§5 线性时序逻辑

在命题逻辑和一阶逻辑的基础上增加模态算子用以描述时间先后次序有关的性质的一类逻辑称为时序逻辑。本章介绍线性时序逻辑。

§5.1 命题线性时序逻辑(PLTL)

考虑建立在命题逻辑上的线性时序逻辑，即命题线性时序逻辑，记作PLTL。给定一个原子命题集合AP。用p表示AP中的任意命题。PLTL公式的集合由以下语法给出。

$$\phi ::= \quad p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \to \phi \mid \phi \leftrightarrow \phi \mid O\,\phi \mid \Diamond\,\phi \mid \Box\,\phi \mid \phi\, U\, \phi \mid \phi\, R\, \phi$$

符号$O, \Diamond, \Box, U, R$称为PLTL的时序算子。前三个时序算子在不同的场合和应用背景下也写成X, F, G。

模型： AP上的PLTL公式在AP上的标号Kripke结构上解释。

PLTL公式的语义： 给定$M = \langle S, R, I, L\rangle$。状态$s \in S$满足PLTL公式$\varphi$记为$M, s \models \varphi$当且仅当对所有$s$起点的无穷路径$\pi$有$M, \pi \models \varphi$。用$\pi^k$来表示$\pi_k$开始的序列$[\pi_i]_{i\geq k}$。$M, \pi \models \varphi$定义如下。

$M, \pi \models p$	若$p \in AP$且$p \in L(\pi_0)$
$M, \pi \models \neg\varphi$	若$M, \pi \not\models \varphi$
$M, \pi \models \varphi \vee \psi$	若$M, \pi \models \varphi$ 或$M, \pi \models \psi$
$M, \pi \models \varphi \wedge \psi$	若$M, \pi \models \varphi$ 且$M, \pi \models \psi$
$M, \pi \models \varphi \to \psi$	若$M, \pi \models \varphi$ 则$M, \pi \models \psi$
$M, \pi \models \varphi \leftrightarrow \psi$	若$M, \pi \models \varphi \to \psi$ 且$M, \pi \models \psi \to \varphi$
$M, \pi \models O\varphi$	若$M, \pi^1 \models \varphi$
$M, \pi \models \Box\psi$	若$\forall i \geq 0, M, \pi^i \models \psi$
$M, \pi \models \Diamond\varphi$	若$\exists i \geq 0, M, \pi^i \models \varphi$
$M, \pi \models \varphi U \psi$	若$\exists i \geq 0.(M, \pi^i \models \psi$ 且$\forall 0 \leq j < i, M, \pi^j \models \varphi)$
$M, \pi \models \varphi R \psi$	若$\forall i \geq 0.(M, \pi^i \models \psi$ 或$\exists 0 \leq j < i, M, \pi^j \models \varphi)$

为方便叙述，以下说某个时刻就是代表这个时刻开始的无穷路径。直观来讲，O算子表示路径的下一时刻满足跟在O后面的给定公式（下一时刻满足给定公式），$\Diamond$算子表示路径的某一时刻满足给定公式（将来满足给定公式），$\Box$算子表示路径的每个时刻都满足给定公式（总是满足给定公式），U算子表示在某个时刻满足第二个公式且之前的每个时刻都满足第一个公式（第一个公式满足直到第二个公式满足），R算子表示如果某个时刻满足第一个公式那么之后第二个公式可以不满足且此前第二个公式必须满足（第一个公式的满足之后放弃了对第二个公式满足的要求）。模型M满足一个PLTL公式就是M的所有计算都满足该公式。

定义 5.1 *$M \models \varphi$当且仅当对所有$s \in I$有$M, s \models \varphi$。*

可满足性： 设φ为PLTL公式。φ是可满足的，当且仅当存在标号Kripke结构M使得$M \models \varphi$。

重言式和等价： 设φ和ψ为PLTL公式。φ是重言式，记作$\models \varphi$，当且仅当对任意标号Kripke结构M有$M \models \varphi$。φ等价于ψ，记作$\varphi \equiv \psi$，当且仅当$\models \varphi \leftrightarrow \psi$。

等价公式： 为方便起见，定义$\top = (p_0 \vee \neg p_0)$和$\bot = (p_0 \wedge \neg p_0)$其中$p_0 \in AP$为给定命题。设$\varphi$和$\psi$为PLTL公式。我们有以下等价的公式对。

1. $O\varphi \equiv \neg(O\neg\varphi)$
2. $\Box\varphi \equiv \neg(\Diamond\neg\varphi)$
3. $\varphi R\psi \equiv \neg(\neg\varphi U\neg\psi)$
4. $\Box\varphi \equiv (\varphi \wedge O(\Box\varphi))$
5. $\Diamond\varphi \equiv (\varphi \vee O(\Diamond\varphi))$
6. $\varphi R\psi \equiv (\psi \wedge (\varphi \vee O(\varphi R\psi)))$
7. $\varphi U\psi \equiv (\psi \vee (\varphi \wedge O(\varphi U\psi)))$
8. $\Diamond\varphi \equiv (\top U\varphi)$
9. $\Box\varphi \equiv (\bot R\varphi)$
10. $\varphi R\psi \equiv (\psi U(\varphi \wedge \psi) \vee G\psi)$

完全集： 一个命题逻辑联接符和时序算子的集合Y称为PLTL的完全集，当且仅当每个PLTL公式都等价于一个命题逻辑联接符和时序算子都在Y中的PLTL公式。一个时序算子的集合Y称为PLTL的时序算子完全集，当且仅当每个PLTL公式都等价于一个时序算子在Y中的PLTL公式。

极小完全集： 一个命题逻辑联接符和时序算子的集合Y称为PLTL的极小完全集，当且仅当Y是PLTL的完全集且Y的真子集都不是PLTL的完全集。一个时序算子的集合Y称为PLTL的时序算子极小完全集，当且仅当Y是PLTL的时序算子完全集且Y的真子集都不是PLTL的时序算子完全集。

命题 5.1 *$\{O, U\}$是PLTL的时序算子极小完全集。*

由以上等价的公式类型，我们知道$\{O, U\}$是PLTL的时序算子完全集。设$AP = \{p\}$和$\varphi = (\neg pUp)$。我们可以构造两个序列的标号Kripke结构M_k和M'_k使得$M_k \models \varphi$和$M'_k \not\models \varphi$，但不存在任何只使用时序算子O的公式具有同样性质，即$(\neg pUp)$不等价于任何一个仅包含O和命题逻辑联接符的PLTL公式，因而$\{O\}$不是PLTL的时序算子完全集。类似地，我们可以证明$\{U\}$不是PLTL的时序算子完全集。

表达能力的强弱关系： 用$LTL(Y)$表示仅用集合Y中的时序算子和命题逻辑连接符构造的公式的集合。用>表示表达能力存在强弱关系。则有如下结论。

- $LTL(\{O, U\}) > LTL(\{O, F\}) > LTL(\{O\})$。
- $LTL(\{O, U\}) > LTL(\{U\}) > LTL(\{F\})$。
- $LTL(\{O, F\}) > LTL(\{F\})$。

对于$\{O, U, F\}$的不同子集，表达能力的强弱关系若不能由以上关系推导得出，则这些子集的表达能力存在互补关系。

NNF范式： 只使用逻辑连接符$\wedge, \vee, \neg$且逻辑联接符$\neg$只出现在命题前面的公式称为NNF范式。

命题 5.2 *每个PLTL公式等价于一个PLTL的NNF范式公式。*

对于每个PLTL公式，我们首先可以将其转换成等价的只使用$\{\neg, \vee, \wedge\}$中命题逻辑联接符和$\{O, U\}$中时序算子的公式。然后使用以下等价关系将其转换成时序算子在$\{O, U, R\}$中的NNF范式公式。

$\neg\neg\varphi$	$\equiv$	φ
$\neg(\varphi \vee \psi)$	$\equiv$	$\neg\varphi \wedge \neg\psi$
$\neg(\varphi \wedge \psi)$	$\equiv$	$\neg\varphi \vee \neg\psi$
$\neg(O\varphi)$	$\equiv$	$O(\neg\varphi)$
$\neg(\varphi U \psi)$	$\equiv$	$\neg\varphi R \neg\psi$
$\neg(\varphi R \psi)$	$\equiv$	$\neg\varphi U \neg\psi$

可满足性判定问题： 判定PLTL公式是否可满足的问题称为PLTL可满足性问题。PLTL可满足性问题的复杂性为PSPACE完全。只允许时序算子$\Box$和$\Diamond$的PLTL公式的子集记为PLTL(F)。PLTL(F)可满足性问题的复杂性为NP完全。

命题 5.3 *设φ为PLTL公式。定义$|\varphi|$为φ中出现的符号个数。若φ可满足，则存在M和$\pi = \pi_0 \cdots \pi_{i-1}(\pi_i \cdots \pi_k)^\omega$使得$M, \pi \models \varphi$且$k \leq 2^{|\varphi|}$。*

模型检测问题： 判定Krikpe模型是否满足PLTL公式的问题称为PLTL模型检测问题。PLTL模型检测问题的复杂性为PSPACE完全。

§5.1.1 PLTL公式的推理

以$\{O, U, \Box, \Diamond\}$为PLTL公式的时序算子集。PLTL的推理系统包含以下三部分：一部分为PLTL公式相关的时序逻辑公理；另一部分为命题逻辑推理系统；第三部分为时序推理规则。设φ和ψ为PLTL公式。

时序逻辑公理： 我们有以下公理。

$\Diamond\neg\neg\varphi \leftrightarrow \Diamond\varphi$	$\Box(\varphi \to O\varphi) \to (\varphi \to \Box\varphi)$
$\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$	$O\neg\varphi \leftrightarrow \neg O\varphi$
$\Box\varphi \to \varphi$	$O(\varphi \to \psi) \to (O\varphi \to O\psi)$
$\Box\varphi \to O\varphi$	$(\varphi U \psi) \leftrightarrow (\psi \vee (\varphi \wedge O(\varphi U \psi))$
$\Box\varphi \to O\Box\varphi$	$(\varphi U \psi) \to \Diamond\psi$

命题逻辑推理系统：

(AX) 若φ是命题逻辑的重言式的实例，则$\vdash \varphi$。

(MP) 若$\vdash \varphi \to \psi$且$\vdash \varphi$，则$\vdash \psi$。

时序推理规则：

(G) 若$\vdash \varphi$，则$\vdash \Box\varphi$。

命题 5.4 *PLTL推理系统是可靠且完备的。*

§5.1.2 PLTL限界语义

给定有穷状态标号Kripke结构$M = \langle S, R, I, L\rangle$。称长度$k+1$的路径为$k$路径。$k$路径$[\pi_i]_{i=0}^{k}$称为$(k,\ell)$环当且仅当$R(\pi_k, \pi_\ell)$。

定义 5.2 *设φ为PLTL公式。$M, s \models_E \varphi$当且仅当存在s起点的无穷路径π使得$M, \pi \models \varphi$。*

命题 5.5 *设φ为PLTL公式。$M, s \models_E \varphi$当且仅当存在一个s起点的(k,ℓ)环使得以下成立：*

$$M, \pi_0 \cdots \pi_{\ell-1}(\pi_\ell \cdots \pi_k)^\omega \models \varphi \text{ 且 } k \le |M| \cdot 2^{|\varphi|}。$$

定义 5.3 *设φ为PLTL公式。$M \models_E \varphi$当且仅当存在$s \in I$使得$M, s \models \varphi$。*

推论 5.1 *设φ为PLTL公式。$M \not\models \varphi$当且仅当$M \models_E \neg\varphi$。*

以下考虑仅用$O, \Box, U$时序算子的NNF范式的PLTL公式。

设π为k路径。用$U_{x,y}(\pi, \varphi, \psi, i, n)$表示以下公式（用于以下非环和环的语义中$\models_{x,y}^{j}$的定义）。

$$U_{x,y}(\pi, \varphi, \psi, i, n) = \bigvee_{j=i}^{n}((M, \pi \models_{x,y}^{j} \psi) \wedge \bigwedge_{m=i}^{j-1}(M, \pi \models_{x,y}^{m} \varphi))$$

非环的语义： 定义$M, \pi \models_{a,k} \varphi$为$M, \pi \models_{a,k}^{0} \varphi$且后者的定义如下。

$M, \pi \models_{a,k}^{i} p$	若$p \in AP$且$p \in L(\pi_i)$
$M, \pi \models_{a,k}^{i} \neg p$	若$M, \pi \not\models_{a,k}^{i} p$
$M, \pi \models_{a,k}^{i} \varphi \wedge \psi$	若$M, \pi \models_{a,k}^{i} \varphi$且$M, \pi \models_{a,k}^{i} \psi$
$M, \pi \models_{a,k}^{i} \varphi \vee \psi$	若$M, \pi \models_{a,k}^{i} \varphi$或$M, \pi \models_{a,k}^{i} \psi$
$M, \pi \models_{a,k}^{i} O\varphi$	若$i < k$且$M, \pi \models_{a,k}^{i+1} \varphi$
$M, \pi \models_{a,k}^{i} \Box\varphi$	若$false$
$M, \pi \models_{a,k}^{i} \varphi U \psi$	若$U_{a,k}(\pi, \varphi, \psi, i, k)$

命题 5.6 *$M, \pi \models_{a,k} \varphi$当且仅当对任意$\pi' \in \pi \cdot (S)^\omega$，$M, \pi' \models \varphi$。*

环的语义： 设$0 \le \ell \le k$。定义$M, \pi \models_{\ell,k} \varphi$为$M, \pi \models_{\ell,k}^{0} \varphi$且后者的定义如下。

$M, \pi \models_{\ell,k}^{i} p$	若$p \in AP$且$p \in L(\pi_i)$
$M, \pi \models_{\ell,k}^{i} \neg p$	若$M, \pi \not\models_{\ell,k}^{i} p$
$M, \pi \models_{\ell,k}^{i} \varphi \wedge \psi$	若$M, \pi \models_{\ell,k}^{i} \varphi$且$M, \pi \models_{\ell,k}^{i} \psi$
$M, \pi \models_{\ell,k}^{i} \varphi \vee \psi$	若$M, \pi \models_{\ell,k}^{i} \varphi$或$M, \pi \models_{\ell,k}^{i} \psi$
$M, \pi \models_{\ell,k}^{i} O\varphi$	若$i < k$且$M, \pi \models_{\ell,k}^{i+1} \varphi$或$i = k$且$M, \pi \models_{\ell,k}^{\ell} \varphi$
$M, \pi \models_{\ell,k}^{i} \Box\varphi$	若$\bigwedge_{j=\min(i,\ell)}^{k}(M, \pi \models_{\ell,k}^{j} \varphi)$
$M, \pi \models_{\ell,k}^{i} \varphi U \psi$	若$U_{\ell,k}(\pi, \varphi, \psi, i, k) \vee \bigwedge_{j=i}^{k}(M, \pi \models_{\ell,k}^{j} \varphi) \wedge U_{\ell,k}(\pi, \varphi, \psi, \ell, i-1)$

命题 5.7 *$M, \pi \models_{\ell,k} \varphi$其中$0 \le \ell \le k$，当且仅当$M, \pi_0 \cdots \pi_{\ell-1}(\pi_\ell \cdots \pi_k)^\omega \models \varphi$。*

限界语义：

定义 5.4 $M,\pi \models_k \varphi$当且仅当$M,\pi \models_{a,k} \varphi$或$\bigvee_{\ell=0}^{k}(R(\pi_k,\pi_\ell) \wedge (M,\pi \models_{\ell,k} \varphi))$。

用$M,s \models_{E,k} \varphi$表示存在$s$起点的$k$路径$\pi$使得$M,\pi \models_k \varphi$。

命题 5.8 *对所有$k \geq 0$，若$M,s \models_{E,k} \varphi$，则$M,s \models_{E,k+1} \varphi$。*

正确性与完备性：

命题 5.9 $M,s \models_E \varphi$当且仅当存在$k \geq 0$使得$M,s \models_{E,k} \varphi$。

用$M \models_{E,k} \varphi$表示存在初始状态为起点的k路径π使得$M,\pi \models_k \varphi$。

推论 5.2 $M \models_E \varphi$当且仅当存在$k \geq 0$使得$M \models_{E,k} \varphi$。

推论 5.3 $M \not\models \varphi$当且仅当存在$k \geq 0$使得$M \models_{E,k} \neg\varphi$。

完备阈值： 定义(M,φ)的完备阈值为满足以下条件的k。

$$M \not\models_{E,k} \neg\varphi，则对所有 i \geq 0, M \not\models_{E,k+i} \neg\varphi。$$

记(M,φ)的最小完备阈值为$lct(M,\varphi)$。

对任何M和φ，最小完备阈值$lct(M,\varphi)$存在且不超过$|M| \cdot 2^{|\varphi|}$。同时我们有以下结论。

推论 5.4 *若$k \geq lct(M,\varphi)$且$M \not\models_{E,k} \neg\varphi$，则$M \models \varphi$。*

推论 5.5 *若$M \models \varphi$，则$lct(M,\varphi) = 0$。*

注： 若不考虑非环语义部分，以上理论的各个命题同样成立，但对给定(M,φ)，其最小完备阈值可能不同。

§5.1.3 PLTL公式的Büchi 自动机表示

记$L(\pi) = [L(\pi_i)]_{i\geq 0}$。

2^{AP}上的字符串$\xi \in (2^{AP})^\omega$满足φ当且仅当存在$M = \langle S,R,I,L\rangle$和$M$的计算$\pi$使得$L(\pi) = \xi$且$M,\pi \models \varphi$。

记$[[\varphi]] \subseteq (2^{AP})^\omega$为满足$\varphi$的字符串的集合。

命题 5.10 *对任意PLTL公式φ，存在一个Büchi 自动机$A = \langle 2^{AP},S,\Delta,I,F\rangle$使得$\mathcal{L}(A) = [[\varphi]]$。*

由于Büchi 自动机可通过泛Büchi 自动机的转换得到，以下是一个构造语言等价于$[[\varphi]]$的泛Büchi 自动机$B_\varphi = \langle 2^{AP},S,\Delta,I,F\rangle$的方法。

1. 首先构造状态$x = (\{\varphi\},\{\},\{\})$，记$a(x) = \{\epsilon\}$。将其加入状态集$S$。

2. 对任意$x = (b,c,d) \in S$：

若$b = \emptyset$，构造状态$y = (d,\{\},\{\})$。若$y \in S$，则修改$a(y) = a(y) \cup \{x\}$，若$y \quad S$，记$a(y) = \{x\}$，并将y加入状态集S。

若$b = b_0 \cup \{\varphi\}$，我们分以下几种情况：

- 若$\varphi = \varphi_0 U \varphi_1$，构造状态$(b_0 \cup \{\varphi_0\}, c \cup \{\varphi\}, d \cup \{\varphi\})$ 和$(b_0 \cup \{\varphi_1\}, c \cup \{\varphi\}, d)$。
- 若$\varphi = \varphi_0 R \varphi_1$，构造状态$(b_0 \cup \{\varphi_1\}, c \cup \{\varphi\}, d \cup \{\varphi\})$ 和$(b_0 \cup \{\varphi_0, \varphi_1\}, c \cup \{\varphi\}, d)$。
- 若$\varphi = \varphi_0 \vee \varphi_1$，构造状态$(b_0 \cup \{\varphi_0\}, c \cup \{\varphi\}, d)$ 和$(b_0 \cup \{\varphi_1\}, c \cup \{\varphi\}, d)$。
- 若$\varphi = \varphi_0 \wedge \varphi_1$，构造状态$(b_0 \cup \{\varphi_0, \varphi_1\}, c \cup \{\varphi\}, d)$。
- 若$\varphi = O\varphi_0$，构造状态$(b_0, c \cup \{\varphi\}, d \cup \{\varphi_0\})$。
- 若$\varphi = p$或$\varphi = \neg p$，且$p \in AP$，构造状态$(b_0, c \cup \{\varphi\}, d)$。

用新构造的状态替代原状态x。

（a）化简：对每个新构造的状态$y = (b, c, d)$，若c中命题的集合是不可满足的，则从S中删除y；若$c \cap b \quad \emptyset$（广义上讲，若$\varphi \in b$且c蕴含φ，则可认为$\varphi \in c \cap b$），则从b 中删除公共部分$c \cap b$。

（b）检查是否重复构造：对每个新构造的状态y，若$y \in S$ （若$y' \in S$且y'与y要满足的公式是等价的，则亦可认为$y = y' \in S$）且$a(y) \quad \emptyset$，则修改$a(y) = a(y) \cup a(x)$; 若$y \in S$且$a(y) = \emptyset$，则对所有直接或间接替代y的状态$y' \in S$，修改$a(y') = a(y') \cup a(x)$; 然后将所有$a(z)$中出现x的地方用新构造的状态替代；若$y \quad S$，记$a(y) = a(x)$，并将y加入状态集S。

（c）完成替代：修改$a(x) = \emptyset$表示x已为新构造的状态所替代（并记录x与这些状态的关系待用）；返回第二步直至没有新加入状态集的状态。

3. 对任意$x = (b, c, d) \in S$，若$y \in a(x)$且$y = (b', c', d') \in S$，构造迁移(y, σ, x)，并将其加入迁移集合Δ，其中$\sigma \in 2^{AP}$ 满足$\forall p \in AP.(\{p, \neg p\} \not\subseteq \sigma \cup c') \wedge (p \in c' \to p \in \sigma)$。

4. 对任意$x = (b, c, d) \in S$，若$\epsilon \in a(x)$，则将x加入初始状态集合I。

5. 对每个公式φ，若$\varphi = \varphi_0 U \varphi_1$，构造$f_\varphi = \{(b, c, d) \in S \mid \varphi \in c \to \varphi_1 \in c\}$，并将其加入接受状态集集合$F$。

命题 5.11 *给定PLTL公式φ。设a为φ中出现的U和R的个数。定义$B_\varphi = \langle 2^{AP}, S, \Delta, I, F\rangle$其中$S, \Delta, I, F$的构造方法如上。则$\mathcal{L}(B_\varphi) = [[\varphi]]$且$|S| \leq 2^{|\varphi|-a}$。*

推论 5.6 *给定PLTL公式φ。φ可满足当且仅当$\mathcal{L}(B_\varphi)$非空。*

§5.2 PLTL公式的不动点表示与线性μ演算(νTL)

线性结构： 给定原子命题集合AP。一个线性结构为三元组$\langle S, \zeta, L\rangle$，其中$S$为状态集合，$\zeta = [\zeta_i]_{i\geq 0} \in S^\omega$为$S$的无穷序列，$L : S \to 2^{AP}$为标号函数。

定义 5.5 *给定线性结构$\langle S, \zeta, L\rangle$和PLTL公式$\varphi$。若存在标号Kripke模型$M = \langle S, R, I, L\rangle$使得$\zeta$是$M$的计算且$M, \zeta \models \varphi$，则称$\langle S, \zeta, L\rangle \models \varphi$。*

将$\mathbf{N}$的子集$\{i \mid \langle S, \zeta^i, L\rangle \models \varphi\}$记为$[[\varphi]]$。定义函数$o : 2^{\mathbf{N}} \to 2^{\mathbf{N}}$如下：

$$o(A) = \{i \in \mathbf{N} \mid i + 1 \in A\}$$

我们有以下等式：

$[[p]]$	$=$	$\{i \mid p \in L(\zeta_i)\}$
$[[\neg\varphi]]$	$=$	$\mathbf{N} \setminus [[\varphi]]$
$[[\varphi \vee \psi]]$	$=$	$[[\varphi]] \cup [[\psi]]$
$[[O\varphi]]$	$=$	$o([[\varphi]])$
$[[\varphi U \psi]]$	$=$	$[[\psi]] \cup ([[\varphi]] \cap [[O(\varphi U \psi)]]$

由以上等式知$[[\varphi U\psi]]$是$\tau(Z) = [[\psi]] \cup ([[\varphi]] \cap o(Z))$的不动点。根据$\tau$的定义知$\tau$有最小和最大不动点。根据PLTL语义知$[[\varphi U\psi]]$是$\tau$的最小不动点，即

$$[[\varphi U\psi]] \quad = \quad \mu Z.([[\psi]] \cup ([[\varphi]] \cap o(Z))$$

类似地，其它时序算子也可以用不动点刻画。为方便书写，我们直接将φ, ψ看成$\mathbf{N}$的子集，时序算子和逻辑联接符看成是$2^{\mathbf{N}}$上的函数。

$\Diamond\varphi$	$=$	$\mu Z.(\varphi \vee OZ)$
$\Box\varphi$	$=$	$\nu Z.(\varphi \wedge OZ)$
$\varphi U \psi$	$=$	$\mu Z.(\psi \vee (\varphi \wedge OZ))$
$\varphi R \psi$	$=$	$\nu Z.(\psi \wedge (\varphi \vee OZ))$

命题 5.12 *给定线性结构$\langle S, \zeta, L\rangle$和PLTL公式$\varphi$。$\langle S, \zeta, L\rangle \models \varphi$ 当且仅当$0 \in [[\varphi]]$。*

§5.2.1 线性μ演算：

由以上讨论知PLTL公式可以用时序算子O和不动点表示。在这种表示中，命题变量只出现在O, μ, ν之后。将这个约束去掉，我们可以得到一个表达能力更强的逻辑。称为νTL。给定一个原子命题集合AP，一个变量集合V。用p表示AP中任意命题，X表示V中任意变量。νTL 公式的集合由以下语法给出。

$$\phi ::= p \mid X \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid O\phi \mid \mu X.\phi \mid \nu X.\phi$$

其中$\mu X.\phi$和$\nu X.\phi$的ϕ中不受囿的X必须在偶数个$\neg$符号的作用范围之下。

νTL公式在线性结构上的语义解释： 给定线性结构$\langle S, \zeta, L\rangle$和$\nu$TL公式$\varphi$。设$e : V \to 2^N$为变量到$N$子集的赋值。$\nu$TL公式的语义如下：

$[[p]]e$	$=$	$\{i \in N \mid p \in L(\zeta_i)\}$
$[[X]]e$	$=$	$e(X)$
$[[\neg\phi]]e$	$=$	$N \setminus [[\phi]]e$
$[[\phi_1 \wedge \phi_2]]e$	$=$	$[[\phi_1]]e \cap [[\phi_2]]e$
$[[\phi_1 \vee \phi_2]]e$	$=$	$[[\phi_1]]e \cup [[\phi_2]]e$
$[[O\phi]]e$	$=$	$\{i \in N \mid i+1 \in [[\phi]]e\}$
$[[\mu X.\phi]]e$	$=$	$\cap\{M \subseteq N \mid [[\phi]]e[X/M] \subseteq M\}$
$[[\nu X.\phi]]e$	$=$	$\cup\{M \subseteq N \mid M \subseteq [[\phi]]e[X/M]\}$

定义 5.6 *给定线性结构$\langle S, \zeta, L\rangle$和$\nu$TL公式$\varphi$。$\langle S, \zeta, L\rangle \models \varphi$ 当且仅当$0 \in [[\varphi]]$。*

可满足性： 设φ为νTL公式。φ是可满足的，当且仅当存在$\langle S,\zeta,L\rangle$使得$\langle S,\zeta,L\rangle \models \varphi$。

重言式和等价： 设φ为νTL公式。φ是重言式，记作$\models \varphi$，当且仅当对任意$\langle S,\zeta,L\rangle$有$\langle S,\zeta,L\rangle \models \varphi$。$\varphi$等价于$\psi$，记作$\varphi \equiv \psi$，当且仅当$\models (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$。

模态算子的对偶关系与NNF范式： 只使用逻辑连接符$\wedge, \vee, \neg$且逻辑连接符$\neg$只出现在命题前面的公式称为NNF范式。每个νTL公式等价于一个νTL的NNF范式。一个νTL的NNF范式可应用以下对偶关系构造。

$\neg(O p)$	$\equiv$	$O\neg p$
$\neg\mu X.\phi$	$\equiv$	$\nu X.\neg\phi(\neg X/X)$

由对νTL公式中的变量的限制知νTL闭公式（没有自由变量的公式）的NNF范式中的所有变量都不在$\neg$符号的作用之下。

表达能力： νTL公式$\nu X.(p \wedge OO(X))$不能用PLTL公式表示。

命题 5.13 *νTL的表达能力强于PLTL。*

可满足性判定问题： 判定νTL公式是否可满足的问题称为νTL可满足性问题。νTL可满足性问题的复杂性为EXPTIME完全。

定义 5.7 *给定标号Kripke模型$M = \langle S,R,I,L\rangle$。$M$满足$\nu$TL公式$\varphi$，记作$M \models \varphi$，当且仅当对所有$\zeta \in [[M]]$有$\langle S,\zeta,L\rangle \models \varphi$。*

模型检测问题： 判定标号Kripke模型是否满足νTL公式的问题称为νTL模型检测问题。νTL模型检测问题的复杂性为PSPACE完全。

§5.2.2 PLTL公式到νTL公式的转换：

PLTL公式可以看成是νTL的一个子类，可用以下规则将PLTL公式转换到νTL 公式。

$$\begin{aligned}
T(p) &= p\\
T(\neg\varphi) &= \neg T(\varphi)\\
T(\varphi \vee \psi) &= T(\varphi) \vee T(\psi)\\
T(O\varphi) &= OT(\varphi)\\
T(\varphi U \psi) &= \mu Y.(T(\psi) \vee (T(\varphi) \wedge OY))
\end{aligned}$$

命题 5.14 *给定线性结构$\langle S,\zeta,L\rangle$和PLTL公式φ。$\langle S,\zeta,L\rangle \models \varphi$ 当且仅当$\langle S,\zeta,L\rangle \models T(\varphi)$。*

§5.2.3 公平标号Kripke结构上的LTL语义

符号集合AP上的LTL公式可在AP上的公平标号Kripke结构上解释。给定公平标号Kripke结构$M = \langle S,R,I,L,F\rangle$且$F = \{f_1,..,f_k\}$。

语义 设$M' = \langle S, R, I, L\rangle$为$M$去掉公平约束的标号Kripke结构。$M$满足LTL公式$\varphi$当且仅当对所有$M$的公平计算$\pi$，$M', \pi \models \varphi$。我们有以下结论。

命题 5.15 *$M \models \varphi$当且仅当$M' \models (\bigwedge_{i=1}^{k} \Box\Diamond f_i) \to \varphi$。*

§5.3 一阶线性时序逻辑

一阶线性时序逻辑用一阶逻辑来描述状态性质，具有表达能力强的优点。给定$B = (F, P)$上的一阶逻辑。用p表示WFF_B中的任意公式。B上的一阶线性时序逻辑公式的集合LTL由以下语法给出。

$$\phi ::= \quad p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \to \phi \mid \phi \leftrightarrow \phi \mid O\,\phi \mid \Diamond\,\phi \mid \Box\,\phi \mid \phi\, U\, \phi \mid \phi\, R\, \phi$$

给定B的解释I。设变量赋值的集合为Σ。

模型： LTL公式的模型M为Σ^ω的子集。

语义： 设$\zeta = \zeta_0\zeta_1\zeta_2\cdots \in \Sigma^\omega$。$\zeta$满足$\varphi$，记作$\zeta \models \varphi$，定义如下。

$\zeta \models p$	若$p \in WFF_B$且$\zeta_0 \models_I p$
$\zeta \models \neg\varphi$	若$\zeta \not\models \varphi$
$\zeta \models \varphi \vee \psi$	若$\zeta \models \varphi$或$\zeta \models \psi$
$\zeta \models \varphi \wedge \psi$	若$\zeta \models \varphi$且$\zeta \models \psi$
$\zeta \models \varphi \to \psi$	若$\zeta \models \varphi$则$\zeta \models \psi$
$\zeta \models \varphi \leftrightarrow \psi$	若$\zeta \models \varphi \to \psi$且$\zeta \models \psi \to \varphi$
$\zeta \models O\varphi$	若$\zeta^1 \models \varphi$
$\zeta \models \Box\psi$	若$\forall i \geq 0, \zeta^i \models \psi$
$\zeta \models \Diamond\varphi$	若$\exists i \geq 0, \zeta^i \models \varphi$
$\zeta \models \varphi U \psi$	若$\exists i \geq 0.(\zeta^i \models \psi$且$\forall 0 \leq j < i, \zeta^j \models \varphi)$
$\zeta \models \varphi R \psi$	若$\forall i \geq 0.(\zeta^i \models \psi$或$\exists 0 \leq j < i, \zeta^j \models \varphi)$

定义 5.8 *$M \models \varphi$，当且仅当对所有$\zeta \in M$都有$\zeta \models \varphi$。*

可满足性： 设φ为LTL公式。φ是可满足的，当且仅当存在M使得$\zeta \models \varphi$。

重言式和等价： 设φ和ψ为LTL公式。φ是重言式，记作$\models \varphi$，当且仅当对任意M有$M \models \varphi$。φ等价于ψ，记作$\varphi \equiv \psi$，当且仅当$\models \varphi \leftrightarrow \psi$。

完全集： 一阶线性时序逻辑中时序算子相互之间的可表达性和命题线性时序逻辑类似。我们有以下结论。

命题 5.16 *$\{O, U\}$是LTL的时序算子极小完全集。*

推理规则： 用$\varphi \Rightarrow \psi$表示$\Box(\varphi \to \psi)$。设$w, u \in QFF_B$为一元谓词公式(记其变量为x)且$\sqsubseteq$为P中二元谓词符号。设$W = \{\sigma(x) \mid I(w)(\sigma) = true\}$且$U = \{\sigma(x) \mid I(w \wedge u)(\sigma) = true\}$。若$(W, I_0(\sqsubseteq))$为$U$弱基集合，则称$(w, u, \sqsubseteq)$定义一个弱基集合。若$(W, I_0(\sqsubseteq))$为良基集合，则称$(w, \sqsubseteq)$定义一良基集合。

设$e \in T_B$为项，v为没有在公式中出现过的变量，$\sqsubseteq$为P中二元谓词符号，$w, u \in QFF_B$为一元谓词公式且$(w, u, \sqsubseteq)$定义一弱基集合。根据LTL公式的语义，我们有以下推理规则。

$$\frac{\varphi \Rightarrow \psi}{\varphi \Rightarrow \varphi_0 U \psi}$$

$$\frac{\varphi \Rightarrow O(\psi)}{\varphi \Rightarrow O(\varphi_0 U \psi)}$$

$$\frac{\begin{array}{lcl} \phi_2 & \Rightarrow & \psi_2 \\ \phi_2 \wedge \neg\psi_1 & \Rightarrow & O(\psi_2 U \phi_2) \\ \phi_1 & \Rightarrow & \psi_0 \wedge w_x^e \\ \phi_1 \wedge \neg\psi_2 & \Rightarrow & \neg u_x^e \\ \phi_1 \wedge e = v & \Rightarrow & O(\phi_1 U(\phi_2 \vee (\phi_1 \wedge e \sqsubset v))) \\ \varphi & \Rightarrow & (\phi_1 \vee \phi_2) \end{array}}{\varphi \Rightarrow \psi_0 U(\psi_1 R \psi_2)}$$

由以上推理规则，可得出如下规则用于形式为$\psi_1 R \psi_2$和$\psi_1 U \psi_2$的公式的推理（其中$(w, \sqsubseteq)$定义一良基集合）。

$$\frac{\begin{array}{lcl} \phi_2 & \Rightarrow & \psi_2 \\ \phi_2 \wedge \neg\psi_1 & \Rightarrow & O(\psi_2 U \phi_2) \\ \varphi & \Rightarrow & \phi_2 \end{array}}{\varphi \Rightarrow \psi_1 R \psi_2} \qquad \frac{\begin{array}{lcl} \phi_1 & \Rightarrow & \psi_0 \wedge w_x^e \\ \phi_1 \wedge e = v & \Rightarrow & O(\phi_1 U(\psi_1 \vee (\phi_1 \wedge e \sqsubset v))) \\ \varphi & \Rightarrow & (\phi_1 \vee \psi_1) \end{array}}{\varphi \Rightarrow \psi_0 U \psi_1}$$

通过进一步化简可得以下推理规则(右边的规则可由左边规则得到)。

$$\frac{\varphi \Rightarrow \psi' \quad \psi' \wedge \neg\varphi_0 \Rightarrow O\psi' \quad \psi' \Rightarrow \psi}{\varphi \Rightarrow \varphi_0 R \psi} \qquad \frac{\varphi \Rightarrow \psi' \quad \psi' \Rightarrow O\psi' \quad \psi' \Rightarrow \psi}{\varphi \Rightarrow \Box\psi}$$

$$\frac{\varphi \Rightarrow (\psi \vee \phi) \quad \phi \Rightarrow \varphi_0 \wedge w_x^e \quad \phi \wedge e = v \Rightarrow O(\psi \vee (\phi \wedge e \sqsubset v))}{\varphi \Rightarrow \varphi_0 U \psi} \qquad \frac{\varphi \Rightarrow (\psi \vee \phi) \quad \phi \Rightarrow w_x^e \quad \phi \wedge e = v \Rightarrow O(\psi \vee (\phi \wedge e \sqsubset v))}{\varphi \Rightarrow \Diamond\psi}$$

注： 基于谓词逻辑的迁移模型通常对应于满足一定约束的Σ^ω的子集。比如我们可以对模型M添加以下约束。

若$\zeta, \zeta' \in M$且$\zeta_i = \zeta'_j$，	则$\zeta_0 \cdots \zeta_i \zeta'_{j+1} \zeta'_{j+2} \cdots \in M$
若$\zeta \in M$且$\zeta_i = \zeta_j$且$i < j$，	则$\zeta_0 \cdots \zeta_{i-1} (\zeta_i \cdots \zeta_{j-1})^\omega \in M$
若$\zeta \in M$且$\zeta_i = \zeta_{i+1}$，	则$\zeta = \zeta_0 \cdots \zeta_{i-1} (\zeta_i)^\omega$

§5.4 例子

例 5.1 （1）用语义证明$Op \equiv \neg O \neg p$。

证：给定任意标号*Kripke*模型M。设ζ为M的任意计算。我们有如下等价关系。

$$\begin{aligned} \zeta &\models Op \quad &\Leftrightarrow \\ \zeta^1 &\models p \quad &\Leftrightarrow \\ \zeta^1 &\not\models \neg p \quad &\Leftrightarrow \\ \zeta &\not\models O\neg p \quad &\Leftrightarrow \\ \zeta &\models \neg O \neg p \end{aligned}$$

因而$Op \equiv \neg O \neg p$。

（2）用语义证明$pRq \equiv (qU(p \wedge q)) \vee \Box q$。

证：给定任意标号*Kripke*模型M。设ζ为M的任意计算。

（a）从左到右的蕴含。

假设$\zeta \models pRq$。

对任意$i \geq 0$，若对所有$j < i$都有$\zeta^j \not\models p$，则$\zeta^i \models q$。

若对所有$j \geq 0$都有$\zeta^j \not\models p$，那么对所有$i \geq 0$有$\zeta^i \models q$，因而$\zeta \models \Box q$成立。

否则存在最小的j使得$\zeta^j \models p$，那么对所有$i \leq j$有$\zeta^i \models q$，因而$\zeta \models qU(p \wedge q)$成立。

（b）从右到左的蕴含。

假设$\zeta \models (qU(p \wedge q)) \vee \Box q$。

若$\zeta \models \Box q$，那么对所有$i \geq 0$有$\zeta^i \models q$，因而$\zeta \models pRq$成立。

否则$\zeta \models (qU(p \wedge q))$成立，存在最小的$j$使得$\zeta^j \models p \wedge q$且对所有$i < j$有$\zeta^i \models q$，因而$\zeta \models (qU(p \wedge q))$成立。

（3）用语义证明$pRq \to \Box q$不成立。

证：构造$AP = \{p, q\}$上的模型$M = (S, R, I, L)$其中$S = \{s_0, s_1\}, R = \{(s_0, s_1), (s_1, s_1)\}, I = \{s_0\}, L(s_0) = \{p, q\}, L(s_1) = \{\}$。

我们有$M \models pRq$且$M \not\models \Box q$。因而存在不满足$pRq \to \Box q$的模型。

例 5.2 （1）O算子不能用仅用U算子和命题逻辑连接符表示。

证：定义$M = \langle S, R, I, L\rangle$其中$S = \{s_0, s_1, s_2\}$，$R = \{(s_0, s_1), (s_1, s_2), (s_2, s_0)\}$，$I = \{s_0\}$，$L(s_0) = L(s_1) = \{\}$且$L(s_2) = \{p\}$。

定义$M' = \langle S, R, I', L\rangle$其中$I = \{s_1\}$。

我们有$M \not\models Op$且$M' \models Op$。

设φ为仅用U算子和命题逻辑连接符构造的公式。

若φ的长度为1。则$M \models \varphi$当且仅当$M' \models \varphi$。

假设对φ_0, φ_1有$M \models \varphi_0$当且仅当$M' \models \varphi_0$且$M \models \varphi_1$当且仅当$M' \models \varphi_1$。

设φ是用φ_0, φ_1和命题逻辑连接符构造的公式，则易知$M \models \varphi$当且仅当$M' \models \varphi$。

设$\varphi = \varphi_0 U \varphi_1$。

设$\zeta = s_0 s_1 s_2 (s_0 s_1 s_2)^\omega$。

分以下三种情况讨论。

- $\zeta^0 \models \varphi_1$。

  由假设知$\zeta^1 \models \varphi_1$。因而我们有$\zeta^0 \models \varphi$且$\zeta^1 \models \varphi$。

- $\zeta^0 \models \neg\varphi_1$且$\zeta^0 \models \varphi_0$。

  我们有$\zeta^0 \models \varphi$当且仅当$\zeta^1 \models \varphi$。

- $\zeta^0 \models \neg\varphi_1$且$\zeta^0 \models \neg\varphi_0$。

  由假设知$\zeta^1 \models \neg\varphi_1$且$\zeta^1 \models \neg\varphi_0$。因而我们有$\zeta^0 \models \neg\varphi$且$\zeta^1 \models \neg\varphi$。

因而$M \models \varphi$当且仅当$M' \models \varphi$。

由归纳法知对任意长度的仅用U算子和命题逻辑连接符的公式φ，我们有$M \models \varphi$当且仅当$M' \models \varphi$。

因而Op不等价于任何这样的一个公式。

（2）U算子不能用仅用O算子和命题逻辑连接符表示。

证：定义$M_k = \langle S_k, R, I, L\rangle$和$M'_k = \langle S_k, R, I, L'\rangle$如下。

$$
\begin{aligned}
&S_k = \{s_0, s_1, ..., s_k\}\\
&R = \{(s_0, s_1), (s_1, s_2), ..., (s_{k-1}, s_k), (s_k, s_k)\}\\
&I = \{s_0\}\\
&L(s_0) = \cdots = L(s_{k-1}) = L(s_k) = \{\}\\
&L'(s_0) = \cdots = L'(s_{k-1}) = \{\}\\
&L'(s_k) = \{p\}
\end{aligned}
$$

我们有$M_k \not\models (\neg p) U p$且$M' \models (\neg p) U p$。

设φ为仅用O算子和命题逻辑连接符构造的公式。

若φ中O的个数为1。则对所有$k \geq 1$有$M_k \models \varphi$当且仅当$M'_k \models \varphi$。

假设对φ_0, φ_1有对所有$k \geq m$有$M_k \models \varphi_0$当且仅当$M'_k \models \varphi_0$且$M_k \models \varphi_1$当且仅当$M'_k \models \varphi_1$。

设φ是用φ_0, φ_1和命题逻辑连接符构造的公式，则易知对所有$k \geq m$有$M_k \models \varphi$当且仅当$M'_k \models \varphi$。

设$\varphi = O\varphi_0$。则易知对所有$k \geq m+1$有$M_k \models \varphi$当且仅当$M'_k \models \varphi$。

由归纳法知对仅用m个O和任意多个命题逻辑连接符的公式φ，我们有$M_{m+1} \models \varphi$当且仅当$M'_{m+1} \models \varphi$。

因而$(\neg p)Up$不等价于任何这样的一个用有限个O和任意多个命题逻辑连接符构造的公式。

例 5.3 （1）用推理系统证明$p \wedge \Box Op \to \Box p$。

证：用A_i表示第i条时序逻辑公理。简单起见用a, b, c分别代表$\Box Op, \Box(p \to Op), p \to \Box p$。我们证明$p \wedge \Box Op \to \Box p$如下。

1	$Op \to (p \to Op)$	AX
2	$\Box(Op \to (p \to Op))$	$1, G$
3	$\Box Op \to \Box(p \to Op)$	$2, A_2, MP$
4	$(a \to b) \to ((b \to c) \to (a \to c))$	AX
5	$(b \to c) \to (a \to c)$	$4, 3, MP$
6	$\Box Op \to (p \to \Box p)$	$5, A_6, MP$
7	$(\Box Op \to (p \to \Box p)) \to (p \wedge \Box Op \to \Box p)$	AX
8	$p \wedge \Box Op \to \Box p$	$7, 6, MP$

若将p和Op列为前提条件，则$\Box p$的证明如下。

1	p	–
2	$\Box Op$	–
3	$Op \to (p \to Op)$	AX
4	$\Box(Op \to (p \to Op))$	$3, G$
5	$\Box Op \to \Box(p \to Op)$	$4, A_2, MP$
6	$\Box(p \to Op)$	$5, 2, MP$
7	$p \to \Box p$	$6, A_6, MP$
8	$\Box p$	$7, 1, MP$

（2）用推理系统证明$(Op \to Oq) \to O(p \to q)$。

证：用e, f分别代表$(Op \to Oq), O(p \to q)$。我们证明$e \to f$如下。

1	$\neg p \to (p \to q)$	AX
2	$\Box(\neg p \to (p \to q))$	G
3	$O(\neg p \to (p \to q))$	A_4, MP
4	$O\neg p \to f$	A_8, MP
5	$(\neg Op \leftrightarrow O\neg p) \to ((O\neg p \to f) \to (\neg Op \to f))$	AX
6	$\neg Op \to O(p \to q))$	$A_7, 4, 5, MP$
7	$q \to (p \to q)$	AX
8	$\Box(q \to (p \to q))$	G
9	$O(q \to (p \to q))$	A_4, MP
10	$Oq \to f$	A_8, MP
11	$(\neg Op \to f) \to (Oq \to f) \to (e \to f)$	AX
12	$(e \to f)$	$6, 10, 11, MP$

例 5.4 设r, g, a为命题，φ为以下公式的合取。

$$\Box(r \wedge \neg a \to ((r \wedge \neg a)U(r \wedge a)))$$
$$\Box(r \wedge a \to ((r \wedge a)U(g \wedge \neg a)))$$
$$\Box(g \wedge \neg a) \to ((g \wedge \neg a)U((r \wedge \neg a) \vee (g \wedge a)))$$
$$\Box(g \wedge a) \to ((g \wedge a)U(r \wedge \neg a)))$$
$$\Box(\neg(r \wedge g))$$
$$r \wedge \neg a$$

若r, g表示过街用的红绿灯的状态，a表示行人按过过街绿色按钮（重复按不产生效果）的状态，$\neg a$表示行人可按过街绿色按钮的状态。则公式φ可表示以下描述：

- 初始状态为红灯且行人可按过街绿色按钮。
- 行人按了绿色按钮之后一段时间红灯变为绿灯，且在这段时间内没法再按绿色按钮（或者说重复按不产生效果）。
- 红灯变为绿灯之后，可有效地重复按过街绿色按钮一次以保持绿灯。
- 若红灯变为绿灯之后没有行人按过街绿色按钮，则一段时间之后绿灯变为红灯、返回初始状态。
- 若红灯变为绿灯之后有行人按过街绿色按钮，则继续保持绿灯且在这段时间内没法再按绿色按钮。
- 若红灯变为绿灯之后且有行人按过过街绿色按钮，则过一段时间之后绿灯变为红灯、返回初始状态。
- 红灯和绿灯不能同时出现。

例 5.5 （1）设AP和$K_3 = (S, R, I, L)$如例2.3中所定义。用限界语义证明$K_3 \not\models \Diamond(p_3 \vee p_6)$。

证：尝试找到k和从初始状态出发的k路径π使得$K_3, \pi \models_k \Box\neg(p_3 \vee p_6)$成立。

（a）$k = 0$时有如下长度为1的初始状态出发的k路径：s_0 和s_1。这些路径均不满足所需条件。

（b）$k = 1$时有如下初始状态出发的k路径：$s_0s_{12}, s_1s_{12}, s_0s_{27}, s_1s_{27},$。这些路径均不满足所需条件。

（c）检查$k = 2$时所有初始状态出发的k路径，其中$\pi = s_0s_{27}s_{38}$是$(2,1)$环路径且$K_3, \pi \models_k \Box\neg(p_3 \vee p_6)$成立。因而$K_3 \not\models \Diamond(p_3 \vee p_6)$。

（d）由以上分析知$(K_3, \Diamond(p_3 \vee p_6))$的最小完备阈值为$k = 2$，即用限界语义能够证明$K_3 \not\models \Diamond(p_3 \vee p_6)$的最小$k$。

（2）设AP和S, R', I, L如例2.3中所定义。令$K_3' = (S, R', I, L)$。用限界语义证明$K_1 \models \Diamond(p_3 \vee p_6)$。

证：尝试寻找k和从初始状态出发的k路径π使得$M, \pi \models_k \Box\neg(p_3 \vee p_6)$成立。

由限界语义理论知$K_3' \models \Diamond(p_3 \vee p_6)$的完备阈值不超过$|M| \cdot 2^4$。

在k从零到完备阈值的范围不存在初始状态出发的k路径π使得$K_3', \pi \models_k \Box\neg(p_3 \vee p_6)$ 成立，因而$K_3' \models \Diamond(p_3 \vee p_6)$成立。

例 5.6 （1）将$PLTL$公式Gp化为等价的自动机的构造如下。

（a）将Gp写成$\bot R p$，我们有初始节点$n_0 = (\{\bot R p\}, \{\}, \{\})$且$a(n_0) = \{\epsilon\}$。

（b）演化如下。

label	*n*	*a*(*n*)	*eq*
1	$\{\bot R p\}, \{\}, \{\}$	$\{\epsilon\}$	*11,12*
11	$\{\bot, p\}, \{\bot R p\}, \{\}$	$\{\epsilon\}$	*11'*
12	$\{p\}, \{\bot R p\}, \{\bot R p\}$	$\{\epsilon\}$	*12'*
11'	$\{\}, \{\bot, p, \bot R p\}, \{\}$	$\{\epsilon\}$	*0*
12'	$\{\}, \{p, \bot R p\}, \{\bot R p\}$	$\{\epsilon\}$	
2	$\{\bot R p\}, \{\}, \{\}$	$\{12'\}$	*1*

开始时我们有节点1，然后转化为11和12，然后这两个节点分别转化为11′和12′。节点11′由于不可满足被删除（最右列的值为0表示删除），12′产生后继2，2等同于1。

（c）去掉完成转化的剩余的节点并且合并相同的节点，最后剩下的节点的标号为12′。

（d）我们有$S = \{12'\}$，$I = \{12'\}$。由于不存在最外层时序算子为U的子公式，$F = \{\}$。由自动机的构造方法知Σ为$\{p\}$的幂集。$\Delta = \{(12', \{p\}, 12')\}$。

由以上构造知$(\Sigma, S, \Delta, I, F)$是等价于$Gp$的泛*Büchi* 自动机。

（2）将$PLTL$公式qUr化为等价的自动机的构造如下。

（a）我们有初始节点$n_0 = (\{qUr\}, \{\}, \{\})$且$a(n_0) = \{\epsilon\}$。

（b）演化如下。

label	*n*	*a*(*n*)	*eq*
1	$\{qUr\},\{\},\{\}$	$\{\epsilon\}$	*11,12*
11	$\{r\},\{qUr\},\{\}$	$\{\epsilon\}$	*11'*
12	$\{q\},\{qUr\},\{qUr\}$	$\{\epsilon\}$	*12'*
11'	$\{\},\{qUr,r\},\{\}$	$\{\epsilon\}$	
12'	$\{\},\{qUr,q\},\{qUr\}$	$\{\epsilon\}$	
2	$\{\},\{\},\{\}$	$\{\epsilon,11'\}$	
3	$\{qUr\},\{\},\{\}$	$\{\epsilon,12'\}$	*1*
4	$\{\},\{\},\{\}$	$\{\epsilon,2\}$	*2*

开始时我们有节点1，然后转化为11和12，然后这两个节点分别转化为$11'$和$12'$。由$11'$产生后继2，由$12'$产生后继3。由2产生后继4。3和4分别等同于2和1。

（*c*）去掉完成转化的节点并且合并相同的节点，最后剩下的节点的标号为$11', 12', 2$。

（*d*）我们有$S = \{11', 12', 2\}$，$I = \{11', 12'\}$，$F = \{\{11', 2\}\}$。由自动机的构造方法知Σ为$\{q, r\}$的幂集。用a表示$\{q, r\}$的子集。Δ为以下集合的并集。

$$\{(11', a, 2) \mid a \models r\}$$
$$\{(12', a, 31') \mid a \models q\}$$
$$\{(2, a, 2) \mid a \subseteq \{q, r\}\}$$

由以上构造知$(\Sigma, S, \Delta, I, F)$是等价于$qUr$的泛*Büchi* 自动机。

（*3*）将*PLTL*公式$pU(qUr)$化为等价的自动机的构造如下。

（*a*）我们有初始节点$n_0 = (\{pU(qUr)\},\{\},\{\})$且$a(n_0) = \{\epsilon\}$。

（*b*）演化如下。

label	*n*	*a*(*n*)	*eq*
1	$\{pU(qUr)\},\{\},\{\}$	$\{\epsilon\}$	*11,12*
11	$\{qUr\},\{pU(qUr)\},\{\}$	$\{\epsilon\}$	*111,112*
12	$\{p\},\{pU(qUr)\},\{pU(qUr)\}$	$\{\epsilon\}$	*12'*
111	$\{r\},\{pU(qUr),qUr\},\{\}$	$\{\epsilon\}$	*111'*
112	$\{q\},\{pU(qUr),qUr\},\{,qUr)\}$	$\{\epsilon\}$	*112'*
111'	$\{\},\{pU(qUr),qUr,r\},\{\}$	$\{\epsilon\}$	
112'	$\{\},\{pU(qUr),qUr,q\},\{qUr)\}$	$\{\epsilon\}$	
12'	$\{\},\{pU(qUr),p\},\{pU(qUr)\}$	$\{\epsilon\}$	
2	$\{\},\{\},\{\}$	$\{\epsilon,111'\}$	
3	$\{qUr\},\{\},\{\}$	$\{\epsilon,112'\}$	*31,32*
4	$\{pU(qUr)\},\{\},\{\}$	$\{\epsilon,12'\}$	*1*
31	$\{r\},\{qUr\},\{\}$	$\{\epsilon,112'\}$	*31'*
32	$\{q\},\{qUr\},\{qUr\}$	$\{\epsilon,112'\}$	*32'*
31'	$\{\},\{qUr,r\},\{\}$	$\{\epsilon,112'\}$	
32'	$\{\},\{qUr,q\},\{qUr\}$	$\{\epsilon,112'\}$	
5	$\{\},\{\},\{\}$	$\{\epsilon,111',2\}$	*2*
6	$\{\},\{\},\{\}$	$\{\epsilon,112',31'\}$	*2*
7	$\{qUr\},\{\},\{\}$	$\{\epsilon,112',32'\}$	*3*

(*c*)去掉完成转化的节点并且合并相同的节点，最后剩下的节点的标号为$111',112',12',2,31',32'$。
(*d*) 我们有

$$
\begin{aligned}
&S=\{111',112',12',2,31',32'\},\\
&I=\{111',112',12'\},\\
&F=\{\{111',112',2,31',32'\},\{111',12',2,31'\}\}。
\end{aligned}
$$

由自动机的构造方法知Σ为$\{p,q,r\}$的幂集。用a表示$\{p,q,r\}$的子集。Δ为以下集合的并集。

$$
\begin{array}{ll}
\{(111',a,2)\mid a\models r\} & \{(112',a,31')\mid a\models q\}\\
\{(112',a,32')\mid a\models q\} & \{(12',a,111')\mid a\models p\}\\
\{(12',a,112')\mid a\models p\} & \{(12',a,12')\mid a\models p\}\\
\{(2,a,2)\mid a\subseteq\{p,q,r\}\} & \{(31',a,2)\mid a\models r\}\\
\{(32',a,2)\mid a\models q\} & \{(32',a,32')\mid a\models q\}
\end{array}
$$

由以上构造知(Σ,S,Δ,I,F)是等价于$pU(qUr)$的泛*Büchi* 自动机。

§5.5 练习

1. 用PLTL语义证明$\Box(p\to Op)\to(p\to\Box p)$成立且解释这个蕴含关系反过来不成立。
2. 用PLTL推理系统证明$O(p\vee q)\leftrightarrow(Op\vee Oq)$。
3. 用PLTL写下信号灯变化的规范：信号灯依次序绿黄红变化，每个状态有且只有一个信号，初始信号为绿色，黄色只停留一个状态，红绿色可以连续在多个状态上成立。

4. 设AP和$K_3' = (S, R', I, L)$如例5.5中所定义。设$\varphi_1 = (p_1 \vee p_2)Up_3$和$\varphi_2 = (p_1 \vee p_2)U(p_3 \vee p_6)$。用限界语义证明$K_3' \models \varphi_1$不成立且$K_3' \models \varphi_2$成立。

5. 分别构造与公式$(p \vee (qUr))$和$(Xp \wedge (qRr))$等价的自动机。

§6 分枝时序逻辑

本章介绍可用以描述程序模型性质的分枝时序逻辑。抽象模型中的一个状态通常有多个可能的后继状态和多条可能从该状态出发的路径。线性时序逻辑仅表达线性运行过程的性质。表达这类分枝路径的性质则需要在逻辑中添加路径量词。

§6.1 计算树逻辑CTL

考虑建立在命题逻辑上的计算树逻辑，记作CTL。给定一个原子命题集合AP。用p表示AP中的任意命题。PLTL公式的集合由以下语法给出。

$$\begin{aligned}\phi ::= \quad & p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \phi \to \phi \mid \phi \leftrightarrow \phi \mid \\ & EX\,\phi \mid EF\,\phi \mid EG\,\phi \mid E(\phi\, U\, \phi) \mid E(\phi\, R\, \phi) \mid AX\,\phi \mid AF\,\phi \mid AG\,\phi \mid A(\phi\, U\, \phi) \mid A(\phi\, R\, \phi)\end{aligned}$$

符号$EX, EF, EG, EU, ER, AX, AF, AG, AU, AR$称为CTL的时序算子。

模型： AP上的CTL公式在AP上的标号Kripke结构上解释。

CTL公式的语义： 给定$M = \langle S, R, I, L\rangle$。状态$s \in S$满足CTL公式$\varphi$，记为$M, s \models \varphi$，在$M$已确定的情况亦写做$s \models \varphi$，定义如下。

$s \models p$	若$p \in AP$且$p \in L(s)$
$s \models \neg\varphi$	若$s \not\models \varphi$
$s \models \varphi \vee \psi$	若$s \models \varphi$ 或$s \models \psi$
$s \models \varphi \wedge \psi$	若$s \models \varphi$ 且$s \models \psi$
$s \models \varphi \to \psi$	若$s \models \varphi$ 则$s \models \psi$
$s \models \varphi \leftrightarrow \psi$	若$s \models \varphi \to \psi$ 且$s \models \psi \to \varphi$
$s \models EX\varphi$	若存在s的后继v使得$v \models \varphi$
$s \models EG\psi$	若存在s为起点的无穷路径ζ使得$\forall i \geq 0, \zeta_i \models \psi$
$s \models EF\psi$	若存在s为起点的无穷路径ζ使得$\exists i \geq 0, \zeta_i \models \psi$
$s \models E(\varphi U \psi)$	若存在s为起点的无穷路径ζ使得$\exists i \geq 0.(\zeta_i \models \psi$ 且$\forall 0 \leq j < i, \zeta_j \models \varphi)$
$s \models E(\varphi R \psi)$	若存在s为起点的无穷路径ζ使得$\forall i \geq 0.(\zeta_i \models \psi$ 或$\exists 0 \leq j < i, \zeta_j \models \varphi)$
$s \models AX\varphi$	若对所有s的后继v有$v \models \varphi$
$s \models AG\psi$	若对所有s为起点的无穷路径ζ有$\forall i \geq 0, \zeta_i \models \psi$
$s \models AF\psi$	若对所有s为起点的无穷路径ζ有$\exists i \geq 0, \zeta_i \models \psi$
$s \models A(\varphi U \psi)$	若对所有s为起点的无穷路径ζ有$\exists i \geq 0.(\zeta_i \models \psi$ 且$\forall 0 \leq j < i, \zeta_j \models \varphi)$
$s \models A(\varphi R \psi)$	若对所有s为起点的无穷路径ζ有$\forall i \geq 0.(\zeta_i \models \psi$ 或$\exists 0 \leq j < i, \zeta_j \models \varphi)$

定义 6.1 $M \models \varphi$当且仅当对所有$s \in I$有$M, s \models \varphi$。

可满足性： 设φ为CTL公式。φ是可满足的，当且仅当存在标号Kripke结构M使得$M \models \varphi$。

重言式和等价： 设φ和ψ为CTL公式。φ是重言式，记作$\models \varphi$，当且仅当对标号Kripke结构M有$M \models \varphi$。φ等价于ψ，记作$\varphi \equiv \psi$，当且仅当$\models \varphi \leftrightarrow \psi$。

等价公式： 设φ和ψ为CTL公式。我们有以下等价的公式对。

$AX\varphi$	$\equiv$	$\neg EX\neg\varphi$
$AG\varphi$	$\equiv$	$\neg EF\neg\varphi$
$AF\varphi$	$\equiv$	$\neg EG\neg\varphi$
$A(\varphi R\psi)$	$\equiv$	$\neg E(\neg\varphi U\neg\psi)$
$A(\varphi U\psi)$	$\equiv$	$\neg E(\neg\varphi R\neg\psi)$
$E(\varphi U\psi)$	$\equiv$	$\psi\vee(\varphi\wedge EXE(\psi U(\varphi\wedge\psi)))$
$E(\varphi R\psi)$	$\equiv$	$\psi\wedge(\varphi\vee EXE(\psi U(\varphi\wedge\psi)))$
$EF\varphi$	$\equiv$	$E(\top U\varphi)$
$EG\varphi$	$\equiv$	$E(\neg\top R\varphi)$
$E(\varphi R\psi)$	$\equiv$	$E(\psi U(\varphi\wedge\psi))\vee EG\psi$

命题 6.1 *$\{EX, EG, EU\}$是CTL的时序算子极小完全集。*

NNF范式： 只使用逻辑连接符$\wedge,\vee,\neg$且逻辑联接符$\neg$只出现在命题前面的公式称为NNF范式。

命题 6.2 *每个CTL公式等价于一个CTL的NNF范式。*

对每个CTL公式，我们可以将其转换成等价的只使用$\{\wedge,\vee,\neg\}$中的命题逻辑联接符和$\{EX, EG, EU\}$中的时序算子的公式，然后再继续使用以上提到的等价关系和以下与命题逻辑联接符相关的等价关系将其转换成时序算子在$\{EX, ER, EU, AX, AR, AU\}$中的NNF范式公式。

$\neg\neg\varphi$	$\equiv$	φ
$\neg(\varphi\vee\psi)$	$\equiv$	$\neg\varphi\wedge\neg\psi$
$\neg(\varphi\wedge\psi)$	$\equiv$	$\neg\varphi\vee\neg\psi$

可满足性判定问题： 判定CTL公式是否可满足的问题称为CTL可满足性问题。CTL可满足性问题的复杂性为EXPTIME完全。

模型检测问题： 判定模型是否满足CTL公式的问题称为CTL模型检测问题。CTL模型检测问题的复杂性为P完全。

§6.1.1 CTL公式的推理

以$\{EX, EU, EG, EF, AX, AU, AG, AF\}$为CTL公式的时序算子集。CTL的推理系统包含以下三部分：一部分为CTL式相关的时序逻辑公理；另一部分为命题逻辑的推理系统；第三部分为时序推理规则。设p, q, r为CTL公式。

时序逻辑公理：

$EFp \leftrightarrow E(\top Up)$	$A(pUq) \leftrightarrow (q \vee (p \wedge AXA(pUq))$
$AGp \leftrightarrow \neg EF\neg p$	$EX\top \wedge AX\top$
$AFp \leftrightarrow A(\top Up)$	$AG(r \rightarrow (\neg q \wedge EXr)) \rightarrow (r \rightarrow \neg A(pUq))$
$EGp \leftrightarrow \neg AF\neg p$	$AG(r \rightarrow (\neg q \wedge EXr)) \rightarrow (r \rightarrow \neg AFq)$
$EX(p \vee q) \leftrightarrow EXp \vee EXq$	$AG(r \rightarrow (\neg q \wedge (p \rightarrow AXr))) \rightarrow (r \rightarrow \neg E(pUq))$
$AXp \leftrightarrow \neg EX\neg p$	$AG(r \rightarrow (\neg q \wedge AXr)) \rightarrow (r \rightarrow \neg EFq)$
$E(pUq) \leftrightarrow (q \vee (p \wedge EXE(pUq))$	$AG(p \rightarrow q) \rightarrow (EXp \rightarrow EXq)$

命题逻辑推理系统：

（AX）若p是命题逻辑的重言式的实例，则p是公理。

（MP）若$\vdash p \rightarrow q$且$\vdash p$，则$\vdash q$。

时序推理规则：

（G）若$\vdash p$，则$\vdash AGp$。

命题 6.3 *CTL推理系统是可靠且完备的。*

§6.1.2 CTL限界语义

给定有穷状态标号Kripke结构$M = \langle S, R, I, L\rangle$。

称长度$k+1$的路径为k路径。记k路径的集合为P_k。

以下考虑仅用AX, AR, AU, EX, ER, EU时序算子的NNF范式的CTL公式。

用$\pi \in P_k(s)$表示π是以s为起点的k路径。

用$\gamma(\pi)$表示π中有重复出现的状态，定义如下。

$$\gamma(\pi) = \bigvee_{i=0}^{k-1} \bigvee_{j=i+1}^{k} \pi_i = \pi_j$$

用$\gamma_0(M, \pi, k, \varphi)$表示以下公式（用于定义6.2中限界语义$\models_k$的定义）。

$$\bigwedge_{i=0}^{k} (M, \pi_i \not\models_k \varphi) \rightarrow \gamma(\pi)$$

定义 6.2 *设φ为CTL公式。限界语义$M, s \models_k \varphi$定义如下。*

$M, s \models_k p$	若$p \in AP$且$p \in L(s)$
$M, s \models_k \neg p$	若$M, s \not\models_k p$
$M, s \models_k \varphi \vee \psi$	若$M, s \models_k \varphi$ 或$M, s \models_k \psi$
$M, s \models_k \varphi \wedge \psi$	若$M, s \models_k \varphi$ 且$M, s \models_k \psi$
$M, s \models_k AX\varphi$	若$k \geq 1$且$\forall \pi \in P_k(s)$，$M, \pi_1 \models_k \varphi$
$M, s \models_k A(\varphi U \psi)$	若$\forall \pi \in P_k(s)$，$\exists i \leq k, M, \pi_i \models_k \psi$ 且$\forall j < i, M, \pi_j \models_k \varphi$
$M, s \models_k A(\varphi R \psi)$	若$\forall \pi \in P_k(s)$，$(\forall i \leq k.(\forall j < i.(M, \pi_j \not\models_k \varphi) \rightarrow (M, \pi_i \models_k \psi)))$且$\gamma_0(M, \pi, k, \varphi)$
$M, s \models_k EX\varphi$	若$k \geq 1$且$\exists \pi \in P_k(s)$，$M, \pi_1 \models_k \varphi$
$M, s \models_k E(\varphi U \psi)$	若$\exists \pi \in P_k(s)$，$\exists i \leq k, M, \pi_i \models_k \psi$ 且$\forall j < i, M, \pi_j \models_k \varphi$
$M, s \models_k E(\varphi R \psi)$	若$\exists \pi \in P_k(s)$，$(\forall i \leq k.(\forall j < i.(M, \pi_j \not\models_k \varphi) \rightarrow (M, \pi_i \models_k \psi)))$且$\gamma_0(M, \pi, k, \varphi)$

命题 6.4 *对所有$k \geq 0$，若$M, s \models_k \varphi$，则$M, s \models_{k+1} \varphi$。*

正确性与完备性：

命题 6.5 *$M, s \models \varphi$当且仅当存在$k \geq 0$使得$M, s \models_k \varphi$。*

用$M \models_k \varphi$表示对所有初始状态s有$M, s \models_k \varphi$。

推论 6.1 *$M \models \varphi$当且仅当存在$k \geq 0$使得$M \models_k \varphi$。*

推论 6.2 *$M \not\models \varphi$当且仅当存在$k \geq 0$和$s \in I$使得$M, s \models_k \neg\varphi$。*

§6.2 CTL公式的不动点表示与模态μ演算

给定一个AP上的Kripke结构$M = \langle S, R, I, L\rangle$。

给定的一个CTL公式p。S的子集$\{s \in S \mid M, s \models p\}$记为$[[p]]$。定义函数$ex : 2^S \to 2^S$如下：

$$ex(A) = \{s \in S \mid \exists s' \in S.((s, s') \in R \wedge s' \in A)\}$$

我们有以下等式：

$[[p]]$	$=$	$\{s \mid p \in L(s)\}$
$[[\neg p]]$	$=$	$S \setminus [[p]]$
$[[p \vee q]]$	$=$	$[[p]] \cup [[q]]$
$[[EXp]]$	$=$	$ex([[p]])$
$[[EGp]]$	$=$	$[[p]] \cap ex([[EGp]])$
$[[E(pUq)]]$	$=$	$[[q]] \cup ([[p]] \cap ex([[E(pUq)]])$

由以上等式知$[[EGp]]$和$[[E(pUq)]]$分别是$\tau_1(Z) = [[p]] \cap ex(Z)$和$\tau_2(Z) = [[q]] \cup ([[p]] \cap ex(Z))$的不动点。根据$\tau_1$和$\tau_2$的定义知$\tau_1$和$\tau_2$有最小和最大不动点。根据CTL语义知$[[EGp]]$是$\tau_1$的最大不动点，$[[E(pUq)]]$是$\tau_2$的最小不动点，即

$$\begin{aligned} [[EGp]] &= \nu Z.([[p]] \cap ex(Z)) \\ [[E(pUq)]] &= \mu Z.([[q]] \cup ([[p]] \cap ex(Z))) \end{aligned}$$

类似地，其它模态算子也可以用不动点刻画。

定义$ax(A) = \{s \in S \mid \forall s' \in S.((s, s') \in R \to s' \in A)\}$。则$[[AXp]] = ax([[p]])$。

为方便书写，我们直接将p, q看成S的子集，时序算子和命题逻辑联接符看成是2^S上的函数。

AFp	$=$	$\mu Z.(p \vee AXZ)$	EFp	$=$	$\mu Z.(p \vee EXZ)$
AGp	$=$	$\nu Z.(p \wedge AXZ)$	EGp	$=$	$\nu Z.(p \wedge EXZ)$
$A(pUq)$	$=$	$\mu Z.(q \vee (p \wedge AXZ))$	$E(pUq)$	$=$	$\mu Z.(q \vee (p \wedge EXZ))$
$A(pRq)$	$=$	$\nu Z.(q \wedge (p \vee AXZ))$	$E(pRq)$	$=$	$\nu Z.(q \wedge (p \vee EXZ))$

命题 6.6 *给定Kripke结构M和CTL公式φ。$M, s \models \varphi$当且仅当$s \in [[\varphi]]$。*

推论 6.3 *给定标号Kripke结构M和CTL公式φ。$M \models \varphi$当且仅当$I \in [[\varphi]]$。*

§6.2.1 模态μ演算

由关于CTL的讨论我们知道CTL公式可以用时序算子AX,EX,命题变量和不动点表示。在这种表示中，命题变量可以出现在AX, EX, μ, ν之后。将这个约束去掉，我们可以得到一个表达能力更强的逻辑。称为模态μ演算或简称为μ演算。给定一个原子命题集合AP，一个变量集合V。用p表示AP中任意命题，X表示V中任意变量。一种简单的μ-演算的公式的集合可由以下语法给出。

$$\phi ::= p \mid X \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \langle . \rangle \phi \mid [.]\phi \mid \mu X.\phi \mid \nu X.\phi$$

其中$\mu X.\phi$和$\nu X.\phi$的ϕ中不受囿的X必须在偶数个¬符号的作用范围之下。

带动作的描述： 对前述简单μ演算做扩充，增加动作的描述，我们可以得到一种能够描述动作的时序关系的时序逻辑。给定一个原子命题集合AP，一个变量集合V，和一个动作集合A。用p表示AP中任意命题，X表示V中任意变量，a表示A中任意动作。μ演算公式的集合由以下语法给出。

$$\phi ::= p \mid X \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid \langle a \rangle \phi \mid [a]\phi \mid \mu X.\phi \mid \nu X.\phi$$

其中$\mu X.\phi$和$\nu X.\phi$的ϕ中不受囿的X必须在偶数个¬符号的作用范围之下。

μ演算公式在双标号迁移系统上的语义解释： 设$M = \langle \Sigma, S, \Delta, I, L \rangle$为原子命题集$AP$上的双标号迁移系统，$e : V \to 2^S$为变量到$S$子集的赋值。$\mu$演算公式的语义如下：

$[[p]]e$	$=$	$\{s \mid p \in L(s)\}$
$[[X]]e$	$=$	$e(X)$
$[[\neg\phi]]e$	$=$	$S \setminus [[\phi]]e$
$[[\phi_1 \wedge \phi_2]]e$	$=$	$[[\phi_1]]e \cap [[\phi_2]]e$
$[[\phi_1 \vee \phi_2]]e$	$=$	$[[\phi_1]]e \cup [[\phi_2]]e$
$[[\langle a \rangle \phi]]e$	$=$	$\{s \mid \exists s'.s \xrightarrow{a} s' \wedge s' \in [[\phi]]e\}$
$[[[a]\phi]]e$	$=$	$\{s \mid \forall s'.s \xrightarrow{a} s' \Rightarrow s' \in [[\phi]]e\}$
$[[\mu X.\phi]]e$	$=$	$\cap\{S' \subseteq S \mid [[\phi]]e[X/S'] \subseteq S'\}$
$[[\nu X.\phi]]e$	$=$	$\cup\{S' \subseteq S \mid S' \subseteq [[\phi]]e[X/S']\}$

所有变量都是受囿变量的公式称为闭公式。闭公式的语义不受e的影响。设M为双标号迁移系统，φ为闭公式。φ在M中的语义可写为$[[\varphi]]$。

定义 6.3 $M \models \varphi$ 当且仅当 $I \subseteq [[\varphi]]$。

可满足性： 设φ为μ演算公式。φ是可满足的，当且仅当存在M使得$M \models \varphi$。

重言式和等价： 设φ为μ演算公式。φ是重言式，记作$\models \varphi$，当且仅当对任意M有$M \models \varphi$。φ等价于ψ，记作$\varphi \equiv \psi$，当且仅当$\models (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$。

模态算子的对偶关系与NNF范式： 逻辑连接符¬只出现在命题前面的公式称为NNF范式。每个μ演算公式等价于一个μ演算的NNF范式。一个μ演算的NNF范式可应用以下对偶关系构造。

$[a]\phi$	$\equiv$	$\neg\langle a\rangle\neg\phi$
$\mu X.\phi$	$\equiv$	$\neg\nu X.\neg\phi(\neg X/X)$

表达能力： μ演算公式$\nu X.(p \wedge [.][.](X))$不能用CTL公式表示。

命题 6.7 *μ演算的表达能力强于CTL。*

可满足性判定问题： 判定μ演算公式是否可满足的问题复杂性为EXPTIME完全。

模型检测问题： 判定双标号迁移系统是否满足μ演算公式的问题复杂性为NP $\cap$ coNP。

§6.2.2 CTL公式到μ演算公式的转换

由于CTL公式不牵涉到动作的描述，可将CTL所描述系统中的动作都归为同一类。用点表示动作，则可用以下规则将CTL公式转换到μ演算公式。

$$
\begin{array}{lcl}
T(p) & = & p \\
T(\neg\varphi) & = & \neg T(\varphi) \\
T(\varphi \vee \psi) & = & T(\varphi) \vee T(\psi) \\
T(EX\varphi) & = & \langle . \rangle T(\varphi) \\
T(E(\varphi U \psi)) & = & \mu Y.(T(\psi) \vee (T(\varphi) \wedge \langle . \rangle Y)) \\
T(EG\varphi) & = & \nu Y.(T(\varphi) \wedge \langle . \rangle Y)
\end{array}
$$

命题 6.8 *给定AP上的标号$Kripke$模型$M = \langle S, R, I, L\rangle$。定义双标号迁移系统$M' = \langle \Sigma, S, \Delta, I, L\rangle$其中$\Sigma = \{.\}$和$\Delta = \{(s, a, s') \mid (s, s') \in R, a \in \Sigma\}$。设$\varphi$为$CTL$公式。$M \models \varphi$当且仅当$M' \models T(\varphi)$。*

§6.2.3 公平标号Kripke结构下的CTL语义

符号集合AP上的CTL公式可在AP上的公平标号Kripke结构上解释。给定公平标号Kripke结构$M = \langle S, R, I, L, F\rangle$且$F = \{f_1, .., f_k\}$。

语义 状态$s \in S$满足CTL公式φ，记为$M, s \models \varphi$，其语义与CTL公式在标号Kripke结构上解释的解释类似，仅将存在s起点的无穷路径换成存在s起点的公平路径，对所有s起点的无穷路径换成对所有s起点的公平路径。

不动点表示 为方便区分，用EX_f, EU_f, EG_f表示公平标号Kripke结构上的CTL性质的相应算子，依然用EX, EU, EG表示去掉公平约束的标号Kripke结构上的CTL性质。用$fair$表示公平状态集合。将公式理解为状态集合。我们有以下等式。

$fair$	$=$	$\nu Z.(\bigwedge_{i=1}^{k} EX(EF(Z \wedge f_i)))$
$EX_f p$	$=$	$EX(p \wedge fair)$
$E(pU_f q)$	$=$	$E(pU(q \wedge fair))$
$EG_f p$	$=$	$\nu Z.(p \wedge \bigwedge_{i=1}^{k} EX(E(pU(Z \wedge f_i))))$

设φ为时序算子在$\{EX_f, EU_f, EG_f\}$中的CTL公式。

命题 6.9 *$M \models \varphi$当且仅当$I \subseteq \varphi$。*

§6.3 计算树逻辑CTL*

由于CTL中描述分枝情况和描述状态的前后关系的算子成对出现，在一定程度上限制了CTL的表达能力。我们可以将其拆开使用。这个逻辑记作CTL*。给定一个原子命题集合AP。用p表示AP中任意命题。CTL*公式的集合由以下语法给出。

$$\phi ::= p \mid \neg\phi \mid \phi \wedge \phi \mid \phi \vee \phi \mid X\phi \mid F\phi \mid G\phi \mid \phi\, U\, \phi \mid \phi\, R\, \phi \mid A\phi \mid E\phi$$

我们可以将CTL*中的公式分为状态公式和路径公式。

若$p \in AP$，	则p是状态公式
若φ和ψ是状态公式，	则$\neg\varphi, \varphi \vee \psi, \varphi \wedge \psi$是状态公式
若φ是路径公式，	则$E\varphi$和$A\varphi$是状态公式
若φ是状态公式，	则φ是路径公式
若φ和ψ是路径公式，	则$\neg\varphi, \varphi \vee \psi, \varphi \wedge \psi, X\varphi, F\varphi, G\varphi, \varphi U\psi, \varphi R\psi$是路径公式

模型： AP上的CTL*公式在AP上的标号Kripke结构上解释。

CTL*语义： 设$M = \langle S, R, I, L\rangle$是$AP$上的Kripke结构。CTL*公式的语义如下：

$M, s \models p$	若$p \in AP$且$p \in L(s)$
$M, s \models \neg\varphi$	若$M, s \not\models \varphi$
$M, s \models \varphi \vee \psi$	若$M, s \models \varphi$或$M, s \models \psi$
$M, s \models \varphi \wedge \psi$	若$M, s \models \varphi$且$M, s \models \psi$
$M, s \models A\varphi$	若对于所有M中s为起点的路径π：$M, \pi \models \varphi$
$M, s \models E\varphi$	若存在M中s为起点的路径π：$M, \pi \models \varphi$
$M, \pi \models p$	若$p \in AP$且$M, \pi_0 \models p$
$M, \pi \models A\varphi$	若$M, \pi_0 \models A\varphi$
$M, \pi \models E\varphi$	若$M, \pi_0 \models E\varphi$
$M, \pi \models \neg\varphi$	若$M, \pi \not\models \varphi$
$M, \pi \models \varphi \vee \psi$	若$M, \pi \models \varphi$或$M, \pi \models \psi$
$M, \pi \models \varphi \wedge \psi$	若$M, \pi \models \varphi$且$M, \pi \models \psi$
$M, \pi \models X\varphi$	若$M, \pi^1 \models \varphi$
$M, \pi \models G\psi$	若$\forall i \geq 0, M, \pi^i \models \psi$
$M, \pi \models F\varphi$	若$\exists i \geq 0, M, \pi^i \models \varphi$
$M, \pi \models \varphi U\psi$	若$\exists i \geq 0, M, \pi^i \models \psi$且$\forall 0 \leq j < i, M, \pi^j \models \varphi$
$M, \pi \models \varphi R\psi$	若$\forall i \geq k$,若$\forall 0 \leq j < i, M, \pi^j \not\models \varphi$则$M, \pi^i \models \psi$

定义 6.4 *设φ为CTL*状态公式，M为Kripke结构。$M \models \varphi$当且仅当对所有$s \in I$，$M, s \models \varphi$。*

可满足公式： 设φ为CTL*状态公式。φ是可满足的，当且仅当存在M使得$M \models \varphi$。

重言式和等价： 设φ为CTL*状态公式。φ是重言式，记作$\models \varphi$，当且仅当对任意M有$M \models \varphi$。φ等价于ψ，记作$\varphi \equiv \psi$，当且仅当$\models (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$。

表达能力： PLTL和CTL是CTL*的子集。设PLTL、CTL和CTL*都在Kripke结构上解释。一个PLTL公式φ等价于一个CTL*公式$A\varphi$。这样PLTL公式就可以看成是状态公式。在这样的解释下，我们可以比较PLTL、CTL和CTL*的状态公式。我们有以下结论。

CTL公式$AGEFp$不能用PLTL表示。
PLTL公式$F(p \wedge Xp)$不能用CTL表示。
CTL*公式$E(GFp)$不能用CTL表示，不能用PLTL表示。

命题 6.10 *PLTL和CTL的表达能力存在互补关系且CTL*的表达能力强于PLTL和CTL的并集。*

可满足性判定问题： 判定CTL*公式是否可满足的问题复杂性为双指数时间完全。

模型检测问题： 判定标号Kripke模型是否满足CTL*公式的问题复杂性为PSPACE完全。

§6.4 例子

例 6.1 设$AP = \{p_0, p_1, p_2, p_3, p_4, q_0, q_1, q_2\}$。定义$S, R, I, L$如下。

$S = \{s_0, s_1, s_2, s_3, s_4, s_5\}$。

$R = \{(s_0, s_1), (s_0, s_2), (s_1, s_3), (s_1, s_5), (s_2, s_5), (s_2, s_4), (s_3, s_4), (s_3, s_5), (s_4, s_5), (s_5, s_0)\}$。

$I = \{s_0\}$。

L定义如下。

$L(s_0) = \{p_0, q_0\}$

$L(s_1) = \{p_1, q_0\}$

$L(s_2) = L(s_3) = \{p_2, q_0\}$

$L(s_4) = \{p_4, q_1\}$

$L(s_5) = \{p_3, q_2\}$

则$K = (S, R, I, L)$为标号*Kripke*模型。

（*1*）对*CTL*性质$\varphi_0 = E(q_0 U q_2)$和*CTL*性质$\varphi_1 = AG(q_0 \vee q_2)$，我们有如下结论。

$$
\begin{array}{cccc}
K \not\models_0 \varphi_0 & K \not\models_0 \neg\varphi_0 & K \not\models_0 \varphi_1 & K \not\models_0 \neg\varphi_1 \\
K \not\models_1 \varphi_0 & K \not\models_1 \neg\varphi_0 & K \not\models_1 \varphi_1 & K \not\models_1 \neg\varphi_1 \\
K \models_2 \varphi_0 & K \not\models_2 \neg\varphi_0 & K \not\models_2 \varphi_1 & K \models_2 \neg\varphi_1
\end{array}
$$

因而模型满足φ_0且可以确定模型满足$E(q_0 U q_2)$的最小的界为$k = 2$，模型不满足φ_1且可以确定模型不满足$AG(q_0 \vee q_2)$的最小的界同样为$k = 2$。

例 6.2 设AP和$K = (S, R, I, L)$如例*6.1*中所定义。

（*1*）我们有$E(q_0Uq_2) = \mu Z.(q_2 \vee (q_0 \wedge EXZ))$。根据不动点算法，$[[E(q_0Uq_2)]]$的计算过程如下。

$$\begin{array}{lcll} S_0 & = & false & = \{\} \\ S_1 & = & q_2 & = \{s_5\} \\ S_2 & = & \{s_5\} \cup (\{s_0, s_1, s_2, s_3\} \cap \{s_1, s_2, s_3, s_4\} & = \{s_1, s_2, s_3, s_5\} \\ S_3 & = & \{s_5\} \cup (\{s_0, s_1, s_2, s_3\} \cap \{s_0, s_1, s_2, s_3, s_4\} & = \{s_0, s_1, s_2, s_3, s_5\} \\ S_4 & = & \{s_5\} \cup (\{s_0, s_1, s_2, s_3\} \cap \{s_0, s_1, s_2, s_3, s_4, s_5\} & = S_3 \end{array}$$

因而$[[E(q_0Uq_2)]] = \{s_0, s_1, s_2, s_3, s_5\}$。

（*2*）我们有$AG(q_0 \vee q_2) = \nu Z.((q_0 \vee q_2) \wedge AXZ))$。根据不动点算法，$[[AG(q_0 \vee q_2)]]$的计算过程如下。

$$\begin{array}{lcll} S_0 & = & true & = \{s_0, s_1, s_2, s_3, s_4, s_5\} \\ S_1 & = & q_0 \vee q_2 & = \{s_0, s_1, s_2, s_3, s_5\} \\ S_2 & = & \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_0, s_1, s_4, s_5\} & = \{s_0, s_1, s_5\} \\ S_3 & = & \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_4, s_5\} & = \{s_5\} \\ S_4 & = & \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_4\} & = \{\} \\ S_5 & = & \{s_0, s_1, s_2, s_3, s_5\} \cap \{\} & = S_4 \end{array}$$

因而$[[AG(q_0 \vee q_2)]] = \{\}$。

（*3*）由以上计算知模型满足$E(q_0Uq_2)$且模型不满足$AG(q_0 \vee q_2)$。

例 6.3 设AP和S, R, I, L如例*6.1*中所定义。设$\Sigma = \{1, 2, qc, qq\}$。定义$\Delta$为以下集合的并集。

$$\{(s_0, 1, s_1), (s_0, 2, s_2)\}$$
$$\{(s_1, 1, s_3), (s_1, 2, s_5)\}$$
$$\{(s_2, 1, s_5), (s_2, 2, s_4)\}$$
$$\{(s_3, 2, s_4), (s_3, 1, s_5)\}$$
$$\{(s_4, qq, s_5), (s_5, qc, s_0)\}$$

则$K' = (\Sigma, S, \Delta, I, L)$为双标号迁移系统。

（*1*）$\mu Z.(q_2 \vee \langle 1 \rangle Z)$的计算过程如下。

$$\begin{array}{lcll} S_0 & = & false & = \{\} \\ S_1 & = & q_2 \vee \langle 1 \rangle \{\} & = \{s_5\} \\ S_2 & = & \{s_5\} \cup \{s_2, s_3\} & = \{s_2, s_3, s_5\} \\ S_3 & = & \{s_5\} \cup \{s_1, s_2, s_3\} & = \{s_1, s_2, s_3, s_5\} \\ S_4 & = & \{s_5\} \cup \{s_0, s_1, s_2, s_3\} & = \{s_0, s_1, s_2, s_3, s_5\} \\ S_5 & = & \{s_5\} \cup \{s_0, s_1, s_2, s_3\} & = S_4 \end{array}$$

因而$\mu Z.(q_2 \vee \langle 1 \rangle Z) = \{s_0, s_1, s_2, s_3, s_5\}$。

（2）$\nu Z.(\neg q_2 \wedge [1]Z)$的计算过程如下。

$$\begin{array}{lcll} S_0 & = & true & = \{s_0, s_1, s_2, s_3, s_4, s_5\} \\ S_1 & = & \neg q_2 \wedge [1]\{s_0, s_1, s_2, s_3, s_4, s_5\} & = \{s_0, s_1, s_2, s_3, s_4\} \\ S_2 & = & \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_0, s_1, s_4, s_5\} & = \{s_0, s_1, s_4\} \\ S_3 & = & \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_0, s_4, s_5\} & = \{s_0, s_4\} \\ S_4 & = & \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_4, s_5\} & = \{s_4\} \\ S_5 & = & \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_4, s_5\} & = S_4 \end{array}$$

因而$\nu Z.(\neg q_2 \wedge [1]Z) = \{s_4\}$。

由ν和μ的对偶关系亦可知$\nu Z.(\neg q_2 \wedge [1]Z) = \neg\mu Z.(q_2 \vee \langle 1\rangle Z) = \{s_4\}$。

（3）$\mu Z.(\neg q_2 \vee [1]Z)$的计算过程如下。

$$\begin{array}{lcll} S_0 & = & false & = \{\} \\ S_1 & = & q_2 \vee [1]\{\} & = \{s_4, s_5\} \\ S_2 & = & \{s_5\} \cup \{s_2, s_3, s_4, s_5\} & = \{s_2, s_3, s_4, s_5\} \\ S_3 & = & \{s_5\} \cup \{s_1, s_2, s_3, s_4, s_5\} & = \{s_1, s_2, s_3, s_4, s_5\} \\ S_4 & = & \{s_5\} \cup \{s_0, s_1, s_2, s_3, s_4, s_5\} & = \{s_0, s_1, s_2, s_3, s_4, s_5\} \\ S_5 & = & \{s_5\} \cup \{s_0, s_1, s_2, s_3, s_4, s_5\} & = S_4 \end{array}$$

因而$\mu Z.(\neg q_2 \vee [1]Z) = \{s_0, s_1, s_2, s_3, s_4, s_5\}$。

（4）由以上计算知模型满足$\mu Z.(q_2 \vee \langle 1\rangle Z)$和$\mu Z.(\neg q_2 \vee [1]Z)$且模型不满足$\nu Z.(\neg q_2 \wedge [1]Z)$。

例 6.4 （1）CTL公式$AGEFp$不能用LTL公式表示。

证：定义$M = \langle S, R, I, L\rangle$其中

$$\begin{aligned} &S = \{s_0, s_1\}, \\ &R = \{(s_0, s_0), (s_0, s_1), (s_1, s_1)\}, \\ &I = \{s_0\}, \\ &L(s_0) = \{\}, L(s_1) = \{p\}。 \end{aligned}$$

定义$M' = \langle S', R', I', L'\rangle$其中$S' = \{s_0\}$，$R' = \{(s_0, s_0)\}$，$I' = \{s_0\}$，$L'(s_0) = \{\}$。

我们有$M \models AGEFp$且$M' \not\models AGEFp$。

设$AGEFp$能用LTL公式φ表示。则$M \models \varphi$且$M' \not\models \varphi$。

根据语义，由于M'的计算是M的计算的一个子集，我们有$M \models \varphi$蕴含$M' \models \varphi$，与$M' \not\models \varphi$矛盾。

因而$AGEFp$不能用LTL公式表示。

（2）LTL公式$F(p \wedge Xp)$不能用CTL公式表示。

证：定义$M_1, N_1, M_{i+}, N_{i+1}$如下。

$M_1 = \langle S_1, R_1, I_1, L_1\rangle$其中
$S_1 = \{s_2, s_1, s_0\}$,
$R_1 = \{(s_2, s_1), (s_1, s_0), (s_0, s_0)\}$,
$I_1 = \{s_2\}$,
$L_1(s_2) = L_1(s_1) = \{p\}$且$L_1(s_0) = \{\}$。
$N_1 = \langle S'_1, R'_1, I'_1, L'_1\rangle$其中
$S'_1 = \{s'_2, s'_1\}$,
$R'_1 = \{(s'_2, s'_1), (s'_1, s'_1)\}$,
$I'_1 = \{s'_2\}$,
$L'_1(s'_2) = \{p\}$且$L'_1(s'_1) = \{\}$。
$M_{i+1} = \langle S_{i+1}, R_{i+1}, I_{i+1}, L_{i+1}\rangle$其中
$S_{i+1} = S_i \cup S'_i \cup \{s_{2i+2}, s_{2i+1}\}$,
$R_{i+1} = R_i \cup R'_i \cup \{(s_{2i+2}, s_{i+1}), (s_{2i+1}, s_{2i}), (s_{2i+2}, s_{2i}), (s_{2i+2}, s'_{2i})\}$,
$I_{i+1} = \{s_{2i+2}\}$,
$L_{i+1} = L_i \cup L'_i \cup \{(s_{2i+2}, \{p\}), (s_{2i+1}, \{\})\}$。
$N_{i+1} = \langle S'_{i+1}, R'_{i+1}, I'_{i+1}, L'_{i+1}\rangle$其中
$S'_{i+1} = S_i \cup S'_i \cup \{s'_{2i+2}, s'_{2i+1}\}$,
$R'_{i+1} = R_i \cup R'_i \cup \{(s'_{2i+2}, s'_{i+1}), (s'_{2i+1}, s'_{2i}), (s'_{2i+2}, s'_{2i}), (s'_{2i+2}, s_{2i})\}$,
$I'_{i+1} = \{s'_{2i+2}\}$,
$L'_{i+1} = L_i \cup L'_i \cup \{(s'_{2i+2}, \{p\}), (s'_{2i+1}, \{\})\}$。

我们有$M_{i+1} \models F(p \wedge Xp)$且$N_{i+1} \not\models F(p \wedge Xp)$。
考虑CTL算子EX, EG, EU。设φ为仅用$\{EX, EG, EU\}$算子和命题逻辑连接符构造的CTL公式。
若φ的长度为i，则对所有$k \geq i$有$M_k \models \varphi$当且仅当$N_k \models \varphi$。
因而$F(p \wedge Xp)$不能用CTL公式表示。

§6.5 练习

1. 分别用CTL语义和推理系统证明$AG(p \to AXp) \to (p \to AGp)$。

2. 设K如例6.1中所定义。用限界语义验证该模型是否满足$A(q_0 U q_1)$和$EG(q_0 \vee q_1)$并讨论最小的可以确定模型是否满足以上公式的界。

3. 设K如例6.1中所定义。用不动点算法计算$[[A(q_0 U q_1)]]$和$[[EG(q_0 \vee q_1)]]$并讨论模型是否满足$A(q_0 U q_1)$和$EG(q_0 \vee q_1)$。

4. 设K'如例6.3中所定义。用不动点算法计算$\mu Z.(q_1 \vee \langle 1\rangle Z)$和$\mu Z.(q_1 \vee \langle 2\rangle Z)$并讨论模型是否满足$\mu Z.(q_1 \vee \langle 1\rangle Z)$和$\mu Z.(q_1 \vee \langle 2\rangle Z)$。

5. 讨论满足公式$A((p \vee q)Ur), A((pUr) \vee (qUr))$与$A(pUr) \vee A(qUr)$的模型的特点、指出这些公式之间的强弱关系。