§4 推理验证

§4.1 卫式迁移系统的推理

例子: 最大公约数

设 $B=(F,P)$ 和 V 如下:

F	$=$	$\{0,1,s_0,s_1,s_2,s_3,s_4,s_5,-\}$
P	$=$	$\{=,>,<\}$
V	$=$	$\{a,x,y,i,j,k,l\}$

$I=(Int,I_0)$

$I_0(s_0)=I_0(0)$	$=$	0
$I_0(s_1)=I_0(1)$	$=$	1
$I_0(s_2)$	$=$	2
$I_0(s_3)$	$=$	3
$I_0(s_4)$	$=$	4
$I_0(s_5)$	$=$	5
$I_0(-)$	$=$	$-$
$I_0(=)$	$=$	$=$
$I_0(>)$	$=$	$>$
$I_0(<)$	$=$	$<$

最大公约数算法表示为 (B,V) 上的迁移系统 (T,Θ) 如下:

T	$(a=s_0)$	$\longrightarrow$	$(i,j,k,l,a):=(1,0,0,1,s_1)$
	$(a=s_1\wedge x=y)$	$\longrightarrow$	$(a):=(s_5)$
	$(a=s_1\wedge\neg(x=y))$	$\longrightarrow$	$(a):=(s_2)$
	$(a=s_2\wedge x>y)$	$\longrightarrow$	$(a):=(s_3)$
	$(a=s_2\wedge\neg(x>y))$	$\longrightarrow$	$(a):=(s_4)$
	$(a=s_3)$	$\longrightarrow$	$(x,i,j,a):=(x-y,i-k,j-l,s_1)$
	$(a=s_4)$	$\longrightarrow$	$(y,k,l,a):=(y-x,k-i,l-j,s_1)$
Θ	$(x>0\wedge y>0\wedge a=s_0)$		

安全性质

程序满足以下性质:

$(T,\Theta)\models_I x=m\wedge y=n\rightarrow\Box(a=s_2\rightarrow x=gcd(m,n)\wedge x=i*a+j*b)$

只需证明

$$\begin{aligned}(T,\Theta)\quad\models_I\quad&\Box(x>0\wedge y>0\wedge a=s_0\wedge x=m\wedge y=n\rightarrow\\&\Box(a=s_2\rightarrow x=gcd(m,n)\wedge x=i*m+j*n))\end{aligned}$$

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 1

令

$$\begin{array}{lcl}\zeta & \equiv & (x > 0 \wedge y > 0 \wedge a = s_0 \wedge x = m \wedge y = n) \\ \varphi & \equiv & (a = s_2 \rightarrow x = gcd(m,n) \wedge x = i * m + j * n) \\ \varphi' & \equiv & (a = s_1 \rightarrow (gcd(x,y) = gcd(m,n) \wedge x = i * m + j * n \wedge y = k * m + l * n)) \wedge \varphi\end{array}$$

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

活性性质

程序满足以下性质：

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

只需证明

$$(T, \Theta) \models_I \Box(x > 0 \wedge y > 0) \rightarrow \Diamond a = s_1$$

主要适用规则如下

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

尝试 1

选择 f 满足

$$\begin{array}{ll}I(f(x,y)) = x + y & if\ (x > 0 \wedge y > 0) \\ I(f(x,y)) = 1 & if\ (x \leq 0 \vee y \leq 0)\end{array}$$

令

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

需要

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

§4.2 谓词迁移系统的推理

§4.3 流程图程序的推理

归纳断言方法：部分正确

例子

定义 T_{91} 如下：

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

Example 4.1 设 $I = (NAT, I_0)$ 。用归纳断言方法证明 $\{x \leq 100\}T_{91}\{z = 91\}$ 。

证明分四个步骤。

- 确定标号集合 $C = \{beg, test_1, end\}$ 。
- 挑选断言 q_{beg}, q_{end}, q_{test_1}

$$
\begin{array}{ll}
q_{beg} & x \leq 100 \\
q_{end} & z = 91 \\
q_{test} & y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101)
\end{array}
$$

- 确定需要证明的路径

$$
\begin{array}{l}
(beg, test_1) \\
(test_1, test_2, udp_2, test_1) \\
(test_1, udp_1, test_1) \\
(test_1, test_2, res, end)
\end{array}
$$

- 证明路径正确性

$$
\begin{array}{l}
\models_I vc(q_{beg}, (beg, test_1), q_{test_1}) \\
\models_I vc(q_{test_1}, (test_1, test_2, udp_2, test_1), q_{test_1}) \\
\models_I vc(q_{test_1}, (test_1, udp_1, test_1), q_{test_1}) \\
\models_I vc(q_{test_1}, (test_1, test_2, res, end), q_{end})
\end{array}
$$

§4.4 结构化程序的推理

§4.4.1 指称语义

Example 4.2 设 T 为

$z = 1; \text{while}\,(x \neq y)\,\text{do}\,z := (y+1) * (y+2) * z; y := y+2\,\text{od}$

证明若 $M_I(T)(\sigma)$ 有定义，则 $M_I(T)(\sigma)(z) = \sigma(x)!/\sigma(y)!$ 。

可定义

$$g(\sigma) = \begin{cases} \sigma[y/\sigma(x)][z/(\sigma(x)!/\sigma(y)!)] & \text{若 } \sigma(x) \geq \sigma(y) \text{ 且 } \sigma(x) - \sigma(y) \text{ 为偶数} \\ \omega & \text{否则} \end{cases}$$

或

$$g(\sigma) = \begin{cases} \sigma[y/\sigma(x)][z/(\sigma(x)!/\sigma(y)!)] & \text{若 } \sigma(x) \geq \sigma(y) \\ \omega & \text{否则} \end{cases}$$

§4.4.2 Hoare 逻辑

例子

给定以下程序，记为 T_1 。

$y_1 := 0;\ y_2 := 1;\ y_3 := 1;$
while $y_3 \leq x$ do
    $y_1 := y_1 + 1;$
    $y_2 := y_2 + 2;$
    $y_3 := y_2 + y_3;$
    od

证明 $PA \vdash \{x = c\} T_1 \{y_1 = \sqrt{c}\}$ 。

证明

首先将程序分为四部分，记为 S_1, S_2, S_3, S_4 。
我们有

$$\{x = c\} S_1 \{x = c \wedge y_1 = 0\}$$

$$\{x = c \wedge y_1 = 0\} S_2 \{x = c \wedge y_1 = 0 \wedge y_2 = 1\}$$

$$\{x = c \wedge y_1 = 0 \wedge \wedge y_2 = 1\} S_3 \{x = c \wedge y_1 = 0 \wedge y_2 = 1 \wedge y_3 = 1\}$$

因此根据顺序复合规则，有

$$\{x = c\} S_1; S_2; S_3 \{x = c \wedge y_1 = 0 \wedge y_2 = 1 \wedge y_3 = 1\}$$

根据顺序复合规则，还需要证明

$$\{x = c \wedge y_1 = 0 \wedge y_2 = 1 \wedge y_3 = 1\} S_4 \{y_1^2 \leq c \wedge c < (y_1+1)^2\}$$

我们有

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

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

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

因此根据顺序复合规则，有

$$\{x = c \wedge (y_1+1)^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1\}$$
$$y_1 := y_1 + 1; y_2 := y_2 + 2; y_3 := y_2 + y_3$$
$$\{x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1\}$$

由于

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

有

$$\{y_3 \leq x \wedge x = c \wedge (y_1)^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1\}$$
$$y_1 := y_1 + 1; y_2 := y_2 + 2; y_3 := y_2 + y_3$$
$$\{x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1\}$$

因此根据循环规则，有

$$\{x = c \wedge (y_1)^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1\}$$
$$S_4$$
$$\{\neg(y_3 \leq x) \wedge x = c \wedge y_1^2 \leq x \wedge y_3 = (y_1+1)^2 \wedge y_2 = 2 * y_1 + 1\}$$

因此

$$\{x = c \wedge y_1 = 0 \wedge y_2 = 1 \wedge y_3 = 1\} S_4 \{y_1^2 \leq c \wedge c < (y_1+1)^2\}$$

例子

给定以下程序，记为 T_2 。

$y_1 := x;$
$y_2 := 1;$
while $y_1 \leq 100 \vee y_2 \neq 1$ do
  if $y_1 \leq 100$ then
    $y_1 := y_1 + 11;$
    $y_2 := y_2 + 1;$
    else
    $y_1 := y_1 - 10;$
    $y_2 := y_2 - 1;$
    fi
  od
$z := y_1 - 10;$

证明 $PA \vdash \{x \leq 100\} T_2 \{z = 91\}$ 。

证明

根据顺序复合规则，只需要证明

$$\{x \leq 100 \wedge y_1 = x \wedge y_2 = 1\} S_1 \{y_1 = 101\}$$

有

$$\{y_1 \leq 121 \wedge y_2 \geq 2 \wedge (y_1 \geq 111 \wedge y_2 = 2 \rightarrow y_1 = 111)\}$$
$$y_1 := y_1 - 10; y_2 := y_2 - 1$$
$$\{y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101)\}$$

$$\{y_1 \leq 100 \wedge y_2 \geq 0 \wedge (y_1 \geq 100 \wedge y_2 = 0 \rightarrow y_1 = 100)\}$$
$$y_1 := y_1 + 11; y_2 := y_2 + 1$$
$$\{y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101)\}$$

因此

$\{ y_1 \leq 100 \wedge y_1 \leq 100 \wedge y_2 \geq 0 \wedge (y_1 \geq 100 \wedge y_2 = 0 \rightarrow y_1 = 100) \vee$
$\neg(y_1 \leq 100) \wedge y_1 \leq 121 \wedge y_2 \geq 2 \wedge (y_1 \geq 111 \wedge y_2 = 2 \rightarrow y_1 = 111) \}$
if $y_1 \leq 100$ then $y_1 := y_1 + 11$; $y_2 := y_2 + 1$;
else $y_1 := y_1 - 10$; $y_2 := y_2 - 1$; fi
$\{ y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101)\}$

因此

$\{ y_1 \leq 100 \wedge y_2 \geq 0 \wedge (y_1 \geq 100 \wedge y_2 = 0 \rightarrow y_1 = 100) \vee$
$y_1 > 100 \wedge y_1 \leq 121 \wedge y_2 \geq 2 \wedge (y_1 \geq 111 \wedge y_2 = 2 \rightarrow y_1 = 111) \}$
if $y_1 \leq 100$ then $y_1 := y_1 + 11$; $y_2 := y_2 + 1$;
else $y_1 := y_1 - 10$; $y_2 := y_2 - 1$; fi
$\{ y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101)\}$

又有

$(y_1 \leq 100 \vee y_2 \neq 1) \wedge y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101)$

$\rightarrow$

$y_1 \leq 100 \wedge y_2 \geq 0 \wedge (y_1 \geq 100 \wedge y_2 = 0 \rightarrow y_1 = 100) \vee$

$y_1 > 100 \wedge y_1 \leq 121 \wedge y_2 \geq 2 \wedge (y_1 \geq 111 \wedge y_2 = 2 \rightarrow y_1 = 111)$

因此

$\{ (y_1 \leq 100 \vee y_2 \neq 1) \wedge y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101) \}$

if $y_1 \leq 100$ then $y_1 := y_1 + 11$; $y_2 := y_2 + 1$;

else $y_1 := y_1 - 10$; $y_2 := y_2 - 1$; fi

$\{ y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101) \}$

因此，根据循环规则

$\{ y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101) \}$

S_1

$\{ \neg(y_1 \leq 100 \vee y_2 \neq 1) \wedge y_1 \leq 111 \wedge y_2 \geq 1 \wedge (y_1 \geq 101 \wedge y_2 = 1 \rightarrow y_1 = 101) \}$

根据推论规则，

$$\{x \leq 100 \wedge y_1 = x \wedge y_2 = 1\} S_1 \{y_1 = 101\}$$

扩展的 Hoare 逻辑

例子

Example 4.3 证明 $PA \vdash [x = c] T_1 [y_1 = \sqrt{c}]$ 。

需证明

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

S_4

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

取 $w = true$ ， $t = x + 1 - y_3$

需证明

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

$y_1 := y_1 + 1; y_2 := y_2 + 2; y_3 := y_2 + y_3$

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

需证明

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

$\rightarrow$

$x = c \wedge (y_1 + 1)^2 \leq x \wedge y_3 + (y2 + 2) = (y_1 + 1 + 1)^2 \wedge y_2 = 2 * (y_1 + 1) + 1 \wedge$

$x + 1 - (y_3 + (y_2 + 1)) < a$