# 混合投影时序逻辑与混合系统的形式化验证*)

张海宾　段振华

(西安电子科技大学计算机学院　西安 710071)

**摘　要**　为了描述混合系统的性质和行为,10 多年来,各种时序逻辑,如 Hybrid Temporal Logic 等相继出现。这些时序逻辑适用于刻画混合系统的性质和规范,但不适宜表示描述系统的实现模型。本文定义了一个混合投影时序逻辑(Hybrid Projection Temporal Logic,简称 HPTL),既能刻画混合系统的性质,又能表示混合系统的实现。这样,混合系统的验证就可以很方便地在统一的数学模型框架下进行。同时,给出了 HPTL 的基本的逻辑等价式系统和一个用 HPTL 进行混合系统验证的实例。

**关键词**　混合系统,混合自动机,区间时序逻辑,形式化验证

## Hybrid Projection Temporal Logic and Formal Verifications of Hybrid Systems

ZHANG Hai-Bin　DUAN Zhen-Hua

(School of Computer Science and Technology, Xidian University, Xi'an 710071)

**Abstract**　To describe properties of hybrid systems, many temporal logics such as Hybrid Temporal Logic have been formalized. Although being good at describing properties of hybrid systems, these logics are not suitable for describing the behaviors of such systems. In this paper, a hybrid projection temporal logic (HPTL) is formalized. It can be used to describe both properties and implementations of hybrid systems, which enables us to do verifications of hybrid systems over the same mathematical model. In addition, a set of logical equivalent formulas and an example of verifications using HPTL are given.

**Keywords**　Hybrid systems, Hybrid automata, Interval temporal logic, Formal verification

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[1,5],在数控系统、商业、工业和军事领域广泛存在着混合系统。混合系统的研究内容主要是系统的建模、分析与验证。混合系统研究中采用的数学工具主要是各种时序逻辑、自动机等。作为混合系统的规范语言(specification languages),时序逻辑,如 Hybrid Temporal Logic[3]等主要用于刻画系统的性质(如安全性、可达性、公平性等),但不适宜描述混合系统的实现模型。混合系统的实现模型通常是用混合自动机(hybrid automata)[6~8]等系统描述语言(system description languages)来表示的。可是,这些系统描述语言又无法刻画系统性质。这样,在基于时序逻辑的混合系统的研究中,系统的性质和实现通常是用不同的语言来表示的。这种做法不利于系统性质的验证,因为性质和实现不是用同一语言表示的,它们不在同一推演系统下。

本文提出了一种带投影操作符的混合时序逻辑,它是区间时序逻辑[2](Interval Temporal Logic,简称 ITL)在混合系统领域的一种扩展。通过引进投影操作符'$prj$',可以把系统的连续状态与离散转换有机地联系起来。因而,HPTL 不仅可以刻画系统性质,也很适宜描述系统行为。这样,混合系统的形式化验证就可以在统一的模型框架下进行。本文还给出了 HPTL 的基本的逻辑等价式系统,这些逻辑定理可以很好地帮助我们进行公式推演,从而完成系统的验证。最后,给出了一个用 HPTL 进行混合系统性质验证的实例。

## 1　HPTL 的语法与语义

在定义 HPTL 的语义与语法之前,先来回顾一下区间时序逻辑的定义。用 $AP$ 表示原子命题集,区间时序逻辑的语法定义如下:

$$e ::= r \mid x \mid \bigcirc e \mid f(e_1,\cdots,e_n)$$

$$\phi ::= \pi \mid e_1 = e_2 \mid P(e_1,\cdots,e_n) \mid \neg\phi \mid \bigcirc\phi \mid \exists x:\phi \mid \phi_1 \vee \phi_2 \mid \phi_1;\phi_2$$

其中 $\pi \in AP$ 是一个原子命题,$r,x,f$ 和 $P$ 分别是常数、实变量、函数和谓词。

由于篇幅的限制,在此我们不给区间时序逻辑的语义解释,只介绍其语义模型。状态 $s$ 是个赋值方程,它把每个原子变量赋予一个真假值,把每一个实变量 $x$ 赋予一个实数值。$\sum$ 表示状态的集合,$s|\pi|$ 表示 $s$ 赋予命题变量 $\pi$ 的真假值,$s(x)$ 表示 $s$ 赋予 $x$ 的实数值。区间 $\sigma$ 是一个状态的序列$\langle s_0,\cdots,s_{|\sigma|}\rangle$,其中$|\sigma|$表示 $\sigma$ 的长度。如果 $\sigma$ 为无限状态序列,则$|\sigma|=\infty$;如果 $\sigma$ 为有限状态序列,则$|\sigma|$等于状态的个数减 1。用 $\sigma_i$ 表示 $s_i,\sigma_{(i,\cdots,j)}$ 表示子区间$\langle\sigma_i,\cdots,\sigma_j\rangle$。用元组$(\sigma,i,k,j)$来解释区间时序逻辑,其中 $\sigma$ 为区间,$i\leqslant k\leq^3 j$ 为整数,详细的语义解释参照文[1,2]。如下是一些扩充的 ITL 公式:false $\stackrel{def}{=}\phi\wedge\neg\phi$, $true\stackrel{def}{=}\phi\vee\neg\phi$, $Empty\stackrel{def}{=}k=j$, $More\stackrel{def}{=}\neg Empty$, $\odot\phi\stackrel{def}{=}Empty\vee\bigcirc\phi$, $\Diamond\psi\stackrel{def}{=}true;\psi$, $\Box\psi\stackrel{def}{=}\neg\Diamond\neg\psi$。

### 1.1　HPTL 语法

*)国家自然科学基金资助项目(60373103);国家自然科学基金重大资助项目(60433010);博士点基金资助项目(20030701015)。**张海滨**　博士研究生,研究方向为混合系统、形式化验证。

用 $X$ 表示非命题的变量集合，HPTL 的语义定义如下：

$e::=u|x|x^-|x^+|\dot{x}|\dot{x}^-|\dot{x}^+|f(e_1,\cdots,e_n)$

$\phi::=\pi|e_1=e_2|P(e_1,\cdots,e_n)|\neg\phi|\phi_1\vee\phi_2|\exists x:\phi|\phi_1;\phi_2|$

其中 $\pi\in AP$，$x,u\in X$ 分别是静态变量，$x^+$，$x^-$，$\dot{x}^+$ 和 $\dot{x}^-$ 分别是的左极限、右极限、$x$ 微分的左极限、右极限，$f$ 和 $P$ 分别是函数和谓词。

### 1.2 HPTL 语义

令 $[a,\infty]=[a,\infty)\cup\{\infty\}$，通过定义 $[b,\infty]\subseteq[a,\infty]$，其中 $a\leqslant b$，我们把'$\subseteq$'扩展为 $2^{[0,\infty]}$ 上的操作符。用 $c\in[a,b]$ 表示 $a\leqslant c\leq b$。定义一个时间区间 $I=[a,b]$，$I\neq[\infty,\infty]$ 为 $[0,\infty]$ 的一个子集。

令 $I=[a,b]$ 为一个时间区间，如果函数 $f:[a,b]\to R$ 满足如下条件，称 $f$ 为 $[a,b]$ 上的分段光滑函数：(1)在 $I$ 的左端点 $a$，$f$ 的右极限和右微分存在；(2)在 $I$ 时间区间内的任一点 $t\in(a,b)$，$f$ 的左右极限和左右微分都存在，并且 $f$ 要么左连续，要么右连续；(3)在 $I$ 的右端点 $b$，$f$ 的左极限和左微分存在。

相位是三元组 $(I,l,g)$，其中 $I=[a,b]$ 是个时间区间，$l:[a,b]\to\sum_o$ 是一个函数，$g=\{g_x:x\in X\}$ 是个 $[a,b]$ 上的分段光滑的函数集。给定相位 $\eta=(I,l,g)$ 和 $\eta'=(I',l',g')$，其中 $I=[a,b]$，$I'=[a',b']$。如果 $I'\subseteq I$，$l$ 和 $g$ 在 $I'$ 上的投影函数分别为 $l'$ 和 $g'$，称 $\eta'$ 是 $\eta$ 的子相位，并且用 $\eta_{I'}$ 表示 $\eta$ 的子相位 $\eta'$；如果 $b=a'$，$l(b)=l'(b)$，$g(b)=g'(b)$，称 $\eta$ 和 $\eta'$ 是相邻的。对于两个相邻的相位 $\eta,\eta'$，用 $\eta\frown\eta'_2$ 表示相位 $([a,b'],l^*,g^*)$，其中函数 $l^*$ 在 $I$ 和 $I'$ 上的投影函数分别是 $l$ 和 $l'$，$g^*$ 在 $I$ 和 $I'$ 上的投影函数分别是 $g$ 和 $g'$。如果 $\eta^*=\eta\frown\eta'$，称 $\eta$ 和 $\eta'$ 分割相位 $\eta^*$。对于相位 $\eta=(I,l,g)$ 和 $\eta'=(I',l',g')$，如果 $I=I'$，$l=l'$，并且对任意的 $y\in X\backslash\{x\}$ 和任意的 $t\in I$，有 $g_y(t)=g'_y(t)$，称 $\eta$ 与 $\eta'$ $x$-等价，简记为 $\eta\overset{x}{=}\eta'$。我们用相位来解释 HPTL 公式，相位 $\eta=([a,b],l,g)$ 满足公式 $\phi$，简记为 $\eta\models\phi$，递归定义为：

(1)$\eta[u]=g_u(a)=g_u(t)$，$u$ 是个静态变量，$t$ 为 $I$ 上任意一点；

(2)$\eta[x]=g_x(a)$，$x$ 是个动态变量；

(3)$\eta[x^+]=\lim_{t\to a}(g_x(t))(t-a>0)$；

(4)$\eta[x^-]=\lim_{t\to b}(g_x(t))(t-b<0)$；

(5)$\eta[\dot{x}=\begin{cases}\eta[\dot{x}^-],\text{如果 }\eta[\dot{x}^-]=\eta[\dot{x}^+]\\ nill,\text{如果 }\eta[\dot{x}^-]\neq\eta[\dot{x}^+]\end{cases}$；

(6)$\eta[\dot{x}^+]=\lim_{t\to a}(g_x(t)-g_x(a))/(t-a)(t-a>0)$；

(7)$\eta[\dot{x}^-]=\lim_{t\to b}(g_x(t)-g_x(b))/(t-b)(t-b<0)$；

(8)$\eta[f(e_1,\cdots,e_m)]=$

$\begin{cases}nill,\text{如果存在某个 }h\in\{1,\cdots,m\}\text{ 满足 }\eta[e_h]=nill;\\ f(\eta[e_1],\cdots,\eta[e_m]),\text{其他情况；}\end{cases}$

(9)$\eta\models\pi$ 当且仅当 $l(a)[\pi]=true$，$\pi$ 为原子命题；

(10)$\eta\models P(e_1,\cdots,e_m)$ 当且仅当 $P(\eta[e_1],\cdots,\eta[e_m])=true$，$P$ 是一个非'='的谓词。其中对任意的 $h.0\leqslant h\leqslant m$，有 $\eta[e_h]\neq nil$；

(11)$\eta\models e_1=e_2$ 当且仅当 $\eta[e_1]=\eta[e_2]$，$e_1$ 和 $e_2$ 为项；

(12)$\eta\models\neg\phi$ 当且仅当 $\eta\not\models\phi$；

(13)$\eta\models\phi_1\vee\phi_2$ 当且仅当 $\eta\models\phi_1$ 或 $\eta\models\phi_2$；

(14)$\eta\models\exists x:\phi$ 当且仅当存在相位 $\eta'.\eta'\overset{x}{=}\eta$ 使得 $\eta'\models\phi$；

(15)$\eta\models(\phi_1,\phi_2)$ 当且仅当存在 $t\in I$ 使得 $\eta_{[a,t]}\models\phi_1$，$\eta_{[t,b]}\models\phi_2$。

### 1.3 投影操作符

投影公式结构定义如下：

$(\phi_1;\cdots;\phi_m)prj\ \phi$

其中 $\phi_i$ 是 HPTL 公式，$\phi$ 是 ITL 公式。为了解释带投影操作符的公式，我们先给出投影区间的概念。令 $\eta=([a,b],l,g)$ 为一个相位，$a\leqslant r_1\leqslant r_2\leqslant\cdots\leqslant r_h\leqslant b$ 是一个序列，则 $\eta$ 在 $r_1,\cdots,r_h$ 上的投影为

$\eta\downarrow(r_1,\cdots,r_h)=\langle l(t_0),l(t_1),\cdots,l(t_l)\rangle$

其中 $t_0,t_1,\cdots,t_l$ 为 $r_1,\cdots,r_h$ 互不相等的最大子序列。例如：$([0,3],l,g)\downarrow(0,0,1,2.5,2.5)=\langle l(0),l(1),l(2.5)\rangle$。

相位 $\eta=([a,b],l,g)$ 满足公式 $(\phi_1;\cdots;\phi_m)prj\ \phi$，当且仅当 $\eta\downarrow(a)\models\phi$，并且 $\eta\models\phi_1;\cdots;\phi_m$；或者存在序列 $a\leqslant r_1\leqslant r_2\leqslant\cdots\leqslant r_h\leqslant b$ 满足如下条件：

- $\eta_{[a,r_1]}\models\phi_1$，并且对任意的 $1<l\leqslant h$，有 $\eta_{[r_{l-1},r_l]}\models\phi_l$；
- 如果 $h<m$，则有 $\eta\downarrow(a,r_1,\cdots,r_h)\models\phi$ 和 $\eta_{[r_h,b]}\models\phi_{h+1};\cdots;\phi_m$；
- 如果 $h=m$，则有 $r_m=b$ 和 $\eta\downarrow(a,r_1,\cdots,r_h)\models\phi$。

### 1.4 扩充的 HPTL 公式

(1)$\phi_1\wedge\phi_2\overset{def}{=}\neg(\neg\phi_1\vee\neg\phi_2)$

(2)$\forall x:\phi\overset{def}{=}\neg\exists x:(\neg\phi)$

(3)$empty\overset{def}{=}a=b$　　(4)$more\overset{def}{=}\neg empty$

(5)$\Diamond\phi\overset{def}{=}true;\phi$　　(6)$\Box\phi\overset{def}{=}\neg\Diamond\neg\phi$

(7)$hold(\phi)\overset{def}{=}(more\to\phi)$　　(8)$fin(\phi)\overset{def}{=}\Box(empty\to\phi)$

(9)$halt(\phi)\overset{def}{=}\Box(empty\leftrightarrow\phi)$　(10)$keep(\phi)\overset{def}{=}\Box(more\to\phi)$

(11)$(\phi_0;\cdots;\phi_h)^{(0)}\ prj\phi\overset{def}{=}empty\ prj\ \phi$

(12)$(\phi_0;\cdots;\phi_h)^{(m)}\ prj\phi\overset{def}{=}((\phi_0;\cdots;\phi_h;(\phi_0;\cdots;\phi_h)^{(m-1)})\ prj\ \phi)\wedge m\in N$

(13)$(\phi_0;\cdots;\phi_h)^{(+)}\ prj\phi\overset{def}{=}\exists m:(m\in N\wedge(\phi_0;\cdots;\phi_h)^{(m)}\ prj\ \phi)$

### 1.5 操作符优先级

(1)$\neg$　(2)$\Diamond$　$\Box$　(3)$\exists$　$\forall$　(4)$=$　(5)$\wedge$　$\vee$　(6)$\to$　$\leftrightarrow$　(7)$;prj$

## 2 HPTL 的逻辑等价公式

给定相位 $\eta=(I,l,g)$ 和 HPTL 公式 $\phi$，如果 $\eta\models\phi$，称 $\eta$ 满足 $\phi$；如果任意的相位都满足 $\phi$，称 $\phi$ 为有效的，简记为 $\models\phi$。我们用 $\phi\equiv\varphi$ 表示 $\models\Box(\phi\leftrightarrow\varphi)$；$\phi\approx\varphi$ 表示 $\models\phi\leftrightarrow\varphi$；$\phi\Rightarrow\varphi$ 表示 $\models\Box(\phi\to\varphi)$；$\phi\to\varphi$ 表示 $\models\phi\to\varphi$。对于 ITL 公式 $\varphi$，也有相应的定义。

设 $\phi,\varphi,\psi$ 为 ITL 公式，则

| | |
|---|---|
| $FD1\bigcirc(\phi\wedge\varphi)\equiv\bigcirc\phi\wedge\bigcirc\varphi$ | $FD2\bigcirc(\phi\vee\varphi)\equiv\bigcirc\phi\vee\bigcirc\varphi$ |
| $FD3\odot(\phi\wedge\varphi)\equiv\odot\phi\wedge\odot\varphi$ | $FD4\odot(\phi\vee\varphi)\equiv\odot\phi\vee\odot\varphi$ |
| $FD5\bigcirc(\phi\to\varphi)\equiv\odot\phi\to\bigcirc\varphi$ | $FD6\odot(\phi\to\varphi)\equiv\bigcirc\phi\to\odot\varphi$ |
| $FD7\neg\odot\phi\equiv\bigcirc\neg\phi$ | $FD8\neg\bigcirc\phi\equiv\odot\neg\phi$ |
| $FD9\Diamond\phi\equiv\phi\vee\bigcirc\Diamond\phi$ | $FD10\Box\phi\equiv\phi\wedge\odot\Box\phi$ |
| $FD11\Diamond\phi\vee\Diamond\varphi\equiv\Diamond(\phi\vee\varphi)$ | $FD12\Box\phi\wedge\Box\varphi\equiv\Box(\phi\wedge\varphi)$ |
| $FD13\psi;\phi\vee\varphi\equiv\psi;\phi\vee\psi;\varphi$ | $FD14\bigcirc\phi;\varphi\equiv\bigcirc(\phi;\varphi)$ |

[3] $\leq$b 当且仅当 a$\leqslant$b$\wedge$a$<\infty$。

$FD15 Empty;\phi \equiv \phi$　　$FD16 \phi;(\varphi;\psi) \equiv (\phi;\varphi);\psi$

设 $\phi,\varphi,\psi,\phi_1,\cdots,\phi_m$ 为 HPTL 公式，则

$FC1 \Diamond\phi \vee \Diamond\varphi \equiv \Diamond(\phi \vee \varphi)$

$FC2 \Box\phi \wedge \Box\varphi \equiv \Box(\phi \wedge \varphi)$

$FCD3 \psi;\phi \vee \varphi \equiv \psi;\phi \vee \psi;\varphi$

$FC4 \phi \vee \varphi;\psi \equiv \psi;\psi \vee \varphi;\psi$

$FPj3(\phi_1;\cdots;\phi_m)prj\ empty \equiv \phi_1;\cdots;\phi_m$

$FPj4(\phi_1;\cdots;\phi_t;empty;\phi_{t+1};\cdots;\phi_m)prj\ \varphi \equiv (\phi_1;\cdots;\phi_t;\phi_{t+1};\cdots;\phi_m)prj\ \varphi$

$FPj5(\phi_1;\cdots;\phi_m)prj\ \bigcirc\varphi \equiv (\phi_1 \wedge more;(\phi_2;\cdots;\phi_m)prj\ \varphi) \vee (\phi_1 \wedge empty;(\phi_2;\cdots;\phi_m)prj\ \bigcirc\varphi)$

$FPj6(\phi_1;\cdots;\phi_m)prj\ \bigcirc\varphi \equiv (\phi_1 \wedge mpre;(\phi_2;\cdots;\phi_m)prj\ \varphi) \bigvee_{t=1}^{m-2}((\phi_1 \wedge \cdots \wedge \phi_t) \wedge empty;\phi_{t+1} \wedge more;(\phi_{t+2};\cdots;\phi_m)prj\ \varphi) \vee (\phi_1 \wedge \cdots \wedge \phi_{m-1}) \wedge empty;\phi_m \wedge more\ prj\ \bigcirc\varphi)$

由于篇幅的限制，本文不给出这些逻辑等价式的证明。

## 3　使用 HPTL 描述与验证混合系统

图 1 所示的混合自动机模拟了一个水面监测器系统[4]。容器中的水面高度由一个水面监测器来实时监控。监测器控制一个水泵的开与关。当水泵处于关闭状态时，用变量 $y$ 表示的水面高度每秒下降 2 英寸；当水泵处于打开状态时，水面高度每秒上升 1 英寸。假设开始时水面高度为 1 英寸，当水面高度上升到 10 英寸时，监测器关闭水泵；水面高度下降到 5 英寸时，监测器打开水泵。水泵的开与关有 2s 的延迟。也就是从开/关水泵到水泵开始/停止工作，需要 2s 的时间。

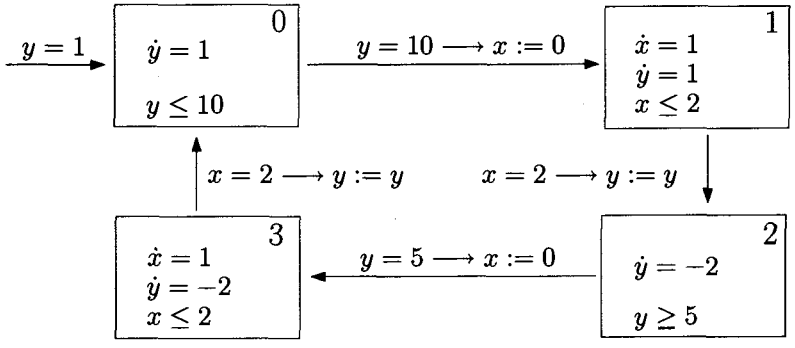


图 1　水面监测器系统

HPTL 不仅适用于刻画系统性质，由于引进了强大的'prj'操作符，它同样适用于描述系统行为。下面我们用 HPTL 公式描述图 1 所示的系统。

$p_1 \overset{def}{=} keep(\dot{y}=1) \wedge halt(y=10)$,

$p_2 \overset{def}{=} keep(\dot{x}=1 \wedge \dot{y}=1) \wedge halt(x=2)$,

$p_3 \overset{def}{=} keep(\dot{y}=-2) \wedge halt(y=5)$,

$p_4 \overset{def}{=} keep(\dot{x}=1 \wedge \dot{y}=-2) \wedge halt(x=2)$,

$q_0 \overset{def}{=} pc=0 \wedge y=1$,

$q_1 \overset{def}{=} pc=0 \wedge More \rightarrow \bigcirc(pc^+=1 \wedge y^+=y \wedge x^+=0)$

$q_2 \overset{def}{=} pc^+=1 \wedge More \rightarrow \bigcirc(pc^+=2 \wedge y^+=y)$,

$q_3 \overset{def}{=} pc^+=2 \wedge More \rightarrow \bigcirc(pc^+=3 \wedge y^+=y \wedge x^+=0)$,

$q_4 \overset{def}{=} pc^+=3 \wedge More \rightarrow \bigcirc(pc^+=0 \wedge y^+=y)$,

$q \overset{def}{=} q_0 \wedge \Box(q_1 \wedge q_2 \wedge q_3 \wedge q_4)$。

其中 $pc$ 是个用来表示系统所处状态的离散变量。水面监测器系统可由如下的 HPTL 描述：

$$(p_1,p_2,p_3,p_4)^{(+)}prj\ q \vee (p_1,(p_2,p_3,p_4,p_1)^{(+)}prj\ q \vee (p_1,p_2,(p_3,p_4,p_1,p_2)^{(+)})prj\ q \vee (p_1,p_2,p_3,(p_4,p_1,p_2,p_3)^{(+)}prj\ q \quad (1)$$

接下来我们验证 HPTL 公式(1)描述的图 1 所示的水面检测器系统满足性质'水面高度始终保持在 1 到 12 英寸之间'。该性质可以用 HPTL 公式描述为 $\Box(1 \leqslant y \leqslant 12)$。下面我们证明：

$$(p_1,p_2,p_3,p_4)^{(+)}prj\ q \vee (p_1,(p_2,p_3,p_4,p_1)^{(+)})prj\ q \vee (p_1,p_2,(p_3,p_4,p_1,p_2)^{(+)})prj\ q \vee (p_1,p_2,p_3,(p_4,p_1,p_2,p_3)^{(+)}prj\ q \rightarrow \Box(1 \leqslant y \leqslant 12) \quad (2)$$

对于任意的相位 $\eta=([a,b],l,g)$，如果 $\eta \models (p_1,p_2,p_3,p_4)^{(+)}prj\ q \vee (p_1,(p_2,p_3,p_4,p_1)^{(+)})prj\ q \vee (p_1,p_2,(p_3,p_4,p_1,p_2)^{(+)})prj\ q \vee (p_1,p_2,p_3,(p_4,p_1,p_2,p_3)^{(+)})prj\ q$，下面我们证明 $\eta \models \Box(1 \leqslant y \leqslant 12)$。

不失一般性，假设 $\eta \models (p_1,(p_2,p_3,p_4,p_1)^{(+)}prj\ q$，即存在 $k>0$，满足 $\eta \models (p_1,(p_2,p_3,p_4,p_1)^{(k)})prj\ q$。由公式 $p_1$，$p_2,p_3,p_4,q$ 的结构和'$prj$'的语义解释，存在 $a=r_0 \leqslant r_1 \leqslant \cdots \leqslant r_{4k+1} \leqslant b$ 使得 $\eta_{[r_0,r_1]} \models p_1, \eta_{[r_1,r_2]} \models p_2, \cdots, \eta_{[r_{4k},r_{4k+1}]} \models p_1$，并且

$$\eta \downarrow (r_0,r_1,\cdots,r_{4k+1}) = \langle (l(r_0),l(r_1),\cdots,l(r_{4k+1})) \rangle \models q$$

下面我们证明对于任意的 $0 \leqslant i \leqslant k$，有

$$g_y+(r_{4i})=1, g_y+(r_{4i+1})=10, g_y+(r_{4i+2})=12, g_y+(r_{4i+3})=5 \quad (3)$$

$$\begin{aligned} q &\approx q_0 \wedge q_1 \wedge q_2 \wedge q_3 \wedge q_4 \wedge \odot(\Box(q_1 \wedge q_2 \wedge q_3 \wedge q_4)) \\ &\approx pc=0 \wedge y=1 \wedge \bigcirc(pc^+=1 \wedge y^+=10 \wedge x^+=0) \wedge \bigcirc(\Box(q_1 \wedge q_2 \wedge q_3 \wedge q_4)) \\ &\approx pc=0 \wedge y=1 \wedge \bigcirc(pc^+=1 \wedge y^+=10 \wedge x^+=0 \wedge q_1 \wedge q_2 \wedge q_3 \wedge q_4 \wedge \odot(\Box(q_1 \wedge q_2 \wedge q_3 \wedge q_4)) \\ &\approx pc=0 \wedge y=1 \wedge \bigcirc(pc^+=1 \wedge y^+=10 \wedge x^+=0) \wedge \bigcirc^2(pc^+=2 \wedge y^1=12) \wedge \bigcirc^2(\Box(q_1 \wedge q_2 \wedge q_3 \wedge q_4)) \end{aligned}$$

可以归纳得到：

$$\begin{aligned} q \approx\ & pc=0 \wedge y=1 \wedge \bigcirc(pc^+=1 \wedge y^+=10 \wedge x^+=0) \wedge \bigcirc^2(pc^+=2 \wedge y^+=12) \wedge \bigcirc^3(pc^+=3 \wedge y^+=5 \wedge x^+=0) \wedge \bigcirc^4(pc^+=0 \wedge y^+=1) \wedge \bigcirc^5(pc^+=1 \wedge y^+=10 \wedge x^+=0) \wedge \bigcirc^5(\Box(q_1 \wedge q_2 \wedge q_3 \wedge q_4)) \end{aligned}$$

可以很容易地归纳证明 (3)成立，下面我们证明 (2)。

由于 $\eta_{[r_{4i},r_{4i+1}]} \models p_1$，并且 $p_1 \overset{def}{=} keep(\dot{y}=1) \wedge halt(y=10)$，因此 $\eta_{[r_{4i},r_{4i+1}]} \models keep(\dot{y}=1), \eta_{[r_{4i},r_{4i+1}]} \models halt(y=10)$。

由 $halt(x=d)$ 的定义知，如果 $\eta_{[r_{4i},r_{4i+1}]} \models halt(y=10)$，则 $g_y(r_{4i+1})=10$。$\eta_{[r_{4i},r_{4i+1}]} \models keep(\dot{y}=1)$ 说明 $y$ 是个区间 $[r_{4i}, r_{4i+1}]$ 上斜率始终为 1 的连续变量。由于 $g_y{}^+(r_{4i})=1$，因此，在区间 $[r_{4i}, r_{4i+1}]$ 上，恒有 $1 \leqslant y \leqslant 10$。即 $\eta_{[r_{4i},r_{4i+1}]} \models \Box(1 \leqslant y \leqslant 10)$。

类似地，如果 $\eta_{[r_{4i},r_{4i+2}]} \models halt(x=2)$，则 $g_x(r_{4i+2})=2$。$\eta_{[r_{4i},r_{4i+2}]} \models keep(\dot{x}=1) \wedge keep(\dot{y}=1)$ 说明 $x$ 和 $y$ 是区间 $[r_{4i+1}, r_{4i+2}]$ 上斜率都始终为 1 的连续变量。由于 $g_x{}^+(r_{4i+1})=0$，$g_y{}^+(r_{4i+1})=10$，因此，在区间 $[r_{4i+1}, r_{4i+2}]$ 上，恒有 $10 \leqslant y \leqslant 12$。即 $\eta_{[r_{4i+1},r_{4i+2}]} \models \Box(10 \leqslant y \leqslant 12)$。

同样的方法可以证明 $\eta_{[r_{4i+2},r_{4i+3}]} \models \Box(5 \leqslant y \leqslant 12)$，$\eta_{[r_{4i+3},r_{4i+4}]} \models \Box(1 \leqslant y \leqslant 5)$。因此，对任意的 $0 \leqslant j \leqslant 4k+1$，有 $\eta_{[r_j,r_{j+1}]} \models \Box(1 \leqslant y \leqslant 12)$。即(1)成立。

**结论** 本文定义了混合投影时序逻辑 HPTL，HPTL 不仅适用于刻画系统性质，也很适用于描述系统行为。这样，就可以在统一的模型框架下进行混合系统的验证。本文给出了 HPTL 的逻辑等价式系统，同时给出了一个用 HPTL 进行系统验证的实例。然而，本文仅仅对混合系统的验证进行了简单的尝试，验证实例采用的方法也只是逻辑推演。但是，本文定义了一种全新的逻辑，开辟了混合系统建模和验证的一个新的领域。作为今后的一项任务，我们将研究 HPTL 的模型检查问题，进行混合系统自动化验证的探索。

## 参 考 文 献


1 Duan Z. Modeling of hybrid systems: [Ph D thesis]. Shefield: Department of Computer Science. UK: University of Shefield, Department of Computer Science, 1997

2 Moskowski B. Executing Temporal Logic. UK: Cambridge University, Department of Computer Science, 1986

3 Kapur A, Henzinger T A, Manna Z, et al. Proving Safety Properties of Hybrid Systems. In: Formal Techniques in Real-Time and Fault-Tolerant Systems, LNCS 863, Springer-Verlag, 1994

4 Alur R, Courcoubetisz C, et al. The Algorithmic Analysis of Hybrid Systems. Theoretical Computer Science, 1995, 138(1): 3～34

5 Li G Y. LTLC: A Continuous-Time Temporal Logic for Real-Time and Hybrid Systems[D]: [Ph D thesis]. Beijing: Institute of Software, the Chinese Academy of Sciences, 2001

6 Henzinger T A, Kopke P W, Puri A, et al. What's Decidable About Hybrid Automata? J Comput Syst Sci, 1998, 57: 94～124

7 Alur R, Henzinger T A, Lafferriere G, et al. Discrete Abstractions of Hybrid Systems. Proceedings of the IEEE, 2000, 88(7): 971～984

8 Alur R, Courcoubetis C, Henzinger T A, et al. Hybrid Automata: An Algorithmic Approach to the Specification and Verification of Hybrid Systems. In: Proceedings of Hybrid Systems' 93, LNCS 736, Springer-Verlag, 1993


(上接第 273 页)

的更新操作均记录在日志中。当移动客户端重新连接上服务器时，Venus 将缓存中的数据重新集成至服务器中。在此过程中，若 Venus 探测到有数据分歧时，将启动移动客户端上的应用协调器来解决这样的不一致性，甚至在必要时需要人工介入。文[11]中采用了文[4]中的版本管理与加锁机制、文[6]中的分歧协调机制，给出了三类具体的更新算法，用以解决何时移动客户端应连接上 Web 服务器，使得整个通信开销达到最优。上述现有工作较少考虑当移动客户端发生失败情形时如何继续维持构件组装访问过程的高效与可靠。此外，在这些工作中，移动客户端与服务器进行交互时需要长久、持续地连接在无线网络中，并增加了一些不必要的网络连接开销。

本文针对无线移动环境中服务构件组装应用场景，给出一种基于移动 Agent 的无线环境中实时服务构件组装访问机制 MAWA，可有效避免移动客户端不必要的无线网络连接开销；同时该机制能根据应用的要求，重配置对服务构件的组装协同逻辑结构，从而能满足移动应用动态变化的需求；本文还对应用执行过程中关注于服务构件状态信息实时变化的可靠性及相关的执行开销进行分析，并提供了支持移动客户端发生故障后的状态恢复机制，从而确保了整个应用执行过程的可靠性。

进一步的工作包括移动 Agent 自身安全性的考虑、移动 Agent 在基点(base station)之间自主性迁移以更好适应移动设备切换(handoff)的需求，及利用移动 Agent 对构件组装信息进行数据压缩/解压缩以提高传输效率等方面。

## 参 考 文 献


1 Dhawan C. Mobile Computing: A systems Integrator's Handbook. McGraw- Hill, USA, 1997

2 Joshi A, Weerawarana S, Houstis E, On Disconnected Browsing of Distributed Information. In: Proceeding of the 7th IEEE Work-shop on Research Issues in Data Engineering RIDE, 1997. 101～107

3 Floyd R, Housel R, Tait C. Mobile Web access using eNetwork Web Express. IEEE Personal Communications, 1998, 5(5): 47～52

4 Whitehead E J, Wiggins M. WEBDAV: IEIF Standard for collaborative Authoring on the Web. IEEE Internet Computing, Sept. 1998, 2(5): 34～40

5 Mazer M S, Brooks C L. Writing the Web while disconnected. IEEE Personal Communications, 1998, 5(5): 35～41

6 Kaashoek M F, Pinckney T, Tauber J A. Dynamic documents: mobile wireless access to the WWW. In: IEEE Workshop on Mobile Computing Systems and Applications, Santa Cruz, CA, Dec 1994. 179～184

7 Debra V M, Anindya D, Kaushik D. Mobile User Recovery in the Context of Internet Transactions. IEEE Transactions on Mobile Computing, 2003, 2(2)

8 Jing A S. Client-Server Computing in Mobile Environ-ments. ACM Computing Survey, June 1999, 31(2): 117～157

9 Pitoura E, Samaras G. Data Management for Mobile Computing. Kluwer Academic Publishers, 1998

10 Floyd R, Housel R, Tait C. Mobile Web access using eNetwork Web Express. IEEE Personal Communications, 1998, 5(5): 47～52

11 Chen I R, Phan N A, Yen I L. Algorithms for Supporting Disconnected Write Operations for wireless Web Access in Mobile Client-Server Environments. IEEE Transactions on Mobile Computing, 2002, 1(1)

12 Pedregal-Martin C, Ramamritham K. Support for recovery in mobile Systems. IEEE Transactions on Computers, October 2002, 51(10)

13 胡海洋，马晓星，陶先平，等. 反射中间件的研究与进展. 计算机学报，2005, 28(9): 1407～1420

14 胡海洋，杨玫，陶先平，等. Cogent 后组装机制的研究与实现. 电子学报，2002, 30(12): 1823～1827