§4　推理验证

§4.1　卫式迁移系统的推理

例子 4.1.1 : 互斥协议

T	$a = s_0$	$\longrightarrow$	$(y, t, a) := (1, 1, s_1)$
	$a = s_1 \wedge (x = 0 \vee t = 0)$	$\longrightarrow$	$(a) := (s_2)$
	$a = s_2$	$\longrightarrow$	$(y, a) := (0, s_3)$
	$a = s_3$	$\longrightarrow$	$(y, t, a) := (1, 1, s_1)$
	$b = t_0$	$\longrightarrow$	$(x, t, b) := (1, 0, t_1)$
	$b = t_1 \wedge (y = 0 \vee t = 1)$	$\longrightarrow$	$(b) := (t_2)$
	$b = t_2$	$\longrightarrow$	$(x, b) := (0, t_3)$
	$b = t_3$	$\longrightarrow$	$(x, t, b) := (1, 0, t_1)$
Θ	$(a = s_0 \wedge b = t_0 \wedge x = 0 \wedge y = 0 \wedge t = 0)$		

安全性质: 互斥协议满足以下性质:

$$(T, \Theta) \models_I \Box(a = s_1 \wedge b \neq t_1 \wedge b \neq t_2 \rightarrow a = s_2 R b \neq t_2)$$

主要适用规则

主要适用规则如下

$$\frac{\begin{array}{l}\zeta \Rightarrow \varphi' \\ \{\varphi' \wedge \neg\psi\} T \{\varphi'\} \\ \varphi' \Rightarrow \varphi\end{array}}{\zeta \Rightarrow \psi R \varphi}$$

尝试 1（简单尝试）

令

$$\begin{array}{lcl}\zeta & \equiv & (a = s_1 \wedge b \neq t_1 \wedge b \neq t_2) \\ \psi & \equiv & (a = s_2) \\ \varphi & \equiv & (b \neq t_2) \\ \varphi' & \equiv & \varphi\end{array}$$

需要 $\zeta \Rightarrow \varphi$ 和 $\forall t \in T, \{\varphi' \wedge \neg\psi\} t \{\varphi'\}$ 。

试证:
$\{\varphi' \wedge \neg\psi\} t_6 \{\varphi'\}$ 。
需要

$$(b \neq t_2) \wedge (a \neq s_2) \wedge b = t_1 \wedge (y = 0 \vee t = 1) \rightarrow (t_2 \neq t_2)$$

证明失败。

尝试 2（简单补充）

令

$$\begin{aligned}\zeta &\equiv (a = s_1 \wedge b \neq t_1 \wedge b \neq t_2)\\ \psi &\equiv (a = s_2)\\ \varphi &\equiv (b \neq t_2)\\ \varphi' &\equiv (a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge b \neq t_2)\end{aligned}$$

试证：

$\{\varphi' \wedge \neg\psi\}t_6\{\varphi'\}$ 。

需要

$$\begin{aligned}&((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge b \neq t_2))\wedge\\ &(a \neq s_2)\wedge\\ &b = t_1 \wedge (y = 0 \vee t = 1)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

$$\begin{aligned}&((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0)))\wedge\\ &(a \neq s_2)\wedge\\ &b = t_1 \wedge (y = 0 \vee t = 1)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

$$\begin{aligned}&((a = s_1 \wedge ((b = t_1 \wedge x = 1 \wedge t = 0))) \wedge (y = 0)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

证明失败。

尝试 3（充分补充）

令

$$\begin{aligned}\zeta &\equiv (a = s_1 \wedge b \neq t_1 \wedge b \neq t_2)\\ \psi &\equiv (a = s_2)\\ \varphi &\equiv (b \neq t_2)\\ \varphi' &\equiv (a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge b \neq t_2)\end{aligned}$$

试证：

$\{\varphi' \wedge \neg\psi\}t_6\{\varphi'\}$ 。

需要

$$\begin{aligned}&((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge b \neq t_2))\wedge\\ &(a \neq s_2) \wedge b = t_1 \wedge (y = 0 \vee t = 1)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

$$\begin{aligned}&((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1)))\wedge\\ &(a \neq s_2) \wedge b = t_1 \wedge (y = 0 \vee t = 1)\\ &\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge t_2 \neq t_2)\end{aligned}$$

因此 $a = s_1 \wedge b \neq t_1 \wedge b \neq t_2 \Rightarrow a = s_2 R b \neq t_2$ ，

即 $\Box(a = s_1 \wedge b \neq t_1 \wedge b \neq t_2 \rightarrow a = s_2 R b \neq t_2)$ 。

分两种情况来证明，分析的时候可能方便些。

我们有 $\zeta \rightarrow \zeta_1 \vee \zeta_2$ ，

其中 $\zeta_1 = (a = s_1 \wedge b = t_0)$, $\zeta_2 = (a = s_1 \wedge b = t_3)$,

令

$$\varphi_1 \quad = \quad (a = s_1 \wedge (b = t_0 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge b \neq t_2)$$

则 $\zeta_1 \Rightarrow \psi R \varphi_1$ 。
因此 $\zeta_1 \Rightarrow a = s_2 R b \neq t_2$ 。

同理 $\zeta_2 \Rightarrow a = s_2 R b \neq t_2$ 。
因此 $\zeta \Rightarrow a = s_2 R b \neq t_2$ 。

$\cdots$

活性性质: 互斥协议满足以下性质:

$$(T, \Theta) \models_I \Box(a = s_1 \rightarrow \Diamond a = s_2)$$

主要适用规则

主要适用规则如下

$$\frac{\begin{array}{l}\varphi \Rightarrow (\psi \vee \zeta) \\ \zeta \Rightarrow (w_x^e \wedge (\psi \vee E(T))) \\ \{\zeta \wedge e = v\} T \{\psi \vee (\zeta \wedge e \sqsubset v)\}\end{array}}{\varphi \Rightarrow \Diamond \psi}$$

尝试 1（简单尝试）

选择 f 满足

$$\begin{array}{llll} I(f(t_0,0)) = 1 & I(f(t_1,0)) = 0 & I(f(t_2,0)) = 2 & I(f(t_3,0)) = 1 \\ I(f(t_0,1)) = 1 & I(f(t_1,1)) = 3 & I(f(t_2,1)) = 2 & I(f(t_3,1)) = 1 \end{array}$$

令

$$\begin{array}{rcl} W & = & (\{0,1,2,3\}, \leq) \\ w & = & (0 \leq x \leq 3) \\ e & = & f(b,t) \\ \varphi & = & (a = s_1) \\ \psi & = & (a = s_2) \\ \zeta & = & (a = s_1) \end{array}$$

需要

$$\begin{array}{l} \varphi \Rightarrow (\psi \vee \zeta) \\ \zeta \Rightarrow w_x^e \wedge (\psi \vee E(T)) \\ \forall t \in T, \{\zeta \wedge e = v\} t \{\psi \vee (\zeta \wedge e < v)\} \end{array}$$

试证:
$\{\zeta \wedge e = v\} t_6 \{\psi \vee (\zeta \wedge e < v)\}$ 。
需要

$$\begin{array}{l} ((a = s_1 \wedge f(b,t) = v) \wedge b = t_1 \wedge (y = 0 \vee t = 1)) \\ \rightarrow (a = s_2 \vee (a = s_1 \wedge f(t_2,t) < v)) \end{array}$$

$$\begin{array}{l} ((a = s_1 \wedge f(t_1,t) = v) \wedge b = t_1 \wedge (y = 0 \vee t = 1)) \\ \rightarrow (a = s_2 \vee (a = s_1 \wedge f(t_2,t) < v)) \end{array}$$

$$\begin{array}{l} ((a = s_1) \wedge b = t_1 \wedge (y = 0 \vee t = 1)) \\ \rightarrow (a = s_2 \vee (a = s_1 \wedge f(t_2,t) < f(t_1,t))) \end{array}$$

尝试 2

令

$$\begin{aligned} W &= (\{0,1,2,3\},\leq) \\ w &= (0 \leq x \leq 3) \\ e &= f(b,t) \\ \varphi &= (a = s_1) \\ \psi &= (a = s_2) \\ \zeta &= (a = s_1 \wedge y = 1) \end{aligned}$$

因此 $\varphi \Rightarrow \Diamond\psi$ 。

例子 4.1.2 : 开平方

T	$a = s_0$	$\longrightarrow$	$(y_1, y_2, y_3, a) := (0, 1, 1, s_1)$
	$a = s_1 \wedge (y_3 \leq x)$	$\longrightarrow$	$(a) := (s_2)$
	$a = s_1 \wedge \neg(y_3 \leq x)$	$\longrightarrow$	$(a) := (s_4)$
	$a = s_2$	$\longrightarrow$	$(y_1, y_2, a) := (y_1 + 1, y_2 + 2, s_3)$
	$a = s_3$	$\longrightarrow$	$(y_3, a) := (y_3 + y_2, s_1)$
Θ	$(a = s_0)$		

安全性质:

$$(T, \Theta) \models_I x > 0 \rightarrow \Box(a = s_4 \rightarrow y_1 = \sqrt{x})$$

只需证明

$$(T, \Theta) \quad \models_I \quad \Box(x > 0 \wedge a = s_0 \rightarrow \Box(a = s_4 \rightarrow y_1 = \sqrt{x}))$$

主要适用规则

主要适用规则如下

$$\frac{\begin{array}{l}\zeta \Rightarrow \varphi' \\ \{\varphi'\}T\{\varphi'\} \\ \varphi' \Rightarrow \varphi\end{array}}{\zeta \Rightarrow \Box\varphi}$$

尝试

令

$$\begin{array}{lcl}\zeta & \equiv & (x > 0 \wedge a = s_0) \\ \varphi & \equiv & (a = s_4 \rightarrow y_1 = \sqrt{x}) \\ \varphi' & \equiv & (a = s_0 \wedge \varphi_0) \vee (a = s_1 \wedge \varphi_1) \vee (a = s_2 \wedge \varphi_2) \vee (a = s_3 \wedge \varphi_3) \vee (a = s_4 \wedge \varphi_4)\end{array}$$

其中 φ' 为

$$\begin{array}{lcl}\varphi_0 & \equiv & (x > 0) \\ \varphi_1 & \equiv & (y_1^2 \leq x \wedge y_2 = 2 * y_1 + 1 \wedge y_3 = (y_1 + 1)^2) \\ \varphi_2 & \equiv & ((y_1 + 1)^2 \leq x \wedge y_2 = 2 * y_1 + 1 \wedge y_3 = (y_1 + 1)^2) \\ \varphi_3 & \equiv & (y_1^2 \leq x \wedge y_2 = 2 * y_1 + 1 \wedge y_3 = y_1^2) \\ \varphi_4 & \equiv & (y_1 = \sqrt{x}) \\ & \equiv & (y_1^2 \leq x \wedge x < (y_1 + 1)^2\end{array}$$

需要 $\zeta \Rightarrow \varphi$ 和 $\forall t \in T, \{\varphi'\}t\{\varphi'\}$ 。

活性性质: 满足以下性质:

$$(T, \Theta) \models_I x > 0 \rightarrow \Diamond a = s_4$$

只需证明

$$(T, \Theta) \quad \models_I \quad \Box(x > 0 \wedge a = s_0 \rightarrow \Diamond(a = s_4)$$

主要适用规则

主要适用规则如下

$$\frac{\begin{array}{l}\varphi \Rightarrow (\psi \vee \zeta) \\ \zeta \Rightarrow (w_x^e \wedge (\psi \vee E(T)) \\ \{\zeta \wedge e = v\} T \{\psi \vee (\zeta \wedge e \sqsubset v)\}\end{array}}{\varphi \Rightarrow \Diamond \psi}$$

尝试 1

选择 f 满足

$$\begin{array}{l} I(f(s_0, x, y)) = 3x + 1 \\ I(f(s_i, x, y)) = 3(x - y_3 + 1) + 1 - i \quad (i = 1, 2, 3) \\ I(f(s_4, x, y)) = 0 \end{array}$$

令

$$\begin{array}{rcl} W & = & (NAT, \leq) \\ w & = & true \\ e & = & f(a, x, y) \\ \varphi & = & (x > 0 \wedge a = s_0) \\ \psi & = & (a = s_4) \\ \zeta & = & \varphi' \end{array}$$

需要

$$\begin{array}{l} \varphi \Rightarrow (\psi \vee \zeta) \\ \zeta \Rightarrow w_x^e \wedge (\psi \vee E(T)) \\ \forall t \in T, \{\zeta \wedge e = v\} t \{\psi \vee (\zeta \wedge e < v)\} \end{array}$$

§4.2 谓词迁移系统的推理

例子 4.2.1 : 互斥协议

ρ	$\bigvee$	$[a = s_0$	$\wedge$	$a' = s_1 \wedge b' = b \wedge x' = x \wedge y' = 1 \wedge t' = 1]$
		$[a = s_1 \wedge (x = 0 \vee t = 0)$	$\wedge$	$a' = s_2 \wedge b' = b \wedge x' = x \wedge y' = y \wedge t' = t]$
		$[a = s_2$	$\wedge$	$a' = s_3 \wedge b' = b \wedge x' = x \wedge y' = 0 \wedge t' = t]$
		$[a = s_3$	$\wedge$	$a' = s_1 \wedge b' = b \wedge x' = x \wedge y' = 1 \wedge t' = 1]$
		$[b = t_0$	$\wedge$	$a' = a \wedge b' = t_1 \wedge x' = 1 \wedge y' = y \wedge t' = 0]$
		$[b = t_1 \wedge (y = 0 \vee t = 1)$	$\wedge$	$a' = a \wedge b' = t_2 \wedge x' = x \wedge y' = y \wedge t' = t]$
		$[b = t_2$	$\wedge$	$a' = a \wedge b' = t_3 \wedge x' = 0 \wedge y' = y \wedge t' = t]$
		$[b = t_3$	$\wedge$	$a' = a \wedge b' = t_1 \wedge x' = 1 \wedge y' = y \wedge t' = 0]$
Θ	$(a = s_0 \wedge b = t_0 \wedge x = 0 \wedge y = 0 \wedge t = 0)$			

安全性质: 互斥协议满足以下性质:

$$(T, \Theta) \models_I \Box(a = s_1 \wedge b \neq t_1 \wedge b \neq t_2 \rightarrow a = s_2 R b \neq t_2)$$

主要适用规则

主要适用规则如下

$$\frac{\begin{array}{l}\zeta \Rightarrow \varphi' \\ \{\varphi' \wedge \neg\psi\}\rho\{\varphi'\} \\ \varphi' \Rightarrow \varphi\end{array}}{\zeta \Rightarrow \psi R \varphi}$$

尝试

令

$$\begin{array}{lcl}\zeta & \equiv & (a = s_1 \wedge b \neq t_1 \wedge b \neq t_2) \\ \psi & \equiv & (a = s_2) \\ \varphi & \equiv & (b \neq t_2) \\ \varphi' & \equiv & (a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge b \neq t_2)\end{array}$$

需要

$\{\varphi' \wedge \neg\psi\}\rho\{\varphi'\}$ 。

即

$$\begin{array}{l}((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee (a = s_2 \wedge b \neq t_2)) \wedge \\ \neg(a = s_2) \wedge \rho \rightarrow \\ ((a' = s_1 \wedge (b' = t_0 \vee b' = t_3 \vee (b' = t_1 \wedge x' = 1 \wedge t' = 0 \wedge y' = 1))) \vee (a' = s_2 \wedge b' \neq t_2))\end{array}$$

即

$$\begin{array}{l}(a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \wedge \\ \neg(a = s_2) \wedge \rho \rightarrow \\ ((a' = s_1 \wedge (b' = t_0 \vee b' = t_3 \vee (b' = t_1 \wedge x' = 1 \wedge t' = 0 \wedge y' = 1))) \vee (a' = s_2 \wedge b' \neq t_2))\end{array}$$

即

$$\begin{array}{l}(a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \wedge \\ \rho \rightarrow \\ ((a' = s_1 \wedge (b' = t_0 \vee b' = t_3 \vee (b' = t_1 \wedge x' = 1 \wedge t' = 0 \wedge y' = 1))) \vee (a' = s_2 \wedge b' \neq t_2))\end{array}$$

...

活性性质：互斥协议满足以下性质：

$$(T,\Theta) \models_I \Box(a = s_1 \to \Diamond a = s_2)$$

主要适用规则

主要适用规则如下

$$\frac{\begin{array}{l}\varphi \Rightarrow (\psi \vee \zeta) \\ \zeta \Rightarrow (w_x^e \wedge (\psi \vee \exists v_1' ... v_n' . \rho)) \\ \{\zeta \wedge e = v\}\rho\{\psi \vee (\zeta \wedge e \sqsubset v)\}\end{array}}{\varphi \Rightarrow \Diamond\psi}$$

尝试

选择 f 满足

$$\begin{array}{llll} I(f(t_0,0)) = 1 & I(f(t_1,0)) = 0 & I(f(t_2,0)) = 2 & I(f(t_3,0)) = 1 \\ I(f(t_0,1)) = 1 & I(f(t_1,1)) = 3 & I(f(t_2,1)) = 2 & I(f(t_3,1)) = 1 \end{array}$$

令

$$\begin{array}{lcl} W & = & (\{0,1,2,3\}, \leq) \\ w & = & (0 \leq x \leq 3) \\ e & = & f(b,t) \\ \varphi & = & (a = s_1) \\ \psi & = & (a = s_2) \\ \zeta & = & (a = s_1 \wedge y = 1) \end{array}$$

我们有

$$\begin{array}{l} \varphi \Rightarrow (\psi \vee \zeta) \\ \zeta \Rightarrow w_x^e \wedge (\psi \vee \exists v_1' ... v_n' . \rho) \end{array}$$

且

$$\begin{array}{l} (a = s_1 \wedge y = 1 \wedge f(b,t) = v) \wedge \\ \rho \to \\ (a' = s_2) \vee (a' = s_1 \wedge y' = 1 \wedge f(b',t') < v) \end{array}$$

因此 $\varphi \Rightarrow \Diamond\psi$ 。

例子 4.3.2 ： 开平方

设

$$(B,V)=((\{0,1,2,3,...,+,*\},\{\leq\}),\{x,y_1,y_2,y_3\})$$

beg:	$(y_1,y_2,y_3):=(0,1,1)$; goto test
test:	if $(y_3\leq x)$ goto loop else goto end
loop:	$(y_1,y_2):=(y_1+1,y_2+2)$; goto inloop
inloop:	$y_3:=y_3+y_2$; goto test

3.2a 部分正确

证明程序 T_0 在解释 $I=(NAT,I_0)$ 下对于前断言 $x\geq 0$ 和后断言 $y_1=\sqrt{x}$ 是部分正确的。

假设程序运行过程如下：

$$(beg,\sigma_0)(test,\sigma_1)(loop,\sigma_2)(inloop,\sigma_3)(test,\sigma_4)(loop,\sigma_5)\cdots(test,\sigma_{n-1})(end,\sigma_n)\cdots$$

这时迁移个数为 n ，即 $l_n=end$ 。我们需要证明的是 $(y_1=\sqrt{x})(\sigma_n)$ 即 $\sigma_n(y_1)=\sqrt{\sigma_n(x)}$ 。

由于 $\sigma_n=\sigma_{n-1}$ 且 $(test,\sigma_{n-1})\Rightarrow(end,\sigma_n)$ 则

$$\neg(\sigma_n(y_3)\leq\sigma_n(x))$$

因此，如果存在 φ' ，使得 $\varphi'(\sigma_{n-1})$ 成立且

$$\neg(\sigma_n(y_3)\leq\sigma_n(x))\wedge\varphi'(\sigma_n)\rightarrow\sigma_n(y_1)=\sqrt{\sigma_n(x)}$$

则

$$\sigma_n(y_1)=\sqrt{\sigma_n(x)}$$

设 φ' 为

$$x=\sigma_0(x)\wedge y_1^2\leq x\wedge y_2=2*y_1+1\wedge y_3=(y_1+1)^2$$

$\neg(\sigma_n(y_3)\leq\sigma_n(x))\wedge\varphi'(\sigma_n)\rightarrow\sigma_n(y_1)=\sqrt{\sigma_n(x)}$ 是成立的。我们需证 $\varphi'(\sigma_{n-1})$ ，即

$$\begin{aligned}&\sigma_{n-1}(x)=\sigma_0(x)\wedge\\&\sigma_{n-1}(y_1)^2\leq\sigma_{n-1}(x)\wedge\\&\sigma_{n-1}(y_2)=2*\sigma_{n-1}(y_1)+1\wedge\\&\sigma_{n-1}(y_3)=(\sigma_{n-1}(y_1)+1)^2\end{aligned}$$

我们用归纳法证明以上公式。

由于 $n-1$ 时所对应的标号时 $test$ ，

我们只要证明对任意 k 当 σ_k 所对应的状态其标号为 $test$ 时

$$\begin{aligned}&\sigma_k(x)=\sigma_0(x)\wedge\\&\sigma_k(y_1)^2\leq\sigma_k(x)\wedge\\&\sigma_k(y_2)=2*\sigma_k(y_1)+1\wedge\\&\sigma_k(y_3)=(\sigma_k(y_1)+1)^2\end{aligned}$$

成立。

- $k=0$ 时，由于标号为 beg ，无须证明。

- $k = 1$ 时，标号为 $test$ 。由于 $\sigma_1(y_1) = 0, \sigma_1(y_2) = 1, \sigma_1(y_3) = 1, \sigma_1(x) = \sigma_0(x)$ 且 $\sigma_0(x) \geq 0$ 。

  因此

  $$\sigma_k(x) = \sigma_0(x) \wedge$$
  $$\sigma_k(y_1)^2 \leq \sigma_k(x) \wedge$$
  $$\sigma_k(y_2) = 2 * \sigma_k(y_1) + 1 \wedge$$
  $$\sigma_k(y_3) = (\sigma_k(y_1) + 1)^2$$

  成立。

- 假设 $k \leq i$ 时，目标成立。当 $k = i + 1$ 且 $i \geq 1$ 时，若标号不为 $test$ 则无须证明。若标号为 $test$ 则 $k \geq 4$ 且

  $$(test, \sigma_{k-3}) \Rightarrow (loop, \sigma_{k-2})$$
  $$(loop, \sigma_{k-2}) \Rightarrow (inloop, \sigma_{k-1})$$
  $$(inloop, \sigma_{k-1}) \Rightarrow (test, \sigma_k)$$

  因此

  $$\sigma_k = \sigma_{k-1}[y_3/I(y_2 + y_3)(\sigma_{k-1})]$$
  $$\sigma_{k-1} = \sigma_{k-2}[y_1/I(y_1 + 1)(\sigma_{k-2}][y_2/I(y_2 + 2)(\sigma_{k-2})]$$
  $$\sigma_{k-2} = \sigma_{k-3} \wedge I(y_3 \leq x)(\sigma_{k-3})$$

  因此

  $$\sigma_k(x) = \sigma_{k-3}(x) = \sigma_0(x)$$
  $$(\sigma_k(y_1))^2 = (\sigma_{k-3}(y_1) + 1)^2 = \sigma_{k-3}(y_3) \leq \sigma_{k-3}(x) = \sigma_k(x)$$
  $$\sigma_k(y_2) = \sigma_{k-3}(y_2) + 2 = 2 * \sigma_{k-2}(y_1) + 3 = 2 * \sigma_k(y_1) + 1$$
  $$\sigma_k(y_3) = \sigma_{k-3}(y_2) + \sigma_{k-3}(y_3) + 2 = (\sigma_{k-3}(y_1) + 2)^2 = (\sigma_k(y_1) + 1)^2$$

  因此对任意 k 当 σ_k 所对应的状态其标号为 $test$ 时

  $$\sigma_k(x) = \sigma_0(x) \wedge$$
  $$\sigma_k(y_1)^2 \leq \sigma_k(x) \wedge$$
  $$\sigma_k(y_2) = 2 * \sigma_k(y_1) + 1 \wedge$$
  $$\sigma_k(y_3) = (\sigma_k(y_1) + 1)^2$$

成立。

3.2b ： 终止

证明程序 T_0 在解释 $I = (NAT, I_0)$ 下对于前断言 $true$ 是终止的。

假设程序不终止，则程序的运行过程为

$$(l_0, \sigma_0)(l_1, \sigma_1)(l_2, \sigma_2)(l_3, \sigma_3)(l_4, \sigma_4)(l_5, \sigma_5) \cdots$$

其中 $l_0 = beg$, 对所有 $k \geq 0$ 有

$l_{3k+1} = test, l_{3k+2} = loop$,$l_{3k+3} = inloop$ 且 $\sigma_{3k+1}(y_3) \leq x$

以下我们证明对所有 $k \geq 0$

有 $\sigma_{3k+1}(y_3) \geq k$ 且 $\sigma_{3k+1}(x) = \sigma_0(x)$ 。

- 由于 $\sigma_1(y_3)=1$ 且 $\sigma_1(x)=\sigma_0(x)$ 。
  因此 $\sigma_{3*0+1}(y_3)\geq 0$ 且 $\sigma_{3*0+1}(x)=\sigma_0(x)$ 。

- 假设 $k=i$ 时有 $\sigma_{3i+1}(y_3)\geq i$ 且 $\sigma_{3i+1}(x)=\sigma_0(x)$ ，
  我们需证 $k=i+1$ 时有 $\sigma_{3(i+1)+1}(y_3)\geq i+1$ 且
  $\sigma_{3i+1}(x)=\sigma_0(x)$ 。
  根据前面的分析我们有

  $$\sigma_{3(i+1)+1}(x)=\sigma_{3(i+1)+1-3}(x)=\sigma_0(x)$$
  $$\sigma_{3(i+1)+1}(y_3)=\sigma_{3(i+1)+1-3}(y_2)+\sigma_{3(i+1)+1-3}(y_3)+2\geq i+1$$

  因此 $k=i+1$ 时有
  $\sigma_{3(i+1)+1}(y_3)\geq i+1$ 且 $\sigma_{3i+1}(x)=\sigma_0(x)$ 。

因此对所有 $k\geq 0$ 有 $\sigma_{3k+1}(y_3)\geq k$ 且 $\sigma_{3k+1}(x)=\sigma_0(x)$ 。
取 $k=\sigma_0(x)+1$ ，则 $\sigma_{3k+1}(y_3)\leq\sigma_{3k+1}(x)$ 不成立，与程序不终止的前提矛盾。

3.2c ：完全正确

证明程序 T_0 在解释 $I=(NAT,I_0)$ 下对于前断言 $x\geq 0$ 和后断言 $y_1=\sqrt{x}$ 是完全正确的。

首先证明引理：对所有状态 $\sigma\in\Sigma$ 和所有 $0\leq k\leq\sqrt{\sigma_0(x)}$ ，

$$(l_0=beg,\sigma_0)\Rightarrow(l_{3k+1},\sigma_{3k+1})$$

且

$$\begin{aligned}&l_{3k+1}=test\\&\sigma_{3k+1}(x)=\sigma_0(x)\\&\sigma_{3k+1}(y_1)=k\\&\sigma_{3k+1}(y_2)=2k+1\\&\sigma_{3k+1}(y_3)=(k+1)^2\end{aligned}$$

引理的证明使用归纳法如下：

- $k=0$ 时，显然引理成立。

- 假设 $k=i$ 且 $k\leq\sqrt{\sigma_0(x)}$ 时有

  $$\begin{aligned}&l_{3k+1}=test\\&\sigma_{3k+1}(x)=\sigma_0(x)\\&\sigma_{3k+1}(y_1)=k\\&\sigma_{3k+1}(y_2)=2k+1\\&\sigma_{3k+1}(y_3)=(k+1)^2\end{aligned}$$

  则 $k=i+1$ 且 $k\leq\sqrt{\sigma_0(x)}$ 时有

  $$\begin{aligned}&l_{3(i+1)+1}=test\\&\sigma_{3(i+1)+1}(x)=\sigma_{3i+1}(x)=\sigma_0(x)\\&\sigma_{3(i+1)+1}(y_1)=\sigma_{3i+1}(y_1)+1=i+1=k\\&\sigma_{3(i+1)+1}(y_2)=\sigma_{3i+1}(y_2)+2=2(i+1)+1=2k+1\\&\sigma_{3(i+1)+1}(y_3)=\sigma_{3i+1}(y_3)+\sigma_{3i+1}(y_2)+2=(i+2)^2=(k+1)^2\end{aligned}$$

因此引理成立。

设 $k=\sqrt{\sigma_0(x)}$

则 $\sigma_{3k+1}(y_3)=(k+1)^2=(\sqrt{\sigma_0(x)}+1)^2>\sigma_0(x)=\sigma_{3k+1}(x)$ 。因此

$$(l_0=beg,\sigma_0)\overset{*}{\Rightarrow}(l_{3k+1},\sigma_{3k+1})\Rightarrow(end,\sigma_{3k+2})$$

且 $\sigma_{3k+2}(y_1)=\sigma_{3k+1}(y_1)=k=\sqrt{\sigma_0(x)}$ 。

例子 4.3.3 ： T91

对于开平方程序

beg:	$(y_1, y_2, y_3) := (0, 1, 1)$ goto test
test:	if $(y_3 \leq x)$ goto loop else goto end
loop:	$(y_1, y_2) := (y_1 + 1, y_2 + 2)$ goto inloop
inloop:	$(y_3) := (y_3 + y_2)$ goto test

其运行过程为如下序列：

$$(beg = l_0, \sigma_0)(test, \sigma_1)(loop, \sigma_2)(inloop, \sigma_3)(test, \sigma_4)(loop, \sigma_5) \cdots\cdots$$

这个例子很简单，只有一个循环。一般来讲，确定程序运行过程有一定的难度。设

$$(B, v) = ((\{0, 1, 2, 3, ..., +, -\}, \{=, >\}), \{x, y_1, y_2, z\})$$
$$LB = \{beg, end, test_1, test_2, upd_1, upd_2, res\}$$

以下是一个带有两个循环的程序，记为 T_{91} 。

beg:	$(y_1, y_2) := (x, 1)$; goto test-1;
test-1:	if $y_1 > 100$ then goto test-2 else upd-1 fi;
test-2:	if $y_2 \neq 1$ then goto upd-2 else res fi;
upd-1:	$(y_1, y_2) := (y_1 + 11, y_2 + 1)$; goto test-1;
upd-2:	$(y_1, y_2) := (y_1 - 10, y_2 - 1)$; goto test-1;
res:	$z := y_1 - 10$; goto end

由于两个循环相互作用，不可能用一个或几个带循环次数参数的序列来表示。虽然简单地罗列程序运行过程有一定的难度，但如果我们略去运行过程中的具体变量状态，我们可以将运行过程表示如下

$$beg, (test_1, ((upd_1)|(test_2, upd_2)))^*, test_1, test_2, res, end$$

但如果我们有方法分析一些关键的标号之间的关系和证明某些性质在一些关键的标号时成立，我们就可以证明程序所具有的性质。以上运行过程也可以写成

$$(beg), ((test_1, upd_1)^*, (test_1, test_2, upd_2)^*)^*, (test_1, test_2, res, end)$$

我们可以考虑以下标号序列

$(beg, test_1)$
$(test_1, test_2, upd_2, test_1)$
$(test_1, upd_1, test_1)$
$(test_1, test_2, res, end)$

我们将标号序列称为路径。假设

$$\forall\sigma.(\varphi(\sigma) \wedge (beg, \sigma) \Rightarrow (test_1, \sigma') \rightarrow \zeta(\sigma'))$$
$$\forall\sigma.(\zeta(\sigma) \wedge (test_1, \sigma) \Rightarrow (test_2, \sigma') \Rightarrow (upd_2, \sigma'') \Rightarrow (test_1, \sigma''') \rightarrow \zeta(\sigma'''))$$
$$\forall\sigma.(\zeta(\sigma) \wedge (test_1, \sigma) \Rightarrow (upd_1, \sigma') \Rightarrow (test_1, \sigma'') \rightarrow \zeta(\sigma''))$$
$$\forall\sigma.(\zeta(\sigma) \wedge (test_1, \sigma) \Rightarrow (test_2, \sigma') \Rightarrow (res, \sigma'') \Rightarrow (end, \sigma''') \rightarrow \psi(\sigma'''))$$

则 $\{\varphi\}T_2\{\psi\}$ 成立。

对于这样的分析，我们有两个方面需要继续讨论的。

第一，挑选路径的方法，即怎样保证我们考虑了所有应该考虑的路径。

第二，路径正确性的证明方法，即怎样证明路径对于给定的公式是正确的。

例子 4.3.2d ： 开平方

设 $I = (NAT, I_0)$ 。用归纳断言方法证明 $\{x = c\}T_1\{y_1 = \sqrt{c}\}$ 。

归纳断言方法：部分正确

证明要点

(1) 确定标号集合 C
(2) 为 C 中每个标号挑选断言
(3) 确定需要证明的路径
(4) 证明路径正确性
证明分四个步骤。

- 确定标号集合 $C = \{beg, test, end\}$ 。
- 挑选断言 q_{beg}, q_{end}, q_{test}

$$\begin{array}{ll} q_{beg} & x = c \\ q_{end} & y_1 = \sqrt{c} \\ q_{test} & x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \end{array}$$

- 确定需要证明的路径

$$\begin{array}{l} (beg, test) \\ (test, loop, inloop, test) \\ (test, end) \end{array}$$

- 证明路径正确性

$$\begin{array}{l} \models_I vc(q_{beg}, (beg, test), q_{test}) \\ \models_I vc(q_{test}, (test, loop, inloop, test), q_{test}) \\ \models_I vc(q_{test}, (test, end), q_{end}) \end{array}$$

例子 4.3.2e1 ： 开平方

证明程序 T_1 在解释 $I = (NAT, I_0)$ 下对于前断言 $x = c \wedge c \geq 0$ 是终止的。

归纳断言方法：终止 (1)

证明要点

(1) 确定标号集合 C 。
(2) 为 C 中每个标号挑选断言
(3) 确定需要证明的路径
(4) 证明路径正确性 (a)
(5) 确定标号集合 C' 。
(6) 挑选 $(W, \sqsubseteq)$
(7) 为 C' 中每个标号挑选函数 $g_c : \Sigma \to W$
(8) 确定需要证明的路径
(9) 证明路径正确性 (b)
证明。

- 确定标号集合 $C = \{beg, test\}$ 。
- 挑选断言 q_{beg}, q_{test}

q_{beg} $\quad x = c \wedge c \geq 0$
q_{test} $\quad x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1$

- 确定需要证明的路径

$$(beg, test)$$
$$(test, loop, inloop, test)$$

- 证明路径正确性

$$\models_I vc(q_{beg}, (beg, test), q_{test})$$
$$\models_I vc(q_{test}, (test, loop, inloop, test), q_{test})$$

- 确定标号集合 $C' = \{test\}$ 。
- 挑选 $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
- 挑选函数 $g_{test} : \Sigma \to W$

$$g_{test}(\sigma) = \sigma(x) + 1 - \sigma(y_3)$$

- 确定需要证明的路径

$$(test, loop, inloop, test)$$

- 证明路径正确性

$I(q_{test})(\sigma) = true \wedge M_I(test, loop, inloop, test)(\sigma) \downarrow$
$\to$
$g_{test}(M_I(test, loop, inloop, test)(\sigma)) < g_{test}(\sigma)$

即（简单起见省略了符号 σ ）

$x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge (y_3 \leq x)$
$\to$
$x + 1 - (y_2 + y_3 + 2) < x + 1 - y_3$

例子 4.3.2e2 ： 开平方

证明程序 T_1 在解释 $I = (INT, I_0)$ 下对于前断言 $x = c \wedge c \geq 0$ 是终止的。

归纳断言方法：终止 (2)

证明。

- 确定标号集合 $C = \{beg, test\}$ 。
- 挑选断言 q_{beg}, q_{test}

$$\begin{array}{ll} q_{beg} & x = c \wedge c \geq 0 \\ q_{test} & y_2 \geq 0 \end{array}$$

- 确定需要证明的路径

$$\begin{array}{l} (beg, test) \\ (test, loop, inloop, test) \end{array}$$

- 证明路径正确性

$$\begin{array}{l} \models_I vc(q_{beg}, (beg, test), q_{test}) \\ \models_I vc(q_{test}, (test, loop, inloop, test), q_{test}) \end{array}$$

- 确定标号集合 $C' = \{test\}$ 。
- 挑选 $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
- 挑选函数 $g_{test} : \Sigma \to W$

$$g_{test}(\sigma) = \begin{cases} \sigma(x) + 1 - \sigma(y_3) & \text{若 } \sigma(y_3) \leq \sigma(x) \\ 0 & \text{否则。} \end{cases}$$

- 确定需要证明的路径

$$(test, loop, inloop, test)$$

- 证明路径正确性

$$\begin{array}{l} I(q_{test})(\sigma) = true \wedge M_I(test, loop, inloop, test)(\sigma) \downarrow \\ \to \\ g_{test}(M_I(test, loop, inloop, test)(\sigma)) < g_{test}(\sigma) \end{array}$$

即

$$\begin{array}{l} y_2 \geq 0 \wedge (y_3 \leq x) \\ \to x + 1 - (y_2 + y_3 + 2) < x + 1 - y_3 \end{array}$$

或

$$\begin{array}{l} y_2 \geq 0 \wedge (y_3 \leq x) \\ \to 0 < x + 1 - y_3 \end{array}$$

例子 4.3.2f1 ： 开平方

证明程序 T_1 在解释 $I = (NAT, I_0)$ 下对于前断言 $x = c \wedge c \geq 0$ 是终止的。

基于谓词公式的终止性证明 (1)

证明要点

(1) 确定标号集合 C 。
(2) 为 C 中每个标号挑选断言 q_c
(3) 确定需要证明的路径
(4) 证明路径正确性 (a)
(5) 确定标号集合 C'
(6) 挑选 $(W \subseteq D, I_0(\sqsubseteq))$ 、挑选 w 并证明 $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$
(7) 为 C 中每个标号挑选项 t_c 并证明 $q_c \to w_x^{t_c}$
(8) 确定需要证明的路径
(9) 证明路径正确性 (b)
证明。

- 确定标号集合 $C = \{beg, test\}$ 。
- 挑选断言 q_{beg}, q_{test}

$$q_{beg} \quad x = c \wedge c \geq 0$$
$$q_{test} \quad x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1$$

- 确定需要证明的路径

$$(beg, test)$$
$$(test, loop, inloop, test)$$

- 证明路径正确性

$$\models_I vc(q_{beg}, (beg, test), q_{test})$$
$$\models_I vc(q_{test}, (test, loop, inloop, test), q_{test})$$

- 确定标号集合 $C' = \{test\}$ 。
- 挑选 $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$

  挑选 $w = true$

  证明 $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$

- 挑选项 $t_{test} = x + 1 - y_3$ 、证明 $q_{test} \to w_x^{t_{test}}$
- 确定需要证明的路径

$$(test, loop, inloop, test)$$

- 证明路径正确性

$$\models_I vc(q_{test} \wedge t_{test} = v, (test, loop, inloop, test), t_{test} < v)$$

即

$$x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge x + 1 - y_3 = v$$
$$\to$$
$$((y_3 \leq x) \to x + 1 - (y_2 + y_3 + 2) < v)$$

例子 4.3.2f2 ： 开平方

证明程序 T_1 在解释 $I = (INT, I_0)$ 下对于前断言 $x = c \wedge c \geq 0$ 是终止的。

基于谓词公式的终止性证明 (2)

证明。

- 确定标号集合 $C = \{beg, test\}$ 。
- 挑选断言 q_{beg}, q_{test}

$$\begin{array}{ll} q_{beg} & x = c \wedge c \geq 0 \\ q_{test} & x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge y_2 \geq 1 \end{array}$$

- 确定需要证明的路径

$$(beg, test)$$
$$(test, loop, inloop, test)$$

- 证明路径正确性

$$\models_I vc(q_{beg}, (beg, test), q_{test})$$
$$\models_I vc(q_{test}, (test, loop, inloop, test), q_{test})$$

- 挑选 $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$

  挑选 $w = (x \geq 0)$

  证明 $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$

- 确定标号集合 $C' = \{test\}$ 。
- 挑选项 $t_{test} = x + 1 - y_3 + y_2$ 、证明 $q_{test} \rightarrow w_x^{t_{test}}$
- 确定需要证明的路径

$$(test, loop, inloop, test)$$

- 证明路径正确性

$$\models_I vc(q_{test} \wedge t_{test} = v, (test, loop, inloop, test), t_{test} < v)$$

即

$$x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge y_2 \geq 1 \wedge x + 1 - y_3 + y_2 = v$$
$$\rightarrow$$
$$((y_3 \leq x) \rightarrow x + 1 - (y_2 + y_3 + 2) + (y_2 + 2) < v)$$

例子 4.4.4：阶乘

以下是一个计算阶乘的结构化程序，记为 T_{jc} 。

$$y := 1;\ \text{while } x > 0 \text{ do } y := y * x; x := x - 1 \text{ od}$$

给定 $a, b \in NAT$ 。定义 $gcd(a, b)$ 如下。

若 $a, b > 0$ 则 $gcd(a, b)$ 为 a, b 的最大公约数；否则 $gcd(a, b)$ 没定义。

以下是一个计算 $gcd(x, y)$ 的程序，记为 T_{gcd} 。

$$\text{while } \neg(x = y) \text{ do if } (x > y) \text{ then } x := x - y \text{ else } y := y - x \text{ fi od}$$

§4.4.1 指称语义

例子 4.4.4a

证明若 $M_I(T_{jc})(\sigma)$ 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 $\mathcal{M}_I^\omega(\text{while } (x > 0) \text{ do } y := y * x; x := x - 1 \text{ od})(\sigma)$ 。

设

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

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

定义 $\Phi : [\Sigma_\omega \to \Sigma_\omega] \to [\Sigma_\omega \to \Sigma_\omega]$ 如下。

$$\Phi(f)(\sigma) = \begin{cases} \omega & \text{若 } \sigma = \omega \\ ite(I(x > 0)(\sigma), f(\mathcal{M}_I^\omega(y := y * x; x := x - 1)(\sigma)), \sigma) & \text{若 } \sigma \neq \omega \end{cases}$$

则

$$\mathcal{M}_I^\omega(T_{jc})(\sigma) = \mu\Phi(\sigma_1)$$

我们需要证明

$$\mu\Phi(\sigma_1)(y) \sqsubseteq \sigma(x)!$$

定义 $g : [\Sigma_\omega \to \Sigma_\omega]$ 如下

$$g(\sigma) = \begin{cases} \omega & \text{若 } \sigma = \omega \\ \sigma[x/0][y/\sigma(x)! \cdot \sigma(y)] & \text{若 } \sigma \neq \omega \end{cases}$$

我们证明 $\mu\Phi \sqsubseteq g$ 。首先我们证明 g 是 Φ 的一个不动点，即 $\Phi(g)(\sigma) = g(\sigma)$ ，如下。

(1) 若 $\sigma = \omega$ ，则 $\Phi(g)(\sigma) = \omega = g(\sigma)$ 。

(2) 若 $\sigma \neq \omega$ 且 $\sigma(x) = 0$ ，则 $\Phi(g)(\sigma) = \sigma = \sigma[x/0][y/\sigma(x)! \cdot \sigma(y)] = g(\sigma)$ 。

(3) 若 $\sigma \neq \omega$ 且 $\sigma(x) > 0$ ，则

$$\begin{aligned} &\Phi(g)(\sigma) \\ &= g(\mathcal{M}_I^\omega(y := y * x; x := x - 1)(\sigma)) \\ &= g(\mathcal{M}_I^\omega(x := x - 1)\mathcal{M}_I^\omega(y := y * x)(\sigma)) \\ &= g(\mathcal{M}_I^\omega(x := x - 1)(\sigma[y/\sigma(y) \cdot \sigma(x)]) \\ &= g(\sigma[y/\sigma(y) \cdot \sigma(x)][x/\sigma(x) - 1]) \end{aligned}$$

设 $\sigma_2 = \sigma[y/\sigma(y) \cdot \sigma(x)][x/\sigma(x) - 1]$ 。则 $g(\sigma_2) = \sigma_2[x/0][y/\sigma_2(x)! \cdot \sigma_2(y)]$ 。

需要证明 $\sigma_2[x/0][y/\sigma_2(x)! \cdot \sigma_2(y)] = \sigma[x/0][y/\sigma(x)! \cdot \sigma(y)]$ 。

需要证明对任意 z ， $\sigma_2[x/0][y/\sigma_2(x)! \cdot \sigma_2(y)](z) = \sigma[x/0][y/\sigma(x)! \cdot \sigma(y)](z)$ 。

若 z 不是 x,y 则两边都等于 $\sigma(z)$ 。若 z 是 x 则两边都等于 0 。若 z 是 y 则两边都等于 $\sigma(x)! \cdot sigma(y)$ 。因此等式成立。

因此 g 是 Φ 的一个不动点。因此

$$\mu\Phi \sqsubseteq g$$

因此

$$\mu\Phi(\sigma_1)(y) \sqsubseteq g(\sigma_1)(y) = \sigma_1(x)! \cdot \sigma_1(y) = \sigma(x)!$$

例子 4.4.4b

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 $M_I(\text{while } (x > 0) \text{ do } S_1 \text{ od})(\sigma_1)(y) = \sigma_1(x)! \cdot \sigma_1(y) = \sigma(x)!$.

例子 4.4.4c

证明 $M_I^{\omega}(T_{jc})$ 处处有定义。

$M_I(T_{jc}) = \mathcal{M}_I^{\omega}(\text{while } (x>0) \text{ do } y := y{*}x; x := x{-}1 od \text{ od}) \circ \mathcal{M}_I^{\omega}(y := 1)$ 。

已知 $\mathcal{M}_I^{\omega}(\text{while } (x>0) \text{ do } y := 1; x := x-1 od \text{ od}) \circ \mathcal{M}_I^{\omega}(y := 1)$ 处处有定义。

定义 $\Phi : [\Sigma_\omega \to \Sigma_\omega] \to [\Sigma_\omega \to \Sigma_\omega]$ 如下。

$$\Phi(f)(\sigma) = \begin{cases} \omega & \text{若 } \sigma = \omega \\ ite(I(x>0)(\sigma), f(\mathcal{M}_I^{\omega}(y := y*x; x := x-1)(\sigma)), \sigma) & \text{若 } \sigma \neq \omega \end{cases}$$

定义 $\Phi' : [\Sigma_\omega \to \Sigma_\omega] \to [\Sigma_\omega \to \Sigma_\omega]$ 如下。

$$\Phi'(f)(\sigma) = \begin{cases} \omega & \text{若 } \sigma = \omega \\ ite(I(x>0)(\sigma), f(\mathcal{M}_I^{\omega}(y := 1; x := x-1)(\sigma)), \sigma) & \text{若 } \sigma \neq \omega \end{cases}$$

只需证明 $\mu\Phi' \circ \mathcal{M}_I^{\omega}(y := 1) \sqsubseteq one \circ \mu\Phi \circ \mathcal{M}_I^{\omega}(y := 1)$

(1) $\Phi'(\bot) \circ \mathcal{M}_I^{\omega}(y := 1) \sqsubseteq one \circ \Phi(\bot) \circ \mathcal{M}_I^{\omega}(y := 1)$

(1a) $x = 0$: $\mathcal{M}_I^{\omega}(y := 1) \sqsubseteq one \circ \mathcal{M}_I^{\omega}(y := 1)$

(1b) $x > 0$: $\bot \circ \mathcal{M}_I^{\omega}(y := 1) \sqsubseteq one \circ \bot \circ \mathcal{M}_I^{\omega}(y := 1)$

(2) 假设

$f' \circ \mathcal{M}_I^{\omega}(y := 1) \sqsubseteq one \circ f \circ \mathcal{M}_I^{\omega}(y := 1)$

那么需要

$\Phi'(f') \circ \mathcal{M}_I^{\omega}(y := 1) \sqsubseteq one \circ \Phi(f) \circ \mathcal{M}_I^{\omega}(y := 1)$

(2a) $x = 0$: $\mathcal{M}_I^{\omega}(y := 1) \sqsubseteq one \circ \mathcal{M}_I^{\omega}(y := 1)$

(2b) $x > 0$: $f'(\mathcal{M}_I^{\omega}(y := 1; x := x-1)) \circ \mathcal{M}_I^{\omega}(y := 1) \sqsubseteq one \circ f(\mathcal{M}_I^{\omega}(y := y := y*x; x := x-1)) \circ \mathcal{M}_I^{\omega}(y := 1)$

$f'(\mathcal{M}_I^{\omega}(y := 1; x := x-1) \circ \mathcal{M}_I^{\omega}(y := 1) \sqsubseteq one \circ f(\mathcal{M}_I^{\omega}(y := y*x; x := x-1) \circ \mathcal{M}_I^{\omega}(y := 1)$

(2b1) $f'(\mathcal{M}_I^{\omega}(y := 1; x := x-1) \circ \mathcal{M}_I^{\omega}(y := 1)(\sigma) = f'(\sigma[y/1][x/\sigma(x)-1]) = f' \circ \mathcal{M}_I^{\omega}(y := 1)(\sigma[x/\sigma(x)-1]) \sqsubseteq one \circ f \circ \mathcal{M}_I^{\omega}(y := 1)(\sigma[x/\sigma(x)-1])$

$one \circ f(\mathcal{M}_I^{\omega}(y := y*x; x := x-1) \circ \mathcal{M}_I^{\omega}(y := 1) = one \circ f(\sigma[y/\sigma(x)][x/\sigma(x)-1])$

需要

$one \circ f \circ \mathcal{M}_I^{\omega}(y := 1)(\sigma[x/\sigma(x)-1]) = one \circ f(\sigma[y/\sigma(x)][x/\sigma(x)-1])$

用归纳法证明

对任意 $f = \Phi^n(\bot)$，任意 z_1, z_2，对任意 y，任意 $x > 0$，$one \circ f(\sigma[y/z_1][x/\sigma(x)-1]) = one \circ f(\sigma[y/z_2][x/\sigma(x)-1])$

用归纳法证明

(a) $\sigma(x) = 1$：

$one \circ \Phi^n(\bot) \circ f(\sigma[y/z_1][x/\sigma(x)-1]) = one \circ f(\sigma[y/z_1][x/\sigma(x)-1]) = \sigma[x/\sigma(x)-1][y/1]$

$one \circ \Phi^n(\bot)(\sigma[y/z_2][x/\sigma(x)-1]) = one(\sigma[y/z_2][x/\sigma(x)-1]) = \sigma[x/\sigma(x)-1][y/1]$

(b) 假设 $\sigma(x) = k$ 成立

证明 $\sigma(x) = k+1$ 成立

(b1) $f = \bot$

$one \circ (\bot)(\sigma[y/z_1][x/\sigma(x) - 1]) = \omega$

$one \circ (\bot)(\sigma[y/z_2][x/\sigma(x) - 1]) = \omega$

(b2)

$one \circ \Phi(f)(\sigma[y/z_1][x/\sigma(x) - 1]) = one \circ f(\sigma[y/z_1 * (\sigma(x) - 1)][x/\sigma(x) - 2])$

$one \circ \Phi(f)(\sigma[y/z_2][x/\sigma(x) - 1]) = one \circ f(\sigma[y/z_2 * (\sigma(x) - 1)][x/\sigma(x) - 2])$

§4.4.2 Hoare 逻辑

例子 4.4.5 ： 公式

理解 $\mathcal{I}(\{p\}T\{q\})(\sigma) = true$ 的涵义

$\mathcal{I}(\{x > 5\}x := 2 * x\{x > 10\})(\sigma) = true$
$\mathcal{I}(x > 5)(\sigma) \to I(x > 10)(M_I(x := 2 * x)(\sigma)) = true$
$\sigma(x) > 5 \to I(x > 10)(\sigma[x/2 * \sigma(x)]) = true$
$\sigma(x) > 5 \to 2 * \sigma(x) > 10 = true$

$\mathcal{I}(\{x > 5\}x := 2 * x\{x > 20\})(\sigma) = true$
$\mathcal{I}(x > 5)(\sigma) \to I(x > 20)(M_I(x := 2 * x)(\sigma)) = true$
$\sigma(x) > 5 \to I(x > 20)(\sigma[x/2 * \sigma(x)]) = true$
$\sigma(x) > 5 \to 2 * \sigma(x) > 20 = true$
$\sigma(x) \leq 5 \vee \sigma(x) > 10$

$\mathcal{I}(\{true\}\text{while } x \neq 10 \text{ do } x := x + 1 \text{ od}\{x = 10\})(\sigma)$=$true$

$\mathcal{I}(\{true\}x := y + 1\{x > y\})(\sigma) = true$
$I(x > y)(M_I(x := y + 1)(\sigma)) = true$
$I(x > y)(\sigma[x/\sigma(y) + 1]) = true$
$I(y + 1 > y)\sigma$
$y + 1 > y \models \{true\}x := y + 1\{x > y\}$

例子 4.4.4d ： 阶乘

定义 T_{jc} 如下：

$$y := 1; \text{ while } x > 0 \text{ do } y := y * x; x := x - 1 \text{ od}$$

证明 $PA \vdash \{x = n \wedge x \geq 0\} T_{jc} \{y = n!\}$ 。
将程序分为两个部分，记为 S_1, S_2 。
我们有

$$\{x = n \wedge x \geq 0\} S_1 \{x = n \wedge x \geq 0 \wedge y = 1\}$$

根据顺序复合规则，还需要证明

$$\{x = n \wedge x \geq 0 \wedge y = 1\} S_2 \{y = x!\}$$

我们有

$$\{y * x * (x-1)! = n!\} y := y * x \{y * (x-1)! = n!\}$$
$$\{y * (x-1)! = n!\} x := x - 1 \{y * x! = n!\}$$

因此

$$\{y * x * (x-1)! = n!\} y := y * x; x := x - 1 \{y * x! = n!\}$$

又有

$$(y * x! = n!) \wedge x > 0 \rightarrow y * x * (x-1)! = n!$$

且

$$x = n \wedge x \geq 0 \wedge y = 1 \rightarrow (y * x! = n!)$$
$$(y * x! = n!) \wedge \neg(x > 0) \rightarrow y = x!$$

因此根据循环规则，有

$$\{x = n \wedge x \geq 0 \wedge y = 1\} S_2 \{y = x!\}$$

例子 4.4.4e

证明

$\{x = n \wedge y = 1\}$
while $x > 0$ do $y := y * x; x := x - 1$ od
$\{y = n!\}$

设 r 为 $y' = x! * y$.
根据规则需证

$\neg x > 0 \rightarrow y = x! * y$
$\{x > 0 \wedge \neg y' = x! * y\}$y:=y*x; x:=x-1$\{\neg y' = x! * y\}$
$(x = n \wedge y = 1 \wedge y' = x! * y) \rightarrow y' = n!$

扩展的 Hoare 逻辑

例子 4.4.4f

证明 $PA \vdash [x \geq 0]T_{jc}[y = x!]$ 。
将程序分为两个部分，记为 S_1, S_2 。
我们有

$$[x = n \wedge x \geq 0]S_1[x = n \wedge x \geq 0 \wedge y = 1]$$

根据顺序复合规则，还需要证明

$$[x = n \wedge x \geq 0 \wedge y = 1]S_2[y = x!]$$

取 $w = true$ ， $t = x$
我们有

$$[y * x * (x-1)! = n! \wedge x - 1 < a]y := y * x[y * (x-1)! = n! \wedge x - 1 < a]$$
$$\{y * (x-1)! = n! \wedge x - 1 < a\}x := x - 1\{y * x! = n! \wedge x < a\}$$

因此

$$[y * x * (x-1)! = n! \wedge x - 1 < a]y := y * x; x := x - 1[y * x! = n!]$$

又有

$$(y * x! = n!) \wedge x > 0 \wedge x = a \rightarrow y * x * (x-1)! = n! \wedge x - 1 < a$$

且

$$(y * x! = n!) \wedge x > 0 \rightarrow w[x/x]$$

因此根据循环规则，有

$$[y * x! = n!]S_2[y * x! = n! \wedge \neg(x > 0)]$$

又有

$$x = n \wedge x \geq 0 \wedge y = 1 \rightarrow (y * x! = n!)$$
$$(y * x! = n!) \wedge \neg(x > 0) \rightarrow y = x!$$

因此

$$[x = n \wedge x \geq 0 \wedge y = 1]S_2[y = x!]$$

例子 4.5.2 ：开平方

带有前断言、后断言和循环不变式的 XYZ/SE 格式的程序：

{x=c}
%PROC wl(%INP/x:INT;%IOP/y1:INT)==
%LOC [y2,y3:INT]
%STM [
LB=START => $Oy1=0 ∧ $Oy2=1 ∧ $Oy3=1 ∧ $OLB=l2;
*[
LB=l2 ∧ (le(y3,x)) => ($OLB=l3 | $OLB=END)
LB=l3 => $Oy1=+(y1,1) ∧ $Oy2 = +(y2,2) ∧ $OLB=l4;
LB=l4 => $Oy3=+(y2,y3) ∧ $OLB=l2;
$\{x = c \wedge le(*(y1, y1), x) \wedge y3 = *(+(y1, 1), +(y1, 1)) \wedge y2 = +(*(2, y1), 1)\}$
]
]
$\{le(*(y1, y1), c) \wedge lt(c, *(+(y1, 1), +(y1, 1)))\}$

为阅读方便，我们 $le, lt, +, *$ 等表示为我们熟悉的写法。由这个程序，我们可以用 XYZ/VERI-II 获取以下验证条件

$y3 \le x \wedge x = c \wedge y1 * y1 \le x \wedge y3 = (y1 + 1) * (y1 + 1) \wedge y2 = 2 * y1 + 1$
$\rightarrow$
$x = c \wedge (y1 + 1) * (y1 + 1) \le x$
$\wedge (y2 + 2) + y3 = ((y1 + 1) + 1) * ((y1 + 1) + 1)$
$\wedge y2 + 2 = 2 * (y1 + 1) + 1$
$\neg y3 \le x \wedge x = c \wedge y1 * y1 \le x \wedge y3 = (y1 + 1) * (y1 + 1) \wedge y2 = 2 * y1 + 1$
$\rightarrow$
$y1 * y1 \le c \wedge c < (y1 + 1) * (y1 + 1)$
$x = c$
$\rightarrow x = c \wedge 0 * 0 \le x \wedge 1 = (0 + 1) * (0 + 1) \wedge 1 = 2 * 0 + 1$

通过自动化简得到以下条件：

$(y1 + 1) * (y1 + 1) \le c, y1 * y1 \le c \rightarrow 2 + (1 + y1 * 2) = 1 + 2 * (y1 + 1)$
$y1 * y1 \le c \rightarrow c < (y1 + 1) * (y1 + 1), (y1 + 1) * (y1 + 1) \le c$
$T \rightarrow 1 = 1 + 2 * 0$
$(y1 + 1) * (y1 + 1) \le c, y1 * y1 \le c$
$\rightarrow (2 + (1 + y1 * 2)) + (y1 + 1) * (y1 + 1) = (1 + (y1 + 1)) * (1 + (y1 + 1))$
$T \rightarrow 0 * 0 \le c$
$T \rightarrow 1 = (1 + 0) * (1 + 0)$