§3 程序逻辑

§3.1 线性时序逻辑 (LTL)

例子：证明 $(Op) \equiv \neg(O\neg p)$

证明

$M, \pi \models Op$ 成立
即 $M, \pi^1 \models p$ 成立
即 $M, \pi^1 \models \neg p$ 不成立
即 $M, \pi \models O(\neg p)$ 不成立
即 $M, \pi \not\models O(\neg p)$ 成立
即 $M, \pi \models \neg O(\neg p)$ 成立

例子：证明 $pRq \equiv (qU(q \wedge p)) \vee \Box q$

证明

$M, \pi \models (qU(q \wedge p)) \vee \Box q$
即 $\forall i \geq 0, M, \pi^i \models q$ (1)
或 $\exists i \geq 0, M, \pi^i \models p$ 且 $\forall 0 \leq j \leq i, M, \pi^j \models q$ (2)

$M, \pi \models pRq$
即 $\forall i \geq 0, M, \pi^i \models q$ 或 $\exists 0 \leq j < i, M, \pi^j \models p$ 成立

方向 $\rightarrow$

要证任意对 i_0,
(a) $M, \pi^{i_0} \models q$ 或
(b) $\exists 0 \leq j < i_0, M, \pi^j \models p$ 成立
由条件 (1)(2) 要么 (1) 则 (a) 成立,
要么 (2) 则
有最小 i 满足 $M, \pi^i \models p$ 且 $\forall 0 \leq j \leq i, M, \pi^j \models q$
即 $M, \pi^{i_1} \models p$ 且 $\forall 0 \leq j \leq i_1, M, \pi^j \models q$
若 $\pi^{i_0} \models q$ 则 (a) 成立。
若 $\pi^{i_0} \not\models q$ 则 $i_1 < i_0$,
因 $M, \pi^{i_1} \models p$ ，因此 $\exists 0 \leq j < i_0, \pi^j \models p$ 即 (b) 成立

方向 $\leftarrow$

有 $\forall i \geq 0, M, \pi^i \models q$ 或 $\exists 0 \leq j < i, M, \pi^j \models p$
要证
$\forall i \geq 0, M, \pi^i \models q$ (1)
或 $\exists i \geq 0, M, \pi^i \models p$ 且 $\forall 0 \leq j \leq i, M, \pi^j \models q$ (2)

若 $\forall i \geq 0, M, \pi^i \models q$ 则 (1) 成立
否则找最小 i_0 不满足 $\forall i \geq 0, M, \pi^i \models q$
则 $M, \pi^{i_0} \not\models q$ 且 $\forall 0 \leq j < i_0, M, \pi^j \models q$
还需要 $M, \pi^{i_0 - 1} \models p$ 或任意 $i < i_0$ 使得 $M, \pi^i \models p$
根据前提， $\exists 0 \leq j < i_0, M, \pi^j \models p$
所以 (2) 成立。

例子：证明 $(p \wedge \Box Op) \to \Box p$

证明

$$
\begin{aligned}
& Op \to (p \to Op) \\
& \Box(Op \to (p \to Op)) \\
& \Box Op \to \Box(p \to Op) \\
& \Box(p \to Op) \\
& p \to \Box p \\
& \Box p
\end{aligned}
$$

例子：证明 $(Op \to Oq) \to O(p \to q)$

证明

$$
\begin{aligned}
& O(\neg p \to p \to q) \to O(\neg p) \to O(p \to q) \\
& O(\neg p) \to O(p \to q) \\
& \neg O(p) \to O(p \to q) \\
& O(q \to p \to q) \to O(q) \to O(p \to q) \\
& O(q) \to O(p \to q) \\
& (Op \to Oq) \to O(p \to q)
\end{aligned}
$$

§3.2 计算树逻辑 CTL

例子：证明 $AFp = \mu Z(p \vee AXZ)$

证明

$$
\begin{aligned}
AFp = \quad & p \vee AXAFp \\
AFp = \quad & \neg EG\neg p = \\
& \neg(\nu Z.(\neg p \wedge EXZ)) = \\
& \mu Z.\neg(\neg p \wedge EX\neg Z) = \\
& \mu Z.(p \vee AXZ)
\end{aligned}
$$

$$
\begin{aligned}
& \mu Z.\tau(Z) = \cap\{Z \mid \tau(Z) \subseteq Z\} \\
& \mu Z.\neg\tau(\neg Z) = \cap\{Z \mid \neg\tau(\neg Z) \subseteq Z\} \\
& \mu Z.\neg\tau(\neg Z) = \cap\{Z \mid \tau(\neg Z) \supseteq \neg Z\} \\
& \neg\mu Z.\neg\tau(\neg Z) = S \setminus \cap\{Z \mid \tau(\neg Z) \supseteq \neg Z\} \\
& \neg\mu Z.\neg\tau(\neg Z) = \cup\{S \setminus Z \mid \tau(\neg Z) \supseteq \neg Z\} \\
& \neg\mu Z.\neg\tau(\neg Z) = \cup\{Z \mid \tau(Z) \supseteq Z\} \\
& \nu Z.\tau(Z) = \cup\{Z \mid \tau(Z) \supseteq Z\}
\end{aligned}
$$

例子：简化自动售茶机

自动售茶机的模型 $\langle S, \Delta, I, L\rangle$

- $S = \{s_0, s_1, s_2, s_3, s_4, s_5\}$
- $\Delta = \{(s_0, s_1), (s_0, s_2), (s_1, s_3), (s_1, s_5),$
  $(s_2, s_5), (s_2, s_4), (s_3, s_5), (s_3, s_4),$
  $(s_4, s_5), (s_5, s_0)\}$
- $I = \{s_0\}$
- L 定义如下：

$L(s_0) = \{p_0, q_0\}$
$L(s_1) = \{p_1, q_0\}$
$L(s_2) = \{p_2, q_0\}$
$L(s_3) = \{p_2, q_0\}$
$L(s_4) = \{p_4, q_1\}$
$L(s_5) = \{p_3, q_2\}$

（ 1 ）计算

$$E(q_0 U q_2) = \mu Z.(q_2 \vee (q_0 \wedge EXZ))$$

$S_0 = false$
$S_1 = q_2 = \{s_5\}$
$S_2 = \{s_5\} \cup (\{s_0, s_1, s_2, s_3\} \cap \{s_1, s_2, s_3, s_4\}) = \{s_1, s_2, s_3, s_5\}$
$S_3 = \{s_1, s_2, s_3, s_5\} \cup (\{s_0, s_1, s_2, s_3\} \cap \{s_0, s_1, s_2, s_3, s_4\}) = \{s_0, s_1, s_2, s_3, s_5\}$
$S_4 = \{s_0, s_1, s_2, s_3, s_5\} \cup (\{s_0, s_1, s_2, s_3\} \cap \{s_0, s_1, s_2, s_3, s_4, s_5\}) = \{s_0, s_1, s_2, s_3, s_5\}$

因此该模型满足这个公式。

（ 2 ）计算

$$AG(q_0 \vee q_2) = \nu Z.((q_0 \vee q_2) \wedge AXZ)$$

$S_0 = true$
$S_1 = q_0 \vee q_2 = \{s_0, s_1, s_2, s_3, s_5\}$
$S_2 = \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_0, s_1, s_4, s_5\} = \{s_0, s_1, s_5\}$
$S_3 = \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_4, s_5\} = \{s_5\}$
$S_4 = \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_4\} = \{\}$

因此该模型不满足这个公式。

§3.3 计算树逻辑 CTL*

例子： $E(GFp)$ 不同于 $EGEFp$ 。

定义以下结构：

- $S = \{s_0, s_1, s_2\}$
- $\Delta = \{(s_0, s_0), (s_0, s_1), (s_1, s_2), (s_2, s_2)\}$
- $I = \{s_0\}$
- L 定义如下：

$L(s_0) = \{p\}$
$L(s_1) = \{\}$
$L(s_2) = \{p\}$

该结构满足 $AFGp$ 而不满足 $AFAGp$ ，因此这两个公式是不一样的。

因此他们的否定也是不一样的。

§3.4 μ- 演算

例子：自动售茶机

$\mu X.(q_2 \vee \langle 1 \rangle X)$ 表示：

对于非确定型系统,

如果你一直投 1 分钱，

存在到达一个下一动作为取茶的状态（即满足 q_2 的状态）的可能性。

对于确定型系统，

如果你一直投 1 分钱，

则一定到达一个下一动作为取茶的状态。

$[[q_2]] = \{s_5\}$

$S_0 = \{s_5\} \cup [[\langle 1\rangle\{\}]] = \{s_5\}$
$S_1 = \{s_5\} \cup [[\langle 1\rangle\{s_5\}]] = \{s_5\} \cup \{s_2, s_3\}$
$S_2 = \{s_5\} \cup [[\langle 1\rangle\{s_2, s_3, s_5\}]] = \{s_5\} \cup \{s_1, s_2, s_3\}$
$S_3 = \{s_5\} \cup [[\langle 1\rangle\{s_1, s_2, s_3, s_5\}]] = \{s_5\} \cup \{s_0, s_1, s_2, s_3\}$
$S_4 = \{s_5\} \cup [[\langle 1\rangle\{s_0, s_1, s_2, s_3, s_5\}]] = \{s_5\} \cup \{s_0, s_1, s_2, s_3\}$

例子

$\nu X.(\neg q_2 \wedge \neg\langle 1\rangle\neg X)$
$S_0 = \{s_0, s_1, s_2, s_3, s_4\} \cap (S \setminus [[\langle 1\rangle\{\}]]) = \{s_0, s_1, s_2, s_3, s_4\}$
$S_1 = \{s_0, s_1, s_2, s_3, s_4\} \cap (S \setminus [[\langle 1\rangle\{s_5\}]]) = \{s_0, s_1, s_4\}$
$S_2 = \{s_0, s_1, s_2, s_3, s_4\} \cap (S \setminus [[\langle 1\rangle\{s_2, s_3, s_5\}]]) = \{s_0, s_4\}$
$S_3 = \{s_0, s_1, s_2, s_3, s_4\} \cap (S \setminus [[\langle 1\rangle\{s_1, s_2, s_3, s_5\}]]) = \{s_4\}$
$S_4 = \{s_0, s_1, s_2, s_3, s_4\} \cap (S \setminus [[\langle 1\rangle\{s_0, s_1, s_2, s_3, s_5\}]]) = \{s_4\}$

例子

$\nu X.(\neg q_2 \wedge [1]X)$

$$
\begin{aligned}
S_0 &= \{s_0, s_1, s_2, s_3, s_4\} \cap [[[1]S]] \\
&= \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_0, s_1, s_2, s_3, s_4, s_5\} = \{s_0, s_1, s_2, s_3, s_4\} \\
S_1 &= \{s_0, s_1, s_2, s_3, s_4\} \cap [[[1]\{s_0, s_1, s_2, s_3, s_4\}]] \\
&= \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_0, s_1, s_4, s_5\} = \{s_0, s_1, s_4\} \\
S_2 &= \{s_0, s_1, s_2, s_3, s_4\} \cap [[[1]\{s_0, s_1, s_4\}]] \\
&= \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_0, s_4, s_5\} = \{s_0, s_4\} \\
S_3 &= \{s_0, s_1, s_2, s_3, s_4\} \cap [[[1]\{s_0, s_4\}]] \\
&= \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_4, s_5\} = \{s_4\} \\
S_4 &= \{s_0, s_1, s_2, s_3, s_4\} \cap [[[1]\{s_4\}]] \\
&= \{s_0, s_1, s_2, s_3, s_4\} \cap \{s_4, s_5\} = \{s_4\}
\end{aligned}
$$

例子

$\mu X.(q_2 \vee [1]X)$

如果你一直投 1 分钱，

则一定到达一个下一动作为取茶的状态。

（但是可能有没法投一分钱的时候）。

$S_0 = \{s_5\} \cup [[[1]\{\}]] = \{s_5\} \cup \{s_4, s_5\}$
$S_1 = \{s_5\} \cup [[[1]\{s_4, s_5\}]] = \{s_5\} \cup \{s_1, s_2, s_3, s_4, s_5\}$
$S_2 = \{s_5\} \cup [[[1]\{s_1, s_2, s_3, s_4, s_5\}]] = \{s_5\} \cup \{s_0, s_1, s_2, s_3, s_4, s_5\}$