命题时态逻辑的分划式扩充

沈恩绍

(上海交通大学计算机系 上海 200030)

摘要 在PTL(propositional temporal logic)上加入一个∪算子的自然拓广——2分划算子,便导出Wolper－Vardi－Sistla之ETL(extend PTL)的一个完全的子逻辑.它有更简洁的语法及公理系统、更好的判定算法等,是研究有限状态并发程序的一种理想的规范语言.

关键词 分划算子,ETL,公理演绎系统,判定复杂性,Tableau方法.

自1977年Pnueli的奠基性工作[1]以来,时态逻辑已被应用于并发程序设计的几乎各个侧面:规范、验证、合成与开发等.[2]为了支持这些广泛的应用,已进行了大量的基础性研究.其中一个方向是:设法在命题时态逻辑PTL(propositional temporal logic)上添加递归机制以扩充其表达能力,特别是使之具有正规ω语言的能力.已有种种扩充模式:直接加入对应连接与Kleene星运算的算子;加入最小不动点算子;量词化的PTL(QPTL);也有加入对应右线性文法或Büchi ω自动机之算子的ETL(extend PTL)等等.[3]其中以文法与自动机模式最为成功.[4,5]但上述的扩充模式有一个共同的不足之处:将动态的操作式的语义直接作为语法算子,生硬地加到PTL上去;它们与原有的静态的指称性的时态算子(○,◇,∪)在"精神"上不"匹配",在机能上又有部分重叠.作为描叙性的规范语言,这是不够理想的.

本文介绍一种全新的扩充PTL的静态模式,只须加入一个2分划算子$P^{1,1}$. $P^{1,1}$是∪算子的一个简单自然的拓广,在精神上也与PTL内的时态算子相一致.$(PTL+P^{1,1})$可嵌入ETL,但已具有与ETL相同的表达能力、更好的判定算法(但属相同的复杂性类)、简洁又完备的有限公理系.进一步地,$(PTL+P^{1,1})$又有一个完全的子逻辑$(PTL+P_0^{1,\cdots,1})$. $P_0^{1,\cdots,1}$是$P^{1,1}$的多分划拓广,但只作用于原子命题.由此出发易于刻画那些复杂的操作式的线性文法或ω自动机(算子).本文的思想可追溯到我们关于分划逻辑与有限自动机的研究[6],但这里$P^{1,1}$作为命题算子而不是约束变元的广义量词.PTL的分划式扩充(PETL)是研究有限状态并发程序的理想的形式规范语言.

本文只限于讨论线性命题时态逻辑.分划的思想也适用于分枝型的(命题)时态逻辑(相应的经典逻辑场合,见文献[7]).这些均属于点基(Point－Base)理论.此外,2分划算子也是区间式时态逻辑(ITL)或时段演算(DC)中chop运算的一种自然推广.因此,它也为时态逻

* 本文研究得到国家自然科学基金资助.作者沈恩绍,1947年生,副教授,主要研究领域为模型论逻辑,有限模型论,计算机科学中的逻辑方法.

本文通讯联系人:沈恩绍,上海200030,上海交通大学计算机系

本文1995－11－14收到修改稿

辑中 2 大范畴—点基与区间基(Interval－Base)理论的统一提供了一种新思路.

1　分划算子的引入,PETL 的语法与语义学

PTL 中的$\cup$算子(或联词)有一个自然的区间式拓广,记为$\cup^I$.

若$\alpha\cup\beta$的图示为：$\overset{\alpha}{\frown}_{\beta}\cdots$，则$\alpha\cup^I\beta$的图示为：$\overset{\alpha}{\frown}\ \overset{\beta}{\frown}\cdots$.

$\cup^I$ 与 ITL 或 DC 中的 $chop$ 算子很相似,而且$\cup^I$ 与$\cup$在语义上是不可区分的(引理 1.2),故这一拓广不能实质性地扩充 PTL 的表达能力.再进一步,将$\cup^I$ 由局部延拓到整个时间轴$\mathbb{N}$上,且 α 与 β 的满足区间可以交替出现,便得到 $P^{1,1}(\alpha,\beta)$. $L(\bigcirc,P^{1,1})=(PTL+P^{1,1})$是 PTL 的一个实质性扩充.

语法系统　形式符号集由$\mathbb{P}$(原子命题集),$\mathbb{B}=\{\mathbf{t},\mathbf{f}\}$(布尔常元),命题联词$\rightarrow$及时态联词$\bigcirc$与 $P^{1,1}$组成.

众所周知,由 $\mathbf{f}$ 与$\rightarrow$出发可以定义其它 4 个命题联词.后面将证明:由 $P^{1,1}$出发(借助命题联词)可以定义其他的时态联词$\Diamond$,$\Box$,$\cup$(因而$\bigcirc$).这里仍保留 $next$ 算子$\bigcirc$,是因它蕴含了线性时间结构的全序性,且 $P^{1,1}$的递归刻画也少不了它.记 $AP=\mathbb{P}\cup\mathbb{B}$,其中$\mathbb{P}$ 的元素又称为命题变元,而 $\mathbf{t}$ 与 $\mathbf{f}$ 称为命题常元.公式的归纳法定义如下:

合适公式$::=|p|\varphi\rightarrow\psi|\bigcirc\varphi|P^{1,1}(\varphi,\psi)$,其中 $p\in AP$,φ与 ψ 为已定义的合适公式.

语义系统　标准的线性时间结构为 $M=(S,\pi,L)$,其中 S 是(有限)状态集,$\pi:\mathbb{N}\rightarrow S$,$L:S\rightarrow 2^{AP}$. M 即带赋值 L 的状态序列,常简记为 π(当 L 固定时).如 $\pi=s_0s_1\ldots s_i\ldots$,则记 $\pi^i=s_is_{i+1}\ldots$(特别 $\pi^0=\pi$).另有一种不涉及状态的线性时间结构概念 $\sigma:\mathbb{N}\rightarrow 2^{AP}$.这 2 种定义是等效的[3],但在涉及形式语言与自动机的场合,后者有时更方便.

关于$\cup$算子,本文将采用严格的 unless 解释,按文献[2]中记号为$\cup_{w}^{>}$.

定义 1.1. $\pi\models P^{1,1}(\alpha,\beta)$ iff 存在$\mathbb{N}$ 的一个非平凡分划:$\mathbb{N}=N_\alpha\dot{\cup}N_\beta$,$N_\alpha\neq\varnothing\neq N_\beta$,使得对任意 $i\in N_\alpha$,$j\in N_\beta$,有 $\pi^i\models\alpha$,$\pi^j\models\beta$.

N_α 与 N_β 分别为$\mathbb{N}$ 中 α 与 β 的均匀地成立的小区间(包括点区间)的并集,通常要求是非空的(特别是在$\neg P^{1,1}$场合).但在某些理论分析时,有时也需考察退化或平凡场合,即某个分划子集(N_α 或 N_β)为空集.

公式的等价,类似于 PTL 场合,也有 2 种类型[2]:

初始等价:$\alpha\equiv_i\beta$ iff 对任一结构 π,$\pi^0\models\alpha\Leftrightarrow\pi^0\models\beta$;

整体等价:$\alpha\equiv_g\beta$ iff $\Box\alpha\equiv_i\Box\beta$.

文中如不特别指出,语义等价$\equiv$总是指$\equiv_i$.

在 $P^{1,1}(\alpha,\beta)$定义中,α 与 β 的地位是对称或平等的.另可引入其非对称或有优先的变形:$\vec{P}^{1,1}(\alpha,\beta)$.为此,只须在 $P^{1,1}(\alpha,\beta)$的定义中再加一限制:$0\in N_\alpha$.这时其退化场合只有一种可能,即 $N_\beta=\varnothing$,对应$\Box\alpha$.易导出二者的相互关系:

$$\vec{P}^{1,1}(\alpha,\beta)\equiv_i\alpha\wedge P^{1,1}(\alpha,\beta),\ P^{1,1}(\alpha,\beta)\equiv_g\vec{P}^{1,1}(\alpha,\beta)\vee\vec{P}^{1,1}(\beta,\alpha).$$

2 分划算子有多分划拓广及其优先变形.下面以 3 分划为例.

$P^{1,1,1}(\alpha,\beta,\gamma)$的语义定义与定义 1.1 相似(略). $P^{1,1}$可以视为 $P^{1,1,1}$的一种退化场合(其

中一个分划子集，如 $N_\gamma=\varnothing$；或 $P^{1,1}(\alpha,\beta)\equiv_g\Box(\alpha\vee\beta)\wedge P^{1,1,1}(\alpha,\beta,\mathbf{t})$. $\overset{\alpha}{\vec{P}}{}^{1,1,1}(\alpha,\beta,\gamma)$表示 $0\in N_\alpha$；其退化场合：N_β 或 N_γ 可分别或同时取 $\varnothing$. $\overset{\alpha,\beta}{\vec{P}}{}^{1,1,1}(\alpha,\beta,\gamma)$表示 $0\in N_\alpha$ 即 N 的这个分划中的第 1 个均匀小区间 $\subseteq N_\alpha$，紧接着第 2 个均匀小区间 $\subseteq N_\beta$，以后均匀小区间在 $N_\alpha,N_\beta,N_\gamma$ 中的分布便无限制了；其退化场合：$N_\gamma=\varnothing$ 或 $N_\gamma=\varnothing=N_\beta$. $\overset{\alpha,\beta,\gamma}{\vec{P}}{}^{1,1,1}(\alpha,\beta,\gamma)$表示存在 N 的一个分划，其第 1～3 个均匀小区间分别属于 N_α,N_β 与 N_γ；退化场合与 $\overset{\alpha,\beta}{\vec{P}}{}^{1,1,1}$者相同. *

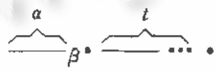
下面将讨论如何从 $P^{1,1}$ 出发来定义 $\Box$，$\Diamond$，$\cup$ 及 $P^{1,1,1}$.

$\Box\alpha\equiv\alpha\wedge\neg P^{1,1}(\alpha,\neg\alpha)$（注意：$\neg P^{1,1}(\alpha,\neg\alpha)\equiv\Box\,\alpha\vee\Box\neg\alpha$），

$\Diamond\alpha\equiv\alpha\vee\vec{P}^{1,1}(\mathbf{t},\alpha)$，$\Diamond_r\alpha\equiv\alpha\vee P^{1,1}(\neg\alpha,\alpha)$.

上面 3 式易由定义出发或利用对偶性来验证.

由文献[4]，$\alpha\cup\beta$（这里 $\cup$ 作 $\cup_W$ 解）对应的右线性文法为 $\{V_0\to v_1V_0,V_0\to v_2\}$. 不难看出，$P^{1,1}(\alpha,\beta)$相应于右线性文法 $G=\{V_0\to v_1V_0,V_0\to v_2V_0\}$. $P^{1,1}$的文法是 $\cup$ 之文法的某种对称化. 在此意义下可视 $P^{1,1}$ 为 $\cup$ 的对称化. 但用整体(Global)算子 $P^{1,1}$ 来直接刻画局部(Local)算子 $\cup$ 是不可行的. 为此，应先将 $\cup$ 算子整体化. 从线性时间结构的整体效应看，

$\alpha\cup\beta$的图示宜为： 

生成此类 ω 字的相应的右线性文法应为 $\bar{G}=\{V_0\to v_1V_0,V_0\to v_2V_r,V_r\to uV_r\}$，其中 V_r 是新引入的重复(Repeat)非终端字母，u 是新的未定义(Undefined)终端字母. $\alpha,\beta,\mathbf{t}$ 分别替换 v_1,v_2,u，将有限字视为后缀是 $uuu\ldots$ 的 ω 字，则 $\alpha\cup\beta\equiv\overline{\mathscr{G}}(\alpha,\beta,\mathbf{t}\ )$（包括退化场合），其中 $\overline{\mathscr{G}}$ 为相应于 $\bar{G}$ 的文法算子.

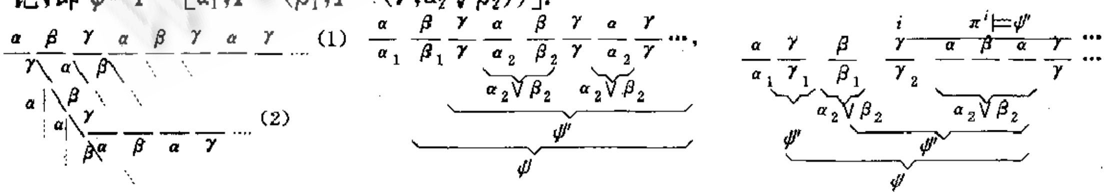
引理 1.2. $\alpha\cup\beta\equiv\overset{\alpha,\beta}{\vec{P}}{}^{1,1,1}(\alpha,\beta,\mathbf{t}\ )\equiv\alpha\cup^{l}\beta$（包括退化场合）.

从定义出发，视单点集为特殊的均匀小区间，易验证之（略）.

引理 1.3. $\overset{\alpha}{\vec{P}}{}^{1,1,1}(\alpha,\beta,\gamma)\equiv\vec{P}^{1,1}[\alpha,P^{1,1}(\beta,P^{1,1}(\gamma,\alpha\vee\beta))]$.

证明：令 $\varphi:=\overset{\alpha}{\vec{P}}{}^{1,1,1}(\alpha,\beta,\gamma)$，$\psi:=\vec{P}^{1,1}(\alpha,\psi')$，其中 $\psi':=P^{1,1}(\beta,\psi'')$，$\psi'':=P^{1,1}(\gamma,\alpha\vee\beta)$. 先证 $\varphi\Rightarrow\psi$，即要证，对任 π，$\pi\models\varphi\Rightarrow\pi\models\psi$. 设 $\pi\models\varphi$. 由 $\overset{\alpha}{\vec{P}}{}^{1,1,1}(\alpha,\beta,\gamma)$的语义，下图中无限 2 元树的每一条分枝对应 π 对 φ 的一种可能的解释（不计均匀区间的长度）. 反之亦然. 如能在每条分枝上分别给出适合 ψ 的一种解释，便得证 $\pi\models\psi$ 了.

下面以分枝(1)与(2)为例说明之. 为说明方便，对 ψ 中不同分划层次中的 α 与 β 作标记，即 $\psi=\vec{P}^{1,1}[\alpha_1,P^{1,1}(\beta_1,P^{1,1}(\gamma,\alpha_2\vee\beta_2))]$.



(1)　　(2)

图1

---

* 退化的规定方式不唯一，这里主要考虑到在刻画相应的右线性文法时的方便性.

图 1(1)中已清楚地说明了如何在分枝(1)上给出 ψ 中 3 个分划算子的解释(细节可参考(2)中的说明). 将图 1(2)中的 α_1 节解释为 ψ 中唯一的 α_1 均匀区间. 为了使自 γ_1 节起的后段为 ψ' 的均匀区间,除了将 β_1 节解释为 ψ' 中唯一的 β_1 均匀区间外,还须设法使 γ_1 节及自 γ_2 节起之后段解释为 ψ'' 的 2 个均匀区间. 为此,先考察 γ_1 节. 对任 $i\in\gamma_1$,注意 β_1 节 $\subset\pi^i$. 如将 β_1 节又同时视为 $\alpha_2\vee\beta_2$ 的均匀区间,则 $\pi^i\models\psi''$. 至于由 γ_2 节起的后段为 ψ'' 均匀小区是显然的.

(1)代表了较简单的一类分枝,易验证. 而(2)代表了较复杂的一类场合,利用多重解释技巧,也总能达到目的. 因此,$\pi\models\psi$. 由于 π 的任意性,$\varphi\Rightarrow\psi$.

其次,要证 $\psi\Rightarrow\varphi$. 设 $\pi\models\psi$,由对 ψ 中三重分划算子的语义解释,可得到 α,β 及 γ 的均匀小区间(包括将 $\alpha\vee\beta$ 均匀区间分解所得者). 其全体必覆盖整个时间轴(虽然它们之间可能互有重叠). 因此总可以在 N 上选出一个(非退化)3 分划,使得 α,β 与 γ 在各自的分划子集上是均匀地成立,同时又使 $\bigcirc\in N_a$. 换言之,$\pi\models\varphi$.

上面的图示及讨论是关于非退化场合的. 退化场合要简单些(略). 证毕.

同理可证.

推论 1.4. $\overset{\alpha,\beta}{\vec{P}}{}^{1,1,1}(\alpha,\beta,\gamma)\equiv\vec{P}^{1,1}[\alpha,\vec{P}^{1,1}(\beta,P^{1,1}(\gamma,\alpha\vee\beta))]$; $\overset{\alpha,\beta,\gamma}{\vec{P}}{}^{1,1,1}(\alpha,\beta,\gamma)\equiv\vec{P}^{1,1}[\alpha,\vec{P}^{1,1}(\beta,\vec{P}^{1,1}(\gamma,\alpha\vee\beta))]$; $\overset{\alpha,\beta,\gamma}{P}{}^{1,1,1}(\alpha,\beta,\gamma)\equiv P^{1,1}[\alpha,P^{1,1}(\beta,P^{1,1}(\gamma,\alpha\vee\beta))]$;

进一步,任一 k 分划算子,因而 $\cup$ 算子均可用 2 分划算子来定义.

多分划算子有一类特别有用的特例,即只作用于原子命题,记为 $P_0^{1,\cdots,1}$. 在 $L(\bigcirc,P^{1,1})$ 中可分离出一个子逻辑 $L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$,即在 PL 上加入 $\bigcirc,\Diamond$ 及可数无限个只作用于原子命题的分划算子.

2 PETL 的表达能力

先举几个实例,再讨论 $PETL$ 与 $ETL,QPTL$ 等的联系.

例 1:设 $p,q,r\in AP$. p,q,r 的单事件条件(Single Event Condition)$SEC(p,q,r)$: $=\Box[(p\vee q\vee r)\wedge\neg(p\wedge q)\wedge\neg(q\wedge r)\wedge\neg(r\wedge p)]$. 注意,$SEC(p,q,r)\wedge\Diamond p\wedge\Diamond q\wedge\Diamond r$ 不能刻画 $P^{1,1,1}(p,q,r)$. 即使去掉 p,q,r 的互斥约束,$\Box(p\vee q\vee r)\wedge\Diamond p\wedge\Diamond q\wedge\Diamond r$ 仍不能刻画 $P^{1,1,1}(p,q,r)$(易作反例).

例 2:$Even(\alpha)$表示时态性质 $\alpha(\alpha\in PTL)$在每个偶数时刻为真,而在奇数时刻取值不确定. $Even(\alpha)$不能在 PTL 中定义[4],但 $Even(\alpha)\equiv\vec{P}^{1,1}(\mathbf{t},\mathbf{f})\wedge\Box(\mathbf{t}\to\alpha\wedge\bigcirc\mathbf{f})\wedge\Box(\mathbf{f}\to\bigcirc\mathbf{t})$.

例 3:作为线性时间结构之时间轴,自然数全体$\mathbb{N}$ 是不能在 **PTL** 中定义的. 故只能在 **PTL** 框架之外,**规定**所讨论的结构之时间轴为$\mathbb{N}$. 在 **EPTL** 内,利用公式 $\mathbf{I}:=\neg[\mathbf{P}^{1,1}_{(\mathbf{t},\mathbf{f})}\wedge\Box(\mathbf{t}\to\bigcirc\mathbf{t})]$,可在有首元的后继结构类(可在一阶逻辑或等价地在 PTL 中定义)中分离出唯一的N. 实际上,I 刻画了自然数的归纳法原理.[8]

例 2 与例 3 说明,$L(\bigcirc,P^{1,1})$是 PTL 的一个实质性扩充,且具有刻画简单的递归过程的能力.

引理 2.1. $L(\bigcirc,\Diamond,P_0^{1,\cdots,1})\leqslant L(\bigcirc,P^{1,1})\leqslant ETL_l\leqslant ETL_r$,其中 $ETL_l=(PTL+$右线性文法算子族$)=(PTL+Wolper$ 自动机算子族$)$,$ETL_r=(PTL+$Büchi 自动机算子族$)$.

Wolper 自动机是一类特殊的 Büchi 自动机，其每一个状态都是接收态.[3,4]

如将原子命题视为命题变元，则分划算子 $P_0^{1,\cdots,1}$ 又可视为一种特殊的存在量词. 这时，公式 $P_0^{1,1,1}(p,q,r)\wedge\varphi(p,q,r,\bar{s})$ 可写成 $\psi(\bar{s})=P_{p,q,r}^{1,1,1}\varphi(p,q,r,\bar{s})$，其中 $p,q,r,\bar{s}\in AP$. 显然 $\psi\equiv\exists_{p,q,r}\{\exists_{p',q',r'}[SEC(p',q'.r')\wedge\Box(p'\to p)\wedge\Box(q'\to q)\wedge\Box(r'\to r)\ \wedge\Diamond p'\wedge\Diamond q'\wedge\Diamond r']\wedge\varphi^*(p,q,r,\bar{s})\}$，其中 $p',q'.r'$ 是不在 φ^* 中出现的新的命题变元，而 φ^* 是等价地消去 φ 中的分划量词所得的公式(由归纳假设，φ^* 存在). 当 $\varphi\in PTL,\varphi^*=\varphi$.

引理 2.2. $L(\bigcirc,\Diamond,P_0^{1,\cdots,1})\leqslant QPTL$.

$QPTL$ 是在 PTL 上加入作用于命题变元的量词后所得的量词化命题时态逻辑. 它与 ETL_r 有相同的表达能力，但其判定复杂性是非初等的.[5]

定理 2.3. $ETL_r\leqslant L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$.

证 明：我们不从由 Büchi 自动机转换而成的语法算子出发，而是设法在 $L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$ 中直接刻画 Büchi 自动机本身. 即对每一给定的 Büchi 自动机 $B=(\Sigma,Q,q_0,\Delta,F)$，构造一个公式 $\Psi_B\in L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$，使得 B 所接收的 ω 字正好是满足 Ψ_B 的线性时间结构(无状态的定义). 换言之 $\mathscr{L}^\omega(B)=\mathrm{Mod}\Psi_B$.

设 $Q=\{q_0,q_1,\ldots,q_k\}\supseteq F,\Sigma=\{a_1,a_2,\ldots,a_n\},\Delta:\Sigma\times Q\to 2^Q$.

首先，要在一般的线性时间结构 $N\to 2^\Sigma$ 中分离出 ω 字结构 $\in\Sigma^\omega$. 利用 PTL 公式 $SEC(a_1,a_2,\ldots,a_n)$ 可达到此目的.

其次，B 在 ω 字 $\sigma\in\Sigma^\omega$ 上的一个计算或操作，可以视为状态关于位置(或时间)的一个$(k+1)$分划(可有退化)；而 B 的迁移操作(Transition Move)可由 $Tr_B=\Box\bigwedge_{(a,q)\in\mathrm{dom}\Delta}[a\wedge q\to\bigcirc\vee q'(a,q;q')\in\Delta$ 来描述；Büchi 接收条件即 $Ac_B=\Box\Diamond(\vee\ F)$. 因此，

$$\Psi_B:=SEC(a_1,\ldots,a_n)\wedge\vec{P}_0^{1,\cdots,1}(q_0,\ldots,q_k)\wedge SEC(q_0,\ldots,q_k)\wedge Tr_B\wedge Ac_B$$

如果视 $\vec{P}_0^{1,\cdots,1}$ 为量词，作用于命题变元 $q_0,\ldots,q_k$，则 Ψ_B 中自由的命题变属于 $\{a_1,a_2,\ldots,a_n\}$，故其线性时间模型是 ω 字 $\in\Sigma^\omega$. 由此，$\mathscr{L}^\omega(B)=\{\sigma\in\Sigma^\omega|\sigma\models\Psi_B\}=\mathrm{Mod}\boldsymbol{\Psi}_B$. 因此，$ETL_r\leqslant L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$. (证毕)

注记：(1)在 $L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$ 的语法构成中，$\cup$ 算子没有显式出现；而引理 1.2 在这里并不适用. 但 $\cup$ 算子可由特定的自动机算子或线性文法算子来表示.[3] 由定理 2.3 便可间接地证明：$L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$ 中 $\cup$ 是导出算子，将 $L(\bigcirc,\Diamond,P^{1,\cdots,1}{}_0)$ 归入 $PETL$ 是合理的.

(2)设 $\mathbb{R}=(\Sigma,Q,q_0,\Delta,\Omega)$ 是 Rabin ω 自动机，其中 $\Omega=\{(L_1,U_1),\ldots,(L_r,U_r)\},L_i,U_i\subseteq Q$. 则 $Rabin$ 接收条件[9]可由 $Ac_R:=\bigwedge_{i\in I}[\Box\Diamond(\vee U_i)\wedge\Diamond\Box(\neg\vee L_i)]$ 来规范. 将上面 Ψ_B 中的 Ac_B 换成 Ac_R，即得到刻画 Rabin ω 自动机的公式 $\Psi_R\in L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$.

推论 2.4. $L(\bigcirc,\Diamond,P_0^{1,\cdots,1})=L(\bigcirc,P^{1,1})=ETL_l=ETL_r=QPTL$，且它们与 Büchi ω 自动机或正规 ω 语言有相同的表达能力.

如果注意到 Ψ_B 或 Ψ_R 中 $P_0^{1,\cdots,1}$ 只使用了一次，便有：

推论 2.5. (范式定理)对每一个 $PETL$ 公式 φ，存在一个公式 $\theta,\theta=P_0^{1,\cdots,1}(s_1,\ldots,s_k)\wedge\psi(s_1,\ldots,s_k,\bar{t})$，其中 $\psi\in PTL,s_1,\ldots,s_k,\bar{t}$ 是 ψ 中出现的原子命题，使得 $\varphi\equiv\theta$.

仿 $QPTL$，在 $L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$ 中以分划量词的叠代次数为测度，可引入公式的一个分层(Hierarchy). 范式定理说明，$L(\bigcirc,\Diamond,P_0^{1,\cdots,1})$ 中的这个分层有塌缩(Collapsing)现象.

具体应用时，采用 $PETL$ 的 $L(\bigcirc,\diamond,P_0^{1,\cdots,1})$ 框架有时较方便(如对 Büchi 自动机的刻画)；但涉及理论性探讨时(如 SAT 判定问题或公理系之完备性等)，从 $L(\bigcirc,P^{1,1})$ 出发更简便.

3 PETL 的公理系统与判定问题

从 $P^{1,1}$ 的语义定义易导出：

对称性：$P^{1,1}(\alpha,\beta)\equiv P^{1,1}(\beta,\alpha)$；

递推公式：$P^{1,1}(\alpha,\beta)\equiv(\alpha\vee\beta)\wedge\bigcirc P^{1,1}(\alpha,\beta)$；$\neg P^{1,1}(\alpha,\beta)\equiv(\neg\alpha\wedge\neg\beta)\vee\bigcirc\neg P^{1,1}(\alpha,\beta)$.

仔细分析 $\neg P^{1,1}$ 的语义，不难看出 $\diamond(\neg\alpha\wedge\neg\beta)$ 是 $\neg P^{1,1}(\alpha,\beta)$ 的见证(Witness)；上面关于 $\neg P^{1,1}$ 的递推式说明，此见证的出现可以不定期地向后推延. 形如 $\neg P^{1,1}(\alpha,\beta)$ 的性质称为 eventuality 性质(简称为 Ev 性质). 形如 $\neg(\alpha\cup\beta)$ 之性质也属此类.

下面先给出 $PETL$ 的 2 个公理系 I 与 II(与文献[4]中的 2 个公理系对应)

I. 在 PTL 的公理系(包括推理规则)之上增加关于 $P^{1,1}$ 的公理：

$\vdash P^{1,1}(\alpha,\beta)\leftrightarrow P^{1,1}(\alpha,\beta)$，$\vdash\Box\alpha\vee\Box\beta\rightarrow P^{1,1}(\alpha,\beta)$，$\vdash P^{1,1}(\alpha,\beta)\leftrightarrow[(\alpha\vee\beta)\wedge\bigcirc P^{1,1}(\alpha,\beta)]$

II. 请比较文献[4]中 ETL_l 的那个无限公理系. 因 $P^{1,1}$ 算子只有一个，相应 $L(\bigcirc,P^{1,1})$ 的公理系是有限的且要简单得多.

$\vdash\bigcirc\neg\alpha\Leftrightarrow\neg\bigcirc\alpha$，$\vdash\bigcirc(\alpha\rightarrow\beta)\rightarrow(\bigcirc\alpha\rightarrow\bigcirc\beta)$；

$\vdash P^{1,1}(\alpha,\beta)\rightarrow P^{1,1}(\beta,\alpha)$；

$\vdash P^{1,1}(\alpha,\beta)\rightarrow(\alpha\vee\beta)\wedge\bigcirc P^{1,1}(\alpha,\beta)$；

$\vdash u\wedge\Box\{u\rightarrow[(\alpha\vee\beta)\wedge\bigcirc u]\}\rightarrow P^{1,1}(\alpha,\beta)$，

其中 u 是不在 α 与 β 中出现的原子命题. 上面最后一式中的算子 $\Box$ 虽可消去(用更原始的符号 $\bigcirc$，$P^{1,1}$ 来表达之)，但这将使表达式复杂化且其中的不动点构造将不明显，故仍保留之.

推理规则：

(I_1) 若 γ 为 PL 之重言式，则 $\vdash\gamma$；

(I_2) $\vdash p$，$\vdash p\rightarrow q\Rightarrow\vdash q$；

(I_3) $\vdash\gamma\Rightarrow\vdash\bigcirc\gamma$；

(I_4) $\vdash\gamma\Rightarrow\vdash\neg P^{1,1}_{(\gamma,\neg\gamma)}$，

不难验证，公理系 I 与 II 是等价的(证明略).

为证明公理系 II 的完备性，先讨论 $L(\bigcirc,P^{1,1})$ 的可判定性. 研究一个逻辑的判定问题有多种途径，其中 $Tableau$(简记为 $Tab.$)方法通常能给出更好的判定算法.[2] $Tab.$ 方法在本质上是一种归纳方法，这从下面关于 $L(\bigcirc,P^{1,1})$ 的 $Tab.$ 分解规则也可看出.

$\neg\neg f\rightarrow\{\{f\}\}$，$\neg\bigcirc f\rightarrow\{\{\bigcirc\neg f\}\}$，$f_1\wedge f_2\rightarrow\{\{f_1,f_2\}\}$，

$\neg(f_1\vee f_2)\rightarrow\{\{\neg f_1,\neg f_2\}\}$，$f_1\vee f_2\rightarrow\{\{f_1\},\{f_2\}\}$，$\neg(f_1\wedge f_2)\rightarrow\{\{\neg f_1\},\{\neg f_2\}\}$，

$P^{1,1}(f_1,f_2)\rightarrow\{\{f_1\vee f_2,\bigcirc P^{1,1}(f_1,f_2)\}\}$，$\neg P^{1,1}(f_1,f_2)\rightarrow\{\{\neg f_1,\neg f_2\},\{\bigcirc\neg P^{1,1}(f_1,f_2)\}\}$.

由于 $L(\bigcirc,P^{1,1})\leqslant ETL_l$(通过算子 $P^{1,1}$ 与线性文法 $\{V_0\rightarrow v_1V_0,V_0\rightarrow v_2V_0\}$ 之一一对应，

嵌入过程是线性时间的），故 ETL_l 的 Wolper 算法[4]一定也适用于 $L(\bigcirc, P^{1,1})$. 又因对应 $P^{1,1}$ 的线性文法（算子）非常简洁，故具体运用该算法于 $L(\bigcirc, P^{1,1})$ 时，必有相当程度的简化.

定理 3.1. $L(\bigcirc, P^{1,1})$ 的 SAT 判定问题是多项式空间完全的.

证明：下面只概述判定算法，同时说明在何处 Wolper 的 Tab. 算法能得到简化或改进. 具体细节可参考文献[4].

Tab. 算法的基本思想及程序如下：

(1) 分解程序. 利用上述的分解规则，将待判定的公式 f（称为初始公式）分解为有限个公式集，每个公式集只含有有限个基本公式（原子命题或其否定）或$\bigcirc$－公式（以算子$\bigcirc$开头的公式）. 这 2 类公式分别相应于"当前状态"及"余下的后续状态列". 注意，这里关于 $P^{1,1}$ 的分解规则比 ETL_l 中对应一般文法算子 $\mathscr{G}$ 的分解规则要简单得多，特别是$\neg P^{1,1}$的分解式中只含有一个$\neg P^{1,1}$即 Ev. 公式. 这是在程序(3)中算法获得改进的根据.

(2) 从上述公式集出发构造 Tableau（又称为模型图）. 此图"含有"初始公式 f 的所有潜在的线性模型（对应图的路径）.

(3) 消去程序. 消去模型图中不可满足的节点，同时又保证可满足的 Ev 公式最终将会能行地实现. 在 ETL_l 场合，验证 Ev. 性质时，必须考察有关分解式中 Ev. 公式集的所有子集. 而这里只需考察分解式中的单个 Ev. 公式（类似 PTL 场合）. 故消去程序最多只需进行 2^{4l}次（l 为 f 的长度），比 ETL_l 场合少一个 2^l 因子.

同样有 $Tab.$ 方法的完备性：f 可满足 iff $Tab.$ 算法生成的模型图之初始节点$\{f\}$不会被消去. 进而可证 $L(\bigcirc, P^{1,1})$之 SAT 判定问题是可解的，其复杂性是单幂(Single Exponent)时间因而是多项式空间的. 如再注意到 PTL 的判定复杂性已是 PSPACE 完全的，遂证：$L(\bigcirc, P^{1,1})$的判定复杂性是 PSPACE 完全的.（证毕）

二公理系的可靠性是显然的；在定理 3.1 之 $Tab.$ 算法基础上，仿文献[4]中相应场合，可证其完备性.

定理 3.2. 公理系 II 是完备的.

证明：（大意）利用 $Tab.$ 算法可验证：若$\neg f$ 之模型图的初始节点$\{\neg f\}$可以消去，则 f 是可证明的(Provable from Ⅰ). 再利用上述 $Tab.$ 方法的完备性，便可导出：恒真的 $L(\bigcirc, P^{1,1})$公式是可以证明的.（证毕）

由于 ETL_l 的公理系过于复杂，在 PTL 框架中发展起来的演绎方法的各种应用[2]，难以拓广到 ETL 场合. 而这里简明的公理系将为 $PETL$ 之应用的证明论途径，提供了一个理想的出发点. 其中一项有意义的尝试，便是设法将文献[10]中 PTL 的一个定理自动证明技术推广到 $PETL$ 上去.

致谢　贲可荣同志阅读了本文初稿，提出有益建议，在此表示感谢.

参考文献

1 Pnueli A. The temporal logic of programs. In: 8th FOCS, 1977. 46～57.

2 Emerson E A. Temporal and model logic. In: van Leeuwen ed. Handbook of Theoretical Computer Science, Vol.

B J, Elsevier, 1990. 995～1072.

3 Wolper P. On the relation of programs and computations to models of temporal logic. LNCS, 1987, **398**: 75～123.

4 Wolper P. Temporal logic can be more expressive. Inform. & Control, 1983, **56**: 72～99.

5 Sistla A, Vardi M, Wolper P. The complementation problem for Büchi automata with applications to temporal logic. Theoretical Comput. Sci., 1987, **49**: 217～237.

6 Shen Enshao, Tian Qijia. Partition logics and finite automata. TCS, 1996 (to appear).

7 沈恩绍. 分划逻辑与树形自动机. 理论计算机科学进展. 长沙：国防科大出版社，1994.

8 沈恩绍. 分划逻辑与传递闭包逻辑. 科学通报，1993，**38**(**14**).

9 Thomas W. Automata on infinite objects. In: Leeuwen ed. Handbook of Theoretical Computer Science, Vol. B, Elsevier, 1990. 133～191.

10 贲可荣，陈火旺. 命题时态逻辑相继式演算系统. 中国科学(A 辑)，1994，**24**(**10**).

PARTITION EXTENSIONS OF PROPOSITIONAL TEMPORAL LOGIC

Shen Enshao

(*Department of Computer Science Shanghai Jiaotong University Shanghai* 200030)

Abstract Augmenting PTL (propositional temporal logic) with a 2－partition operator, which is a natural generalization of unless operator, leads to a simple but complete fragment of Wolper－Vardi－Sistla's ETL (extend PTL). It has succinct deductive system, better decision algorithm, easy translation to ETL, and is an ideal specification formalism for finite－state concurrent programs.

Key words Partition operator, extend PTL, deductive system, complexity of decision problem, Tableaux method.