45}$$

参见 (39)，其中第二步使用了柯西–施瓦茨不等式，并代入了 (44)。 □

注 2。 定理 4 表明，对 ROM 进行输入到状态稳定跟踪（即偏差 d 衰减至零或处于零的某个邻域内）会使 FOS 保持在集合 $\mathcal{C}_{\mathrm{d}}(t)$ 中。利用 σ 和 σ_{b}，参见 (43)，可以将该集合调节得任意接近安全集 $\mathcal{C}$，并且它不再依赖于 h 和 h_{b} 的梯度界。然而，我们无法再声称存在满足 (41) $\forall x \in \mathcal{S}_{\mathrm{d}}$ 的控制器 k。因此，可以采用松弛优化问题代替 (19):

$$\begin{aligned}
k(x) = \underset{\substack{u\in\mathcal{U} \\ \delta_i,\delta_{\mathrm{b}}\geq 0}}{\operatorname{argmin}}\ &\|u - k_{\mathrm{d}}(x)\|_\Gamma^2 + \sum_{i\in\mathcal{I}} p_i\delta_i^2 + p_{\mathrm{b}}\delta_{\mathrm{b}}^2 \\
\text{s.t. } &\dot{\bar{h}}_i(x,u) \geq -\alpha\big(\bar{h}_i(x)\big) + \sigma\left\|\frac{\partial \bar{h}_i(x)}{\partial x}\right\|^2 - \delta_i, \\
&\qquad\qquad \forall i\in\mathcal{I}, \\
&\dot{\bar{h}}_{\mathrm{b}}(x,u) \geq -\alpha_{\mathrm{b}}\big(\bar{h}_{\mathrm{b}}(x)\big) + \sigma_{\mathrm{b}}\left\|\frac{\partial \bar{h}_{\mathrm{b}}(x)}{\partial x}\right\|^2 - \delta_{\mathrm{b}},
\end{aligned} \tag{46}$$

引入松弛变量 $\delta_i,\ \delta_{\mathrm{b}} \geq 0$并设置惩罚项 $p_i,\ p_{\mathrm{b}} \gg 1, i \in \mathcal{I}$。如何在不进行这种松弛的情况下，制定可证明安全且可行的控制器，仍有待未来研究。

示例2（四足运动）。 考虑图3所示的 Unitree A1 四足机器人。我们希望实现腿式运动，并完成示例1中的避障任务。我们将四足机器人视为全阶系统，并依靠现有的步行控制器，以给定的速度和偏航角速度实现运动。

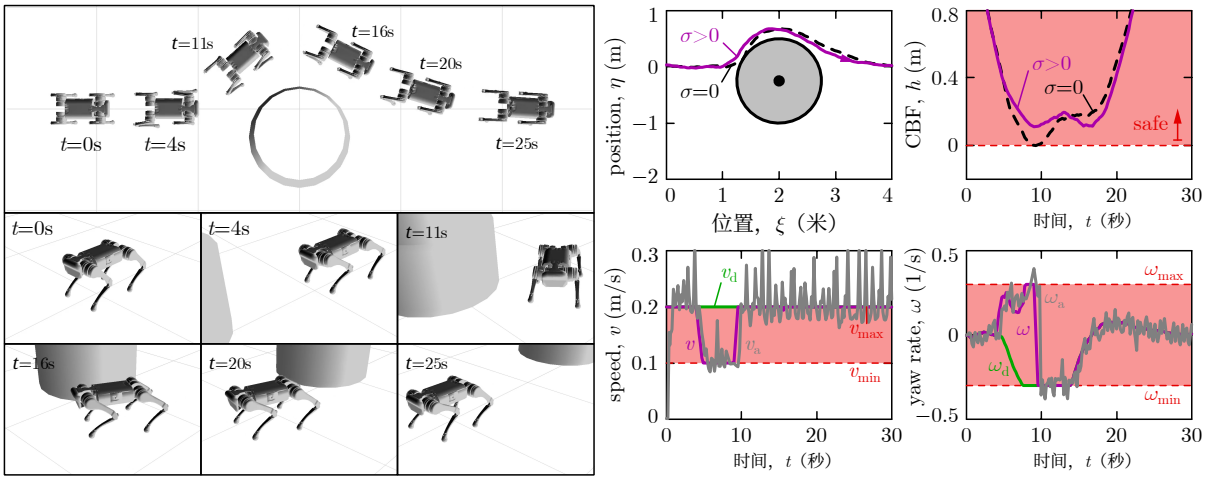


图 3. 在四足运动中，采用输入受限降阶模型的所提出安全关键控制框架。四足机器人通过跟踪由独轮车模型和输入到状态安全备份集方法合成的速度和偏航角速度，实现安全导航。

在给定速度和偏航角速度的情况下，步行过程会跟踪示例1中的独轮车模型，该模型作为降阶模型。

四足机器人具有 18 个自由度和 12 个驱动关节。其运动由构型$q \in \mathbb{R}^{18}$、速度 $\dot{q} \in \mathbb{R}^{18}$、输入 $U \in \mathbb{R}^{12}$ 以及完整约束 $c(q) \equiv 0 \in \mathbb{R}^{n_c}$ 下足部与地面之间的接触数量 n_c 描述。其动力学由欧拉-拉格朗日方程支配：

$$\begin{aligned} D(q)\ddot{q} + H(q,\dot{q}) &= BU + J(q)^\top \lambda, \\ J(q)\ddot{q} + \dot{J}(q,\dot{q})\dot{q} &= 0, \end{aligned} \tag{47}$$

质量矩阵 $D(q) \in \mathbb{R}^{18\times 18}$、科里奥利项和重力项$H(q,\ \dot{q}) \in \mathbb{R}^{18}$、雅可比矩阵 $J(q) = \partial c(q)/\partial q \in \mathbb{R}^{n_c \times 18}$以及约束力旋量 $\lambda \in \mathbb{R}^{n_c}$。由此得到状态为 $X = \begin{bmatrix} q^\top & \dot{q}^\top \end{bmatrix}^\top \in \mathbb{R}^{36}$ 的全阶系统（29）以及以下表达式：

$$F(X) = \begin{bmatrix} \dot{q} \\ -D(q)^{-1}\big(H(q,\dot{q}) - J(q)^\top \lambda\big) \end{bmatrix},\ G(X) = \begin{bmatrix} 0 \\ D(q)^{-1}B \end{bmatrix}. \tag{48}$$

在避障过程中，安全性由平面机身位置 ξ 和 η 以及偏航角 ψ决定，从而得到示例1中的降阶状态 $x \in \mathbb{R}^3$。这些状态是全状态 X的元素。全阶系统（47）中的相应方程在忽略横滚和俯仰后可简化为独轮车模型（20），因此选择独轮车作为降阶模型。对于腿式运动，我们使用基于逆动力学二次规划的步行控制器 $U = K(X,\ u)$，详见 [20]。只要降阶输入 $u \in \mathbb{R}^2$ 中的速度和偏航角速度指令分别低于 $v_{\max}$ 并处于 $\pm\omega_{\max}$之间，该控制器就能跟踪这些指令。我们还规定最小速度 $v_{\min}$，以确保四足机器人不会停下。我们采用示例1中详述的输入到状态安全备份集方法，在这些界限内寻找安全的速度和偏航角速度指令。

图 3 展示了四足运动的高保真仿真[2]。速度和偏航角速度通过以下方式设定：

[2]视频链接：https://youtu.be/h8-x7-4eqWs。

所提出的控制器 (46)、示例1中的公式、表 I 中的参数以及 CVXOPT 求解器 [21]。半径 R_O 内是机器人中心不得进入的区域，该半径由障碍物半径 (0.45m) 和四足机器人的尺寸 (0.3 m) 组成。使用所提出的控制器时，四足机器人如运动轨迹图所示，成功绕过了障碍物。请注意，系统始终满足安全性规范 h。同时，速度和偏航角速度指令保持在期望范围内（尽管其实际值可能超出范围）。该图还通过比较实际速度 v_a 和偏航角速度 ω_a（从 X中提取）与指令 v 和 ω，展示了步行控制器的跟踪性能。事实上，如假设3中的 (40) 所示，指令速度 $\dot{x} = \begin{bmatrix} v\cos\psi & v\sin\psi & \omega \end{bmatrix}^\top$ 与相应实际值之间的偏差 d 逐渐衰减并保持有界。最后，图中以虚线显示了采用标准备份集方法时的轨迹（即控制器 (19) 和 $\sigma = 0, \sigma_b = 0$）。由于缺乏对降阶模型与全阶系统之间偏差的鲁棒性，这种情况下的轨迹更接近安全违规边界。

此示例展示了所提出的安全关键控制方法的有效性。该方法将受输入约束的降阶模型与备份集方法以及可靠的跟踪控制器相结合。结果表明，在避障过程中，复杂四足机器人能够安全运行。

IV. 结论

本文研究了采用具有有界输入的降阶模型进行安全关键控制。为在满足输入约束的同时从形式上保证安全，本文采用了备份集方法。本文分析了降阶模型与全阶系统之间偏差所带来的鲁棒性问题，并推导出确保全阶系统安全的条件，提出了输入到状态安全备份集方法，以增强系统对上述偏差的鲁棒性。通过使用独轮车模型控制四足机器人进行障碍物

避障，本文验证了所提出控制框架的有效性。未来工作将研究鲁棒化控制器的可行性。

附录

引理 *1* 的证明。 根据 $\mathcal{S}_{\mathrm{I}}$ 的定义 (11) 和假设 1，我们有：

$$x \in \mathcal{S}_{\mathrm{I}} \implies \phi_{\mathrm{b}}(\theta, x) \in \mathcal{S}_{\mathrm{b}} \subseteq \mathcal{S},\ \forall \theta \geq T. \tag{49}$$

由此，并根据以下事实：

$$\phi_{\mathrm{b}}(\theta + \vartheta, x_0) = \phi_{\mathrm{b}}(\theta, \phi_{\mathrm{b}}(\vartheta, x_0)), \tag{50}$$

对任意 $\theta,\ \vartheta \geq 0$ 和 $x_0 \in \mathbb{R}^n$ 均成立，我们得到：

$$x \in \mathcal{S}_{\mathrm{I}} \implies \phi_{\mathrm{b}}(T, \phi_{\mathrm{b}}(\vartheta, x)) \in \mathcal{S}_{\mathrm{b}},\ \forall \vartheta \geq 0. \tag{51}$$

此外， $\mathcal{S}_{\mathrm{I}}$ 的定义 (11) 和 (49) 给出：

$$x \in \mathcal{S}_{\mathrm{I}} \implies \phi_{\mathrm{b}}(\theta, x) \in \mathcal{S},\ \forall \theta \geq 0. \tag{52}$$

再次利用性质 (50)，我们得到：

$$x \in \mathcal{S}_{\mathrm{I}} \implies \phi_{\mathrm{b}}(\theta,\ \phi_{\mathrm{b}}(\vartheta,\ x)) \in \mathcal{S},\quad \forall \theta \in [0, T],\ \forall \vartheta \geq 0. \tag{53}$$

因此，由 (51)、(53) 以及 $\mathcal{S}_{\mathrm{I}}$ 的定义 (11)，可得 (12)。□

引理 *2* 的证明。 $\mathcal{S}_{\mathrm{I}}$ 的定义 (11) 可改写为：

$$\mathcal{S}_{\mathrm{I}} = \left\{ x \in \mathbb{R}^n :\ \begin{array}{l} h(\phi_{\mathrm{b}}(\theta, x)) \geq 0,\ \forall \theta \in [0, T], \\ h_{\mathrm{b}}(\phi_{\mathrm{b}}(T, x)) \geq 0 \end{array} \right\}. \tag{54}$$

根据引理 1，$\mathcal{S}_{\mathrm{I}}$ 由备份控制器 k_{b} 渲染为正向不变。因此，Nagumo 定理 [22] 表明：

$$\begin{aligned} h(\phi_{\mathrm{b}}(\theta, x)) = 0 &\implies \dot{h}\big(\phi_{\mathrm{b}}(\theta, x), k_{\mathrm{b}}(x)\big) \geq 0, \\ h_{\mathrm{b}}(\phi_{\mathrm{b}}(T, x)) = 0 &\implies \dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T, x), k_{\mathrm{b}}(x)\big) \geq 0. \end{aligned} \tag{55}$$

考虑第二个条件，并令：

$$\tilde{\mathcal{S}}(x) = \{\tilde{x} \in \mathbb{R}^n : h_{\mathrm{b}}(\phi_{\mathrm{b}}(T, x)) \geq h_{\mathrm{b}}(\phi_{\mathrm{b}}(T, \tilde{x})) \geq 0\}. \tag{56}$$

注意到 $\forall x \in \mathcal{S}_{\mathrm{b}}$, $\mathcal{S}(x)$ 非空且 $x \in \mathcal{S}(x)$，因此：

$$\dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T, x), k_{\mathrm{b}}(x)\big) \geq \inf_{\tilde{x} \in \tilde{\mathcal{S}}(x)} \dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T, \tilde{x}), k_{\mathrm{b}}(\tilde{x})\big). \tag{57}$$

现在定义集合 $\mathcal{S}_r$，其中 $r \geq 0$ 和 $\tilde{\alpha}_{\mathrm{b}}$ 为：$\mathbb{R}_{\geq 0} \to \mathbb{R}$：

$$\tilde{\mathcal{S}}_r = \{\tilde{x} \in \mathbb{R}^n : r \geq h_{\mathrm{b}}(\phi_{\mathrm{b}}(T, \tilde{x})) \geq 0\}. \tag{58}$$

$$\tilde{\alpha}_{\mathrm{b}}(r) = -\inf_{\tilde{x} \in \tilde{\mathcal{S}}_r} \dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T, \tilde{x}), k_{\mathrm{b}}(\tilde{x})\big). \tag{59}$$

那么，(57) 等价于：

$$\dot{h}_{\mathrm{b}}\big(\phi_{\mathrm{b}}(T, x), k_{\mathrm{b}}(x)\big) \geq -\tilde{\alpha}_{\mathrm{b}}\big(h_{\mathrm{b}}(\phi_{\mathrm{b}}(T, x))\big). \tag{60}$$

注意，由于随着 r 增大，取下确界的集合更大，因此 $\tilde{\alpha}_{\mathrm{b}}$ 关于 r 单调递增 $\mathcal{S}_r$。此外，根据（55），$\tilde{\alpha}_{\mathrm{b}}$ 满足 $\tilde{\alpha}_{\mathrm{b}}(0) \leq 0$。因此，存在 $\alpha_{\mathrm{b}} \in \mathcal{K}_\infty$ 使得 $\alpha_{\mathrm{b}}(r) \geq \tilde{\alpha}_{\mathrm{b}}(r),\ \forall r \geq 0$。结合（60），可得（14）中的第二个结论。第一个结论也可用相同方法证明：对每个 $\theta \in [0, T]$ 证明 $\alpha_\theta \in \mathcal{K}_\infty$ 的存在，并定义 $\alpha \in \mathcal{K}_\infty$，使得 $\alpha(r) = \max_{\theta \in [0,T]} \alpha_\theta(r)$。□

致谢。感谢 Albert Li 和 Andrew Taylor 就基于降阶模型的安全问题进行讨论，也感谢 Wyatt Ubellacker 在为四足机器人综合低层控制器方面给予的宝贵帮助。

参考文献

[1] R. T. Fawcett、K. Afsari、A. D. Ames 和 K. A. Hamed，《面向四足运动的数据驱动模板模型》，IEEE《机器人学与自动化快报》，第 7 卷第 3 期，第 7636–7643 页，2022 年。[2] X. Xiong 和 A. Ames，《基于 H-LIP 步态合成与迈步稳定化的三维欠驱动双足行走》，IEEE《机器人学汇刊》，第 38 卷第 4 期，第 2405–2425 页，2022 年。[3] A. D. Ames、X. Xu、J. W. Grizzle 和 P. Tabuada，《面向安全关键系统的基于控制障碍函数的二次规划》，IEEE《自动控制汇刊》，第 62 卷，第 8 期，第 3861–3876 页，2017 年。[4] P. Glotfelter、J. Cort´es 和 M. Egerstedt，《非光滑障碍函数及其在多机器人系统中的应用》，IEEE《控制系统快报》，第 1 卷第 2 期，第 310–315 页，2017 年。[5] K. Dunlap、M. Hibbard、M. Mote 和 K. Hobbs，《安全航天器对接的运行时保障方法比较》，IEEE《控制系统快报》，第 6 卷，第 1849–1854 页，2022 年。[6] T. Gurriet、M. Mote、A. Singletary、P. Nilsson、E. Feron 和 A. D. Ames，《面向非线性系统的可扩展安全关键控制框架》，IEEE Access，第 8 卷，第 187 249–187 275 页，2020 年。[7] D. R. Agrawal 和 D. Panagou，《通过输入受限控制障碍函数进行安全控制综合》，载于第 60 届 IEEE 决策与控制会议，2021 年，第 6113–6118 页。[8] S. Liu、J. Dolan 和 C. Liu，《利用神经控制障碍函数实现输入饱和下的安全控制》，载于第 6 届机器人学习年会，2022 年。[9] S. Kolathaya 和 A. D. Ames，《利用控制障碍函数实现输入到状态安全》，IEEE《控制系统快报》，第 3 卷第 1 期，第 108–113 页，2019 年。[10] A. Alan、A. J. Taylor、C. R. He、G. Orosz 和 A. D. Ames，《利用可调输入到状态安全控制障碍函数进行安全控制器综合》，IEEE《控制系统快报》，第 6 卷，第 908–913 页，2022 年。[11] M. Jankovic，《用于非线性系统受约束稳定化的鲁棒控制障碍函数》，Automatica，第 96 卷，第 359–367 页，2018 年。[12] J. Ding、E. Li、H. Huang 和 C. J. Tomlin，《在有界扰动下针对运动规划的反馈策略的基于可达性的综合》，载于 IEEE 国际机器人与自动化会议，2011 年，第 2160–2165 页。[13] S. Bansal、M. Chen、S. Herbert 和 C. J. Tomlin，《Hamilton-Jacobi可达性：简要综述与最新进展》，载于第 56 届 IEEE 决策与控制会议，2017 年，第 2242–2253 页。[14] S. Kousik、S. Vaskov、F. Bu、M. Johnson-Roberson 和 R. Vasude-van，《弥合移动机器人滚动时域轨迹设计中的安全性与实时性能之间的差距》，《国际机器人研究期刊》，第 39 卷第 12 期，第 1419–1469 页，2020 年。[15] J. J. Choi、D. Lee、K. Sreenath、C. J. Tomlin 和 S. L. Herbert，《用于安全关键控制的鲁棒控制障碍值函数》，载于第 60 届 IEEE 决策与控制会议，2021 年，第 6814–6821 页。[16] Y. Chen、M. Jankovic、M. Santillo 和 A. D. A mes，《备用控制屏障函数：构建与比较研究》，载于第 60 届 IEEE 决策与控制会议，2021 年，第 6835–6841 页。[17] I. Exarchos、P. Tsiotras 和 M. Pachter，《关于自杀式行人的微分博弈》，《动态博弈与应用》，第 5 卷第 3 期，第 297–317 页，2015 年。[18] Y. Shoukry、P. Tabuada、S. Tsuei、M. B. Milam、J. W. Grizzle 和 A. D. Ames，《用于行人避障的闭式受控不变集》，载于美国控制会议，2017 年，第 1622–1628 页。[19] T. G. Molnar、R. K. Cosner、A. W. Singletary、W. Ubellacker 和 A. D. Ames，《面向机器人系统的无模型安全关键控制》，IEEE《机器人学与自动化快报》，第 7 卷第 2 期，第 944–951 页，2022 年。[20] W. Ubellacker、N. Csomay-Shanklin、T. G. Molnar 和 A. D. Ames，《验证腿式机器人上动态运动基元之间的安全转换》，载于 IEEE/RSJ 智能机器人与系统国际会议，2021 年，第 8477–8484 页。[21] M. S. Andersen、J. Dahl 和 L. Vandenberghe，《CVXOPT：用于凸优化的 Python软件包》，2012 年，网址：https://cvxopt.org/。[22] M. Nagumo，《关于常微分方程积分曲线的位置》，《日本物理数学会会刊》第三辑，第 24 卷，第 551–559 页，1942 年。