§4　推理验证

§4.1　一阶迁移系统的推理

§4.2　流程图程序的推理

最弱前断言和最强后断言

1. (1a) T 对于 φ 和 ψ 是部分正确的。
   (1b) T 对于 φ' 和 ψ 是部分正确的，则 $\varphi' \to \varphi$ 。
2. (2a) T 对于 φ 和 ψ 是完全正确的。
   (2b) T 对于 φ' 和 ψ 是完全正确的，则 $\varphi' \to \varphi$ 。
3. (3a) T 对于 φ 和 ψ 是部分正确的。
   (3b) T 对于 φ 和 ψ' 是部分正确的，则 $\psi \to \psi'$ 。

证明：

(1)

条件：$\varphi(\sigma) \leftrightarrow (M_I(T)(\sigma)\uparrow \vee (M_I(T)(\sigma)\downarrow \wedge \psi(M_I(T)(\sigma))))$

(1a) T 对于 φ 和 ψ 是部分正确的：

由条件 (1) 有

$\varphi(\sigma) \to (M_I(T)(\sigma)\uparrow \vee (M_I(T)(\sigma)\downarrow \wedge \psi(M_I(T)(\sigma))))$

因此

$\varphi(\sigma) \wedge M_I(T)(\sigma)\downarrow \to \psi(M_I(T)(\sigma))$

(1b)

T 对于 φ' 和 ψ 是部分正确的则 $\varphi' \to \varphi$ ：

前提即 $\varphi'(\sigma) \wedge (M_I(T)(\sigma)\downarrow \to \psi(M_I(T)(\sigma))$

即 $\varphi'(\sigma) \to (M_I(T)(\sigma)\uparrow \vee (M_I(T)(\sigma)\downarrow \wedge \psi(M_I(T)(\sigma))))$

由条件 (1) 即 $\varphi'(\sigma) \to \varphi(\sigma)$

(2)

条件：　$\varphi(\sigma) \leftrightarrow (M_I(T)(\sigma)\downarrow \wedge \psi(M_I(T)(\sigma))))$

(2a) T 对于 φ 和 ψ 是完全正确的：

由条件 (2) 就有

$\varphi(\sigma) \to (M_I(T)(\sigma)\downarrow \wedge \psi(M_I(T)(\sigma))))$

(2b) T 对于 φ' 和 ψ 是完全正确的，则 $\varphi' \to \varphi$ ：

前提即 $\varphi'(\sigma) \to (M_I(T)(\sigma)\downarrow \wedge \psi(M_I(T)(\sigma))))$

由条件 (2) 即 $\varphi'(\sigma) \to \varphi(\sigma)$

(3)

条件：　$\psi(\sigma') \leftrightarrow \exists \sigma''.(\varphi(\sigma'') \wedge M_I(T)(\sigma'') = \sigma')$

(3a) T 对于 φ 和 ψ 是部分正确的：

要证 $\varphi(\sigma) \wedge M_I(T)(\sigma)\downarrow \to \psi(M_I(T)(\sigma))$

即 $\varphi(\sigma) \wedge M_I(T)(\sigma) = \sigma' \to \psi(\sigma')$

由条件 (3) 即

$\varphi(\sigma) \wedge M_I(T)(\sigma) = \sigma' \to \exists \sigma''.(\varphi(\sigma'') \wedge M_I(T)(\sigma'') = \sigma')$

显然成立。

(3b) T 对于 φ 和 ψ' 是部分正确的，则 $\psi \to \psi'$ ：

前提即 $\varphi(\sigma) \wedge (M_I(T)(\sigma)\downarrow \to \psi'(M_I(T)(\sigma))$

即 $\varphi(\sigma) \wedge M_I(T)(\sigma) = \sigma' \to \psi'(\sigma')$

又由条件 (3) 有 $\psi(\sigma') \to \exists \sigma''.(\varphi(\sigma'') \wedge M_I(T)(\sigma'') = \sigma')$

因此 $\psi(\sigma') \to \psi'(\sigma')$

§4.2.1 基于路径的推理

Proposition 4.1 $I(wlp(\alpha, q))$ 是路径 α 和 q 的最弱宽松前断言。

要证明

$$I(wlp(\alpha,q))(\sigma) = true \leftrightarrow M_I(\alpha)(\sigma)\uparrow \vee (M_I(\alpha)(\sigma)\downarrow \wedge I(q)(M_I(\alpha)(\sigma))$$

设 $\alpha = (l_0, l_1, ..., l_n)$ 为一路径。

(1) $n = 0$.

(2) $n = 1$.
(2a) l_0: $(v_1, v_2, ..., v_n) := (e_1, e_2, ..., e_n)$ goto l_1

$$wlp(\alpha, q) = q[v_1/e_1]\cdots[v_n/e_n].$$

$$M_I(\alpha)(\sigma) = \sigma[v_1/e_1]\cdots[v_n/e_n]$$

(2b) l_0: if (b) goto l else goto l' ,
(2b1) $l = l_1$

$$wlp(\alpha, q) = b \rightarrow q$$

(a) $I(b)(\sigma) = true$

$$M_I(\alpha)(\sigma) = \sigma$$

(b) $I(b)(\sigma) = false$
(2b2) $l' = l_1$

$$wlp(\alpha, q) = \neg b \rightarrow q$$

(a) $I(b)(\sigma) = true$
(b) $I(b)(\sigma) = false$

$$M_I(\alpha)(\sigma) = \sigma$$

(3) $\alpha_0 = (l_0, l_1)$, $\alpha_1 = (l_1, ..., l_k)$ 。
$wlp(\alpha, q) = wlp(\alpha_0, wlp(\alpha_1, q))$
要证

$$I(wlp(\alpha_0, wlp(\alpha_1, q)))(\sigma) = true \leftrightarrow M_I(\alpha)(\sigma)\uparrow \vee (M_I(\alpha)(\sigma)\downarrow \wedge I(q)(M_I(\alpha)(\sigma))$$

有

$$I(wlp(\alpha_0, wlp(\alpha_1, q)))(\sigma) = true \leftrightarrow M_I(\alpha_0)(\sigma)\uparrow \vee (M_I(\alpha_0)(\sigma)\downarrow \wedge I(wlp(\alpha_1, q))(M_I(\alpha_0)(\sigma))$$

(1) $M_I(\alpha_0)(\sigma)\uparrow$ 则两个右边等价。
(2) $M_I(\alpha_0)(\sigma)\downarrow$ 要证

$$M_I(\alpha)(\sigma)\uparrow \vee (M_I(\alpha)(\sigma)\downarrow \wedge I(q)(M_I(\alpha)(\sigma)) \leftrightarrow I(wlp(\alpha_1, q))(M_I(\alpha_0)(\sigma))$$

即

$$M_I(\alpha)(\sigma)\uparrow \vee (M_I(\alpha)(\sigma)\downarrow \wedge I(q)(M_I(\alpha)(\sigma))$$

$\leftrightarrow$

$$(M_I(\alpha_1)(M_I(\alpha_0)(\sigma))\uparrow \vee (M_I(\alpha_1)(M_I(\alpha_0)(\sigma))\downarrow \wedge I(q)(M_I(\alpha_1)(M_I(\alpha_0)(\sigma)))$$

显然成立

Definition 4.1 设 $\alpha = (l_0, ..., l_k)$ 为一路径。

$$vc(p, \alpha, q) = p \rightarrow wlp(\alpha, q)$$

Proposition 4.2 若 $\models_I vc(p, \alpha, q)$ 则 $\models_I \{p\}\alpha\{q\}$ 。

证明

$$I(vc(p, \alpha, q))(\sigma) = true \equiv$$
$$I(p \rightarrow wlp(\alpha, q))(\sigma) = true \equiv$$
$$I(p)(\sigma) \rightarrow I(wlp(\alpha, q))(\sigma) \equiv$$
$$I(p)(\sigma) \rightarrow I(M_I(\alpha))(\sigma)\downarrow \rightarrow I(q)(M_I(\alpha)(\sigma))$$

Proposition 4.3 设 C 是标号集合， $beg, end \in C$, T 的每个循环至少有一个标号包含于 C 且 C 中的每个标号 l 有一个对应的公式 q_l 。若

$$\forall \alpha = (l_0, ..., l_k) \in \gamma(T, C), \models_I vc(q_{l_0}, \alpha, q_{l_k})$$

则

$$\models \{q_{beg}\}T\{q_{end}\}$$

证明

我们先证明一个更为一般的结论，即
若 $l_a, l_b \in C$ 且 $\alpha = (l_a, ..., l_b)$ 为 T 的路径，
则 $\models \{q_{l_a}\}\alpha\{q_{l_b}\}$ 。
我们假设定理的前提成立。
设 $len(l_a, ..., l_b)$ 为 $(l_a, ..., l_b)$ 中 C 中元素的个数。
我们用归纳法证明 $\models \{q_{l_a}\}\alpha\{q_{l_b}\}$ 。

- 若 $len(l_a, ..., l_b) = 2$ 则根据假设 $\models_I vc(q_{l_a}, (l_a, ..., l_b), q_{l_b})$ 成立，

  因此 $\models_I \{q_{l_a}\}(l_a, ..., l_b)\{q_{l_b}\}$ 成立。

- 假设对任意 $l_a, l_b \in C$ ， $len(l_a, ..., l_b) \leq k$ 时
  $\models_I \{q_{l_a}\}(l_a, ..., l_b)\{q_{l_b}\}$ 成立。
  对任意 l_a, l_b ， $len(l_a, ..., l_b) \leq k + 1$ 时，
  我们可将 $(l_a, ..., l_b)$ 分成两段 $(l_a, ..., l_c)$ 和 $(l_c, ..., l_b)$ ，
  其中 $l_c \in C$ 且 $len(l_a, ..., l_c), len(l_c, ..., l_b) \leq k$ 。
  根据假设我们有 $\models_I \{q_{l_a}\}(l_a, ..., l_c)\{q_{l_c}\}$ 和 $\models_I \{q_{l_c}\}(l_c, ..., l_b)\{q_{l_b}\}$ 。

  因此 $\models_I \{q_{l_a}\}(l_a, ..., l_b)\{q_{l_b}\}$ 成立。

根据归纳法对任意 $l_a, l_b \in C$ ， $\models_I \{q_{l_a}\}(l_a, ..., l_b), \{q_{l_b}\}$ 成立。由于 $l_0 = beg \in C, l_n = end \in C$ ，
因此 $\models_I \{q_{beg}\}(l_0, ..., l_n)\{q_{end}\}$ 成立。
因此对所有以 beg, end 为开始和终结点的路径 α ， $\models_I \{q_{beg}\}\alpha\{q_{end}\}$ 成立。

§4.3 结构化程序的推理

§4.3.1 指称语义

Proposition 4.4 设 S =while (e) do S_1 od 。

$$\forall \sigma \in \Sigma, M_I(S)(\sigma) \downarrow \Rightarrow \varphi(\sigma, M_I(S)(\sigma))$$

若

$$\forall \sigma \in \Sigma, I(\neg e)(\sigma) \Rightarrow \varphi(\sigma, \sigma)$$
$$\forall \sigma, \sigma' \in \Sigma, I(e)(\sigma) \wedge M_I(S_1)(\sigma) \downarrow \wedge \varphi(M_I(S_1)(\sigma), \sigma') \Rightarrow \varphi(\sigma, \sigma')$$

证明:将 φ 看作它的 ω- 扩展,则 $\forall \sigma \in \Sigma, M_I(S)(\sigma) \downarrow \Rightarrow \varphi(\sigma, M_I(S)(\sigma))$ 即

$$\forall \sigma \in \Sigma, \varphi(\sigma, M_I^\omega(S)(\sigma)) \sqsubseteq true$$

定义 Φ 如下:

$$\Phi(f)(\sigma) = \begin{cases} \omega & \text{若 } \sigma = \omega \\ ite(I(e)(\sigma), f(\mathcal{M}_I^\omega(S_1)(\sigma)), \sigma) & \text{若 } \sigma \neq \omega \end{cases}$$

则需证 $\forall \sigma \in \Sigma, \varphi(\sigma, \mu\Phi(\sigma)) \sqsubseteq true$ 。

用不动点归纳法。首先 $\forall \sigma \in \Sigma, \varphi(\sigma, \perp(\sigma)) \sqsubseteq true$ 成立。剩下的就是要证对任意给定 $f : [\Sigma_\omega \to \Sigma_\omega]$ ， $\forall \sigma \in \Sigma, \varphi(\sigma, f(\sigma)) \sqsubseteq true$ 则 $\forall \sigma' \in \Sigma, \varphi(\sigma', \Phi(f)(\sigma')) \sqsubseteq true$ 。
即要证对任意给定 σ' ，

$$\varphi(\sigma', ite(I(e)(\sigma'), f(M_I^\omega(S_1)(\sigma')), \sigma')) \sqsubseteq true$$

若 $I(e)(\sigma') = false$,则 $\varphi(\sigma', ite(I(e)(\sigma'), f(M_I^\omega(S_1)(\sigma')), \sigma')) = \varphi(\sigma', \sigma')$. 根据前提条件 $\varphi(\sigma', \sigma') \sqsubseteq true$ 成立。

若 $I(e)(\sigma') = true$,则 $\varphi(\sigma', ite(I(e)(\sigma'), f(M_I^\omega(S_1)(\sigma')), \sigma')) = \varphi(\sigma', f(M_I^\omega(S_1)(\sigma')))$. 分三种情况。

- 若 $f(M_I^\omega(S_1)(\sigma')) = \omega$ ， 则 $\varphi(\sigma', f(M_I^\omega(S_1)(\sigma'))) \sqsubseteq true$ 成立。
- 若 $f(M_I^\omega(S_1)(\sigma')) \neq \omega$ 而 $M_I^\omega(S_1)(\sigma') = \omega$ ，由于 f 的单调性， $f(M_I^\omega(S_1)(\sigma'))) = f(\sigma')$ 。根据归纳假设 $\varphi(\sigma', f((\sigma')) \sqsubseteq true$ 成立。
- 若 $f(M_I^\omega(S_1)(\sigma')) \neq \omega$ 且 $M_I^\omega(S_1)(\sigma') \neq \omega$ ，根据归纳假设 $\varphi(M_I^\omega(S_1)(\sigma'), f(M_I^\omega(S_1)(\sigma'))) \sqsubseteq true$ 成立。由于 $M_I^\omega(S_1)(\sigma') \neq \omega$ 且 $f(M_I^\omega(S_1)(\sigma')) \neq \omega$ ， $\varphi(M_I^\omega(S_1)(\sigma'), f(M_I^\omega(S_1)(\sigma'))) = true$ 。根据前提假设 $\varphi(\sigma', f(M_I^\omega(S_1)(\sigma'))) = true$ 成立。

Example 4.1 证明若 $M_I(T_{jc})$ 有定义,则 $M_I(T_{jc})(\sigma)(y) = \sigma(x)!$ 。

证明：只需证明 $\mathcal{M}_I^{\omega}(T_{jc})(\sigma)(y) \sqsubseteq (\sigma)(x)!$ 。由于有 $\mathcal{M}_I^{\omega}(T_1;T_2) = \mathcal{M}_I^{\omega}(T_2)\mathcal{M}_I^{\omega}(T_1)$ 。我们可以分别分析 $\mathcal{M}_I^{\omega}(y := 1)(\sigma)$ 和 $\mathcal{M}_I^{\omega}(\text{while } (x > 0) \text{ do } y := y * x; x := x - 1od \text{ od})(\sigma)$ 。设

$$\sigma_1 = \mathcal{M}_I^{\omega}(y := 1)(\sigma) = \sigma[y/1]$$

只需证明 $\mathcal{M}_I^{\omega}(\text{while } (x > 0) \text{ do } y := y * x; x := x - 1 \text{ od})(\sigma_1)(y) \sqsubseteq (\sigma)(x)!$ 。设 S_1 为

$$y := y * x; x := x - 1$$

定义

$$\varphi(\sigma, \sigma') = true \text{ 当且仅当 } \sigma'(y) = \sigma(x)! \cdot \sigma(y).$$

若 $I(x > 0)(\sigma) = false$ 则 $\varphi(\sigma, \sigma) = true$ 当且仅当 $\sigma(y) = \sigma(x)! \cdot \sigma(y)$ ，由于 $x = 0$ ， $\varphi(\sigma, \sigma) = true$ 成立。

若 $I(x > 0)(\sigma) = true$, $M_I(S_1)(\sigma) \downarrow$ 且 $\varphi(M_I(S_1)(\sigma), \sigma') = true$ ，由于 $M_I(S_1)(\sigma) = \sigma[y/\sigma(y) \cdot \sigma(x)][x/\sigma(x) - 1]$ ， $\sigma'(y) = \sigma(y) \cdot \sigma(x) \cdot (\sigma(x) - 1)! = \sigma(y) \cdot \sigma(x)!$ 。因此 $\varphi(\sigma, \sigma') = true$ 。

因此 $\forall \sigma \in \Sigma, \varphi(\sigma, M_I(\text{while } (x > 0) \text{ do } S_1 \text{ od})(\sigma)) \sqsubseteq true$ 。

因此 $\varphi(\sigma_1, M_I(\text{while } (x > 0) \text{ do } S_1 \text{ od})(\sigma_1)) \sqsubseteq true$ 。

因此若 $M_I(\text{while } (x > 0) \text{ do } S_1 \text{ od})(\sigma_1)$ 有定义，则 $M_I(\text{while } (x > 0) \text{ do } S_1 \text{ od})(\sigma_1)(y) = \sigma_1(x)! \cdot \sigma_1(y) = \sigma(x)!$.

§4.3.2 Hoare 逻辑

Proposition 4.5 我们有以下性质

$\models_I \{q_x^t\}x := t\{q\}$
$\models_I \{p\}S_1\{r\}$ 且 $\models_I \{r\}S_2\{q\}$ ，则 $\models_I \{p\}S_1; S_2\{q\}$
$\models_I \{p \wedge e\}T_1\{q\}$ 且 $\models_I \{p \wedge \neg e\}T_2\{q\}$ ，则 $\models_I \{p\}\textit{if } e \textit{ then } T_1 \textit{ else } T_2 \textit{ fi}\{q\}$
$\models_I \{p \wedge e\}T_1\{p\}$ ，则 $\models_I \{p\} \textit{ while } e \textit{ do } T_1 \textit{ od}\{p \wedge \neg e\}$
$\models_I \{q\}S_1\{r\}$ ， $\models_I p \supset q$ 且 $\models_I r \supset s$ ，则 $\models_I \{p\}S_1\{q\}$

首先对于公理 $\{p_x^t\}x := t\{p\}$, 即 $\vdash \{p_x^t\}x := t\{p\}$ 。我们必须证明 $\models \{p_x^t\}x := t\{p\}$, 即对任意 I ， $\models_I \{p_x^t\}x := t\{p\}$ 。我们必须证明对任意 σ ， $I(\{p_x^t\}x := t\{p\})(\sigma) = true$ 。根据定义 $I(\{p_x^t\}x := t\{p\})(\sigma) = true$ 当且仅当

$$I(p_x^t)(\sigma) = true \wedge \mathcal{M}_{\mathcal{I}}(x := t)(\sigma) \downarrow \Rightarrow \mathcal{I}(q)(\mathcal{M}_{\mathcal{I}}(x := t)(\sigma)) = true$$

由于

$$I(p_x^t)(\sigma) = I(p)(\sigma[x/I(t)(\sigma)] = \mathcal{I}(q)(\mathcal{M}_{\mathcal{I}}(x := t)(\sigma))$$

因此

$$I(p_x^t)(\sigma) = true \wedge \mathcal{M}_{\mathcal{I}}(x := t)(\sigma) \downarrow \Rightarrow \mathcal{I}(q)(\mathcal{M}_{\mathcal{I}}(x := t)(\sigma)) = true$$

因此

$$I(\{p_x^t\}x := t\{p\})(\sigma) = true$$

对于组合规则，我们必须证明 $\models_I \{p\}T_1\{q\}$ 且 $\models_I \{q\}T_2\{r\}$ 则 $\models_I \{p\}T_1;T_2\{r\}$。若 $M_I(T_1;T_2)(\sigma)$ 无定义，则 $I(\{p\}T_1;T_2\{r\})(\sigma) = true$。假设 $M_I(T_1;T_2)(\sigma)$ 有定义且 $M_I(T_1;T_2)(\sigma) = \sigma'$。需要证明的就是 $I(p)(\sigma)$ 则 $I(r)(\sigma')$。$M_I(T_1;T_2)(\sigma) = \sigma'$ 则 $(T_1;T_2,\sigma)\overset{*}{\Rightarrow}\sigma'$。因此存在 σ'' 使得

$$(T_1;T_2,\sigma)\overset{*}{\Rightarrow}(T_2,\sigma'')\overset{*}{\Rightarrow}\sigma'$$

因此

$$(T_1,\sigma)\overset{*}{\Rightarrow}\sigma'' \text{ 且 } (T_2,\sigma'')\overset{*}{\Rightarrow}\sigma'$$

根据 $\models_I \{p\}T_1\{q\}$ 和 $\models_I \{q\}T_2\{r\}$，若 $I(p)(\sigma)$，则 $I(q)(\sigma'')$，则 $I(r)(\sigma')$。因此

$$I(\{p\}T_1;T_2\{r\})(\sigma) = true$$

对于条件规则，我们必须证明 $\models_I \{p \wedge e\}T_1\{q\}$ 且 $\models_I \{p \wedge \neg e\}T_2\{q\}$ 则 $\models_I \{p\}\text{if } e \text{ then } T_1 \text{ else } T_2 \text{ fi}\{q\}$。若 $M_I(\text{if } e \text{ then } T_1 \text{ else } T_2 \text{ fi})(\sigma)$ 无定义，则结论成立。若 $M_I(\text{if } e \text{ then } T_1 \text{ else } T_2 \text{ fi})(\sigma) = \sigma'$，我们分两种情况讨论。若 $I(e)(\sigma)$ 成立则

$$M_I(\text{if } e \text{ then } T_1 \text{ else } T_2 \text{ fi})(\sigma) = M_I(T_1)(\sigma)$$

根据 $\models_I \{p\wedge e\}T_1\{q\}$，若 $I(p)(\sigma)$ 则 $I(q)(M_I(T_1)(\sigma))$ 成立。因此

$$\models_I \{p\}\text{if } e \text{ then } T_1 \text{ else } T_2 \text{ fi}\{q\}$$

同理，若 $I(\neg e)(\sigma)$ 成立，根据 $\models_I \{p \wedge \neg e\}T_2\{q\}$，以上命题也成立。

对于循环规则，我们必须证明 $\models_I \{p \wedge e\}T_1\{p\}$ 则 $\models_I \{p\}\text{while } e \text{ do } T_1 \text{ od}\{p \wedge \neg e\}$。

若 $M_I(\text{while } e \text{ do } T_1 \text{ od})(\sigma)$ 无定义，则结论成立。

若 $M_I(\text{while } e \text{ do } T_1 \text{ od})(\sigma) = \sigma'$，则 $(\text{while } e \text{ do } T_1 \text{ od},\sigma)\overset{k}{\Rightarrow}\sigma'$。

我们用归纳法证明对任意 σ，$I(p)(\sigma)$ 则 $I(p\wedge\neg e)(\sigma)$。

若 $k = 1$，则 $\sigma' = \sigma$，$I(e)(\sigma) = false$。因此 $I(p)(\sigma) \Rightarrow I(p \wedge \neg e)(\sigma')$。

若 $k > 1$，假设对任意 σ，$i < k$，$(\text{while } e \text{ do } T_1 \text{ od},\sigma)\overset{i}{\Rightarrow}\sigma'$。则 $I(p)(\sigma) \Rightarrow I(p \wedge \neg e)(\sigma')$。由于 $(\text{while } e \text{ do } T_1 \text{ od},\sigma)\overset{k}{\Rightarrow}\sigma'$ 且 $k > 1$，则

$$I(e)(\sigma) \text{ 且 } (\text{while } e \text{ do } T_1 \text{ od},\sigma)\Rightarrow(T_1;\text{while } e \text{ do } T_1 \text{ od},\sigma)\overset{k-1}{\Rightarrow}\sigma'。$$

存在 σ'' 使得

$$(T_1,\sigma)\overset{k_1}{\Rightarrow}\sigma'' \text{ 且 } (\text{while } e \text{ do } T_1 \text{ od},\sigma'')\overset{k_2}{\Rightarrow}\sigma'$$

根据 $\models_I \{p\wedge e\}T_1\{p\}$，由于已有 $I(e)(\sigma)$，若 $I(p)(\sigma)$，则 $I(p)(\sigma'')$。根据归纳假设有 $I(p)(\sigma'')$ 则 $I(p\wedge\neg e)(\sigma')$。因此

$$\models_I \{p\}\text{while } e \text{ do } T_1 \text{ od}\{p\wedge\neg e\}$$

以上证明了系统的可靠性。

Proposition 4.6 *对于给定的 I 且 I 的表达能力足够强，那么*

$$\models_I \{p\}T\{q\} \text{ 则 } th(I)\vdash\{p\}T\{q\}$$

证明基于 T 的结构。我们首先证明以下事实。

$\models_I \{p\}S_1;S_2\{q\}$ 且 $I(r)$ 为 S_2 和 $I(q)$ 的最弱自由前断言， 则 $\models_I \{p\}S_1\{r\}$ 且 $\models_I \{r\}S_2\{q\}$
$\models_I \{p\}\text{if } e \text{ then } T_1 \text{ else } T_2 \text{ fi}\{q\}$ ， 则 $\models_I \{p\wedge e\}T_1\{q\}$ 且 $\models_I \{p\wedge\neg e\}T_2\{q\}$
$\models_I \{p\}$ while e do T_1 od$\{q\}$ ， 则 $\models_I \{p\}$ if (e) T_1; while e do T_1 od else $x := x$ fi $\{q\}$

若 $\models_I \{p\}x := t\{q\}$ 则根据语义有 $\models_I p\supset q_x^t$。因此 $th(I)\vdash p\supset q_x^t$。根据赋值公理和推论规则可以得出

$$th(I)\vdash\{p\}T\{q\}$$

若 $\models_I \{p\}S_1;S_2\{q\}$。设 $I(r)$ 为 S_2 和 $I(q)$ 的最弱自由前断言。由于 $\models_I \{p\}S_1\{r\}$ 且 $\models_I \{r\}S_2\{q\}$，则 $th(I)\vdash\{p\}S_1\{r\}$ 且 $th(I)\vdash\{r\}S_2\{q\}$。根据组合规则可以得出

$$th(I)\vdash\{p\}S_1;S_2\{q\}$$

若 $\models_I \{p\}\text{if } e \text{ then } T_1 \text{ else } T_2 \text{ fi}\{q\}$。由于 $\models_I \{p\wedge e\}T_1\{q\}$ 且 $\models_I \{p\wedge\neg e\}T_2\{q\}$。则 $th(I)\vdash\{p\wedge e\}T_1\{q\}$ 且 $th(I)\vdash\{p\wedge\neg e\}T_2\{q\}$。根据条件规则可以得出

$$th(I)\vdash\{p\}\text{if } e \text{ then } T_1 \text{ else } T_2 \text{ fi}\{q\}$$

若 $\models_I \{p\}\text{while } e \text{ do } T_1 \text{ od}\{q\}$。设 $I(r)$ 为 while e do T_1 od 和 $I(q)$ 的最弱自由前断言。则

$$\models_I p\supset r \text{ 且}$$
$$\models_I \{r\} \text{ if (e) } T_1\text{; while } e \text{ do } T_1 \text{ od else x:=x fi } \{q\}$$

则

$$\models_I \{r\wedge e\}T_1;\text{while } e \text{ do } T_1 \text{ od}\{q\} \text{ 且}$$
$$\models_I \{r\wedge\neg e\}x := x\{q\}\text{。}$$

则

$$\models_I \{r\wedge e\}T_1\{r\} \text{ 且 } \models_I (r\wedge\neg e)\supset q\text{。}$$

根据循环规则和推论规则可以得出 $th(I)\vdash\{p\}T\{q\}$。以上四种情况证明了系统的相对完备性。