多速率混合系统的模型检查

张海宾，段振华
(西安电子科技大学 计算机学院，陕西 西安 710071)

摘要：研究了初始化的多速率混合系统的模型检查问题，即检验初始化的多速率自动机是否满足某个混合区间时序逻辑公式描述的性质.首先定义了一套转换规则把混合区间时序逻辑公式转化为区间时序逻辑公式.接着定义了初始化的多速率自动机状态空间上的等价关系及其对应的域自动机，并且通过构造域自动机对应的标注有限状态自动机，把初始化的多速率混合系统的模型检查问题等价地转换成了可解的区间时序逻辑的模型检查问题.利用区间时序逻辑的模型检查算法加上上述的转换规则，就可以解决初始化的多速率混合系统的模型检查问题.

关键词：模型检查；混合系统；多速率自动机；区间时序逻辑
中图分类号：TP301 **文献标识码**：A **文章编号**：1001-2400(2008)01-0060-05

Model checking multirate hybrid systems

ZHANG Hai-bin, *DUANG Zhen-hua*
(School of Computer Science and Technology, Xidian Univ., Xi′an 710071, China)

Abstract: The model checking problem for initialized multirate hybrid systems is investigated, which is to check whether or not an initialized multirate automaton satisfies a property described by a hybrid interval temporal logic (HITL) formula. Firstly, some rules are defined to translate an HITL formula to an interval temporal logic (ITL) formula. Then, an equivalence relation over state spaces of multirate automata is defined to construct region automata from multirate automata. By constructing a labeled finite state automaton from a region automaton, the model checking issue for initialized multirate automata is translated to the same issue for ITL. Thus, by using the model checking algorithms for ITL and the translating rules defined in this paper, the model checking problem for initialized multirate hybrid systems can be solved.

Key Words: model checking; hybrid systems; multirate automata; interval temporal logic

混合系统是连续和离散设备互联的网络[1~4]，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.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.目前存在的系统验证方法主要有两类：一类是基于数学推理的演绎方法；另一类是基于算法的模型检查方法.由于模型检查的自动化优点，它在最近的一二十年里得到了广泛的应用.基于算法的模型检查检验一个结构 M 是否为一个时序逻辑公式 ϕ 的模型，也就是说 M 是否满足 ϕ，简写为 $M\models\phi$，其中 M 是描述系统行为的数学模型，一般为自动机模型，ϕ 是用来刻画要验证的系统性质的逻辑公式.

混合系统是无穷状态空间系统，这就使得混合系统的模型检查问题不一定是可判定的.多速率混合系统是一类广泛使用的混合系统子集，遗憾的是多速率混合系统的模型检查问题同样被证明是不可判定的，但多速率混合系统的某些子集的模型检查问题往往是可判定的，研究这些系统的模型检查问题具有现实意义.文献[2]给出了多速率混合系统的样本模型检查方法，然而，样本多速率混合系统只是多速率混合系统的简单子集，它处理问题的范围太过狭窄.笔者的主要贡献就是验证了初始化的多速率混合系统(一个更大的多速

收稿日期：2007-03-27
基金项目：国家自然科学基金资助(60373103，60433010)
作者简介：张海宾(1982-)，男，讲师，博士，E-mail：hbzhang@mail.xidian.edu.cn.

率混合系统子集)的模型检查问题是可判定的.

1　多速率自动机

多速率自动机[2,5]是描述多速率混合系统的数学模型,它是个 6 元组 $(Q, X, I, E, \kappa, i_{mv})$,其中 Q 是个有穷控制状态集;$X=\{x_1,\cdots,x_n\}$ 是有穷连续变量集;$I\subseteq Q\times Z^n$ 是初始状态集;E 是边的集合,它的每个元素都有形式$(q,\varphi,\lambda,\sigma,q')$,其中 $q, q'\in Q$,$\varphi\in B_n$(B_n 是 n 维矩形的集合),σ 是一个 n 维向量,$\lambda\subseteq\{1,\cdots,n\}$;$i_{mv}: Q\to B_n$ 表示连续变量在控制状态上应满足的约束条件;$\kappa: Q\to Z^n$ 表示在控制状态上连续变量的斜率.笔者处理初始化的多速率混合系统,关于它的详细定义可参照文献[2,5].

指派是个赋值方程,它为每个连续变量赋予一个特定的实数值,用 V 表示所有指派的集合. $v\in V$, $d\in R^+$, $l\in Z^n$, $v+l\cdot d$ 表示这样的指派 v':对于任意的 $x_i\in X$, $v'(x_i)=v(x_i)+l_i\cdot d$. $\beta\subseteq\{1,\cdots,n\}$, $[\beta\mapsto\sigma]v$ 表示这样的指派 v'':对 $i\in\beta$,有 $v''(x_i)=\sigma_i$;对 $j\in\{1,\cdots,n\}\backslash\beta$,有 $v''(x_j)=v(x_j)$. 多速率自动机 M 的一个状态是 $Q\times V$ 中的一个元素.给定一个状态(q, v),M 的一次(q, v) 执行是一个满足如下条件的无穷序列(q_0,v_0,t_0), (q_1,v_1,t_2),…(t_i 相当于一个时间变量):(1) $q_0=q$, $v_0=v$, $t_0=0$;(2) 对于任意的 $i\geqslant 0$,有 $t_i+1>t_i$,并且 $\exists e_i=(q_i,\varphi,\lambda,\sigma,q_{i+1})$ 使得 $v_i+\kappa(q_i)(t_{i+1}-t_i)\in\varphi$, $v_{i+1}=[\lambda\mapsto\sigma](v_i+\kappa(q_i)(t_{i+1}-t_i))$;(3) 对于任意的 $t\in R^+$,都存在某个 j 使得 $t_j>t$. 用 $<M,(q,v)>$ 表示 M 的所有(q, v) 执行的集合.

2　时序逻辑

用 π 表示原子命题集,区间时序逻辑(ITL)的语法定义如下:

$$\phi::=p\mid\neg\phi\mid\bigcirc\phi\mid\phi\vee\phi\mid\phi;\phi\quad,$$

其中 $p\in\pi$ 为原子命题.原子指派是个赋值方程,它为每个命题变量赋予一个真假值.区间 σ 是一个有穷或无穷的原子指派序列 $\sigma_0,\cdots,\sigma_{|\sigma|}$,其中 $|\sigma|$ 表示 σ 的长度,当 $|\sigma|<\infty$ 时,它等于原子指派的个数减 1.用 $\sigma_{(i,\cdots,j)}$ 表示子区间 $\sigma_i,\cdots,\sigma_j$,ITL 公式用元组 (σ, i, k, j) 来解释,$(\sigma, i, k, j)\vDash\phi$ 表示 σ 满足逻辑公式 ϕ. 详细的语义解释可参照文献[6].

混合区间时序逻辑(HITL)的语法定义如下:

$$\phi::=p\mid x\leqslant r\mid x=r\mid x^-\leqslant r\mid x^-=r\mid x^+\leqslant r\mid x^+=r\mid\neg\phi\mid\phi\vee\phi\mid\phi;\phi\quad,$$

其中 $p\in\pi$ 为原子命题,r 是整型常数,x 为实型变量,x^- 和 x^+ 分别为 x 的左右极限.仍用相位[7]作为 HITL 的语义解释,相位是个二元组 (I,g),其中 $I=[a, b]\subset R$, $g=\{g_x\}\cup\{g_p\}$ 是定义域为 I 的函数集.对于 $t\in I$,用 $\eta(t)$ 表示 $g(t)$.对于相位 $\eta=(I,g)$,用 $\eta_{I'}$. 表示 η 在 I' 上的投影子相位.对于 $c\in I=[a, b]$,分别用 $\eta_{[a,c]}$ 和 $\eta_{[c,b]}$ 表示点 c 把 η 分裂成的子相位.用 $\eta\vDash\psi$ 表示相位 η 满足公式 ψ. HITL 的语义解释可参照文献[7].

3　多速率混合系统的模型检查

给定多速率自动机 M 和 HITL 公式 ϕ,模型检查问题检验 M 的任意地开始于某个初始状态的执行 $\rho=(q_0,v_0,t_0)$, (q_1,v_1,t_1),… 是否满足公式 ϕ. 对于 M 的执行 ρ,可以构造惟一的相位 $\eta=([0,\infty),g)$ 与之对应,其中函数集 g 满足条件:对任意的 $t\in[t_i,t_{i+1})$,有 $g(t)=v_i+\kappa(q_i)(t-t_i)$. 记 ρ 对应的相位 η 为 $P(\rho)$(P 相当于执行序列对应相位的产生函数).这样,多速率混合系统的模型检查问题就是检验多速率自动机 M 任意执行 ρ 对应的相位 $P(\rho)$ 是否满足 HITL 公式 ϕ.由于多速率自动机是无穷状态空间系统,要对其进行模型检查,必须定义其状态空间上存在有限个数等价类的等价关系.在此之前,先给出几个简写形式:对于 $t\in R^+$,用 $i_{nt}(t)$ 表示 t 的整数部分,$f(t)$ 表示 t 的小数部分.对于多速率自动机 M,用 c_x 表示在 M 中变量 x 需要与之比较的最大常数.

3.1 指派等价关系

给定多速率自动机 $M=(Q, X, I, E, \kappa, i_{mv})$,假设 m 是 M 中所有非零斜率的最小公倍数.下面定义指派集 V 上的等价关系.

定义 1 给定控制状态 $q \in Q$ 和指派 v, v',称 v 与 v' q- 等价,记为 $v \simeq_q v'$,当且仅当:

(1) 对于任意的变量 $x_i \in X$, $v(x_i) > c_{x_i} \wedge v'(x_i) > c_{x_i}$,或者

① $\kappa(q)_i = 0$,并且 $i_{nt}(m \cdot v(x_i)/\kappa(q)_i) = i_{nt}(m \cdot v'(x_i)/\kappa(q)_i)$.

② $\kappa(q)_i = 0$,并且 $v(x_i) = v'(x_i) \in Z$.

(2) 对于任意变量 $x_i, x_j \in X$ 满足 $\kappa(q)_i \cdot \kappa(q)_j \neq 0$, $v(x_i) \leqslant c_{x_i}$ 和 $v(x_j) \leqslant c_{x_j}$,

① $f(m \cdot v(x_i)/\kappa(q)_i) \leqslant f(m \cdot v(x_j)/\kappa(q)_j)$ 当且仅当 $f(m \cdot v'(x_i)/\kappa(q)_i) \leqslant f(m \cdot v'(x_j)/\kappa(q)_j)$.

② $f(m \cdot v(x_i)/\kappa(q)_i) = 0$ 当且仅当 $f(\cdot v'(x_i)/\kappa(q)_i) = 0$.

用 $[v]_q$ 表示与 v q- 等价的指派集.

对于多速率自动机 M,如果把时间看作一个在 M 的每个控制状态上斜率都为 1 的变量 t,就可以把 M 的变量集扩充为 $X' = X \cup \{t\}$. 对于 X 上的指派 v, (v, t) 可以看作 X' 上的指派. 应用定义 1,如果 $(v, t) \simeq_q (v', t')$,称 (v, t) 与 (v', t') q- 广义等价,记作 $(v, t) \approx_q (v', t')$.

引理 1 对于多速率混合自动机 M 的一条边 $e = (q, \varphi, \lambda, \sigma, q')$,实数 t 和 t',如果 v, $v' \in \varphi$, $(v, t) \approx_q (v', t')$,那么 $([\lambda \mapsto \sigma]v, t) \approx_{q'} ([\lambda \mapsto \sigma]v', t')$.

证明 该引理的证明很直接,在此不做证明.

该引理保证了两个广义等价的指派经过某个跳跃转换,某些变量重新赋值后得到的两个指派仍然广义等价.

定义 2 对于多速率自动机 M 的两个执行 $\rho = (q_0, v_0, t_0), (q_1, v_1, t_1)\cdots$ 和 $\rho' = (q'_0, v'_0, t'_0), (q'_1, v'_1, t'_1), \cdots$,如果 ρ 与 ρ' 满足条件:(1) $q_0 = q'_0$, $v_0 \simeq_{q_0} v'_0$;(2) $q_i = q'_i$, ρ 在 t_i 时刻与 ρ' 在 t'_i 时刻经过相同的边转换,并且 $(v_{i-1} + \kappa(q_{i-1})(t_i - t_{i-1}), t_i) \approx_{qi-1} (v'_{i-1} + \kappa(q'_{q-1})(t'_i - t'_{i-1}), t'_i)$,说 ρ 与 ρ' 相似. 假设 Λ_1, Λ_2 是 M 的两个执行序列集,如果对 $\forall \rho \in \Lambda_1$, $\exists \rho' \in \Lambda_2$ 使得 ρ 与 ρ' 相似,反之亦然,称 Λ_1 与 Λ_2 相似.

引理 2 给定多速率混合自动机 M 的控制状态 q,如果 v 与 v' q- 等价,则 $< M, (q, v) >$ 与 $< M, (q, v') >$ 相似.

证明 首先证明对于任意的 (q, v) 执行 $\rho = (q, v, 0), (q_1, v_1, t_1), \cdots$,存在 (q, v') 执行 $\rho' = (q, v', 0), (q'_1, v'_1, t'_1), \cdots$ 使得 ρ 与 ρ' 相似. 可以由 ρ 采用如下的方法逐步求得 ρ':ρ 与 ρ' 的第一个元素显然满足相似的要求,因为 $v \simeq_q v'$. 取实数 $\delta = t_{i+1} - t_i$. 假设状态 $(q_i, v_i + \delta \cdot \kappa(q_i))$ 在 t_{i+1} 时刻通过边 $(q_i, \varphi, \lambda, \sigma, q_{i+1})$ 跳跃转换到状态 (q_{i+1}, v_{i+1}),并且已经构造出了 ρ' 的第 i 个元素 (q_i, v'_i, t'_i). 下面寻找实数 δ',使得 $(v_i + \delta \cdot \kappa(q_i), t_{i+1}) \simeq_q (v'_i + \delta' \cdot \kappa(q_i), t'_i + \delta')$.

按照定义 1 判断 $(v_i + \delta \cdot \kappa(q_i), t_i + 1) \approx_{q_i} (v'_i + \delta' \cdot \kappa(q_i), t'_i + \delta')$ 的过程就是求解 δ' 的过程. 下面给出一个实例:假设多速率混合自动机 M 的 $X = \{x, y\}$,在控制状态 $q \in Q$ 上, $\kappa(q)_x = 2$, $k(q)_y = 3$, $m = 12$. 并假设 $v_i = (0.05, 0.35)$, $t_i = t'_i = 1$, $v'_i = (0.1, 0.45)$, $t_{i+1} = 1.4$, $v_{i+1} = (0.85, 1.65)$. 则 $\delta = 0.4$, δ' 应满足如下条件:$6(0.1 + 2\delta') \in (5, 6)$, $4(0.45 + 3\delta') \in (6, 7)$, $12(1 + \delta') \in (16, 17)$. 可以选择 $(11/30, 5/12)$ 上的某个 δ' 值.

令 $t'_{i+1} = t'_i + \delta'$, $v'_{i+1}[\lambda \mapsto \sigma](v'_i + \delta' \cdot \kappa(q_i))$,由引理 1, $(v_i + \delta \cdot \kappa(q_i), t_{i+1}) \simeq_{q_i} (v'_i + \delta' \cdot \kappa(q_i), t'_{i+1})$ 可以推出 $(v_{i+1}, t_{i+1}) \simeq_{q_{i+1}} (v'_{i+1}, t'_{i+1})$,这样就可以构造出 ρ' 的第 $i+1$ 个元素 $(q_{i+1}, v'_{i+1}, t'_{i+1})$.

反之,对于任意的 (q, v') 执行 ρ',可以类似地证明存在 (q, v) 执行 ρ 使得 ρ' 与 ρ 相似.

定理 1 设 $q \in Q$ 是多速率混合自动机 M 的控制状态, v 与 v' 是两个 q- 等价的指派,则对于任意的 HITL 公式 ϕ, $< M, (q, v) > \vDash \phi$ 当且仅当 $< M, (q, v') > \vDash \phi$.

证明 由引理 2, $< M, (q, v) >$ 与 $< M, (q, v') >$ 相似. 对于任意的 $\rho \in < M, (q, v) >$,假设 ρ' 是 $< M, (q, v') >$ 中与 ρ 对应的执行. 令 $\eta = P(\rho)$, $\eta' = P(\rho')$,下面证明 $\eta \vDash \phi$ 当且仅当 $\eta' \vDash \phi$.

首先证明对任意的 $i < j$, $a \in [t_i, t_{i+1}]$, $a' \in [t'_i, t'_{i+1}]$, $b \in [t_j, t_{j+1}]$, $b' \in [t'_j, t'_{j+1}]$,如果 $a \leqslant b \wedge a' \leqslant b'$,

$(\eta(a),a)\approx_{q_i}(\eta'(a'),a')$ 和 $(\eta(b),b)\approx_{q_j}(\eta'(b'),b')$,则对于任意的 HITL 公式 ϕ,$\eta_{[a,b]}\vdash\phi$ 当且仅当 $\eta'_{[a',b']}\vdash\phi$.依据 HITL 公式的结构进行归纳证明,由于篇幅的限制,仅证 ϕ 为 $x\leqslant r$ 和 $\phi_1;\phi_2$ 的情形.(1) 若 $\eta_{[a,b]}\vdash x\leqslant r$,则 $\eta(a)(x)\leqslant r$.如果 $\eta(a)(x)=r$,由于 $\eta(a)\simeq_{q_i}\eta'(a')$,所以 $\eta'(a')(x)=\eta(a)(x)=r$;如果 $\eta(a)(x)<r$,则 $i_{mt}(\eta(a)(x))<r$.由于 $\eta(a)\simeq_{q_i}\eta'(a')$,则 $i_{mt}(\eta(a)(x))=i_{mt}(\eta'(a')(x))<r$,所以 $\eta'(a')(x)<r$.因而 $\eta'_{[a',b']}\vdash x\leqslant r$.反之证明类似.(2) 若 $\eta_{[a,b]}\vdash\phi_1;\phi_2$,则存在 $t\in[a,b]$ 使得 $\eta_{[a,t]}\vdash\phi_1$ 和 $\eta_{[t,b]}\vdash\phi_2$ 成立.假设 $t\in[t_k,t_{k+1}]$,则可以运用引理 2 的方法找到 $t'\in[t'_k,t'_{k+1}]$,使得 $(\eta(t),t)\simeq_{q_k}(\eta'(t'),t')$.由归纳假设,$\eta'_{[a',t']}\vdash\phi_1$,$\eta'_{[t',b']}\vdash\phi_2$.因而 $\eta'_{[a',b']}\vdash\phi_1;\phi_2$.反之类似.同理可证对任意的 i,$a\in[t_k,t_{k+1}]$,$a'\in[t'_k,t'_{k+1}]$,如果 $(\eta(a),a)\approx_{q_i}(\eta'(a'),a')$,则对于任意的 HITL 公式 ϕ,$\eta_{[a,\infty)}\vdash\phi$ 当且仅当 $\eta'_{[a',\infty)}\vdash\phi$.取 $a=0$,则 $\eta\vdash\phi$ 当且仅当 $\eta'\vdash\phi$.

定理 1 说明了同一个控制状态上的等价指派区分不出 HITL 公式,也就是说他们同时满足或不满足某个 HITL 公式.这条性质是笔者划分多速率自动机的无穷状态空间为有限个等价类的依据.下一节将定义这有限个等价类上的有限状态自动机——域自动机.

3.2　域自动机

定义 3　区域是个二元组 $(q,[v]_q)$,其中 $q\in Q$,$v\in V$.对于两个不等的区域 $r=(q,[v_1]_q)$,$r'=(q',[v_2]_{q'})$,称区域 r' 是区域 r 的后继当且仅当:(1) $q=q'$;(2) 对于任意的 $v\in[v_1]_q$,存在 $d\in R^+$ 使得 $v+d\cdot\kappa(q)\in[v_2]_{q'}$,并且对任意的 $0\leqslant t\leqslant d$,$v+t\cdot\kappa(q)\in[v_1]_q\cup[v_2]_{q'}$.用 $s(r)$ 表示 r 的后继区域.

对于区域 $r=(q,[v]_q)$,如果对于任意的指派 $v'\in[v]_q$,任意的变量 $x\in X$,都有 $v'(x)>c_x$,称 r 为无界区域;如果对于任意的 $t\in R^+$,任意的指派 $v''\in[v]_q$,$v''+t\cdot\kappa(q)$ 都不与 $v''q^-$ 等价,称 r 为边界区域.

定义 4　域自动机 $R(M)$(M 是一个多速率自动机)是个二元组 (S,E^*),其中 S 为 M 的所有区域的集合,E^* 为边的集合,它包含如下两种类型转换:

① 对于顶点 $r\in S$,如果 r 不是无界区域,则有 $(r,s(r))\in E^*$;如果 r 是无界区域,则有 $(r,r)\in E^*$.称此类边为流边.

② 对于顶点 $r=(q,[v]_q)\in S$ 和 M 的一条边 $e=(q,\varphi,\lambda,\sigma,q')$,如果 r 不是边界区域,并且 $v\in\varphi$,则 $(r,(q',[[\lambda\mapsto\sigma]v']_{q'}))\in E^*$,其中 $v'\in[v]_q$ 或者 $(q,v')\in s(r)$.称此类边为跳边.

对于多速率自动机 M 的任意的执行 $\rho=(q_0,v_0,t_0),(q_1,v_1,t_1),\cdots$,存在区域自动机 $R(M)$ 的执行 $\xi=(q_0,[v_0]_{q_0}),\cdots,(q_i,[v_{i_0}]_{q_i}),(q_i,[v_{i_1}]_{q_i}),\cdots,(q_i,[v_{i_{m_i}}]_{q_i}),\cdots$ 与之对应,其中 $v_{i_0}=v_i$,$(q_i,[v_{i_{k+1}}]_{q_i})=s(q_i,[v_{i_k}]_{q_i})$.反之对 $R(M)$ 的任意执行,有 M 的一族执行与之对应.把 ξ 排成区域的无穷序列 $r_0,r_1,\cdots$,其中 $r_j=(q_i,[v_{i_k}]_{q_i})$,定义函数 l_Γ 为 $l_\Gamma(t)=j$,其中对于 $t\in[t_i,t_{i+1})$,j 满足约束条件 $r_j=(q_i,[v_{i_k}]_{q_i})$ 和 $v_{i_k}\simeq_{q_i}P(\rho)(t)$.

定义 5　对于任意的 HITL 公式 ϕ,归纳定义 ITL 公式 $\bar{\phi}$ 如下:

① $\bar{p}\overset{\text{def}}{=\!=}p$,$p$ 是原子命题.

② $\overline{x\leqslant r}\overset{\text{def}}{=\!=}p_{x\leqslant r}$,$\overline{x=r}\overset{\text{def}}{=\!=}p_{x=r}$,$\overline{x^-\leqslant r}\overset{\text{def}}{=\!=}p_{x^-\leqslant r}$,$\overline{x^-=r}\overset{\text{def}}{=\!=}p_{x^-=r}$,$\overline{x^+\leqslant r}\overset{\text{def}}{=\!=}p_{x^+\leqslant r}$,$\overline{x^+=r}\overset{\text{def}}{=\!=}p_{x^+=r}$.

③ $\overline{\neg\phi}\overset{\text{def}}{=\!=}\neg\bar{\phi}$,$\overline{\phi_1\vee\phi_2}\overset{\text{def}}{=\!=}\bar{\phi}_1\vee\bar{\phi}_2$,$\overline{\phi_1;\phi_2}\overset{\text{def}}{=\!=}\bar{\phi}_1;\bar{\phi}_2$.

其中 $p_{x\leqslant r},p_{x=r},p_{x^-\leqslant r},p_{x^-=r},p_{x^+\leqslant r},p_{x^+=r}$ 为新定义的原子命题.

对于一个域自动机 $R(M)=(S,E^*)$,HITL 公式 ϕ 及其对应的 ITL 公式 $\bar{\phi}$,可以按如下规则把 $R(M)$ 的每个顶点适当分割,同时标注上 $\bar{\phi}$ 中出现的原子命题,从而构造一个标注有限状态自动机 $L(R,M)=(S^*,E^*,l)$(用 γ 表示经过跳边转换得到的区域的集合):

① $S^*=S_1^*\cup S_2^*$,其中 $S_1^*=\{(q,[v]_q,0),(q,[v]_q,1)\mid(q,[v]_q)\in\gamma\}$;$S_2^*=\{(q,[v]_q,1)\mid(q,[v]_q)\in S\backslash\gamma\}$.

② 对于任意的非边界区域 $(q,[v]_q)\in S$,如果存在 $(q,[v]_q,0)\in S^*$,那么 $((q,[v]_q,0),(q,[v]_q,$

1)) $\in E^*$;对于 $R(M)$ 的任意跳边$((q,[v]_q),(q',[v']_{q'}))$,如果$(q,[v]_q)\in\gamma$,则$((q,[v]_q,0),(q',[v']_{q'},0))\in E^*$;否则,$((q,[v]_q,1),(q',[v']_{q'},0))\in E^*$. 对于 $R(M)$ 的任意流边$((q,[v]_q),(q,[v']_q))$,如果$(q,[v]_q)\in\gamma$,那么$((q,[v]_q,0),(q,[v']_q,1))\in E^*$;否则,$((q,[v]_q,1),(q,[v']_q,1))\in E^*$. E^* 不包含任何其他的元素.

③ 对于任意的 $w=(q,[v]_q,0)$,把 p_{sing} 添加到 $l(w)$. 对于任意的$(q,[v]_q,1)$,任意的$x\in X$,令 $v(x^-)$, $v(x^+)\in[v(x)]_q$, 对于$((q,[v]_q,b),(q',[v']_{q'},0))\in E^*$ $(b=0$ 或 $b=1)$, 令 $v'(x^+)\in[v'(x)]_{q'}$,$v'(x^-)\in[v(x)]_q$. 对于任意的$w=(q,[v]_q,b)$,HITL 公式 ϕ 以及 ϕ 的子公式$x\leqslant r$, $x=r$,如果$v(x)=r$,则把 $p_{x=r}$,$p_{x\leqslant r}$ 添加到$l(w)$集中,如果$v(x)<r$,则把$\neg p_{x=r}$,$p_{x\leqslant r}$ 添加到$l(w)$集中,如果$v(x)>r$,则把$\neg p_{x=r}$,$\neg p_{x\leqslant r}$ 添加到 $l(w)$ 集中. 对于 ϕ 的子公式$x^-\leqslant r$, $x^-=r$, $x^+\leqslant r$, $x^+=r$,情形与 $x\leqslant r$,$x=r$ 类似. l 不包含任何其他的元素.

由域自动机构造标注有限状态自动机的基本思想是:把那些经过跳边转换得到的区域一分为二,从而把跳跃转换产生的不连续点单独拿出来作为一个区域(标注有 p_{sing}). 之所以这样做,是由于在多速率自动机每次执行所对应的相位上,每个变量的右极限都等于该变量的值(右连续),而其左极限在不连续点上则不等.

对于 $R(M)$ 的执行 $\xi=r_0,r_1,\cdots$,存在 $L(R,M)$ 的执行 $\sigma=(r_0,b_0),(r_1,b_1),\cdots$ 与之对应,其中$b_i=0$ 或$b_i=1$,反之亦然. 这样多速率自动机 M、区域自动机 $R(M)$、标注有限状态自动机 $L(R,M)$ 的执行之间存在简单的对应关系. 对于多速率自动机M的任意的执行$\rho=(q_0,v_0,t_0),(q_1,v_1,t_1),\cdots$,和对应的$R(M)$的执行$\xi=r_0,r_1,\cdots$ 以及对应的 $L(R,M)$ 的执行$\sigma=\sigma_0,\sigma_1,\sigma_2,\cdots$,定义函数 l_h 为$l_h(t)=j$,其中对于$t=t_i$,j 满足约束条件$\sigma_j=(r_{l_\Gamma}(t),0)$;对于$t\in(t_i,t_{i+1})$,$j$ 满足约束条件$\sigma_j=(r_{l_\Gamma}(t),1)$.

定理 2 对于多速率混合自动机 M 和 HITL 公式 ϕ,设 $L(R,M)$ 和 $\bar{\phi}$ 分别为 M 和 ϕ 所对应的标注自动机和 ITL 公式,则$M\vDash\phi$ 当且仅当 $L(R,M)\vDash\bar{\phi}$.

证明 由于多速率自动机 M 的执行与$L(R,M)$ 的执行之间存在对应关系,对于 M 的执行 ρ 以及 ρ 对应的 $L(R,M)$ 的执行 σ,令$\eta=P(\rho)$,证$\eta\vDash\phi$ 当且仅当$\sigma\vDash\bar{\phi}$.

首先证明对任意的$[a,b]\subset[0,\infty)$,$\eta_{[a,b]}\vDash\phi$ 当且仅当$\sigma_{(l_h(a),\cdots,l_h(b))}\vDash\bar{\phi}$. 对 HITL 公式的结构进行归纳证明. 由于篇幅的限制,仅考虑 ϕ 为$x\leqslant r$ 和 ϕ_1; ϕ_2 的情形. (1) 若 $\eta_{[a,b]}\vDash x\leqslant r$, 则 $\eta(a)(x)=r$ 或 $\eta(a)(x)<r$. 由标注自动机的构造规则,无论哪种情况,都有 $\sigma_{l_h(a)}(p_{x\leqslant r})$ 为 true,因而$\sigma_{(l_h(a),\cdots,l_h(b))}\vDash\bar{\phi}$. 反之类似. (2) 若$\eta_{[a,b]}\vDash\phi_1;\phi_2$,则存在$a\leqslant t\leqslant b$ 使得$\eta_{[a,t]}\vDash\phi_1$,$\eta_{[t,b]}\vDash\phi_1$. 取$k=l_h(t)$,由归纳假设,$\sigma_{(l_h(a),\cdots,k)}\vDash\bar{\phi}_1$, $\sigma_{(k,\cdots,l_h(b))}\vDash\bar{\phi}_2$,因而$\sigma_{(l_h(a),\cdots,l_h(b))}\vDash\bar{\phi}_1;\bar{\phi}_2$. 反之类似. 同理可证对任意的$a\in[0,\infty)$, $\eta_{[a,\infty)}\vDash\phi$ 当且仅当 $\sigma_{(l_h(a),\cdots,\infty)}\vDash\bar{\phi}$. 取$a=0$,则$\eta\vDash\phi$ 当且仅当$\sigma\vDash\bar{\phi}$.

利用定理 2,基于 HITL 的初始化的多速率混合系统的模型检查问题可以等价地转换为 ITL 的模型检查问题. 文献[6]解决了 ITL 的可满足性判定问题,并给出了算法,由给定的 ITL 公式 ϕ 构造有限状态自动机N,使得 N 接收的语言恰好是满足φ 的所有原子命题序列的集合. 这样可以通过判断两个自动机的交自动机(接受的语言为两个自动机接受语言的交集)接受的语言是否为空来解决 ITL 的模型检查问题,从而相应地解决初始化的多速率混合系统的模型检查问题.

4 结 束 语

虽然多速率混合系统的模型检查问题被证明是不可判定的,但是它的某些子集的模型检查问题却是可判定的. 研究这些子系统的模型检查问题也是很有意义的. 目前虽然已经解决了样本多速率混合系统的模型检查问题,然而多速率混合系统的样本模型只是稍稍大于实时系统的多速率混合系统的很小的子集,它要求所有跳跃转换必须发生在整数点上. 笔者解决了初始化的多速率混合系统的模型检查问题. 初始化的多速率混合系统只要求在两个相邻的离散状态转换时,如果变量斜率发生变化,必须进行重新赋值. 因此,笔者解决问题的范围要远远大于样本多速率混合系统.

(下转第 86 页)