软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2016,27(3):645−654 [doi: 10.13328/j.cnki.jos.004986]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

运用栅栏函数验证连续系统的有界时间安全性*

甘 庭, 夏壁灿

(北京大学 数学科学学院,北京 100871)

通讯作者: 甘庭, E-mail: gant@pku.edu.cn, xbc@math.pku.edu.cn

摘 要: 栅栏函数在连续系统验证方面有着广泛的应用,其主要想法在于:在可达集和非安全集之间寻找一个栅栏,从初始区域出发的路径不会越过这个栅栏,而非安全区域在栅栏的另外一端.这样,就可以通过寻找栅栏函数来验证一个系统的安全性.近年来,已有一些工作讨论连续系统在无界时间情况下的栅栏函数生成.但是对于有些系统,人们可能只关心其在有界时间内的安全性.因为在无界时间内不安全并不能说明在给定时间内也是不安全的,所以对于这类问题,无界时间栅栏函数方法并不适用.受无界时间栅栏函数方法的启发,针对有界时间的情况,给出有界时间栅栏函数生成方法.首先给出有界时间栅栏函数的一些充分条件,对于多项式系统,将多项式非负的条件做平方和松弛后利用平方和规划工具求解这些充分条件得到栅栏函数;对于初等系统(包含一些初等函数),先将该初等系统转化为一个多项式系统,然后求解对应多项式系统的栅栏函数.对一些无界时间不安全的实例,演示了该方法在验证有界时间安全性问题上的有效性.

关键词: 连续系统;安全性验证;栅栏函数;半定规划;平方和

中图法分类号: TP301

中文引用格式: 甘庭,夏壁灿.运用栅栏函数验证连续系统的有界时间安全性.软件学报,2016,27(3):645−654. http://www.jos.org.cn/1000-9825/4986.htm

英文引用格式: Gan T, Xia BC. Barrier certificate generation for safety verification of continuous systems for a bounded time. Ruan Jian Xue Bao/Journal of Software, 2016,27(3):645−654 (in Chinese). http://www.jos.org.cn/1000-9825/4986.htm

Barrier Certificate Generation for Safety Verification of Continuous Systems for a Bounded Time

GAN Ting, XIA Bi-Can

(School of Mathematical Sciences, Peking University, Beijing 100871, China)

Abstract: Barrier certificates have been widely used in verification of continuous systems. The main idea is to find a barrier which separates the reachable set from the unsafe set such that all the trajectories starting from the initial set will never go across the barrier. Thus the system's safety can be guaranteed by constructing a barrier. In recent years, barrier certificates have been successfully used for verification of continuous systems with unbounded time. However sometimes the safety for bounded time needs to be addressed. Since a system is unsafe with unbounded time cannot imply it is also unsafe with a bounded time, the unbounded time barrier certificate method could fail to verify the safety with bounded time. In this paper, a method is presented to generate a bounded time barrier certificate for safety verification of continuous systems with bounded time. Some sufficient conditions for the bounded time barrier certificate are specified. If the continuous system is a polynomial system, relax all the conditions of positive semi-definite polynomial to the sum of squares (SOS) polynomial and then use semi-definite programming (SDP) to solve the conditions for a bounded time barrier certificate; if the continuous system is an elementary system (containing some elementary functions), transform it to a polynomial system

* 基金项目: 国家自然科学基金(11271034, 11290141)
Foundation item: National Natural Science Foundation of China (11271034, 11290141)
收稿时间: 2015-07-16; 修改时间: 2015-10-20; 采用时间: 2015-11-27; jos 在线出版时间: 2016-01-05
CNKI 网络优先出版: 2016-01-05 16:40:00, http://www.cnki.net/kcms/detail/11.2560.TP.20160105.1640.012.html

approximately, and then solve the corresponding polynomial system for a bounded time barrier certificate. For some practical examples which are unsafe for unbounded time, the paper shows the effectiveness of the proposed method for generating bounded time barriers.

Key words: continuous system; safety verification; barrier certificate; SDP (semi-definite programming); SOS (sum of squares)

嵌入式系统是一种完全嵌入到受控制器件的内部,为该器件的某一特定应用而设计的专用计算机系统.近几年,随着计算机、互联网和通信技术的不断发展,嵌入式系统也不断地应用到社会的各个领域,比如工业控制中的数字机床、过程控制、电网设备监控,环境工程中的防洪体系、地震监测网、实时气象信息网以及和人们日常生活息息相关的交通系统、智能家电等等,甚至在国防和航天方面,嵌入式系统也有着广泛的应用.一般由计算机程序和物理设备交互作用形成的嵌入式系统被广泛地称为混成系统.由于嵌入式系统的广泛应用以及特殊行业的严格要求,对混成系统的研究成为一个重要而又复杂的课题.

混成系统的建模一般会包含多个连续系统[1−8],在某些连续系统之间会有一些离散的跳转.目前,对混成系统的研究工作主要还是着重于对其中连续系统的研究,然后结合这些连续系统的性质和离散跳转的条件,得到该混成系统的性质.大部分已有的对混成系统研究的工作[9−12]本质上也只是在于对连续系统的研究.

混成系统安全性验证或连续系统的安全性验证是指,验证该系统从给定的初始区域出发沿着给定的向量场且不会经过指定的非安全区域.一个简单而直接的想法是:寻找一个栅栏(barrier),系统可以达到的区域和非安全区域分别位于该栅栏的两侧,也就是从初始区域出发的轨迹不会越过这个栅栏而非安全区域在栅栏的另一侧.这种方法被称为栅栏函数法,即,通过寻找一个栅栏函数来证明系统的安全性.文献[13]首先提出利用栅栏函数来证明系统的安全性,并提出栅栏函数的充分条件.文献[14,15]推广了文献[13]中栅栏函数的条件,给出更为一般的栅栏函数的条件.文献[4]进一步推广了文献[14,15]的栅栏函数条件,给出了栅栏函数的一类条件.这些栅栏函数的条件都是在考虑时间无界的情况,也就是在证明时间无界情况下系统的安全性.

在某些情况下,人们只关心系统在某一个给定时间$[0,T]$内的安全性.当然,如果用无界时间栅栏函数方法可以找到栅栏函数,系统在此给定时间$[0,T]$内的安全性自然也得到了验证.然而很多情况并非如此,即,在有界时间内安全的系统并不一定会在无界时间情况下也安全.这一点也是很容易理解的.那么这个时候,用无界时间栅栏函数方法来验证有界时间的安全性必然不会奏效.

受文献[13−16]的启发,本文改进了栅栏函数的条件,给出了有界时间栅栏函数的生成方法,从而验证连续系统在有界时间内的安全性.我们首先给出有界时间栅栏函数的一些充分条件.对于多项式系统,将多项式非负条件做平方和松弛后利用平方和规划工具求解这些充分条件得到栅栏函数;对于初等系统(包含一些初等函数),先将该初等系统转化为一个多项式系统,然后求解对应多项式系统的栅栏函数.后文中将看到:文献[14,15]中针对时间无界情况下的栅栏函数条件实际上是本文中时间$[0,T]$内栅栏函数的特例,这是因为在时间界 $T\to+\infty$时,本文的有界时间栅栏函数条件就退化成文献[14,15]中所给出的条件.

本文的主要工作包括:给出有界时间栅栏函数的充分条件;对多项式系统和初等系统给出求解栅栏函数的方法.

本文第 1 节给出一些基本概念和应考虑的问题.第 2 节提出有界时间栅栏函数的条件以及组合栅栏函数的条件.第 3 节针对多项式系统给出求解栅栏函数的方法并推广到初等系统的情况.第 4 节对全文做总结.

1 预备知识

首先介绍一些基本概念,然后阐明本文希望解决的问题.后文中,$\mathbb{R}$代表实数集,$x=(x_1,\ldots,x_n)^T$代表变量.

1.1 基本概念

自治的连续动力系统通常由如下常微分方程表示:

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

其中,$f(x)=(f_1(x),\ldots,f_n(x))^T$是向量函数,一般称 $f(x)$为向量场.本文要求 f 的每个分量都是解析函数,因此该常微分方程满足局部 Lipschitz 条件.在实际情况下,对一个连续动力系统,常常关心在给定初始区域和非安全区域时,

该连续系统是否可以从初始区域出发到达非安全区域.下面将扩展连续动力系统的定义,并在下一节中描述本文试图解决的问题.

定义 1(扩展连续系统).扩展连续系统是四元组$(f(x),D,I,U)$,其中$f(x)$是 n 维向量函数;$D\subseteq\mathbb{R}^n$ 是可行域(domain)表示该系统只在该区域内考虑,$I,U\subset D$ 是两个不相交的子集,I 表示初始区域,U 表示非安全区域.

一般 D 指的是系统考虑的范围,在可行域 D 之外的部分是不予考虑的.如果系统从初始区域出发,在某一时刻越过了可行域的边界达到 D 之外的区域,则从此刻起,系统的一切演化都是不予考虑的,即,只关心系统在跳出可行域 D 之前的轨迹.如果对 D 没有特殊的说明,则视 D 为全空间$\mathbb{R}^n$.

定义 2(可达集). 给定扩展连续系统$(f(x),D,I,U)$,在 t 时刻的可达集定义为

$$\mathcal{R}_t:=\{x(t)\in D\mid \dot{x}=f(x)\wedge x(0)\in I\wedge\forall 0\leqslant\tau\leqslant t,x(\tau)\in D\} \tag{2}$$

在一段时间$[0,T]$,$0<T\leqslant+\infty$的可达集定义为

$$\mathcal{R}_{(0,T)}:=\bigcup_{0\leqslant t\leqslant T}\mathcal{R}_t \tag{3}$$

定义 3(T-栅栏函数). 给定扩展连续系统$(f(x),D,I,U)$和时间界 $0<T<+\infty$.如果存在有限个函数$\phi_1,\ldots,\phi_k:\mathbb{R}^n\to\mathbb{R}$满足下面两个条件:

$$\forall x\in\mathcal{R}_{(0,T)},\wedge_{i=1}^{k}\phi_i(x)\geqslant 0 \tag{4}$$

$$\forall x\in U,\vee_{i=1}^{k}\phi_i(x)\geqslant 0 \tag{5}$$

则称$(\phi_1,\ldots,\phi_k)$是组合 T-栅栏函数.特别地,当 $k=1$ 时,称为 T-栅栏函数.

1.2 问题描述

对给定的扩展连续系统$(f(x),D,I,U)$,假设其在给定时间$[0,T]$内是安全的,也就是说,该系统从初始区域 I 出发,在时间$[0,T]$内不会经过非安全区域 U,即$\mathcal{R}_{(0,T)}\cap U$ 是空集.

由 T-栅栏函数的定义可以看到:如果能够找到系统$(f(x),D,I,U)$的 T-栅栏函数,即$\mathcal{R}_{(0,T)}\cap U=\varnothing$,也就证明了该系统在时间$[0,T]$内是安全的.

本文考虑在给定系统$(f(x),D,I,U)$和时间界 T 时,如何生成该系统的 T-栅栏函数,从而验证系统在时间$[0,T]$内的安全性.

2 有界时间栅栏函数条件

从上一节可以看到,T-栅栏函数可以把指定时间内的可达集和非安全集分开.通常情况下,非安全集是已知的,但指定时间内的可达集却不是容易计算的.即使是在线性情况下,可达集的计算也是不可判定的.因此,一个函数是否是栅栏函数,往往不能通过其定义来直接判断.本节将给出 T-栅栏函数的一个充分条件.

引理 1. 对于一阶连续可微的实函数$\theta(t):\mathbb{R}\to\mathbb{R}$,如果其满足下面微分方程:

$$\begin{cases}\dfrac{\mathrm{d}\theta}{\mathrm{d}t}-\lambda\theta(t)-\eta=0\\ \theta(0)\leqslant 0\end{cases},\lambda,\eta\in\mathbb{R},\lambda<0,\eta>0,$$

则$\forall 0\leqslant\xi\leqslant 1,\theta(\xi)<\eta$.

证明:令 $\beta=\dfrac{\eta}{\lambda},\theta_0=\theta(0)$,则$\beta<0,\theta_0\leqslant 0$.

$$\frac{\mathrm{d}\theta}{\mathrm{d}t}-\lambda\theta(t)-\eta=0\Rightarrow\frac{\mathrm{d}\theta}{\lambda\theta+\eta}=\mathrm{d}t\Rightarrow\frac{\mathrm{d}\theta}{\theta+\beta}=\lambda\mathrm{d}t\Rightarrow\theta(t)=\theta_0\mathrm{e}^{\lambda t}+\beta(\mathrm{e}^{\lambda t}-1).$$

当 $0<\xi\leqslant 1$,有$\lambda\xi<0$.因此,$\mathrm{e}^{\lambda\xi}>1+\lambda\xi$,即 $\mathrm{e}^{\lambda\xi}-1>\lambda\xi$.又因为$\beta<0$,从而$\beta(\mathrm{e}^{\lambda\xi}-1)<\beta\lambda\xi=\eta\xi\leqslant\eta$,所以$\beta(\mathrm{e}^{\lambda\xi}-1)<\eta$.

因为$\theta_0\mathrm{e}^{\lambda\xi}\leqslant 0$,从而不难发现:$\forall 0\leqslant\xi\leqslant 1,\theta(\xi)<\eta$. □

利用引理 1,可以得到下面关于 T-栅栏函数的定理 1.

定理 1. 给定扩展连续系统$(f(x),D,I,U)$,如果存在两个实数$\lambda<0,\eta>0$ 和一阶连续可微的实函数

$\varphi(x):\mathbb{R}^n\to\mathbb{R}$满足下面 3 个条件:

$$\forall x\in I:\varphi(x)\leqslant 0 \tag{6}$$

$$\forall x\in D:\mathcal{L}_f\varphi(x)-\lambda\varphi(x)-\eta\leqslant 0 \tag{7}$$

$$\forall x\in U:\varphi(x)\geqslant \eta \tag{8}$$

其中,$\mathcal{L}_f\varphi(x)$是函数$\varphi(x)$关于向量场 f 的李导数.那么,在 $t\in[0,1]$时间内,扩展连续系统$(f(x),D,I,U)$是安全的,并且$\varphi(x)-\eta$是 T=1 时的 T-栅栏函数.

证明:假设存在$\lambda,\eta,\varphi(x)$满足定理 1 中的条件,由公式(7),有:

$$\mathcal{L}_f\varphi-\lambda\varphi-\eta\leqslant 0.$$

又因为 $\dfrac{\partial\varphi(x(t))}{\partial t}=\dfrac{\partial\varphi}{\partial x}\dfrac{\partial x}{\partial t}=\dfrac{\partial\varphi}{\partial x}f(x)=\mathcal{L}_f\varphi$,从而有:

$$\frac{\partial\varphi}{\partial t}-\lambda\varphi-\eta\leqslant 0 \tag{9}$$

设$\theta:\mathbb{R}\to\mathbb{R}$是一阶连续可微函数,满足$\theta(0)=\varphi(0)=\varphi_0\leqslant 0$,并且

$$\frac{\partial\theta}{\partial t}-\lambda\theta-\eta=0 \tag{10}$$

则由引理 1 可以得到:

$$\forall 0\leqslant t\leqslant 1,\theta(t)<\eta \tag{11}$$

由不等式(9)和等式(10),有:

$$\begin{cases}(\varphi-\theta)_0=\varphi(0)-\theta(0)=0\\ \dfrac{\partial(\varphi-\theta)}{\partial t}-\lambda(\varphi-\theta)\leqslant 0\end{cases} \tag{12}$$

因此,由文献[14]中的定理 1,有$\varphi-\theta\leqslant 0$.结合公式(11),有:

$$\forall 0\leqslant t\leqslant 1,\varphi(x(t))<\eta.$$

这意味着对任意 $t\in[0,1]$,连续系统能到达的点 x 都满足$\varphi(x)<\eta$.但是由条件(8)知道,非安全集里的点 x 都满足$\varphi(x)\geqslant\eta$,所以该系统是安全的.并且很容易看出:$\varphi(x)-\eta=0$ 将[0,1]上的可达集$\mathcal{R}_{(0,1)}$和非安全集 U 分离,所以$\varphi(x)-\eta$是 T=1 的 T-栅栏函数. □

推论 1. 在定理 1 中,将条件(7)更换为下面的条件(13),而其他条件不变:

$$\forall x\in D:\mathcal{L}_f\varphi(x)-\lambda\varphi(x)-\frac{\eta}{T}\leqslant 0 \tag{13}$$

其中,$0<T<+\infty$.则在 $t\in[0,T]$时间内,扩展连续系统$(f(x),D,I,U)$是安全的,并且$\varphi(x)-\eta$是一个 T-栅栏函数.

证明:令 $p=\dfrac{t}{T}$,用 p 取代 t 的位置来作为时间变量.条件(6)和条件(8)不会变化,因为它们和时间无关.考虑条件(13),此时:

$$\frac{\partial\varphi}{\partial p}=\frac{\partial\varphi}{\partial t}T.$$

所以,由条件(13)乘以 T 得到:

$$\forall x\in\mathbb{R}^n:\frac{\partial\varphi}{\partial p}-T\lambda\varphi(x)-\eta\leqslant 0.$$

视此条件为定理 1 中的条件(7),p 为定理 1 中的 t,$T\lambda$为定理 1 中的λ.由定理 1 有:在 $p\in[0,1]$时间内,扩展连续系统$(f(x),D,I,U)$是安全的,并且$\varphi(x)-\eta$是栅栏函数.即:在 $t\in[0,T]$时间内,扩展连续系统$(f(x),D,I,U)$是安全的,并且$\varphi(x)-\eta$是 T-栅栏函数.

可以看到:在时间界 $T\to+\infty$时,推论 1 中的条件(13)将变成:

$$\forall x\in D:\mathcal{L}_f\varphi(x)-\lambda\varphi(x)\leqslant 0.$$

而这个条件结合另外两个条件(6)和条件(8)正好就是文献[14,15]中无界时间栅栏函数的条件. □

定理 1 和推论 1 分别给出了在特定时间界[0,1]和一般时间界[0,T]下栅栏函数的条件.一般情况下,其中第 1 个和第 3 个条件是容易验证和满足的,但是第 2 个条件却不是很容易验证和满足.无论是定理 1 中还是推论 1 中,第 2 个条件要求 x 在 D 上都成立.第 2 个条件实际上是栅栏函数在向量场上的变化,可以想象,如果事先有对可达集$\mathcal{R}_{(0,T)}$的包含近似 $\boldsymbol{B}$,那么第 2 个条件就应该可以限制在 $\boldsymbol{B}$ 上.下面给出的定理将阐述这个事实.

定理 2. 给定扩展连续系统($f(x)$,D,I,U)和时间界 T,假设 $\boldsymbol{B}$ 是可达集$\mathcal{R}_{(0,T)}$的包含近似,即$\mathcal{R}_{(0,T)}\subseteq\boldsymbol{B}$.如果存在两个实数$\lambda<0$,$\eta>0$ 和一阶连续可微的实函数$\varphi(x):\mathbb{R}^n\to\mathbb{R}$满足下面 3 个条件:

$$\forall x\in I:\varphi(x)\leqslant 0 \tag{14}$$

$$\forall x\in \boldsymbol{B}\cap D:\mathcal{L}_f\varphi(x)-\lambda\varphi(x)-\frac{\eta}{T}\leqslant 0 \tag{15}$$

$$\forall x\in U\cap\boldsymbol{B}:\varphi(x)\geqslant\eta \tag{16}$$

则在 $t\in[0,T]$时间内,扩展连续系统($f(x)$,D,I,U)是安全的.

证明:任意取定 $x_0\in I$,令$\mathcal{T}(T)=\{x(t)|0\leqslant t\leqslant T\wedge x(0)=x_0\}$,则$\mathcal{T}(T)\subset B$.在$\mathcal{T}(T)$上考虑,有下式成立:

$$\begin{cases}\mathcal{L}_f\varphi(x(t))-\lambda\varphi(x(t))-\dfrac{\eta}{T}\leqslant 0\\ \varphi(x(0))=\varphi(x_0)\leqslant 0\end{cases}.$$

由定理 1 和推论 1 容易看到:对任意的$x\in\mathcal{T}(T)$,有$\varphi(x)<\eta$.由 x_0 的任意性有,对任意 $x\in\mathcal{R}_{(0,T)}$,都有$\varphi(x)<\eta$成立. □

从定理 2 可以看到,定理 1 和推论 1 中的第 2 个条件可以限制在可达集的包含近似上.事实上,从定理 1 和推论 1 的证明可以很容易得到可达集包含近似的条件.

命题 1. 给定扩展连续系统($f(x)$,D,I,U)和时间界 T.假设ψ是关于 x 的一阶连续可微函数,并且存在两个实数$\lambda_1<0$,$\eta_1>0$ 使得下面两个条件成立:

$$\forall x\in I:\psi(x)\leqslant 0 \tag{17}$$

$$\forall x\in D:\mathcal{L}_f\psi(x)-\lambda_1\psi(x)-\frac{\eta_1}{T}\leqslant 0 \tag{18}$$

则 $\boldsymbol{B}=\{x|\psi(x)-\eta_1\leqslant 0\}$是$\mathcal{R}_{(0,T)}$的一个包含近似,即$\mathcal{R}_{(0,T)}\subseteq\boldsymbol{B}$.

证明:由定理 1 和推论 1 的证明直接可得. □

命题 1 给出了可达集包含近似的条件,结合定理 2,很容易得到下面的结论:

定理 3. 给定扩展连续系统($f(x)$,D,I,U)和时间界 T.设ψ,φ是两个一阶连续可微的函数,并且存在$\lambda<0$,$\lambda_1<0$,$\eta>0$,$\eta_1>0$,使得条件(17)、条件(18)和条件(14)~条件(16)都成立.其中,$\boldsymbol{B}=\{x|\psi(x)-\eta_1\leqslant 0\}$.则在 $t\in[0,T]$时间内,扩展连续系统($f(x)$,D,I,U)是安全的,而且$(\varphi(x)-\eta,\psi(x)-\eta_1)$是组合 T-栅栏函数.

证明:直接由定理 2 和命题 1 可以得到. □

3 求解栅栏函数

在上一节中给出了栅栏函数的条件以及组合栅栏函数的条件,这一节视这些条件为栅栏函数的约束,然后提出方法来求解这些约束,从而得到栅栏函数.本节主要针对扩展连续系统($f(x)$,D,I,U)是多项式系统和初等系统两种情况进行讨论.

3.1 求解多项式系统的栅栏函数

定义 4(多项式系统). 给定扩展连续系统($f(x)$,D,I,U),如果 $f(x)$是多项式函数,并且存在有限个多项式$g_1(x),\ldots,g_r(x),h_1(x),\ldots,h_s(x),p_1(x),\ldots,p_q(x)$,使得 $I=\{x|g_1(x)\geqslant 0\wedge\ldots\wedge g_r(x)\geqslant 0\}$,$U=\{x|h_1(x)\geqslant 0\wedge\ldots\wedge h_s(x)\geqslant 0\}$,$D=\{x|p_1(x)\geqslant 0\wedge\ldots\wedge p_q(x)\geqslant 0\}$,则称该系统是多项式系统.

对于多项式系统($f(x)$,D,I,U)和给定时间界 T,下面将描述如何通过求解定理 1 中的条件得到栅栏函数,或通过求解定理 3 中的条件得到组合栅栏函数.其中,主要的想法在于松弛定理 1 或者定理 3 中的条件得到一些平

方和(SOS)约束[14−17],然后利用平方和规划工具 YALMIP**来求解[18,19].

定理 4. 给定如定义 4 中描述的多项式系统$(f(x),D,I,U)$和时间界 T.如果存在两个实数$\lambda<0,\eta>0$、一阶连续可微的实函数$\varphi(x)$和 SOS 多项式 $u_1,\ldots,u_r,w_1,\ldots,w_q,v_1,\ldots,v_s$ 使得下面 3 个多项式都是 SOS 多项式:

$$-\varphi-u_1g_1-\ldots-u_rg_r \tag{19}$$

$$-\mathcal{L}_f\varphi+\lambda\varphi+\frac{\eta}{T}-w_1p_1-\ldots-w_qp_q \tag{20}$$

$$\varphi-\eta-v_1h_1-\ldots-v_sh_s \tag{21}$$

则在 $t\in[0,T]$时间内,多项式系统$(f(x),D,I,U)$是安全的,并且$\varphi(x)-\eta$是 T-栅栏函数.

证明:事实上,这里的条件(19)~条件(21)分别是推论 1 中条件(6)、条件(13)、条件(8)的 SOS 松弛.即,这里的 3 个条件分别可以蕴含推论 1 中的相应条件.这里只证明条件(19)可以蕴含推论 1 中条件(6),其他两个类似.

假设这里的条件(19)成立,即 $u_1,\ldots,u_r$ 是 SOS,并且使得$-\varphi-u_1g_1-\ldots-u_rg_r$也是 SOS.任取 $x_0\in I$,则:

$$g_1(x_0)\geqslant 0\wedge\ldots\wedge g_r(x_0)\geqslant 0.$$

由 $u_1,\ldots,u_r$ 是 SOS 可知:

$$-u_1(x_0)g_1(x_0)-\ldots-u_r(x_0)g_r(x_0)\leqslant 0.$$

又因为$-\varphi-u_1g_1-\ldots-u_rg_r$也是 SOS,所以$-\varphi(x_0)\geqslant 0$.由 x_0 的任意性,则推论 1 中的条件(6)成立.

这样,由这里的条件(19)~条件(21),分别可以得到推论 1 中的条件(6)、条件(13)、条件(8).由推论 1 得知结论成立. □

类似地,定理 3 也有下面的松弛.

定理 5. 给定扩展连续系统$(f(x),D,I,U)$和时间界 T.如果存在$\lambda<0,\lambda_1<0,\eta>0,\eta_1>0$,两个多项式函数$\psi,\varphi$和 SOS 多项式 $u_1,\ldots,u_r,u_{r+1},\ldots,u_{2r_s},w_0,w_1,\ldots,w_q,w_{q+1},\ldots,w_{2q},v_1,\ldots,v_s$ 使得下面的 5 个多项式都是 SOS 多项式:

$$-\psi-u_1g_1-\ldots-u_rg_r \tag{22}$$

$$-\mathcal{L}_f\psi+\lambda_1\psi+\frac{\eta_1}{T}-w_1p_1-\ldots-w_qp_q \tag{23}$$

$$-\varphi-u_{r+1}g_1-\ldots-u_{2r}g_r \tag{24}$$

$$-\mathcal{L}_f\varphi+\lambda\varphi+\frac{\eta}{T}-w_{q+1}p_1-\ldots-w_{2q}p_r+w_0(\psi-\eta_1) \tag{25}$$

$$\varphi-\eta-v_1h_1-\ldots-v_sh_s \tag{26}$$

则在 $t\in[0,T]$时间内,多项式系统$(f(x),D,I,U)$是安全的,$(\varphi(x)-\eta,\psi(x)-\eta_1)$是组合 T-栅栏函数.

证明:利用定理 4 的证明方法,结合定理 3 可知结论成立. □

本文利用设置模板的方法来求解定理 4 和定理 5 中的约束.例如在定理 5 中,对多项式φ,ψ,u_i,v_j,w_k设置模板,比如设置φ是关于变量 x_1,x_2 的二次多项式模板,这样可以令 $\varphi=c_1x_1^2+c_2x_1x_2+c_3x_2^2+c_4x_1+c_5x_2+c_6$,其中,$c_1,\ldots,c_6$是待求解的实值参数,其他多项式也类似的设置模板.这样就只需要求解这些实值系数和$\lambda,\lambda_1,\eta,\eta_1$ 使得定理 5 中的所有条件得以满足.

可以看到,问题就转化成一个平方和规划求可行解的问题.目前,平方和规划问题的求解方法主要是将多项式是平方和的约束转化成相应的矩阵是半正定的约束,然后利用半定规划工具求解.本文利用 MATLAB 平台下的工具包 YALMIP 来求解,见文献[16].但是在设置模板之后,约束系统中公式(23)和公式(25)对于这些参数系统不是线性的,目前的平方和规划工具包都无法求解的,因此先设置λ和λ_1 的值,然后再求解.

对于定理 4 的求解也是类似.

例 1:考虑多项式系统$(f(x),I,U)$定义如下[13,14,20]:

** YALMIP 是 MATLAB 平台下的 SOS 规划求解器,它将平方和约束问题转化成半定规划问题,然后调用 MATLAB 下的半定规划求解器 STDP3 或 SeDuMi.

$$\begin{cases} f(x_1,x_2)=\left(x_2,-x_1+\dfrac{1}{3}x_1^3-x_2\right)^T \\ I=\{(x_1,x_2)\in\mathbb{R}^2\mid g=0.25-(x_1-1.5)^2-x_2^2\geqslant 0\} \\ U=\{(x_1,x_2)\in\mathbb{R}^2\mid h=0.16-x_1^2-x_2^2\geqslant 0\} \end{cases}'$$

其中,时间界 T=0.5.由于 D 没有说明,那么 $D=\mathbb{R}^n$ 表示全空间.

图 1 是该系统的向量场和可达集的示意图(右边圆盘是初始区域,左边圆盘是非安全区域,两条曲线之间部分是数值模拟的时间无界的可达集).可以看到:从右边圆盘表示的初始区域出发,最终会与左边圆盘表示的非安全区域相交,那么此时无界时间栅栏函数法必然失效.下面将通过求解定理 5 中的 5 个条件来得到组合 T-栅栏函数,从而验证该系统在给定时间范围[0,0.5]内的安全性.

- 首先考虑前两个条件:使得公式(22)和公式(23)是平方和.

已知 T=0.5,设定λ_1=−1,η=2,这样就只需求解多项式ψ和平方和多项式 u_1,使得下面两个多项式是平方和:

$$-\psi-u_1 g,\mathcal{L}_f\psi-\psi+4.$$

设置ψ为关于变量 x_1,x_2 的 2 次多项式,$u_1\geqslant 0$(正实数是特殊的 SOS 多项式),利用 YALMIP 软件包求解并保留到小数点后 4 位,得到解为

$$\psi=-1.0000x_1^2-1.8285x_1x_2-0.9317x_1+0.3245x_2-1.0907,$$
$$u_1=1.8293.$$

- 然后考虑后 3 个条件:使得公式(24)~公式(26)是平方和.

已知 T=0.5,设定λ=−0.1,η=0.2,这样就只需求解多项式ψ和平方和多项式 u_2,v_1,w_0,使得下面 3 个多项式是平方和:

$$-\varphi-u_2 g,-\mathcal{L}_f\varphi-0.1\psi+0.4+w_0(\psi-2),\varphi-0.2-v_1 h.$$

利用 YALMIP,设置ψ为 2 次,$u_2\geqslant 0,v_1\geqslant 0,w_0\geqslant 0$,并保留到小数点后 4 位,得到解为

$$\varphi=-0.1586x_1^2-0.2420x_1x_2-0.2629x_1+0.0131x_2+0.3623,$$
$$u_2=0.4740,w_0=0.0088,v_1=0.5180.$$

(φ−0.2,ψ−2)组成组合 T-栅栏函数,如图 2 所示.

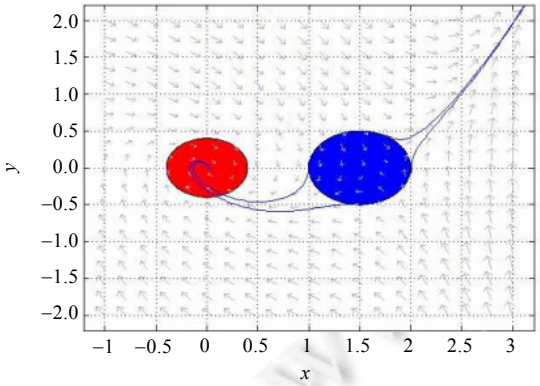

Fig.1

图 1

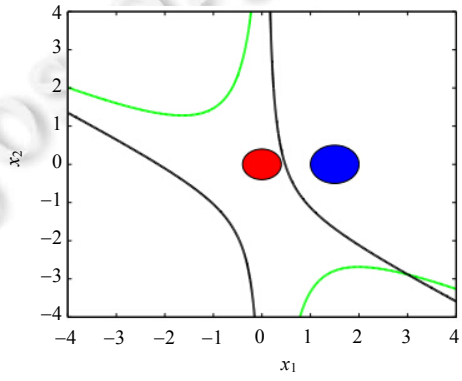

Fig.2

图 2

由于 YALMIP 工具是基于半定规划的数值求解工具,其得到的结果往往是在一定容忍度范围内的可行解.因此,由 YALMIP 求解出来的解只是一个近似解,是不可以完全相信的.为了确保得到结果的正确性,需要验证利用 YALMIP 工具求得的解确实是满足定理 5 中条件,即,多项式(22)~多项式(26)均为平方和多项式.注意到,本文的目的在于寻找栅栏函数.事实上很容易看出,只需要多项式(22)~多项式(26)全局非负即可.这样,需要验证的问题可以转化成验证多项式全局非负问题,即:

问题 1. 给定多项式 $f(x)\in\mathbb{R}[x]$,是否对任意的 $x\in\mathbb{R}^n$,都有 $f(x)\geqslant 0$ 成立?

目前已经有很多工作来讨论问题 1,这里利用文献[21]中基于改进柱形代数分解(CAD)的符号方法来判断一个多项式是否全局非负,即问题 1.文献[21]的作者将此方法实现成基于符号计算的工具 CADpsd,当输入多项式是全局非负时,其返回'True',否则返回'False'.

将上述 $\lambda,\lambda_1,\eta,\eta_1$ 的值和 $\psi,\varphi,u_1,u_2,w_0,v_1$ 带入到定理 5 的 5 个多项式(22)~多项式(26),利用工具 CADpsd 可以验证该 5 个多项式均为全局非负的,则(φ–0.2,ψ–2)确实是组合 *T*-栅栏函数.

3.2 求解初等系统的栅栏函数

定义 1(初等系统). 给定扩展连续系统($f(x),D,I,U$),如果 $f(x)$是初等函数,并且存在有限个初等函数 $g_1(x),\ldots,g_r(x),h_1(x),\ldots,h_s(x),p_1(x),\ldots,p_q(x)$,使得 $I=\{x|g_1(x)\geqslant 0\wedge\ldots\wedge g_r(x)\geqslant 0\}$,$U=\{x|h_1(x)\geqslant 0\wedge\ldots\wedge h_s(x)\geqslant 0\}$ 并且 $D=\{x|p_1(x)\geqslant 0\wedge\ldots\wedge p_q(x)\geqslant 0\}$,则称该系统是初等系统.

考虑到初等函数对求导算子的封闭性,通过引入新变量,初等系统是可以近似成更高维的多项式系统的.在文献[22]中给出了如何将一个初等系统近似成一个更高维多项式系统的方法,其主要的想法在于:引入新变量 y_1,y_2,z 分别替换初等系统中可能出现的正弦函数 $\sin(x)$、余弦函数 $\cos(x)$和指数函数 e^x,再将 $\dot{y}_1=y_2\dot{x}$, $\dot{y}_2=-y_1\dot{x}$ 和 $\dot{z}=z\dot{x}$ 加入到向量场.这样得到关于 x,y_1,y_2,z 的多项式系统,然后用第 3.1 节中的方法来求解该多项式系统的栅栏函数,再将新变量 y_1,y_2,z 用 $\sin(x),\cos(x)$和 e^x 替换即可.下面用例 2 阐明这一方法.

例 2:考虑如下定义的初等系统[16]:

$$\begin{cases} f(x_1,x_2)=(e^{-x_1^2}+x_2-1,-\sin^2(x_1))^T \\ D=\{(x_1,x_2)\in\mathbb{R}^2\,|\,-2\leqslant x_1\leqslant 2\wedge -2\leqslant x_2\leqslant 2\} \\ I=\{(x_1,x_2)\in\mathbb{R}^2\,|\,0.04-(x_1+1)^2-(x_2-1)^2\geqslant 0\} \\ U=\{(x_1,x_2)\in\mathbb{R}^2\,|\,0.09-x_1^2-x_2^2\geqslant 0\} \end{cases},$$

其中,时间界为 T=0.1.

首先,通过引入新变量将此初等系统转化成多项式系统.令:

$$y_1=\sin(x_1),y_2=\cos(x_1),z=e^{-x_1^2}.$$

可以得到下面的多项式向量场函数:

$$\begin{bmatrix}\dot{x}_1\\ \dot{x}_2\\ \dot{y}_1\\ \dot{y}_2\\ \dot{z}\end{bmatrix}=\hat{f}(x_1,x_2,y_1,y_2,z)=\begin{bmatrix}z+x_2-1\\ -y_1^2\\ y_2(z+x_2-1)\\ -y_1(z+x_2-1)\\ -2zx_1(z+x_2-1)\end{bmatrix}.$$

这样,2 维的初等函数向量场转化成了 5 维的多项式向量场,而其对应的可行域 $\hat{D}$、初始区域 $\hat{I}$ 和非安全区域 $\hat{U}$ 则相应的变成如下集合:

$$\hat{D}=\{(x_1,x_2,y_1,y_2,z)\,|\,-2\leqslant x_1\leqslant 2\wedge -2\leqslant x_2\leqslant 2\wedge y_1=\sin(x_1)\wedge y_2=\cos(x_2)\wedge z=e^{-x_1^2}\},$$

$$\hat{I}=\{(x_1,x_2,y_1,y_2,z)\,|\,0.25-(x_1+1)^2-(x_2-1)_2^2\geqslant 0\wedge y_1=\sin(x_1)\wedge y_2=\cos(x_2)\wedge z=e^{-x_1^2}\},$$

$$\hat{U}=\{(x_1,x_2,y_1,y_2,z)\,|\,0.04-x_1^2-x_2^2\geqslant 0\wedge y_1=\sin(x_1)\wedge y_2=\cos(x_2)\wedge z=e^{-x_1^2}\}.$$

这样就可以得到扩展连续系统 $(\hat{f},\hat{D},\hat{I},\hat{U})$.容易看到: $\hat{f}$ 是关于该系统的变量(x_1,x_2,y_1,y_2,z)是多项式的,但可行域 $\hat{D}$、初始区域 $\hat{I}$ 和非安全区域 $\hat{U}$ 不是.针对初等函数的性质,可以对 $\hat{D},\hat{I},\hat{U}$ 有如下的包含近似:

$$\bar{D}=\{(x_1,x_2,y_1,y_2,z)\,|\,-2\leqslant x_1\leqslant 2\wedge -2\leqslant x_2\leqslant 2\wedge 1-y_1^2\geqslant 0\wedge 1-y_2^2\geqslant 0\wedge z\geqslant 0\wedge 1-z\geqslant 0\},$$

$$\bar{I}=\left\{(x_1,x_2,y_1,y_2,z)\,|\,\frac{1}{4}-(x_1+1)^2-(x_2-1)^2\geqslant 0\wedge 1-y_1^2\geqslant 0\wedge 1-y_2^2\geqslant 0\wedge z\geqslant 0\wedge 1-z\geqslant 0\right\},$$

$$\bar{U}=\{(x_1,x_2,y_1,y_2,z)\,|\,0.04-x_1^2-x_2^2\geqslant 0\wedge 1-y_1^2\geqslant 0\wedge 1-y_2^2\geqslant 0\wedge z\geqslant 0\wedge 1-z\geqslant 0\}.$$

系统 $(\hat{f},\bar{D},\bar{I},\bar{U})$ 是一个多项式系统.对系统(f,D,I,U)和系统 $(\hat{f},\bar{D},\bar{I},\bar{U})$ 之间的关系,文献[22]有更详细的讨

论.不难发现:若 $\overline{\varphi}(x_1,x_2,y_1,y_2,z)$ 是系统 $(\hat{f},\overline{D},\overline{I},\overline{U})$ 的 T-栅栏函数,则 $\varphi(x_1,x_2)=\overline{\varphi}(x_1,x_2,\sin(x_1),\cos(x_1),\mathrm{e}^{-x_1^2})$ 是系统(f,D,I,U)的一个 T-栅栏函数.

利用定理 4 求解系统 $(\hat{f},\overline{D},\overline{I},\overline{U})$ 的 T-栅栏函数.这里设置λ=−0.1,φ的模板为关于 x_1,x_2 的二次多项式系数待定.利用 YALMIP 工具,可以求得(保留小数点后 4 位):

$$\varphi=-0.1771x_1^2-0.2948x_1x_2+0.1472x_2^2+3.6819x_1-4.5156x_2+5.1926,$$
$$\eta=2.1422.$$

利用符号计算工具 CADpsd 软件包,类似例 1 可以验证$\varphi-\eta$确实是系统 $(\hat{f},\overline{D},\overline{I},\overline{U})$ 的 T-栅栏函数.因其中不含有变量 y_1,y_2,z,则$\varphi-\eta$也是系统(f,D,I,U)的 T-栅栏函数.

4 总 结

在以往的工作中,只有对无界时间栅栏函数的讨论.虽然无界时间栅栏函数可以证明有界时间的安全性,但是对于有界时间的安全性问题,通常不应该要求其具有无界时间的安全性.本文针对有界时间安全性问题,定义有界时间的栅栏函数,T-栅栏函数.同时,给出在时间有界情况下 T-栅栏函数的条件和组合 T-栅栏函数的条件,并对于多项式系统和初等系统分别给出 T-栅栏函数的生成方法.

References:

[1] Alur R, Courcoubetis C, Halbwachs N, Henzinger T, Ho PH, Nicollin X, Olivero A, Sifakis J, Yovine S. The algorithmic analysis of hybrid systems. Theoretical Computer Science, 1995,138(1):3−34. [doi: 10.1016/0304-3975(94)00202-T]

[2] Alur R, Courcoubetis C, Henzinger TA, Ho PH. Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. In: Proc. of the Hybrid Systems. LNCS 736, Springer-Verlag, 1993. 209−229. [doi: 10.1007/3-540-57318-6_30]

[3] Bu L, Li Y, Wang LZ, Chen X, Li XD. Bach 2: Bounded reachability checker for compositional linear hybrid systems. In: Proc. of the Conf. on Design, Automation and Test in Europe. European Design and Automation Association, 2010. 1512−1517. [doi: 10.1109/DATE.2010.5457051]

[4] Gulwani S, Tiwari A. Constraint-Based approach for analysis of hybrid systems. In: Proc. of the CAV 2008. LNCS 5123, Springer-Verlag, 2008. 19õ 03. [doi: 10.1007/978-3-540-70545-1_18]

[5] Henzinger TA, Sifakis J. The embedded systems design challenge. In: Proc. of the FM 2006. LNCS 4085, Springer-Verlag, 2006. 1−15. [doi: 10.1007/11813040_1]

[6] Lee E. What's ahead for embedded software? IEEE Computer, 2000,33(9):18−26. [doi: 10.1109/2.868693]

[7] Maler O, Manna Z, Pnueli A. From timed to hybrid systems. In: Proc. of the Real-Time: Theory in Practice, REX Workshop. Springer-Verlag, 1992. 447−484. [doi: 10.1007/BFb0032003]

[8] Zhan NJ, Wang SL, Zhao HJ. Formal modelling, analysis and verification of hybrid systems. In: Proc. of the Unifying Theories of Programming and Formal Engineering Methods. LNCS 8050, Springer-Verlag, 2013. 207−281. [doi: 10.1007/978-3-642-39721-9_5]

[9] Henzinger TA, Ho PH. Algorithmic analysis of nonlinear hybrid systems. In: Proc. of the CAV'95. LNCS 939, Springer-Verlag, 1995. 225−238. [doi: 10.1007/3-540-60045-0_53]

[10] Lafferriere G, Pappas GJ, Yovine S. Symbolic reachability computation for families of linear vector fields. Journal of Symbolic Computation, 2001,32(3):231−253. [doi: 10.1006/jsco.2001.0472]

[11] Puri A, Varaiya P. Decidability of hybrid systems with rectangular differential inclusions. In: Proc. of the CAV'94. LNCS 818, Springer-Verlag, 1994. 95−104. [doi: 10.1007/3-540-58179-0_46]

[12] Sanfelice RG, Teel AR. Dynamical properties of hybrid systems simulators. Automatica, 2010,46(2):239−248. [doi: 10.1016/j.automatica.2009.09.026]

[13] Prajna S, Jadbabaie A. Safety verification of hybrid systems using barrier certificates. In: Proc. of the HSCC 2004. LNCS 2993, Springer-Verlag, 2004. 477−492. [doi: 10.1007/978-3-540-24743-2_32]

[14] Kong H, He F, Song XJ, Hung WNN, Gu M. Exponential-Condition based barrier certificate generation for safety verification of hybrid systems. In: Proc. of the CAV 2013. LNCS 8044, Springer-Verlag, 2013. 242−257. [doi: 10.1007/978-3-642-39799-8_17]

[15] Kong H, Song XY, Han D, Gu M, Sun JG. A new barrier certificate for safety verification of hybrid systems. The Computer Journal, 2014,57(7):1033−1045. [doi: 10.1093/comjnl/bxt059]

[16] Dai LY, Gan T, Xia BC, Zhan NN. Barrier certificates revisited. http://arxiv.org/abs/1310.6481

[17] Dai LY, Xia BC, Zhan NJ. Generating non-linear interpolants by semidefinite programming. In: Proc. of the CAV 2013. LNCS 8044, Springer-Verlag, 2013. 364−380. [doi: 10.1007/978-3-642-39799-8_25]

[18] Löfberg J. Pre- and post-processing sum-of-squares programs in practice. IEEE Trans. on Automatic Control, 2009,54(5): 1007−1011. http://users.isy.liu.se/johanl/yalmip/ [doi: 10.1109/TAC.2009.2017144]

[19] Parrilo PA. Structured semidefinite programs and semi-algebraic geometry methods in robustness and optimization [Ph.D. Thesis]. California Inst. of Tech., 2000.

[20] Khalil HK. Nonlinear Systems. 3rd ed., Prentice Hall, 2002.

[21] Han JJ, Jin Z, Xia BC. Proving inequalities and solving global optimization problems via simplified CAD projection. Journal of Symbolic Computation, 2016,72(2016):206−230. [doi: 10.1016/j.jsc.2015.02.007]

[22] Liu J, Zhan NJ, Zhao HJ, Zou L. Abstraction of elementary hybrid systems by variable transformation. In: Proc. of the FM 2015. LNCS 9109. 2015. 360−377. [doi: 10.1007/978-3-319-19249-9_23]

甘庭(1989－),男,湖北武汉人,主要研究领域为符号计算,程序验证.

夏壁灿(1968－),男,博士,教授,博士生导师,主要研究领域为符号计算,程序验证.