

§4 推理验证

§4.1 一阶迁移系统的推理

例子: 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

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

主要适用规则

主要适用规则如下

$$\frac{\zeta \Rightarrow \varphi' \quad \{\varphi'\}T\{\varphi'\} \quad \varphi' \Rightarrow \varphi}{\zeta \Rightarrow \Box\varphi}$$

尝试

令

$$\zeta \equiv (x > 0 \wedge a = s_0)$$

$$\varphi \equiv (a = s_4 \rightarrow y_1 = \sqrt{x})$$

$$\varphi' \equiv (a = s_0 \wedge \varphi_0) \vee (a = s_1 \wedge \varphi_1) \vee (a = s_2 \wedge \varphi_2) \vee (a = s_3 \wedge \varphi_3) \vee (a = s_4 \wedge \varphi_4)$$

其中 φ' 为

$$\varphi_0 \equiv (x > 0)$$

$$\varphi_1 \equiv (y_1^2 \leq x \wedge y_2 = 2 * y_1 + 1 \wedge y_3 = (y_1 + 1)^2)$$

$$\varphi_2 \equiv ((y_1 + 1)^2 \leq x \wedge y_2 = 2 * y_1 + 1 \wedge y_3 = (y_1 + 1)^2)$$

$$\varphi_3 \equiv (y_1^2 \leq x \wedge y_2 = 2 * y_1 + 1 \wedge y_3 = y_1^2)$$

$$\varphi_4 \equiv (y_1 = \sqrt{x})$$

$$\equiv (y_1^2 \leq x \wedge x < (y_1 + 1)^2)$$

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

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

主要适用规则

主要适用规则如下

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

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

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

需要

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

§4.2 流程图程序的推理

例子

设

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

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

部分正确

Example 4.1 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 $\varphi'(\sigma_{n-1})$ 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

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

成立。

- 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

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

因此

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

因此

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

因此对任意 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。

终止

Example 4.2 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

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

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

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

因此 $k = i + 1$ 时有

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

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。

完全正确

Example 4.3 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

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

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

基于路径的推理

Example 4.4 以下是一个带有两个循环的程序。

```

beg:   (y1, y2) := (x, 1); goto test-1;
test-1: if y1 > 100 then goto test-2 else upd-1 fi;
test-2: if y2 ≠ 1 then goto upd-2 else res fi;
upd-1:  (y1, y2) := (y1 + 11, y2 + 1); goto test-1;
upd-2:  (y1, y2) := (y1 - 10, y2 - 1); goto test-1;
res:   z := y1 - 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

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

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。

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

Example 4.5 设 $I = (NAT, I_0)$ 。用归纳断言方法证明 $\{x = c\}T_1\{y_1 = \sqrt{c}\}$ 。

证明分四个步骤。

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

$$q_{beg} \quad x = c$$

$$q_{end} \quad y_1 = \sqrt{c}$$

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

- 确定需要证明的路径

$$(beg, test)$$

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

$$(test, end)$$

- 证明路径正确性

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

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 $g_c : \Sigma \rightarrow W$
- (8) 确定需要证明的路径
- (9) 证明路径正确性 (b)

Example 4.6 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。

证明。

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

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

- 确定需要证明的路径

$$\begin{aligned} & (beg, test) \\ & (test, loop, inloop, test) \end{aligned}$$

- 证明路径正确性

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

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

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

- 确定需要证明的路径

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

- 证明路径正确性

$$\begin{aligned}
I(q_{test})(\sigma) &= true \wedge M_I(test, loop, inloop, test)(\sigma) \downarrow \\
&\rightarrow \\
g_{test}(M_I(test, loop, inloop, test)(\sigma)) &< g_{test}(\sigma)
\end{aligned}$$

即 (简单起见省略了符号 σ)

$$\begin{aligned}
x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1 + 1)^2 \wedge y_2 = 2 * y_1 + 1 \wedge (y_3 \leq x) \\
\rightarrow \\
x + 1 - (y_2 + y_3 + 2) < x + 1 - y_3
\end{aligned}$$

归纳断言方法: 终止 (2)

Example 4.7 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。

证明。

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

$$\begin{aligned}
q_{beg} \quad x = c \wedge c \geq 0 \\
q_{test} \quad y_2 \geq 0
\end{aligned}$$

- 确定需要证明的路径

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

- 证明路径正确性

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

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

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

- 确定需要证明的路径

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

- 证明路径正确性

$$\begin{aligned}
I(q_{test})(\sigma) &= true \wedge M_I(test, loop, inloop, test)(\sigma) \downarrow \\
&\rightarrow \\
g_{test}(M_I(test, loop, inloop, test)(\sigma)) &< g_{test}(\sigma)
\end{aligned}$$

即

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

或

$$\begin{aligned}
y_2 \geq 0 \wedge (y_3 \leq x) \\
\rightarrow 0 < x + 1 - y_3
\end{aligned}$$

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 $q_c \rightarrow w_x^{t_c}$
- (8) 确定需要证明的路径
- (9) 证明路径正确性 (b)

Example 4.8 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。

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 $(W, \sqsubseteq) = (\{0, 1, 2, \dots\}, \leq)$

$$\text{挑选 } w = true$$

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

- 挑选项 $t_{test} = x + 1 - y_3$ 、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

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

\rightarrow

$$((y_3 \leq x) \rightarrow x + 1 - (y_2 + y_3 + 2) < v)$$

基于谓词公式的终止性证明 (2)

Example 4.9 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。

证明。

- 确定标号集合 $C = \{beg, test\}$ 。

- 挑选断言 q_{beg}, q_{test}

$$q_{beg} \quad x = c \wedge c \geq 0$$

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

- 确定需要证明的路径

$$(beg, test)$$

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

- 证明路径正确性

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

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

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

$$\text{挑选 } w = (x \geq 0)$$

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

- 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

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

→

$$((y_3 \leq x) \rightarrow x + 1 - (y_2 + y_3 + 2) + (y_2 + 2) < v)$$

§4.3 结构化程序的推理

例子: 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} 。

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

§4.3.1 指称语义

例子 (1)

Example 4.10 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 $\Phi: [\Sigma_\omega \rightarrow \Sigma_\omega] \rightarrow [\Sigma_\omega \rightarrow \Sigma_\omega]$ 如下。

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

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 $g: [\Sigma_\omega \rightarrow \Sigma_\omega]$ 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 $\sigma(x)! \cdot \text{sigma}(y)$ 。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 (2)

Example 4.11 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 $\mathcal{M}_I^\omega(\text{while } (x > 0) \text{ do } y := y * x; x := x - 1 \text{ od})(\sigma)$ 。设

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

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

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

定义

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

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

若 $I(x > 0)(\sigma) = \text{true}$, $M_I(S_1)(\sigma) \downarrow$ 且 $\varphi(M_I(S_1)(\sigma), \sigma') = \text{true}$, 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 $\varphi(\sigma, \sigma') = \text{true}$ 。

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

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

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 (3)

Example 4.12 证明 $M_I^\omega(T_{jc})$ 处处有定义。

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

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

定义 $\Phi: [\Sigma_\omega \rightarrow \Sigma_\omega] \rightarrow [\Sigma_\omega \rightarrow \Sigma_\omega]$ 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 $\Phi' : [\Sigma_\omega \rightarrow \Sigma_\omega] \rightarrow [\Sigma_\omega \rightarrow \Sigma_\omega]$ 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 $\mu\Phi' \circ \mathcal{M}_I^\omega(y := 1) \sqsubseteq one \circ \mu\Phi \circ \mathcal{M}_I^\omega(y := 1)$

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

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

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

(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

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

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

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

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

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

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

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

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

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

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

$$one \circ f(\sigma[y/\sigma(x)][x/\sigma(x) - 1])$$

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 $f = \Phi^n(\perp)$, 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) $\sigma(x) = 1$:

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

$$1]) = \sigma[x/\sigma(x) - 1][y/1]$$

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

$$1]) = \sigma[x/\sigma(x) - 1][y/1]$$

(b) 假设 $\sigma(x) = k$ 成立

证明 $\sigma(x) = k + 1$ 成立

(b1) $f = \perp$

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

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

(b2)

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

$$(\sigma(x) - 1)][x/\sigma(x) - 2])$$

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

$$(\sigma(x) - 1)][x/\sigma(x) - 2])$$

§4.3.2 Hoare 逻辑

例子

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

$$\begin{aligned}
\mathcal{I}(\{x > 5\}x := 2 * x\{x > 10\})(\sigma) &= true \\
\mathcal{I}(x > 5)(\sigma) \rightarrow \mathcal{I}(x > 10)(M_I(x := 2 * x)(\sigma)) &= true \\
\sigma(x) > 5 \rightarrow \mathcal{I}(x > 10)(\sigma[x/2 * \sigma(x)]) &= true \\
\sigma(x) > 5 \rightarrow 2 * \sigma(x) > 10 &= true
\end{aligned}$$

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

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

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

例子

定义 T_{jc} 如下:

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

例子

Example 4.13 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

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

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

$$\begin{aligned} x = n \wedge x \geq 0 \wedge y = 1 \rightarrow (y * x! = n!) \\ (y * x! = n!) \wedge \neg(x > 0) \rightarrow y = x! \end{aligned}$$

因此根据循环规则，有

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

例子

证明

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

设 r 为 $y' = x! * y$.

根据规则需证

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

扩展的 Hoare 逻辑

Example 4.14 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

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

§4.4 工具

例子: 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 w1(%INP/x:INT;%IOP/y1:INT)==
%LOC [y2,y3:INT]
%STM [
  LB=START => $Oy1=0 ^ $Oy2=1 ^ $Oy3=1 ^ $OLB=12;
  * [
    LB=12 ^ (le(y3,x)) => ($OLB=13 | $OLB=END)
    LB=13 => $Oy1=+(y1,1) ^ $Oy2 = +(y2,2) ^ $OLB=14;
    LB=14 => $Oy3=+(y2,y3) ^ $OLB=12;
    {x = c ^ le(*(y1, y1), x) ^ y3 = *(+(y1, 1), +(y1, 1)) ^ y2 = +( *(2, y1), 1)}
  ]
]
{le(*(y1, y1), c) ^ 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

$$y3 \leq x \wedge x = c \wedge y1 * y1 \leq x \wedge y3 = (y1 + 1) * (y1 + 1) \wedge y2 = 2 * y1 + 1$$

→

$$x = c \wedge (y1 + 1) * (y1 + 1) \leq x$$

$$\wedge (y2 + 2) + y3 = ((y1 + 1) + 1) * ((y1 + 1) + 1)$$

$$\wedge y2 + 2 = 2 * (y1 + 1) + 1$$

$$\neg y3 \leq x \wedge x = c \wedge y1 * y1 \leq x \wedge y3 = (y1 + 1) * (y1 + 1) \wedge y2 = 2 * y1 + 1$$

→

$$y1 * y1 \leq c \wedge c < (y1 + 1) * (y1 + 1)$$

$$x = c$$

$$\rightarrow x = c \wedge 0 * 0 \leq x \wedge 1 = (0 + 1) * (0 + 1) \wedge 1 = 2 * 0 + 1$$

通过自动化简得到以下条件:

$$(y1 + 1) * (y1 + 1) \leq c, y1 * y1 \leq c \rightarrow 2 + (1 + y1 * 2) = 1 + 2 * (y1 + 1)$$

$$y1 * y1 \leq c \rightarrow c < (y1 + 1) * (y1 + 1), (y1 + 1) * (y1 + 1) \leq c$$

$$T \rightarrow 1 = 1 + 2 * 0$$

$$(y1 + 1) * (y1 + 1) \leq c, y1 * y1 \leq c$$

$$\rightarrow (2 + (1 + y1 * 2)) + (y1 + 1) * (y1 + 1) = (1 + (y1 + 1)) * (1 + (y1 + 1))$$

$$T \rightarrow 0 * 0 \leq c$$

$$T \rightarrow 1 = (1 + 0) * (1 + 0)$$
