软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(3):366−380 [doi: 10.3724/SP.J.1001.2011.03918]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

有穷时间投影时序逻辑的完备公理系统*

舒新峰[1,2,3], 段振华[1,2+]

[1](西安电子科技大学 计算理论与技术研究所,陕西 西安 710071)

[2](西安电子科技大学 ISN 国家重点实验室,陕西 西安 710071)

[3](西安邮电学院 计算机学院,陕西 西安 710121)

Complete Axiomatization for Projection Temporal Logic with Finite Time

SHU Xin-Feng[1,2,3], DUAN Zhen-Hua[1,2+]

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

[2](State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China)

[3](School of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

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

Shu XF, Duan ZH. Complete axiomatization for projection temporal logic with finite time. *Journal of Software*, 2011,22(3):366−380. http://www.jos.org.cn/1000-9825/3918.htm

Abstract: To verify the properties of concurrent and reactive systems based on the theorem proving approach, a complete axiomatization is formulized over finite domains for first order projection temporal logic (PTL) with finite time. First, the syntax, semantics and the axiomatization of PTL are presented; next, a normal form (NF) and a normal form graph (NFG) of PTL formulas are defined respectively; further, the algorithm for constructing the NFG is formalized upon the NF; moreover, the decision theorem for PTL formulas and the completeness of the axiomatic system have been proven to be based on the property that the NFG can-describe the models of PTL formulas; finally, an example is given to illustrate how to do system verification based on PTL and its axiomatic system, and the results indicate that the PTL based theorem proving approach can be conveniently applied to modeling and verification of concurrent systems.

Key words: projection temporal logic; axiomatization; completeness proof; theorem proving; formal method

摘 要: 为采用定理证明的方法对并发及交互式系统进行验证,研究了有穷论域下有穷时间一阶投影时序逻辑(projection temporal logic,简称 PTL)的一个完备公理系统.在介绍 PTL 的语法、语义并给出公理系统后,提出了 PTL 公式的正则形(normal form,简称 NF)和正则图(normal form graph,简称 NFG).基于 NF 给出了 NFG 的构造算法,并利用 NFG 可描述公式模型的性质证明 PTL 公式的可满足性判定定理和公理系统的完备性.最后,结合实例展示了 PTL 及其公理系统在系统验证中的应用.结果表明,基于 PTL 的定理证明方法可方便用于并发系统的建模与验证.

关键词: 投影时序逻辑;公理系统;完备性证明;定理证明;形式化方法

中图法分类号: TP301 **文献标识码**: A

* 基金项目: 国家自然科学基金(60433010, 60910004, 60873018, 91018010, 61003078, 61003079); 国家重点基础研究发展计划(973)(2010CB328102); 中央高校基本科研业务费专项资金(JY10000903004)

收稿时间:2010-04-06; 修改时间: 2010-06-09; 定稿时间: 2010-07-28

© 中国科学院软件研究所 http://www.jos.org.cn

一阶投影时序逻辑(projection temporal logic,简称 PTL)[1]是一阶区间时序逻辑(interval temporal logic,简称 ITL)[2]的扩展,引入了全新投影操作符 *prj*,并同时支持有穷和无穷模型,具备了完全正则表达式的表达能力,能够方便地描述顺序、选择、循环、并发、信号量等程序结构[3],可在同一 PTL 逻辑框架内完成对待验证系统的建模和性质描述,适用于各类软硬件系统的验证[4−7].

在过去的 20 多年里,已经有一些时序逻辑的公理系统面世并在并发及反应式系统的验证中取得了成功,然而研究的重点主要集中在命题时序逻辑方面[8,9].由于一阶时序逻辑本身不可判定,而且有许多派生的一阶时序逻辑甚至不是递归可枚举的,因此,一阶时序逻辑真正的完备性无法建立[10],只能寻求相对完备性[11],或者对一阶时序逻辑加以限制从而实现完备性[12].

文献[13]给出了 PTL 的一个公理系统及验证实例,然而并没有证明公理系统的完备性.笔者将 PTL 公理系统的完备性证明分为有穷时间和无穷时间分别进行研究,本文只涉及有穷时间下的情况.为实现完备性,采取了与 QPTL(quantified propositional temporal logic)[14]及 ITL[15]的公理系统类似的策略,将 PTL 的论域限制为有穷,然而该论域可以是任何的有穷域,如整数、集合、线性表等,而不仅仅是布尔或者有穷整数集合.此外,PTL 的公理系统同时支持时态项(带有时态操作符的项)、函数和谓词,这是目前已知的首次全部支持这些项的时序逻辑公理系统.

为证明完备性,将命题投影时序逻辑(propositional projection temporal logic,简称 PPTL)公式的正则形及正则图技术[16]扩展到一阶投影时序逻辑中,提出了 PTL 的正则形及正则图,并基于正则图的性质证明了 PTL 逻辑公式的可满足性判定定理及公理系统的完备性.

本文第 1 节回顾 PTL 的语法和语义.第 2 节给出 PTL 在有穷时间下的公理系统和一些定理.第 3 节提出 PTL 的正则形与正则图,并给出正则图的构造算法.第 4 节证明 PTL 公式的可满足性判定定理和 PTL 公理系统的完备性.第 5 节通过实例展示 PTL 及其公理系统在并发系统的验证应用.最后,对全文的工作进行总结.

1 投影时序逻辑

1.1 语 法

定义 1. 令 *Prop* 是原子命题的可数集合;V 为静态变量和动态变量的可数集合,为任何数据类型的有穷论域;N_0 为非负整数集合.一阶投影时序逻辑的项 e 和公式 P 归纳定义如下[1]:

$$e ::= d \mid a \mid x \mid \bigcirc e \mid f(e_1,...,e_n),$$

$$P ::= p \mid \neg P \mid P_1 \vee P_2 \mid \bigcirc P \mid \exists v.P \mid (P_1,...,P_m)\, prj\, P,$$

其中,$d \in D$ 为常量,$a \in V$ 是静态变量,$x \in V$ 是动态变量,$v \in V$ 是任意的静态或者动态变量,$p \in Prop$ 为原子命题,$P_1,\ldots,P_m$ 及 P 为 PTL 的合式公式,$f(e_1,\ldots,e_n)$与$\rho(e_1,\ldots,e_n)$分别表示带有 n 元参数的函数与谓词,○(next)及 *Prj*(projection)是原始时态操作符.

定义 2. 除了连接符∧、→、↔、全称量词∀及公式 *true* 和 *false* 的定义与经典一阶逻辑相同外,使用如下派生的时态公式[1]:

$$\varepsilon \stackrel{\text{def}}{=} \neg\bigcirc true \qquad \overline{\varepsilon} \stackrel{\text{def}}{=} \neg\varepsilon$$

$$\odot P \stackrel{\text{def}}{=} \neg\bigcirc\neg P \qquad P;Q \stackrel{\text{def}}{=} (P,Q)\, prj\, \varepsilon$$

$$\Diamond P \stackrel{\text{def}}{=} true;P \qquad \Box P \stackrel{\text{def}}{=} \neg\Diamond\neg P$$

$$\bigcirc^0 P \stackrel{\text{def}}{=} P \qquad \bigcirc^n P \stackrel{\text{def}}{=} \bigcirc(\bigcirc^{n-1} P),\ n > 0$$

$$len(n) \stackrel{\text{def}}{=} \bigcirc^n \varepsilon \qquad keep(P) \stackrel{\text{def}}{=} \Box(\overline{\varepsilon} \rightarrow P)$$

$$fin(P) \stackrel{\text{def}}{=} \Box(\varepsilon \rightarrow P) \qquad halt(P) \stackrel{\text{def}}{=} \Box(\varepsilon \leftrightarrow P)$$

$$P \parallel Q \stackrel{\text{def}}{=} ((P;true) \wedge Q) \vee (P \wedge (Q;true)) \vee (P \wedge Q)$$

© 中国科学院软件研究所 http://www.jos.org.cn

其中,○(weak-next),;(chop), ◇ (sometimes), □ (always)及‖(parallel)是派生的时态操作符.

定义 3. 投影时序逻辑操作符的优先级定义如下(数字越小优先级越高)[1]:

1 ¬ 2 ○, ⊙, □, ◇ 3 ∃, ∀ 4 = 5 ∧ 6 ∨, ‖ 7 →, ↔ 8 *prj*, ;

如果一个公式(项)不包含时态操作符,则称该公式为状态公式(项),否则称它为时态公式(项);如果一个公式(项)不包含动态变量,则称其为静态公式(项).约定大写字母 $P,Q,\ldots$及其带下标的形式表示任意的 PTL 公式,小写字母 $p,q,...$表示任意的原子命题,带下标的小写字母 $p_s,q_1,\ldots$表示任意的状态公式.另外,统称原子命题公式 p 以及不包含时态项的等词公式 $e_1=e_2$ 和谓词公式$\rho(e_1,\ldots,e_n)$为原子公式,并用符号φ表示.

1.2 语 义

定义 4(语义模型). 状态 s 是一个赋值的序偶(I_p,I_v).对于任意变量 $v\in V$,有 $s[v]=I_v[v],I_v[v]\in D$ 表示变量的值;对于任意 $p\in Prop$,有 $s[p]=I_p[p]\in\{true,false\}$.PTL 的解释区间(模型)是一个非空的有穷状态序列$\sigma=\langle s_0,...,s_{|\sigma|}\rangle$,其长度记为$|\sigma|$,为状态个数减 1.对于任意的区间$\sigma=\langle s_0,...,s_{|\sigma|}\rangle$与 $\sigma'=\langle s'_0,...,s'_{|\sigma'|}\rangle$,$\sigma$与$\sigma'$之间的连接运算(•)表示为$\sigma\bullet\sigma'$且 $\sigma\bullet\sigma'=\langle s_0,...,s_{|\sigma|},s'_0,...,s'_{|\sigma'|}\rangle$.为定义投影操作符的语义,需要区间上的一个辅助运算符↓.令$\sigma=\langle s_0,...,s_{|\sigma|}\rangle$为任意一个区间,对于 $r_1,\ldots,r_h\in N_0(h\geqslant 1)$且 $0\leqslant r_1\leqslant\ldots\leqslant r_h\leqslant|\sigma|$,$\sigma$在 $r_1,\ldots,r_h$ 上的投影区间定义为

$$\sigma\downarrow(r_1,...,r_h)=\langle s_{t_1},...,s_{t_l}\rangle\ (t_1<...<t_l),$$

其中,$t_1,\ldots,t_l$ 是在 $r_1,\ldots,r_h$ 中删除所有重复项而得到严格递增序列.公式(项)的解释是一个三元组 $I=(\sigma,i,j),i,j\in N_0$ 且 $0\leqslant i\leqslant j\leqslant|\sigma|$,表示公式(项)在区间$\sigma_{(i..j)}$上且当前状态是 s_i 时的解释[1]. 例如,

$$\langle s_0,s_1,s_2,s_3,s_4,s_5\rangle\downarrow(0,2,2,4,4,5)=\langle s_0,s_2,s_4,s_5\rangle.$$

定义 5. 项 e 相对于解释 I 的值,记为 $I[e]$,归纳定义如下[1]:

- $I[d]=d$,其中 $d\in D$ 为常量;
- $I[a]=s_i[a]=I_v^i[a]=s_0=I_v^0[a]$,其中,$a\in V$ 为静态变量;
- $I[x]=s_i[x]=I_v^i[x]$,其中,$x\in V$ 为动态变量;
- $I[f(e_1,...,e_n)]=\begin{cases}f(I[e_1],...,I[e_n]), & \text{对于任意}e_h(1\leqslant h\leqslant n)\text{满足}I[e_h]\neq nil\\ nil, & \text{其他情况}\end{cases}$;
- $I[\bigcirc e]=\begin{cases}(\sigma,i+1,j)[e], & i<j\\ nil, & \text{其他情况}\end{cases}$.

在项的解释中,考虑到 D 上的某些函数 f 可能为部分函数,其会返回一个未定义的值,特引入一个特殊值 nil(未定义)将其扩充为全函数.扩充后的论域为 $D'=D\cup\{nil\}$.等词与谓词在 D'上的定义保持不变.

定义 6. 对于任意变量 v,区间σ与σ'是 v–等价的,记为 $\sigma'\overset{v}{=}\sigma$,当且仅当$\sigma$与$\sigma'$除了可以对变量 v 赋给不同的值之外,其他完全相同[1].

定义 7. PTL 公式的可满足关系(⊨)归纳定义如下[1]:

- $I\models p$ 当且仅当 $s_i[p]=I_p^i[p]=true$;
- $I\models\rho(e_1,\ldots,e_n)$ 当且仅当 ρ为除等词(=)之外的原子谓词,任何 $I[e_h]\neq nil(1\leqslant h\leqslant n)$,并且$\rho(I[e_1],\ldots,I[e_n])=true$;
- $I\models e_1=e_2$ 当且仅当 $I[e_1]\neq nil,I[e_2]\neq nil$ 并且 $I[e_1]=I[e_2]$;
- $I\models\neg P$ 当且仅当 $I\not\models P$;
- $I\models P\vee Q$ 当且仅当 $I\models P$ 或 $I\models Q$;
- $I\models\exists v.P$ 当且仅当 存在区间$\sigma',\sigma'_{(i,..,j)}\overset{v}{=}\sigma_{(i,..,j)}$ 且$(\sigma',i,j)\models P$;
- $I\models\bigcirc P$ 当且仅当 $i<j$ 且$(\sigma,i+1,j)\models P$;
- $I\models(P_1,\ldots,P_m)prjP$ 当且仅当 存在整数 $i=r_0\leqslant\ldots\leqslant r_m\leqslant j$ 使得对于任何 $1\leqslant l\leqslant m,(\sigma,r_{l-1},r_l)\models P_l$ 且$(\sigma',0,|\sigma|)\models P$,其中,$\sigma'$为以下两种情况之一:

(1) $r_m<j$ 时,$\sigma'=\sigma\downarrow(r_0,...,r_m)\bullet\sigma_{(r_m+1,..,j)}$;

© 中国科学院软件研究所 http://www.jos.org.cn

(2) $r_m=j$ 时存在某个 $h,\sigma'=\sigma\downarrow(r_0,\ldots,r_h)$.

定义 8(可满足性与有效性). 公式 P 是可满足的,当且仅当存在区间$\sigma,(\sigma,0,|\sigma|)\models P$ 成立,简记为$\sigma\models P$.P 是有效的,当且仅当对于所有区间$\sigma,\sigma\models P$ 成立,简记为$\models P$.为描述方便,简记$\models P\leftrightarrow Q$ 为 $P\equiv Q$,并简记$\models P\rightarrow Q$ 为 $P\supset Q$[1].

2 PTL 的公理系统

定义 9. 令τ表示任何的公式(项),t 为一个项,v 是τ中出现的一个变量,$\tau[t/v]$表示同时将τ中所有自由出现的 v 替换为 t 所得到公式(项).如果 v 与 t 均是静态项或者 v 是动态变量,且 t 中出现的变量没有以约束变元的形式在τ中出现,则称替换$\tau[t/v]$对于$\tau(v)$是相容的,或称 t 与 v 在$\tau(v)$下是替换相容,并使用$\tau(t)$来表示$\tau[t/v]$[1].

符号$\vdash$表示公理系统中的形式可推演关系.为方便起见,将$\vdash(P\leftrightarrow Q)$简记为 $P\cong Q$,并简记$\vdash(P\rightarrow Q)$为 $P\sqsupset Q$,符号“$\Rightarrow$”表示推导出.在深入研究了 PTL 的语法和语义,分析参考已有的 QPTL 及 ITL 公理系统[14,15],并经过数百计的定理证明验证和优化后,提炼出的有穷时间 PTL 的公理系统,见表 1.

Table 1 Axiomatization for PTL with finite time

表 1 有穷时间投影时序逻辑的公理系统

Axioms	AT	$\vdash P$, where P is a substitution instance of classical first order tautology	FIN	$P\sqsupset\Diamond\varepsilon$
	AXO	$\bigcirc(P\vee Q)\cong\bigcirc P\vee\bigcirc Q$	AXC	$\bigcirc(P;Q)\cong\bigcirc P;Q$
	AXN	$\neg\bigcirc P\cong\varepsilon\vee\bigcirc\neg P$	APEF	$\varepsilon\ prj\ Q\cong Q$
	APEB1	$P\ prj\ \varepsilon\cong P$	APEB2	$(P_1,\ldots,P_m)\ prj\ \varepsilon\cong P_1;\ldots;P_m$, $m>1$
	APX1	$(P_1\wedge\overline{\varepsilon})\ prj\ \bigcirc Q\cong P_1\wedge\overline{\varepsilon};\ Q$	APX2	$(P_1\wedge\overline{\varepsilon},\ldots,P_m)\ prj\ \bigcirc Q\cong P_1\wedge\overline{\varepsilon};(P_2,\ldots,P_m)\ prj\ Q$
	ATSX	$\overline{\varepsilon}\sqsupset(e_s=\bigcirc e_s)$, where e_s is a static state term	AEX	$\exists x.(p_s\wedge\bigcirc P)\cong\exists x.p_s\wedge\bigcirc\exists x.P$
	AUR	$\forall v.P(v)\sqsupset P(e)$	AEI	$P(e)\sqsupset\exists v.P(v)$, where v does not quantified in $P(v)$
	ATSR	$e_s=e'_s\wedge P(e_s)\cong e_s=e'_s\wedge P(e'_s)$, where $P(v)$ is a formula-expression, e_s and e'_s are static state terms		
	ATXE	$e_1=e_2(t_1,\ldots,\bigcirc t_i,\ldots,t_m)\cong\exists a.(e_1=e_2(t_1,\ldots,a,\ldots,t_m)\wedge\bigcirc(a=t_i))$, where e_2 is a term-expression, e_1 and $t_1,\ldots,\bigcirc t_i,\ \ldots,t_m$ are terms, a is a fresh static variable which does not appear in $e_1=e_2(t_1,\ldots,\bigcirc t_i,\ldots,t_m)$		
	ATXP	$\rho(t_1,\ldots,\bigcirc t_i,\ldots,t_m)\cong\exists a.(\rho(t_1,\ldots,a,\ldots,t_m)\wedge\bigcirc(a=t_i))$, where $t_1,\ldots,\bigcirc t_i,\ldots,t_m$ are terms and a is a fresh static variable which does not appear in $\rho(t_1,\ldots,\bigcirc t_i,\ldots,t_m)$		
	APS	$(p_s\wedge P_1,\ldots,P_m)\ prj\ Q\cong p_s\wedge(P_1,\ldots,P_m)\ prj\ Q\cong(P_1,\ldots,P_m)\ prj\ p_s\wedge Q$		
	APF	$(P_1,\ldots,P_i,\ldots,P_m)\ prj\ Q\cong(P_1,\ldots,P_i\wedge\Diamond\varepsilon,\ldots,P_m)\ prj\ Q$, where, $1\leqslant i<m$		
	APOF	$(P_1,\ldots,P_i\vee P'_i,\ldots,P_m)\ prj\ Q\cong((P_1,\ldots,P_i,\ldots,P_m)\ prj\ Q)\vee((P_1,\ldots,P'_i,\ldots,P_m)\ prj\ Q)$		
	APOB	$(P_1,\ldots,P_m)\ prj\ (Q\vee Q')\cong((P_1,\ldots,P_m)\ prj\ Q)\vee((P_1,\ldots,P_m)\ prj\ Q')$		
	APSEF	$(P_1,\ldots,p_s\wedge\varepsilon,P_i,\ldots,P_m)\ prj\ Q\cong(P_1,\ldots,p_s\wedge P_i,\ldots,P_m)\ prj\ Q$		
	APSEB	$(P_1,\ldots,P_i,p_s\wedge\varepsilon,\ldots,P_m)\ prj\ Q\cong(P_1,\ldots,\Diamond(p_s\wedge\varepsilon)\wedge P_i,\ldots,P_m)\ prj\ Q$		
	AEPF	$\exists v.(P_1,\ldots,P_i,\ldots,P_m)\ prj\ Q\cong(P_1,\ldots,\exists v.P_i,\ldots,P_m)\ prj\ Q$, where v does not occur freely in sub-formulas $P_1,\ldots,P_m$ (except for P_i) and Q		
	AEPB	$\exists v.(P_1,\ldots,P_m)\ prj\ Q\cong(P_1,\ldots,P_m)\ prj\ \exists v.Q$, where v does not occur freely in sub-formulas $P_1,\ldots,P_m$		
	ADF	$f(d_1,\ldots,d_m)=d$, where $d_1,\ldots,d_m$ and d have the mapping relation f over domain D		
	ADPT	$\rho(d_1,\ldots,d_m)\cong true$, where $d_1,\ldots,d_m$ have the m-place relation ρ over D		
	ADPF	$\rho(d_1,\ldots,d_m)\cong false$, where $d_1,\ldots,d_m$ do not have the m-place relation ρ over D		
Inference rules	IXR	$P\sqsupset\bigcirc P\vee Q\ \Rightarrow\ P\sqsupset\Diamond Q$	IAG	$\vdash P\ \Rightarrow\ \vdash\bigcirc P$
	IMP	$\vdash(P\rightarrow Q),\vdash P\Rightarrow\vdash Q$	IRUG	$\vdash P\Rightarrow\vdash\forall v.P$, for any variable v
	IR	$P_1\cong P_2\ \Rightarrow\ Q\cong Q[P_1/P_2]$, where $Q[P_1/P_2]$ denotes the formula given by replacing some occurrences of P_2 in Q by P_1		
	IPG	$P_1\sqsupset P'_1,\ldots,P_m\sqsupset P'_m,Q\sqsupset Q'\ \Rightarrow\ (P_1,\ldots,P_m)\ prj\ Q\sqsupset(P'_1,\ldots,P'_m)\ prj\ Q'$		

© 中国科学院软件研究所 http://www.jos.org.cn

不难证明,PTL 的公理系统是可靠的.即在模型系统下,所有公理均有效且所有推导规则均保持推论有效.本文不给出可靠性的证明细节,而专注于完备性证明.

从 PTL 的公理系统可以推导出许多实用的定理.由于篇幅所限,只在表 2 中列举出完备性证明和验证实例里用到的一些定理,并忽略了相关证明.

Table 2 Some theorems of PTL

表 2 投影时序逻辑的一些定理

TXM	$\bigcirc P=\overline{\varepsilon}\wedge\bigcirc P$	TXC	$\bigcirc P=len(1);P$
TXF	$\bigcirc false\cong false$	TXA	$\bigcirc(P\wedge Q)\cong\bigcirc P\wedge\bigcirc Q$
TCOF	$P_1\vee P_2;Q\cong(P_1;Q)\vee(P_2;Q)$	TCOB	$P;Q_1\vee Q_2\cong(P;Q_1)\vee(P;Q_2)$
TCE	$\varepsilon;P\cong P\cong P;\varepsilon$	TRSA	$(p_s\wedge P)\|Q\cong p_s\wedge(P\|Q)\cong P\|(p_s\wedge Q)$
TCSA	$p_s\wedge P;Q\cong p_s\wedge(P;Q)$	TCF	$false;P\cong P;\ false\cong false$
TCS	$(P;Q);R\cong P;(Q;R)$	TSC	$p_s\cong p_s;true$
TSR	$\Diamond P\cong P\vee\bigcirc\Diamond P$	TSF	$\Diamond false\cong false$
TSD	$\Diamond\Diamond P\cong\Diamond P$	TCA	$P\wedge Q;R\sqsupset(P;R)\wedge(Q;R)$
TAR	$\Box P\cong P\wedge\varepsilon\vee P\wedge\bigcirc\Box P$	TAA	$\Box(P\wedge Q)\cong\Box P\wedge\Box Q$
TECF	$\exists v.(P;Q)\cong(\exists v.P;Q)$, where v does not occur freely in sub-formula Q	TECB	$\exists v.(P;Q)\cong(P;\exists v.Q)$, where v does not occur freely in sub-formula P
DICI	$P\sqsupset P',Q\sqsupset Q'\Rightarrow(P;Q)\sqsupset(P';Q')$	DIRI	$P\sqsupset P',Q\sqsupset Q'\Rightarrow(P\|Q)\sqsupset(P'\|Q')$

3 PTL 的正则形与正则图

ITL 领域的正则形最初出现在文献[1]中,用来捕获区间时序逻辑程序的语义模型.文献[8]将正则形引入到命题区间时序逻辑(propositional interval temporal logic,简称 PITL)中,利用 PITL 公式的正则形构造 Tableau 图解决了有穷时间下 PITL 公式的判定问题.文献[16]提出了 PPTL 公式的正则形和正则图技术,并基于该技术给出了 PPTL 公式在有穷及无穷模型下的判定算法,该算法同样适用于 PITL 公式的可满足性判定.相比于 Tableau 图,正则图更加简洁,并且对于同样的逻辑公式,正则图的节点数远小于对应的 Tableau 图.本文将 PPTL 正则形及正则图技术扩展到 PTL 中,以解决 PTL 逻辑公式在有穷时间有穷论域下的可满足性判定问题,进而证明公理系统的完备性.

3.1 正则形

定义 10(基础合取项与最小合取项). 一个基础合取项是 *true* 或 *false* 或由文字(literal)构成的合取公式,其中一个文字或者是 p 或$\neg p(p\in Prop)$,或者是形如 $v=d(v\in V,d\in D)$的等词公式.如果一个基础合取项满足下面两个条件,则称其为最小合取项:

- 对于任何原子命题 $p\in Prop$,p 与$\neg p$ 不能同时出现;
- 对于任何变量 $v\in V$ 和任意两个不相等常量 $d,d'\in D$,等词公式 $v=d$ 和 $v=d'$不能同时出现.

定义 11. 对于任意的 PTL 公式集合Γ_1与Γ_2,Γ_1与Γ_2的合取运算$\Gamma_1\wedge\Gamma_2$定义为

$$\Gamma_1\wedge\Gamma_2=\begin{cases}\{P_1\wedge P_2\mid P_1\in\Gamma_1,P_2\in\Gamma_2\}, & \text{其中},\Gamma_1\neq\varnothing\text{且}\Gamma_2\neq\varnothing\\ \Gamma_1, & \text{其中},\Gamma_2=\varnothing\\ \Gamma_2, & \text{其中},\Gamma_1=\varnothing\end{cases}.$$

定义 12(正则形). 对于 PTL 公式 P,令 P 中出现的原子命题集合为Φ^P,P 中出现的自由变量集合为 V^P,Σ^P 为Φ^P与 V^P上所有最小合取项的集合,即

$$\Sigma^P=\cup_{\Phi_s\subseteq\Phi^P}\cup_{V_s\subseteq V^P}(\bigwedge_{p_i\in\Phi_s}\{p_i,\neg p_i\}\wedge\bigwedge_{v_j\in V_s}\{v_j=d_k\mid d_k\in D\})\cup\{true,false\}.$$

(不难证明$|\Sigma^P|\leqslant 3^{|\Phi^P|}\bullet(|D|+1)^{|V^P|}$).$P$ 的正则形(normal form,简称 NF)定义为

$$P\cong\bigvee_{j=1}^{n_0}(p_{ej}\wedge\varepsilon)\vee\bigvee_{i=1}^{n}(p_{ci}\wedge\bigcirc P_i'),$$

© 中国科学院软件研究所 http://www.jos.org.cn

其中,$p_{ei}\in\Sigma^P$ 且 $p_{ci}\in\Sigma^P$ 为不含量词的状态公式; P_i' 为一般的 PTL 公式;$1\leqslant n_0\leqslant|\Sigma^P|$且 $1\leqslant n\leqslant|\Sigma^P|$.正则形中的 $p_{ei}\wedge\varepsilon$ 称为终端分量, $p_{ci}\wedge\bigcirc P_i'$ 称为未来分量, P_i' 称为 P 的后继公式.

特别地,如果 $\bigvee_{i=1}^{n}p_{ci}\cong\text{true}$ 且 $\bigvee_{i\neq k}(p_{ci}\wedge p_{ck})\cong false$,则称该正则形为完全正则形(complete normal form,简称 CNF).为了证明方便,有时将正则形中的 $\bigvee_{j=1}^{n_0}(p_{ej}\wedge\varepsilon)$ 简写为 $p_e\wedge\varepsilon$,将 $\bigvee_{i=1}^{n}(p_{ci}\wedge\bigcirc P_i')$ 简写为

$$\bigvee_{i=1}^{n}(p_i\wedge\bigcirc P_i').$$

例如,对于公式 $P\cong p\wedge x_1<2\wedge\bigcirc(x_2\geqslant 1)$,如果 $D=\{1,2\}$,则 $\Phi^P=\{p\}$,$V^P=\{x_1,x_2\}$,且 $\Sigma^P=\{true,false,p,\neg p,x_1=1,x_1=2,x_2=1,x_2=2,p\wedge x_1=1,p\wedge x_1=2,\neg p\wedge x_1=1,\neg p\wedge x_1=2,p\wedge x_2=1,p\wedge x_2=2,\neg p\wedge x_2=1,\neg p\wedge x_2=2,p\wedge x_1=1\wedge x_2=1,p\wedge x_1=1\wedge x_2=2,p\wedge x_1=2\wedge x_2=1,p\wedge x_1=2\wedge x_2=2,\neg p\wedge x_1=1\wedge x_2=1,\neg p\wedge x_1=1\wedge x_2=2,\neg p\wedge x_1=2\wedge x_2=1,\neg p\wedge x_1=2\wedge x_2=2\}$.$P$ 的正则形为

$$p\wedge x_1=1\wedge\bigcirc(x_2\geqslant 1).$$

完全正则形在“非”运算下封闭[8,16],即如果公式 P 的完全正则形如定义 12 所示,则$\neg P$ 的完全正则形为 $(\bigwedge_{j=1}^{n_0}\neg p_{ej}\wedge\varepsilon)\vee\bigvee_{i=1}^{n}(p_{ci}\wedge\bigcirc\neg P_i')$.另外,任意的正则形可以等价地转变为完全正则形,具体证明如下.

引理 1. 对于任意 PTL 公式 P,如果 P 能够等价地转换为 NF,则 P 也能等价地转换为 CNF.

证明:采用构造证明法.首先,基于 P 的 NF 构造一个 CNF Q,然后证明 $P\cong Q$.

假设 P 的 NF 为 $P\cong p_e\wedge\varepsilon\vee\bigvee_{i=1}^{n}(p_i\wedge\bigcirc P_i')$.令 Φ为公式 $\bigvee_{i=1}^{n}p_i$ 中出现的原子命题集合,X 为 $\bigvee_{i=1}^{n}p_i$ 中出现的变量集合.基于 Φ和 X 构造集合最小合取项集合 $\Psi=\bigwedge_{p_i\in\Phi}\{p_i,\neg p_i\}\wedge\bigwedge_{v_j\in X}\{v_j=d_k\mid d_k\in D\}$.特别地,如果 Φ=∅且 X=∅,则令 Ψ={*true*,*false*}.显然,对于任意的 $\psi_i,\psi_j\in\Psi$,有 $\bigvee_{i=1}^{|\Psi|}\psi_i\cong true$ 且 $\bigvee_{i\neq j}(\psi_i\wedge\psi_j)\cong false$.

接着,基于 Ψ构造 CNF Q 为 $Q\cong false\wedge\varepsilon\vee\bigvee_{j=1}^{|\Psi|}(\psi_j\wedge\bigcirc false)$.不难证明 $Q\cong false$.

最后,将 P 的 NF 合并到 Q 中.对于 P 的 NF 中任何一个合取分量 $\overline{P}$,如果 $\overline{P}$ 为终端分量 $p_e\wedge\varepsilon$,则称令 Q 等于 $Q\vee\overline{P}$;否则, $\overline{P}$ 必然为未来分量 $p_i\wedge\bigcirc P_i'$.此时,对于 Q 中所有未来分量 $\psi_j\wedge\bigcirc Q_j'$,如果 p_i 为 ψ_j 的子公式,即 $\psi_j\sqsupset p_i$,将 Q 中的 $\psi_j\wedge\bigcirc Q_j'$ 替换为 $\psi_j\wedge\bigcirc(Q_j'\vee P_i')$.

经过上面的合并后,Q 仍然保持为 CNF.下面证明 $Q\cong P$.对于 Q 中任何一个未来分量 $\psi_j\wedge\bigcirc Q_j'$,根据定理 TXO,可以等价地转换为 $\psi_j\wedge\bigcirc Q_j'\cong\psi_j\wedge\bigcirc P_{i_1}'\vee\ldots\vee\psi_j\wedge\bigcirc P_{i_k}'$,其中, $Q_j'\cong P_{i_1}'\vee\ldots\vee\bigcirc P_{i_k}'$.从而,可以将 Q 等价地转换为 $Q'\cong p_e\wedge\varepsilon\vee\bigvee_{i=1}^{n}((\psi_{j_1}^i\vee\ldots\vee\psi_{j_m}^i)\wedge\bigcirc P_i')$.对于任何一个 $(\psi_{j_1}^i\vee\ldots\vee\psi_{j_m}^i)(1\leqslant i\leqslant n)$,根据 Ψ的构造以及前面的替换规则,有 $\psi_{j_1}^i\vee\ldots\vee\psi_{j_m}^i\cong p_i$,从而有 $Q\cong Q'\cong P$. □

引理 2. 对于任意的原子公式φ,φ能被等价地转换为 NF.

证明:原子公式φ只能是以下几种情况:

- φ为原子命题 p.根据公理 AT,有 $p\cong p\wedge(\bigcirc true\vee\neg\bigcirc true)\cong p\wedge\varepsilon\vee p\wedge\bigcirc true$.
- φ为带有变量 $v_1,\ldots,v_m(m\geqslant 0)$等词公式 $e_1=e_2$.根据公理 AT,有

$$e_1=e_2\cong\bigvee_{k_1=1}^{|D|}\ldots\bigvee_{k_m=1}^{|D|}(v_1=d_{k_1}\wedge\ldots\wedge v_m=d_{k_m}\wedge(e_1=e_2)[d_{k_1}/v_1]\ldots[d_{k_m}/v_m]\wedge\varepsilon)\vee$$
$$\bigvee_{k_1=1}^{|D|}\ldots\bigvee_{k_m=1}^{|D|}(v_1=d_{k_1}\wedge\ldots\wedge v_m=d_{k_m}\wedge(e_1=e_2)[d_{k_1}/v_1]\ldots[d_{k_m}/v_m]\wedge\bigcirc true).$$

  而对于其中的子公式 $(e_1=e_2)[d_{k_1}/v_1]\ldots[d_{k_m}/v_m]$,由于不包含任何变量,根据公理 AT、公理 ADF 及推导规则 IR 将其进一步化简为 *true* 或 *false*,从而可将上公式等价地转换为 NF.
- φ为带有变量 $v_1,\ldots,v_m(m\geqslant 0)$原始谓词公式$\rho(e_1,\ldots,e_n)$.根据公理 AT,有

$$\rho(e_1,\ldots,e_n)\cong\bigvee_{k_1=1}^{|D|}\ldots\bigvee_{k_m=1}^{|D|}(v_1=d_{k_1}\wedge\ldots\wedge v_m=d_{k_m}\wedge\rho(e_1,\ldots,e_n)[d_{k_1}/v_1]\ldots[d_{k_m}/v_m]\wedge\varepsilon)\vee$$
$$\bigvee_{k_1=1}^{|D|}\ldots\bigvee_{k_m=1}^{|D|}(v_1=d_{k_1}\wedge\ldots\wedge v_m=d_{k_m}\wedge\rho(e_1,\ldots,e_n)[d_{k_1}/v_1]\ldots[d_{k_m}/v_m]\wedge\bigcirc true).$$

  同理,对于不包含任何变量的子公式 $\rho(e_1,\ldots,e_n)[d_{k_1}/v_1]\ldots[d_{k_m}/v_m]$,根据公理 AT、公理 ADF、公理 ADPT、公理 ADPF 及推导规则 IR 将其进一步化简为 *true* 或 *false*,从而也可将上公式进一步等价地转换为 NF. □

引理 3. 对于任意的存在公式$\exists v.P$,如果 P 能等价地转换为 NF,则$\exists v.P$ 也能等价地转换为 NF.

© 中国科学院软件研究所 http://www.jos.org.cn

证明:假设公式 P 的 NF 为 $\bigvee_{j=1}^{n_0}(p_{ej}\wedge\varepsilon)\vee\bigvee_{i=1}^{n}(p_{ci}\wedge\bigcirc P_i')$.当 v 为动态变量 x 时,由公理 AT、公理 AEX 及推导规则 IR,有

$$\begin{aligned}\exists x.P &\cong \exists x.(\bigvee_{j=1}^{n_0}(p_{ej}\wedge\varepsilon))\vee\bigvee_{i=1}^{n}(p_{ci}\wedge\bigcirc P_i')\\ &\cong \bigvee_{k=1}^{|D|}\bigvee_{j=1}^{n_0}(p_{ej}[d_k/x]\wedge\varepsilon)\vee\bigvee_{k=1}^{|D|}\bigvee_{i=1}^{n}(p_{ci}[d_k/x]\wedge\bigcirc\exists x.P_i').\end{aligned}$$

当 v 为静态变量 a 时,根据公理 AT、公理 ATSR 及推导规则 IR,有

$$\exists a.P\cong\bigvee_{k=1}^{|D|}\bigvee_{j=1}^{n_0}(p_{ej}[d_k/a]\wedge\varepsilon)\vee\bigvee_{k=1}^{|D|}\bigvee_{i=1}^{n}(p_{ci}[d_k/a]\wedge\bigcirc P_i'[d_k/a]).$$ □

定义 13. 对于任意的 PTL 项 e,计算 e 中○(next)操作符嵌套层数的函数 *DeptNext* 归纳定义如下:

- *DeptNext*(d)=*DeptNext*(a)=*DeptNext*(x)=0,其中,d 为常量,a 为静态变量,x 为动态变量;
- *DeptNext*($\bigcirc e$)=*DeptNext*(e)+1;
- *DeptNext*($f(e_1,\ldots,e_n)$)=Max{*DeptNext*(e_1),…,*DeptNext*(e_n)}.

引理 4. 任何包含时态项的等词公式 $e_1=e_2$ 能等价地转换为一个不包含时态项的 PTL 公式.

证明:令 *Dept*=Max{*DeptNext*(e_1),*DeptNext*(e_2)}.下面对 *Dept* 的值做归纳法:

归纳基础:*Dept*=1.假设 e_1 与 e_2 中的时态项分别为 $\bigcirc t_1^1,\ldots,\bigcirc t_m^1$ 及 $\bigcirc t_1^2,\ldots,\bigcirc t_n^2$,其中,$m+n\geqslant 1$.根据定义 13,所有 t_i^1 ($1\leqslant i\leqslant m$) 及 t_j^2 ($1\leqslant j\leqslant n$) 均为状态项.由公理 ATXE,有

$$e_1(\bigcirc t_1^1,\ldots,\bigcirc t_m^1)=e_2(\bigcirc t_1^2,\ldots,\bigcirc t_n^2)\cong\exists a_1.\ldots.\exists a_m.\exists b_1.\ldots.\exists b_n.(e_1(a_1,\ldots,a_m)=e_2(b_1,\ldots,b_m)\wedge\bigcirc(\bigwedge_{i=1}^{m}(t_i^1=a_i)\wedge\bigwedge_{j=1}^{n}(t_j^2=b_j))).$$

由于 $e_1(a_1,\ldots,a_m)=e_2(b_1,\ldots,b_m)$, $(t_i^1=a_i)$ 及 $(t_j^2=b_j)$ 均不包含时态项,引理成立.

归纳步骤:假设对于所有 *Dept*<k($k\geqslant 2$)引理成立.当 *Dept*=k 时,令 e_1 与 e_2 中的时态项分别为 $\bigcirc t_1^1,\ldots,\bigcirc t_m^1$ 及 $\bigcirc t_1^2,\ldots,\bigcirc t_n^2$ ($m+n\geqslant 1$).由公理 ATXE,有

$$e_1(\bigcirc t_1^1,\ldots,\bigcirc t_m^1)=e_2(\bigcirc t_1^2,\ldots,\bigcirc t_n^2)\cong\exists a_1.\ldots.\exists a_m.\exists b_1.\ldots.\exists b_n.(e_1(a_1,\ldots,a_m)=e_2(b_1,\ldots,b_n)\wedge\bigcirc(\bigwedge_{i=1}^{m}(t_i^1=a_i)\wedge\bigwedge_{j=1}^{n}(t_j^2=b_j))).$$

由定义 13,所有 $DeptNext(t_i^1)<k$ ($1\leqslant i\leqslant m$) 及 $DeptNext(t_j^2)<k$ ($1\leqslant j\leqslant n$).根据归纳假设,等词公式 $t_i^1=a_i$ ($t_j^2=b_j$)可以等价的转换为一个不包含时态项的 PTL 公式,令其为 P_i^1 (P_j^2).由推导规则 IR

$$e_1(\bigcirc t_1^1,\ldots,\bigcirc t_m^1)=e_2(\bigcirc t_1^2,\ldots,\bigcirc t_n^2)\cong\exists a_1.\ldots.\exists a_m.\exists b_1.\ldots.\exists b_n.(e_1(a_1,\ldots,a_m)=e_2(b_1,\ldots,b_n)\wedge\bigcirc(\bigwedge_{i=1}^{m}P_i^1\wedge\bigwedge_{j=1}^{n}P_j^2)).$$ □

引理 5. 任何包含时态项$\bigcirc t_1,\ldots,\bigcirc t_m$($m\geqslant 1$)的谓词公式$\rho(\bigcirc t_1,\ldots,\bigcirc t_m)$能等价地转换为一个不包含时态项的 PTL 公式.

证明:由公理 ATXP,有 $\rho(\bigcirc t_1,\ldots,\bigcirc t_m)\cong\exists a_1.\ldots.\exists a_m.(\rho(a_1,\ldots,a_m)\wedge\bigcirc\bigwedge_{i=1}^{m}(t_i=a_i))$.

对于其中的子公式(t_i=a_i)($1\leqslant i\leqslant m$),根据引理 4,能转换为一个不包含时态项的 PTL 公式,令其为 P_i.根据推导规则 IR, $\rho(\bigcirc t_1,\ldots,\bigcirc t_m)\cong\exists a_1.\ldots.\exists a_m.(\rho(a_1,\ldots,a_m)\wedge\bigcirc(\bigwedge_{i=1}^{m}P_i))$,引理成立. □

引理 6. 对于任意的投影公式$(P_1,\ldots,P_m)prjP_{m+1}$,如果所有 P_k($1\leqslant k\leqslant m+1$)能等价地转换为正则形,则$(P_1,\ldots,P_m)prjP_{m+1}$ 能等价地转换为正则形.

证明:证明方法和文献[16]中的引理 1 相同,具体略. □

定理 1. 任何 PTL 公式 P 能够等价地转换为正则形.

证明:对 P 做结构归纳法.

归纳基础:P 为原子公式φ时,根据引理 2,定理成立.

归纳步骤:假设公式 P_k($1\leqslant k\leqslant m+1$)的正则形为 $\bigvee_{j=1}^{n_0^k}(p_{ej}^k\wedge\varepsilon)\vee\bigvee_{i=1}^{n^k}(p_{ci}^k\wedge\bigcirc P_i^k)$.

- 当 P 为 $P_1\vee P_2$ 时,根据推导规则 IR,定理显然成立;
- 当 P 为$\bigcirc P_1$ 时, $\bigcirc P_1\cong true\wedge\bigcirc P_1$;
- 当 P 为$\exists v.P_1$ 时,根据引理 3,定理成立;
- 当 P 为 $e_1(\bigcirc t_1^1,\ldots,\bigcirc t_m^1)=e_2(\bigcirc t_1^2,\ldots,\bigcirc t_n^2)$ 时,由引理 4,公式 $e_1(\bigcirc t_1^1,\ldots,\bigcirc t_m^1)=e_2(\bigcirc t_1^2,\ldots,\bigcirc t_n^2)$ 可以等价地转换为一个不含时态项的 PTL 公式.根据其他情况的证明,定理成立;

© 中国科学院软件研究所 http://www.jos.org.cn

- 当 P 为$\rho(\bigcirc t_1,\ldots,\bigcirc t_m)$时,由引理 5,公式$\rho(\bigcirc t_1,\ldots,\bigcirc t_m)$可以等价地转换为一个不含时态项的 PTL 公式.根据其他情况的证明,定理成立;
- 当 P 为$(P_1,\ldots,P_m)prjP_{m+1}$时,根据引理 6,定理成立;
- 当 P 为$\neg P_1$时,由引理 1,可将 P_1 的 NF 等价地转换为 CNF,令其为 $\bigvee_{j=1}^{n_0}(p_{ej}\wedge\varepsilon)\vee\bigvee_{i=1}^{n}(p_{ci}\wedge\bigcirc P_i')$,从而有 $\neg P_1\cong(\bigwedge_{j=1}^{n_0}\neg p_{ej}\wedge\varepsilon)\vee\bigvee_{i=1}^{n}(p_{ci}\wedge\bigcirc\neg P_i')$,定理成立. □

对于 PTL 公式 P 的正则形,根据公理 ADF、公理 ADPT、公理 ADPF、公理 AT 以及推导规则 IR 对 p_{ej} 及 p_{ci} 作进一步的化简,使得其成为 *true*,*false* 或者仅由原子命题和形如 $v=d(v\in V,d\in D)$的等词公式构成的最小合取项.如果 p_{ej} 或 p_{ci} 为 *false*,将其对应的终端或未来分量从正则形中移去.特别地,如果正则形中全部终端及未来分量都被移去,则 $P\cong$ *false* .下面在构造正则图时使用的是化简后的正则形.

3.2 正则图

对于任意的公式 P,可以根据 PTL 的正则形对 P 及 P 的后继公式不断展开,从而构成了一个有向图,称为正则图,用于描述 P 的模型.

定义 14(正则图). 对于任意 PTL 公式 P,P 的正则图(normal form graph,简称 NFG)是一个有向图 $G=(CL(P),EL(P))$,其中,$CL(P)$是节点的集合,$EL(P)$是弧的集合.正则图的节点是一个 PTL 公式,而从节点 P 到 Q 的弧则是一个三元组$\langle P,p_s,Q\rangle$,其中,p_s 是一个状态公式.P 的正则图定义如下:

(1) $P\in CL(P)$为根节点;

(2) 对于任意节点 $Q\in CL(P)-\{false,\varepsilon\}$,如果 Q 的正则形为 $\bigvee_{j=1}^{n_0}(q_{ej}\wedge\varepsilon)\vee\bigvee_{i=1}^{n}(q_{ci}\wedge\bigcirc Q_i)$,则若 $n_0\geqslant 1$ 时,$\varepsilon\in CL(P)$ 且对于全部 $1\leqslant j\leqslant n_0$ 有 $\langle Q,q_{ej},\varepsilon\rangle\in EL(P)$;对于所有 $1\leqslant i\leqslant n$,有 $Q_i\in CL(P)$且$\langle Q,q_{ci},Q_i\rangle\in EL(P)$[**].

图 1 给出了一个 PTL 公式的正则图实例.在正则图中,根节点表示为嵌套的同心圆,ε节点表示为小实心圆,一般节点则表示为空心圆,节点间的弧表示为单向箭头.

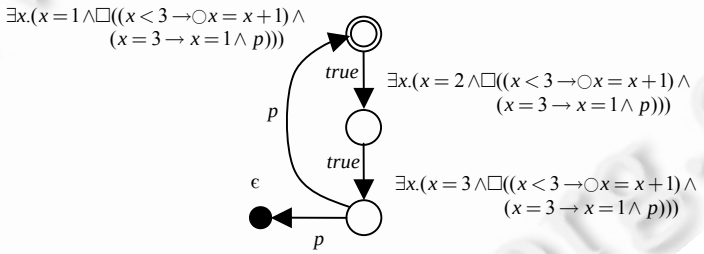

Fig.1 Example of NFG of PTL formula

图 1 PTL 公式的 NFG 实例

从直观意义上,公式 P 的正则图描述了 P 的模型.每条从根节点到达 ϵ 节点的有穷路径对应了 P 的一个有穷模型,并且沿着该路径上每条弧描述了模型的一个状态.

例如,公式 $\exists x.(x=1\wedge\Box((x<3\rightarrow\bigcirc x=x+1)\wedge(x=3\rightarrow x=1\wedge p)))$ 的正则图如图 1 所示,其正则图表明该公式的模型包含了所有长度为 $3\cdot n-1(n\geqslant 1)$且原子命题 p 在每个 $3\cdot k-1(1\leqslant k\leqslant n)$状态均成立的模型.

正则图的构造算法如下:

算法 1. 构造 PTL 公式 P 的正则图.

输入参数:P 为任意 PTL 公式;

** 在正则图里可能存在一些特殊节点,其正则形的后继公式为ε,例如 $q_e\wedge\varepsilon\vee q_i\wedge\bigcirc\varepsilon$.为加以区别,在正则图中将终端分量 $q_e\wedge\varepsilon$对应的节点表示 ϵ ,而如果未来分量里的后继公式是ε,则保持不变.

© 中国科学院软件研究所 http://www.jos.org.cn

返回值:P 的正则图 $G=(CL(P),EL(P))$.

算法步骤:

S1. 令 $CL(P)=\{P\}$,$EL(P)=\varnothing$,$Tag[P]=0$;

S2. 如果存在 $Q\in CL(P)-\{false,\varepsilon\}$ 且 $Tag[Q]=0$ 则转 S3,否则转 S4;

S3. 令 $Tag[Q]=1$.计算 Q 的正则形 $\bigvee_{j=1}^{n_0}(q_{ej}\wedge\varepsilon)\vee\bigvee_{i=1}^{n}(q_{ci}\wedge\bigcirc Q_i)$,

(1) 如果 $n_0>0$,则令 $CL(P)=CL(P)\cup\{\epsilon\}$ 且 $EL(P)=EL(P)\cup\bigcup_{j=1}^{n_0}\{\langle Q,q_{ej},\epsilon\rangle\}$;

(2) 如果 $n>0$,则:

① 对于每一个 $1\leqslant i\leqslant n$,如果 $Q_i\notin CL(P)$则令 $CL(P)=CL(P)\cup\{Q_i\}$且 $Tag[Q_i]=0$;

② 令 $EL(P)=EL(P)\cup\bigcup_{i=1}^{n}\{\langle Q,q_{ci},Q_i\rangle\}$;

(3) 转 S2.

S4. 正则图构造完毕.

下面需要证明:对于任何 PTL 公式 P,算法 1 均可以在有穷步骤内结束.其等价于证明:对于任意公式 P,P 的正则图中的节点个数是有穷的.

定理 2. 对于任意公式 P,P 的 NFG $G=(CL(P),EL(P))$中节点个数是有穷的,即$|CL(P)|\in N_0$.

证明:对 P 的结构作归纳法.

归纳基础:P 为原子公式φ时,虽然φ可能是原子命题 p、等词 $e_1=e_2$ 或谓词$\rho(e_1,\ldots,e_n)$,但根据引理 2,φ的 NF 均形如$\varpi\wedge\varepsilon\vee\varpi\wedge\bigcirc true$ 且其后继公式为 $true$.另外,$true\cong(true\wedge\varepsilon)\vee(true\wedge\bigcirc true)$,从而有$|CL(\varphi)|\leqslant 3\in N_0$.原子公式$\varphi$的 NFG 如图 2 所示.

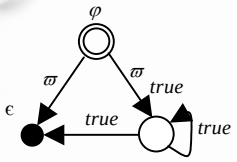

Fig.2 NFG of formula φ

图 2 原子公式φ的 NFG

归纳步骤:假设对于任意 $P_k(1\leqslant k\leqslant m+1)$,$|CL(P_k)|\in N_0$ 成立.令公式 P_k 的正则形为

$$P_k\cong(p_e^k\wedge\varepsilon)\vee\bigvee_{i_k=1}^{n_k}(p_{i_k}^k\wedge\bigcirc P_{i_k}'^k).$$

当公式 P 为$\bigcirc P_1$,$P_1\vee P_2$,$\neg P_1$ 及$(P_1,\ldots,P_m)prjP_{m+1}$ 时,证明方法和文献[16]中引理 2、引理 4、引理 6 及引理 7 相同,这里仅给出剩余情况的证明.

- 当 P 为$\exists v.P_1$ 时,如果 v 为动态变量 x,下面首先证明 $CL(\exists x.P_1)$中所有非 ϵ 节点均形如$\exists x.Q$ 并且 $Q\in CL(P_1)$.对算法 1 的构造过程做归纳法,初始时$\exists x.P_1\in CL(\exists x.P_1)$且 $P_1\in CL(P_1)$.假设在构造到第 k 步时 $CL(\exists x.P_1)$中所有非 ϵ 节点均满足该性质.当算法执行到第 $k+1$ 步时对节点$\exists x.R$ 展开,令 $R\cong r_e\wedge\varepsilon\vee\bigvee_{i=1}^{n}(r_i\wedge\bigcirc R_i')$,根据引理 3,$\exists x.R\cong\bigvee_{k=1}^{|D|}(r_e[d_k/x]\wedge\varepsilon)\vee\bigvee_{k=1}^{|D|}\bigvee_{i=1}^{n}(r_i[d_k/x]\wedge\bigcirc\exists x.R_i')$,节点$\exists x.R$ 的任意一个后继公式均形如 $\exists x.R_i'$,且当 $\exists x.R_i'$ 被添加到 $CL(\exists x.P_1)$时 $R_i'\in CL(P)$,因此有

$$|CL(\exists x.P_1)|\leqslant|CL(P_1)|\in N_0.$$

如果 v 为静态变量 a,由引理 3 有 $\exists a.P_1\cong\bigvee_{k=1}^{|D|}(p_e^1[d_k/a]\wedge\varepsilon)\vee\bigvee_{k=1}^{|D|}\bigvee_{i_1=1}^{n_1}(p_{i_1}^1[d_k/a]\wedge\bigcirc P_{i_1}'^1[d_k/a])$.对算法 1 的构造步骤做归纳法,同理可证 $CL(P_{i_1}'^1[d_k/a])$ 中所有节点均形如 $R[d_k/a]$且 $R\in CL(P_{i_1}'^1)$,从而有 $|CL(P_{i_1}'^1[d_k/a])|\leqslant|CL(P_{i_1}'^1)|$,因此,

$$|CL(\exists a.P_1)|=|\{\exists a.P_1,\epsilon\}\cup\bigcup_{k=1}^{|D|}\bigcup_{i_1=1}^{n_1}CL(P_{i_1}'^1[d_k/a])|\leqslant|D|\bullet|\{P_1,\epsilon\}\cup\bigcup_{i_1=1}^{n_1}CL(P_{i_1}'^1)|=|D|\bullet|CL(P_1)|\in N_0.$$

- P 为包含时态项的等词公式 $e_1(\bigcirc t_1^1,\ldots,\bigcirc t_m^1)=e_2(\bigcirc t_1^2,\ldots,\bigcirc t_n^2)$.由引理 4,公式 P 可以等价地转换为一个不含

© 中国科学院软件研究所 http://www.jos.org.cn

时态项的 PTL 公式.根据其他情况的证明,定理成立;

- P 为包含时态项的谓词公式$\rho(\bigcirc t_1,\ldots,\bigcirc t_m)$.由引理 5,公式 P 可以等价地转换为一个不含时态项的 PTL 公式.根据其他情况的证明,定理成立. □

4 完备性证明

4.1 PTL公式的可满足性判定

引理 7. 在 PTL 公式 P 的正则图中,如果 $\epsilon \notin CL(P)$,则 $P \sqsupset false$.

证明:P 的正则图中任意一个节点 Q 只可能是下面两种情况之一:

(1) 没有后继节点.根据正则图的构造算法(算法 1),节点 Q 没有后继仅当其是ε,$false$ 或者其正则形是为空.由于 $\epsilon \notin CL(P)$,显然 $Q \cong false$,从而有 $Q \sqsupset \bigvee_{P_i \in CL(P)} \bigcirc P_i$;

(2) 有后继节点.此时,Q 的正则形中只有未来分量 $\bigvee_{i=1}^{n}(q_{ci} \wedge \bigcirc Q_i)$,从而有 $Q \sqsupset \bigvee_{i=1}^{n} \bigcirc Q_i \sqsupset \bigvee_{P_i \in CL(P)} \bigcirc P_i$.

综上,有 $\bigvee_{P_i \in CL(P)} P_i \sqsupset false \vee \bigvee_{P_i \in CL(P)} \bigcirc P_i$.由推导规则 IXR 及定理 TSF 有 $\bigvee_{P_i \in CL(P)} P_i \sqsupset \Diamond false \cong false$,从而有 $P \sqsupset false$. □

引理 8. 在 PTL 公式 P 的正则图中,如果 $\varepsilon \in CL(P)$,则 P 是可满足的.

证明:令 P 的正则形为 $\bigvee_{j=1}^{n_0}(p_{ej} \wedge \varepsilon) \vee \bigvee_{i=1}^{n}(p_{ci} \wedge \bigcirc P_i')$,根据定理 1 及公理系统的可靠性,$P$ 与其正则形的等价性在模型系统中亦成立,即 $P \equiv \bigvee_{j=1}^{n_0}(p_{ej} \wedge \varepsilon) \vee \bigvee_{i=1}^{n}(p_{ci} \wedge \bigcirc P_i')$.由于 $\epsilon \in CL(P)$,在 P 的正则图中必然存在路径 $\Pi = \langle P, p_0, P_0, \ldots, P_{m-1}, p_m, \epsilon\rangle$ $(m \geqslant 0)$.根据定义 12,$p_i(0 \leqslant i \leqslant m)$为 $true$ 或者由原子命题、原子命题的非及形如 $v=d$ $(v \in V, d \in D)$的等词公式构成的最小合取项,基于Π可构造模型$\sigma=\langle s_0,\ldots,s_m\rangle$,其中对于每一 s_i,如果原子命题 p 在 p_i 中出现,则令 $I_p^i[p] = true$,否则令 $I_p^i[p] = false$;如果等词公式 $v=d$ 在 p_i 中出现,则令 $I_v^i[v] = d$.下面对Π的长度$|\Pi|$作归纳法证明$\sigma \vDash P$.

归纳基础:$|\Pi|=1$,此时 $\Pi = \langle P, p_0, \epsilon\rangle$ 且$\sigma=\langle s_0\rangle$.根据正则图的构造算法,$p_0 \wedge \varepsilon$是 P 正则形的终端分量 $p_{ej} \wedge \varepsilon$之一,故 $p_{ej} \wedge \varepsilon \sqsupset P$.根据 s_0 的构造及 PTL 的语义,显然$\langle s_0\rangle \vDash p_0$;另外,$\langle s_0\rangle \vDash \varepsilon$,故$\sigma \vDash P$.

归纳步骤:假设$|\Pi|<k(k \geqslant 2)$时结论成立.当$|\Pi|=k$ 时,$\Pi = \langle P, p_0, P_0, \ldots, P_{k-1}, p_k, \epsilon\rangle$,令 $\Pi' = \langle P_0, p_1, \ldots, P_{k-1}, p_k, \epsilon\rangle$.由于$|\Pi'|=k-1$,由归纳假设,基于$\Pi'$构造的模型$\sigma'=\langle s_1,\ldots,s_k\rangle$满足$\sigma' \vDash P_0$.此外,根据 s_0 的构造,有$\langle s_0\rangle \vDash p_0$.显然,$\sigma=\langle s_0\rangle \bullet \sigma'$且$\sigma \vDash p_0 \wedge \bigcirc P_0$.另外,$p_0 \wedge \bigcirc P_0$ 必然是 P 的正则形的未来分量 $p_{ci} \wedge \bigcirc P_i'$ 之一,故 $p_{ci} \wedge \bigcirc P_i' \sqsupset P$,因此$\sigma \vDash P$. □

定理 3(可判定性). 对于任意 PTL 公式 P,P 是可满足的当且仅当 P 的正则图中存在ε节点.

证明:($\Rightarrow$):等价于证明如果 ϵ 节点不属于 P 的正则图,则 $P \sqsupset false$.由引理 7 及公理系统的可靠性,显然成立.

($\Leftarrow$):如果公式 P 的正则图中存在 ϵ 节点,根据引理 8,定理亦成立. □

4.2 完备性定理

定理 4(完备性). 对于任意 PTL 公式 P,如果 P 在模型系统中是有效的,则 P 在公理系统中是可证明的,即

$$\vDash P \Rightarrow \vdash P.$$

证明:假设$\nvdash P$,则$\nvdash \neg P \rightarrow false$.根据引理 7,在公式$\neg P$ 的正则图中存在 ϵ 节点;进而根据引理 8,$\neg P$ 是可满足的,与公式 P 的有效性假设产生矛盾.故$\vdash P$. □

5 验证实例

在基于 PTL 采用定理证明方法对并发及交互式系统验证时,首先需要使用 PTL 公式对待验证系统建模,得到系统的模型 S;其次根据系统需求,用 PTL 公式描述系统应该满足的性质 R;最后,在 PTL 公理系统的基础上,通过证明 $S \sqsupset R$ 为一个定理来验证系统 S 满足性质 R.在对待验证系统建模时,PTL 的投影操作符具备直接描述进程间并发和同步的能力.投影公式$(P_1,\ldots,P_m)prjQ$ 表达的含义是进程 Q 与进程序列 $P_1,\ldots,P_m$ 并行在两个不同

© 中国科学院软件研究所 http://www.jos.org.cn

的时态空间内执行,其中,进程 $P_1,\ldots,P_m$ 在一个时态空间顺序执行,进程 Q 执行的时态空间则由每个进程 $P_i(1\leqslant i\leqslant m)$执行时态空间的端点构成.子进程 $P_1,\ldots,P_m$ 与 Q 的执行高度自治,每个进程都可以决定自己执行的时态空间,仅在每个进程 P_i 执行开始和结束时才和 Q 发生信息交互,从而使用 PTL 可以方便地对并发和交互式系统进行建模.

下面以交通违章自动监测系统为案例,使用 PTL 逻辑公式对其进行建模和性质描述,并在 PTL 公理系统基础上以定理证明的方法完成系统验证.

5.1 系统描述

交通违章自动监测系统是一种典型的并发式系统,其构成如图 3 所示,由多个分布于城市各个角落的监控终端 M_i(每个监控终端的编号 i 唯一)以及位于交通监控中心的中央服务器构成;监控终端和中央服务器间通过网络连接.

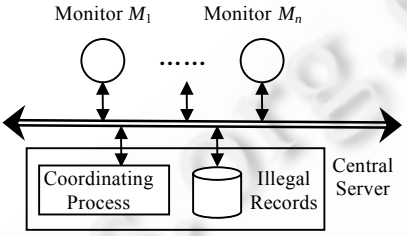

Fig.3 Automated traffic violation monitoring and reporting system

图 3 交通违章自动监测系统示意图

每个监控终端(简称“终端”)包含摄像头和违章检测单元.摄像头负责拍摄通过的车辆照片,而违章检测单元则利用图像处理和模式识别技术对拍摄的照片进行检测.如果当前车辆违章(如闯红灯或超速)则将违章的车辆信息通过网络写入到位于中央服务器中的违章记录文件(简称“文件”)中.

由于可能有多个监控终端同时向文件中写入违章记录数据,该文件作为临界资源必须实现互斥访问.这里采用集中式算法来解决互斥问题,为此,在中央服务器上专门设置了一个协调进程,任何终端要想访问文件,必须先向协调进程发出访问请求.如果当前没有任何终端访问文件,协调进程回复许可使用的应答消息;否则,保存该终端的使用请求.当正在访问文件的终端离开时,如果有终端在等待访问文件,协调进程对最先提出访问请求的监控发出应答消息;仅当监控终端收到应答消息后,才能去访问违章记录文件.

5.2 待验证系统建模

令 Δ 为系统中所有终端编号的集合.对于每个终端 $M_i(i\in\Delta)$,用原子命题 p_i 表示 M_i 对文件提出访问请求;定义静态变量 a_i 来存储终端 M_i 提出访问的时间;用原子命题 q_i 表示终端 M_i 访问文件完毕.另外,定义动态变量 t 来存储系统时间,动态变量 u 来存储正在访问文件的终端编号,动态变量 r 来存储文件末尾的位置.为简单起见,将各终端向文件中添加违章记录抽象为对文件末尾的修改,并且限定每个终端在获取到文件的访问权后仅在文件中追加一条违章记录.

任何一个监控终端 $M_i(i\in\Delta)$的监控行为包含正常监测、发现违章并申请访问文件和使用文件 3 个阶段.在正常监测期间,由于未发现违章而不需要对文件提出访问请求,可以描述为 PTL 公式 $P_i^1 \stackrel{\text{def}}{=} keep(\neg p_i)$.

在发现违章后,向协调进程发出访问请求、记录当前时间并一直等待直到获得协调进程应答为止,表达为 PTL 公式 $P_i^2 \stackrel{\text{def}}{=} a_i = t \wedge \Box p_i \wedge halt(u=i)$.$M_i$ 在获取到文件的访问权后,会在文件中追加一条违章记录,表示为公式 $P_i^3 \stackrel{\text{def}}{=} u=i \wedge \bigcirc r = r+1 \wedge \bigcirc(q_i \wedge \varepsilon)$.从而,终端 M_i 的行为可以抽象为 PTL 公式序列 $M_i:(P_i^1,P_i^2,P_i^3)$.

协调进程在进行文件的访问控制时,任何时候必须保证满足以下 4 个条件:

a) 如果有终端 M_i 对文件提出了访问请求,则必然会有终端获得访问权,即 $C_1 \stackrel{\text{def}}{=} p_i \rightarrow \bigvee_{k\in\Delta} u=k$;

b) 终端 M_i 要使用文件,必须首先对提出访问请求,即 $C_2 \stackrel{\text{def}}{=} u=i \rightarrow p_i$;

© 中国科学院软件研究所 http://www.jos.org.cn

c) 必须确保终端 M_i 在对文件提出了访问请求但并没有获取到文件使用权的情况下,后来的进程不能率先获得,即 $C_3 \overset{\text{def}}{=} \bigwedge_{k\in\Delta,k\neq i}\neg(u=k\wedge p_i\wedge p_k\wedge a_i<a_k)$;

d) 文件空闲当且仅当目前没有终端对文件提出访问请求,即 $C_4 \overset{\text{def}}{=} \bigwedge_{k\in\Delta}\neg(u=k)\leftrightarrow\bigwedge_{k\in\Delta}\neg p_k$.

以上 4 个控制条件在任何时候对任何终端均成立,即 $Con \overset{\text{def}}{=} \Box\bigwedge_{i\in\Delta}(C_1\wedge C_2\wedge C_3\wedge C_4)$.

协调进程和终端 M_i 各自运行在自己的时态空间,仅在 M_i 对文件提出访问请求并且在该文件空闲时两者才发生交互,因此协调进程对终端 M_i 的访问控制可以表达为投影公式 $M_i prjCon\wedge len(3)$.其中,$Con\wedge len(3)$表示协调进程最多需要参与 4 次就可以完成对终端 M_i 的访问控制.由于协调进程在进行文件访问控制时对所有终端完全平等,从而系统中所有终端对文件的并发访问控制可用下面的 PTL 公式表达:

$$Sys \overset{\text{def}}{=} ((M_1\ prjCon\wedge len(3))\|\ldots\|(M_{|\Delta|}\ prjCon\wedge len(3)))\wedge t=0\wedge keep(\bigcirc t=t+1)\wedge\bigwedge_{k\in\Delta}\Box(q_k\rightarrow\Box\neg p_k),$$

其中,子公式 $t=0\wedge keep(\bigcirc t=t+1)$用来记录系统时间,子公式 $\bigwedge_{k\in\Delta}\Box(q_k\rightarrow\Box\neg p_k)$ 用来表示任何终端只要访问完文件后则不再对文件提出访问请求.

5.3 系统验证

定理 5. 在上述交通违章自动监测系统中,先对文件提出访问请求的终端会率先结束对文件的访问,即

$$Sys\wedge a_x<a_y\supset\bigcirc\Diamond q_x;\bigcirc\Diamond q_y\ \ (x,y\in\Delta,x\neq y).$$

证明:为方便证明,令 $Cs\cong C_1\wedge C_2\wedge C_3\wedge C_4$.按照各终端对文件提出访问请求的时间顺序,可以将终端编号分为$\Delta_1,\ldots,\Delta_n$ 共 $n(1\leqslant n\leqslant|\Delta|)$个集合.不失一般性,令集合$\Delta_k(1\leqslant k\leqslant n)$中终端对文件提出访问请求的时间为 $T_k^{\Delta}(T_k^{\Delta}\in N_0)$,从而有 $0\leqslant T_1^{\Delta}<\ldots<T_n^{\Delta}$.

对于任意 $k\in\Delta$,根据 *keep* 与 *len*(*n*)的定义及公理 APOF、公理 APSEF、公理 APX2 和定理 TAR、定理 TXM,可证:

$$(P_k^1,P_k^2,P_k^3)\ prjCon\wedge len(3)\cong((P_k^2,P_k^3)\ prjCon\wedge len(3))\vee(\neg p_k\wedge\bigcirc keep(\neg p_k);(P_k^2,P_k^3)\ prjCon\wedge len(2)) \tag{1}$$

下面首先证明在时刻 $T(T\in N_0$且$T\geqslant T_l^{\Delta})$,描述自动监测系统运行状况的 PTL 公式 *Sr*(*T*)具有以下的形式:

$$Sr(T)\overset{\text{def}}{=}\left.\begin{array}{l} t=T\wedge Ks\wedge\bigwedge_{k\in\Delta_F}\Box\neg p_k\wedge(\|_{k\in\Delta_l-\Delta_F}\ (a_k=T_l^{\Delta}\wedge R)\|\ \|_{z=i}^{j}\|_{k\in\Delta_z}\ (a_k=T_z^{\Delta}\wedge(P_k^2,P_k^3)\ prjCon\wedge len(X_z))\\ \qquad\|\ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}\ ((P_k^1,P_k^2,P_k^3)\ prjCon\wedge len(3)))\end{array}\right\} \tag{2}$$

其中,

- $1\leqslant l\leqslant n(1\leqslant n\leqslant|\Delta|)$;
- $Ks\cong keep(\bigcirc t=t+1)\wedge\Box\bigwedge_{k\in\Delta}(q_k\rightarrow\Box\neg p_k)\wedge Cs$;
- R 为 $P_k^2;P_k^3\ prjCon\wedge len(X_l)$ 或 $(P_k^2,P_k^3)\ prjCon\wedge len(X_l)$,这里,$X_l\in\{1,2\},X_z\in\{2,3\}$.

令集合 $\Upsilon=\{k\mid T\geqslant T_k^{\Delta}$且$k>l\}$,如果 $\Upsilon\neq\varnothing$,则 i=Min(Υ)且 j=Max(Υ).否则,公式(2)中不存在子公式:

$$\|_{z=i}^{j}\|_{k\in\Delta_z}\ (a_k=T_z^{\Delta}\wedge(P_k^2,P_k^3)\ prjCon\wedge len(X_z)).$$

令集合 $\Omega=\{k\mid T<T_k^{\Delta}\}$,如果$\Omega\neq\varnothing$,则 h=Min(Ω).否则,公式(2)中不存在子公式:

$$\|_{k\in\Delta_h\cup\ldots\cup\Delta_n}\ ((P_k^1,P_k^2,P_k^3)\ prjCon\wedge len(3)).$$

Δ_F 为已访问完文件的终端编号集合,$(\Delta_l-\Delta_F)\cup\Delta_l\cup\ldots\cup\Delta_j$ 为正在等待访问文件的终端编号集合,$\Delta_h\cup\ldots\cup\Delta_n$ 为尚未对文件提出访问请求的终端编号集合,且$\Delta_F\cup\Delta_l\cup\ldots\cup\Delta_n=\Delta$.特别地,如果$\Delta_F=\varnothing$,则公式(2)中不存在子公式 $\bigwedge_{k\in\Delta_F}\Box\neg p_k$;如果$\Delta_F=\Delta$,则 *Sr*(*T*)为 $t=T\wedge Ks\wedge\bigwedge_{k\in\Delta}\Box\neg p_k$.对系统时间 T 作归纳法.

归纳基础:$T=T_1^{\Delta}$.对于 $k\in\Delta$,由公理 APS 及定理 TAR,$M_k\ prjCon\wedge len(3)\cong Cs\wedge(M_k\ prjCon\wedge len(3))$.

当 $T_1^{\Delta}=0$ 时,根据公式(1)、公理 APSEF、公理 APX2、定理 TRSA 及公式 *Sys* 的定义,有

© 中国科学院软件研究所 http://www.jos.org.cn

$$Sys \cong t=0 \wedge keep(\bigcirc t=t+1) \wedge \bigwedge_{k\in\Delta}\Box(q_k \rightarrow \Box\neg p_k) \wedge Cs \wedge (\|_{k\in\Delta_1}(a_k=0 \wedge ((P_k^2,P_k^3)prjCon \wedge len(3))) \| \ \|_{k\in\Delta_2\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \tag{3}$$

当 $T_1^{\Delta}>0$ 时,由公式(1)、公理 AXC、公理 APX2、定理 TRSA 及公式 *Sys* 的定义可证:

$$Sys \cong \bigcirc^{T_1^{\Delta}}\varepsilon; t=T_1^{\Delta} \wedge keep(\bigcirc t=t+1) \wedge \bigwedge_{k\in\Delta}\Box(q_k \rightarrow \Box\neg p_k) \wedge Cs \wedge (\|_{k\in\Delta_1}(a_k=T_1^{\Delta} \wedge ((P_k^2,P_k^3)prjCon \wedge len(2))) \| \ \|_{k\in\Delta_2\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \tag{4}$$

由公式(3)和公式(4)可知,在 T_1^{Δ} 时刻,系统运行状况可用公式 $Sr(T_1^{\Delta})$ 描述.

归纳步骤:假设 *T* 时刻系统运行状况可以用 *Sr*(*T*)描述,根据 *Sr*(*T*)的形式可分为以下几种情况:

a) *Sr*(*T*)中子公式 $\|_{k\in\Delta_l-\Delta_F}(a_k=T_l^{\Delta} \wedge R)$ 为 $a_g=T_l^{\Delta} \wedge R$ (即$|\Delta_l-\Delta_F|=1$ 且$\Delta_l-\Delta_F=\{g\}$)且 *Sr*(*T*)中存在子公式:

$$\|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(X_z)).$$

当 $j<n$ 且 $T_h^{\Delta}=T+1$ 时,可证,

$$\left.\begin{array}{l} t=T \wedge Ks \wedge \bigwedge_{k\in\Delta_F}\Box\neg p_k \wedge ((a_g=T_l^{\Delta} \wedge R) \| \ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(X_z)) \\ \quad \| \ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \\ \supset\bigcirc(q_g \wedge \varepsilon); t=T+1 \wedge Ks \wedge \bigwedge_{k\in\Delta_F\cup\{g\}}\Box\neg p_k \wedge (\|_{k\in\Delta_i}(a_k=T_i^{\Delta} \wedge (P_k^2;P_k^3 prjCon \wedge len(X_i-1))) \\ \quad \| \ \|_{z=i+1}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(X_z)) \| \ \|_{k\in\Delta_h}(a_k=T_h^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(2)) \\ \quad \| \ \|_{k\in\Delta_{h+1}\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \end{array}\right. \tag{5}$$

当 $j<n$ 且 $T_h^{\Delta}>T+1$ 时,有

$$\left.\begin{array}{l} t=T \wedge Ks \wedge \bigwedge_{k\in\Delta_F}\Box\neg p_k \wedge ((a_g=T_l^{\Delta} \wedge R) \| \ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(X_z)) \\ \quad \| \ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \\ \supset\bigcirc(q_g \wedge \varepsilon); t=T+1 \wedge Ks \wedge \bigwedge_{k\in\Delta_F\cup\{g\}}\Box\neg p_k \wedge (\|_{k\in\Delta_i}(a_k=T_i^{\Delta} \wedge (P_k^2;P_k^3 prjCon \wedge len(X_i-1))) \\ \quad \| \ \|_{z=i+1}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(X_z)) \| \ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \end{array}\right. \tag{6}$$

当 $j=n$ 时,根据公式(2)的定义,显然 *Sr*(*T*)中不存在子公式 $\|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))$,从而

$$\left.\begin{array}{l} t=T \wedge Ks \wedge \bigwedge_{k\in\Delta_F}\Box\neg p_k \wedge ((a_g=T_l^{\Delta} \wedge R) \ \| \ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(X_z))) \\ \supset\bigcirc(q_g \wedge \varepsilon); t=T+1 \wedge Ks \wedge \bigwedge_{k\in\Delta_F\cup\{g\}}\Box\neg p_k \wedge (\|_{k\in\Delta_i}(a_k=T_i^{\Delta} \wedge (P_k^2;P_k^3 prjCon \wedge len(X_i-1))) \\ \quad \| \ \|_{z=i+1}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(X_z))) \end{array}\right. \tag{7}$$

b) *Sr*(*T*)中子公式 $\|_{k\in\Delta_l-\Delta_F}(a_k=T_l^{\Delta} \wedge R)$ 为 $a_g=T_l^{\Delta} \wedge R$ (即$|\Delta_l-\Delta_F|=1$ 且$\Delta_l-\Delta_F=\{g\}$))且 *Sr*(*T*)不包含子公式

$$\|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(X_z)) .$$

当 $l<n$ 且 $T_h^{\Delta}=T+1$ 时,可证,

$$\left.\begin{array}{l} t=T \wedge Ks \wedge \bigwedge_{k\in\Delta_F}\Box\neg p_k \wedge ((a_g=T_l^{\Delta} \wedge R) \| \ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \\ \supset\bigcirc(q_g \wedge \varepsilon); t=T+1 \wedge Ks \wedge \bigwedge_{k\in\Delta_F\cup\{g\}}\Box\neg p_k \wedge (\|_{k\in\Delta_h}(a_k=T_h^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(2)) \\ \quad \| \ \|_{k\in\Delta_{h+1}\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \end{array}\right. \tag{8}$$

当 $l<n$ 且 $T_h^{\Delta}>T+1$ 时,有

$$\left.\begin{array}{l} t=T \wedge Ks \wedge \bigwedge_{k\in\Delta_F}\Box\neg p_k \wedge ((a_g=T_l^{\Delta} \wedge R) \| \ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \\ \supset\bigcirc(q_g \wedge \varepsilon); \bigcirc^{T_h^{\Delta}-T}\varepsilon; t=T_h^{\Delta} \wedge Ks \wedge \bigwedge_{k\in\Delta_F\cup\{g\}}\Box\neg p_k \wedge (\|_{k\in\Delta_h}(a_k=T_h^{\Delta} \wedge (P_k^2,P_k^3)prjCon \wedge len(2)) \\ \quad \| \ \|_{k\in\Delta_{h+1}\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon \wedge len(3))) \end{array}\right. \tag{9}$$

© 中国科学院软件研究所 http://www.jos.org.cn

当 $l=n$ 时,根据公式(2)的定义,显然 $Sr(T)$也中不存在子公式$\|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon\wedge len(3))$,从而有

$$t=T\wedge Ks\wedge\bigwedge\nolimits_{k\in\Delta_F}\Box\neg p_k\wedge(a_g=T_n^{\Delta}\wedge R)\sqsupset\bigcirc(q_g\wedge\varepsilon);t=T_h^{\Delta}\wedge Ks\wedge\bigwedge\nolimits_{k\in\Delta_F\cup\{g\}}\Box\neg p_k \tag{10}$$

c) $Sr(T)$中子公式$\|_{k\in\Delta_l-\Delta_F}(a_k=T_l^{\Delta}\wedge R)$满足$|\Delta_l-\Delta_F|>1$且$Sr(T)$中存在子公式:

$$\|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)\ prjCon\wedge len(3)).$$

当$T_h^{\Delta}=T+1$时,可证,

$$\left.\begin{array}{l} t=T\wedge Ks\wedge\bigwedge\nolimits_{k\in\Delta_F}\Box\neg p_k\wedge(\|_{k\in\Delta_l-\Delta_F}(a_k=T_l^{\Delta}\wedge R)\|\ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta}\wedge(P_k^2,P_k^3)prjCon\wedge len(X_z))\\ \quad\|\ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon\wedge len(3)))\\ \sqsupset\bigvee\nolimits_{g\in\Delta_l-\Delta_F}(\bigcirc(q_g\wedge\varepsilon);t=T+1\wedge Ks\wedge\bigwedge\nolimits_{k\in\Delta_F\cup\{g\}}\Box\neg p_k\wedge(\|_{k\in\Delta_l-\Delta_F-\{g\}}(a_k=T_l^{\Delta}\wedge(P_k^2;P_k^3\,prjCon\wedge len(X_l)))\\ \quad\|\ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta}\wedge(P_k^2,P_k^3)prjCon\wedge len(X_z))\|\ \|_{k\in\Delta_h}(a_k=T_h^{\Delta}\wedge(P_k^2,P_k^3)prjCon\wedge len(2))\\ \quad\|\ \|_{k\in\Delta_{h+1}\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon\wedge len(3))))\end{array}\right\} \tag{11}$$

当$T_h^{\Delta}>T+1$时,有

$$\left.\begin{array}{l} t=T\wedge Ks\wedge\bigwedge\nolimits_{k\in\Delta_F}\Box\neg p_k\wedge(\|_{k\in\Delta_l-\Delta_F}(a_k=T_l^{\Delta}\wedge R)\|\ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta}\wedge(P_k^2,P_k^3)prjCon\wedge len(X_z))\\ \quad\|\ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon\wedge len(3)))\\ \sqsupset\bigvee\nolimits_{g\in\Delta_l-\Delta_F}(\bigcirc(q_g\wedge\varepsilon);t=T+1\wedge Ks\wedge\bigwedge\nolimits_{k\in\Delta_F\cup\{g\}}\Box\neg p_k\wedge(\|_{k\in\Delta_l-\Delta_F-\{g\}}(a_k=T_l^{\Delta}\wedge(P_k^2;P_k^3\,prjCon\wedge len(X_l)))\\ \quad\|\ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta}\wedge(P_k^2,P_k^3)prjCon\wedge len(X_z))\|\ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon\wedge len(3))))\end{array}\right\} \tag{12}$$

d) $Sr(T)$中子公式$\|_{k\in\Delta_l-\Delta_F}(a_k=T_l^{\Delta}\wedge R)$满足$|\Delta_l-\Delta_F|>1$且$Sr(T)$中无子公式:

$$\|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon\wedge len(3)).$$

由公理 APX2、公理 APSEF、公理 ATSR 及定理 TRSA、定理 DIRI 可证,

$$\left.\begin{array}{l} t=T\wedge Ks\wedge\bigwedge\nolimits_{k\in\Delta_F}\Box\neg p_k\wedge(\|_{k\in\Delta_l-\Delta_F}(a_k=T_l^{\Delta}\wedge R)\|\ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta}\wedge(P_k^2,P_k^3)prjCon\wedge len(X_z)))\\ \sqsupset\bigvee\nolimits_{g\in\Delta_l-\Delta_F}(\bigcirc(q_g\wedge\varepsilon);t=T+1\wedge Ks\wedge\bigwedge\nolimits_{k\in\Delta_F\cup\{g\}}\Box\neg p_k\wedge(\|_{k\in\Delta_l-\Delta_F-\{g\}}(a_k=T_l^{\Delta}\wedge(P_k^2;P_k^3\,prjCon\wedge len(X_l)))\\ \quad\|\ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta}\wedge(P_k^2,P_k^3)prjCon\wedge len(X_z))))\end{array}\right\} \tag{13}$$

根据公式(2)及证明过程,显然,对于任意的$\Delta_l(1\leqslant l\leqslant n,1\leqslant n\leqslant|\Delta|)$,存在时刻 T_l,使得描述自动监测系统运行状况的 PTL 公式 $Srl(l,T_l)$恰好为

$$\left.\begin{array}{rl} Srl(l,T_l)\stackrel{\text{def}}{=} & t=T_l\wedge Ks\wedge\bigwedge\nolimits_{k\in\Delta_F}\Box\neg p_k\wedge(\|_{k\in\Delta_l}(a_k=T_l^{\Delta}\wedge R)\|\ \|_{z=i}^{j}\|_{k\in\Delta_z}(a_k=T_z^{\Delta}\wedge(P_k^2,P_k^3)prjCon\wedge len(X_z))\\ & \|\ \|_{k\in\Delta_h\cup\ldots\cup\Delta_n}((P_k^1,P_k^2,P_k^3)prjCon\wedge len(3)))\end{array}\right\} \tag{14}$$

其中,当 $l=1$ 时$\Delta_F=\varnothing$,$l>1$ 时$\Delta_F=\Delta_1\cup\ldots\cup\Delta_{l-1}$;$Srl(l,T_l)$其他参数含义和公式(2)相同.由于$\Delta_l$ 为有穷集合,根据公式(3)~公式(13)对Δ_l中终端编号个数$|\Delta_l|$做归纳法,可证,

$$\left.\begin{array}{l} Srl(l,T_l)\sqsupset\bigvee\nolimits_{k_1,\ldots,k_{|\Delta_l|}\in[\Delta_l!]}(\bigcirc(q_{k_1}\wedge\varepsilon);\ldots;\bigcirc(q_{k_{|\Delta_l|}}\wedge\varepsilon));\bigcirc^{T_{l+1}-T_l-|\Delta_l|}\varepsilon;Srl(l+1,T_{l+1})\\ \quad\sqsupset\bigwedge\nolimits_{k\in\Delta_l}\bigcirc\Diamond q_k;Srl(l+1,T_{l+1})\end{array}\right\} \tag{15}$$

其中,$[\Delta_l!]$表示Δ_l中终端编号全排列的集合,$k_1,\ldots,k_{|\Delta_l|}$为$[\Delta_l!]$上的一个排列.另外,由公式(3)、公式(4)有

$$Sys\sqsupset\bigcirc^{T_1^{\Delta}}\varepsilon;Srl(1,T_1^{\Delta}) \tag{16}$$

对于每个 $l(1\leqslant l\leqslant n)$,根据公式(15)及定理 DICI 不断替换公式(16)右侧出现子公式 $Srl(l,T_l)$,可证,

$$Sys\sqsupset\bigwedge\nolimits_{k\in\Delta_1}\bigcirc\Diamond q_k;\ldots;\bigwedge\nolimits_{k\in\Delta_n}\bigcirc\Diamond q_k \tag{17}$$

根据假设 $a_x<a_y$,必然有 $x\in\Delta_i,y\in\Delta_j$ 且 $1\leqslant i<j\leqslant n$,从而由公式(17)及定理 TCA,有

$$Sys\wedge a_x<a_y\sqsupset\bigwedge\nolimits_{k\in\Delta_i}\bigcirc\Diamond q_k;\bigwedge\nolimits_{k\in\Delta_j}\bigcirc\Diamond q_k\sqsupset\bigcirc\Diamond q_x;\bigcirc\Diamond q_y.\qquad\Box$$

© 中国科学院软件研究所 http://www.jos.org.cn

6 结 论

本文将命题投影时序逻辑的正则形及正则图技术扩展到了一阶投影时序逻辑,提出了 PTL 的正则形和正则图;并基于正则图的性质给出了 PTL 的可满足性判定定理,进而证明了有穷时间 PTL 公理系统的完备性;最后,结合验证实例展示了 PTL 及其公理系统在并发系统验证中的应用,为使用 PTL 以定理证明方法进行系统验证奠定了基础.在未来的研究中,将进一步探索无穷模型下 PTL 的完备公理系统.

References:

[1] Duan ZH. An extended interval temporal logic and a framing technique for temporal logic programming [Ph.D. Thesis]. University of Newcastle Upon Tyne, 1996.

[2] Moszkowski B. Executing temporal logic programs [Ph.D. Thesis]. Cambridge: Cambridge University Press, 1986.

[3] Duan ZH, Yang XX, Koutny M. Framed temporal logic programming. Science of Computer Programming, 2008,70(1):31−61. [doi: 10.1016/j.scico.2007.09.001]

[4] Duan ZH, Tian C. A unified model checking approach with projection temporal logic. In: Proc. of the 10th Int'l Conf. on Formal Engineering Methods (ICFEM 2008). LNCS 5256, Berlin: Springer-Verlag, 2008. 167−186. [doi: 10.1007/978-3-540-88194-0_12]

[5] Wang XB, Duan ZH. Object-Oriented temporal logic language. Journal of University of Electronic Science and Technology of China, 2009,38(1):97−101 (in Chinese with English abstract).

[6] Lei LH, Duan ZH. Specification and verification of composite Web services based on extended projection temporal logic. Journal of Xi'an Jiaotong University, 2007,41(10):1155−1159 (in Chinese with English abstract).

[7] Xiao MH, Xue JY. Formal description of properties of concurrency system by temporal logic. Journal of Naval University of Engineering, 2004,16(5):10−13 (in Chinese with English abstract).

[8] Bowman H, Thompson S. A decision procedure and complete axiomatization of finite interval temporal logic with projection. Journal of Logic and Computation, 2003,13(2):195−239. [doi: 10.1093/logcom/13.2.195]

[9] Moszkowski B. A hierarchical completeness proof for propositional interval temporal logic with finite time. Journal of Applied Non-Classical Logics, 2004,14(1-2):55−104. [doi: 10.1007/978-3-540-39910-0_22]

[10] Abadi M. The power of temporal proofs. Theoretical Computer Science, 1989,65(1):35−83. [doi: 10.1016/0304-3975(89)90138-2]

[11] Cook S. Soundness and completeness of an axiom system for program verification. SIAM Journal on Computing, 1978,7(1):70−90. [doi: 10.1137/0207005]

[12] Hodkinson I, Wolter F, Zakharyaschev M. Decidable fragments of first-order temporal logics. Annals of Pure and Applied Logic, 2000,106:85−134. [doi: 10.1016/S0168-0072(00)00018-X]

[13] Shu XF, Duan ZH. Axiomatization for the first-order projection temporal logic and formal verifications. Journal of Xidian University, 2009,36(4):680−685 (in Chinese with English abstract).

[14] Kesten Y, Pnueli A. Complete proof system for QPTL. Journal of Logic and Computation, 2002,12(5):701−745. [doi: 10.1093/logcom/12.5.701]

[15] Moszkowski B. An automata-theoretic completeness proof for interval temporal logic. In: Proc. of the 27th Int'l Colloquium on Automata, Languages and Programming. LNCS 1853, Springer-Verlag, 2000. 223−234. [doi: 10.1007/3-540-45022-X_19]

[16] Duan ZH, Tian C, Zhang L. A decision procedure for propositional projection temporal logic with infinite models. Acta Information, 2008,45(1):43−78. [doi: 10.1007/s00236-007-0062-z]

附中文参考文献:

[5] 王小兵,段振华.面向对象的时序逻辑语言.电子科技大学学报,2009,38(1):97−101.

[6] 雷丽晖,段振华.基于扩展投影时序逻辑的组合 Web 服务描述与验证.西安交通大学学报,2007,41(10):1155−1159.

[7] 肖美华,薛锦云.时态逻辑形式化描述并发系统性质.海军工程大学学报,2004,16(5):10−13.

[13] 舒新峰,段振华.投影时序逻辑的公理系统与形式验证.西安电子科技大学学报,2009,36(4):680−685.

舒新峰(1975－),男,陕西西安人,博士生,副教授,主要研究领域为算法与数据结构,形式化技术.

段振华(1948－),男,博士,教授,博士生导师,主要研究领域为互联网计算,可信软件理论与技术.

© 中国科学院软件研究所 http://www.jos.org.cn