ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.12, December 2008, pp.3111−3121
DOI: 10.3724/SP.J.1001.2008.03111

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

混合系统的符号化可达性分析*

张海宾, 段振华+

(西安电子科技大学 计算理论与技术研究所,陕西 西安 710071)

Symbolic Reachability Analysis of Hybrid Systems

ZHANG Hai-Bin, DUAN Zhen-Hua+

(Institute of Computing Theory and Technology, Xidian University, Xi'an 710071, China)

+ Corresponding author: E-mail: ZhhDuan@mail.xidian.edu.cn

Zhang HB, Duan ZH. Symbolic reachability analysis of hybrid systems. *Journal of Software*, 2008,19(12): 3111−3121. http://www.jos.org.cn/1000-9825/19/3111.htm

Abstract: A restricted constraint system called hybrid zone is formalized for the representation and manipulation of rectangular automata state-spaces. Hybrid zones are proved to be closed over reachability operations of rectangular hybrid systems. In addition, rectangular hybrid systems are used to simulate nonlinear hybrid systems, which enables us to use hybrid zones for reachability analysis of nonlinear hybrid systems. After the hybrid zone has been converted to the canonical form, reachability operations for hybrid systems can be implemented straightforwardly. Hence, the main computation is the operation for obtaining the canonical form of hybrid zones. Finding the canonical form can be automated by an algorithm for linear programming.

Key words: hybrid system; rectangular hybrid system; reachability analysis; verification; nonlinear hybrid system

摘 要: 定义了一种称作混合区域的形式化结构表示矩形混合系统的状态集,它实际上是由一组特殊形式的线性不等式联立表示的多面体空间.证明了混合区域对于矩形混合系统的可达性操作的封闭性.此外,用矩形混合系统近似模拟非线性混合系统,相应地解决了非线性混合系统的可达性问题.使用混合区域,可以直接计算由某个正则的混合区域开始的可达集,这样,混合系统的可达性问题主要是求解混合区域的正则型问题,而这问题是一种线性规划问题,可以使用经典的线性规划算法加以解决.

关键词: 混合系统;矩形混合系统;可达性分析;验证;非线性混合系统

中图法分类号: TP301 **文献标识码**: A

混合系统(hybrid system)是连续和离散事件系统非平凡混合的系统[1−3],典型的实例是与连续变化的物理环境相互作用的数字控制器.混合系统广泛存在于数控系统、商业、工业和军事领域,特别是对安全性要求极高的系统,如飞机、导弹、核电站等.在这样的系统中一个很小的错误也会造成严重的、甚至灾难性的后果.因此,混合系统的验证就显得极为重要,尤其对混合系统自动验证的研究更是目前国际上计算机专家和控制论专

* Supported by the National Natural Science Foundation of China under Grant No.60433010 (国家自然科学基金); the Defense Pre-Research Project of China under Grant No.51315050105 (装备预先研究项目)

Received 2007-06-18; Accepted 2008-08-07

家的研究热点之一.

目前计算机专家的研究焦点是混合系统的可达性问题.可达性问题是混合系统验证技术的基础,许多验证问题都可以转化为可达性问题,例如,安全性是计算机专家非常关心的混合系统性质,我们可以通过判定不安全状态是否可达来验证系统的安全性.对于混合系统来说,可达集的计算是相当复杂的,因为混合系统是无穷状态空间系统,在这种情况下,符号化方法就成为一种有效的可达性分析方法.

采用符号化方法计算可达集,关键问题就是选择什么样的数据结构表示状态集.我们知道,混合系统主要有两种类型的转换操作,系统在某个控制状态上停留一段时间称为一个延迟(delay)转换,系统从一个控制状态到另一个控制状态的转化称为跳跃(jump)转换.表示混合系统状态集的数据结构必须满足对延迟转换和跳跃转换的封闭性.对于实时系统的符号化可达性分析,Dill 采用了一种称为时间区域[4,5](clock zone)的结构表示状态集.时间区域是由不等式联立表示的多面体区域,这些不等式是单个时间变量或两个时间变量的差与某个整数常量的比较.给定一个时间区域,很容易给出一套规则来计算经过实时系统的延迟转换和跳跃转换所有可达状态组成的时间区域.文献[5]指出,实时系统的可达性分析关键是计算时间区域的正则型.对于线性混合系统,大多数研究者都是采用普通的多面体[6−9](polyhedra)或类似于普通多面体的结构[10]来表示状态集.普通多面体是由形如 $\sum_{i=1}^{n} a_i x_i \prec c$ 的线性不等式的联立表示的线性空间.使用普通多面体结构,必须采用量词消去这类方法来计算可达集.然而,量词消去运算的计算复杂度是双指数级的,但这也是不得已的办法,因为线性混合系统的可达性问题本身是不可判定的.

矩形混合系统是线性混合系统的子集.目前还没有专门的数据结构表示矩形混合系统的可达状态集.本文的目标之一就是定义一种类似于时间区域的形式化结构进行矩形混合系统的可达性分析.时间区域显然不能表示矩形混合系统可达集,因为时间区域对于矩形混合系统的可达性操作(延迟转换操作和跳跃转换操作)是不封闭的.也就是说,给定时间区域,经过矩形混合系统的某种转换所有可达的状态不一定能够用时间区域表示.当然,对于线性混合系统的子集,我们可以用普通多面体表示矩形混合系统的状态集,用量词消去运算计算可达集,但是这样就会有线性混合系统的双指数级的复杂度.通过大量研究,我们发现了一种类似于时间区域的形式化结构可以作为矩形混合系统可达性分析的基本单位,我们称其为混合区域.

混合区域是由不等式联立表示的线性多面体区域,这些不等式都是由两个变量或单个变量构成的线性表达式和一个有理数的比较.表达式中变量的系数与变量微分取值域的端点有关.使用混合区域进行矩形混合系统可达性分析,必须保证其对于矩形自动机可达性操作的封闭性.本文用了很大篇幅来证明混合区域对于矩形自动机两种类型的转换操作是封闭的,即一个混合区域经过一个延迟转换,或一个跳跃转换后所有可达的状态仍可用一个混合区域表示.我们可以像时间区域那样,给出一套规则,求解正则的混合区域经过转换操作后可达的混合区域,这样,矩形混合系统的可达性问题主要的计算就是求解混合区域的正则型.虽然混合区域正则型的求解不像时间区域那样简单,直接用 Floyd-Warshall 算法就可以,但是,研究中我们发现,求解混合区域中的每个不等式的正则型实际上是一种线性规划问题,可以直接使用多项式复杂度的经典线性规划算法求解混合区域的正则型.

为了在计算机中存储混合区域,本文定义了一种矩阵数据结构称作不同上限矩阵,并且用它实现了矩形混合系统的可达性运算.此外,混合区域还被用来进行非线性混合系统的可达性分析.本文用矩形混合系统近似模拟非线性混合系统,然后使用混合区域判定矩形混合系统的可达性问题,进而近似地判定非线性混合系统的可达性问题.

本文第 1 节简单介绍混合自动机的相关定义.第 2 节定义混合区域,并证明混合区域可用于矩形混合系统的符号化可达性分析.第 3 节定义不同上限矩阵用于计算机中混合区域的表示,并实现基于该矩阵的矩形混合系统的可达性分析算法.第 4 节给出非线性混合系统可达性问题的一种解决办法.第 5 节与相关工作进行比较并得出相应的结论.

1 混合自动机

设 $Y=\{y_1,\ldots,y_n\}$是一组取值域为实数的变量集,R 是实数集,R^+表示正实数集合.矩形 $B\subseteq R^n$ 是由形如 $y_i\sim c$ 的不等式联立表示的 n 维向量空间,其中~为<,≤,=,≥或>.对于矩形 B,我们用 B_i 表示 B 在第 i 维(y_i)向量轴上的投影矩形,并且用β_n表示所有 n 维矩形的集合.指派 $v=(a_1,\ldots,a_n)$是一个赋值函数,它为集合 Y 中的任意元素 y_i 赋予一个实数值 $a_i\in\mathrm{R}$.用 V 表示所有指派的集合.对于 $v\in V,d\in\mathrm{R}^+,\theta\subseteq(1,\ldots,n),\lambda\in R^n$ 和 $B\in\beta_n$,用 $v+\lambda\cdot d$ 表示这样的指派 v':对于任意的 $y_i,v'(y_i)=v(y_i)+\lambda_i\cdot d$;用 $[\theta\mapsto B]v$ 表示这样的指派 v'':对于任意的 $i\notin\theta,v''(y_i)=v(y_i)$,对于任意的 $i\in\theta,v''(y_i)\in B_i$.对于 Y 上的断言φ,用 $v\in\varphi$表示指派 v 可以使断言φ成立;用$|\varphi|$表示能使φ成立的所有指派的集合,用$|\varphi_i|$表示$|\varphi|$在第 i 维(y_i)向量轴上的投影区域[11].对于矩形 $B\subseteq R^n$,B 既可以被视为一个指派的集合($B\subseteq R^n$),也可以被视为 Y 上的一个断言(B 是形如 $y_i\sim c$ 的不等式的联立),也就是说,B 和$|B|$具有相同的意义.

混合自动机[11]是一个九元组 $(Q,X,init,E,inv,act,jump,update,reset)$,其中:

- Q 是一个有穷的控制状态集合.
- $X=\{x_1,\ldots,x_n\}$是一个取值为实数的连续变量的集合.
- $init$ 是一个赋值函数,它为每个控制状态赋予一个 X 上的断言表示的初始条件.
- $E\subseteq Q\times Q$ 是所有边的集合.
- inv 是一个赋值函数,它为每个控制状态赋予一个 X 上的断言表示的连续变量取值限制条件.
- act 是一个赋值函数,它为每个控制状态赋予一个 X 上的断言表示的连续变量微分取值限制条件.
- $jump$ 是一个赋值函数,它为每条边 $e\in E$ 赋予一个能够触发 e 边的连续变量取值条件.
- $update:E\to 2^{\{1,\ldots,n\}}$,$update(e)$代表经过 e 边跳跃转换后需要重新赋值的变量集 $\{x_i\mid i\in update(e)\}$.
- $reset$ 是一个赋值函数,它为每条边 e 赋予一个表示经过 e 转换后连续变量重新赋值的限制条件.

状态 s 是一个二元组(q,v),其中 $q\in Q,v\in V$,我们用 S 表示所有状态的集合.矩形自动机[12−14]是混合自动机的子集.对于矩形自动机 H 的任意控制状态 $q\in Q$ 和边 $e\in E$,H 的 $init(q),inv(q),act(q),jump(e)$和 $reset(e)$都是矩形.矩形自动机的一次执行是一个 S 上的包含如下两种类型的转换的无穷序列:

- $(q,v)\xrightarrow{d}(q,v')$,其中 $v,v'\in inv(q)$,$d\in\mathrm{R}^+$,并且$\exists\lambda\in act(q)$使得 $v'=v+\lambda\cdot d$,
- $(q,v)\longrightarrow(q',v')$,其中 $e=(q,q')\in E$,$v\in inv(q)\wedge jump(e)$,$v'\in inv(q')\wedge reset(e)$,并且 $v'=[update(e)\mapsto reset(e)]v$.

对于矩形自动机任意的边 $e=(q,q')\in E$,如果 $act(q')_i\neq act(q)_i$,必有 $i\in update(e)$,则称该矩形自动机为初始化的(initialized)[14].本文处理的矩形自动机不仅要求初始化,而且要求对任意的控制状态 q,$init(q)$有界,$act(q)_i\subset(-\infty,0]$或 $act(q)_i\subset[0,\infty)$,并且 $act(q)_i$的端点为整数;对于任意的边 e,$jump(e)$和 $reset(e)$有界.

2 矩形混合系统的可达性分析

给定矩形自动机 H 的两个状态 s 和 s',可达性问题检验是否存在 H 的某次执行,该执行开始于状态 s,终止于状态 s'.由于矩形自动机是无穷状态空间系统,我们不能像离散系统那样,在状态空间中逐个状态地搜索,直至找到某个状态或搜索完状态空间.必须定义一种结构来表示状态集,这种结构应该具备封闭性,即由某个状态集经过可达性操作所有可达的状态还可以由这种结构表示;判空性,即可以判定某个状态集是否为空;包含性,即可以判定两个状态集是否有包含关系.本文使用混合区域作为矩形混合系统符号化可达性分析的基本单位.

我们利用图 1 中的算法[15]进行矩形混合系统的可达性分析.这种算法检验某个矩形自动机是否可以到达某个满足公式ϕ 的状态.它以状态集为基本操作单位.该算法通过反复计算状态集上的 3 种可达性操作来判断某个状态是否可达,或不再有新的可达状态产生.对于矩形自动机 H,设 D 和 D'为两个指派集合,$q,q'\in Q$ 为控制状态,$e=(q,q')\in E$ 为一条边,指派集上的 3 种可达性操作(指派集的交我们也看作是一种可达性操作,因为在跳跃转换前必须计算可以触发跳跃转换的指派集)分别是:交操作 $D\wedge D'$:由所有同时包含在集合 D 和 D'中的指派组成;控制状态 q 上的时间流逝操作 $D^{\uparrow_q}=\{u+\lambda\cdot d\mid u\in D\wedge\lambda\in act(q)\wedge d\in\mathrm{R}^+\}$:由 D 中的指派在 q 上随时间流逝

所有可达的指派组成;变量重赋值操作 $Reset_e(D)=\{[update(e)\mapsto reset(e)]u \mid u\in D\}$:由 D 中的指派经过边 e 跳跃转换而得到的指派组成.在图 1 中, $(q,D)\xrightarrow{trans.}(q_s,D_s)$ 当且仅当 $q_s=q\wedge D_s=(D\wedge inv(q))^{\uparrow q}$ 或者 $D_s=Reset_e(D\wedge jump(e))\wedge e=(q,q_s)$.

```
Passed:={}
Wait:={(q0,D0)}
While Wait ≠ {}
    get (q,D) from Wait
    if (q,D) satisfies φ then return 'YES'
    else if D ⊄ D' for all (q,D') ∈ Passed
    add (q,D) to Passed
    Next:={(qs,Ds)|(q,D) --trans.--> (qs,Ds) ∧ Ds ≠ ∅}
    for all (qs',Ds') ∈ Next do
        put (qs',Ds') to Wait
Return 'NO'
```

Fig.1 An algorithm for symbolic reachability analysis

图 1 符号化可达性分析算法

2.1 混合区域

对于整数 a 和 b,定义函数 $\tilde{g}(a,b)$ 为:当 $a\cdot b\neq 0$ 时, $\tilde{g}(a,b)=gcd(a,b)$;否则, $\tilde{g}(a,b)=1$,其中 $gcd(a,b)$为 a 和 b 的最大公约数.

定义 1. 给定矩形自动机的一个状态 q,令 l_k 和 r_k 分别表示 $act(q)_k$ 的左右端点,q-区域是由如下形式的不等式联立表示的一块 n 维多面体区域:

$$\bigwedge_{0<i\le n} x_i\prec c_{i0}\wedge -x_i\prec c_{0i}\wedge \bigwedge_{0<i\neq j\le n} a_{ij}x_i-b_{ij}x_j\prec c_{ij},$$

其中, $\prec$ 为<或≤; c_{ij} 为有理数;对任意的 $0<i\neq j\le n$, a_{ij} 和 b_{ij} 满足:

$$\begin{cases} a_{ij}=l_j/\tilde{g}(l_j,r_i) & b_{ij}=r_i/\tilde{g}(l_j,r_i), \quad \text{if} \quad l_i\ge 0\wedge l_j\ge 0\\ a_{ij}=l_j/\tilde{g}(l_j,l_i) & b_{ij}=l_i/\tilde{g}(l_j,l_i), \quad \text{if} \quad l_i\ge 0\wedge r_j\le 0\\ a_{ij}=r_j/\tilde{g}(r_j,r_i) & b_{ij}=r_i/\tilde{g}(r_j,r_i), \quad \text{if} \quad r_i\le 0\wedge l_j\ge 0\\ a_{ij}=r_j/\tilde{g}(r_j,l_i) & b_{ij}=l_i/\tilde{g}(r_j,l_i), \quad \text{if} \quad r_i\le 0\wedge r_j\le 0 \end{cases}.$$

混合区域是由某个 q-区域表示的 n 维多面体空间.为了给出混合区域的统一形式,我们引入一个特殊的恒为 0 的变量 x_0,这样,混合区域的一般形式为

$$x_0=0\wedge \bigwedge_{0\le i\neq j\le n} a_{ij}x_i-b_{ij}x_j\prec c_{ij} \tag{1}$$

其中对任意的 $1\le i\le n$, $a_{0i}=b_{0i}=a_{i0}=b_{i0}=1$.

给定一个不等式联立表示的混合区域 D,称 D 中的每个不等式 $ax-by\prec c$ 的右半部分 $(\prec,c)$ 为线性表达式 $ax-by$ 的边界.对于两个边界 $(\prec,c)$ 和 $(\prec',c')$,称 $(\prec,c)$ 比 $(\prec',c')$ 更紧凑,表示为 $(\prec,c)\sqsubseteq(\prec',c')$,当且仅当 $c<c'$,或者 $c=c'\wedge \prec=\text{'}<\text{'}\wedge\prec'=\text{'}\le\text{'}$.对于 $\prec$ 和 $\prec'$,定义 $\min(\prec,\prec')=\text{'}\le\text{'}$,当 $\prec=\text{'}\le\text{'}\wedge\prec'=\text{'}\le\text{'}$;否则, $\min(\prec,\prec')=\text{'}<\text{'}$.假设 $(\prec',c')$ 是线性表达式 $ax-by$ 的可以由 D 中除去 $ax-by\prec c$ 之外的不等式联立推出的最紧凑的边界.称 $ax-by\prec'' c''$ 为正则的,其中边界 $(\prec'',c'')$ 为 $(\prec,c)$ 和 $(\prec',c')$ 中比较紧凑的一个.如果 D 中的每个联立不等式都是正则的,则称混合区域 D 是正则的.

混合区域要想作为矩形混合系统符号化可达性分析的基本操作单位,必须满足判空性、包含性和对于图 1 算法中所用到的 3 种可达性操作的封闭性.对于两个正则的混合区域,包含性是很容易判定的,如下的引理和定理将保证混合区域的封闭性和判空性.

我们知道,线性混合系统可达性分析的一个基本运算就是量词消去,无论是连续的延迟转换,还是离散的跳

跃转换,可达的状态集都可以由原来的状态集经过量词消去运算而得到.量词消去也是我们进行矩形混合系统可达性分析的基本运算.线性不等式组表示的状态集经过量词消去必然会产生新的不等式约束条件,因此,混合区域要想保持 3 种可达性操作上的封闭性,就必须具备一种特殊的性质,即经过量词消去运算产生的新的不等式必须是冗余的,也就是说,它可以由原来的不等式联立推导出来.下面我们将给出混合区域的这种特殊性质.

对于矩形自动机 H 的一个控制状态 $q\in Q$,令 l_i 和 r_i 分别表示 $act(q)_i$ 的左、右端点,给定 q-区域 D,设 D 的正则型由公式(1)表示,我们称 D 具有 q-性质,当且仅当对于任意的 $0<i\neq k\neq j\leq n$,如下条件成立:

1. 若 $l_i\geq 0, l_j\geq 0, l_k\geq 0$,则 $\tilde{g}(l_j,r_i)l_k c_{ij}+(r_k r_i-l_k r_i)c_{0j}\leq \tilde{g}(l_k,r_i)l_j c_{ik}+\tilde{g}(l_j,r_k)r_i c_{kj}$.
2. 若 $l_i\geq 0, l_j\geq 0, r_k\leq 0$,则 $-\tilde{g}(l_j,r_i)r_k c_{ij}+(r_k r_i-l_k r_i)c_{0j}\leq \tilde{g}(r_i,r_k)l_j c_{ki}+\tilde{g}(l_k,l_j)r_i c_{jk}$.
3. 若 $l_i\geq 0, r_j\leq 0, l_k\geq 0$,则 $\tilde{g}(l_j,l_i)r_k c_{ij}+(r_k l_i-l_k l_i)c_{j0}\leq \tilde{g}(l_j,l_k)l_i c_{kj}-\tilde{g}(l_i,r_k)l_j c_{ki}$.
4. 若 $l_i\geq 0, r_j\leq 0, r_k\leq 0$,则 $-\tilde{g}(l_j,l_i)l_k c_{ij}+(r_k l_i-l_k l_i)c_{j0}\leq \tilde{g}(r_k,l_j)l_i c_{jk}-\tilde{g}(l_k,l_i)l_j c_{ik}$.
5. 若 $r_i\leq 0, l_j\geq 0, l_k\geq 0$,则 $\tilde{g}(r_j,r_i)r_k c_{ij}+(l_k r_i-r_k r_i)c_{0j}\leq \tilde{g}(r_k,r_i)r_j c_{ik}-\tilde{g}(l_k,r_j)r_i c_{jk}$.
6. 若 $r_i\leq 0, l_j\geq 0, r_k\geq 0$,则 $-\tilde{g}(r_j,r_i)l_k c_{ij}+(l_k r_i-r_k r_i)c_{0j}\leq \tilde{g}(r_i,l_k)r_j c_{ki}-\tilde{g}(r_j,r_k)r_i c_{kj}$.
7. 若 $r_i\leq 0, r_j\leq 0, l_k\geq 0$,则 $\tilde{g}(r_j,l_i)l_k c_{ij}+(l_k l_i-r_k l_i)c_{j0}\leq -\tilde{g}(l_i,l_k)r_j c_{ki}-\tilde{g}(r_k,r_j)l_i c_{jk}$.
8. 若 $r_i\leq 0, r_j\leq 0, r_k\leq 0$,则 $-\tilde{g}(r_j,l_i)r_k c_{ij}+(l_k l_i-r_k l_i)c_{j0}\leq -\tilde{g}(r_k,l_i)r_j c_{ik}-\tilde{g}(r_j,l_k)l_i c_{kj}$.

很容易证明,如果 q-区域 D 具有 q-性质,则对于 D 中任意的两个不等式 $f_1(x_i,x_j)\prec c$ 和 $f_2(x_i,x_k)\prec' c'$,经过量词消去运算产生的不等式 $\exists x_i[f_1(x_i,x_j)\prec c\wedge f_2(x_i,x_k)\prec' c']$ 是冗余的.q-区域 D 具有 q-性质,保证了 D 经过量词消去运算后不会有新的不等式约束条件产生.这种性质将保证一个混合区域经过跳跃转换后得到的状态集仍是一个混合区域.下面的引理成立.

引理 1. 给定矩形自动机 H 的一个控制状态 $q\in Q$,如果 D 是一个具有 q-性质的 q-区域,$x_r\in X$ 是一个连续变量,则 $\exists x_r[D]$ 是一个变量集 $X\setminus\{x_r\}$ 上具有 q-性质的 q-区域.

证明:假设 D 的正则型由公式(1)表示,不失一般性,设 $r=n>0$,很容易证明 $\exists x_n[D]$ 是由 $x_0=0\wedge\bigwedge_{0\leq i\neq j<n} a_{ij}x_i-b_{ij}x_j\prec c_{ij}$ 表示的 q-区域.由于 D 具有 q-性质,所以,$\exists x_n[D]$ 也具有 q-性质. □

引理 2. 给定一个由 $x_0=0\wedge\bigwedge_{0\leq i\neq j\leq n} a_{ij}x_i-b_{ij}x_j\prec_{ij} c_{ij}$ 表示的正则的混合区域 D,对每对 $0\leq i,j\leq n$,设 $(\prec'_{ij},d_{ij})$ 是表达式 $-(a_{ij}x_i-b_{ij}x_j)$ 的可由 D 中所有不等式联立推出的最紧凑的边界,则 D 为空,当且仅当存在某对 i,j,使得 $(\min(\prec_{ij},\prec'_{ij}),(c_{ij}+d_{ij}))\sqsubseteq(\leq,0)$.

证明:如果存在某对 i,j,使得 $(\min(\prec_{ij},\prec'_{ij}),(c_{ij}+d_{ij}))\sqsubseteq(\leq,0)$,则 $D\Rightarrow a_{ij}x_i-b_{ij}x_j\prec_{ij} c_{ij}\wedge-(a_{ij}x_i-b_{ij}x_j)\prec'_{ij} d_{ij}\Rightarrow 0<0$,所以 D 为空;反之,若 D 为空,则存在某对 i,j,使得 $a_{ij}x_i-b_{ij}x_j\prec_{ij} c_{ij}\wedge-(a_{ij}x_i-b_{ij}x_j)\prec'_{ij} d_{ij}\Rightarrow\text{false}$,进而 $(\min(\prec_{ij},\prec'_{ij}),(c_{ij}+d_{ij}))\sqsubseteq(\leq,0)$. □

引理 3. 给定矩形自动机 H,对于任意的控制状态 $q\in Q$,一个有界矩形是一个具有 q-性质的 q-区域.

证明:不失一般性,我们仅证明有界矩形 D 为 $\bigwedge_{0<i\leq n} x_i\prec_{i0} c_{i0}\wedge -x_i\prec_{0i} c_{0i}$ 的情形,其中 $c_{i0}>0, c_{0i}<0$.D 可以由 q-区域 $x_0=0\wedge\bigwedge_{0\leq i\neq j\leq n} a_{ij}x_i-b_{ij}x_j\prec_{ij} c_{ij}$ 表示,其中 a_{ij} 和 b_{ij} 满足定义 1,并且对每对 $i\cdot j\neq 0$,有 $\prec_{ij}=\min(\prec_{i0},\prec_{0j})$ 和 $c_{ij}=a_{ij}c_{i0}+b_{ij}c_{0j}$ 成立.令 l_i 和 r_i 分别表示 $act(q)_i$ 的左、右端点,下面来证明 D 具有 q-性质,以任意的 $l_i>0$ 为例.由于 $\tilde{g}(l_j,r_i)l_k c_{ij}+(r_k r_i-l_k r_i)c_{0j}=\tilde{g}(l_j,r_i)l_k a_{ij}c_{i0}+\tilde{g}(l_j,r_i)l_k b_{ij}c_{0j}+r_k r_i c_{0j}-l_k r_i c_{0j}=l_j l_k c_{i0}+l_k r_i c_{0j}+r_k r_i c_{0j}-l_k r_i c_{0j}=l_j l_k c_{i0}+r_k r_i c_{0j}$ 和 $\tilde{g}(l_k,r_i)l_j c_{ik}+\tilde{g}(l_j,r_k)r_i c_{kj}=\tilde{g}(l_k,r_i)l_j a_{ik}c_{i0}+\tilde{g}(l_k,r_i)l_j b_{ik}c_{0k}+\tilde{g}(l_j,r_k)r_i a_{kj}c_{k0}+\tilde{g}(l_j,r_k)r_i b_{kj}c_{0j}=l_j l_k c_{i0}+l_j r_i c_{0k}+r_i l_j c_{k0}+r_i r_k c_{0j}$,并且 D 不为空使得 $c_{0k}+c_{k0}\geq 0$,因此,$\tilde{g}(l_j,r_i)l_k c_{ij}+(r_k r_i-l_k r_i)c_{0j}=l_j l_k c_{i0}+r_k r_i c_{0j}\leq l_j l_k c_{i0}+l_j r_i c_{0k}+r_i l_j c_{k0}+r_i r_k c_{0j}=\tilde{g}(l_k,r_i)l_j c_{ik}+\tilde{g}(l_j,r_k)r_i c_{kj}$. □

定理 1. 给定矩形自动机 H 的一个控制状态 $q\in Q$,如果 D 是一个具有 q-性质的 q-区域,则 $D^{\uparrow_q}$ 也是一个具有 q-性质的 q-区域.

证明:令 l_i 和 r_i 分别表示 $act(q)_i$ 的左右端点,设 D 的正则型由公式(1)表示.在如下的证明中,我们省略等式

$x_0=0$,则($\gamma_0=0$):

$$D^{\uparrow_q}=\exists\gamma_1\in act(q)_1...\exists\gamma_n\in act(q)_n\exists t\geq 0[((x_0,...,x_n)-(\gamma_0,...,\gamma_n)t)\in D]=$$

$$\exists\gamma_1...\exists\gamma_n\exists t[-t\leq 0\wedge\bigwedge_{0<i\leq n}(\gamma_i\prec r_i\wedge-\gamma_i\prec-l_i)\wedge\bigwedge_{0\leq i\neq j\leq n}a_{ij}x_i-b_{ij}x_j\prec c_{ij}+(a_{ij}\gamma_i-b_{ij}\gamma_j)t]\Leftrightarrow$$

$$\exists t[-t\leq 0\wedge\bigwedge_{0<i\leq n}(-x_i\prec c_{0i}-l_i\cdot t\wedge x_i\prec c_{i0}+r_i\cdot t)\wedge\bigwedge_{0<i\neq j\leq n}a_{ij}x_i-b_{ij}x_j\prec c_{ij}]\Leftrightarrow$$

$$\bigwedge_{0<i\leq n}(x_0-x_i\prec' c'_{0i}\wedge x_i-x_0\prec' c'_{i0})\wedge\bigwedge_{0<i\neq j\leq n}a_{ij}x_i-b_{ij}x_j\prec c_{ij}.$$

其中,当 $l_i\geq 0$ 时,$(\prec',c'_{0i})=(\prec,c_{0i})$,$(\prec',c'_{i0})=(<,\infty)$;当 $r_i\leq 0$ 时,$(\prec',c'_{i0})=(\prec,c_{i0})$,$(\prec',c'_{0i})=(<,\infty)$.由于 D 是具有 q-性质的 q-区域,由上面的推导可得,$D^{\uparrow_q}$ 也是具有 q-性质的 q-区域. □

定理 2. 给定矩形自动机 H 的一个控制状态 $q\in Q$,如果 $D'\subseteq R^n$ 为一个有界矩形,D 为一个具有 q-性质的 q-区域,则 $D\wedge D'$也是一个具有 q-性质的 q-区域.

证明:由引理 3,$D\wedge D'$为 q-区域.下面我们证明其 q-性质.令 l_i 和 r_i 分别表示 $act(q)_i$ 的左、右端点.我们仅证任意 $l_i>0$ 的情形,其他情形证明类似.假设 D 的正则型为

$$x_0=0\wedge\bigwedge_{0<i\leq n}(x_0-x_i\prec c_{0i}\wedge x_i-x_0\prec c_{i0})\wedge\bigwedge_{0<i\neq j\leq n}(l_jx_i-r_ix_j)/gcd(l_j,r_i)\prec c_{ij},$$

令 $l_jd_{i0}+r_ic_{0j}=gcd(l_j,r_i)c_{ij}$,则上式可表示为

$$x_0=0\wedge\bigwedge_{0<i\leq n}(x_0-x_i\prec c_{0i}\wedge x_i-x_0\prec c_{i0})\wedge\bigwedge_{0<i\neq j\leq n}(l_jx_i-r_ix_j)\prec l_jd_{i0}+r_ic_{0j}.$$

由于 D 具有 q-性质,则 $-c_{0i}\leq d_{i0}$.假设 $D\wedge D'$的正则型为

$$x_0=0\wedge\bigwedge_{0<i\leq n}(x_0-x_i\prec c'_{0i}\wedge x_i-x_0\prec c'_{i0})\wedge\bigwedge_{0<i\neq j\leq n}(l_jx_i-r_ix_j)/gcd(l_j,r_i)\prec c'_{ij},$$

则对任意的 $0<i\neq j\leq n$,有 $c'_{0i}\leq c_{0i}$,$c'_{i0}\leq c_{i0}$ 和 $c'_{ij}=\min(c_{ij},(l_jc'_{i0}+r_ic'_{0j})/gcd(l_j,r_i))$ 成立.进而,

$$\tilde{g}(l_j,r_i)c'_{ij}\leq l_jc'_{i0}+r_ic'_{0j},\ \tilde{g}(l_k,r_i)c'_{ik}\leq l_kc'_{i0}+r_ic'_{0k},\ l_jc'_{i0}\leq\ \tilde{g}(l_j,r_i)\ c'_{ij}+r_ic'_{j0},\ l_kc'_{i0}\leq\tilde{g}(l_k,r_i)c'_{ik}+r_ic'_{k0}.$$

为了证明 $D\wedge D'$具有 q-性质,我们只需证明对任意的 $0<i\neq k\neq j\leq n$,下式

$$\tilde{g}(l_j,r_i)l_kc'_{ij}+(r_kr_i-l_kr_i)c'_{0j}\leq\tilde{g}(l_k,r_i)l_jc'_{ik}+\tilde{g}(l_j,r_k)r_ic'_{kj}$$

成立.由于 D 具有 q-性质,所以 $\tilde{g}(l_j,r_i)l_kc_{ij}+(r_kr_i-l_kr_i)c_{0j}\leq\tilde{g}(l_k,r_i)l_jc_{ik}+\tilde{g}(l_j,r_k)r_ic_{kj}$,

- 如果 $c'_{ij}=c_{ij}$,$c'_{kj}=c_{kj}$,$c'_{ik}=c_{ik}$,由于 $c'_{0j}\leq c_{0j}$,因此,$\tilde{g}(l_j,r_i)l_kc'_{ij}+(r_kr_i-l_kr_i)c'_{0j}\leq\tilde{g}(l_k,r_i)l_jc'_{ik}+\ \tilde{g}(l_j,r_k)r_ic'_{kj}$;
- 如果 $c'_{ij}=c_{ij}$,$c'_{ik}=c_{ik}$,$c'_{kj}=(l_jc'_{k0}+r_kc'_{0j})/gcd(l_j,r_k)$,由于 $\tilde{g}(l_i,r_i)c'_{ij}\leq l_jc'_{i0}+r_ic'_{0j}$,$l_kc'_{i0}\leq\ \tilde{g}(l_k,r_i)c'_{ik}+r_ic'_{k0}$,即 $l_jd_{i0}+r_ic_{0j}\leq l_jc'_{i0}+r_ic'_{0j}$,$l_kc'_{i0}\leq l_kd_{i0}+r_ic_{0k}+r_ic'_{k0}$,因此,$r_i(c_{0j}-c'_{0j})\leq l_j(c'_{i0}-d_{i0})$,$l_k(c'_{i0}-d_{i0})\leq r_i(c_{0k}+c'_{k0})$,进而,$l_k(c_{0j}-c'_{0j})\leq l_j(c_{0k}+c'_{k0})$,所以 $\tilde{g}(l_j,r_i)l_kc'_{ij}+(r_kr_i-l_kr_i)c'_{0j}=l_kl_jd_{i0}+r_kr_ic'_{0j}+l_kr_i(c_{0j}-c'_{0j})\leq l_kl_jd_{i0}+r_kr_ic'_{0j}+r_il_j(c'_{k0}+c_{0k})=\tilde{g}(l_j,r_k)r_ic'_{kj}+\tilde{g}(l_k,r_i)l_jc'_{ik}$;
- 如果 $c'_{ij}=c_{ij}$,$c'_{kj}=c_{kj}$,$c'_{ik}=(l_kc'_{i0}+r_ic'_{0k})/gcd(l_k,r_i)$,证明与上面类似;
- 如果 $c'_{ij}=c_{ij}$,$c'_{kj}=(l_jc'_{k0}+r_kc'_{0j})/gcd(l_j,r_k)$,$c'_{ik}=(l_kc'_{i0}+r_ic'_{0k})/gcd(l_k,r_i)$,由于 $D\wedge D'$ 非空,因此,对任意的 $0<j\leq n$,$c'_{j0}+c'_{0j}\geq 0$,进而 $\tilde{g}(l_j,r_i)l_kc'_{ij}+(r_kr_i-l_kr_i)c'_{0j}\leq l_kl_jc'_{i0}+l_kr_ic'_{0j}+r_kr_ic'_{0j}-l_kr_ic'_{0j}=l_kl_jc'_{i0}+r_kr_ic'_{0j}\leq l_kl_jc'_{i0}+r_kr_ic'_{0j}+l_jr_i(c'_{k0}+c'_{0k})=\tilde{g}(l_j,r_k)r_ic'_{kj}+\tilde{g}(l_k,r_i)l_jc'_{ik}$;
- 如果 $c'_{ij}=(l_jc'_{i0}+r_ic'_{0j})/gcd(l_j,r_i)$,$c'_{kj}=(l_jc'_{k0}+r_kc'_{0j})/gcd(l_j,r_k)$,$c'_{ik}=(l_kc'_{i0}+r_ic'_{0k})/gcd(l_k,r_i)$,则 $\tilde{g}(l_j,r_i)l_kc'_{ij}+(r_kr_i-l_kr_i)c'_{0j}=l_kl_jc'_{i0}+l_kr_ic'_{0j}+r_kr_ic'_{0j}-l_kr_ic'_{0j}=l_kl_jc'_{i0}+r_kr_ic'_{0j}\leq l_kl_jc'_{i0}+r_kr_ic'_{0j}+l_jr_i(c'_{k0}+c'_{0k})=\tilde{g}(l_j,r_k)r_ic'_{kj}+\tilde{g}(l_k,r_i)l_jc'_{ik}$. □

引理 4. 给定矩形自动机 H 的一个控制状态 $q\in Q$,设变量集 $X\setminus\{x_n\}$ 上具有 q-性质的 q-区域 D 的正则型为 $x_0=0\wedge\bigwedge_{0\leq i\neq j<n}a_{ij}x_i-b_{ij}x_j\prec c_{ij}$,$q'$为 H 的一种控制状态,满足对任意的 $0<i<n$,$act(q')_i=act(q)_i$,则 D':

$$x_0=0\wedge x_0-x_n\prec c_{0n}\wedge x_n-x_0\prec c_{n0}\wedge\bigwedge_{0\leq i\neq j<n}a_{ij}x_i-b_{ij}x_j\prec c_{ij}$$

为一具有 q'-性质的 q'-区域,其中,c_{0n} 和 c_{n0} 为两个满足 $c_{0n}+c_{n0}\geq 0$ 的有理数.

证明:与引理 3 类似,很容易证明 D'是一个 q'-区域,下面我们重点证明其 q'-性质.令 l_i 和 r_i 分别表示 $act(q)_i$ 的左、右端点.我们仅证明任意 $l_i>0$ 的情形,其他情形证明类似.假设 D'的正则型为

$$x_0=0\wedge\bigwedge_{0<i\le n}(x_0-x_i\prec c_{0i}\wedge x_i-x_0\prec c_{i0})\wedge\bigwedge_{0<i\ne j\le n}(l_jx_i-r_ix_j)/gcd(l_j,r_i)\prec c_{ij},$$

其中对任意 $0<i<n$,有 $c_{in}=(l_nc_{i0}+r_ic_{0n})/gcd(l_n,r_i)$ 和 $c_{ni}=(l_ic_{n0}+r_nc_{0i})/gcd(l_i,r_n)$ 成立,因此,对任意 $0<k\ne j\le n$, $r_kc_{0j}\le\tilde g(l_j,r_k)c_{kj}+l_jc_{0k}$.由于 D 具有 q-性质,则对任意 $0<i\ne k\ne j<n$,

$$\tilde g(l_j,r_i)l_kc_{ij}+(r_kr_i-l_kr_i)c_{0j}\le\tilde g(l_k,r_i)l_jc_{ik}+\tilde g(l_j,r_k)r_ic_{kj}\tag{2}$$

因此,为了证明 D'具有 q'-性质,我们仅需证明用 n 替代不等式(2)中的 k,i 或 j 后,该不等式仍然成立.我们仅证明 $\tilde g(l_j,r_i)l_nc_{ij}+(r_nr_i-l_nr_i)c_{0j}\le\tilde g(l_n,r_i)l_jc_{in}+\tilde g(l_j,r_n)r_ic_{nj}$ 成立,其他形式的不等式的证明类似.由于 D'非空,因此,对于任意 $0<j\le n$,有 $c_{j0}+c_{0j}\ge0$ 成立,进而,$\tilde g(l_j,r_i)l_nc_{ij}+(r_nr_i-l_nr_i)c_{0j}\le l_n(l_jc_{i0}+r_ic_{0j})+(r_nr_i-l_nr_i)c_{0j}=l_nl_jc_{i0}+r_nr_ic_{0j}\le l_nl_jc_{i0}+r_nr_ic_{0j}+l_jr_i(c_{n0}+c_{0n})=l_j(l_nc_{i0}+r_ic_{0n})+r_i(l_jc_{n0}+r_nc_{0j})\le\tilde g(l_n,r_i)l_jc_{in}+\tilde g(l_j,r_n)r_ic_{nj}$. □

定理 3. 给定矩形自动机 H 的控制状态 $p,q\in Q$,设 D 为一个具有 p-性质的 p-区域, $e=(p,q)$ 为一条边,则 $Reset_e[D]$ 为一具有 q-性质的 q-区域.

证明:设 $update(e)=\{j_1,...,j_m\}$, $\{0,...,n\}\setminus update(e)=\{i_1,...,i_h\}$,$D$ 的正则型由公式(1)表示.由引理 1,

$$Reset_e[D]=\exists x_{j_1}\in reset(e)_{j_1}...\exists x_{j_m}\in reset(e)_{j_m}[D]$$

等价于

$$x_0=0\wedge\bigwedge_{1\le k\ne l\le h}a_{i_ki_l}x_{i_k}-b_{i_ki_l}x_{i_l}\prec c_{i_ki_l}\wedge\bigwedge_{1\le k\le m}x_{j_k}\in reset(e)_{j_k}.$$

由初始化矩形自动机的定义可知,对 $\forall k\in\{1,...,n\}\setminus update(e)$,有 $act(p)_k=act(q)_k$ 成立.由引理 4,该定理成立. □

3 不同上限矩阵

为了在计算机中存储混合区域,我们定义一种称为不同上限矩阵的矩阵数据结构.存储混合区域 D 的不同上限矩阵Γ的每个元素 $\Gamma_{ij}(0\le i\ne j\le n)$ 为 $(a_{ij},b_{ij},d_{ij},\prec_{ij})$,表示 D 中的不等式 $a_{ij}x_i-b_{ij}x_j\prec_{ij}d_{ij}$; $\Gamma_{ii}(0\le i\le n)$ 为 $(1,1,d,\prec)$.其中,索引 0 的作用与混合区域中的 x_0 是一样的.假设混合区域 D 由公式(1)表示,可以很容易地构造不同上限矩阵Γ来表示 D:

- 对于任意的 $0\le i\ne j\le n$, $\Gamma_{ij}=(a_{ij},b_{ij},c_{ij},\prec)$,
- 对于任意的 $0\le i\le n$, $\Gamma_{ii}=(1,1,0,\le)$.

给定一个不同上限矩阵Γ,如果它表示的混合区域是正则的,我们称Γ是正则的.引理 2 给出了求解不同上线矩阵的正则型的一种方法.第 2 节证明了混合区域可以作为矩形混合系统符号化可达性分析的基本操作单位,并且混合区域是由不同上限矩阵表示的,因此,我们可以用不同上限矩阵实现矩形混合系统的 3 种可达性操作.

3.1 交操作

给定矩形自动机 H 的一个控制状态 $q\in Q$ 以及两个正则的不同上限矩阵 Γ^1 和 Γ^2 表示的 q-区域.设 $\Gamma^1_{ij}=(a,b,c_1,\prec_1)$, $\Gamma^2_{ij}=(a,b,c_2,\prec_2)$.则 $\Gamma=\Gamma^1\wedge\Gamma^2$ 的元素Γ_{ij}应为 $(a,b,\min(c_1,c_2,)\prec)$,其中,$\prec$定义如下:

- 如果 $c_1<c_2$,则 $\prec=\prec_1$;
- 如果 $c_2<c_1$,则 $\prec=\prec_2$;
- 如果 $c_1=c_2$,并且 $\prec_1=\prec_2$,则 $\prec=\prec_1$;
- 如果 $c_1=c_2$,并且 $\prec_1\ne\prec_2$,则 $\prec=<$.

3.2 变量重赋值操作

给定矩形自动机 H 的边 $e=(q,q')$,以及正则的不同上限矩阵 Γ 表示的 q-区域.设 $\Gamma_{ij}=(a_{ij},b_{ij},c_{ij},\prec_{ij})$, $reset(e)_k=-x_k\prec_k\mu_k\wedge x_k\prec'_k\nu_k$,其中 $k\in update(e)$,则 $\Gamma'=Reset_e(\Gamma)$ 的元素 Γ'_{ij} 应为:

- 对于 $i\in update(e)$ 或 $j\in update(e)$ 满足 $i\ne j$ 和 $i\cdot j\ne0$, $\Gamma'_{ij}=(a_{ij},b_{ij},\infty,<)$,其中 a_{ij} 和 b_{ij} 满足 q'-区域的定义.

- 对于 $(i\neq j)\notin update(e)$, $\Gamma'_{ij}=\Gamma_{ij}$.
- 对于 $i\in update(e)\wedge 0<i\leq n$, $\Gamma'_{0t}=(1,1,\mu_i,\prec_i)$; $\Gamma'_{i0}=(1,1,\nu_i,\prec'_i)$.
- 对于 $0\leq i\leq n$, $\Gamma'_{ij}=\Gamma_{ij}$.

3.3 时间流逝操作

给定矩形自动机 H 的一个控制状态 $q\in Q$ 以及一个正则的不同上限矩阵Γ表示的 q-区域.设 $\Gamma_{ij}=(a_{ij},b_{ij},c_{ij},\prec_{ij})$,则 $\Gamma'=\Gamma^{\uparrow_q}$ 的元素 Γ'_{ij} 定义如下:

- 对于 $i\neq 0$,当 $l_i\geq 0$ 时, $\Gamma'_{i0}=(1,1,\infty,<)$, $\Gamma'_{i0}=\Gamma_{0i}$;当 $r_i\leq 0$ 时, $\Gamma'_{i0}=\Gamma_{i0}$, $\Gamma'_{0i}=(1,1,\infty,<)$.
- 对于 $i=j=0$ 或 $i\cdot j\neq 0$, $\Gamma'_{ij}=\Gamma_{ij}$.

以上 3 种操作产生的新的不同上限矩阵可能不是正则的,因此,在每次操作完成之后,必须重新计算新产生的不同上限矩阵的正则型.给定由公式(1)表示的混合区域 D,计算每个不等式 $a_{ij}x_i-b_{ij}x_j\prec c_{ij}$ 的正则型等价于计算 $f(x_i,x_j)=a_{ij}x_i-b_{ij}x_j$ 在多面体 D 上的最大值.求解线性函数在多面体空间上的最值问题是线性规划的研究课题,可以利用文献[16]中的算法加以解决,该算法的复杂度为 $O(n^{3.5}L^2)$,其中 L 为存储多面体需要的内存容量.进而,计算混合区域的正则型可以在 $O(n^{5.5}L^2)$ 的复杂度内完成.

4 非线性混合系统的可达性分析

非线性混合系统是一般意义上的混合系统.由于非线性混合系统变量形式的多样性(多项式函数变量是非线性变量,指数函数变量是非线性变量等等),要给出一种形式统一的,类似于时间区域,混合区域或一般多面体的结构来表示非线性混合系统的可达状态集是非常困难的.目前,非线性混合系统的可达性问题还没有很好的解决办法,对这个问题的探索性研究仅限于用线性混合系统近似模拟非线性混合系统,从而给出一个非线性混合系统状态可达的必要条件,即与其近似的线性混合系统的对应状态可达.

目前主要有两类近似模拟非线性混合系统的方法:时间转换方法(time translation)和斜率转换方法(rate translation)[11].时间转换方法用时间变量模拟非线性变量,用时间自动机模拟非线性自动机.斜率转换方法主要用线性变量模拟非线性变量,用线性自动机模拟非线性自动机.这两种办法都对非线性混合系统的变量作了很大的限制,要求在每个控制状态上非线性变量必须严格单调,并且经过重新赋值后值必须唯一.这样,很多非线性混合系统都是不适用的.本文给出了一种新的办法,用矩形自动机近似模拟非线性自动机,然后用混合区域解决矩形自动机的可达性问题,从而给出非线性混合自动机可达性问题的一个必要条件.我们仅要求非线性混合系统的每个控制状态上连续变量为分段光滑的有界变量.

对于两个混合自动机 A_1 和 A_2,设 S_1 和 S_2 分别是 A_1 和 A_2 的状态集合.如果存在一种关系 $\ll\subseteq S_1\times S_2$ 满足如下条件,则称 A_2 时间模拟 A_1:

- 对于任意 $s_1\in S_1$ 和 $s_2\in S_2$,如果 $s_1\ll s_2$,并且存在 $s'_1\in S_1$,使得 s_1 到 s'_1 可达,则必存在 $s'_2\in S_2$ 使得 s_2 到 s'_2 可达.
- 对于任意 $s_1=(q\in Q_1,v\in init_1(q))$,存在 $s_2=(q'\in Q_2,v'\in init_2(q'))$,使得 $s_1\ll s_2$.

给定非线性混合自动机 A,我们分两步构造一个矩形自动机 A_H 来近似模拟 A.第 1 步,我们利用一个控制状态分裂操作 *flow* 来构造一个分裂自动机 *flow*(A);第 2 步,我们构造分裂自动机 *flow*(A)的近似矩形自动机 A_H.每一步,我们都保证构造的自动机可以根据时间模拟原自动机.

对于混合自动机 $A=(Q,X,init,E,inv,act,jump,update,reset)$,一个控制状态分裂操作 *flow* 是一个定义域为 Q 的函数.对于任意的 $q\in Q$, $flow(q)=\{flow_1^q,...,flow_k^q\}$,其中任意的 $flow_i^q$ 都是一个 X 上的断言,并且 $\{|flow_1^q|,...,|flow_k^q|\}\in 2^{R^n}$ 为 $|inv(q)|$ 的一个闭包集.基于控制状态分裂操作 *flow*,可以构造 A 的分裂自动机 $flow(A)$: $(Q_f,X_f,init_f,E_f,inv_f,act_f,jump_f,update_f,reset_f)$,其中:

- $Q_f=\{(q,\varphi)\,|\,q\in Q,\varphi\in flow(q)\}$, $X_f=X$.

- 对于任意的 $(q,\varphi)\in Q_f$, $init_f((q,\varphi))=init(q)\wedge\varphi$.
- 对于任意的 $q,q'\in Q$, $E_f=E_1\cup E_2$, 其中 $E_1=\{((q,\varphi),(q',\varphi'))\mid(q,q')\in E,\varphi\in flow(q),\varphi'\in flow(q')\}$, $E_2=\{((q,\varphi),(q,\varphi'))\mid\varphi,\varphi'\in flow(q)\}$.
- 对于任意的 $e=((q,\varphi),(q',\varphi'))\in E_1$, $jump_f(e)=jump((q,q'))\wedge\varphi$, $update_f(e)=update((q,q'))$, $reset_f(e)=reset((q,q'))\wedge\varphi'$,对于 $e=((q,\varphi),(q,\varphi'))\in E_2$, $jump_f(e)=\text{true}$, $update_f(e)=\varnothing$, $reset_f(e)=\text{true}$.
- 对于任意的 $(q,\varphi)\in Q_f$, $inv_f((q,\varphi))=inv(q)\wedge\varphi$, $act_f((q,\varphi))=act(q)$.

如果对于混合自动机 A 的任意的控制状态分裂操作 $flow$,都有 $flow(A)$与 A 相互时间模拟,则称 A 是可分的.

定理 4. 任意的混合自动机都是可分的.

证明:该定理的证明可参照文献[11]中的 Theorem 2.2.

对于两个混合自动机 $A_1=(Q_1,X_1,init_1,E_1,inv_1,act_1,jump_1,update_1,reset_1)$ 和 $A_2=(Q_2,X_2,init_2,E_2,inv_2,act_2,jump_2,update_2,reset_2)$,如果如下条件成立,则称 A_2 近似于 A_1:

- $Q_1=Q_2$, $X_1=X_2$, $E_1=E_2$.
- 对任意的控制状态 q, $init_1(q)$ 蕴涵 $init_2(q)$, $act_1(q)$ 蕴涵 $act_2(q)$, $inv_1(q)$ 蕴涵 $inv_2(q)$.
- 对于任意的边 e, $update_1(e)=update_2(e)$, $jump_1(e)$ 蕴涵 $jump_2(e)$, $reset_1(e)$ 蕴涵 $reset_2(e)$.

引理 5. 对于两个混合自动机 A_1 和 A_2,如果 A_2 近似于 A_1,则 A_2 时间模拟 A_1.

证明:该引理的证明可参照文献[11]中的 Proposition 4.1.

给定一个非线性混合自动机 A,取出变量集 X 中的某个变量 $x_i(i\in\{1,...,n\})$,我们按照如下两个步骤构造与 A 近似的自动机 $A_{\{x_i\}}$.

第 1 步:对于任意的 $q\in Q$,令 $E_q=\{(q',q)\in E\mid q'\in Q\}$, $\xi(q)_i=\{\iota\mid\iota$ 为 $|init(q)_i|$ 或 $|reset(e)_i|$ 的端点, $e\in E_q\}$.对于任意的 $\mu_j\in\xi(q)_i$,假设 $f_j^{x_i}$ 是满足微分条件 $act(q)$ 和初始条件 $f_j^{x_i}(0)=\mu_j$ 的函数,令 q 上 x_i 的边界极值集合 $\varpi(q)_i$ 为所有的 $f_j^{x_i}$ 在值域 $f_j^{x_i}\in|inv(q)_i|$ 上的极值的集合.设 $\bigcup_{q\in Q}\varpi(q)_i=\{m_1,...,m_l\}$,其中 $m_1<...<m_l$,令 $split_A^i(q)=\{x_i\le m_1\wedge inv(q),m_1\le x_i\le m_2\wedge inv(q),...,m_{l-1}\le x_i\le m_l\wedge inv(q),\ x_i\ge m_l\wedge inv(q)\}$,定义 A 的控制状态分裂函数 $flow$ 为:对任意的 $q\in Q$, $flow(q)=\{\varphi\in split_A^i(q)\mid\exists v,v'\in V.\ (v,v'\in|\varphi|\wedge v(x_i)\ne v'(x_i))\}$.然后,按照分裂自动机的构造规则构造 A 对应的分裂自动机 $flow(A)$:$(Q_f,X_f,init_f,E_f,inv_f,act_f,jump_f,update_f,reset_f)$.

第 2 步:对于第 1 步中构造的自动机 $flow(A)$,按照如下规则构造其近似自动机 $A_{\{x_i\}}=(Q_{\{x_i\}},X_{\{x_i\}},init_{\{x_i\}},E_{\{x_i\}},inv_{\{x_i\}},act_{\{x_i\}},jump_{\{x_i\}},update_{\{x_i\}},reset_{\{x_i\}})$:

- $Q_{\{x_i\}}=Q_f$, $X_{\{x_i\}}=X_f$, $E_{\{x_i\}}=E_f$.
- 对于任意的 $(q,\varphi)\in Q_f$,设 $[a,b]=|init_f((q,\varphi))_i|$, $[c,d]=|inv_f((q,\varphi))_i|$, $[l,h]$ 是 $\dot{x}_i$ 在微分条件 $act(q)$ 和限制条件 φ 下的取值范围, a', c' 和 l' 分别是小于 a,c 和 l 的最大整数, b', d' 和 h' 分别是大于 b,d 和 h 的最小整数,构造 $init_{\{x_i\}}((q,\varphi))=\exists x_i\in[a',b'][init_f((q,\varphi))]$, $act_{\{x_i\}}((q,\varphi))=\exists\dot{x}_i\in[l',h'][act_f((q,\varphi))]$, $inv_{\{x_i\}}((q,\varphi))=\exists x_i\in[c',d'][inv_f((q,\varphi))]$.
- 对于任意的 $e=((q,\varphi),(q',\varphi'))\in E_f$,设 $[a,b]=|reset_f(e)_i|$, $[c,d]=|jump_f(e)_i|$, a' 和 c' 分别是小于 a 和 c 的最大整数, b' 和 d' 分别是大于 b 和 d 的最小整数,构造 $update_{\{x_i\}}(e)=update_f(e)$, $reset_{\{x_i\}}(e)=\exists x_i\in[a',b'][reset_f(e)]$, $jump_{\{x_i\}}(e)=\exists x_i\in[c',d'][jump_f(e)]$.

对于 A 的近似自动机 $A_{\{x_i\}}$,取出 $X\setminus\{x_i\}$ 中的某个变量 x_j,重复上面的两个步骤构造 $A'_{\{x_i\}}$ 的近似自动机 $A_{\{x_i,x_j\}}$.然后取出 $X\setminus\{x_i,x_j\}$ 中的某个变量 x_k,重复上面的两个步骤构造 $A_{\{x_i,x_j\}}$ 的近似自动机 $A_{\{x_i,x_j,x_k\}}$,如此继续下去,直到构造出 A 的近似矩形自动机 A_X.

定理 5. 给定一个非线性混合自动机 A,设 A_H 是按照上面的规则构造的 A 的近似矩形自动机,则 A_H 时间模拟 A.

证明:由定理 4 和引理 5,该定理成立.

为了检验非线性混合自动机 A 的两个状态 s_1 和 s_2 是否可达,我们考虑 A 的近似矩形自动机 A_H 的两个对应状态 s_1' 和 s_2' 的可达性问题.如果 s_1' 到 s_2' 不可达,则 s_1 到 s_2 一定不可达.如果 s_1' 到 s_2' 可达,则 s_1 到 s_2 未必可达.这实际上给出了非线性混合系统可达性问题的一个必要条件,但是通过逐步求精,提高线性变量模拟非线性变量的近似度,我们也可以很好地判定非线性混合系统的可达性问题.

5 相关工作与结论

目前,对混合系统可达性问题的研究主要集中在线性混合系统领域.为了表示可达集,文献[6−9]采用了普通多面体,文献[10]采用 polytopes.为了计算可达集,它们都使用量词消去运算.量词消去运算具有双指数级的复杂度,并且线性混合系统的可达性问题本身是不可判定的,所以相应的可达性分析算法是半确定的,对于某些状态并不能判定它们是否可达.文献[13,14]对矩形混合系统的可达性问题进行了研究,但只是从理论上证明了初始化的矩形混合系统的可达性问题是可判定的,并没有给出可行、有效的数据结构和判定算法,对具体的矩形混合系统的可达性判定问题,都是使用线性混合系统的验证工具 HyTech[7].文献[12]主要是解决了一类称为 zero loop-closed automata 的线性混合系统子集的可满足性问题.其主要精力没有放在进行可达性分析的数据结构上,与本文的研究领域不同.文献[11]对非线性混合系统的可达性分析进行了探索性的研究,并给出了两种解决办法,一是用实时系统近似模拟非线性混合系统,二是用线性混合系统近似模拟非线性混合系统,只是这两种方法都对非线性混合系统进行了严格的限制,要求变量在每个控制状态上必须严格单调,并且初始值唯一.

本文研究初始化的矩形混合系统的可达性问题,并利用它近似模拟非线性混合系统,给出了一种非线性混合系统的可达性分析方法.虽然初始化的矩形混合系统没有线性混合系统的适用面广,但其可达性问题是可判定的.本文给出了一种形式化结构,也就是混合区域描述矩形混合系统的状态集,进行矩形混合系统的符号化可达性分析[17].使用混合区域的优点是,不用量词消去运算来计算可达集,这样就避开了双指数级的复杂度.由一个正则的混合区域计算可达的混合区域的方法是很直接的,这里的主要问题就是求解混合区域的正则型问题,这其实就是线性规划问题,可以利用多项式复杂度的算法来解决.使用矩形混合系统近似模拟非线性混合系统,我们仅要求非线性混合系统的每个控制状态上的连续变量为分段光滑的有界变量,因此它比现存的模拟方法具有更大的适用范围.我们下一步的工作是首先对混合区域正则型的求解算法作进一步的研究,以找出更适合求解混合区域正则型、复杂度更低的算法;其次,对非线性混合系统的近似模拟方法进行研究,以提高近似度,使非线性混合系统的可达性判定问题达到更高的精确度.

References:

[1] Duan ZH. Modeling of Hybrid Systems. Beijing: Science Press, 2005.

[2] Henzinger TA, Majumdar R. Symbolic model checking for rectangular hybrid systems. In: Graf S, Schwartzbach M, eds. Proc. of the 6th Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems. LNCS 1785, Berlin: Springer-Verlag, 2000. 142−156.

[3] Li GY. LTLC: A continuous-time temporal logic for real-time and hybrid systems [Ph.D. Thesis]. Beijing: Institute of Software, the Chinese Academy of Sciences, 2001 (in Chinese with English abstract).

[4] Jr Clarke EM, Grumberg O, Peled DA. Model Checking. London: MIT Press, 1999.

[5] Dill DL. Timing assumptions and verification of finite-state concurrent systems. In: Sifakis J, ed. Proc. of the Int'l Workshop on Automatic Verification Methods for Finite State Systems. LNCS 407, Berlin: Springer-Verlag, 1990. 197−212.

[6] Wang F. Symbolic parametric safety analysis of linear hybrid systems with BDD-like data-structures. In: Alur R, Peled D, eds. Proc. of the 16th Int'l Conf. on Computer Aided Verification. LNCS 3114, Berlin: Springer-Verlag, 2004. 295−307.

[7] Frehse G. PHAVer: Algorithmic verification of hybrid systems past HyTech. In: Morari M, Thiele L, eds. Proc. of the 8th Int'l Workshop on Hybrid Systems: Computation and Control. LNCS 3414, Berlin: Springer-Verlag, 2005. 258−273.

[8] Alur R, Courcoubetis C, Halbwachs N, Henzinger TA, Ho PH, Nicollin X, Olivero A, Sifakis J, Yovine S. The algorithmic analysis of hybrid systems. Theoretical Computer Science, 1995,138:3−34.

[9] Alur R, Courcoubetis C, Henzinger TA, Ho PH. Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. In: Morari M, Thiele L, eds. Proc. of the Hybrid Systems. LNCS 736, Berlin: Springer-Verlag, 1993. 209−229.

[10] Chutinan A, Krogh BH. Verification of polyhedral-invariant hybrid automata using polygonal flow pipe approximations. In: Vaandrager FW,van Schuppen JH, eds. Proc. of the 2th Int'l Workshop on Hybrid Systems: Computation and Control. LNCS 1569, Berlin: Springer-Verlag, 1999. 76−90.

[11] Henzinger TA, Ho PH, W Toi H. Algorithm analysis of nonlinear hybrid systems. In: Wolper P, ed. Proc. of the 7th Int'l Conf. on Computer Aided Verification. LNCS 939, Berlin: Springer-Verlag, 1995. 225−238.

[12] Li XD, Pei Y, Zhao JH, Li Y, Zheng T, Zheng GL. Efficient verification of a class of linear hybrid automata using linear programming. In: Margaria T, Melham T, eds. Proc. of the 11th Advanced Research Working Conf. on Correct Hardware Design and Verification Methods. LNCS 2144, Berlin: Springer-Verlag, 2001. 465−479.

[13] kopke PW. The thoery of rectangular hybrid automata [Ph.D. Thesis]. Cornell University, 1996.

[14] Henzinger TA, Kopke PW, Puri A, Varaiya P. What's decidable about hybrid automata? Journal of Computer System Sciences, 1998,57:94−124.

[15] Behrmann G, Larsen KG, Pearson J, Weise C, Yi W. Efficient timed reachability analysis using clock diffierence diagrams. In: Halbwachs N, Peled D, eds. Proc. of the 11th Int'l Conf. on Computer Aided Verification. LNCS 1633, Berlin: Springer-Verlag, 1999. 341−353.

[16] Karmarkar N. A new polynomial-time algorithm for linear programming. Combinatorica, 1984,4(4):373−395.

[17] Zhang HB, Duan ZH. Symbolic algorithm analysis of rectangular hybird systems. In: Agrawal M, *et al*., eds. Proc. of the 5th Annual Conf. on Theory and Applications of Models of Computation. LNCS 4978, Berlin: Springer-Verlag, 2008. 294−305.

附中文参考文献:

[3] 李广元.LTLC:面向实时与混成系统的连续时序逻辑[博士学位论文].北京:中国科学院软件研究所,2001.

张海宾(1981－),男,陕西西安人,博士,讲师,主要研究领域为混合系统,形式化方法.

段振华(1948－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为可信软件理论与技术,混合系统,网络计算,嵌入式系统.