

基于多面体包含的非线性混成系统可达性分析

邹进¹, 林望^{1,2*}, 罗勇¹, 曾振柄²

(1. 温州大学 数学与信息科学学院, 浙江 温州 325035; 2. 华东师范大学 上海市高可信计算重点实验室, 上海 200062)

(* 通信作者电子邮箱 linwang@wzu.edu.cn)

摘要: 针对一类非线性混成系统的可达性问题, 提出了一种基于多面体包含的分析方法。首先介绍了混成系统及其可达性, 讨论了如何应用多面体包含对多项式混成系统进行线性近似, 并采用量词消去和非线性优化方法来构造相应的线性混成系统, 然后运用验证工具 SpaceEx 求得原非线性混成系统的过近似可达集, 并应用于验证系统的安全性。

关键词: 混成系统; 可达性分析; 安全性验证; 多面体包含; 线性近似

中图分类号: TP311 **文献标志码:** A

Reachability analysis of nonlinear hybrid systems based on polyhedron inclusion

ZOU Jin¹, LIN Wang^{1,2*}, LUO Yong¹, ZENG Zhenbing²

(1. College of Mathematics and Information Science, Wenzhou University, Wenzhou Zhejiang 325035, China;

2. Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai 200062, China)

Abstract: To study the reachability of a class of nonlinear hybrid systems, this paper presented an verification method based on polyhedron inclusion. Firstly, some notions about hybrid systems and reachability were introduced. The method based on polyhedron inclusion was proposed to compute the linear approximation of polynomial hybrid systems. Quantifier elimination and nonlinear optimization method were applied to obtain the associated linear hybrid systems. Then the over-approximation of reachable set of original polynomial hybrid systems can be computed by using SpaceEx. Furthermore, the safety properties of the systems also can be verified.

Key words: hybrid system; reachability analysis; safety verification; polyhedron inclusion; linear approximation

0 引言

信息物理融合系统(Cyber-Physical System, CPS)作为计算进程与物理过程的结合体,是集传感、通信、计算与控制于一身的下一代智能系统,已广泛应用于汽车、电力、航空航天、国防、工业自动化等重要领域。混成系统作为CPS的数学模型,是一类既包含连续动态行为又包含离散动态行为的复杂系统,其动力学行为既随时间而连续变化,又受事件而离散驱动。混成系统的分析与验证已成为当今计算机科学与控制学科的前沿研究热点。

可达性分析是混成系统分析与验证中的重要问题,是指系统是否可由初始状态开始,经系统轨迹到达某个给定的目标状态。许多混成系统验证问题,如安全性验证等,都可以转化为可达性分析问题。近年来,混成系统可达性分析已得到广泛研究,并取得了一些重要结果。文献[1-4]通过计算可达集对矩形自动机、多速率自动机、时间自动机等几类特殊的混成系统的可达性问题进行了研究。然而,对于大多数混成系统,连续变量和离散事件间相互作用的特性,使得可达集的精确计算非常困难,因而文献[5]提出了近似计算可达集的思想。在此基础上,文献[6]和文献[7]分别采用多面体(Polyhedron)、椭球体(Ellipsoid)等几何对象表示系统状态空间,并运用图论、几何方法和最优化方法来近似计算一类线性混成系统的可达集。文献[8]将线性混成系统可达性问题

归化为实闭域上的量词消去问题,进而运用现有的计算机代数系统进行有效求解。文献[9]考虑了一类带微分包含的线性混成系统的可达性问题,并通过构造支撑函数来得到系统的过近似可达集。目前,可应用于线性混成系统可达性分析的工具主要有Phaver^[10]、CheckMate^[11]、SpaceEx^[12]、d/dt^[13]等。而对于非线性混成系统,一般先将非线性混成系统转化为近似的线性混成系统,再通过对线性混成系统的研究来实现原先的非线性混成系统的分析与验证。文献[14-16]运用单纯形构造方法对系统状态空间进行划分,从而将非线性系统转化为带外部扰动的线性混成系统,并实现了原系统的近似可达集的计算。文献[17]运用线性phase-portrait近似方法一类特殊的非线性混成系统的可达性问题进行了研究。

本文将讨论多项式混成系统的可达性分析问题。首先提出了一个多面体包含方法来对多项式混成系统进行线性近似,并采用量词消去和非线性优化方法来构造相应的线性混成系统,然后运用验证工具SpaceEx计算系统的过近似可达集,并应用于系统的安全性验证。与已有的方法相比,本文的方法具有普遍性,适用于一般的多项式混成系统的分析与验证。

1 混成系统及其可达性

混成系统通常采用混成自动机来建模,其定义如下所述:

定义1 混成自动机。混成自动机是具有如下形式的八

收稿日期: 2012-11-19; **修回日期:** 2012-12-31。 **基金项目:** 国家自然科学基金资助项目(11001204); 国家973计划项目(2011CB302904); 浙江省教育厅科研项目(Y201120383); 温州大学实验室研究项目(JWS20120612)。

作者简介: 邹进(1990-),男,江西抚州人,硕士研究生,主要研究方向:微分方程、计算机数学; 林望(1982-),男,浙江温州人,博士研究生,主要研究方向:程序验证、混成系统分析与验证; 罗勇(1978-),男,安徽合肥人,副教授,主要研究方向:符号计算、微分方程定性理论; 曾振柄(1963-),男,甘肃皋兰人,教授,博士生导师,主要研究方向:数学机械化、定理机器证明、自动推理。

元组 $H = (\mathbf{x}, L, flow, Init, Inv, E, G, R)$ 。其中:

$\mathbf{x} = (x_1, x_2, \dots, x_n)^T \in \mathbf{R}^n$ 是连续状态变量;

$L = \{l_1, l_2, \dots, l_m\} (m \in \mathbf{N})$ 是离散状态(位置)集;

$flow$ 是一个赋值函数,它为每个位置赋予一个关于 \mathbf{x} 的微分方程,即对于每个位置 $l \in L$, $flow(l)$ 为 $\dot{\mathbf{x}} = f_l(\mathbf{x})$, 其中 $\dot{\mathbf{x}}_1 = f_{l_1}(x_1, x_2, \dots, x_n)$, $\dot{\mathbf{x}}_2 = f_{l_2}(x_1, x_2, \dots, x_n)$, \dots , $\dot{\mathbf{x}}_n = f_{l_n}(x_1, x_2, \dots, x_n)$;

$Init$ 是一个赋值函数,它为每个位置 $l \in L$ 赋予一个关于 \mathbf{x} 的初始条件 $Init(l)$;

Inv 是一个赋值函数,它为每个位置 $l \in L$ 赋予一个关于 \mathbf{x} 的不变集约束 $Inv(l)$, 即对于每个位置 $l \in L$, 都有 $\mathbf{x} \in Inv(l)$;

$E \subseteq L \times L$ 是所有离散变迁(或边)的有限集合;

$G = \{G(e) | e \in E\}$ 是一个赋值函数,它为每条边 $e \in E$ 赋予一个能触发离散变迁的连续变量取值条件;

$R = \{R(e) | e \in E\}$ 是一个赋值函数,它为每条边 $e \in E$ 赋予一个经过 e 转换后连续变量重新赋值的取值条件。

例1 温控系统。图1为温度控制系统的混成自动机模型,其中连续变量 x 表示温度,离散位置 ON、OFF 分别表示系统加热器处于“开”状态和“关”状态。假设起始温度为 x_0 , 加热器为“开”状态。若温度不超过 M 时,温度 x 随微分方程 $\dot{x} = f_1(x)$ 变化而上升;而当温度到达 a_1 时,加热器将由“开”状态转变为“关”状态,系统则变迁至 OFF 位置;此时,若温度不低于 m 时,温度 x 随微分方程 $\dot{x} = f_2(x)$ 变化而下降;而当温度下降至 a_2 时,加热器将由“关”状态转变为“开”状态,系统变迁至 ON 位置又开始加热。

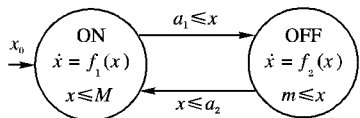


图1 温控系统自动机

混成系统 H 的状态为一个二元组 (l, \mathbf{x}) , 其中 $l \in L, \mathbf{x} \in \mathbf{R}^n$ 。系统轨迹则是由初始状态经连续演变及离散变迁所构成的状态序列,如 $(l_0, \mathbf{x}_0) \rightarrow (l_0, \mathbf{x}_1) \rightarrow \dots \rightarrow (l_1, \mathbf{x}_1') \rightarrow (l_1, \mathbf{x}_2') \rightarrow \dots$, 其中 $(l_0, \mathbf{x}_0) \in L \times Init$ 。当离散位置为 l , 连续变量 $\mathbf{x} \in Inv(l)$ 时, \mathbf{x} 按照 $\dot{\mathbf{x}} = f_l(\mathbf{x})$ 进行演变,且 l 保持不变。当离散位置为 l , 连续变量 $\mathbf{x} \in G(e)$, $e = (l, l') \in E$ 时, 则系统发生离散变迁 e , 状态 (l, \mathbf{x}) 可能跳变到任意的 $(l', \mathbf{x}') \in l' \times R(e)$, 之后当连续变量满足 $\mathbf{x} \in Inv(l')$ 时, 系统根据 $flow(l')$ 进行演变。

本文将讨论混成系统的可达性问题,即混成系统是否可由初始状态开始,经过系统轨迹到达某个给定的目标状态。一般来说,混成系统可达性分析可通过可达集的计算来实现。对于混成系统 H , 其可达集是指起始于任意初始状态 $(l_0, \mathbf{x}_0) \in L \times Init$, 并经连续演变或离散变迁后所能达到的所有状态的集合,记为 $Reach(H)$ 。

2 可达性分析

由上所述,非线性混成系统可达集的计算是非常困难的。本文拟将非线性混成系统转化为一个近似的易于计算的线性混成系统,即任意的 $Init(l)$ 、 $Inv(l)$ 、 $flow(l)$ 、 $G(e)$ 和 $R(e)$ 都是线性表示的,并通过分析该线性混成系统来实现原非线性混成系统的可达性分析。

本文限于考虑多项式混成系统,其定义如下:

定义2 多项式混成系统。多项式混成系统即为满足如

下条件的一类非线性混成系统:

1) 对任意的 $l \in L$ 及 $e \in E$, $Init(l)$ 、 $Inv(l)$ 、 $G(e)$ 和 $R(e)$ 都为 \mathbf{x} 上的多项式不等式(组);

2) 对任意的 $l \in L$, $flow(l)$ 为 $\dot{\mathbf{x}} = f_l(\mathbf{x}) \in \mathbf{R}[\mathbf{x}]$ 。

对于多项式混成系统,本文将提出一个多面体包含方法对其进行线性近似。首先定义如下一个关系:

定义3 蕴含关系^[17]。给定两个约束集 $S(\mathbf{x})$ 、 $S'(\mathbf{x})$, 其中向量 $\mathbf{x} = (x_1, x_2, \dots, x_n)^T \in D \subseteq \mathbf{R}^n$, 若 $S(\mathbf{x}) \subseteq S'(\mathbf{x})$, 则称 $S'(\mathbf{x})$ 蕴含 $S(\mathbf{x})$, 记为 $S(\mathbf{x}) < S'(\mathbf{x})$ 。

那么,给定多项式混成系统 $H = (\mathbf{x}, L, flow, Init, Inv, E, G, R)$, 若存在一个线性混成系统 $H' = (\mathbf{x}, L, flow', Init', Inv', E, G', R')$, 使得对任意的 $l \in L$, 都有 $Init(l) < Init'(l)$, $Inv(l) < Inv'(l)$ 和 $flow(l) < flow'(l)$, 以及对任意的 $e \in E$, 都有 $G(e) < G'(e)$ 和 $R(e) < R'(e)$, 则称线性混成系统 H' 蕴含非线性混成系统 H , 记为 $H < H'$ 。显然, $Reach(H) \subseteq Reach(H')$ 。

2.1 线性近似

本节将讨论如何对非线性混成系统进行线性近似,即对非线性混成系统中的非线性项(如多项式方程、多项式不等式等)应用多面体包含方法进行线性近似,从而得到易于计算的线性混成系统。

定义4 多面体包含。对于函数 $y = f(\mathbf{x})$, 其中 $\mathbf{x} \in X \subseteq \mathbf{R}^n$, 若存在向量 $\mathbf{c} \in \mathbf{R}^n$, $a, b \in \mathbf{R}$, 使得对 $\forall \mathbf{x} \in X$ 有

$$\mathbf{c}^T \cdot \mathbf{x} + a \leq f(\mathbf{x}) \leq \mathbf{c}^T \cdot \mathbf{x} + b \quad (1)$$

成立,则称 $[\mathbf{c}^T \mathbf{x} + a, \mathbf{c}^T \mathbf{x} + b]$ 为 $f(\mathbf{x})$ 的一个多面体包含。

为精确近似非线性混成系统,本文希望计算最小多面体包含,即除满足条件(1)外,还使得 $|a - b|$ 最小的多面体包含。因此,为计算 $f(\mathbf{x})$ 的最小多面体包含,构造如下参数多项式优化问题:

$$\min (a - b)^2 \quad (2)$$

$$\begin{aligned} \text{s. t. } & f(\mathbf{x}) - \mathbf{c}^T \mathbf{x} - a \geq 0 \\ & \mathbf{c}^T \mathbf{x} + b - f(\mathbf{x}) \geq 0 \\ & \mathbf{x} \in X \end{aligned}$$

对于参数多项式优化问题(2),本文将采用以下两个步骤进行求解:

1) 约束条件化简。将式(2)中关于 $\mathbf{x}, a, b, \mathbf{c}$ 的约束条件转换为等价的仅含参数 a, b, \mathbf{c} 的约束条件,即求解 $S(a, b, \mathbf{c})$ 使得

$$S(a, b, \mathbf{c}) \Leftrightarrow \begin{cases} f(\mathbf{x}) - \mathbf{c}^T \mathbf{x} - a \geq 0 \\ \mathbf{c}^T \mathbf{x} + b - f(\mathbf{x}) \geq 0 \\ \mathbf{x} \in X \end{cases}$$

2) 多项式优化问题求解。求解满足 $S(a, b, \mathbf{c})$ 条件,并使得 $(a - b)^2$ 最小的 a, b, \mathbf{c} 的值,即求解多项式约束问题:

$$\begin{aligned} \min & (a - b)^2 \\ \text{s. t. } & S(a, b, \mathbf{c}) \end{aligned}$$

下面将分别考虑这两个问题。对于步骤1),可应用半代数系统求解^[18]来实现约束条件化简。称如下系统

$$\begin{cases} p_1(\mathbf{u}, \mathbf{x}) = 0, p_2(\mathbf{u}, \mathbf{x}) = 0, \dots, p_s(\mathbf{u}, \mathbf{x}) = 0 \\ g_1(\mathbf{u}, \mathbf{x}) \geq 0, g_2(\mathbf{u}, \mathbf{x}) \geq 0, \dots, g_r(\mathbf{u}, \mathbf{x}) \geq 0 \\ g_{r+1}(\mathbf{u}, \mathbf{x}) > 0, g_{r+2}(\mathbf{u}, \mathbf{x}) > 0, \dots, g_t(\mathbf{u}, \mathbf{x}) > 0 \\ h_1(\mathbf{u}, \mathbf{x}) \neq 0, h_2(\mathbf{u}, \mathbf{x}) \neq 0, \dots, h_m(\mathbf{u}, \mathbf{x}) \neq 0 \end{cases}$$

为一个半代数系统,也记为 $[F, N, P, H]$, 其中 F, N, P, H 分别表示 $[p_1, p_2, \dots, p_s]$, $[g_1, g_2, \dots, g_r]$, $[g_{r+1}, g_{r+2}, \dots, g_t]$, $[h_1, h_2, \dots, h_m]$ 。

这里,向量 $\mathbf{x} = (x_1, x_2, \dots, x_n)^T \in \mathbf{R}^n$ 为变量,向量 $\mathbf{u} = (u_1, u_2, \dots, u_d)^T \in \mathbf{R}^d$ 为参数, $p_i, g_j, h_k \in \mathbf{R}[\mathbf{u}, \mathbf{x}]$ 且 $n, s \geq 1, d, r, t, m \geq 0$ 。对于半代数系统求解问题可运用 Maple 软件包 DISCOVERER^[19] 或 Regularchains 来实现。那么,问题(2)的约束条件可等价于半代数系统

$$\begin{cases} f(\mathbf{x}) - \mathbf{c}^T \mathbf{x} - a < 0 \\ \mathbf{c}^T \mathbf{x} + b - f(\mathbf{x}) < 0 \\ \mathbf{x} \in X \end{cases}$$

无解,应用 DISCOVERER 即可得到关于参数 a, b, c 的约束条件 $S(a, b, c)$ 。

例2 已知 $F = [ax^2 + bx + c], N = [], P = [], H = []$, 若求 a, b, c 使得半代数系统 $[F, N, P, H]$ 无解,那么在 Maple15 中键入以下命令:

```
> with(RegularChains);
> with(ParametricSystemTools);
> with(SemiAlgebraicSetTools);
> infolevel[RegularChains] := 1;
> R := PolynomialRing([x, a, b, c]);
> F := [a * x^2 + b * x + c]; N := []; P := []; H := [];
> rrc := RealRootClassification(F, N, P, H, 3, 0, R);
```

则得到结果 $b^2 - 4ac < 0$ 。具体实现可参见 Maple15 中的帮助工具。

此外,也可应用量词消去^[20] 计算 $S(a, b, c)$ 。量词消去运算是计算如下的一个量词公式 θ :

$$\theta = (Q_1 x_1 Q_2 x_2 \dots Q_t x_t) \sigma(F_1, F_2, \dots, F_t),$$

其中:向量 $\mathbf{x} = (x_1, x_2, \dots, x_n)^T \in \mathbf{R}^n$ 是变量,向量 $\mathbf{u} = (u_1, u_2, \dots, u_m)^T \in \mathbf{R}^m$ 是参数;对 $i = 1, 2, \dots, s, Q_i \in \{\forall, \exists\}$ 为量词;对 $j = 1, 2, \dots, t, F_j$ 为式子 $f_j(\mathbf{x}, \mathbf{u}) \sim_j 0$, 其中 $f_j(\mathbf{x}, \mathbf{u}) \in \mathbf{R}[\mathbf{x}, \mathbf{u}]$ 并且 $\sim_j \in \{=, >, \geq, \neq\}$, $\sigma(F_1, F_2, \dots, F_t)$ 是一个关于 F_1, F_2, \dots, F_t 的布尔运算组合的无量词公式,即 $\sigma(F_1, F_2, \dots, F_t) = F_1 \diamond_1 F_2 \diamond_2 \dots F_{t-1} \diamond_{t-1} F_t$, 其中 $\diamond_k \in \{\wedge, \vee, \neg, \dots, \Rightarrow\}$ ($k = 1, 2, \dots, t-1$)。

目前,量词消去工具主要有 QEPCAD^[21]、REDLOG^[22] 等。对量词公式进行量词消去即可得到一个等价的无量词公式。因此,针对问题(2)中的约束条件,运用量词消去也可得到一个等价的仅含有参数 a, b, c 的约束条件 $S(a, b, c)$ 。

例3 对如下量词公式:

$$\forall x [(1 \leq x \leq 5) \Rightarrow (6x - x^2 - ax - b \geq 0 \wedge ax + c - 6x + x^2 \geq 0)] \quad (3)$$

使用 QEPCAD 进行量词消去,依次键入以下命令:

```
Enter an informal description between '[' and ']':
[solve]
Enter a variable list:
(a,b,c,x)
Enter the number of free variables:
3
Enter aprenex formula:
(Ax) [[1 <= x/\x <= 5] == >
[6x - x^2 - ax - c <= 0/\ax + b - 6x + x^2 <= 0]]
```

则可得到下列与式(3)等价的无量词公式

$$\begin{cases} b + a - 5 \leq 0, \\ b + 5a - 5 \leq 0, \\ c + a - 5 \geq 0, \\ c + 5a - 5 \geq 0, \\ a - 4 > 0 \vee a + 4 < 0 \vee 4c - a^2 + 12a - 36 \geq 0 \end{cases} \quad (4)$$

如上所述,采用半代数系统求解或量词消去对问题(2)

中的约束条件进行化简,都可得到等价的仅含参数 a, b, c 的约束条件 $S(a, b, c)$ 。假设所求得 $S(a, b, c)$ 为

$$S(a, b, c) = (g_1(a, b, c) \sim_1 0 \wedge g_2(a, b, c) \sim_2 0 \wedge \dots \wedge g_r(a, b, c) \sim_r 0)$$

其中: $\sim_i \in \{=, >, \geq, \neq\}$ ($i = 1, 2, \dots, r$)。接下来,本文将构造如下的非线性优化问题:

$$\begin{aligned} \min (a - b)^2; & g_1(a, b, c) \sim_1 0, \\ & g_2(a, b, c) \sim_2 0, \dots, g_r(a, b, c) \sim_r 0 \end{aligned} \quad (5)$$

对于非线性优化问题(5),可应用 Matlab、Lingo 等工具进行有效求解。若 $g_i(a, b, c)$ 为多个多项式不等式的析取时,则需对其中各个不等式逐一考虑。

综上,对于给定的多项式混成系统 $H = (\mathbf{x}, L, flow, Init, Inv, E, G, R)$,本文应用半代数系统求解或量词消去与非线性优化方法相结合计算最小多面体包含对 H 中的非线性组件,如 $Init, Inv, G$ 等进行线性近似,从而得到近似的线性混成系统 H' 。显然, $H < H'$ 。

2.2 SpaceEx 验证

本文将运用验证工具 SpaceEx 对所构造的线性混成系统 H' 进行可达性分析。SpaceEx 适用于连续动态行为用线性不确定微分方程描述的混成系统,采用多面体和支撑函数相结合来表示状态集,并运用不动点算法来计算过近似可达集,从而实现系统的可达性分析,以及验证系统状态所应满足的性质。

因此,对于线性混成自动机 H' ,可采用 SpaceEx 计算 H' 的过近似可达集,记为 $Reach'(H')$ 。显然, $Reach'(H')$ 即为原非线性混成系统 H 的过近似可达集。因此,若给定不安全状态集 U ,可通过判断 $Reach'(H') \cap U$ 是否为空来验证 H 的安全性。然而,当 $Reach'(H') \cap U \neq \emptyset$ 时,则不能判定 H 的安全性。此时,需对系统状态进行细分,构造精度更高的线性混成系统来对非线性混成系统 H 进行线性近似,并进行重新验证。

2.3 构造算法

本节将给出一个验证算法,用于非线性混成系统可达性分析以及安全性验证。

算法 可达性分析及安全性验证。

输入 H : 非线性混成系统; U : 不安全集。

输出 $Reach'$: 过近似可达集;“安全或未知”:系统是否安全。

1) 构造线性混成系统 H' : 对于非线性混成系统 H 中的多项式项,如 $flow, Init, Inv, G, R$ 等,分别运用多面体包含方法进行线性近似。

① 假设最小多面体包含为 $[\mathbf{c}^T \mathbf{x} + a, \mathbf{c}^T \mathbf{x} + b], \mathbf{c} \in \mathbf{R}^n, a, b \in \mathbf{R}$,构造参数多项式优化问题(2)。

② 对问题(2)中的约束条件运用半代数系统求解或量词消去进行求解,从而得到一个等价的无量词公式 $S(a, b, c)$ 。

③ 计算多项式优化问题(5),求得 a, b, c 的值。

2) 运用 SpaceEx 计算线性混成系统 H' 的过近似可达集 $Reach'(H')$ 。

3) 判断 $Reach'(H')$ 与不安全集 U 的交集 $Reach'(H') \cap U$ 是否为空;若交集为空,则返回安全;否则,返回未知。

3 实例

下面,本文将通过几个实例来阐明如何运用本文中的算法对非线性混成系统进行可达性分析及安全性验证。

例4^[23] 考虑如下动力系统:

$$f(x, y, t) = \begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{t} \end{pmatrix} = \begin{pmatrix} -5.5y + y^2 \\ 6x - x^2 \\ 1 \end{pmatrix}$$

设初始集为 $Init = \{(x, y, t) \mid 4 \leq x \leq 4.5, y = 1, t = 0\}$

不变集为 $Inv = \{(x, y, t) \mid x \in [1, 5], y \in [1, 5], t \in [0, 4]\}$ 。

试计算该系统的可达集,并验证系统是否会到达不安全集 $U = \{(x, y, t) \mid 1 \leq x < 2, 2 < y < 3, 2 \leq t \leq 4\}$ 。

首先运用多面体包含对 \dot{x} 进行线性近似,假设最小多面体包含为 $[cy + a, cy + b]$, $a, b, c \in \mathbf{R}$ 。

求如下参数多项式优化问题:

$$\min (b - a)^2 \quad (6)$$

$$\text{s. t.} \quad -5.5y + y^2 - cy - a \geq 0$$

$$cy + b + 5.5y - y^2 \geq 0$$

$$1 \leq y \leq 5$$

首先,对式(6)中的约束条件运用 QEPCAD 进行量词消去,可得如下一组等价的约束条件:

$$S(a, b, c) = \begin{cases} 2a + 2c + 9 \leq 0, \\ 2a + 10c + 5 \leq 0 \\ 2b + 2c + 9 \geq 0 \\ 2b + 10c + 5 \geq 0 \\ 2c - 9 > 0 \vee 2c + 7 < 0 \vee \\ 4c^2 + 44c + 16a + 121 \leq 0 \end{cases} \quad (7)$$

然后求解非线性优化问题:

$$\min (b - a)^2 \quad (8)$$

$$\text{s. t.} \quad S(a, b, c)$$

可以得到 $a = -9, b = -5, c = 0.5$ 。因此, \dot{x} 的最小多面体包含为 $[0.5y - 9, 0.5y - 5], y \in [1, 5]$ 。同样,对于 y ,可求得其最小多面体包含为 $5 \leq \dot{y} \leq 9$ 。

这样,使用本文方法可得到系统 $f(x, y, t)$ 的近似线性系统

$$f'(x, y, t) = \begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{t} \end{pmatrix} = \begin{pmatrix} [0.5y - 9, 0.5y - 5] \\ [5, 9] \\ 1 \end{pmatrix}$$

然后,应用 SpaceEx 可计算得 f' 的过近似可达集 $Reach'$,如图2所示。显然, $Reach' \cap U = \emptyset$ 。因此,则原非线性系统是安全的。

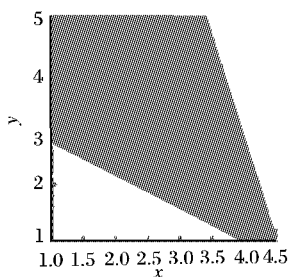


图2 例4 过近似可达集

例5 考虑如图3所示的混成系统,其中

$$f_1(x) = \begin{pmatrix} 1 - 0.83 - 0.34x + 0.01x^2 \\ 0.75 + 0.34x - 0.01x^2 - 1.71y + 0.82y^2 \end{pmatrix}$$

$$f_2(x) = \begin{pmatrix} -0.46 + 0.33y + 0.01x^2 - 0.03xy + 0.01y^2 \\ 1.01 - 0.33y - 0.01x^2 + 0.03xy - 0.62y + 0.06y^2 \end{pmatrix}$$

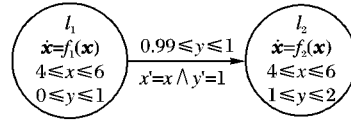


图3 混成系统例5

系统起始位置为 l_1 , 初始状态集为

$$Init = \{(x, y) \in \mathbf{R}^2 : (x - 5.5)^2 + (y - 0.25)^2 \leq 0.0625\}$$

试计算该混成系统的可达集,并验证系统是否会到达不安全状态集

$$U(l_1) = \{(x, y) \in \mathbf{R}^2 :$$

$$(x - 4.25)^2 + (y - 0.25)^2 \leq 0.0625\}$$

运用2.3节中的验证算法分别对 $Init, U(l_1), f_1(x), f_2(x)$ 计算最小多面体包含,可以得到:

$$Init' = \{(x, y) \in \mathbf{R}^2 : 5.25 \leq x \leq 5.75, 0 \leq y \leq 0.5\}$$

$$U'(l_1) = \{(x, y) \in \mathbf{R}^2 : 4 \leq x \leq 4.5, 0 \leq y \leq 0.5\},$$

$$f_1'(x) =$$

$$\begin{pmatrix} [-0.22x - 0.11, -0.22x - 0.10] \\ [0.23x - 0.89y + 0.82, 0.23x - 0.89y + 1.02] \end{pmatrix}$$

$$f_2'(x) =$$

$$\begin{pmatrix} [0.08x + 0.21y - 0.54, 0.08x + 0.21y - 0.49] \\ [-0.08x - 0.68y + 0.95, -0.08x - 0.68y + 1.02] \end{pmatrix}$$

对于相应的近似线性混成系统 H' , 运用 SpaceEx 可计算得 H' 的近似可达集 $Reach'(H')$, 如图4所示。显然, $R'(H') \cap U'(l_1) = \emptyset$ 。因此,原非线性混成系统是安全的。

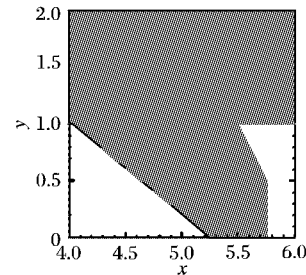


图4 例5 近似可达集

4 结语

基于多面体包含线性近似方法,本文讨论了一类非线性混成系统的可达性问题,并进一步考虑了系统的安全性验证。提出了运用多面体包含来对非线性混成系统进行线性近似,采用半代数系统求解或量词消去与非线性优化方法相结合来构造相应的线性混成系统,然后运用验证工具 SpaceEx 计算原非线性混成系统的过近似可达集,并应用于验证系统的安全性。

参考文献:

- [1] KOPKE P, HENZINGER T A, PURL, A, et al. What's decidable about hybrid automata?[J]. Journal of Computer and System Sciences, 1995, 57(1): 94 - 124.
- [2] LAFFERRIERE G, PAPPAS G, YOVINE S. A new class of decidable hybrid systems[C]// Hybrid Systems: Computation and Control, LNCS 1569. Berlin: Springer, 1999: 137 - 151.
- [3] ZHANG H B, DUAN Z H. Symbolic algorithmic analysis of rectangular hybrid systems[J]. Journal of Computer Science and Technology, 2009, 24(3): 531 - 543.
- [4] HARTMANN A, HERMANN H. A modest approach to checking probabilistic timed automata[C]// Proceedings of the 6th International Conference on Quantitative Evaluation of Systems. Washington, DC: IEEE Computer Society, 2009: 187 - 196.

- [5] COLLINS P. Continuity and computability of reachable sets [J]. Theoretical Computer Science, 2005, 341(1): 162 – 195.
- [6] ASARIN E, BOURNEZ O, DANG T, *et al.* Approximate reachability analysis of piecewise linear dynamical systems[C]// Hybrid Systems: Computation and Control, LNCS 1790. London: Springer, 2000: 21 – 31.
- [7] KURZHANSKIY A, VARAIYA P. Ellipsoidal techniques for reachability analysis of discrete-time linear systems[J]. IEEE Transactions on Automatic Control, 2007, 52(1): 26 – 38.
- [8] THOMAS S, ASHISH T. Verification and synthesis using real quantifier elimination[C]// The 36th International Symposium on Symbolic and Algebraic Computation. New York: ACM, 2011: 329 – 336.
- [9] COLAS L G, ANTOINE G. Reachability analysis of hybrid systems using support functions[C]// Proceedings of the 21th International Conference on Computer Aided Verification, LNCS 5643. Berlin: Springer, 2009: 540 – 554.
- [10] FREHSE G. PHAVer: algorithmic verification of hybrid systems past HyTech[J]. International Journal on Software Tools for Technology Transfer, 2008, 10(3): 263 – 279.
- [11] SILVA B, RICHESON K, KROGH B, *et al.* Modeling and verifying hybrid dynamic systems using CheckMate[C]// Proceedings of the 4th International Conference on Automation of Mixed Processes. Dortmund: Shaker, 2000: 323 – 328.
- [12] FREHSE G, GUERNIC C L, DONZE A, *et al.* SpaceEx: Scalable verification of hybrid systems[C]// Proceedings of the 23th International Conference on Computer Aided Verification, LNCS 6806. Berlin: Springer, 2011: 379 – 395.
- [13] EUGENE A, THAO D, ODED M. The d/dt tool for verification of hybrid systems[C]// Proceedings of the 14th International Conference on Computer Aided Verification, LNCS 2404. Berlin: Springer, 2002: 365 – 370.
- [14] EUGENE A, THAO D, ANTOINE G. Reachability analysis of nonlinear systems using conservative approximation[C]// Proceedings of the 6th ACM International Conference on Hybrid Systems: Computation and Control. New York: ACM, 2003: 20 – 35.
- [15] ASARIN E, DANG T, GIRARD A. Hybridization methods for the analysis of nonlinear systems[J]. Acta Informatica, 2007, 43(7): 451 – 476.
- [16] DANG T, MALER O, TESTYLER R. Accurate hybridization of nonlinear systems[C]// Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control. New York: ACM, 2010: 11 – 20.
- [17] HENZINGER T A, WONG-TOI H. Linear phase-portrait approximations for nonlinear hybrid systems[C]// Hybrid Systems III: Verification and Control, LNCS 1066. Berlin: Springer, 1996: 377 – 388.
- [18] YANG L, ZHOU C, ZHAN N, *et al.* Recent advances in program verification through computer algebra[J]. Frontiers of Computer Science in China, 2010, 4(1): 1 – 16.
- [19] XIA B. DISCOVERER: A tool for solving semi-algebraic systems[J]. ACM Communications in Computer Algebra, 2007, 41(3): 102 – 103.
- [20] HONG H, EI DIN M S. Variant real quantifier elimination: algorithm and application[C]// Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation. New York: ACM, 2009: 183 – 190.
- [21] BROWN C W. QEPCAD B – a program for computing with semi-algebraic sets using CADs[J]. ACM SIGSAM Bulletin, 2003, 37(4): 97 – 108.
- [22] STURM T. REDLOG online resources for applied quantifier elimination[J]. Acta Academiae Aboensis, 2007, 67(2): 177 – 191.
- [23] RATSCHAN S, SHE Z. Safety verification of hybrid systems by constraint propagation-based abstraction refinement[J]. ACM Transactions on Embedded Computing Systems, 2007, 6(1): Article No. 8.

(上接第 1284 页)

4 结语

提高 MIMO 建模效果的关键在于有效利用输出端之间蕴含的背景知识,而这需要对输出端之间的依赖关系进行有效的界定和建模。而直接采用回归分析建模,无法有效描绘输出端参数的真实关系。本文假设 MIMO 输出端的模型参数位于一个流形之上,在现有的 M-SVR 的基础上,构建了基于流形正则化的 MIMO 算法,并采用主曲线作为低维流形的表示,计算各输出端参数到该流形的投影距离,最终采用交替优化的方法,优化得到最优模型参数,并在仿真数据和圆柱壳振动数据集验证了该算法的有效性。该方法的特点主要是构建了流形正则化的优化目标,因此也适用于其他形式的 MIMO SVM 算法。

参考文献:

- [1] 周欣然,滕召胜,赵新闻. 基于 LSSVM 的 MIMO 系统快速在线辨识方法[J]. 计算机应用, 2009, 29(8): 2281 – 2284.
- [2] SÁNCHEZ-FERNÁNDEZ M, DE-PRADO-CUPLIDO M, ARENAS-GARCÍA J, *et al.* SVM multiregression for nonlinear channel estimation in multiple-input multiple-output systems[J]. IEEE Transactions on Signal Processing, 2004, 52(8): 2298 – 2307.
- [3] VAPNIK V N. The nature of statistical learning theory[M]. New York: Springer, 1995.
- [4] MAO W T, TIAN M, YAN G R. Research of load identification based on multiple-input multiple-output SVM model selection[J]. Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineers Science, 2012, 226(5): 1395 – 1409.
- [5] 李建伟,汪友华,吴清. 基于多维输出支持向量回归机的脑电源定位[J]. 中国组织工程研究与临床康复, 2009, 13(17): 3256 – 3259.
- [6] 张军平,王珏. 主曲线研究综述[J]. 计算机学报, 2003, 26(2): 129 – 146.
- [7] KÉGL B, KRZYŻAK A, LINDER T, *et al.* Learning and design of principal curves[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2000, 22(3): 281 – 297.
- [8] 齐红威,张军平,王珏. 主曲线异常检测及其在股票市场中的应用[J]. 计算机研究与发展, 2005, 42(8): 1306 – 1311.
- [9] CAWLEY G C, TALBOT N L C. Preventing over-fitting during model selection via Bayesian regularisation of the hyper-parameters[J]. Journal of Machine Learning Research, 2007, 8: 841 – 861.
- [10] 毛文涛. 支持向量回归机模型选择研究及在综合力学环境预示中的应用[D]. 西安: 西安交通大学, 2011.