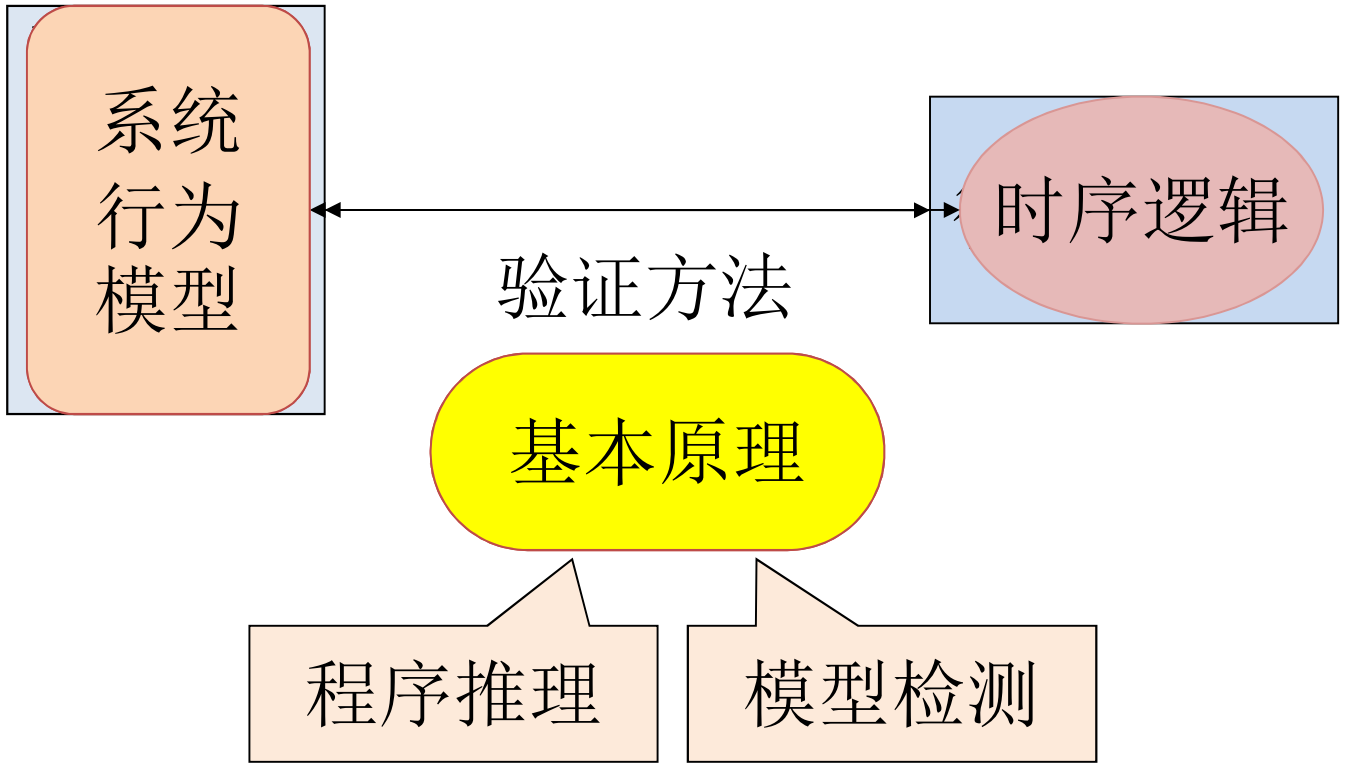
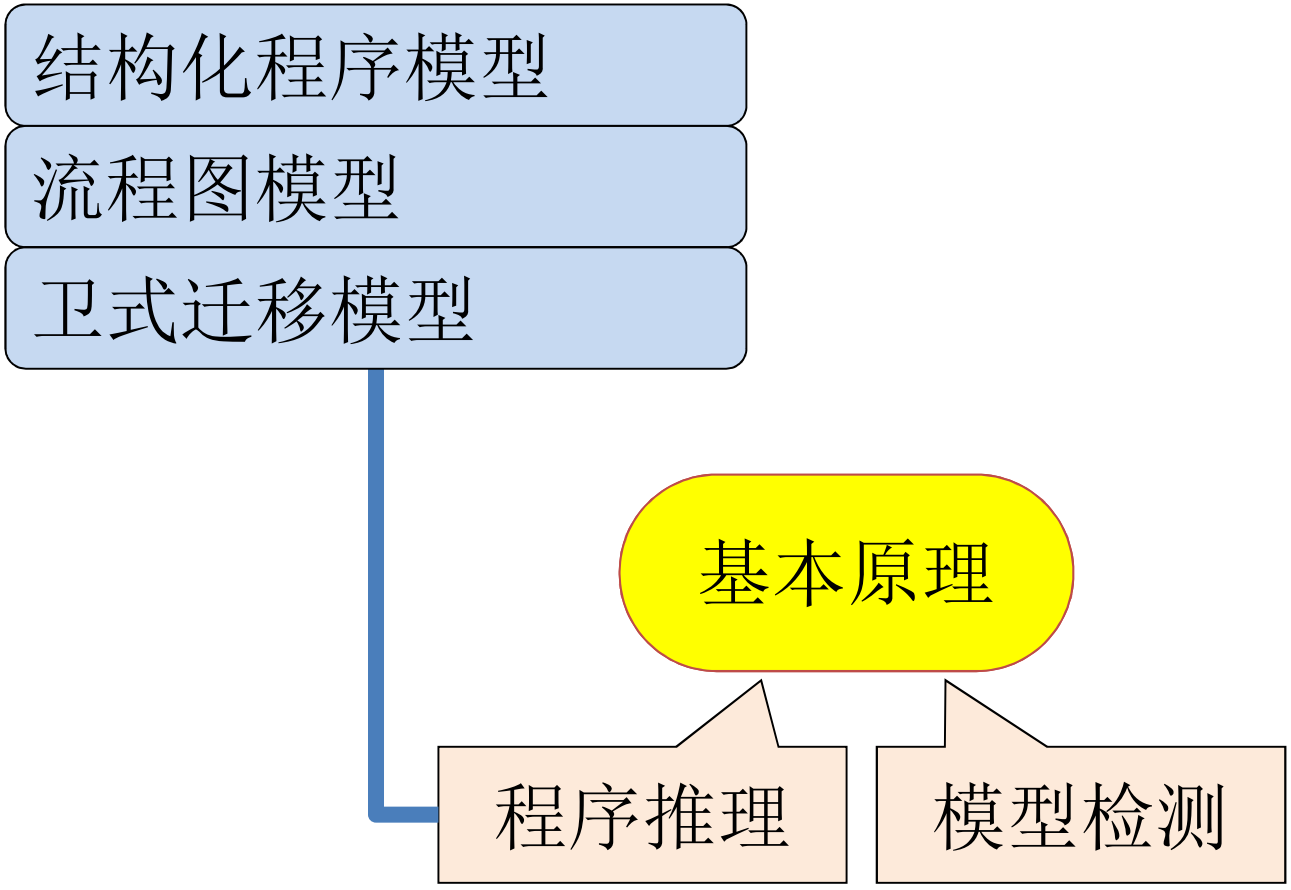
推理验证 -- 顺序流程图模型

中国科学院软件研究所
计算机科学国家重点实验室
张文辉
http://lcs.ios.ac.cn/~zwh/

课程内容

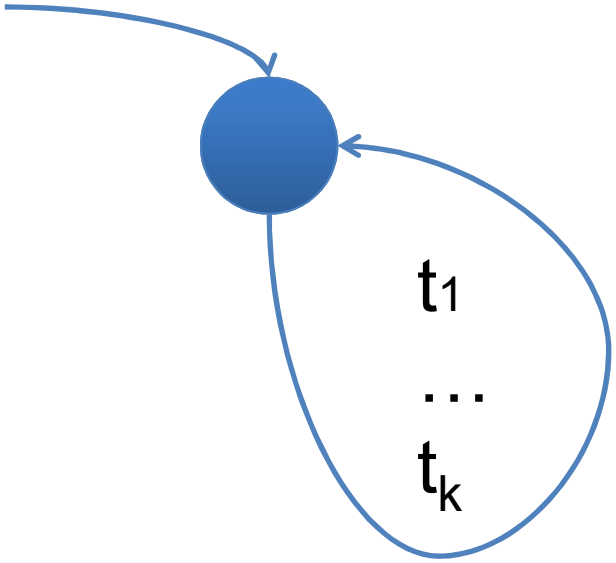


课程内容(3)



回顾：卫式迁移模型

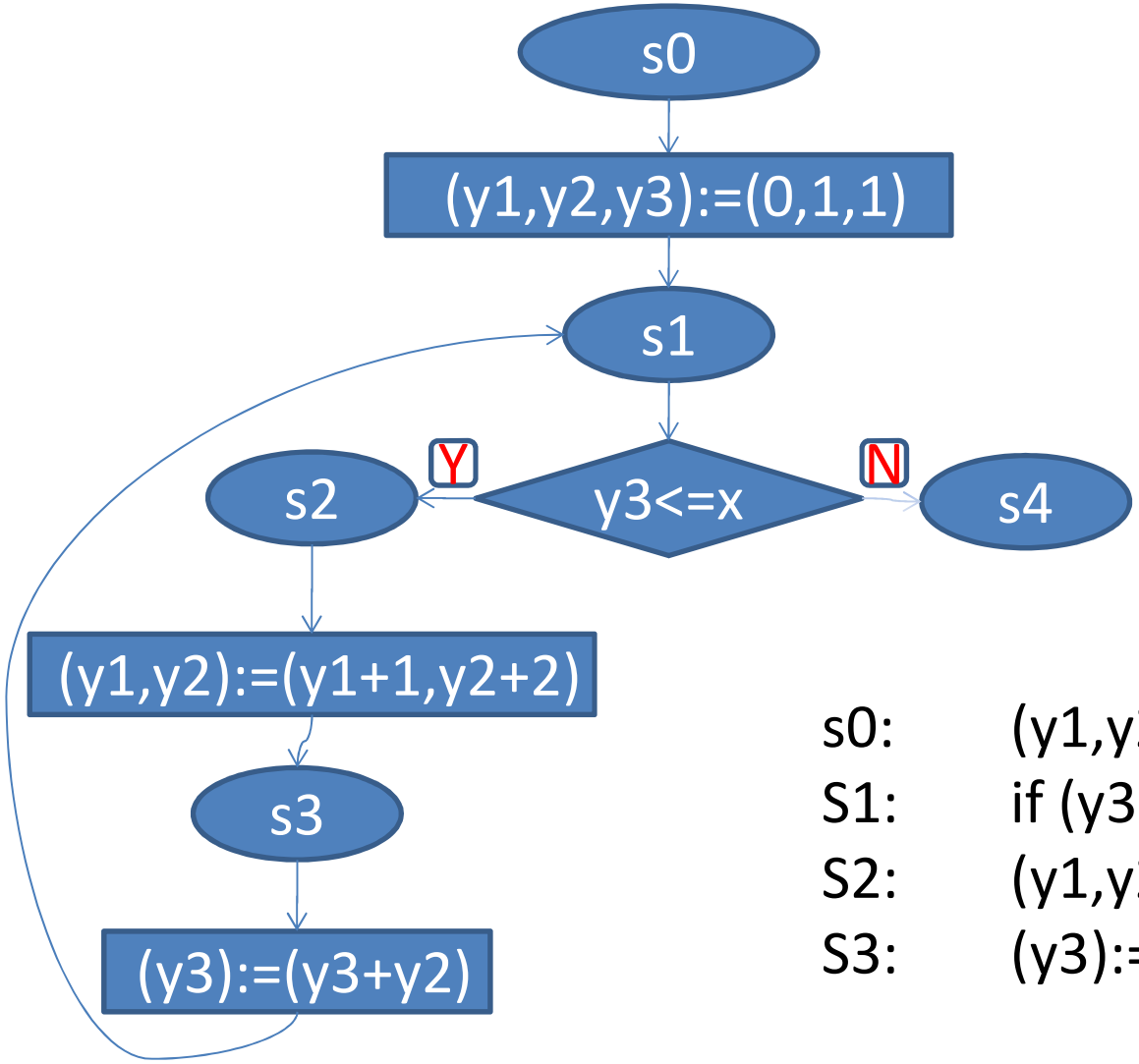
$p \rightarrow (x1,...,xn) := (e1,...,en);$



优点：并发模型

难点：选取不变量
选取秩函数

Integer Square Root



选取不变量

选取秩函数

s0: (y1,y2,y3):=(0,1,1); goto S1
S1: if (y3<=x) goto S2 else goto S4
S2: (y1,y2):=(y1+1,y2+2); goto S3
S3: (y3):=(y3+y2); goto S1

归纳不变量

$$
\begin{aligned}
\varphi' \quad \equiv \quad & (a = s_0 \wedge \varphi_0) \vee \\
& (a = s_1 \wedge \varphi_1) \vee \\
& (a = s_2 \wedge \varphi_2) \vee \\
& (a = s_3 \wedge \varphi_3) \vee \\
& (a = s_4 \wedge \varphi_4)
\end{aligned}
$$

where

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

顺序流程图模型

有一些程序结构的信息可用

关注一些特殊类型性质

可以发展具有针对性的方法

Contents

- Correctness
  - Partial Correctness
  - Termination
  - Total Correctness (Partial Correctness + Termination)

- Assertions
  - Preconditions/Postconditions
  - Weakest Liberal Preconditions

- Verification
  - Partial Correctness
  - Total Correctness

(I) Correctness

- Partial Correctness
- Termination
- Total Correctness (Partial Correctness + Termination)

Correctness (1)

Partial Correctness

DEF

$\models_{I} \{\varphi\}\ M\ \{\psi\}$

iff

$I(\varphi)(\sigma) \rightarrow ((BEG,\sigma) \rightarrow^{*} (END,\sigma')) \rightarrow I(\psi)(\sigma')$

Correctness (2)

Termination

DEF

$\models_{I} [\varphi] M [true]$

iff

$I(\varphi)(\sigma) \rightarrow ((BEG,\sigma) \rightarrow^{*} (END,\sigma'))$

Correctness (3)

Total Correctness

DEF

$\models_{I} [\varphi] M [\psi]$

iff

$I(\varphi)(\sigma) \rightarrow ((BEG,\sigma) \rightarrow^{*} (END,\sigma')) \wedge I(\psi)(\sigma'))$

Correctness

Total Correctness = Partial Correctness + Termination

Proposition:

$\models_{l} [\varphi]\ M\ [\ \psi\ ]$

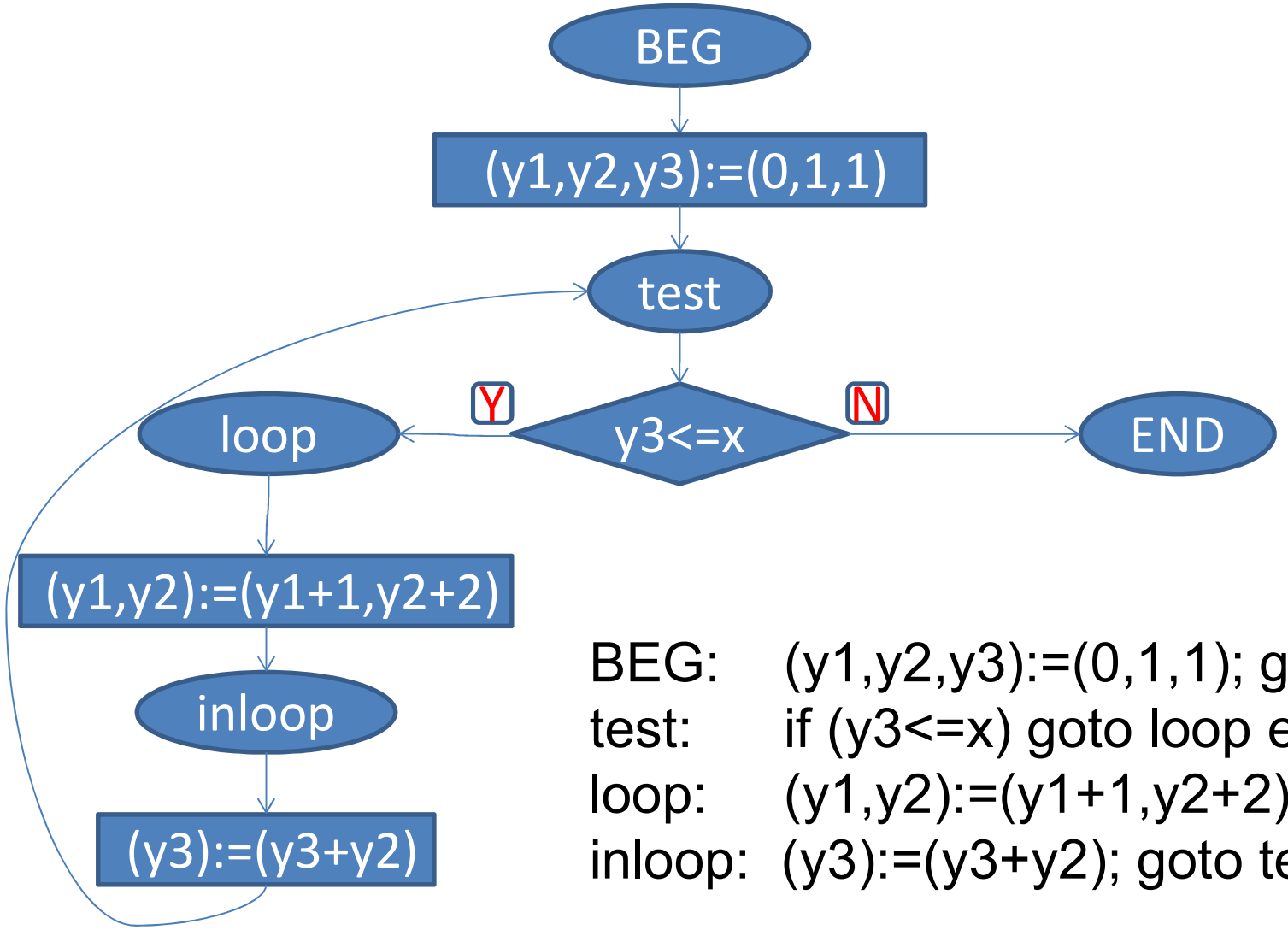
iff

$\models_{l} \{\varphi\}\ M\ \{\ \psi\ \}$ and $\models_{l} [\varphi]\ M\ [\mathtt{true}]$

Proof Based on Semantics

例子 

Integer Square Root




```
BEG:    (y1,y2,y3):=(0,1,1); goto test;
test:   if (y3<=x) goto loop else goto END
loop:   (y1,y2):=(y1+1,y2+2); goto inloop
inloop: (y3):=(y3+y2); goto test;
```

Integer Square Root (P1)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (NAT, I_0)$.

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

Prove: $\models_I \{x \geq 0\} T_0 \{y_1 = \sqrt{x}\}$

Assume a computation is as follows.

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

There are n transitions, and $l_n = end$

Need $(y_1 = \sqrt{x})(\sigma_n)$, i.e., $\sigma_n(y_1) = \sqrt{\sigma_n(x)}$

We have
$\sigma_n = \sigma_{n-1}$ and
$\neg(\sigma_n(y_3) \leq \sigma_n(x))$ (implied by $(test, \sigma_{n-1}) \rightarrow (end, \sigma_n)$).

If there exists φ' such that $\varphi'(\sigma_{n-1})$ and

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

Then we have

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

Let φ' be

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

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

Remain to prove $\varphi'(\sigma_{n-1})$, i.e.,

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

This can be proved by induction.

The label of σ_{n-1} is *test*.

We prove for all k, when σ_k has *test* as the label:

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

(1) $k = 0$, the label is *BEG*, ok.

(2) $k = 1$, the label is *test*, we have
$\sigma_1(y_1) = 0, \sigma_1(y_2) = 1, \sigma_1(y_3) = 1, \sigma_1(x) = \sigma_0(x)$ and $\sigma_0(x) \geq 0$.
Therefore

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

(3) Suppose that $k \leq i$, the goal holds.
Let $k = i + 1$ and $i \geq 1$.
No proof is needed if the label is not *test*.
Suppose that the label is *test* and we have $k \geq 4$.
Then

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

Therefore

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

Therefore

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

Therefore, for all k, when the label of σ_k is *test*, we have

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

Integer Square Root (P2)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (NAT, I_0)$.

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

Prove: $\models_I [true] T_0 [true]$

Suppose that the program does not terminate:

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

For all $k \geq 0$, we have
$l_{3k+1} = test$, $l_{3k+2} = loop$,$l_{3k+3} = inloop$ and $\sigma_{3k+1}(y_3) \leq x$
We prove for all $k \geq 0$
$\sigma_{3k+1}(y_3) \geq k$ and $\sigma_{3k+1}(x) = \sigma_0(x)$

- We have $\sigma_1(y_3) = 1$ and $\sigma_1(x) = \sigma_0(x)$.
  Therefore $\sigma_{3*0+1}(y_3) \geq 0$ and $\sigma_{3*0+1}(x) = \sigma_0(x)$.
- Suppose that for $k = i$,
  we have $\sigma_{3i+1}(y_3) \geq i$ and $\sigma_{3i+1}(x) = \sigma_0(x)$.
  We prove for $k = i + 1$, we have $\sigma_{3(i+1)+1}(y_3) \geq i + 1$ and $\sigma_{3i+1}(x) = \sigma_0(x)$.
  According to the previous calculation, we have

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

  Therefore for $k = i + 1$,
  we have $\sigma_{3(i+1)+1}(y_3) \geq i + 1$ and $\sigma_{3i+1}(x) = \sigma_0(x)$

Therefore for all $k \geq 0$, we have $\sigma_{3k+1}(y_3) \geq k$ and $\sigma_{3k+1}(x) = \sigma_0(x)$.

Let $k = \sigma_0(x) + 1$. Then $\sigma_{3k+1}(y_3) \leq \sigma_{3k+1}(x)$ does not hold, and this contradicts to the supposition.

Integer Square Root (P3)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (NAT, I_0)$.

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

Prove: $\models_I [x \geq 0] T_0 [y_1 = \sqrt{x}]$

Lemma:
For all $\sigma \in \Sigma$ and all $0 \leq k \leq \sqrt{\sigma_0(x)}$, we have

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

and

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

By induction.

- $k = 0$, ok.
- Suppose that for $k = i$ and $k \leq \sqrt{\sigma_0(x)}$, we have

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

Then for $k = i + 1$ and $k \leq \sqrt{\sigma_0(x)}$, we have

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

Therefore the lemma holds.

Let $k = \sqrt{\sigma_0(x)}$
Then $\sigma_{3k+1}(y_3) = (k+1)^2 = (\sqrt{\sigma_0(x)}+1)^2 > \sigma_0(x) = \sigma_{3k+1}(x)$
Therefore

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

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

(II) Assertions

- Preconditions/Postconditions (on Paths)
- Weakest Liberal Preconditions (on Paths)

Paths

A path is a sequence of labels, denoted
(L0,L1,L2,…,Lk).

LETα= (L0,L1,L2,…,Lk).

DEF
$(L0,\sigma_0) \rightarrow^{\alpha} (Lk,\sigma_k)$ iff
there are $\sigma_1,\ldots,\sigma_{k-1}$ such that
$((L0,\sigma_0) \rightarrow (L1,\sigma_1)) \wedge \ldots\ldots \wedge ((L(k-1),\sigma_{k-1}) \rightarrow (Lk,\sigma_k))$

Assertions (Pre-Post-Conditions), Paths

$\models_{I} \{\varphi\}\ (L0,\ldots,Lk)\ \{\psi\}$, iff

$$I(\varphi)(\sigma) \wedge ((L0,\sigma) \rightarrow^{(L0,\ldots,Lk)} (Lk,\sigma')) \rightarrow I(\psi)(\sigma')$$

A special case:

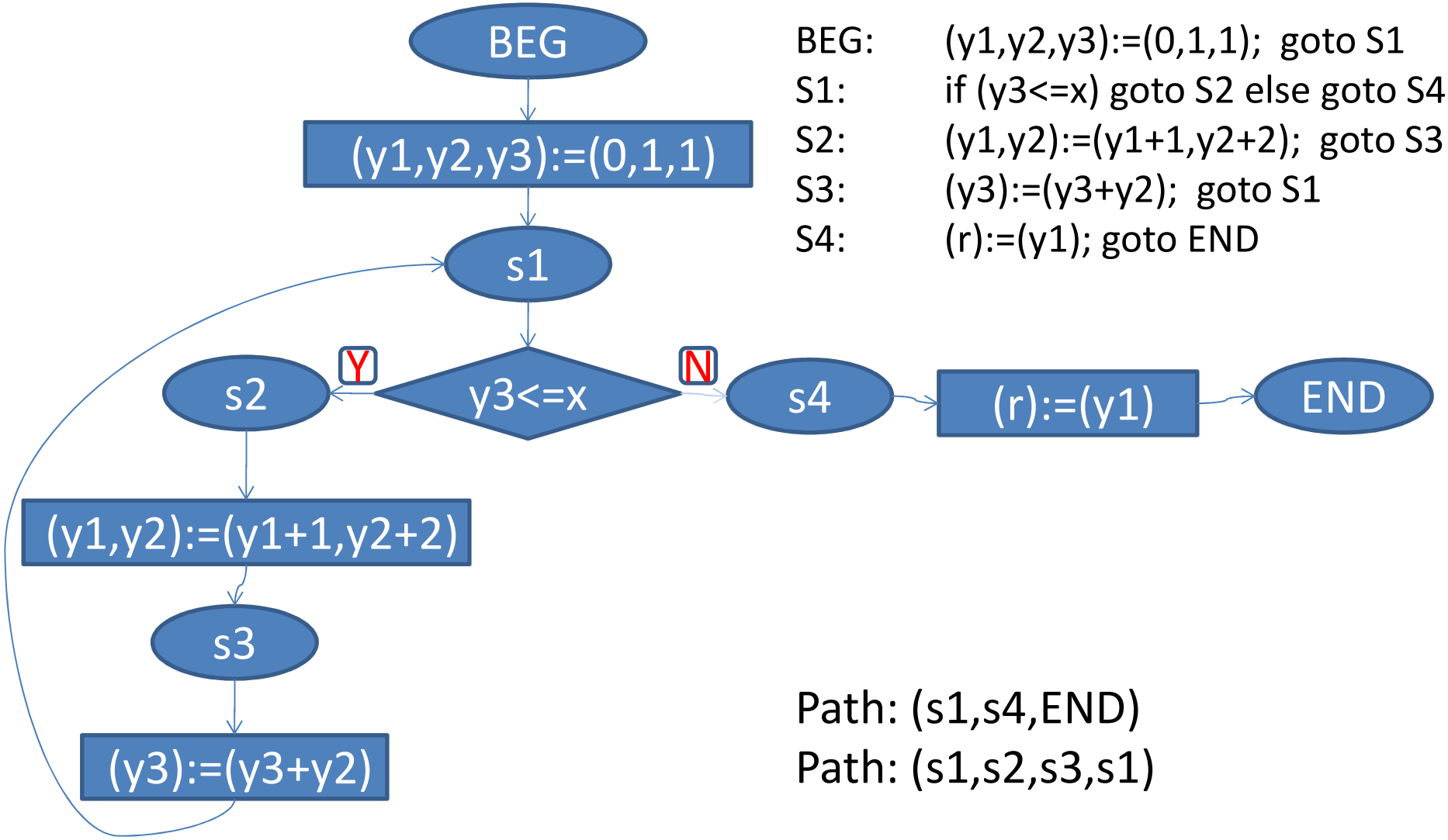
$\models_{I} \{\varphi\}\ (L,L')\ \{\psi\}$, iff $I(\varphi)(\sigma) \rightarrow (((L,\sigma) \rightarrow (L',\sigma')) \rightarrow I(\psi)(\sigma'))$

$$\frac{\varphi' \rightarrow \varphi \qquad \{\varphi\}\ (L0,\ldots,Lk)\ \{\psi\} \qquad \psi \rightarrow \psi'}{\{\varphi'\}\ (L0,\ldots,Lk)\ \{\psi'\}}$$

Composition of Paths

$$\frac{\models_{I} \{\varphi\}\ (L0,\ldots,La)\ \{\varphi'\} \qquad \models_{I} \{\varphi'\}\ (La,\ldots,Lk)\ \{\psi\}}{\models_{I} \{\varphi\}\ (L0,\ldots,Lk)\ \{\psi\}}$$

Examples: Paths



BEG: (y1,y2,y3):=(0,1,1); goto S1
S1: if (y3<=x) goto S2 else goto S4
S2: (y1,y2):=(y1+1,y2+2); goto S3
S3: (y3):=(y3+y2); goto S1
S4: (r):=(y1); goto END

Path: (s1,s4,END)
Path: (s1,s2,s3,s1)

Weakest Liberal Pre-Condition

DEF φ=wlp(α,ψ):

$I(\varphi)(\sigma) \leftrightarrow ((L,\sigma) \rightarrow^{\alpha} (L',\sigma')) \rightarrow I(\psi)(\sigma')$

Theorem

φ=wlp(α,ψ), if and only if

$\models \{\varphi\}\ \alpha\ \{\psi\}$ and, if $\models \{\varphi'\}\ \alpha\ \{\psi\}$ then $(\varphi' \rightarrow \varphi)$

Theorem

$\models \{\varphi\}\ \alpha\ \{\psi\}$ iff $\varphi \rightarrow$ wlp(α ,ψ)

Weakest Liberal Pre-Condition, α

Theorem

wlp((L0,…Lk), ψ) $\equiv$ wlp((L0,L1), wlp((L1,…Lk), ψ)),

Computation of wlp

WLP

DEF

(1) L: $(x_1,\ldots,x_n):=(e_1,\ldots,e_n)$; goto L' $\in$ M

$[L,L']\ \psi = \psi\,(e_1/x_1,\ldots, e_n/x_n)$

(2) L: if (c) goto L' else goto L'' $\in$ M

$[L,L']\ \psi = c \rightarrow \psi$;

$[L,L'']\ \psi = \neg c \rightarrow \psi$.

(3) $[L0,\ldots,Lk]\ \psi = [L0,L1][L1,\ldots Lk]\ \psi$

WLP

Lemma:

$wlp(\alpha, \psi) \equiv [\alpha]\ \psi$

Proof of the lemma (1), $\alpha=(L,L')$

(1) L: $(x_1,\ldots,x_n):=(e_1,\ldots,e_n)$; goto L' $\in$ M

φ=wlp((L,L'), ψ), iff

$\models \{\varphi\}\ (L,L')\{\ \psi\ \}$ and, if $\models \{\varphi'\}\ (L,L')\ \{\ \psi\ \}$ then $(\varphi' \rightarrow \varphi)$

$[L,L']\ \psi\ = \psi(e_1/x_1,\ldots, e_n/x_n)$

(a) $I([L,L']\ \psi)(\sigma) \rightarrow (((L,\sigma) \rightarrow (L',\sigma')) \rightarrow I(\psi)(\sigma'))$

(b) $(I(\varphi')(\sigma) \rightarrow (((L,\sigma) \rightarrow (L',\sigma')) \rightarrow I(\psi)(\sigma')))$

$\rightarrow I(\varphi')(\sigma) \rightarrow I([L,L']\ \psi)(\sigma)$

Proof of the lemma (2a), α=(L,L')

(2a) L: if (c) goto L' else goto L'' $\in$ M

φ=wlp((L,L'), ψ), iff

|= {φ} (L,L'){ ψ } and, if |= {φ'} (L,L') { ψ } then (φ' $\rightarrow$ φ)

[L,L'] ψ = c $\rightarrow$ ψ

(a) I([L,L'] ψ)(σ) $\rightarrow$ (((L,σ) $\rightarrow$ (L',σ')) $\rightarrow$ I(ψ)(σ'))

(b) (I(φ')(σ) $\rightarrow$ (((L,σ) $\rightarrow$ (L',σ')) $\rightarrow$ I(ψ)(σ')))

$\rightarrow$ I(φ')(σ) $\rightarrow$ I([L,L'] ψ)(σ)

Proof of the lemma (2b), $\alpha=(L,L')$

(2b) L: if (c) goto L'' else goto L' $\in$ M

φ=wlp((L,L'), ψ), iff

|= {φ} (L,L'){ ψ } and, if |= {φ'} (L,L') { ψ } then ($\varphi' \rightarrow \varphi$)

[L,L'] ψ = $\neg$c$\rightarrow\psi$

(a) I([L,L'] ψ)(σ) $\rightarrow$ (((L,σ) $\rightarrow$ (L',σ')) $\rightarrow$ I(ψ)(σ'))

(b) (I(φ')(σ) $\rightarrow$ (((L,σ) $\rightarrow$ (L',σ')) $\rightarrow$ I(ψ)(σ')))

$\rightarrow$ I(φ')(σ) $\rightarrow$ I([L,L'] ψ)(σ)

Proof of the lemma (3), α=(L0,L1,…,Lk)

(3) $[L0,\ldots,Lk]\ \psi = [L0,L1][L1,\ldots Lk]\ \psi$

φ=wlp(α, ψ), iff

$\models \{\varphi\}\ \alpha\{\ \psi\ \}$ and, if $\models \{\varphi'\}\ \alpha\ \{\ \psi\ \}$ then $(\varphi' \rightarrow \varphi)$

By induction:

$[L0,L1][L1,\ldots Lk]\ \psi \equiv$ (ind)

$[L0,L1]$ wlp((L1,…Lk), ψ) $\equiv$ (ind)

wlp((L0,L1), wlp((L1,…Lk), ψ) $\equiv$ (thm)

wlp((L0,…Lk), ψ)

Examples: wlp

BEG: (y1,y2,y3):=(0,1,1); goto s1

s1: if (y3<=x) goto S2 else goto s4

s2: (y1,y2):=(y1+1,y2+2); goto s3

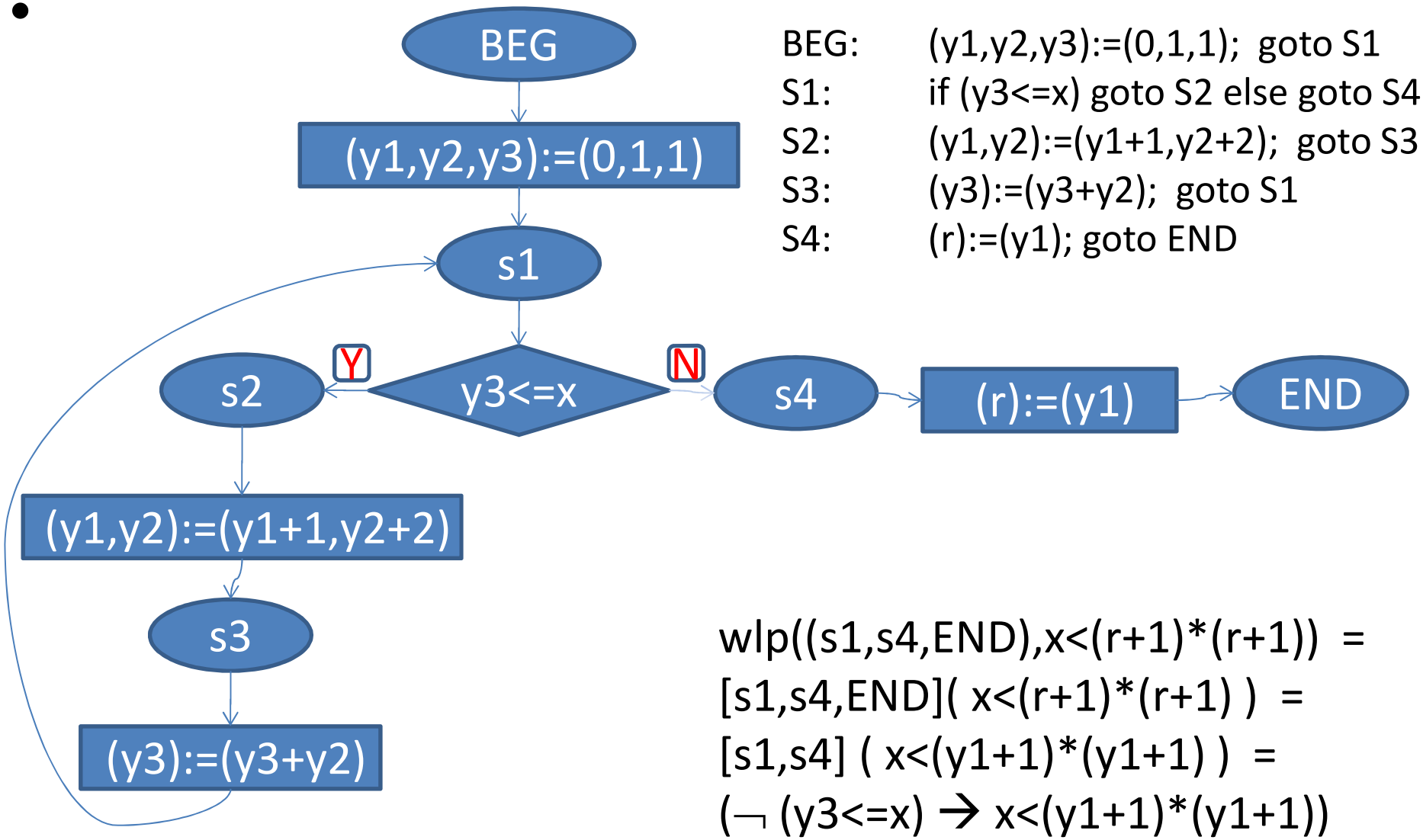
s3: (y3):=(y3+y2); goto s1

s4: (r):=(y1); goto END

wlp((s1,s4,END),x<(r+1)*(r+1)) = ?

wlp((s1,s2,s3,s1), y3=(y1+1)*(y1+1)) = ?

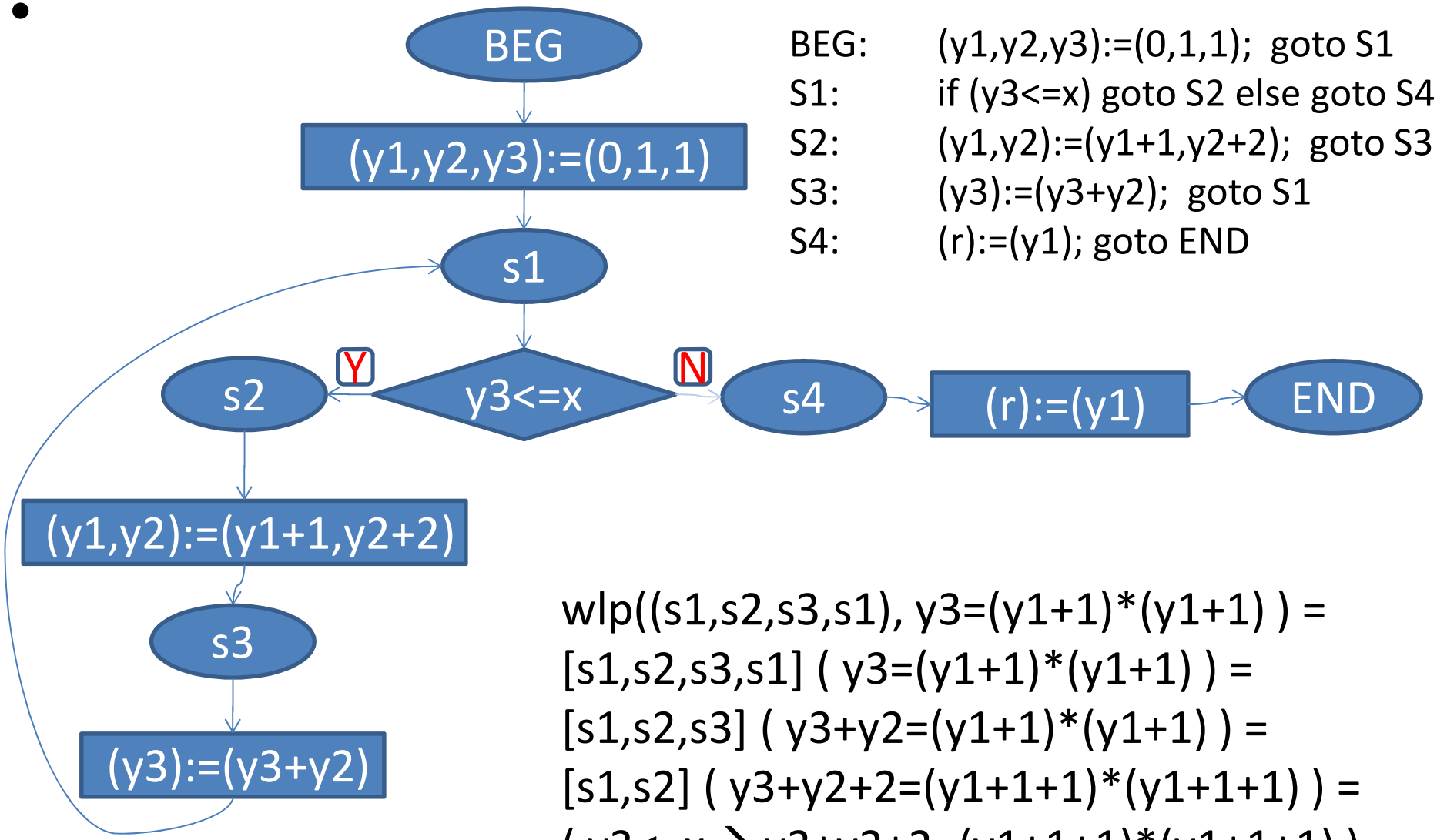
Example 1: wlp

- 

BEG: (y1,y2,y3):=(0,1,1); goto S1
S1: if (y3<=x) goto S2 else goto S4
S2: (y1,y2):=(y1+1,y2+2); goto S3
S3: (y3):=(y3+y2); goto S1
S4: (r):=(y1); goto END

wlp((s1,s4,END),x<(r+1)*(r+1)) =
[s1,s4,END](x<(r+1)*(r+1)) =
[s1,s4] (x<(y1+1)*(y1+1)) =
(¬ (y3<=x) → x<(y1+1)*(y1+1))

Example 2: wlp



BEG: (y1,y2,y3):=(0,1,1); goto S1
S1: if (y3<=x) goto S2 else goto S4
S2: (y1,y2):=(y1+1,y2+2); goto S3
S3: (y3):=(y3+y2); goto S1
S4: (r):=(y1); goto END

wlp((s1,s2,s3,s1), y3=(y1+1)*(y1+1)) =
[s1,s2,s3,s1] (y3=(y1+1)*(y1+1)) =
[s1,s2,s3] (y3+y2=(y1+1)*(y1+1)) =
[s1,s2] (y3+y2+2=(y1+1+1)*(y1+1+1)) =
(y3<=x→ y3+y2+2=(y1+1+1)*(y1+1+1))

Verification Conditions

Corollary

$\models_l \{\varphi\}\ \alpha\ \{\psi\}$ iff $(\varphi \rightarrow [\alpha]\ \psi)$

Verification Condition:

$\varphi \rightarrow [\alpha]\ \psi$, also denoted $vc(\varphi, \alpha, \psi)$,

is called a verification condition for $\models_l \{\varphi\}\ \alpha\ \{\psi\}$

Examples: Verification Condition

BEG: (y1,y2,y3):=(0,1,1); goto s1

s1: if (y3<=x) goto S2 else goto s4

s2: (y1,y2):=(y1+1,y2+2); goto s3

s3: (y3):=(y3+y2); goto s1

s4: (r):=(y1); goto END

(1)

$\models \{y3=(y1+1)*(y1+1)\}\ (s1,s4,END)\ \{(\ x<(r+1)*(r+1)\ )\}$

(2)

$\models \{y3=(y1+1)*(y1+1) \wedge y2=2y1+1\}\ \ (s1,s2,s3,s1)\ \{y3=(y1+1)*(y1+1)\}$

Proof of (1) by Semantics

$\models \{y3=(y1+1)*(y1+1)\}\ (s1,s4,END)\ \{(\ x<(r+1)*(r+1)\ )\}$

Assume $(s1,\sigma1)(s4,\ \sigma2)(END,\sigma3)$ and $\sigma1 \models y3=(y1+1)*(y1+1)$.
We have to prove $\sigma3 \models x<(r+1)*(r+1)$

$\sigma1(y3)=(\sigma1(y1)+1)*(\sigma1(y1)+1)$ [a0]
$(s1,\sigma1) \rightarrow (s4,\ \sigma2)$: $\sigma2= \sigma1 \wedge \neg(\sigma1(y3) <= \sigma1(x))$ [a1]
$(s4,\sigma2) \rightarrow (END,\ \sigma3)$: $\sigma3= \sigma2[r/\sigma2(y1)]$ [a2]

Have to prove:
x1. $\sigma3(x)<(\sigma3(r)+1)*(\sigma3(r)+1)$ [by a2]
x2. $\sigma2(x)<(\sigma2(y1)+1)*(\sigma2(y1)+1)$ [by a1]
x3. $\sigma1(x)<(\sigma1(y1)+1)*(\sigma1(y1)+1)$ [ok, by a0 and a1]

Proof of (1) by Verification Condition

|= {y3=(y1+1)*(y1+1)} (s1,s4,END) {(x<(r+1)*(r+1))} iff

vc(y3=(y1+1)*(y1+1), (s1,s4,END), (x<(r+1)*(r+1))) iff

y3=(y1+1)*(y1+1) → [s1,s4,END](x<(r+1)*(r+1)) iff

y3=(y1+1)*(y1+1) → [s1,s4] (x<(y1+1)*(y1+1)) iff

y3=(y1+1)*(y1+1) → (¬(y3<=x) → x<(y1+1)*(y1+1)) iff

true

Proof of (2) by Verification Condition

$\models \{ y3=(y1+1)*(y1+1) \wedge y2=2y1+1\}$
$(s1,s2,s3,s1)$
$\{y3=(y1+1)*(y1+1) \}$

iff

$vc(y3=(y1+1)*(y1+1) \wedge y2=2y1+1,$
$(s1,s2,s3,s1), y3=(y1+1)*(y1+1))$

iff

$y3=(y1+1)*(y1+1) \wedge y2=2y1+1 \rightarrow [s1,s2,s3,s1] (y3=(y1+1)*(y1+1))$

iff

……

iff

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

iff

true

Complete Paths

A path (L0,L1,L2,…,Lk) is a complete path, if

L0=BEGIN and Lk=END.

Lemma:

$\models_l \{\varphi\}\ M\ \{\psi\}$, iff

for every complete path α, we have $\models_l \{\varphi\}\ \alpha\ \{\psi\}$

Examples: Complete Paths

```
BEG:  (y1,y2,y3):=(0,1,1);  goto s1
s1:     if (y3<=x) goto S2 else goto s4
s2:     (y1,y2):=(y1+1,y2+2);  goto s3
s3:     (y3):=(y3+y2);  goto s1
s4:     (r):=(y1); goto END
```

Complete Path: (BEGIN, s1,s4,END)

Complete Path: (BEGIN,s1,s2,s3,s1,s4,END)

(III) Verification Techniques

(III.a) Partial Correctness

Corollary

$\models_l \{\varphi\}\ M\ \{\psi\}$, iff

for every complete path α, we have $\models_l \varphi \rightarrow [\alpha]\ \psi$

Partial Correctness (M0) $\models_{|} \{\varphi\}M\{\psi\}$

Select a set of labels C such that $\{BEG,END\} \subseteq C$ and

C contains at least one label of every cycle.

Select a formula q_L for every label of C, such that

$q_{BEG} = \varphi$ and $q_{END} = \psi$.

If for every path (l0,…,lk) such that

$\{l0,lk\} \subseteq C$ and $\{l1,\ldots,l(k-1)\} \cap C = \varnothing$, $\models q_{l0} \rightarrow [l0,\ldots,lk] q_{lk}$ holds,

Then $\{\varphi\}$ M $\{\psi\}$.

Proof

Need:

For every complete path α, we have $\models_l \varphi \rightarrow [\alpha]\ \psi$

Prove the following general conclusion by induction:

For every $(l0,\ldots,lk)$ such that $\{l0,lk\} \subseteq C$,

we have $\models_l q_{l0} \rightarrow [l0,\ldots,lk] q_{lk}$

n=2: ok.

n=i+1: Suppose that $(l0,\ldots,lk) = (l0,\ldots,la,\ldots,lk)$

The path (l0,…,lk) = (l0,…,la,…,lk) is split to 2 parts:

(l0,…,la) and (la,…,lk)

we have $\models_l q_{la} \rightarrow [la,\ldots,lk]q_{lk}$ and $\models_l q_{l0} \rightarrow [l0,\ldots,la]q_{la}$

$I(q_{l0})(\sigma) \wedge ((L0,\sigma) \rightarrow^{(L0,\ldots,La)} (La,\sigma')) \rightarrow I(q_{la})(\sigma')$

$I(q_{la})(\sigma') \wedge ((La,\sigma') \rightarrow^{(La,\ldots,Lk)} (Lk,\sigma'')) \rightarrow I(q_{lk})(\sigma'')$

$I(q_{l0})(\sigma) \wedge ((L0,\sigma) \rightarrow^{(L0,\ldots,Lk)} (Lk,\sigma')) \rightarrow I(q_{lk})(\sigma')$

Therefore:

For every (l0,…,lk) such that {l0,lk} $\subseteq$C,

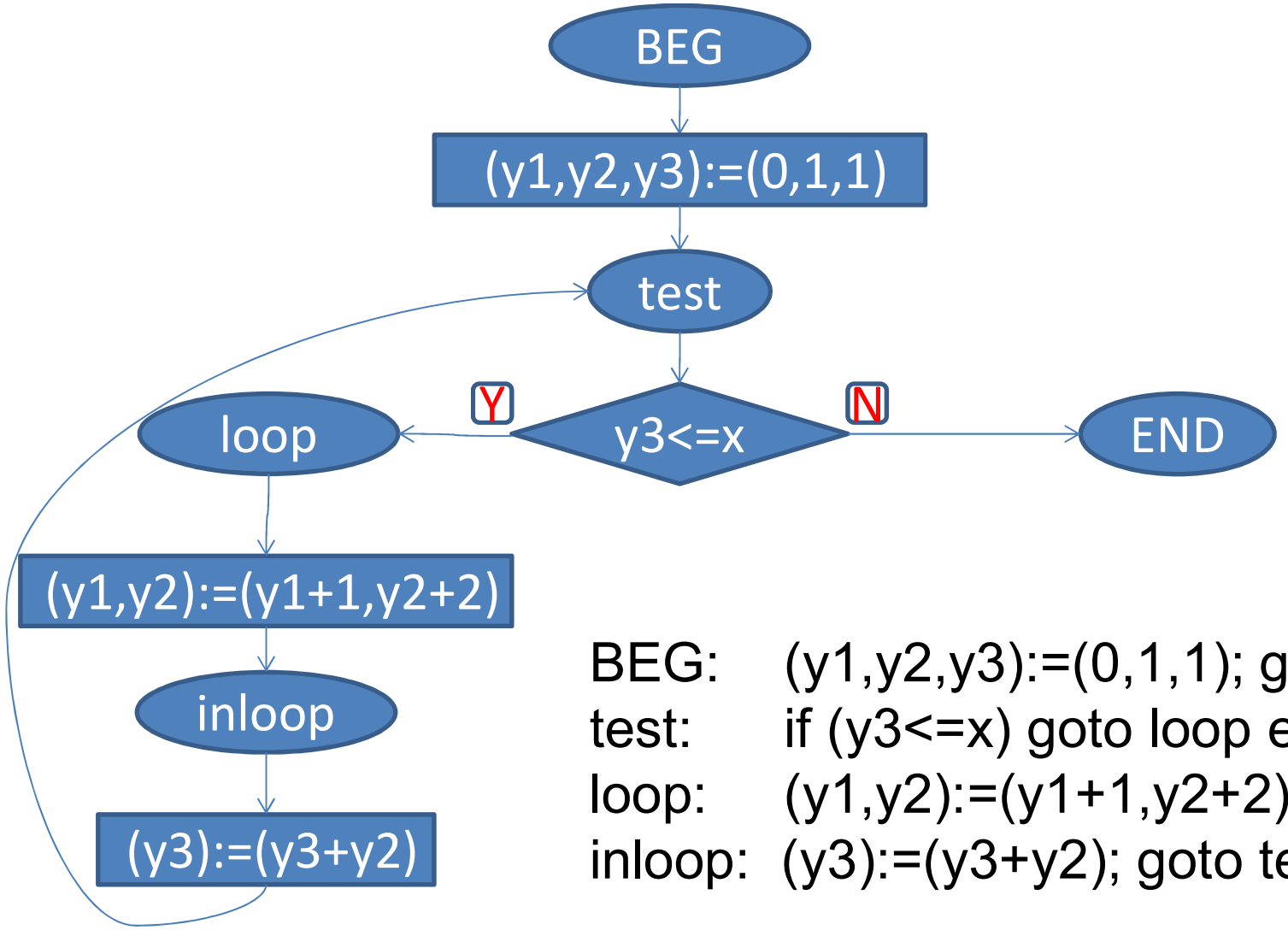
we have $\models_l q_{l0} \rightarrow [l0,\ldots,lk] q_{lk}$

Therefore:

For every complete path α, we have $\models_l \varphi \rightarrow [\alpha]\ \psi$

例子

Integer Square Root




```
BEG:    (y1,y2,y3):=(0,1,1); goto test;
test:   if (y3<=x) goto loop else goto END
loop:   (y1,y2):=(y1+1,y2+2); goto inloop
inloop: (y3):=(y3+y2); goto test;
```

Integer Square Root (M0)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (NAT, I_0)$.

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

Prove: $\models_I \{x = c\} T_0 \{y_1 = \sqrt{c}\}$

Steps
(1) Select C
(2) Select a formula for each element of C
(3) Find the paths for proving
(4) Prove the correctness of the paths

- Select $C = \{beg, test, end\}$
- Select q_{beg}, q_{end}, q_{test} as follows.

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

- Find the Paths

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

- Prove the Correctness

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

(III.b) Termination (M1) $\models_{l} [\varphi] M [true]$

Select a set of labels C such that $\{BEG\} \subseteq C$ and

C contains at least one label of every cycle.

Select a formula q_L for every label of C, such that $q_{BEG} = \varphi$.

Select a set of labels $C' \subseteq C$ such that

C contains at least one label of every cycle.

Select a function $g_L: \Sigma \rightarrow W$ (a WFS) for every label L of C'.

Termination (M1) $\models_l [\varphi] M [true]$

If

for every path (l0,…,lk) such that

($\{l0,lk\} \subseteq C$ and $\{l1,\ldots,l_{k-1}\} \cap C = \emptyset$, $\models q_{l0} \rightarrow [l0,\ldots,lk]\ q_{lk}$ holds,

for every path α=(l0,…,lk) such that

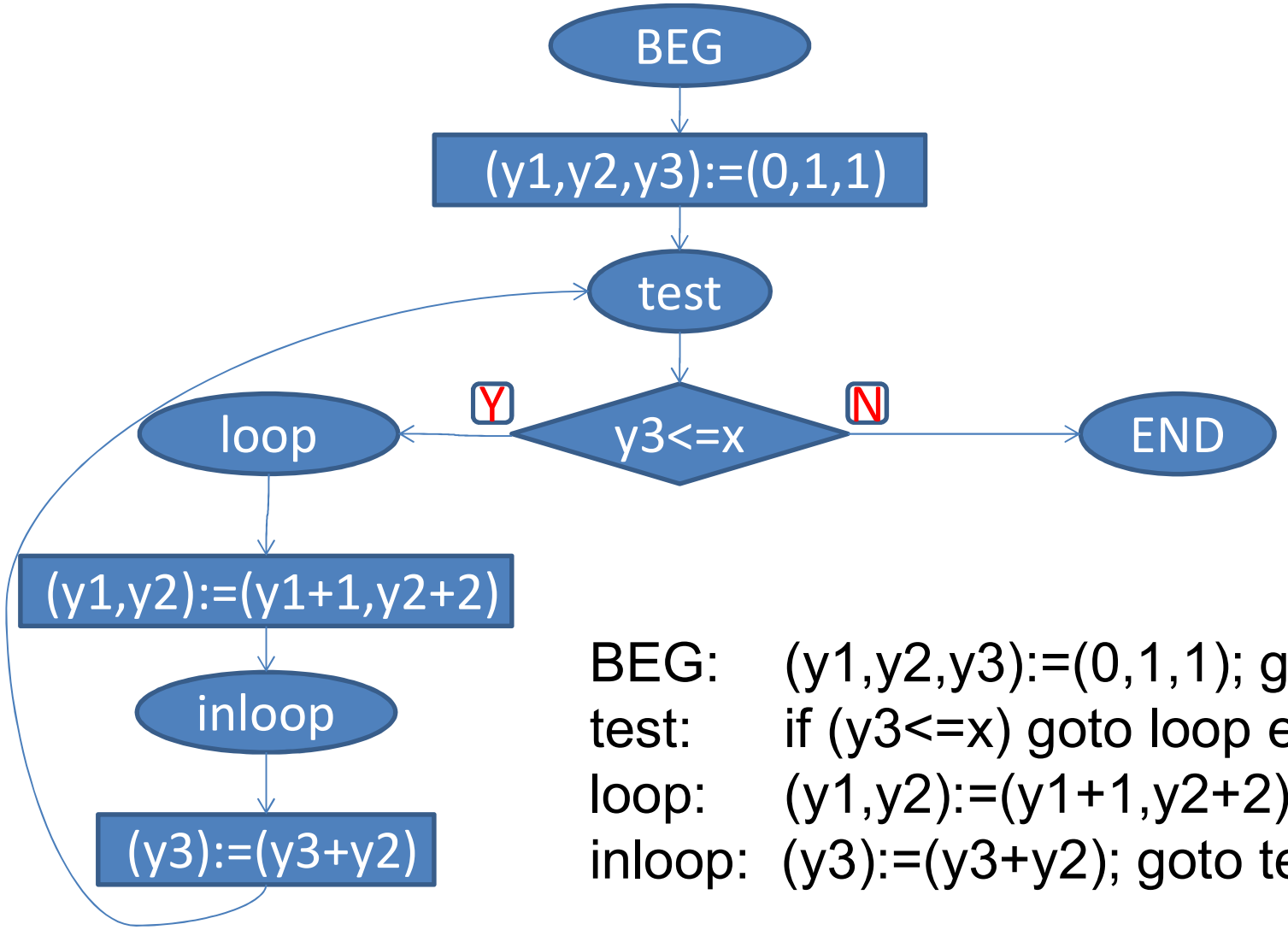
$\{l0,lk\} \subseteq C'$ and $\{l1,\ldots,l_{k-1}\} \cap C' = \emptyset$,

$I(q_{l0})(\sigma) \wedge (\sigma \rightarrow^{\alpha} \sigma') \rightarrow g_{lk}(\sigma') < g_{l0}(\sigma)$

Then $[\varphi] M [true]$

例子

Integer Square Root




```
BEG:    (y1,y2,y3):=(0,1,1); goto test;
test:   if (y3<=x) goto loop else goto END
loop:   (y1,y2):=(y1+1,y2+2); goto inloop
inloop: (y3):=(y3+y2); goto test;
```

Integer Square Root (M1)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (NAT, I_0)$.

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

Prove: $\models_I [true] T_0 [true]$

Steps
(1) Select C
(2) Select a formula for each element of C
(3) Find the paths for proving
(4) Prove the correctness of the paths (a)
(5) Select C'
(6) Select $(W, \sqsubseteq)$
(7) Select a function $g_c : \Sigma \to W$ for each c of C'
(8) Find the paths for proving
(9) Prove the correctness of the paths (b)

- Select $C = \{beg, test\}$
- Select q_{beg}, q_{test}

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

- Find the Paths

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

- Prove the Correctness

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

- Select $C' = \{test\}$
- Select $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
- Select $g_{test} : \Sigma \to W$

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

- Find the Paths

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

- Prove the Correctness

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

i.e., (for simplicity, the symbol σ is omitted)

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

Integer Square Root (M1a)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (INT, I_0)$.

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

Prove: $\models_I [x \geq 0] T_0 [true]$

- Select $C = \{beg, test\}$
- Select q_{beg}, q_{test}

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

- Find the Paths

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

- Prove the Correctness

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

- Select $C' = \{test\}$
- Select $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
- Select $g_{test} : \Sigma \to W$

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

- Find the Paths

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

- Prove the Correctness

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

i.e.,

$$y_2 \geq 0 \wedge (y_3 \leq x) \to x + 1 - (y_2 + y_3 + 2) < x + 1 - y_3$$

i.e.,

$$y_2 \geq 0 \wedge (y_3 \leq x) \to 0 < x + 1 - y_3$$

Termination (M2) $\models_{l}$ [φ] M [true]

Select a set of labels C such that {BEG} $\subseteq$ C and

C contains at least one label of every cycle.

Select a formula q_c for every label c of C, such that $q_{BEG} = \varphi$.

Select a set of labels C' $\subseteq$ C such that

C contains at least one label of every cycle.

Select a formula w for a WFS W.

Select a term t_c for every label c of C', such that qc→w(tc/x)

Termination (M2) $\models_{l} [\varphi] M [true]$

If

for every path (l0,…,lk) such that

($\{l0,lk\} \subseteq C$ and $\{l1,\ldots,l_{k-1}\} \cap C = \emptyset$, $\models q_{l0} \rightarrow [l0,\ldots,lk]\ q_{lk}$ holds,

for every path α=(l0,…,lk) such that

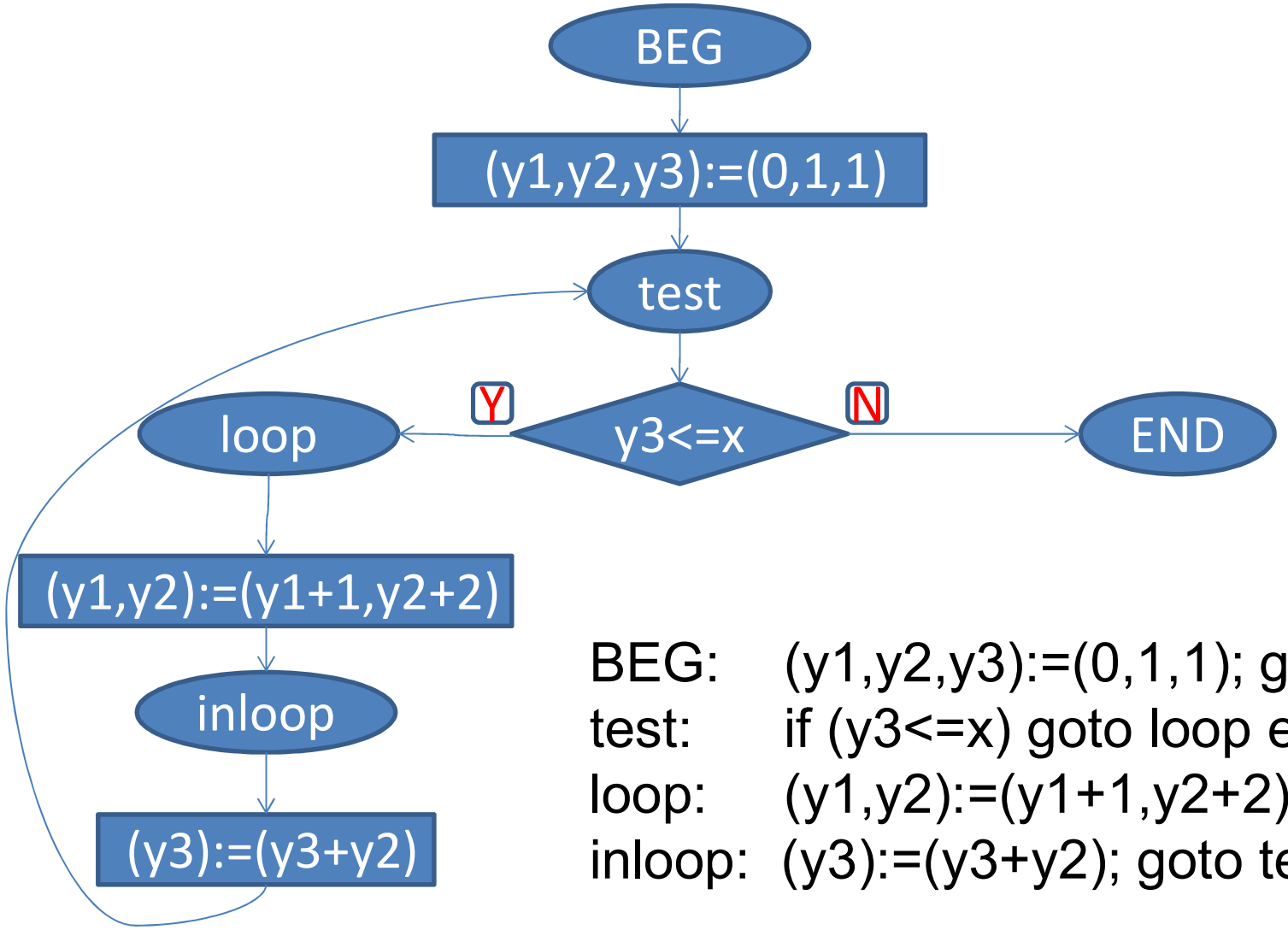
$\{l0,lk\} \subseteq C'$ and $\{l1,\ldots,l_{k-1}\} \cap C' = \emptyset$,

$\models q_{l0} \wedge t_{l0} = v \rightarrow [l0,\ldots,lk]\ t_{lk} < v)$ holds,

Then $[\varphi]$ M [true]

例子

Integer Square Root




```
BEG:    (y1,y2,y3):=(0,1,1); goto test;
test:   if (y3<=x) goto loop else goto END
loop:   (y1,y2):=(y1+1,y2+2); goto inloop
inloop: (y3):=(y3+y2); goto test;
```

Integer Square Root (M2)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (NAT, I_0)$.

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

Prove: $\models_I [true] T_0 [true]$

Steps

(1) Select C

(2) Select a formula q_c for each c of C

(3) Find the paths for proving

(4) Prove the correctness of the paths (a)

(5) Select C'

(6) Select $(W \subseteq D, I_0(\sqsubseteq))$;
Select w and prove $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$

(7) Select a term t_c for each c of C' and prove $q_c \rightarrow w_x^{t_c}$

(8) Find the paths for proving

(9) Prove the correctness of the paths (b)

- Select $C = \{beg, test\}$
- Select q_{beg}, q_{test}

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

- Find the Paths

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

- Prove the Correctness

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

- Select $C' = \{test\}$
- Select $(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
  Select $w = true$, and prove $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$
- Select $t_{test} = x + 1 - y_3$, and prove $q_{test} \rightarrow w_x^{t_{test}}$
- Find the Paths

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

- Prove the Correctness

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

i.e.,

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

Integer Square Root (M2a)

$B = (\{0, 1, 2, 3, ..., +, *\}, \{\leq\})$, $V = \{x, y_1, y_2, y_3\}$
T_0 is as follows, with the usual interpretation $I = (INT, I_0)$.

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

Prove: $\models_I [x \geq 0] T_0 [true]$

- Select $C = \{beg, test\}$
- Select q_{beg}, q_{test}

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

- Find the Paths

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

- Prove the Correctness

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

- Select$(W, \sqsubseteq) = (\{0, 1, 2, ...\}, \leq)$
  Select$w = (x \geq 0)$, and prove $W = \{\sigma(x) \mid I(w)(\sigma) = true\}$
- Select $C' = \{test\}$
- Select $t_{test} = x + 1 - y_3 + y_2$, and prove $q_{test} \rightarrow w_x^{t_{test}}$
- Find the Paths

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

- Prove the Correctness

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

i.e.,

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

(IV) Summary

- Correctness/Properties
- Assertions (Basic Theories)
- Verification Techniques

练习1

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

给定以下程序 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。

计算最弱宽松前断言 [l1,l3,end](y=n*n*n-n)

并证明 |= {(x<=n)∧3y=x*x*x-x} (l1,l3,end) { (y=n*n*n-n) }

练习2

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

给定以下程序 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。

(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。