Reach-Avoid Controllers Synthesis for Safety Critical Systems

安全攸关系统可达-规避控制器生成

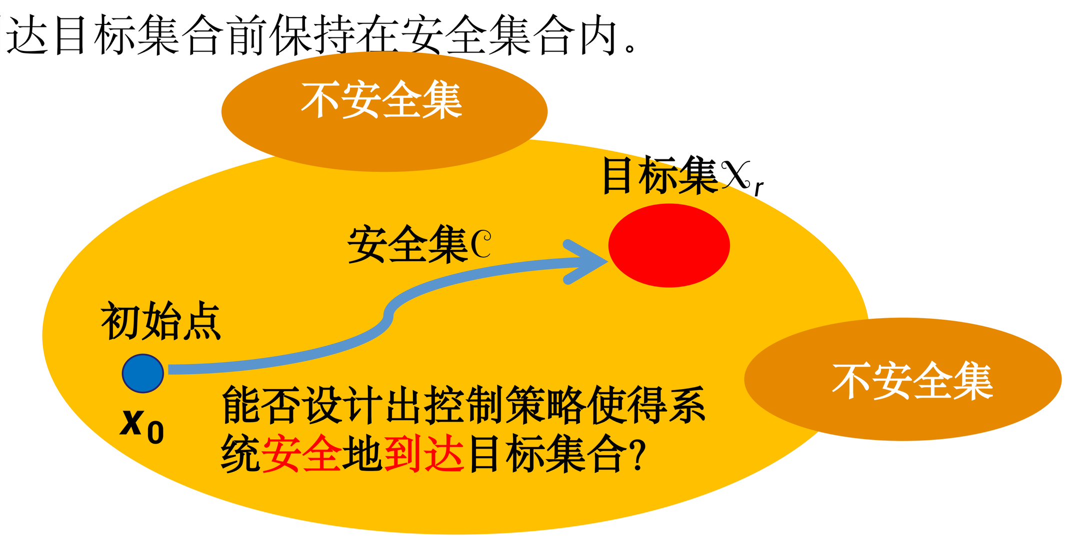
Bai Xue

IEEE Transactions on Automatic Control, vol. 69, no. 12, 8892 - 8899, December 2024.

联系人：薛白　邮箱： xuebai@ios.ac.cn

研究背景

- 针对安全攸关系统，我们需解决如下控制问题：给定一个控制器 $\boldsymbol{u}=\boldsymbol{k}(\boldsymbol{x})$，希望合成新的控制器且满足：(1) 能够最小程度地改变已有控制器 $\boldsymbol{k}(\boldsymbol{x})$; (2) **可达-规避性:** 系统能够到达目标集合，且在到达目标集合前保持在安全集合内。



s. t. $\| \boldsymbol{u}(\boldsymbol{x}) - \boldsymbol{k}(\boldsymbol{x}) \|$
as small as possible

- 我们分别对**仿射确定控制系统**及**仿射确定控制系统,** 在控制器生成的过程中融入了三种可达-规避验证的方法，用**验证**的方法指导并**生成**满足可达-规避性质的最优控制器。

可达-规避分析

仿射确定控制系统与仿射随机控制系统

针对**仿射确定控制系统**

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

给定一个控制器 $\boldsymbol{u}=\boldsymbol{k}(\boldsymbol{x})$(可能不是可达-规避控制器)，我们希望合成新的控制器，且满足：(1) 能够最小程度地改变已有控制器; (2) 可达-规避性。即如下优化问题：

$$\boldsymbol{u}(\boldsymbol{x}) = \arg\min \| \boldsymbol{u}(\boldsymbol{x}) - \boldsymbol{k}(\boldsymbol{x}) \|$$

且 $u(.): \mathbb{C} \to \mathbb{U}$ 是一个**可达-规避控制器**即满足:

$$\left\{u \in \Omega \,\middle|\, \begin{array}{l} \exists t \geq 0.\ \varphi_{x_0}^{u}(t) \in \mathbb{X}_r \wedge \\ \forall \tau \in [0,t] \cdot \varphi_{x_0}^{u}(\tau) \in \mathbb{C} \end{array}\right\}.$$

针对**仿射随机控制系统**

$$\begin{aligned} d\boldsymbol{x}(t,\boldsymbol{w}) = \ & (\boldsymbol{f}(\boldsymbol{x}(t,\boldsymbol{w})) + \boldsymbol{g}(\boldsymbol{x}(t,\boldsymbol{w}))\boldsymbol{u}(\boldsymbol{x}(t)))dt \\ & + \boldsymbol{\sigma}(\boldsymbol{x}(t,\boldsymbol{w}))d\boldsymbol{W}(t,\boldsymbol{w}) \end{aligned}$$

给定一个控制器 $\boldsymbol{u}=\boldsymbol{k}(\boldsymbol{x})$(可能不是可达-规避控制器)，我们希望合成新的控制器，且满足：(1) 能够最小程度地改变已有控制器; (2) 可达-规避性。即如下优化问题：

$$\boldsymbol{u}(\boldsymbol{x}) = \arg\min \| \boldsymbol{u}(\boldsymbol{x}) - \boldsymbol{k}(\boldsymbol{x}) \|$$

且 $u(.): \mathbb{C} \to \mathbb{U}$ 是一个**可达-规避控制器**即满足:

$$\mathbb{P}\left(u \in \Omega \,\middle|\, \begin{array}{l} \exists t \geq 0.\ \varphi_{x_0}^{u}(t) \in \mathbb{X}_r \wedge \\ \forall \tau \in [0,t] \cdot \varphi_{x_0}^{u}(\tau) \in \mathbb{C} \end{array}\right) \geq h(x_0).$$

可达-规避控制器生成

指数控制引导栅栏函数[1]

针对仿射确定控制系统(1)，如果 $h_{\mathbb{C}}(\boldsymbol{x})$ 是一个关于局部Lipschitz连续的控制器 $u(\boldsymbol{x})$ 的**指数控制引导栅栏函数**，即满足约束(2)，

$$\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) + \boldsymbol{g}(\boldsymbol{x})\boldsymbol{u} \quad (1)$$

$$\mathcal{L}_f h_{\mathbb{C}}(\boldsymbol{x}) + \mathcal{L}_g h_{\mathbb{C}}(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x}) - \lambda h_{\mathbb{C}}(\boldsymbol{x}) \geq 0,\ \forall x \in \mathbb{C} \setminus \overline{\mathbb{X}}_r,\ \lambda > 0. \quad (2)$$

其中 $\mathbb{C} = \{\boldsymbol{x} \in \boldsymbol{R}^n \mid h_{\mathbb{C}}(\boldsymbol{x}) > 0\}$ 是安全集合，则系统(1)在控制器 $\boldsymbol{u}(\boldsymbol{x})$ 下满足可达-规避性质。

渐近控制引导栅栏函数

针对仿射确定控制系统(1)，如果 $h_{\mathbb{C}}(\boldsymbol{x})$ 是一个关于局部Lipschitz连续的控制器 $u(\boldsymbol{x})$ 的**渐近控制引导栅栏函数**，即满足存在连续可微函数 $w_{\mathbb{C}}(\boldsymbol{x})$ 使得(3)成立，

$$\begin{aligned} & \mathcal{L}_f h_{\mathbb{C}}(\boldsymbol{x}) + \mathcal{L}_g h_{\mathbb{C}}(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x}) \geq 0,\ \forall x \in \mathbb{C} \setminus \overline{\mathbb{X}}_r, \\ & \mathcal{L}_f w_{\mathbb{C}}(\boldsymbol{x}) + \mathcal{L}_g w_{\mathbb{C}}(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x}) \geq h_{\mathbb{C}}(\boldsymbol{x}),\ \forall x \in \mathbb{C} \setminus \overline{\mathbb{X}}_r. \end{aligned} \quad (3)$$

其中 $\mathbb{C} = \{\boldsymbol{x} \in \boldsymbol{R}^n \mid h_{\mathbb{C}}(\boldsymbol{x}) > 0\}$ 是安全集合，则系统(1)在控制器 $\boldsymbol{u}(\boldsymbol{x})$ 下满足可达-规避性质。

松弛控制引导栅栏函数

针对仿射确定控制系统(1)，如果 $h_{\mathbb{C}}(\boldsymbol{x})$ 是一个关于局部Lipschitz连续的控制器 $u(\boldsymbol{x})$ 的**松弛控制引导栅栏函数**，即满足存在连续可微函数 $w_{\mathbb{C}}(\boldsymbol{x})$ 使得(4)成立，

$$\begin{aligned} & \mathcal{L}_f h_{\mathbb{C}}(\boldsymbol{x}) + \mathcal{L}_g h_{\mathbb{C}}(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x}) \geq -\lambda\eta h_{\mathbb{C}}(\boldsymbol{x}),\ \forall x \in (\mathbb{C} \setminus \overline{\mathbb{D}}) \setminus \mathbb{X}_r,\ \lambda \geq 0, \\ & \mathcal{L}_f w_{\mathbb{C}}(\boldsymbol{x}) + \mathcal{L}_g w_{\mathbb{C}}(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x}) > 0,\quad \forall x \in \mathbb{C} \setminus \overline{\mathbb{X}}_r. \end{aligned} \quad (4)$$

其中 $\mathbb{C} = \{\boldsymbol{x} \in \boldsymbol{R}^n \mid h_{\mathbb{C}}(\boldsymbol{x}) > 0\}$ 是安全集合，$\mathbb{D} = \{\boldsymbol{x} \in \boldsymbol{R}^n \mid h'_{\mathbb{C}}(\boldsymbol{x}) \geq 0\}$ 是一个紧集且满足:

$$1)\ \mathbb{D} \subseteq \mathbb{C};\ 2)\ \partial\mathbb{D} \cap \partial\mathbb{C} = \emptyset;\ 3)\ \mathbb{D} \cap \mathbb{X}_r \neq \emptyset.$$

则系统(1)在控制器 $\boldsymbol{u}(\boldsymbol{x})$ 下满足可达-规避性质。

随机系统的指数控制引导栅栏函数[2]

针对仿射随机控制系统(5)，如果 $h_{\mathbb{C}}(\boldsymbol{x})$ 是一个关于局部Lipschitz连续的控制器 $u(\boldsymbol{x})$ 的**指数控制引导栅栏函数**，即满足约束(6)，

$$\begin{aligned} d\boldsymbol{x}(t,\boldsymbol{w}) = \ & (\boldsymbol{f}(\boldsymbol{x}(t,\boldsymbol{w})) + \boldsymbol{g}(\boldsymbol{x}(t,\boldsymbol{w}))\boldsymbol{u}(\boldsymbol{x}(t)))dt \\ & + \boldsymbol{\sigma}(\boldsymbol{x}(t,\boldsymbol{w}))d\boldsymbol{W}(t,\boldsymbol{w}) \end{aligned} \quad (5)$$

$$\mathcal{L}_f h_{\mathbb{C}}(\boldsymbol{x}) + \mathcal{L}_g h_{\mathbb{C}}(\boldsymbol{x})\boldsymbol{u}(\boldsymbol{x}) \geq a h_{\mathbb{C}}(\boldsymbol{x}),\ \forall x \in \mathbb{C} \setminus \overline{\mathbb{X}}_r,\ a > 0. \quad (6)$$

其中 $\mathbb{C} = \{\boldsymbol{x} \in \boldsymbol{R}^n \mid h_{\mathbb{C}}(\boldsymbol{x}) > 0\}$ 是安全集合，则系统(5)在控制器 $\boldsymbol{u}(\boldsymbol{x})$ 下满足可达-规避性质。**注：** 随机系统的**渐近控制引导栅栏**类似。

注： 通过观察条件(2), (3), (4), 不难发现条件依次减弱。由此可知，通过**松弛控制引导栅栏函数，** 我们可在一个更大的容许控制集中选取反馈控制器 $\boldsymbol{u}(\boldsymbol{x})$，进而使得最终合成的控制器既满足可达-规避性，又与给定控制器 $\boldsymbol{k}(\boldsymbol{x})$ 更加接近 。

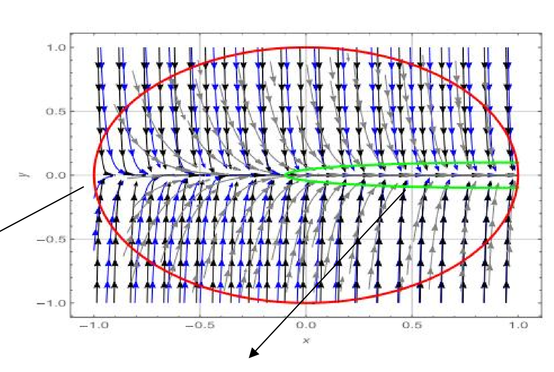
数值仿真

针对**移动机器人巡航控制系统，** 验证了理论的有效性。在满足充分条件的控制器驱动下，**确定系统**与**随机系统**均可实现可达-规避性质。同时，实验表明三种算法（基于指数、渐近、松弛控制引导栅栏函数）各有优缺点，可相互补充并结合使用来提高实际应用的有效性。

$$\begin{cases} \dot{x} = u_1 \\ \dot{y} = u_2 \end{cases}$$

$$\mathbb{C} = \{(x,y)^T \mid 1 - x^2 - y^2 > 0\}$$

$$\mathbb{X}_r = \{(x,y)^T \mid 0.01(x-0.9)^2 + y^2 - 0.01 < 0\}$$



(4)/(24)	Optimization (6)/(27)	(16)
$\xi_0 = 10^{-3}$	$\epsilon' = 10^{-3}$, $\epsilon^* = 10^{-3}$	$\epsilon' = 10^{-3}$, $\epsilon^* = 10^{-3}$

实验参数

Example	Optimization (4)	(6)	(16)
2	0.2329	0.089	3.829×10^{-4}
3	3.2002	3.1563	3.1563
4	1.7967	1.7912	1.7372

计算时间对比

[1] Bai Xue, Naijun Zhan, Martin Fränzle, Ji Wang and Wanwei Liu. Reach-avoid Verification Based on Convex Optimization. IEEE Transactions on Automatic Control (IEEE TAC), 69(1): 598--605, 2024.
[2] Bai Xue, Naijun Zhan, Martin Fränzle. Reach-Avoid Analysis for Polynomial Stochastic Differential Equations. IEEE Transactions on Automatic Control (IEEE TAC), 69(3): 1882--1889, 2024.