中国科学: 数学 2018 年 第 48 卷 第 ? 期: 1 ~ 20
SCIENTIA SINICA Mathematica
论 文

时延混成系统的切换控制器合成

献给张景中、杨路教授 85 华诞

白云军[1,2], 甘庭[3*], 焦莉[1,2], 薛白[1,2], 詹乃军[1,2*]

1. 中国科学院软件研究所计算机科学国家重点实验室, 北京中关村南四街 4 号, 100190
2. 中国科学院大学, 北京市石景山区玉泉路 19 号, 100039
3. 武汉大学计算机学院, 湖北省武汉市武昌区八一路 299 号, 430072
E-mail: baiyj@ios.ac.cn, ganting@whu.edu.cn, ljiao@ios.ac.cn, xuebai@ios.ac.cn, znj@ios.ac.cn

收稿日期: 2018-XX-XX; 接受日期: 2018-XX-XX; 网络出版日期: 2018-01-XX; * 通信作者
国家自然科学基金 (批准号: 61625206, 61732001, 61872341, 61902284, 61836005) 资助项目

摘要 如何设计安全、可靠的信息物理融合系统是计算机科学和控制理论面临的一个重大挑战。时延现象在信息物理融合系统中普遍存在, 时延对系统的稳定性、安全性和控制性能具有实质性影响。但是在已有时延系统验证和控制器合成的工作中往往忽略时延因素, 这会导致在不考虑时延时稳定和安全的系统在实际运行时因为时延原因而不再稳定和安全。因为时延使得系统的行为演化不仅与当前状态有关, 还依赖于系统的历史状态, 这样时延混成系统的验证和控制合成更加困难。本文研究信息物理融合系统在考虑时延情况下切换控制器合成问题, 提出了基于不变式生成技术的控制器合成方法。首先, 我们利用谱分析和线性化技术将时延系统的微分不变式生成问题归结为有界时间的可达集计算问题; 然后, 提出基于抽象精化的算法计算时延系统有界时间可达集的上近似; 最后, 实现本文算法并使用实例验证了该方法的有效性。

关键词 时延混成系统 时延微分方程 微分不变式 切换控制器 安全性

MSC (2010) 主题分类 34K04, 93B50, 93C30

1 引言

近几十年来, 随着计算机、互联网和通信技术的迅猛发展, 传统的嵌入式系统逐渐发展成为了深度融合计算、通信和控制的信息物理融合系统 (Cyber Physical Systems, 简称 CPS), 与物联网 (Internet of Things, 简称 IoT) 技术一起正在掀起新一轮的全球信息技术革命, 深刻影响着人们的生产和生活方式。尤其伴随着 CPS 的大发展, 越来越多的安全攸关系统不断涌现, 如健康医疗、

英文引用格式: Bai Y, Gan T, Jiao L, Xue B, Zhan N. Switching Controller Synthesis for Time-delayed Hybrid Systems (in Chinese). Sci Sin Math, 2018, 48: 1–20, doi: 10.1360/N012017-XXXX

航空航天、智慧交通、核反应堆等。“如何设计安全可靠的信息物理融合系统使得人们在日常生活中放心使用”已经成为计算机科学和控制理论的一个巨大挑战 [1]。

在 CPS 的设计控制过程中，由于模拟信号与数字信号间的相互转换需要时间、传感器收集数据具有周期性、执行器执行命令需要时间、不同带宽网络间数据传输不可避免地出现阻塞、物联网中传感器网络对数据的预处理需要时间等，时延现象难以避免。其中一种时延现象体现在物理设备的连续动态演化中，系统状态变量间产生时延耦合，即系统的行为演化不仅与系统的当前状态有关，还依赖于系统的历史状态，我们称这类系统为时延微分动态系统。时延微分方程（Delayed Differential Equations, 简称 DDEs）是刻画带时延微分动态系统合适的数学模型。Myshkis [2]、Krasovskii [3] 及 Bellman 和 Cooke [4] 等人对时延微分方程做了系统深入的研究，已被广泛应用到生物、化学、分布式控制等领域。例如，在传染疾病传播模型 [5] 中，某些疾病因存在潜伏期不可避免地在模型中需要引入时延；在非线性光学谐振器模型 [6] 中，系统的反馈会带来时延；在生物物种繁衍系统 [7] 中，由于食物供给、繁殖年龄等的限制，物种增长率依赖于当前物种数量和过去某时间点的数量；在网络通信系统 [8] 中，交互网络控制系统不得不处理通信带来的时延。

[9] 一文指出时延可能会对控制系统的稳定性、安全性和控制性能带来实质性影响，因而在控制和通讯领域，DDEs 得到广泛重视。但是在计算机领域，DDEs 的形式化验证和设计研究目前尚处于初步阶段。相比较常微分方法，时延微分方程在理论分析上更加复杂，这是缘于时延微分方程是无穷维的、“有记忆”的，即考虑了历史对现状的影响。这使得系统的设计和验证也更加困难。在工程领域常采用数值仿真的方法来模拟系统行为 [10]，但仿真过程中不可避免地产生误差，导致无法严格保证系统的正确性。一些研究工作以 DDEs 的稳定性为基础，包括利用栅栏函数 [11, 12]、Lyapunov 函数 [11] 以及区间 Taylor 模型 [9] 解决时延系统的安全性验证问题，但这类方法一个共同弱点是其依赖于预先设定的函数模板，而模板的设计很大程度上依赖于设计者的经验。另一类方法是基于 DDEs 的可达集计算，例如 [13] 借助非线性优化计算分段线性的局部误差上界和数值仿真技术，计算 DDEs 的可达集。[8] 利用敏感性分析和数值模拟方法估计了带时延耦合系统的可达集。基于拓扑分析，[14] 研究了 DDEs 解的同胚性质，并将常微分方程中的边界可达性分析方法 [15, 16] 推广到了其解具有同胚性质的 DDEs 中。[17] 将计算常微分方程可达集的泰勒模型方法 [18] 推广到了 DDEs 中。最近，基于动态和混成系统的稳定性理论，[19] 将 DDEs 的稳定性分析和无界时间安全性验证问题归结为有界时间内的对应问题，并推广区间泰勒模型可达集计算理论 [17]，解决了无界时间内 DDEs 稳定性分析和安全性验证问题。

本文我们研究时延混成系统安全设计问题。混成系统是一类既包含连续演化又包含离散迁移的系统，为传统嵌入式系统的安全可靠性提供了很好的刻画模型。然而在传统嵌入式系统形式验证和设计中，往往假设时延足够小不会对系统行为产生影响，因此时延现象往往被忽略。但在实际应用中，时延现象常常带来很多消极作用，使得系统性能下降，甚至出现不可控状态。为此，在本文中我们研究能够刻画时延现象的一类混成系统——时延混成系统，并解决时延混成系统的切换控制器设计问题。给定一安全性质需求，切换控制器设计问题即为系统的每个模式选择符合其对应安全需求的不变式，并为每个迁移选取合适的切换条件，使得系统从初始状态集合出发，按照切换条件执行迁移关系，能够永不停止地运行，并且系统的所有可达状态符合安全需求。为解决此问题，受我们前期关于不带时延混成系统切换控制器合成工作启发 [20]，我们提出一个基于不变式的时延混成

系统切换控制器合成方法。其基本想法如下：受启发于 [19]，首先利用谱分析和线性化技术，将无界时间的微分不变式生成问题归结为有界时间的微分不变式生成问题；然后我们利用基于抽象精化的算法计算有界时间内系统安全可达集的上近似作为其微分不变式；最后，在所求得的微分不变式基础上，我们给出时延混成系统切换控制器设计的算法框架。

本文结构如下：第二章介绍预备知识和时延混成系统切换控制器合成问题；第三章介绍切换控制器合成算法框架；第四章讨论时延动态系统的微分不变式生成；第五章介绍实现和案例研究；最后在第六章总结全文。

2　预备知识

本章介绍时延混成系统的背景知识以及本文要解决的控制器合成问题。2.1 节给出了本文中使用的基本概念和符号，2.2 节简要介绍时延混成系统、可达集和安全性验证等一些背景知识，以及时延混成系统的切换控制器合成问题。

2.1　基本概念和符号

本文使用 $\mathbb{R}$ 表示实数集，$\mathbb{R}^+$ 表示正实数集，$\mathbb{R}_0^+$ 表示非负实数集，$\mathbb{N}$ 表示自然数集，$\mathbb{N}^+$ 表示正整数集，$\mathbb{C}$ 表示复数集。X^n 表示 n 个 X 的笛卡尔积，例如，$\mathbb{R}^n$ 表示 n 维欧几里得空间。给定任意实数 $x \in \mathbb{R}$，$|x|$ 表示 x 的模。对于任意复数 $z = a + ib \in \mathbb{C}$，其中 $a, b \in \mathbb{R}$, i 为虚数单位，则 z 的实部和虚部分别记作 $\mathfrak{R}(z) = a$ 和 $\mathfrak{C}(z) = b$，z 的模为 $|z| = \sqrt{a^2 + b^2}$。给定 $m \times n$ 维矩阵 A，$\lambda_{\max}(A^TA)$ 表示半正定矩阵 A^TA 的最大特征值，A 的范数表示为 $\parallel A \parallel = \sqrt{\lambda_{\max}(A^TA)}$。对于向量 $\mathbf{x}, \mathbf{x}' \in \mathbb{R}^n$，$\parallel \mathbf{x}' - \mathbf{x} \parallel$ 表示向量之间的欧式距离。给定 $\delta \in \mathbb{R}_0^+$，向量 $\mathbf{x}$ 的 δ- 邻域定义为 $\mathcal{N}(\mathbf{x}, \delta) = \{\mathbf{x}' \mid\mid \mathbf{x}' - \mathbf{x} \parallel \leqslant \delta\}$。对于集合 $X \subseteq \mathbb{R}^n$，X 的 δ- 邻域为 $\mathcal{N}(X, \delta) = \bigcup_{\mathbf{x} \in X} \mathcal{N}(\mathbf{x}, \delta)$。给定一个紧集 X，其直径记为 $dia(X) = \sup_{\mathbf{x}, \mathbf{x}' \in X} \parallel \mathbf{x}' - \mathbf{x} \parallel$，它的一个 δ- 覆盖是一个有限点集 $\mathcal{X}$，使得 $X \subseteq \mathcal{N}(\mathcal{X}, \delta)$。给定 $t_1 \leqslant t_2$，$\mathcal{C}([t_1, t_2], \mathbb{R}^n)$ 表示所有从 $[t_1, t_2]$ 映射到 $\mathbb{R}^n$ 的连续函数集合。对于 $\boldsymbol{f} \in \mathcal{C}([t_1, t_2], \mathbb{R}^n)$，$\|\boldsymbol{f}\| = \max_{t \in [t_1, t_2]} \|\boldsymbol{f}(t)\|$。

2.2　时延混成系统

混成系统是一类既包含连续演化又包含离散迁移的系统。一种最简单又最常用的混成系统模型是混成自动机 [21]，其中常微分方程用来刻画系统的连续行为。如果系统连续演化过程存在时延现象，则混成自动机无法准确刻画此类系统。为此，本节给出一种新的混成自动机的定义，称为时延混成自动机，其系统连续行为被时延微分方程刻画。首先我们给出时延微分方程的基本知识。

考虑如下一阶自治时延微分方程：

$$\begin{cases} \dot{\mathbf{x}}(t) = \boldsymbol{f}(\mathbf{x}(t), \mathbf{x}(t - r_1), \ldots, \mathbf{x}(t - r_k)), & t \in [0, \infty) \\ \mathbf{x}(t) = \boldsymbol{\phi}(t), & t \in [-r_k, 0] \end{cases} \tag{2.1}$$

其中，$\mathbf{x} \in \mathbb{R}^n$ 表示系统的状态向量，$\dot{\mathbf{x}}$ 为状态向量关于时间的导数，$t \in [-r_k, \infty)$ 表示时间变量，$r_j \in \mathbb{R}^+$ 是时延常数并且满足 $0 < r_1 < \ldots < r_k$, $j = 1, \ldots, k$, 向量函数 $\boldsymbol{f} : \mathbb{R}^{(k+1)n} \mapsto \mathbb{R}^n$ 表

示系统的向量场。值得注意的是，时延微分方程 (2.1) 不同于一般的常微分方程，$\dot{\mathbf{x}}(t)$ 不仅与当前时刻的系统状态 $\mathbf{x}(t)$ 有关，而且还依赖于若干历史状态 $\mathbf{x}(t-r_1),\ldots,\mathbf{x}(t-r_k)$。因为系统随时间的连续演化过程对历史状态的依赖，所以系统的初始状态必须由一个向量函数 $\boldsymbol{\phi}$ 刻画，即 $\boldsymbol{\phi}\in\mathcal{C}([-r_k,0],\mathbb{R}^n)$。如果向量函数 $\boldsymbol{f}$ 满足全局 Lipschitz 条件，则时延微分方程 (2.1) 从初始状态 $\boldsymbol{\phi}$ 出发在 $[-r_k,\infty)$ 上存在唯一的解，记作 $\boldsymbol{\xi}_{\boldsymbol{\phi}}(\cdot)\in[-r_k,\infty)\mapsto\mathbb{R}^n$。

定义2.1 给定一时延微分方程 (2.1)，假设 $\mathbf{x_e}$ 为它的一个平衡点 (equilibrium)，即 $\boldsymbol{f}(\mathbf{x_e},\ldots,\mathbf{x_e})=\mathbf{0}$，我们称 $\mathbf{x_e}$ 是

1. *Lyapunov 稳定的*: 如果对于任意的 $\epsilon\in\mathbb{R}^+$，存在 $\delta\in\mathbb{R}^+$ 使得如果 $\parallel\boldsymbol{\phi}-\mathbf{x_e}\parallel<\delta$，那么对于任意的 $t\in R_0^+$，$\parallel\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)-\mathbf{x_e}\parallel<\epsilon$;
2. *渐近稳定的*: 如果它是 Lyapunov 稳定的，且满足 $\lim_{t\mapsto\infty}\parallel\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)-\mathbf{x_e}\parallel=0$;
3. *指数稳定的*: 如果它是渐近稳定的，且满足：存在 $\alpha,\beta,\delta\in\mathbb{R}^+$ 使得对于任意 $t\in R_0^+$，$\parallel\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)-\mathbf{x_e}\parallel\leqslant\alpha\parallel\boldsymbol{\phi}-\mathbf{x_e}\parallel\mathrm{e}^{-\beta t}$, 其中 β 是收敛率。

不失一般性，后文我们假设 (2.1) 的向量场满足 $\boldsymbol{f}(\mathbf{0},\ldots,\mathbf{0})=\mathbf{0}$。根据时延微分方程 (2.1)，我们给出时延混成自动机的定义：

定义2.2 *时延混成自动机* 是一个九元组 $\mathcal{H}=(Q,X,U,I,\Xi,F,E,G,R)$，其中

1. $Q=\{q_1,\ldots,q_m\}$ 为有限的离散模式集合;
2. $X\subseteq\mathbb{R}^n$ 为连续状态集合;
3. U 是定义在集合 X 上的连续函数集合，$U\subseteq\mathcal{C}([t_1,t_2],\mathbb{R}^n)$;
4. $I:Q\mapsto 2^{\mathbb{R}^n}$ 赋予每个模式 $q\in Q$ 一个不变式 $I_q\subseteq X$;
5. $\Xi\subset Q\times U$ 为初始状态集合, 在 $q\in Q$ 模式下的初始状态集合为 $\Xi_q\subseteq\{q\}\times U_q, U=\cup_{q\in Q}U_q$;
6. $F=\{\boldsymbol{f}_{q_1},\ldots,\boldsymbol{f}_{q_m}\}$ 为向量场集合，每个模式 $q\in Q$ 具有一个向量场 $\boldsymbol{f}_q$，且其形式为时延微分方程 (2.1)，即 $\dot{\mathbf{x}}(t)=\boldsymbol{f}_q(\mathbf{x}(t),\mathbf{x}(t-r_{1,q}),\ldots,\mathbf{x}(t-r_{k,q}))$, $0<r_{1,q}<\ldots<r_{k,q}$;
7. $E\subseteq Q\times Q$ 表示模式间的离散迁移关系;
8. $G:E\mapsto 2^{\mathbb{R}^n}$ 是迁移条件;
9. $R:E\times X\mapsto U$ 为重置函数[1)]。

定义2.3 给定一个初始状态 $(q_0,\boldsymbol{\phi}_0)$，时延混成系统在时间 $[-r_k,T]$ 的轨道为一序列

$$(q_0,\boldsymbol{\xi}_{\boldsymbol{\phi}_0}),\ldots,(q_l,\boldsymbol{\xi}_{\boldsymbol{\phi}_l})$$

其中 $T\geqslant 0$，$\boldsymbol{\phi}_i\in U$，$i=0,\ldots,l$，$l\in\mathrm{N}$，这一序列满足以下四个条件：

1. 连续演化：对 $i\leqslant l-1$, 存在 $\delta_i\geqslant 0$ 使得时延微分方程 $\dot{\mathbf{x}}=\boldsymbol{f}_{q_i}$ 的解 $\boldsymbol{\xi}_{\boldsymbol{\phi}_i}(\cdot):[-r_{k,q_i},\delta_i]\mapsto\mathbb{R}^n$ 满足：
   a. $\boldsymbol{\xi}_{\boldsymbol{\phi}_i}(t)\in I_{q_i}$ 对于所有 $t\in[-r_{k,q_i},\delta_i]$;
   b. $\mathbf{x}_i=\boldsymbol{\xi}_{\boldsymbol{\phi}_i}(\delta_i)$。
2. 对 $i=l$, 存在 $\delta_i\geqslant 0$ 使得时延微分方程 $\dot{\mathbf{x}}=\boldsymbol{f}_{q_i}$ 的解 $\boldsymbol{\xi}_{\boldsymbol{\phi}_i}(\cdot):[-r_{k,q_i},\delta_i]\mapsto\mathbb{R}^n$ 满足 $\boldsymbol{\xi}_{\boldsymbol{\phi}_i}(t)\in I_{q_i}$ 对于所有 $t\in[-r_{k,q_i},\delta_i]$。
3. 离散迁移：令 $e=(q_i,q_{i+1})$，则有 $e\in E$，$\mathbf{x}_i\in G(e)$ 且 $\boldsymbol{\phi}_{i+1}\in R(e,\mathbf{x}_i)$。

1) 在定义 2.2 中，当发生模式跳转时，重置函数 R 将当前时刻系统状态重置为以函数形式的系统状态，其目的是为满足时延微分方程 (2.1) 的起始状态为函数，与文献 [22] 中的定义无本质性差别，仅需将定义 2.2 中重置后的函数替换成它在跳转时刻的值即可。

4. $T = \sum_{i=1}^{l} \delta_i$。

定义2.4 给定一个初始状态 $(q_0, \boldsymbol{\phi}_0)$，时延混成系统在时间 $t \in [-r_{k,q_0}, T]$ 上的可达状态集合 $R_{\mathcal{H}}(t)$ (简称可达集) 为 $(q, \mathbf{x})$ 的集合，其中 $(q, \mathbf{x})$ 满足

$$\text{存在} i \in \{1, \ldots, l\} \text{且} t \in [-r_{k,q_i}, \delta_i] \text{使得} q = q_i \text{和} \mathbf{x} = \boldsymbol{\xi}_{\boldsymbol{\phi}_i}(t)。$$

给定一个时延混成系统 $\mathcal{H} = (Q, X, U, I, \Xi, F, E, G, R)$，$\mathcal{H}$ 称为是非阻塞的，如果对于任意 $(q_0, \boldsymbol{\phi}_0) \in \Xi$，至少存在一条在 $[-r_{k,q_0}, \infty)$ 上的轨道；反之称为是阻塞的。

对于时延混成系统 $\mathcal{H}$，一个安全需求规范 $\mathcal{S}$ 为每个模式 $q \in Q$ 指定了一个安全区域 $S_q \subseteq I_q$，可以形式化地表示为 $\mathcal{S} = \bigcup_{q \in Q}(\{q\} \times \mathcal{S}_q)$。给定初始状态集 Ξ，我们称 $\mathcal{H}$ 是 T- 安全的，当且仅当其在时间 $[-r_{k,q_0}, T]$ 上的可达集 $R_{\mathcal{H}}$ 包含在 $\mathcal{S}$ 里，即 $R_{\mathcal{H}} \subseteq \mathcal{S}$，否则称之为 T- 不安全。当 $T = \infty$，我们称 $\mathcal{H}$ 是安全的。

切换控制器合成问题：给定时延混成系统 $\mathcal{H} = (Q, X, U, I, \Xi, F, E, G, R)$ 以及安全性质 $\mathcal{S}$，计算时延混成系统 $\mathcal{H}^* = (Q, X, U^*, I^*, \Xi^*, F, E, G^*, R^*)$ 使得

(r1) $\mathcal{H}^*$ 是 $\mathcal{H}$ 的精化，即对任意 $q \in Q$，满足 $\Xi_q^* \subseteq \{(q, \boldsymbol{\phi}_q) \in \Xi_q \mid \forall \tau \in [-r_{k,q}, 0].\boldsymbol{\phi}_q(\tau) \in S_q\}$，$I_q^* \subseteq I_q$，$U_q^* \subseteq U_q$, 且对任意 $e \in E$，满足 $G^*(e) \subseteq G(e)$, $R^*(e, \cdot) \subseteq R(e, \cdot)$；

(r2) $\mathcal{H}^*$ 相对于 $\mathcal{S}$ 是安全的，即在时间 $[-r_{k,q_0}, \infty)$ 上的可达集 $R_{\mathcal{H}^*} \subseteq \mathcal{S}$；

(r3) $\mathcal{H}^*$ 是非阻塞的，且不变式是非空的 (即 $I^* \neq \emptyset$)。

对于满足上述三点的 $\mathcal{H}^*$，则称 $SC = \{G^*(e) \subseteq \mathbb{R}^n \mid e \in E\}$ 为 $\mathcal{H}$ 一个切换控制器。如果对任意 $q \in Q$ 和 $e \in E$，$I_q^* = \emptyset$ 或 $G^*(e) = \emptyset$，我们称 SC 为 $\mathcal{H}$ 一个平凡切换控制器.

直观地讲，切换控制器合成即为系统的每个模式选择符合其对应安全需求的不变式，并为每个迁移选取合适的切换条件，使得系统从初始状态集合出发，按照切换条件执行迁移关系，能够永不停止地运行，并且系统的所有可达状态符合安全需求。

3 切换控制器合成算法框架

这一节我们提出一种基于归纳不变式的时延混成系统控制器合成方法，其基本想法类似基于不变式生成的混成系统切换控制器合成方法 [20]，核心是如何生成每个模式内的时延动态系统的微分不变式及模式间离散迁移切换条件。在下章我们将介绍基于可达集迭代计算求归纳不变式的算法，使得时延混成系统满足安全性质的同时避免合成平凡的控制器。

3.1 不变式

定义3.1 给定时延混成系统中的一模式 $q \in Q$：$(\Xi_q, \boldsymbol{f}_q, I_q)$ 以及时刻 $T \in \mathbb{R}^+$，集合 I_q^* 称为 $(\Xi_q, \boldsymbol{f}_q, I_q)$ 的 T- 微分不变式，如果对于 $\forall \tau \in [-r_{k,q}, 0]$，$\boldsymbol{\phi}_q(\tau) \in I_q^*$，且从 $\boldsymbol{\xi}_{\boldsymbol{\phi}_q}(0) \in I_q^*$ 出发的任意解 $\boldsymbol{\xi}_{\boldsymbol{\phi}_q}(t)$ 满足

$$\forall t \in [-r_{k,q}, T].\boldsymbol{\xi}_{\boldsymbol{\phi}_q}(t) \in I_q \implies \forall t \in [-r_{k,q}, T].\boldsymbol{\xi}_{\boldsymbol{\phi}_q}(t) \in I_q^*. \tag{3.1}$$

直观上，时延系统模式 $q \in Q : (\Xi_q, \boldsymbol{f}_q, I_q)$ 的 T- 微分不变式要求: 如果从初始集合出发沿向量场 $\boldsymbol{f}_q$ 的任何解在时间 $[-r_{k,q}, T]$ 内不离开 I_q，那么它不会离开 I_q^*。特别地，当 $T = \infty$，集合 I_q^* 称为微分不变式。

根据微分不变式定义，下面给出时延混成系统 $\mathcal{H}$ 的归纳不变式。

定义3.2 给定时延混成系统 $\mathcal{H}$，称 $I^* = \bigcup_{q\in Q} I_q^*$ 为 $\mathcal{H}$ 的归纳不变式，若

1. 对 $q \in Q$，集合 I_q^* 是 $(\Xi_q, \boldsymbol{f}_q, I_q)$ 的微分不变式；
2. 对 $e = (q, q') \in E$，若 $\boldsymbol{\xi}_{\phi_q}(t) \in I_q^* \cap G(e)$，则 $\forall \tau \in [-r_{k,q'}, t].\boldsymbol{\phi}_{q'}(\tau) \in I_{q'} \implies \forall \tau \in [-r_{k,q'}, t].\boldsymbol{\phi}_{q'}(\tau) \in I_{q'}^*$ 成立, 其中 $\boldsymbol{\phi}_{q'}(\cdot) = R(e, \boldsymbol{\xi}_{\phi_q}(t))$。

在定义 3.2 中，条件 1 为对时延混成系统的连续部分归纳不变式的约束，归纳不变式 I^* 在每个模式 q 下的 I_q^* 都是相应模式的一个微分不变式。条件 2 为离散迁移对归纳不变式的约束，状态 $\boldsymbol{\xi}_{\phi_q}(t)$ 在满足迁移条件下，迁移后相应模式 q' 对应的时延微分动态系统的状态应属于其微分不变式 $I_{q'}^*$ 内。

3.2 切换控制器合成算法

通过构建满足定义 3.2 的归纳不变式，算法 1 给出了基于不变式的切换控制器合成算法框架。给定时延混成系统 $\mathcal{H}$ 及安全性质 $\mathcal{S}$，首先对每一个模式 $q \in Q$，调用函数 **CBT** 计算一个时间上界 T_q, 将 q 模式下的微分不变式生成问题归结为 T_q- 微分不变式生成问题 (第 4.1 节)；然后调用函数 **CSI**，使用抽象精化方法来计算满足安全性质的微分不变式 I_q^* (第 4.2 节)。最后根据各个模式的微分不变式，计算精化的归纳不变式 $I^* = \cup_{q\in Q} I_q^*$ 和 $G^* = \cup_{e=(q,q')\in E} G^*(e)$，其中 $G^*(e) \subseteq G(e) \cap I_q^*$ 是使得满足 $\boldsymbol{\phi}_{q'}(\cdot) = R(e, \mathbf{x})$ 以及对任意 $\tau \in [-r_{k,q'}, 0]$，$\boldsymbol{\phi}_{q'}(\tau) \subseteq I_{q'}^*$ 的 $\mathbf{x}$ 的集合。如果对于 $\forall e \in E, G_e^* \neq \emptyset$，算法将返回新的时延混成系统 $\mathcal{H}^* = (Q, X, U^*, I^*, \Xi^*, F, E, G^*, R^*)$；否则算法将返回 “FLASE”，表示控制器 SC 为平凡切换控制器。以下定理给出了算法 1 的正确性。

定理3.1 (正确性) 给定时延混成系统 $\mathcal{H} = (Q, X, U, I, \Xi, F, E, G, R)$ 以及安全性质 $\mathcal{S}$，如果对于每一个模式 $q \in Q$，算法调用函数 **CBT** 和 **CSI** 后，得到的是满足公式 (3.1) 的微分不变式，且对于 $\forall e \in E$, $G^*(e) \neq \emptyset$，那么算法 1 将返回一个时延混成系统 $\mathcal{H}^* = (Q, X, U^*, I^*, \Xi^*, F, E, G^*, R^*)$, $SC = \{G_e^* | e \in E\}$ 是 $\mathcal{H}$ 的一个切换控制器。

证明 假设算法 1 通过第 20 行返回时延混成系统 $\mathcal{H}^* = (Q, X, U^*, I^*, \Xi^*, F, E, G^*, R^*)$，这里只需要证明切换控制器合成问题中条件 (r1)，(r2) 和 (r3) 成立。对于任意的 $q \in Q$，由算法的第 8 行可以得到 $\Xi_q^* \subseteq \{(q, \boldsymbol{\phi}_q) \in \Xi_q \mid \forall \tau \in [-r_{k,q}, 0].\boldsymbol{\phi}_q(\tau) \in S_q\}$；由算法的第 2-7 行，可以得到 $I_q^* \subseteq I_q$；U_q^* 和 U_q 分别是定义在 I_q^* 和 I_q 上的连续函数，由于 $I_q^* \subseteq I_q$，则有 $U_q^* \subseteq U_q$；由算法第 12 行和第 11 行分别有 $G^*(e) \subseteq G(e)$，$R^*(e, \cdot) \subseteq R(e, \cdot)$，从而条件（r1）成立。对于任意的 $q \in Q$，I_q^* 是模式 q 中的微分不变式，并且算法 1 返回的 G^* 保证了离散跳转后得到的状态包含在下一模式的微分不变式中，所以 I^* 是整个混成系统的归纳不变式。同时，算法的第 4 行确保了每一个模式 q 的微分不变式 I_q^* 均相对于 $\mathcal{S}_q$ 是安全的，从而得到条件 (r2) 成立。对于条件 (r3)，因为 (a). 对于每个模式 $q \in Q$，算法 **CBT** 和 **CSI** 通过将无界时间的微分不变式生成问题转化到有界时间可达集计算问题，即 I_q^* 包含了该模式中从初始状态集合出发的所有可达状态；(b). 对于 $e = (q, q') \in E$，

迁移条件 $G^*(e)$ 满足 $G^*(e) \subseteq I_q^*$，且 $R^*(e,\cdot)$ 保证了重置后的系统状态在模式 q' 的微分不变式 $I_{q'}^*$，即在模式 q 的微分不变式 I_q^* 中，如果存在 $\mathbf{x} \in G^*(e)$ 且发生离散迁移，那么重置后的系统状态在模式 q' 的微分不变式 $I_{q'}^*$；(c). 算法的第 19 行保证了返回的微分不变式和跳转条件都是非空的，从而可以知道条件 (r3) 成立。 □

算法 1 时延混成系统切换控制器合成算法

输入: 时延混成系统 $\mathcal{H} = (Q, X, U, I, \Xi, F, E, G, R)$，安全性质 $\mathcal{S}$，精度 ϵ，阈值 ϵ_r，步长 τ，$\mathcal{B}$

输出: 时延混成系统 $\mathcal{H}^*$ / FLASE

1: **for** $q \in Q$ **do**
2: $T_q \leftarrow \mathbf{CBT}(\boldsymbol{f_q}, \Xi_q, \epsilon, \mathcal{B})$
3: **if** $T_q < \infty$ **then**
4: $I_q^* \leftarrow \mathbf{CSI}(\boldsymbol{f_q}, \Xi_q, \tau, \mathcal{S}_q, T_q, \epsilon_r, \epsilon)$
5: **else**
6: $I_q^* \leftarrow \emptyset$
7: **end if**
8: $\Xi_q^* \leftarrow \{(q, \boldsymbol{\phi}_q) \in \Xi_q \mid \forall \tau \in [-r_{k,q}, 0].\boldsymbol{\phi}_q(\tau) \in S_q\}$
9: **end for**
10: **for** $e = (q, q') \in E$ **do**
11: $R^*(e,\cdot) \leftarrow \{\boldsymbol{\phi}_{q'}(\cdot) \in R(e,\cdot) \mid$ 对$\tau \in [-r_{k,q'}, 0]\, \boldsymbol{\phi}_{q'}(\tau) \subseteq I_{q'}^*\}$
12: $G^*(e) \leftarrow \{\mathbf{x} \in G(e) \cap I_q^* \mid \boldsymbol{\phi}_{q'}(\cdot) = R^*(e, \mathbf{x})\}$
13: **end for**
14: $\Xi^* \leftarrow \{(q, \Xi_q^*) \mid q \in Q\}$
15: $I^* \leftarrow \{(q, I_q^*) \mid q \in Q\}$
16: $U^* \leftarrow \{(q, U_q) \mid \forall q \in Q, \boldsymbol{\phi} \in I_q^*\}$
17: $G^* \leftarrow \{(e, G^*(e)) \mid e \in E\}$
18: $R^* \leftarrow \{R^*(e,\cdot) \mid e \in E\}$
19: **if** $\forall e \in E, G_e^* \neq \emptyset$ **then**
20: **return** $\mathcal{H}^* \leftarrow (Q, X, U^*, I^*, \Xi^*, F, E, G^*, R^*)$
21: **else**
22: **return** FLASE
23: **end if**

4　微分不变式生成

在时延混成系统切换控制器合成算法，即算法 1 中，核心部分是计算时延混成系统每个模式 $q \in Q$ 的微分不变式 I_q^*。与常微分方程 (Ordinary Differential Equations, 简称 ODEs) 不同，DDEs 依赖于历史状态，使得其在理论分析上更加复杂。目前对 DDEs 微分不变式的研究主要借助 DDEs

的稳定性，包括利用栅栏函数 [11, 12]、Lyapunov 函数 [11] 以及区间 Taylor 模型近似 [9] 等。本节给出一种新的微分不变式的计算方法，分为 **CBT** 和 **CSI** 两步：算法 **CBT** 首先将微分不变式生成问题归结为 T_q- 微分不变式生成问题; 然后基于抽象精化的方法，即算法 **CSI**，计算 T_q- 微分不变式。为方便阐述，下文首先以含有一个时延常数的 DDEs:

$$\begin{cases} \dot{\mathbf{x}}(t) = \boldsymbol{f}(\mathbf{x}(t), \mathbf{x}(t-r)), & t \in [0, \infty) \\ \mathbf{x}(t) = \boldsymbol{\phi}(t), & t \in [-r, 0] \end{cases} \tag{4.1}$$

为例，详细阐述时间上界 T_q 的计算和算法 **CSI**。随后，简要论述该方法可以自然扩展到含有多个时延常数的 DDEs 中。基于方程 (4.1), 本章我们统一用 T^* 来表示 T_q，用 $\boldsymbol{f}$ 表示模式 q 的向量场 $\boldsymbol{f}_q$，用 $\boldsymbol{\phi}$ 表示模式 q 的初始状态 $\boldsymbol{\phi}_q$。

4.1 CBT: 构造时间上界 T^*

经典 DDEs 稳定性理论中指出对于一类具有指数稳定的 DDEs，存在一个随时间指数下降的估计，使得系统从初始函数状态集合出发的所有解都可以被该估计包络在内。基于此结论，本节对线性和非线性 DDEs 分别进行讨论。首先，利用谱分析技术计算具有指数稳定性质的线性 DDE(4.1) 的指数收敛率。然后，基于线性化方法，计算具有指数稳定性质非线性 DDE (4.1) 的指数收敛率。最后基于估计的收敛率，我们得到满足任意精确度的有界时间 T^*。

4.1.1 线性时延方程

考虑时延微分方程 (4.1) 的一类线性方程：

$$\begin{cases} \dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{x}(t-r), & t \in [0, \infty) \\ \mathbf{x}(t) = \boldsymbol{\phi}(t), & t \in [-r, 0] \end{cases} \tag{4.2}$$

其中，$A, B \in \mathbb{R}^{n\times n}$。此方程不平凡解 $\boldsymbol{\xi}_{\boldsymbol{\phi}}(t) = \boldsymbol{c}\mathrm{e}^{zt}$ 的特征方程为

$$\det(zU - A - B\mathrm{e}^{-rz}) = 0, \tag{4.3}$$

其中 U 为 $n \times n$ 维单位矩阵，$\det(\cdot)$ 为行列式，$h(z) = zU - A - B\mathrm{e}^{-rz}$ 为特征矩阵。特征方程 (4.3) 的根称为特征根，记作 $\lambda \in \mathbb{C}$，所有特征根组成的集合称为谱(spectrum)，记作 $\sigma = \{\lambda \mid \det(h(\lambda)) = 0\}$。Hale 和 Diekmann 等人在文献 [4, 23] 中指出 DDEs 的谱 σ 没有有穷聚点的特性，即不会在有穷处存在无穷多个特征根。所以存在一个上界 $\mu \in \mathbb{R}$，使得谱中任意特征根满足 $\Re(\lambda) < \mu$，且该上界 μ 决定了对应线性 DDEs 的渐近稳定性质，即如下定理 4.1：

定理4.1 ([23]) 假设特征根 λ 满足 $\Re(\lambda) < \mu$，那么存在一个 $K > 0$ 使得

$$\| \boldsymbol{\xi}_{\boldsymbol{\phi}}(t) \| \leqslant K\mathrm{e}^{\mu t} \| \boldsymbol{\phi} \|, \forall t \geqslant 0, \forall \boldsymbol{\phi} \in \mathcal{C}([-r, 0], \mathbb{R}^n), \tag{4.4}$$

其中 $\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)$ 是方程 (4.2) 的解。特别地，如果对于任意特征根 λ 满足 $\Re(\lambda) < 0$，则方程 (4.2) 的平衡点 $\mathbf{x_e} = \mathbf{0}$ 是渐近稳定的；相反，如果存在一个特征根 λ 使得 $\Re(\lambda) > 0$，则该平衡点 $\mathbf{x_e} = \mathbf{0}$ 不稳定。

定理 4.1 指出：若特征根上界 $\mu<0$，从初始函数 $\boldsymbol{\phi}$ 出发的所有解都以指数速度收敛于平衡点 $\mathbf{0}$，即存在一个时间 T，使得对于任意 $t\geqslant T$，$\parallel \boldsymbol{\xi}_{\boldsymbol{\phi}}(t)\parallel\leqslant\epsilon$，其中 $\epsilon\in\mathbb{R}^{+}$。此定理揭示了微分不变式可归结为 $T-$ 微分不变式。为了求得具体时间上界 T，我们下面给出估计式 (4.4) 中 (带符号的) 收敛率 μ 及常数 K 的计算方法。

收敛率 μ: 线性 DDEs 特征根的界和分布估计已有很多研究工作 [24–27]，考虑到特征方程 (4.3) 中涉及到指数多项式形式，基于柱形代数分解的符号化方法 [27] 可以将谱中的实根隔离到不同区间，但是对于复根部分，目前还没有相关的符号化方法进行隔离。所以我们采用 Engelborghs 和 Roose 在 [25] 中提出的一种数值估计方法，使用线性多步法离散化解算子来计算特征值的近似，数值估计的绝对误差可以控制在 $O(\tau^{p})$ 以内，其中 τ 为充分小的离散步长，p 依赖于线性多步法使用的阶数。MATLAT 工具包 DDE-BIFTOOL[28] 提供了此数值方法的自动化计算。

常数 K: 我们引入方程 (4.2) 的基本解（简称基解），记作 $\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)$，文献 [4] 指出基解的 Laplace 变换与特征方程的逆 $h^{-1}(z)$ 恰好相等，即 $\mathfrak{L}\{\boldsymbol{\xi}_{\boldsymbol{\phi}'}\}(z)=h^{-1}(z)$，其中 $\mathfrak{L}\{f\}$ 表示函数 f 的 Laplace 变换。文献 [19] 利用这一特性给出了常数 K 的构造方法。下面我们简要叙述 K 的构造过程，具体细节感兴趣的读者可以参阅 [19]。

引理4.1 ([4])　令 $\boldsymbol{\phi}'$ 为 $\boldsymbol{\phi}'(0)=U$ 且 $\boldsymbol{\phi}'(t)=O$，$\forall t\in[-r,0)$，其中 O 表示 $n\times n$ 维的零矩阵。令 $\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)$ 表示在方程 (4.2) 的初始条件变化为 $\boldsymbol{\phi}'$ 后的方程的解，$\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)$ 表示方程 (4.2) 的解。那么对 $t\geqslant 0$，

$$\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)=\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)\phi(0)+\int_{0}^{t}\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t-\tau)B\boldsymbol{\phi}(t-\tau)\,d\tau\,. \tag{4.5}$$

引理 4.1 给出了方程 (4.2) 的解 $\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)$ 与基解 $\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)$ 之间的关系，该引理结合上述定理 4.1，可得：

定理4.2 ([29])　令 $\iota=\max_{\lambda\in\sigma}\Re(\lambda)$ 表示谱 σ 中所有特征根实部的最大值，那么对于任意 $\mu>\iota$，存在 $K>0$ 使得

$$\parallel\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)\parallel\leqslant K\mathrm{e}^{\mu t},\forall t\geqslant 0\,, \tag{4.6}$$

$$\parallel\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)\parallel\leqslant K(1+\parallel B\parallel\int_{0}^{r}\mathrm{e}^{-\mu\tau}\,d\tau)\parallel\boldsymbol{\phi}\parallel\mathrm{e}^{\mu t}\forall t\geqslant 0,\forall\boldsymbol{\phi}\in\mathcal{C}([-r,0],\mathbb{R}^{n})\,. \tag{4.7}$$

特别地，如果 $\iota<0$，则 $\mathbf{x}_{\mathbf{e}}=\mathbf{0}$ 就是方程 (4.2) 的一个全局指数稳定平衡点。

在定理 4.2 中，方程 (4.2) 解 $\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)$ 的指数估计满足如不等式 (4.7) 所示的与基本解 $\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)$ 的指数估计的关系。如果已知基本解 $\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)$ 指数估计中的常数 K，则解 $\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)$ 的指数估计中的常数 (我们记作 $\hat{K}$) $\hat{K}=K(1+\parallel B\parallel\int_{0}^{r}\mathrm{e}^{-\mu\tau}\,d\tau)\parallel\boldsymbol{\phi}\parallel$。下面将给出常数 K 的一个显式表达式。

由 Laplace 逆变换，对于满足 $\Re(z)\geqslant\iota$ 的 z，我们有

$$\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)=\lim_{V\to\infty}\frac{1}{2\pi i}\int_{\mu-iV}^{\mu+iV}\mathrm{e}^{zt}h^{-1}(z)\,dz,$$

其中 $z=\mu+i\nu$，代入上式，得

$$\mathrm{e}^{-\mu t}\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)=\lim_{V\to\infty}\frac{1}{2\pi i}\int_{-V}^{V}\mathrm{e}^{i\nu t}h^{-1}(\mu+i\nu)\,d\nu.$$

将逆特征矩阵中二次项提出：

$$h^{-1}(z)=\frac{U}{z}+(h^{-1}(z)-\frac{U}{z})=\frac{U}{z}+\mathfrak{O}(\frac{U}{z^2}),$$

以二次项为被积函数的积分是收敛的，可得

$$\mathrm{e}^{-\mu t}\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)=\lim_{V\to\infty}\frac{1}{2\pi i}\int_{-V}^{V}\mathrm{e}^{i\nu t}\frac{U}{\mu+i\nu}\,d\nu+\frac{1}{2\pi i}\int_{-\infty}^{\infty}\mathrm{e}^{i\nu t}\mathfrak{O}\frac{U}{(\mu+i\nu)^2}\,d\nu.$$

对等式两边分别取范数，且 $\|\mathrm{e}^{i\nu t}\|=1$，我们有

$$\mathrm{e}^{-\mu t}\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)\leqslant\left\|\lim_{V\to\infty}\frac{1}{2\pi i}\int_{-V}^{V}\mathrm{e}^{i\nu t}\frac{U}{\mu+i\nu}\,d\nu\right\|+\frac{1}{2\pi i}\int_{-\infty}^{\infty}\mathrm{e}^{i\nu t}\left\|\mathfrak{O}\frac{U}{(\mu+i\nu)^2}\right\|\,d\nu. \tag{4.8}$$

如 [19]，对不等式 (4.8) 右边两项分别做处理，可得：

$$\begin{aligned}\left\|\lim_{V\to\infty}\frac{1}{2\pi i}\int_{-V}^{V}\mathrm{e}^{i\nu t}\frac{U}{\mu+i\nu}\,d\nu\right\|&\leqslant\begin{cases}0 & \forall t>0,\forall\mu<0\\ 1 & \forall t>0,\forall\mu>0.\end{cases}\\ \int_{-\infty}^{\infty}\mathrm{e}^{i\nu t}\left\|\mathfrak{O}\frac{U}{(\mu+i\nu)^2}\right\|\,d\nu&\leqslant\int_{-M}^{M}\left\|\mathfrak{O}\frac{U}{(\mu+i\nu)^2}\right\|\,d\nu+\frac{8n}{M}(\|A\|+\|B\|\,\mathrm{e}^{-r\mu}),\end{aligned} \tag{4.9}$$

其中，阈值 $M>0$。联立公式 (4.8) 和公式 (4.9)，可得到 $\mathrm{e}^{-\mu t}\parallel\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)\parallel$ 在时间区间 $t\in(0,\infty)$ 中的一个上界值：

$$K=\frac{1}{2\pi}\left(\int_{-M}^{M}\left\|\mathfrak{O}\frac{U}{(\mu+i\nu)^2}\right\|\,d\nu+\frac{8n}{M}(\|A\|+\|B\|\,\mathrm{e}^{-r\mu})\right)+1_0(\mu), \tag{4.10}$$

其中 $1_0:(\iota,\infty)\setminus\{0\}\to\{0,1\}$ 是集合 $\{\mu\mid\mu>0\}$ 的一个指示函数，即对于 $\mu>0$，$1_0(\mu)=1$，对于 $\iota<\mu<0$，$1_0(\mu)=0$。

结合定理 4.2 以及 μ 和常数 K 的构造过程，我们得到系统 (4.2) 的指数稳定性的定量准则，进而，下面定理将无界时间的微分不变式生成问题归结为有界时间的微分不变式生成问题：

定理4.3 给定初始函数 $\boldsymbol{\phi}$，以及平衡点 $\mathbf{x_e}=\mathbf{0}$，假设已知 $\mu<0$ 和 K，令 $\hat{K}=K(1+\|B\|\int_0^r\mathrm{e}^{-\mu\tau}\,d\tau)\,\|\boldsymbol{\phi}\|$，那么对于任意的 $\epsilon\in\mathbb{R}^+$，存在一个如下定义的时间 T^*：

$$T^*=\max\{0,\inf\{T\mid\forall t>T:\hat{K}\mathrm{e}^{\mu t}<\epsilon\}\}, \tag{4.11}$$

使得系统 (4.2) 的解 $\xi_{\boldsymbol{\phi}}(t)$ 满足：对于任意 $T>T^*$，$\|\xi_{\boldsymbol{\phi}}(T)-\mathbf{x_e}\|<\epsilon$，那么在 ϵ 精度范围内系统 (4.2) 的微分不变式等价于 T- 微分不变式。

证明 “必要性”是显然的，因为由定义 3.1，我们可知微分不变式蕴涵了 T- 微分不变式。对于“充分性”部分，因为由公式 (4.10) 构造的 K 是 $\mathrm{e}^{-\mu t}\left\|\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)\right\|$ 的一个上界，所以由定理 4.2 可知，对于任意 $t>0$ 及初始函数 $\boldsymbol{\phi}$，$\|\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)\|\leqslant\hat{K}\mathrm{e}^{\mu t}$ 成立。此外，平衡点为 $\mathbf{0}$，$\hat{K}\mathrm{e}^{\mu t}$ 关于 t 严格递减，因此给定精度 ϵ，存在有限 $T^*=\max\{0,ln(\epsilon/\hat{k})/\mu\}$ 使得系统 (4.1) 无穷逼近平衡点 $\mathbf{0}$，即在误差 ϵ 允许范围内，系统在时间区间 $t\in(T^*,\infty)$ 的所有可达状态为平衡点 $\mathbf{0}$。 □

4.1.2 非线性时延方程

本节研究对于非线性时延动态系统的微分不变式归结问题。首先利用线性化技术将非线性 DDEs 转化为相应的线性形式，进而将上一小节的理论部分推广到非线性系统。现在考虑 (4.1) 形式只含一个时延项的 DDEs，线性化后得 $\boldsymbol{f}(\mathbf{x},\mathbf{y}) = A\mathbf{x} + B\mathbf{y} + \boldsymbol{g}(\mathbf{x},\mathbf{y})$，其中 $A = \boldsymbol{f}_{\boldsymbol{x}}(\mathbf{0},\mathbf{0})$，$B = \boldsymbol{f}_{\boldsymbol{y}}(\mathbf{0},\mathbf{0})$，这里的 $\boldsymbol{f}_{\boldsymbol{x}}$ 和 $\boldsymbol{f}_{\boldsymbol{y}}$ 分别是 $\boldsymbol{f}$ 关于 $\mathbf{x}$ 和 $\mathbf{y}$ 的 Jacobian 矩阵。向量函数 $\boldsymbol{g}$ 是一个高次项，且在 $(\mathbf{0},\mathbf{0})$ 处 Jacobian 矩阵为零矩阵。略去高次项，以下方程为非线性系统 (4.1) 在平衡点 $\mathbf{0}$ 处的线性化形式：

$$\begin{cases} \dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{x}(t-r), & t \in [0,\infty) \\ \mathbf{x}(t) = \boldsymbol{\phi}(t), & t \in [-r,0] \end{cases} \tag{4.12}$$

显然该形式与上一节中讨论的线性系统 (4.2) 形式一致，因此两者具有相同形式的特征方程，我们用 σ 表示方程 (4.12) 的特征方程的谱。下面定理将给出非线性系统 (4.1) 的局部渐近行为与其线性化 (4.12) 的谱之间的关系：

定理4.4 ([29]) 假设 σ 满足 $\max_{\lambda\in\sigma}\Re(\lambda) < \mu < 0$，那么 $\mathbf{x} = \mathbf{0}$ 是非线性系统 (4.1) 的一个局部指数稳定的平衡点。事实上，存在一个 $K > 0$ 和 δ 使得

$$\| \boldsymbol{\phi} \| \leqslant \delta \Longrightarrow \| \boldsymbol{\xi}_{\boldsymbol{\phi}}(t) \| \leqslant K\mathrm{e}^{\mu t/2} \| \boldsymbol{\phi} \|, t \geqslant 0, \tag{4.13}$$

其中，$\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)$ 是系统 (4.1) 的解。相反，如果存在一个特征根使得 $\Re(\lambda) > 0$，则该平衡点 $\mathbf{x} = \mathbf{0}$ 不稳定。

与线性情况类似，定理 4.4 奠定了非线性系统的解的一个指数包络的存在性，而与线性系统满足全局指数稳定性不同的是，非线性系统仅满足局部指数稳定性，即该定理仅能保证系统在平衡点零处的一个 δ- 邻域内的任意初始函数出发的解以指数速度收敛于该平衡点，这也是定理 4.4 的局部性的含义。同理，为完成无界时间微分不变式生成问题归结于有界时间的微分不变式生成问题，我们需要构造 μ，K 以及 δ。

引理4.2 ([4])

$$\begin{cases} \dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{x}(t-r) + \boldsymbol{\eta}(t), & t \in [0,\infty) \\ \mathbf{x}(t) = \boldsymbol{\phi}(t), & t \in [-r,0] \end{cases} \tag{4.14}$$

$\boldsymbol{\xi}_{\boldsymbol{\phi}}(t)$ 表示方程 (4.14) 的解。令 $\boldsymbol{\phi}'$ 为 $\boldsymbol{\phi}'(0) = U$ 且 $\boldsymbol{\phi}'(t) = O$，$\forall t \in [-r,0)$，其中 O 表示 $n \times n$ 维的零矩阵。令 $\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)$ 表示在方程 (4.12) 的初始条件变化为 $\boldsymbol{\phi}'$ 后的方程的解，那么对 $t \geqslant 0$，

$$\boldsymbol{\xi}_{\boldsymbol{\phi}}(t) = \boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)\boldsymbol{\phi}(0) + \int_0^t \boldsymbol{\xi}_{\boldsymbol{\phi}'}(t-\tau)B\phi(t-\tau)\,d\tau + \int_0^t \boldsymbol{\xi}_{\boldsymbol{\phi}'}(t-\tau)B\boldsymbol{\eta}(\tau)\,d\tau\,. \tag{4.15}$$

借助上述基解的指数估计，下面定理可以刻画非线性系统的一个可计算的指数估计：

定理4.5 ([19]) 假设 $\max_{\lambda\in\sigma}\Re(\lambda) < \mu < 0$，那么存在 $K > 0$ 和 δ 使得线性化方程 (4.12) 的基解 $\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)$ 满足：$\| \boldsymbol{\xi}_{\boldsymbol{\phi}'}(t) \| \leqslant K\mathrm{e}^{\mu t}, \forall t \geqslant 0$，且非线性方程 (4.1) 满足

$$\| \boldsymbol{\phi} \| \leqslant \delta \Longrightarrow \| \boldsymbol{\xi}_{\boldsymbol{\phi}}(t) \| \leqslant K\mathrm{e}^{-r\mu}(1 + \| B \| \int_0^r \mathrm{e}^{-\mu\tau}\,d\tau) \| \boldsymbol{\phi} \| \mathrm{e}^{\mu t/2}, \forall t \geqslant 0\,. \tag{4.16}$$

类似于线性系统，如果非线性系统满足局部指数稳定性，根据定理 4.5 给出的非线性系统的构造性指数估计，我们可以将非线性系统的无界时间的微分不变式生成问题归结为有界时间的微分不变式生成问题：

定理4.6 给定初始函数 $\boldsymbol{\phi}$，假设已知 $\max_{\lambda\in\sigma}\Re(\lambda) < \mu < 0$ 和线性化方程 (4.12) 的基解 $\boldsymbol{\xi}_{\boldsymbol{\phi}'}(t)$ 满足：$\| \boldsymbol{\xi}_{\boldsymbol{\phi}'}(t) \| \leqslant K\mathrm{e}^{\mu t}, \forall t \geqslant 0$。令 $\widehat{K} = K\mathrm{e}^{-r\mu}(1+ \| B \| \int_0^r \mathrm{e}^{-\mu\tau}\, d\tau) \| \boldsymbol{\phi} \|$，那么对于任意的 $\epsilon \in \mathbb{R}^+$，存在一个 $\delta > 0$ 和如下定义的时间 T^*：

$$T^* = \inf\{T | \forall t > T : \widehat{K}\mathrm{e}^{\mu t/2} < \epsilon\}, \tag{4.17}$$

使得如果系统 (4.1) 的初始函数 $\| \boldsymbol{\phi} \| \leqslant \delta$，那么其解 $\xi_{\boldsymbol{\phi}}(t)$ 满足对于任意 $T > T^*$，$\|\boldsymbol{\xi}_{\boldsymbol{\phi}}(T) - \mathbf{x}_{\mathbf{e}}\| < \epsilon$，那么在 ϵ 精度范围内系统 (4.1) 的不变式等价于 T- 微分不变式。

证明 证明细节类似于定理 4.3，主要区别在局部稳定性，此处不再赘述。 □

定理 4.6 利用非线性系统的局部稳定性将微分不变式的生成问题归结为有界时间的微分不变式生成问题，然而，由于线性化过程带来的局限性，此定理所给出的等价性仅在 $\|\boldsymbol{\phi}\| \leqslant \delta$ 前提下成立。为了获得全局性的不变式等价性，我们首先给出一个集合 $\mathcal{B} \subseteq \mathbb{R}^n$ 满足 $\mathcal{B} \subseteq \mathcal{N}(\mathbf{x}_e, \delta)$，并且从 $\mathcal{B}$ 相应的初始函数集中的任意初始条件出发，系统的解最终将收敛于一个吸引子 $\mathbf{0}$。事实上，集合 $\mathcal{B}$ 就是该吸引子 $\mathbf{0}$ 吸引域的一个子集。如果能找到区间 $[T'-r, T']$，使得从初始状态集合出发的所有可达集都包含在集合 $\mathcal{B}$，则 $T' + T^*$ 足以作为一个时间上界：对于任意 $T > T' + T^*$，系统微分不变式等价于 T- 微分不变式。

例 1：(种群动态 [7]) 考虑用于模拟种群动态的著名 Wright 离散时延逻辑方程：

$$\dot{u}(t) = -u(t-r)\left[1 + u(t)\right], t \geqslant 0. \tag{4.18}$$

当时延 $r = 1$ 以及精度 $\epsilon = 0.05$，初始状态集合为 $X_0 = [0.4, 0.6]$，考虑系统 (4.18) 在 $[-r, \infty)$ 上的微分不变式生成问题。为构造系统解的指数估计，我们首先略去高次项 $u(t)u(t-r)$ 从而得到系统 (4.18) 的线性化：

$$\dot{v}(t) = -v(t-1), t \geqslant 0. \tag{4.19}$$

为将问题归结为有界时间的微分不变式生成问题，根据前文阐述的构造性方法，我们得到线性化系统 (4.19) 的常数 $\mu = -0.3, M = 2.69972$ 及 $K = 3.28727$，进而得到针对非线性系统 (4.18) 的常数 $\delta = 0.00351678$，$\hat{K} = 0.0250426$ 及 $T^* = 0s$。然后，借助文献 [30] 给出的 5 阶 Taylor 模型，在区间 $[14.5, 15.5]$ 内，系统解的上近似被完全包络在平衡点 $\mathbf{0}$ 的 δ- 邻域内。结合上述 $T^* = 0s$ 的结果，我们可以得出：对于任意时间 $T > 15.5$, 无界时间上的微分不变式生成问题等价于 T- 微分不变式生成问题。

4.2 CSI: 基于抽象精化的 T- 不变式生成

给定公式 (4.1) 所刻画的一个时延微分动态系统，算法 2 将微分不变式生成问题归结到有界时间 T- 微分不变式生成问题。针对 T- 微分不变式 I_q^* 生成问题，基于 [13] 一文中的工作，本节提出一种基于抽象精化的方法。在介绍算法前，我们先给出几个相关定义。

算法 2 CBT: 计算 T^*

输入: 方程 (4.1)：系统 $\boldsymbol{f}$ 及 $\boldsymbol{\phi}$，精度 ϵ，集合 $\mathcal{B}$

输出: 时间上界 T^*

1: **if** $\boldsymbol{f}$ 是非线性的 **then**
2: 线性化系统 $\boldsymbol{f}$
3: $T' \leftarrow \min\{T' \mid \bigcup_{t\in[T'-r,T']} R_{\boldsymbol{\phi}}(t) \subseteq \mathcal{B}\}$
4: 构造 μ 和 $\hat{K}$
5: **if** $\mu \geqslant 0$ **then**
6: **return** $T^* \leftarrow \infty$
7: **end if**
8: $T \leftarrow \inf\{T|\forall t > T : \widehat{K}\mathrm{e}^{\mu t/2} < \epsilon\}$
9: $T^* \leftarrow T' + T$
10: **else**
11: 构造 μ 和 $\hat{K}$
12: **if** $\mu \geqslant 0$ **then**
13: **return** $T^* \leftarrow \infty$
14: **end if**
15: $T^* \leftarrow \max\{0, \inf\{T \mid \forall t > T : \hat{K}\mathrm{e}^{\mu t} < \epsilon\}\}$
16: **end if**
17: **return** T^*

给定一个状态 $\mathbf{x} \in \mathbb{R}^n$ 及 $d \in R^+$，我们称 $\mathcal{N}(\mathbf{x}, d)$ 为一个抽象状态。一个状态集合 $X \subseteq \mathbb{R}^n$ 的抽象可以定义为 X 的一个划分：$\hat{X} = \{\mathcal{N}(\mathbf{x_i}, d), i = 0, 1, \ldots, m \mid \forall \mathbf{x} \in X, \exists \mathbf{x_i}. \|\mathbf{x} - \mathbf{x_i}\| \leqslant d\}$，即集合 X 中的任意状态 $\mathbf{x}$ 都至少对应一个抽象状态 $\mathcal{N}(\mathbf{x_i}, d)$。如果给定 d' 满足 $0 < d' < d$，我们定义集合 $\hat{M} = \{\mathcal{N}(\mathbf{x_j}, d'), j = 0, \ldots, m' \mid \forall \mathbf{x} \in X, \exists \mathbf{x_j}. \|\mathbf{x} - \mathbf{x_j}\| \leqslant d'\}$ 是 $\mathcal{N}(\mathbf{x}, d)$ 的一个精化。

算法 3[2] **CSI** 给出了基于抽象的 T- 微分不变式计算过程：初始 $t_0 = 0$，算法 δ-**Partition** 计算初始状态集合 X_0 的一个 δ- 覆盖，其中 X_0 满足对于 $(q, \boldsymbol{\phi}_q) \in \Xi_q$, $\forall \tau \in [-r, 0].\boldsymbol{\phi}_q(\tau) \in X_0$。该覆盖中的每个点 $\mathbf{x}$ 都对应于一个可以表示为 $\mathcal{N}(\mathbf{x}_0, \delta)$ 的划分，相应的抽象状态集合记为 $\hat{R}_0$, 同时初始状态集合 X_0 的凸包记为 R_0 （第 2 行）。不变式 $I^*_{q,0}$ 初始化为 R_0，并置 isSafe 为 true （第 3 行）。接下来，给定一个时间戳 $t_n < T$ 以及其对应的抽象状态集合 $\hat{R}_n$，算法 **SafePost** 计算从 $\hat{R}_n$ 出发一次步长为 τ 的离散仿真，得到在时间区间 $[t_n, t_{n+1}]$ 内满足方程 (4.1) 的所有安全解包络，记作 R_{n+1}。同时返回在时间戳 t_{n+1} 的安全抽象状态集合 $\hat{R}_{n+1}$ （第 5 行）。如果当前系统的可达集依然满足安全性质，即 isSafe 为 true，则算法 **SafePost** 将新一轮的 R_{n+1} 与 $I^*_{q,n}$ 求并集来更新不变式 $I^*_{q,n+1}$ （第 7 行），表示当前时刻之前的所有安全解的包络。否则返回空集（第 15 行），即系统的可达集是不安全的。上述过程不断迭代，直至 $I^*_{q,n}$ 不再变化（第 7，8 行），或者到达时间上界 T，算法终止，并返回 $I^*_{q,n} \cup \mathcal{N}(\mathbf{x}_e, \epsilon)$[3]。

2) 根据 [13] 一文中算法修改得到。
3) 假设 $\mathcal{N}(\mathbf{x}_e, \epsilon) \subseteq \mathcal{S}_q$。

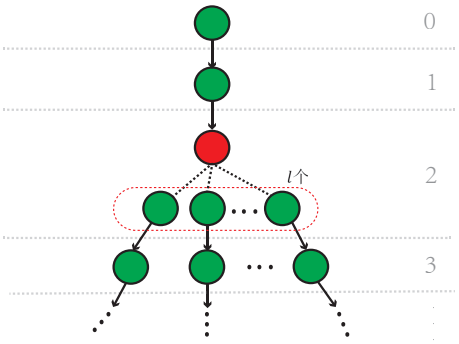

图 1　仿真树状轨迹。每个结点表示一个抽象状态，箭头表示在一个采样时间抽象状态间的迁移关系。第 2 层红色结点表示被精化状态，被精化为 l 个抽象状态，即与之虚线连接的绿色结点，且 l 个绿色结点为红色结点的有穷覆盖。

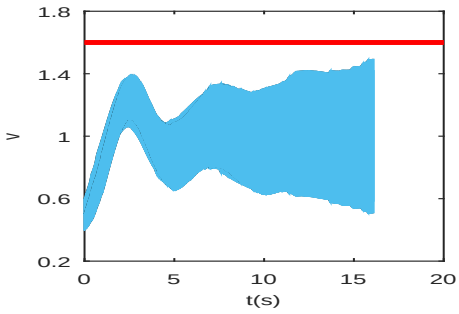

图 2　例 2 系统可达集。其中，采样步长 $\tau = 0.1s$，红色标线为最大安全阈值，蓝色管道区域为 16s 内系统从初始状态 $X_0 = \{v|v \in [0.4, 0.6]\}$ 出发所有可达集的安全上近似。

算法 4 描述了 **SafePost** 的计算，主要包括可靠模拟和抽象精化两部分，下面分别对两者详述:

1. 可靠模拟 （第 3-7 行）：对于任意抽象状态 $\mathcal{N}(\mathbf{x}_n, d_n) \in \hat{R}_n$，$\mathbf{x}_n$ 表示从 $\mathbf{x}_0$ 出发的解在时间戳 t_n 的状态近似，d_n 为其相应的局部误差上界。使用 [13] 提出的数值模拟方法，算法 4 首先利用前向欧拉方法，基于前序近似 $\mathbf{x}_n$ 和 $\mathbf{x}_{n-m}$ 来计算可达精确状态的近似状态 $\mathbf{x}_{n+1}$，其中，m 为偏移量，$\mathbf{x}_{n-m}$ 即 $t_n - r$ 时刻的延迟状态的近似。然后算法通过求解带约束的优化问题 (4.20) 来计算一误差斜率 e_n，进而得到局部误差上界 d_{n+1}。上述模拟获得了在时间戳 t_{n+1} 的可达抽象状态 $\mathcal{N}(\mathbf{x}_{n+1}, d_{n+1})$。

2. 精化与安全 （第 8-23 行）：基于新生成的抽象状态 $\mathcal{N}(\mathbf{x}_{n+1}, d_{n+1})$，算法计算在时间区间 $[t_n, t_{n+1}]$ 方程解的包络 $\mathcal{T}_n$ （第 8 行）。若 $\mathcal{T}_n$ 完全属于安全集合，那么将该集合并入 R_{n+1}，同时更新 $\hat{R}_n$ 及 $\hat{R}_{n+1}$，继续下一轮模拟计算；否则，若 $\mathcal{T}_n$ 被完全包含在不安全状态集合中，那么显然该可达集是不安全的，isSafe 置为 false（第 15 行）; 如果上述两个条件都不满足，算法将在满足阈值 ϵ_r 约束前提下，以 $d_n/2$ 为半径精化抽象状态 $\mathcal{N}(\mathbf{x}_n, d_n)$，随后重新进行新抽象状态的模拟（第 18 行）。值得注意的是，与 [13] 不同，当算法需要精化时，[13] 中只对初始状态进行精化，而 **SafePost** 算法的精化操作可能发生在仿真轨迹的每个时间戳 t_n 所生成的抽象状态 $\mathcal{N}(\mathbf{x}_n, d_n)$ 上。所以从一个初始抽象状态 $\mathcal{N}(\mathbf{x}_0, d_0)$ 出发，迭代调用 **SafePost** 算法会生成仿真树状轨迹，下面给出其直观解释与性质：

仿真树状轨迹：从一个初始抽象状态 $\mathcal{N}(\mathbf{x}_0, d_0)$ 出发，迭代调用 **SafePost** 算法生成仿真树状轨迹 $Tree = (V, v_0, V_{split}, E)$，如图 1, 其中 $v_0 = \mathcal{N}(\mathbf{x}_0, d_0)$ 为初始结点，V 为结点集合，E 为有向边集合，$V_{split} \subseteq V$ 为被分裂结点集合。对于每个边 $e = (v, w) \in E$ 满足：$w = post(v)$，$v = \mathcal{N}(\mathbf{x}_n, d_n), w = \mathcal{N}(\mathbf{x}_{n+1}, d_{n+1})$ 且对于 $t \in [t_n, t_{n+1}]$ $d_{n+1} = d_n + (t - t_n)e_{n+1}$。对于每个结点 $v \in V_{split}$ 满足：如果 $v = \mathcal{N}(\mathbf{x}, d)$，结点 v 分裂成 $v_0, \ldots, v_{l-1}$ l 个结点且 $v_i = \mathcal{N}(\mathbf{x_i}, d/2)$，$0 \leqslant i \leqslant l-1$，则 $\mathcal{N}(\mathbf{x}, d) \subseteq \bigcup_{0 \leqslant i \leqslant l-1} \mathcal{N}(\mathbf{x_i}, d/2)$，即 $v \subseteq \cup_{0 \leqslant i \leqslant l-1} v_i$。

给定初始状态集合 X_0 和有界时间 T，上述算法实现了基于抽象的 DDEs 有界时间内上近似可达集的计算，同时在给定的安全需求 $\mathcal{S}_q$ 的约束下，给出了相应的所有安全可达集的上近似。定理

4.7 给出了算法的正确性：

定理4.7 (正确性)　给定公式 (4.1) 所刻画的时延微分动态系统，以及有界时间 T，如果算法 3 终止时返回的 $I_q^* \neq \emptyset$，则满足下列性质：

1. $I_q^* \subseteq \mathcal{S}_q$，即 I_q^* 所包含的所有状态都是安全的；
2. $\Xi_q^* \subseteq \{(q, \boldsymbol{\phi}_q) \mid \forall \tau \in [-r_{k,q}, 0].\boldsymbol{\phi}_q(\tau) \in I_q^*\}$；
3. I_q^* 满足系统 (4.1) 的微分不变式定义，即任意从 $\boldsymbol{\xi}_{\boldsymbol{\phi}_q}(0) \in I_q^*$ 出发的解 $\boldsymbol{\xi}_{\boldsymbol{\phi}_q}(t)$ 满足

$$\forall t \in [-r_k, \infty).\boldsymbol{\xi}_{\boldsymbol{\phi}}(t) \in I_q \implies \forall t \in [-r_k, \infty).\boldsymbol{\xi}_{\boldsymbol{\phi}}(t) \in I_q^*.$$

算法 3 CSI: T- 微分不变式生成

输入: 向量场 $\boldsymbol{f}$，初始状态集合 Ξ_q，时间步长 τ，安全状态集合 $\mathcal{S}_q$，时间上界 T，阈值 ϵ_r, 精度 ϵ

输出: 不变式 I_q^*

1: $n \leftarrow 0$; $t_0 \leftarrow 0$; $X_0 \leftarrow \{\boldsymbol{\phi}_q(\cdot) \mid (q, \boldsymbol{\phi}_q) \in \Xi_q\}$; $\delta \leftarrow dia(X_0)/2$
2: $\hat{R}_0 \leftarrow \delta$ -**Partition**(X_0); $R_0 \leftarrow conv(X_0)$
3: $I_{q,0}^* \leftarrow R_0$, isSafe $\leftarrow$ true
4: **while** $t_n < T$ **do**
5: $(R_{n+1}, \hat{R}_{n+1}$,isSafe) $\leftarrow$**SafePost**$(\boldsymbol{f}(\mathbf{x}, \mathbf{x_r}), \hat{R}_n, \tau, \mathcal{S}_q, \epsilon_r, r, isSafe)$
6: **if** isSafe == true **then**
7: $I_{q,n+1}^* \leftarrow I_{q,n}^* \cup R_{n+1}$
8: **if** $I_{q,n+1}^* == I_{q,n}^*$ **then**
9: **return** $I_{q,n}^*$
10: **else**
11: $n \leftarrow n+1$; $t_n = t_n + \tau$
12: **end if**
13: **else**
14: **return** $\emptyset$
15: **end if**
16: **end while**
17: **return** $I_{q,n}^* \cup \mathcal{N}(\mathbf{x}_e, \epsilon)$

证明　从算法 4 中直接可以得到性质 1。由算法 3 的第 7-9 行可知 I_q^* 是递增构造的，即 $I_{q,0}^* \subseteq I_{q,1}^* \subseteq \cdots \subseteq I_{q,n}^* \subseteq I_{q,n+1}^* \cdots \subseteq I_q^*$，结合算法 3 的第 2 行和第 3 行，可知 $\boldsymbol{\phi}_q(\cdot) \in I_{q,0}^* \subseteq \cdots \subseteq I_q^*$，即性质 2 成立。下面只需证明性质 3。对于性质 3，若算法在第 9 行终止，则由 $I_{q,n}^* == I_{q,n+1}^*$ 可得 $I_{q,n}^*$ 作为微分不变式满足性质 3；若算法在第 17 行终止，由算法 4 的第 8-11 行可得对于每个时间戳 $t_n \leqslant T$ 有 $\forall t \in [t_n, t_n + \tau].\boldsymbol{\xi}_{\boldsymbol{\phi}}(t) \in \mathcal{T}_n \subseteq \mathcal{S}_q \subseteq I_q$，又由算法 3 的第 5-7 行可知对于 $\forall t \in [-r_k, T], \boldsymbol{\xi}_{\boldsymbol{\phi}}(t) \in I_{q,n}^*$，集合 $\mathcal{N}(\mathbf{x}_e, \epsilon)$ 包含了所有在 $t \geqslant T$ 的系统轨迹，综上可得性质 3 成立。□

例 2：在例 1 中，我们将种群动态系统无界时间的微分不变式生成问题归结到 $[-1, 15.5]$ 上的微分不变式生成问题。给定系统安全性质：$\mathcal{S} = \{u \mid u \leqslant 1.6\}$，根据上述 **CSI** 算法，我们取 $T =$

$16 > T^* = 15.5$, 然后使用工具自动生成 $T = 16s$ 上的微分不变式为 $\{u \in \mathbb{R} \mid 0.4 \leqslant u \leqslant 1.419467\}$, 生成的可达集如图 2 所示。

4.3 扩展到多时延的 DDEs

在实际系统的数学模型中，时延微分方程往往含有多个离散的时延项，用来刻画系统中同时存在不同延时耦合的部件及部件间交互行为。上述小节 4.1 和 4.2 讨论的含有一个时延项方程的算法可以直接扩展到多个时延项的微分方程。例如，在 4.1 节中 $\|B\|$ 直接替换为 $\sum_{i=1}^{k}\|A_i\|$，其中 A_i 表示时延项 $\mathbf{x}(t-r_i)$ 对应的 Jacobian 矩阵；相应地，$\|B\|\,\mathrm{e}^{-r\mu}$ 直接替换为 $\sum_{i=1}^{k}\|A_i\|\,\mathrm{e}^{-r_i\mu}$。在 4.2 节算法 4 中，相应地引入多个不同的偏移量 $m_1 \leftarrow r_1/\tau, \ldots, m_k \leftarrow r_k/\tau$，欧拉方法估计后置状态与优化问题 (4.20) 对 e 的估计相应地更新为 k 个时延项。更多细节不一一赘述。

5 实验分析

基于配置为 1.6Ghz Intel Core-i5 处理器、8GB 内存、64 位 Windows 10 系统的 HP-Pavilion，我们将本文提出的切换控制器合成算法应用于使用 PD- 控制器的时延混成系统的案例研究中。

考虑一个控制车辆运行的 PD- 控制器混成系统。该系统由两个模式组成: q_1 和 q_2。由于 PD- 控制器在感知、计算、传输与控制执行等过程中存在时间延迟，每个模式中的连续行为由 DDE 刻画。在此案例中，我们考虑线性 DDEs:

$$\boldsymbol{f}_{q_1}: \begin{cases} \dot{y}(t) = v(t) \\ \dot{v}(t) = -y(t-r) - 4v(t-r) \end{cases}, \boldsymbol{f}_{q_2}: \begin{cases} \dot{y}(t) = v(t) \\ \dot{v}(t) = -2y(t-r) - 3v(t-r) \end{cases},$$

其中 y 表示车辆位置，v 表示其速度，r 为时延常数且 $r = 0.45$。两个模式的初始集为：$\Xi_{q_1} = \{q_1\} \times U_{q_1}$, $\Xi_{q_2} = \{q_2\} \times U_{q_2}$, 其中 $U_{q_1} = \{\boldsymbol{\phi}_{q_1}(\cdot) : [-r, 0] \to \mathbb{R}^2 \mid$ 对$t \in [-r, 0], \boldsymbol{\phi}_{q_1}(t) \equiv (c_1, c_2)', c_1 \in [-0.1, 0], c_2 \in [0, 0.1]\}$ 和 $U_{q_2} = \{\boldsymbol{\phi}_{q_2}(\cdot) : [-r, 0] \to \mathbb{R}^2 \mid$ 对$t \in [-r, 0], \boldsymbol{\phi}_{q_2}(t) \equiv (c_1, c_2)', c_1 \in [-0.1, 0], c_2 \in [0, 0.1]\}$，安全区域为：$\mathcal{S}_{q_1} = \mathcal{S}_{q_2} = \{(y, v) \in \mathbb{R}^2 \mid y \leqslant 0.6\}$，不变式: $I_{q_1} = I_{q_2} = \{(y, v) \in R^2 \mid y \leqslant 0.6\}$。对于迁移边 $e_1 = (q_1, q_2)$，迁移条件 $G(e1) = \{(y, v) \in \mathbb{R}^2 \mid y \leqslant 0\}$; 对于迁移边 $e_2 = (q_2, q_1)$，迁移条件 $G(e2) = \{(y, v) \in \mathbb{R}^2 \mid y \geqslant 0\}$，且每个迁移边上的重置函数为恒等映射, 即重置后新模式下的初始函数恒等于重置前状态的映射。

在模式 q_1 中，首先调用算法 **CBT**，计算的相关常数如下：$\mu = -0.5$，$M = 12.8403$，$K = 4.54748$ 以及 $\hat{K} = 1.74635$。在此基础上，由定理 4.3 我们得到 $T^* = 7.57838$s, 该模式下微分不变式生成问题转化为满足 $T > T^* = 7.57838$ 的 T- 微分不变式生成问题。在此例中，我们取 $T = 8$s。进而，调用算法 **CSI**，计算该模式下满足安全性质的微分不变式。图 3(a) 所示的蓝色区域为时间 8s 内的此模式下可达集的上近似。我们得到模式 q_1 的微分不变式为：$I^*_{q_1} = \{(y, v) \in \mathbb{R}^2 \mid (y, v) \in [-0.62, 0.46] \times [-1.01, 1.17]\}$。类似地，计算模式 q_2 的微分不变式。调用算法 **CBT**，生成的常数如下：$\mu = -1$，$M = 16.4872$，$K = 3.03144$ 以及 $\hat{K} = 1.28642$。在此基础上，由定理 4.3 我们得到 $T^* = 4.45157$s, 该模式下的微分不变式问题被转化为任意满足

算法 4 SafePost

输入: 向量场 $\boldsymbol{f}$，状态集合 $\hat{R}_n$，步长 τ，安全状态集合 $\mathcal{S}_q$，阈值 ϵ_r，时延 r，isSafe

输出: 可达集 R_{n+1}，$\hat{R}_{n+1}$, isSafe

$m \leftarrow r/\tau$; $R_{n+1} \leftarrow \emptyset$; $\hat{R}_{n+1} \leftarrow \emptyset$

while $\hat{R}_n \neq \emptyset$ **do**

  $\mathcal{N}_2(\mathbf{x}_n, d_n) \leftarrow \text{pop}(\hat{R}_n)$

  $\mathbf{x}_{n+1} \leftarrow \mathbf{x}_n + \boldsymbol{f}(\mathbf{x_n}, \mathbf{x_{n-m}}) * \tau$

  $e_n \leftarrow$ Find minimum e s.t.

$$
\begin{cases}
\|\boldsymbol{f}(\mathbf{x} + t * \boldsymbol{f}, \mathbf{x_r} + t * \boldsymbol{g}) - \boldsymbol{f}(\mathbf{x}_n, \mathbf{x}_{n-m})\| \leqslant e - \sigma, \\
\forall t \in [0, \tau] \\
\forall \mathbf{x} \in \mathcal{N}_2(\mathbf{x}_n, d_n) \\
\forall \mathbf{x_r} \in \mathcal{N}_2(\mathbf{x}_{n-m}, d_{n-m}) \\
\forall \boldsymbol{f} \in \mathcal{N}_2(\boldsymbol{f}(\mathbf{x}_n, \mathbf{x}_{n-m}), e) \\
\forall \boldsymbol{g} \in \mathcal{N}_2(\boldsymbol{f}(\mathbf{x}_{n-m}\mathbf{x}_{n-2m}), e_{n-m})
\end{cases}
\tag{4.20}
$$

  $d_{n+1} \leftarrow d_n + e_n * \tau$

  $\mathcal{T}_n \leftarrow conv(\mathcal{N}_2(\mathbf{x}_n, d_n) \cup \mathcal{N}_2(\mathbf{x}_{n+1}, d_{n+1}))$

  if $\mathcal{T}_n \subseteq \mathcal{S}_q$ **then**

    $R_{n+1} \leftarrow R_{n+1} \cup \mathcal{T}_n$

    $\hat{R}_n \leftarrow \hat{R}_n \setminus \mathcal{N}_2(\mathbf{x}_n, d_n)$

    $\hat{R}_{n+1} \leftarrow \hat{R}_{n+1} \cup \mathcal{N}_2(\mathbf{x}_{n+1}, d_{n+1})$

  end if

  if $\mathcal{T}_n \subseteq \mathcal{S}_q^c$ **then**

    isSafe $\leftarrow$ false

  else

    $\hat{R}_n \leftarrow R_n \setminus \mathcal{N}_2(\mathbf{x}_n, d_n)$

    if $d_n/2 \geqslant \epsilon_r$ **then**

      $\hat{R}_n \leftarrow \hat{R}_n \cup \frac{d_n}{2}$-**Partition** $\mathcal{N}_2(\mathbf{x}_n, d_n)$

    else

      isSafe $\leftarrow$ false

    end if

  end if

end while

return $(R_{n+1}, \hat{R}_{n+1}, \text{isSafe})$

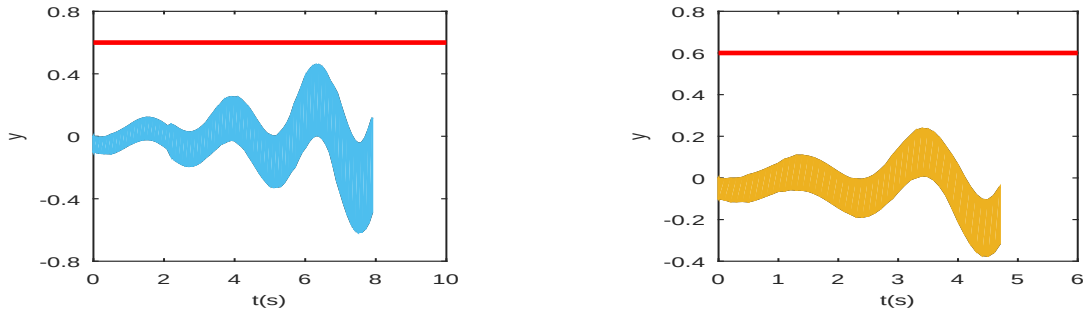

图 3　PD- 控制器时延系统模式 q_1 和 q_2 下的可达集。

$T > T^* = 4.45157$ 的 T- 微分不变式生成问题。我们取 $T = 4.7$s。进而，调用算法 **CSI**，计算该模式下满足安全性质的不变式。图 3(b) 所示的黄色区域为时间 4.7s 内的此模式下可达集的上近似。我们得到模式 q_2 的微分不变式为：$I^*_{q_2} = \{(y, v) \in \mathbb{R}^2 \mid (y, v) \in [-0.38, 0.24] \times [-0.68, 0.76]\}$。

最后，利用所求得的模式 q_1 和 q_2 下微分不变式 $I^*_{q_1}$ 和 $I^*_{q_2}$，我们可以得到 PD- 控制器时延混成系统的微分不变式 $I^* = (q_1, I^*_{q_1}) \bigcup (q_2, I^*_{q_2}) = (q_1, \{(y, v) \in \mathbb{R}^2 \mid (y, v) \in [-0.62, 0.46] \times [-1.01, 1.17]\}) \bigcup (q_2, \{(y, v) \in \mathbb{R}^2 \mid (y, v) \in [-0.38, 0.24] \times [-0.68, 0.76]\})$，和迁移条件：$G^*(e_1) = \{(y, v) \in \mathbb{R}^2 \mid (y, v) \in [-0.38, 0] \times [-0.68, 0.76]\}$，$G^*(e_2) = \{(y, v) \in \mathbb{R}^2 \mid (y, v) \in [0, 0.24] \times [-0.68, 0.76]\}$, 初始集合 $\Xi^* = \Xi$。

6　结论

本文提出了一个基于不变式生成的针对一类时延混成系统的切换控制器合成算法。基于谱分析和线性化技术，我们将时延动态系统的微分不变式生成问题转化为有限时间内的可达集计算问题。基于微分不变式的生成，我们的方法可以计算一个时延混成系统的切换控制器，合成的切换控制器不仅可以保证系统行为是无阻塞的，并且满足给定的安全性质。我们在一个 PD- 控制器时延系统上测试了我们的方法。未来工作我们将对本文所研究的时延混成系统模型做进一步完善, 考虑时延同时存在于不同控制模式的离散切换中，以及考虑更复杂的系统性质如实时性及活性等。

参考文献

1　Wing J. How can we provide people with cyber-physical systems they can bet their lives on[J]. Computing Research News, 2008, 20 No.1.

2　Myshkis A D. Lineare differentialgleichungen mit nacheilendem argument[M]. Deutscher Verlag der Wissenschaften, 1955.

3　Hahn W. Stability of motion[M]. Berlin: Springer, 1967.

4　Hale J K, Lunel S M V, Verduyn L S, et al. Introduction to functional differential equations[M]. Springer Science Business Media, 1993.

5　Cooke K L. Stability analysis for a vector disease model[J]. The Rocky Mountain Journal of Mathematics, 1979, 9(1): 31-42.

6　Ikeda K, Matsumoto K. High-dimensional chaotic behavior in systems with time-delayed feedback[J]. Physica D: Nonlinear Phenomena, 1987, 29(1-2): 223-235. doi:10.1016/0167-2789(87)90058-3

7　Kuang Y. Delay differential equations: with applications in population dynamics[M]. Academic press, 1993.

8　Huang Z, Fan C, Mitra S. Bounded invariant verification for time-delayed nonlinear networked dynamical systems[J]. Nonlinear Analysis: Hybrid Systems, 2017, 23: 211-229. doi:10.1016/j.nahs.2016.05.005

9 Zou L,Franzle M, Zhan N, Mosaad P N. Automatic Verification of Stability and Safety for Delay Differential Equations[C]. Computer Aided Verification, 2015, 338–355. doi:10.1007/978-3-319-21668-3-20

10 Karniadakis G, Sherwin S J. Numerical mathematics and scientific computation[M]. Oxford University Press, 1999.

11 Orosz G, Ames A D. Safety functionals for time delay systems[C]. 2019 American Control Conference (ACC). IEEE, 2019: 4374-4379. doi: 10.23919/ACC.2019.8814681

12 Prajna S, Jadbabaie A. Methods for safety verification of time-delay systems[C]. Proceedings of the 44th IEEE Conference on Decision and Control. IEEE, 2005: 4348-4353. doi: 10.1109/CDC.2005.1582846

13 Chen M, Franzle M, Li Y, et al. Validated simulation-based verification of delayed differential dynamics [C]. International Symposium on Formal Methods. Springer, Cham, 2016: 137-154. doi:10.1007/978-3-319-48989-6-9

14 Xue B, Mosaad P N, Franzle M, et al. Safe over-and under-approximation of reachable sets for delay differential equations[C]. International Conference on Formal Modeling and Analysis of Timed Systems. Springer, Cham, 2017: 281-299. doi:10.1007/978-3-319-65765-3-16

15 Xue B, Easwaran A, Cho N J, et al. Reach-avoid verification for nonlinear systems based on boundary analysis[J]. IEEE Transactions on Automatic Control, 2016, 62(7): 3518-3523. doi:10.1109/TAC.2016.2615599

16 Xue B, She Z, Easwaran A. Under-approximating backward reachable sets by polytopes[C]. International Conference on Computer Aided Verification. Springer, Cham, 2016: 457-476. doi:10.1007/978-3-319-41528-4-25

17 Goubault E, Putot S, Sahlmann L. Inner and outer approximating flowpipes for delay differential equations[C]. International Conference on Computer Aided Verification. Springer, Cham, 2018: 523-541. doi:10.1007/978-3-319-96142-2-31

18 Berz M, Makino K. Verified integration of ODEs and flows using differential algebraic methods on high-order Taylor models[J]. Reliable computing, 1998, 4(4): 361-369. doi:10.1023/A:1024467732637

19 Feng S, Chen M, Zhan N, et al. Taming delays in dynamical systems[C]. International Conference on Computer Aided Verification. Springer, Cham, 2019: 650-669. doi:10.1007/978-3-030-25540-4-37

20 Zhao H, Zhan N, Kapur D. Synthesizing switching controllers for hybrid systems by generating invariants[M]. Theories of Programming and Formal Methods. Springer, Berlin, Heidelberg, 2013: 354-373. doi: 10.1007/978-3-642-39698-4-22

21 Alur R, Courcoubetis C, Henzinger T A, et al. Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems[M]. Hybrid systems. Springer, Berlin, Heidelberg, 1992: 209-229. doi:10.1007/3-540-57318-6-30

22 Zheng G, Tan M, Song Y. An approach to analyze the stability of a class of hybrid systems with delay[C]. Fifth World Congress on Intelligent Control and Automation (IEEE Cat. No.04EX788), Hangzhou, China, 2004:1079-1083 Vol.2. doi: 10.1109/WCICA.2004.1340777

23 Diekmann O, Van Gils S A, Lunel S M V, et al. Delay equations: functional-, complex-, and nonlinear analysis[M]. Springer Science Business Media, 2012.

24 Wulf V, Ford N J. Numerical Hopf bifurcation for a class of delay differential equations[J]. Journal of Computational and Applied Mathematics, 2000, 115(1-2): 601-616. doi:10.1016/S0377-0427(99)00181-8

25 Engelborghs K, Roose D. On stability of LMS methods and characteristic roots of delay differential equations[J]. SIAM Journal on Numerical Analysis, 2002, 40(2): 629-650. doi:10.1137/S003614290037472X

26 Breda D, Maset S, Vermiglio R. Computing the characteristic roots for delay differential equations[J]. IMA Journal of Numerical Analysis, 2004, 24(1): 1-19. doi: 10.1093/imanum/24.1.1

27 Collins G E. Quantifier elimination for real closed fields by cylindrical algebraic decompostion[C]. Automata Theory and Formal Languages 2nd GI Conference Kaiserslautern, May 20 – 23, 1975. Springer, Berlin, Heidelberg, 1975: 134-183. doi:10.1007/3-540-07407-4-17

28 Engelborghs K, Luzyanina T, Roose D. Numerical bifurcation analysis of delay differential equations using DDE-BIFTOOL[J]. ACM Transactions on Mathematical Software (TOMS), 2002, 28(1): 1-21. doi:10.1145/513001.513002

29 Smith H L. An introduction to delay differential equations with applications to the life sciences[M]. New York: Springer, 2011.

30 Goubault E, Putot S. Inner and outer reachability for the verification of control systems[C]. Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control. 2019: 11-22. doi: 10.1145/3302504.3311794

Switching Controller Synthesis for Time-delayed Hybrid Systems

Yunjun Bai , Ting Gan, Li Jiao, Bai Xue & Naijun Zhan

Abstract How to design safe and reliable safety-critical cyber-physical systems (CPS) so that we can bet our daily life on them is a grand challenge to computer science and control theory. Delays in feedback control are ubiquitous, that is, the behavior evolution of a system depends not only on its current state, but also on its execution history. Obviously, delays may invalidate the stability/safety certificates obtained by abstracting them away as in the design of modern CPS normally. In this paper, we study the switching controller synthesis problem of time-delayed hybrid systems, and propose an invariant-based approach by extending the corresponding approach to the design of CPS without delays. To this end, based on spectral analysis and linearization, we first show that the differential invariant generation problem of delay dynamical systems can be reduced to computing reachable sets over bounded time horizon; we then propose an abstract-based algorithm to over-approximate the reachable set over a given time bound; finally, we implement a prototypical tool of our approach and illustrate it with examples.

Keywords **Time-delayed hybrid systems, delay differential equations, differential invariants, switching controller, safety**

MSC(2010) **34K04, 93B50, 93C30**

doi: 10.1360/N012017-XXXX