

多速率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, 710071, 西安)

摘要: 针对目前还没有专门的数据结构处理多速率混合系统的符号化可达性问题, 定义了多速率区域来表示和处理多速率自动机的无穷状态空间, 从而把多速率混合系统的符号化可达性分析等价地转化成多速率区域上的3种操作, 即并操作、变量重赋值操作和控制状态上的时间流逝操作。从理论上证明了多速率区域在这3种操作上的封闭性, 同时定义了矩阵数据结构不同上限矩阵(DCM), 并用其存储多速率区域, 这样就得到了一种专门处理多速率混合系统符号化可达性分析的数据结构。理论上证得, DCM可以大大降低可达性分析算法的复杂度。

关键词: 混合系统; 多速率自动机; 可达性分析

中图分类号: TP301 **文献标识码:** A **文章编号:** 0253-987X(2007)04-0412-04

Symbolic Reachability Analysis of Multirate Hybrid Systems

Zhang Haibin, Duan Zhenhua

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

Abstract: Aiming at the problem that no special data structure has been proposed to deal with the symbolic reachability analysis of multirate hybrid systems yet, a constraint system called multirate zone is defined for the representation and manipulation of multirate automata state-spaces. A multirate zone is a conjunction of inequalities representing sets of states. Multirate zones are used as the basis for the state reachability analysis algorithm for multirate automata, which enable the algorithm to be expressed in terms of three operations in multirate zones. The operations include intersection, variable reset and elapsing of time. To present multirate zones, a matrix data structure called DCM (difference constraint matrix) is defined. Using DCM as a data structure for the reachability analysis algorithm for multirate automata, the complexity can considerably be decreased.

Keywords: hybrid system; multirate automata; reachability analysis

混合系统(Hybrid System)是一种既包含离散变量又包含连续变量的计算系统^[1-2], 如飞机着陆控制系统、核电站控制系统等数控系统就是典型的代表。研究混合系统的可达性问题就是判定系统是否可以由一个初始状态开始, 经过某个路径到达给定的状态。可达性分析是混合系统安全性验证、模型检查等的基础, 而符号化可达性分析处理符号化状态, 并检验混合系统是否可以到达满足某个状态公式的状态^[3]。一个符号化状态实际上是一组混合系统状

态的集合。

矩形混合系统的可达性问题是可判定的, 它是具有此类性质混合系统的最大子集, 实时系统是矩形混合系统的最小子集, 它们的符号化可达性分析处理的符号化状态是二元组 (q, D) 。通常, 广泛采用凸多面体 D 来分析矩形混合系统符号化可达性分析, 凸多面体是由形如 $\sum_i a_i x_i < c$ 的线性不等式联立表示的线性区域, 而多速率混合系统是大于实

时系统的矩形混合系统的子集系统,目前还没有合适的符号化状态来处理这种多速率混合系统,尽管可以采用凸多面体,但凸多面体的不等式没有确定的选取范围,相应的处理算法也就可能有指数级的复杂度.

本文定义了多速率区域,以解决多速率混合系统的符号化可达性问题.由于多速率区域的不等式有确定的范围,所以多速率混合系统的可达性分析算法就可以在多项式复杂度范围内完成.

1 多速率自动机的语法和语义

多速率自动机^[2,4-5]是描述多速率混合系统的最成功的数学模型,它是一个六元组 $(Q, \text{Init}, X, E, \kappa, \text{inv})$,其中: Q 是一个有穷控制状态集; X 是有穷连续变量集; $\text{Init} \subseteq Q \times Z^n$ 是初始状态集; E 是转换关系集(它的每个元素都形如 $(q, \varphi, \lambda, \zeta, q')$, φ 是 n 维空间上的一个矩形区域, ζ 是一个 n 维向量, $\lambda \subseteq \{1, \dots, n\}$; $\text{inv}: Q \rightarrow B_n$ 表示连续变量在每个控制状态上应满足的约束条件(B_n 是 n 维矩形集合); $\kappa: Q \rightarrow Z^n$ 表示在每个控制状态上连续变量的斜率.关于多速率混合系统的详细定义可参考文献^[2,4-5].

一个指派是一个赋值方程,它把每个连续变量赋予一个特定的实数值,并用 V 表示所有指派的集合.对于 $v \in V, d \in R^+, v + ld$ 表示指派 v' 满足 $v'(x_i) = v(x_i) + l_i d$,其中 $x_i \in X$.对于 $\beta \subseteq \{1, \dots, n\}, [\beta \square \zeta]v$ 表示指派 v'' 满足 $v''(x_i) = \zeta_i, i \in \beta$,而 $v''(x_j) = v(x_j), j \in \{1, \dots, n\} \setminus \beta$.

可以用一个无穷状态空间的转换系统对多速率自动机进行语义解释^[4].用计算机来处理多速率自动机,需给出一个基于符号状态 (q, D) 的符号语义解释,这种解释应基于以下2种符号转换

$$\begin{aligned} (q, D) &\rightarrow (q, (D \wedge \text{inv}(q))^{\uparrow q}) \\ (q, D) &\rightarrow (q', \lambda(D \wedge \text{inv}(q) \wedge \varphi) \wedge \text{inv}(q')) \\ e &= (q, \varphi, \lambda, \zeta, q') \in E \end{aligned}$$

它们分别对应于多速率自动机的延迟转换和跳跃转换,而时间操作 $D^{\uparrow q} = \{u + ld \mid u \in D \wedge l = \kappa(q) \wedge d \in R^+\}$,变量重新赋值操作 $\lambda(D) = \{[\lambda \square \zeta]u \mid u \in D\}$.

2 多速率区域

多速率区域是形如 $ax - by < c, x < c, c < x$ 的一系列不等式的合取,其中 $<$ 为 $<$ 或 $\leq$, a 和 b 为整数, c 是有理数.在每个控制状态 q 上,多速率区域就是 q 区域,定义如下.

定义 1 q 区域的一般形式为

$$x_0 = 0 \wedge \bigwedge_{0 \leq i \neq j \leq n} k_j x_i - k_i x_j < c_{ij}$$

式中: x_0 是一个特殊的变量,其值恒为0; $k_i = \kappa(q)_i$ ($0 \leq i \leq n, k_0 = 1$); c_{ij} 为有理数.

称 $(<, c)$ 为一个边界,如果 $c < c'$ 或 $c = c' \wedge < = ' < ' \wedge < ' = ' \leq '$,则称 $(<, c)$ 比 $(<', c')$ 更紧凑,表示为 $(<, c) \sqsubset (<', c')$.给定多速率区域 D ,如果 D 中的任意不等式 $ax - by < c$ 不存在边界 $(<', c')$,使得 $ax - by < ' c'$ 可以由 D 中的其他不等式联立推出,此时 D 是规范的.

多速率区域上的3种操作定义如下,其中 $e = (q, \varphi, \lambda, \zeta, q')$ 为一条边.

并操作: $D \wedge D'$.

变量重赋值操作: $D_e[\lambda \square \zeta]$ 表示由 D 中的某个指派通过重新赋值 $x_i \in X (i \in \lambda)$ 为 ζ_i 而得到的指派.

控制状态 q 上的时间流逝操作: $D^{\uparrow q}$ 表示由 D 中的某个指派随时间流逝而得到的指派.

以上3种操作是多速率混合系统符号化可达性分析所必需的3个算子,下述的定理和引理确保了多速率区域在这3种操作上是封闭的.

定理 1 如果 D 和 D' 是2个 q 区域,那么 $D \wedge D'$ 仍是一个 q 区域.

证明 该定理的证明很直接,所以在此不作详述.

引理 1 如果 D 是一个变量集 X 上的 q 区域,那么对于自由变量 $x_r \in X, \exists x_r[D]$ 是变量集 $X \setminus \{x_r\}$ 上的 q 区域.

证明 不失一般性,可证得 $r = n$ 的情况.当 $k_n = 0$ 时,引理显然成立;否则,假设 D 可表示为

$$x_0 = 0 \wedge \bigwedge_{0 \leq i \neq j \leq n} k_j x_i - k_i x_j < c_{ij} \quad (1)$$

可证得 $\exists x_n[D]$ 等价于

$$\begin{aligned} x_0 = 0 \wedge \bigwedge_{0 \leq i \neq j < n} k_j x_i - k_i x_j < c_{ij} \wedge \\ \bigwedge_{0 \leq i \neq j < n} k_j x_i - k_i x_j < d_{ij} \end{aligned} \quad (2)$$

如果 $k_n \geq 0$,则

$$\left. \begin{aligned} d_{ij} &= (k_j c_{in} + k_i c_{nj}) / k_n, & k_{\geq 0} \wedge k_{\geq 0} \\ d_{ij} &= (k_i c_{nj} + k_j c_{ni}) / k_n, & k_{\geq 0} \wedge k_{\leq 0} \\ d_{ij} &= (k_j c_{in} - k_i c_{jn}) / k_n, & k_{\leq 0} \wedge k_{\geq 0} \\ d_{ij} &= (-k_j c_{ni} - k_i c_{jn}) / k_n, & k_{\leq 0} \wedge k_{\leq 0} \end{aligned} \right\}$$

如果 $k_n < 0$,则

$$\left. \begin{aligned} d_{ij} &= (-k_j c_{ni} - k_i c_{jn}) / k_n, & k_{\geq 0} \wedge k_{\geq 0} \\ d_{ij} &= (k_j c_{in} - k_i c_{jn}) / k_n, & k_{\geq 0} \wedge k_{\leq 0} \\ d_{ij} &= (k_i c_{nj} - k_j c_{ni}) / k_n, & k_{\leq 0} \wedge k_{\geq 0} \\ d_{ij} &= (k_j c_{in} + k_i c_{nj}) / k_n, & k_{\leq 0} \wedge k_{\leq 0} \end{aligned} \right\}$$

在如下的证明中省略了等式 $x_0=0$ 的情形,而仅证明 $k_i>0(0<i\leq n)$ 的情形,其他的证明类似.

首先证明当 v 在满足 $\exists x_n[D]$ 的 $x_1, \dots, x_{n-1}$ 的指派时, v 满足式(2). 为此,式(1)重写为

$$\bigwedge_{0\leq i\neq j\leq n} k_j x_i - k_i x_j < c_{ij} \wedge \bigwedge_{0\leq i\leq n} k_n x_i - k_i x_n < c_{in} \wedge \bigwedge_{0\leq j\leq n} k_j x_n - k_n x_j < c_{nj}$$

由于

$$\begin{aligned} & \bigwedge_{0\leq i\leq n} k_n x_i - k_i x_n < c_{in} \wedge \bigwedge_{0\leq j\leq n} k_j x_n - k_n x_j < c_{nj} \Rightarrow \\ & \bigwedge_{0\leq i\neq j\leq n} k_n x_i - k_i x_n < c_{in} \wedge k_j x_n - k_n x_j < c_{nj} \Rightarrow \\ & \bigwedge_{0\leq i\neq j\leq n} k_n k_j x_i - k_j k_n x_j < k_j c_{in} + k_i c_{nj} \Rightarrow \\ & \bigwedge_{0\leq i\neq j\leq n} k_j x_i - k_i x_j < (k_j c_{in} + k_i c_{nj})/k_n \end{aligned}$$

而且不含变量 x_n , 因此可由 $\exists x_n[D]$ 推出式(2).

反之,证明满足式(2)的 $x_1, \dots, x_{n-1}$ 的指派也同样满足 $\exists x_n[D]$.

如果式(2)成立,那么 $\bigwedge_{0\leq i\neq j\leq n} k_j x_i - k_i x_j < (k_j c_{in} + k_i c_{nj})/k_n$ 成立. 由于 $k_i, k_j > 0$, 并且 $\bigwedge_{0\leq i\neq j\leq n} (k_n x_i - c_{in})/k_i < \min_{0\leq j\leq n} (k_n x_j + c_{nj})/k_j$, 因此 $\max_{0\leq i\leq n} (k_n x_i - c_{in})/k_i < \min_{0\leq j\leq n} (k_n x_j + c_{nj})/k_j$, 取 x_n 使得 $\max_{0\leq i\leq n} (k_n x_i - c_{in})/k_i < x_n < \min_{0\leq j\leq n} (k_n x_j + c_{nj})/k_j$, 则 $\bigwedge_{0\leq i\neq j\leq n} (k_n x_i - c_{in})/k_i < x_n < (k_n x_j + c_{nj})/k_j$, 进而 $\bigwedge_{0\leq i\leq n} k_n x_i - k_i x_n < c_{in} \wedge \bigwedge_{0\leq j\leq n} k_j x_n - k_n x_j < c_{nj}$. 所以, 由式(2)可以推出 $\exists x_n[D]$.

引理2 假设 q 区域的 D 可以表示为

$$x_0 = 0 \wedge \bigwedge_{0\leq i\neq j\leq n} k_j x_i - k_i x_j < c_{ij}$$

q' 为一个满足 $\kappa_i(q') = \kappa_i(q) (0 < i \leq n)$ 的控制状态, 那么

$$x_0 = 0 \wedge x_0 - x_n \leq -c \wedge x_n - x_0 \leq c \wedge \bigwedge_{0\leq i\neq j\leq n} k_j x_i - k_i x_j < c_{ij}$$

为一 q' 区域, 其中 c 是一个有理常数.

证明 该引理的证明很直接, 所以在此不作详述.

推论1 如果 D 为 q 区域, $e = (q, \varphi, \lambda, \zeta, q')$ 是一条边, 那么 $D_e[\lambda \square \zeta]$ 是一个 q' 区域.

定理2 如果 D 是 q 区域, 那么 $D^{\uparrow q}$ 仍然是 q 区域.

证明 假设 D 可以表示为

$$x_0 = 0 \wedge \bigwedge_{0\leq i\neq j\leq n} k_j x_i - k_i x_j < c_{ij}$$

略去等式 $x_0=0$, 则 $D^{\uparrow q}$ 可等价于

$$\exists t \geq 0 \left[\bigwedge_{0\leq i\neq j\leq n} k_j (x_i - \bar{k}_i t) - k_i (x_j - \bar{k}_j t) < c_{ij} \right]$$

其中 $\bar{k}_0=0, \bar{k}_i=k_i, i>0$. 该式同样等价于

$$\begin{aligned} & \exists t \geq 0 \left[\bigwedge_{0\leq i\leq n} (x_0 - x_i < c_{0i} - k_i t \wedge x_i - x_0 < c_{i0} + k_i t) \wedge \right. \\ & \left. \bigwedge_{0\leq i\neq j\leq n} k_j x_i - k_i x_j < c_{ij} \right] \end{aligned}$$

很明显, $D^{\uparrow q}$ 是 q 区域.

3 矩阵数据结构

为了用计算机来处理多速率区域, 需定义矩阵数据结构. 对于一个不同上限矩阵 (DCM) π , 它的每个元素 $\pi_{ij} (i \neq j)$ 都是元组 $(a_{ij}, b_{ij}, c_{ij}, <_{ij})$, 可以表示不等式 $a_{ij}x_i - b_{ij}x_j <_{ij} c_{ij}$, 其中 $<_{ij}$ 为 $<$ 或 $\leq$, 或者 $(<_{ij}, c_{ij})$ 为 $(<, \infty)$. 对于 $i \leq n, \pi_{ii}$ 具有形式 $(1, 1, c, <)$, 其中 c 为一有理数.

给定一个 π , 如果 π 表示的多速率区域是规范的, 则 π 为规范的. 与不同边界矩阵 (DBM)^[6] 类似, 求解 DCM 的规范形式可以用 FloydWarshall 算法, 由于篇幅限制, 在此不作详述. 对于规范的 DCM, 下面定义 3 种操作, 它们分别对应多速率区域上的 3 种操作.

并操作: 定义 $\pi = \pi^1 \wedge \pi^2$, 假设 $\pi_{ij}^1 = (a_1, b_1, c_1, <_1), \pi_{ij}^2 = (a_2, b_2, c_2, <_2)$, 其中 $a_1 = a_2 \wedge b_1 = b_2$, 则 $\pi_{ij} = (a_1, b_1, \min(c_1, c_2), <)$, 故有

$$\begin{aligned} & < = <_1, \quad c_1 < c_2 \\ & < = <_2, \quad c_2 < c_1 \\ & < = <_1, \quad c_1 < c_2 \wedge <_1 = <_2 \\ & < = <, \quad c_1 < c_2 \wedge <_1 \neq <_2 \end{aligned}$$

变量重赋值操作: 假设 $\pi_{ij} = (a_{ij}, b_{ij}, c_{ij}, <_{ij})$, $e = (q, \varphi, \lambda, \zeta, q')$, $k_0=1$, 并且 $k_i = \kappa(q')_i$, 则 $\pi' = \pi_e[\lambda \square \zeta]$ 有如下情形.

如果 $i, j \in \lambda$, 则 $\pi'_{ij} = (k_j, k_i, (k_j \zeta_i - k_i \zeta_j), \leq)$.

如果 $i \in \lambda, j \notin \lambda$, 同时 $k_i \geq 0$, 则 $\pi'_{ij} = (k_j, k_i, (k_j \zeta_i - k_i c_{0j}), <_{0j})$, 否则 $\pi'_{ij} = (k_j, k_i, (k_j \zeta_i - k_i c_{j0}), <_{j0})$.

如果 $i \notin \lambda, j \in \lambda$, 同时 $k_j \geq 0$, 则 $\pi'_{ij} = (k_j, k_i, (k_j c_{i0} - k_i \zeta_j), <_{i0})$, 否则 $\pi'_{ij} = (k_j, k_i, (k_j c_{0i} - k_i \zeta_j), <_{0i})$.

如果 $i, j \notin \lambda$, 则 $\pi'_{ij} = \pi_{ij}$.

控制状态 q 上的时间流逝操作: 定义 $\pi' = \pi^{\uparrow q}$, 则有如下情形.

对于 $i \neq 0$, 如果 $k_i \geq 0$, 则 $\pi'_{0i} = \pi_{0i}, \pi'_{i0} = (1, 1, \infty, <)$; 如果 $k_i < 0$, 则 $\pi'_{i0} = \pi_{i0}, \pi'_{0i} = (1, 1, \infty, <)$.

对于 $i, j \neq 0$, 则 $\pi'_{ij} = \pi_{ij}$.

经由以上 3 种操作产生的 DCM 可能是不规范的, 因此在每一步操作完成之后必须把产生的 π 转换为规范的.

容易证得, 一个 π 表示的多速率区域是空集, 当且仅当至少存在主对角线上的一个元素 $\pi_{ii} = (1, 1,$

$c, <$) 满足 $(<, c) \subset (\leq, 0)$. 给定多速率自动机 M 和满足某个公式 ϕ 的状态 s , 就可以通过本文算法判定 s 是否可达, 算法步骤描述如下.

步骤 1: 初始化集合 Passed 为空集, Wait 为 (q_0, D_0) , 其中 (q_0, D_0) 为 M 的初始符号化状态.

步骤 2: 如果 $\text{Wait} = \emptyset$, 下转步骤 5; 否则, 取出 Wait 中的某个元素 (q, D) , 若 $D \Rightarrow \emptyset$, 下转步骤 4; 再则, 对于任意的 $(q', D') \in \text{Passed}$, 都有 $D \not\subseteq D'$. 故: ①将 (q, D) 添加到集合 Passed 之中; ②令集合 $\text{Next} = \{(q, D^{\uparrow q})\} \cup \{(q', [D \wedge \phi]_e) \mid e = (q, \varphi, \lambda, \zeta, q') \in E\}$, 并且把集合 Next 的所有元素都添加到集合 Wait 之中.

步骤 3: 重复步骤 2.

步骤 4: s 可达.

步骤 5: s 不可达.

该算法实际上是从 M 的初始符号化状态开始, 反复计算 π 之上的 3 种操作来判断 s 是否可达. 由于矩形混合系统的可达性问题是可判定的, 并且多速率混合系统是矩形混合系统的子集, 因此该算法必可终止.

4 结 论

本文定义了不等式系统的多速率区域, 同时通过定义矩阵数据结构来存储和处理多速率区域. 这样的—个数据结构不仅可以解决多速率混合系统的可达性问题, 相信它同样可以作为检查多速率混合

系统模型的数据结构.

参考文献:

- [1] Duan Zhenhua. Modeling of hybrid systems [D]. Western Bank, UK: Department of Computer Science, University of Sheffield, 1997.
- [2] Alur R, Henzinger T A, Lafferriere G, et al. Discrete abstractions of hybrid systems [J]. Proceedings of the IEEE, 2000, 88(7):971-984.
- [3] Zhang Haibin, Duan Zhenhua. Symbolic reachability analysis of rectangular hybrid systems[C]// The 2nd IEEE International Conference on Intelligent Computer Communication and Processing. Piscataway, USA: IEEE, 2006:240-248.
- [4] Alur R, Courcoubetis C, Henzinger T A, et al. Lecture notes in computer science 736—hybrid automata: an algorithmic approach to the specification and verification of hybrid systems [M]. London: Springer-Verlag, 1993:209-229.
- [5] Henzinger T A, Kopke P W, Puri A, et al. What's decidable about hybrid automata? [J]. Journal of Computer System Science, 1998, 57:94-124.
- [6] Dill D L. Timing assumptions and verification of finite-state concurrent systems [C]// Proceedings of the International Workshop on Automatic Verification Methods for Finite State Systems. London: Springer-Verlag, 1989:197-212.

(编辑 苗凌)

[文摘预登]

超高压线路潜供电弧电压的频率特性分析

舒亮, 贾磊, 郑士普, 孙冬慧, 施围

(西安交通大学电气工程学院, 710049, 西安)

针对潜供电弧状态对超高压线路单相自动重合闸的影响问题, 提出了一种基于故障相电压谐波情况的电弧状态判断方法. 该方法在分析了一次及二次电弧的特性及不同补偿度下电弧熄灭后系统振荡特性的基础上, 通过引入总谐波畸变 (THD) 来反映故障相电压谐波含量的变化. 通过对不同补偿度的系统运用 EMTP 进行仿真, 表明电弧熄灭后, 故障点电压的 THD 值将显著降低, 为利用故障点电压的谐波情况来判断电弧状态提供了依据.