§4　推理验证方法

§4.1　一阶迁移系统的推理

习题：　设 $B=(\{x,y,n,a\},\{s_0,s_1,s_2,s_3,s_4,0,1,2,3,...,+,-,*\},\{<,=,>\})$。给定 B 上的迁移系统 (T,Θ)，其中 Θ 为 $a=s_0$ 且 T 为以下迁移：

$a=s_0$	$\longrightarrow$	$(x,y,a):=(0,0,s_1)$
$a=s_1\wedge x<n$	$\longrightarrow$	$(a):=(s_2)$
$a=s_2$	$\longrightarrow$	$(y,x,a):=(y+x*(x+1),x+1,s_1)$
$a=s_1\wedge\neg(x<n)$	$\longrightarrow$	$(a):=(s_3)$
$a=s_3$	$\longrightarrow$	$(y,a):=(3*y,s_4)$

给定 I 为 B 在整数上的正常解释。证明以下命题成立：

(1)	$(T,\Theta)\vdash_I n\geq 0\rightarrow\Box(a=s_4\rightarrow y=n*n*n-n)$
(2)	$(T,\Theta)\vdash_I n\geq 0\rightarrow\Diamond(a=s_4)$

证明 (1)

考虑证明

$$(T,\Theta)\vdash_I n\geq 0\wedge a=s_0\Rightarrow\Box(a=s_4\rightarrow y=n*n*n-n)\qquad(a)$$

有 (a) 则有

$$(T,\Theta)\vdash_I n\geq 0\wedge a=s_0\rightarrow\Box(a=s_4\rightarrow y=n*n*n-n)$$

由于

$$(T,\Theta)\vdash_I a=s_0$$

因此

$$(T,\Theta)\vdash_I n\geq 0\rightarrow\Box(a=s_4\rightarrow y=n*n*n-n)$$

用 $\Box$ 规则：

$$\frac{\begin{array}{l}\zeta\Rightarrow\varphi\\ \forall t\in T,\{\varphi\}t\{\varphi\}\\ \varphi\Rightarrow\varphi'\end{array}}{\zeta\Rightarrow\Box\varphi'}$$

令

$$\begin{array}{rcl}\zeta & = & (a=s_0\wedge n\geq 0)\\ \varphi & = & (a=s_0\wedge n\geq 0)\vee\\ & & (a=s_1\wedge 3*y=(x*x*x-x)\wedge x\leq n)\vee\\ & & (a=s_2\wedge 3*y=(x*x*x-x)\wedge x<n)\vee\\ & & (a=s_3\wedge 3*y=(x*x*x-x)\wedge x=n)\vee\\ & & (a=s_4\wedge y=(n*n*n-n))\\ \varphi' & = & (a=s_4\rightarrow y=(n*n*n-n))\end{array}$$

证明 (2)

用

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

定义 g

$$\begin{array}{l} g(s_0, x) = 2 * n + 2\\ g(s_1, x) = 2 * (n - x) + 1\\ g(s_2, x) = 2 * (n - x)\\ g(s_3, x) = 2 * (n - x)\\ g(s_4, x) = 2 * (n - x)\end{array}$$

令

$$\begin{array}{rcl} W & = & (\{0, 1, 2, 3, ...\}, \leq)\\ w & = & (0 \leq x)\\ e & = & g(a, x)\\ \varphi & = & (a = s_0 \wedge n \geq 0)\\ \psi & = & (a = s_4)\\ \zeta & = & (n \geq 0) \wedge\\ & & ((a = s_0) \vee ((x \leq n) \wedge (a = s_1 \vee a = s_3 \vee a = s_4)) \vee\\ & & ((x < n) \wedge a = s_2))\end{array}$$

需要

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

我们有 $\varphi \Rightarrow (\psi \vee \zeta)$

我们有 $\zeta \Rightarrow (COND_T \vee \psi)$

我们有 $\zeta \Rightarrow w_x^e$。即 $(n \geq 0) \wedge ((a = s_0) \vee ((x \leq n) \wedge (a = s_1 \vee a = s_3 \vee a = s_4)) \vee ((x < n) \wedge a = s_2)) \Rightarrow g(a, x) \geq 0$。

以下验证

$\forall t \in T, \{\zeta \wedge e = v\}t\{\psi \vee (\zeta \wedge e < v)\}$。

(1)

$\{\zeta \wedge e = v\}a = s_0 \longrightarrow (x, y, a) := (0, 0, s_1)\{\psi \vee (\zeta \wedge e < v)\}$

只需：

$\zeta \wedge g(a, x) = v \wedge a = s_0 \rightarrow n \geq 0 \wedge x \leq n \wedge g(s_1, 0) < v)\}$

只需：

$n \geq 0 \wedge g(s_0, x) = v \rightarrow n \geq 0 \wedge 0 \leq n \wedge g(s_1, 0) < v)\}$

(2)

$\{\zeta \wedge e = v\}a = s_1 \wedge x < n \longrightarrow (a) := (s_2)\{\psi \vee (\zeta \wedge e < v)\}$

只需：

$\zeta \wedge g(a, x) = v \wedge a = s_1 \wedge x < n \rightarrow n \geq 0 \wedge x < n \wedge g(s_2, x) < v)\}$

只需：

$n \geq 0 \wedge x \leq n \wedge g(s_0, x) = v \wedge x < n \rightarrow n \geq 0 \wedge x < n \wedge g(s_1, x) < v)\}$

(3)

$\{\zeta \wedge e = v\}a = s_2 \longrightarrow (y, x, a) := (y + x * (x + 1), x + 1, s_1)\{\psi \vee (\zeta \wedge e < v)\}$

只需：

$\zeta \wedge g(a, x) = v \wedge a = s_2 \rightarrow n \geq 0 \wedge x + 1 \leq n \wedge g(s_1, x + 1) < v)\}$

只需：

$n \geq 0 \wedge x < n \wedge g(s_2, x) = v \rightarrow n \geq 0 \wedge x < n \wedge g(s_1, x + 1) < v)\}$

(4)

$\{\zeta \wedge e = v\}a = s_1 \wedge \neg(x < n) \longrightarrow (a) := (s_3)\{\psi \vee (\zeta \wedge e < v)\}$

只需：

$\zeta \wedge g(a, x) = v \wedge a = s_1 \wedge \neg(x < n) \rightarrow n \geq 0 \wedge x \leq n \wedge g(s_3, x) < v)\}$

只需：

$n \geq 0 \wedge x \leq n \wedge g(s_1, x) = v \wedge \neg(x < n) \rightarrow n \geq 0 \wedge x \leq n \wedge g(s_3, x) < v)\}$

(5)

$\{\zeta \wedge e = v\}a = s_3 \longrightarrow (y, a) := (3 * y, s_4)\{\psi \vee (\zeta \wedge e < v)\}$

只需：

$\zeta \wedge g(a, x) = v \wedge a = s_3 \rightarrow s_4 = s_4$

§4.2 流程图程序的推理

习题： 设

$$B = (\{x, y, n, a\}, \{0, 1, 2, 3, ..., +, -, *\}, \{<, =, >\})$$

给定程序 T：

beg:	$(x, y) := (0, 0)$ goto l_1
l_1:	if $(x < n)$ goto l_2 else goto l_3
l_2:	$(y, x) := (y + x * (x + 1), x + 1)$ goto l_1
l_3:	$(y) := (3 * y)$ goto end

给定 I 为 B 在整数上的正常解释。证明以下命题成立：

(1) T 对于前断言 $n \geq 0$ 和后断言 $y = n * n * n - n$ 部分正确。
(2) T 对于前断言 $n \geq 0$ 能够终止。
(3) T 对于前断言 $n \geq 0$ 和后断言 $y = n * n * n - n$ 完全正确。

证明 (1)

假设程序运行过程如下：

$$(beg, \sigma_0)(l_1, \sigma_1)(l_2, \sigma_2)(l_1, \sigma_3)(l_2, \sigma_4) \cdots (l_1, \sigma_{k-2})(l_3, \sigma_{k-1})(end, \sigma_k) \cdots$$

我们有

$\sigma_k(y) = 3 * \sigma_{k-1}(y)$

$\sigma_k(n) = \sigma_{k-1}(n)$

只要证明 $3*\sigma_{k-1}(y) = \sigma_{k-1}(n) * \sigma_{k-1}(n) * \sigma_{k-1}(n) - \sigma_{k-1}(n)$

只要证明 $3*\sigma_{k-1}(y) = \sigma_{k-1}(x) * \sigma_{k-1}(x) * \sigma_{k-1}(x) - \sigma_{k-1}(x) \wedge \sigma_{k-1}(x) = \sigma_{k-1}(n)$

我们有

$\sigma_{k-1}(y) = \sigma_{k-2}(y)$

$\sigma_{k-1}(n) = \sigma_{k-2}(n)$ 且

$\sigma_{k-2}(x) \geq \sigma_{k-2}(n)$

只要证明

$\sigma_{k-2}(y) = \sigma_{k-2}(x) * \sigma_{k-2}(x) * \sigma_{k-2}(x) - \sigma_{k-2}(x) \wedge$

$\sigma_{k-2}(x) \leq \sigma_{k-2}(n)$

根据运行过程，存在 $i \geq 0$, $\sigma_{k-2} = \sigma_{2*i+1}$

用归纳法证明，对所有 $i \geq 0$,

$\sigma_{2i+1}(y) = \sigma_{2i+1}(x) * \sigma_{2i+1}(x) * \sigma_{2i+1}(x) - \sigma_{2i+1}(x) \wedge$

$\sigma_{2i+1}(x) \leq \sigma_{2i+1}(n)$

证明 (2)

假设程序运行不终止，过程如下：

$$(beg, \sigma_0)(m_1, \sigma_1)(m_2, \sigma_2)(m_3, \sigma_3)(m_4, \sigma_4) \cdots (m_{2i+1}, \sigma_3)(m_{2i+2}, \sigma_4) \cdots$$

我们有

$m_{2i+1} = l_1$, $m_{2i+2} = l_2$ 且 $\sigma_{2i+1}(x) < \sigma_{2i+1}(n)$

用归纳法证明，对所有 $i \geq 0$,

$\sigma_{2i+1}(n) = \sigma_0(n)$, $\sigma_{2i+1}(x) = i$

取 $i = \sigma_0(n)$, 则 $\sigma_{2i+1}(x) \geq \sigma_0(n) = \sigma_{2i+1}(n)$

与程序不终止矛盾。

证明 (3)

（或者只是说前两项相结合即证明了第三项）

首先证明引理：对所有 $0 \leq i \leq \sigma_0(n)$ ，

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

且

$\sigma_{2i+1}(n) = \sigma_0(n)$

$\sigma_{2i+1}(x) = i$

$\sigma_{2i+1}(y) = (i * i * i - i)/3$

那么

设 $i = \sigma_0(n)$

则 $\sigma_{2i+1}(x) = \sigma_{2i+1}(n)$ 。

因此

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

且 $\sigma_{2i+3}(y) = 3 * \sigma_{2i+2}(y) = 3 * \sigma_{2i+1}(y) = (i * i * i - i) = \sigma_0(n)^3 - \sigma_0(n)$ 。

习题： 设

$$B = (\{x, y, n, a\}, \{0, 1, 2, 3, ..., +, -, *\}, \{<, =, >\})$$

给定以下 $\mathcal{L}_1^B$ 中的程序 T ：

beg:	$(i,j,k,l) := (1,0,0,1)$ goto l_1
l_1:	if $\neg(x=y)$ goto l_2 else goto end
l_2:	if $(x>y)$ goto l_3 else goto l_4
l_3:	$(x,i,j) := (x-y, i-k, j-l)$ goto l_1
l_4:	$(y,k,l) := (y-x, k-i, l-j)$ goto l_1

给定 I 为 B 在整数上的正常解释。证明以下命题成立：

(1) T 对于前断言 $x=a \wedge y=b \wedge a \geq 0 \wedge b \geq 0$ 和后断言 $x=gcd(a,b) \wedge x = i*a+j*b$ 部分正确。

(2) T 对于前断言 $x=a \wedge y=b \wedge a \geq 0 \wedge b \geq 0$ 能够终止。

证明 (1)

- 确定标号集合 $C=\{beg, l_1, end\}$ 。
- 挑选断言 q_{beg}, q_{l_1}, q_{end}

q_{beg}	$x=a \wedge y=b \wedge a \geq 0 \wedge b \geq 0$
q_{l_1}	$x=i*a+j*b \wedge y=k*a+l*b \wedge gcd(x,y)=gcd(a,b)$
q_{end}	$x=gcd(a,b) \wedge x=i*a+j*b$

- 确定需要证明的路径

$$(beg, l_1)$$
$$(l_1, l_2, l_3, l_1)$$
$$(l_1, l_2, l_4, l_1)$$
$$(l_1, end)$$

- 证明路径正确性

$$\models_I vc(q_{beg}, (beg, l_1), q_{l_1})$$
$$\models_I vc(q_{l_1}, (l_1, l_2, l_3, l_1), q_{l_1})$$
$$\models_I vc(q_{l_1}, (l_1, l_2, l_4, l_1), q_{l_1})$$
$$\models_I vc(q_{l_1}, (l_1, end), q_{end})$$

a. 即

$$x=a \wedge y=b \wedge a \geq 0 \wedge b \geq 0 \rightarrow [x=i*a+j*b \wedge y=k*a+l*b \wedge gcd(x,y)=gcd(a,b)]^{1,0,0,1}_{i,j,k,l}$$

b. 即

$$x=i*a+j*b \wedge y=k*a+l*b \wedge gcd(x,y)=gcd(a,b) \rightarrow$$
$$\neg x=y \rightarrow x>y \rightarrow [x=i*a+j*b \wedge y=k*a+l*b \wedge gcd(x,y)=gcd(a,b)]^{x-y,i-k,j-l}_{x,i,j}$$

c. 即

$$x=i*a+j*b \wedge y=k*a+l*b \wedge gcd(x,y)=gcd(a,b) \rightarrow$$
$$\neg x=y \rightarrow \neg x>y \rightarrow [x=i*a+j*b \wedge y=k*a+l*b \wedge gcd(x,y)=gcd(a,b)]^{y-x,k-i,l-j}_{x,k,l}$$

d. 即

$$x=i*a+j*b \wedge y=k*a+l*b \wedge gcd(x,y)=gcd(a,b) \rightarrow$$
$$\neg(\neg x=y) \rightarrow x=gcd(a,b) \wedge x=i*a+j*b$$

证明 (2a)

- 确定标号集合 $C = \{beg, l_1\}$ 。
- 挑选断言 q_{beg}, q_{l_1}

$$\begin{array}{ll} q_{beg} & x = a \wedge y = b \wedge a > 0 \wedge b > 0 \\ q_{l_1} & x > 0 \wedge y > 0 \end{array}$$

- 挑选 $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
- 令 $w = (x \geq 0)$ 则 $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$
- 确定标号集合 $C' = \{l_1\}$ 。
- 令 $t_{l_1} = x + y$ 则 $q_{l_1} \rightarrow w_x^{t_{l_1}}$
- 确定需要证明的路径

$$\begin{array}{l} (beg, l_1) \\ (l_1, l_2, l_3, l_1) \\ (l_1, l_2, l_4, l_1) \end{array}$$

- 证明路径正确性

$$\begin{array}{l} \models_I vc(q_{beg}, (beg, l_1), q_{l_1}) \\ \models_I vc(q_{l_1}, (l_1, l_2, l_3, l_1), q_{l_1}) \\ \models_I vc(q_{l_1}, (l_1, l_2, l_4, l_1), q_{l_1}) \end{array}$$

- 确定需要证明的路径

$$\begin{array}{l} (l_1, l_2, l_3, l_1) \\ (l_1, l_2, l_4, l_1) \end{array}$$

- 证明路径正确性

$$\begin{array}{l} \models_I vc(q_{l_1} \wedge t_{l_1} = v, (l_1, l_2, l_3, l_1), t_{l_1} < v) \\ \models_I vc(q_{l_1} \wedge t_{l_1} = v, (l_1, l_2, l_4, l_1), t_{l_1} < v) \end{array}$$

证明 (2b)

- 确定标号集合 $C = \{beg, l_1\}$ 。
- 挑选断言 q_{beg}, q_{l_1}

$$\begin{array}{ll} q_{beg} & x = a \wedge y = b \wedge a > 0 \wedge b > 0 \\ q_{l_1} & x > 0 \wedge y > 0 \end{array}$$

- 挑选 $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
- 确定标号集合 $C' = \{l_1\}$ 。
- 挑选项 $g_{l_1} : \Sigma \rightarrow W$

$$g_{l_1}(\sigma) = \begin{cases} \sigma(x) + \sigma(y) & \text{若 } \sigma(y) > 0 \wedge \sigma(x) > 0 \\ 0 & \text{否则。} \end{cases}$$

- 确定需要证明的路径

$$\begin{array}{l} (beg, l_1) \\ (l_1, l_2, l_3, l_1) \\ (l_1, l_2, l_4, l_1) \end{array}$$

- 证明路径正确性

$$\models_I vc(q_{beg}, (beg, l_1), q_{l_1})$$
$$\models_I vc(q_{l_1}, (l_1, l_2, l_3, l_1), q_{l_1})$$
$$\models_I vc(q_{l_1}, (l_1, l_2, l_4, l_1), q_{l_1})$$

- 确定需要证明的路径

$$(l_1, l_2, l_3, l_1)$$
$$(l_1, l_2, l_4, l_1)$$

- 证明路径正确性

$(1) I(q_{l_1})(\sigma) = true \wedge M_I(l_1, l_2, l_3, l_1)(\sigma) \downarrow \rightarrow g_{l_1}(M_I(l_1, l_2, l_3, l_1)(\sigma)) < g_{l_1}(\sigma)$
$(2) I(q_{l_1})(\sigma) = true \wedge M_I(l_1, l_2, l_4, l_1)(\sigma) \downarrow \rightarrow g_{l_1}(M_I(l_1, l_2, l_4, l_1)(\sigma)) < g_{l_1}(\sigma)$

(1)

$\sigma(x) > 0 \wedge \sigma(y) > 0 \wedge \neg\sigma(x) = \sigma(y) \wedge \sigma(x) > \sigma(y) \rightarrow$
$g_{l_1}(\sigma[x/\sigma(x) - \sigma(y)]) < g_{l_1}(\sigma)$

由前提条件，我们有 $\sigma(x) > 0 \wedge \sigma(y) > 0$ 且 $(\sigma[x/\sigma(x) - \sigma(y)])(x) > 0 \wedge (\sigma[x/\sigma(x) - \sigma(y)])(y) > 0$

因此只需证：

$\sigma(x) > 0 \wedge \sigma(y) > 0 \wedge \neg\sigma(x) = \sigma(y) \wedge \sigma(x) > \sigma(y) \rightarrow$
$(\sigma(x) - \sigma(y)) + \sigma(y) < \sigma(x) + \sigma(y)$

(2) 类似。