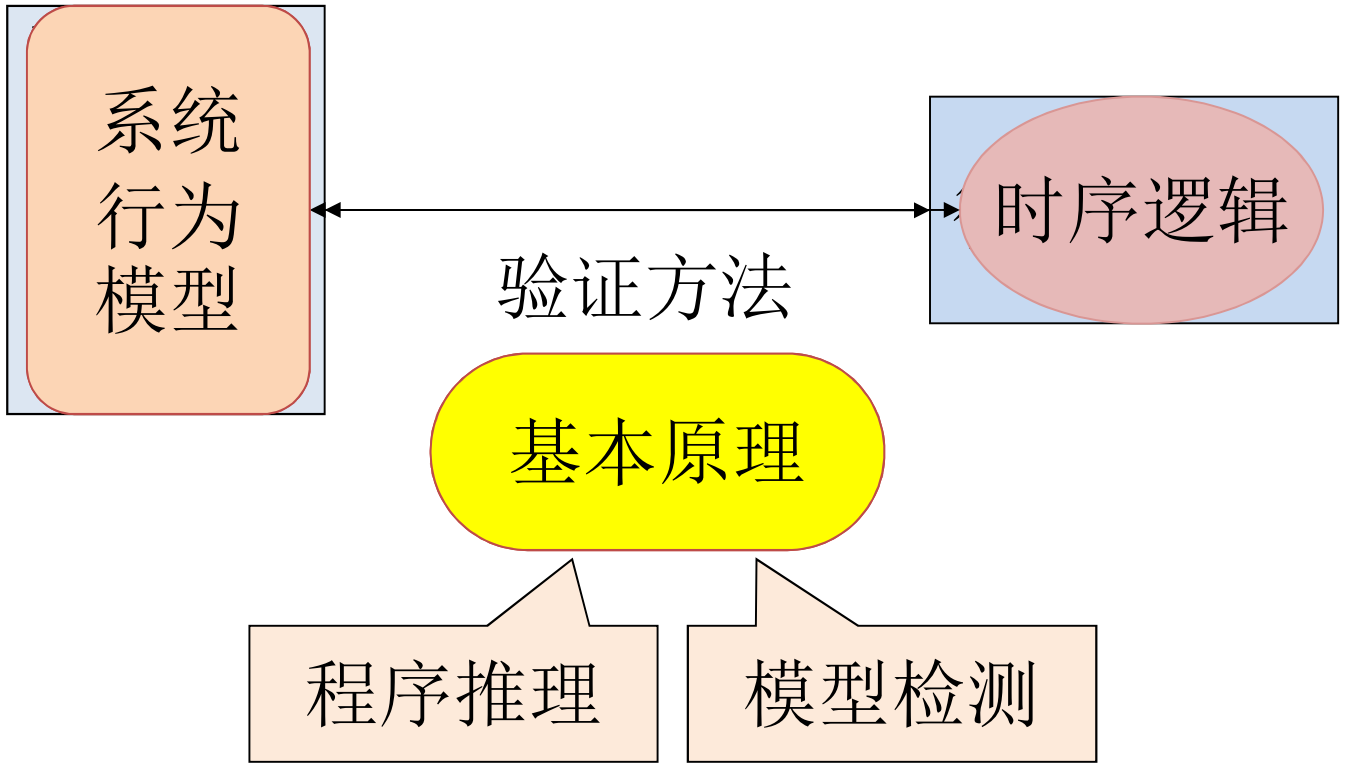
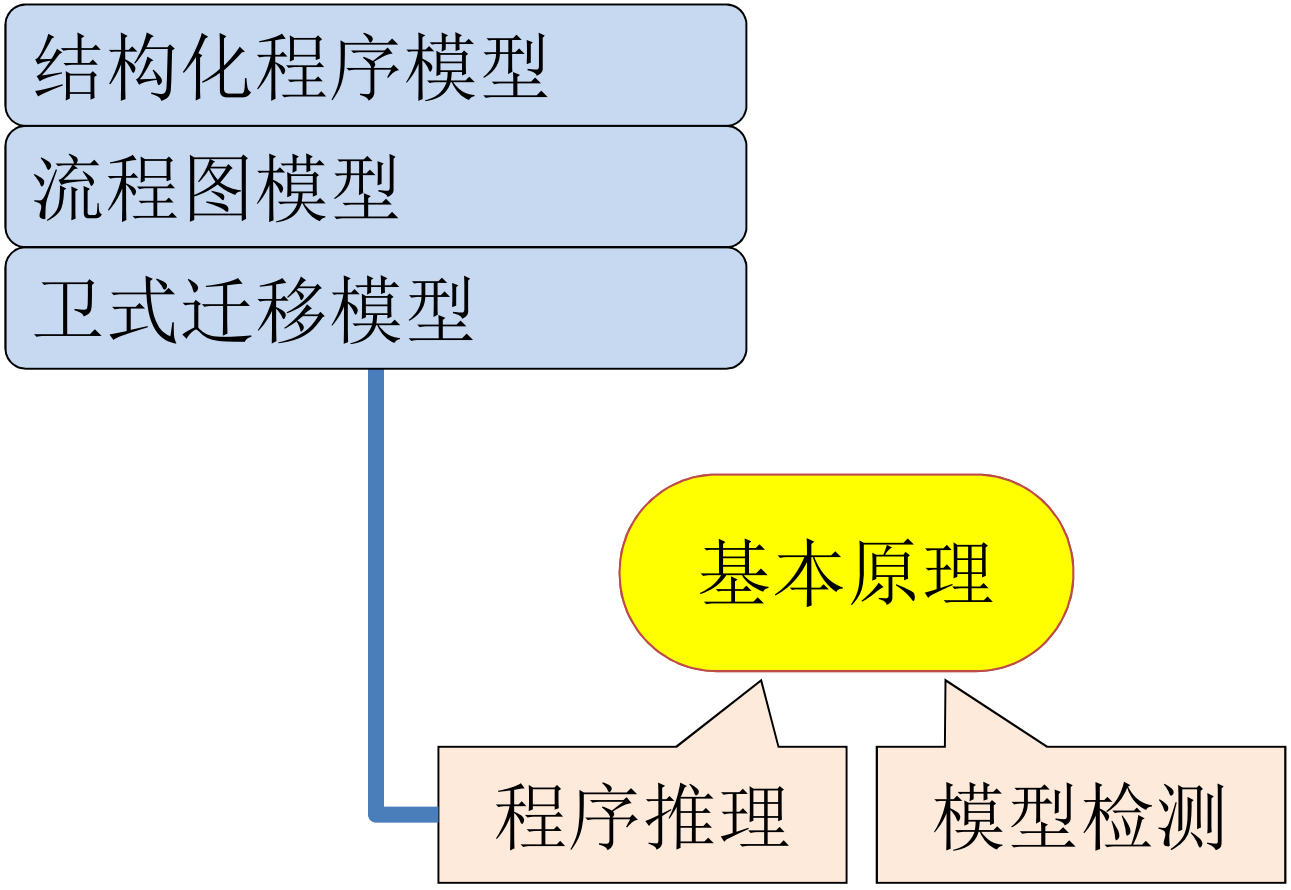
推理验证 -- 卫式迁移模型

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)



一阶(变量赋值)迁移模型

卫式迁移模型	$M=(T,\Theta)$
流程图模型	T
结构化程序模型	S

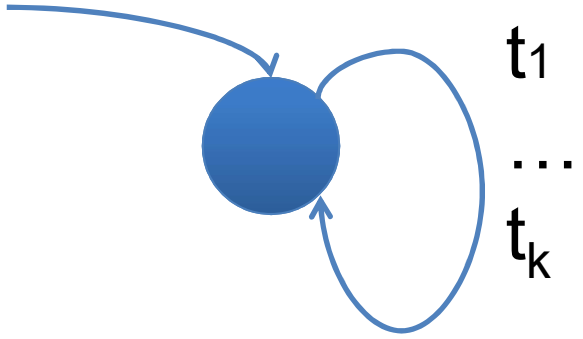
卫式迁移模型

M=(T,Θ)

给定B=(F,P)和变量集合V。

$\sigma_0 \rightarrow \sigma_1$

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



流程图模型

M=T

给定B=(F,P)和变量集合V。

$(L_0,\sigma_0)\rightarrow(L_1,\sigma_1)$

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

结构化程序模型

M=S

给定B=(F,P)和变量集合V。

$(S_0,\sigma_0)\rightarrow(S_1,\sigma_1)$

```
y1:=0; y2:=1; y3:=1;
while (y3<=x) do
        y1:=y1+1;
        y2:=y2+2;
        y3:=y3+y2
od;
ε
```

模型的运行

卫式迁移模型 $\sigma_0\ \sigma_1 \ldots$

流程图模型 $(BEG,\sigma_0)(L_1,\sigma_1)\ldots\ \ldots$

结构化程序模型 $(S_0,\sigma_0)(S_1,\sigma_1)\ldots\ \ldots$

$M \models \varphi$

$\pi \models \varphi$, for every computation π of M

Proof Rule (for R)

$$\phi \Rightarrow \varphi'$$

$$\varphi' \wedge \neg\psi \Rightarrow X\varphi'$$

$$\varphi' \Rightarrow \varphi$$

$$\phi \Rightarrow (\psi R \varphi)$$

Proof Rule (for U)

$\phi \Rightarrow (\psi \vee \varphi)$

$\varphi \Rightarrow (\varphi_0 \wedge w(t/x))$

$(\varphi \wedge t=v) \Rightarrow X(\psi \vee (\varphi \wedge t<v))$

$\phi \Rightarrow (\varphi_0 U \psi)$

Proof Rule (for X)

$\varphi \Rightarrow X\psi$

卫式迁移模型	$\sigma \rightarrow \sigma'$
流程图模型	$(L,\sigma) \rightarrow (L',\sigma')$
结构化程序模型	$(S,\sigma) \rightarrow (S',\sigma')$

卫式迁移模型

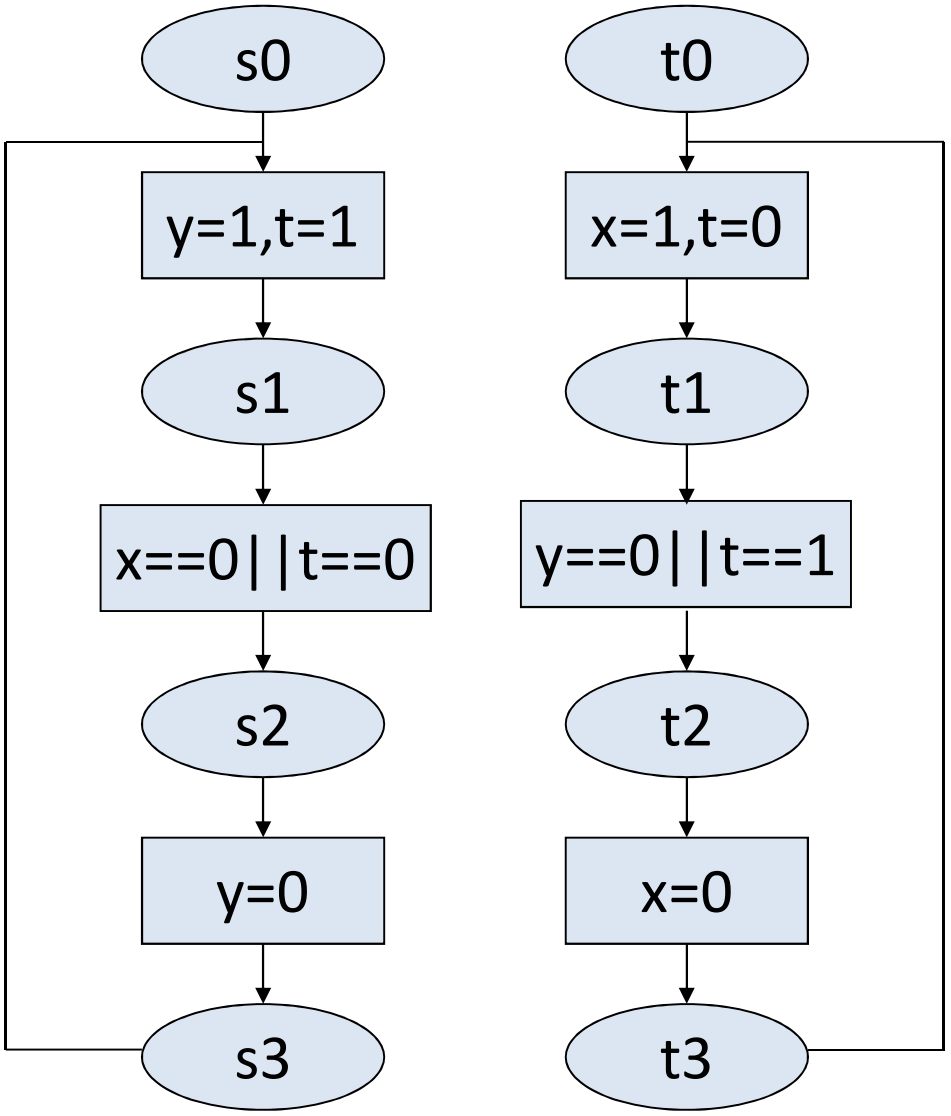
(Guarded Command Transition System)

- Correctness/Properties
  - Safety G, R, G(p→(q R r))
  - Inevitability F, U, G(p→(qU r))
- Assertions (Basic Theories)
  - Preconditions/Postconditions
  - Weakest Liberal Preconditions
- Verification Techniques
  - Safety G, R, G(p→(q R r))
  - Inevitability F, U, G(p→(qU r))

Contents

- Correctness
  - Safety G, R, G(p→(q R r))
  - Inevitability F, U, G(p→(qU r))
- Assertions (basic theories)
  - Preconditions/Postconditions
  - Weakest Liberal Preconditions
- Verification Techniques
  - Safety G, R, G(p→(q R r))
  - Inevitability F, U, G(p→(qU r))
- Verification Examples

Mutual Exclusion



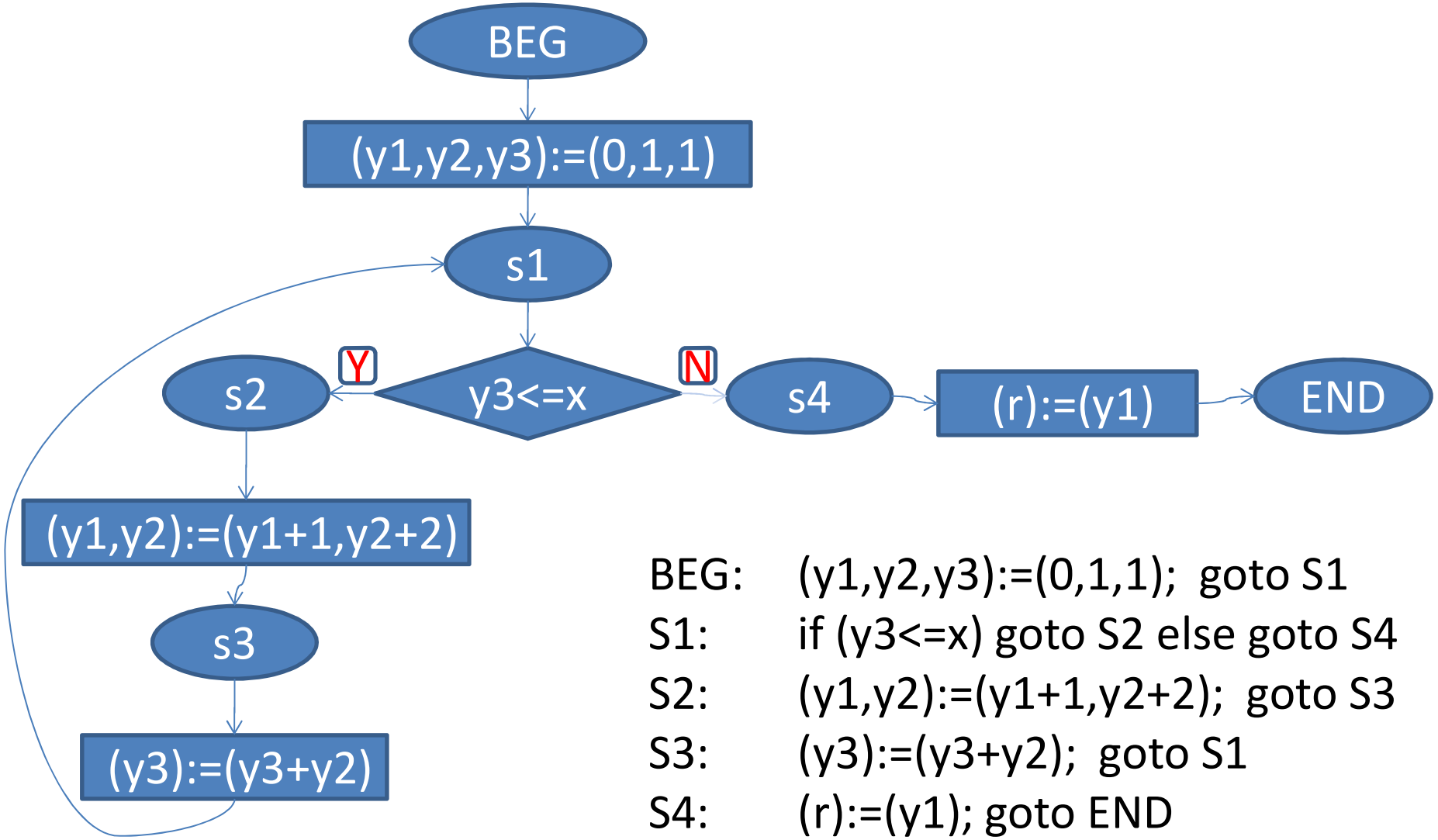
Initial States

s0
t0
x=0
y=0

Mutual Exclusion

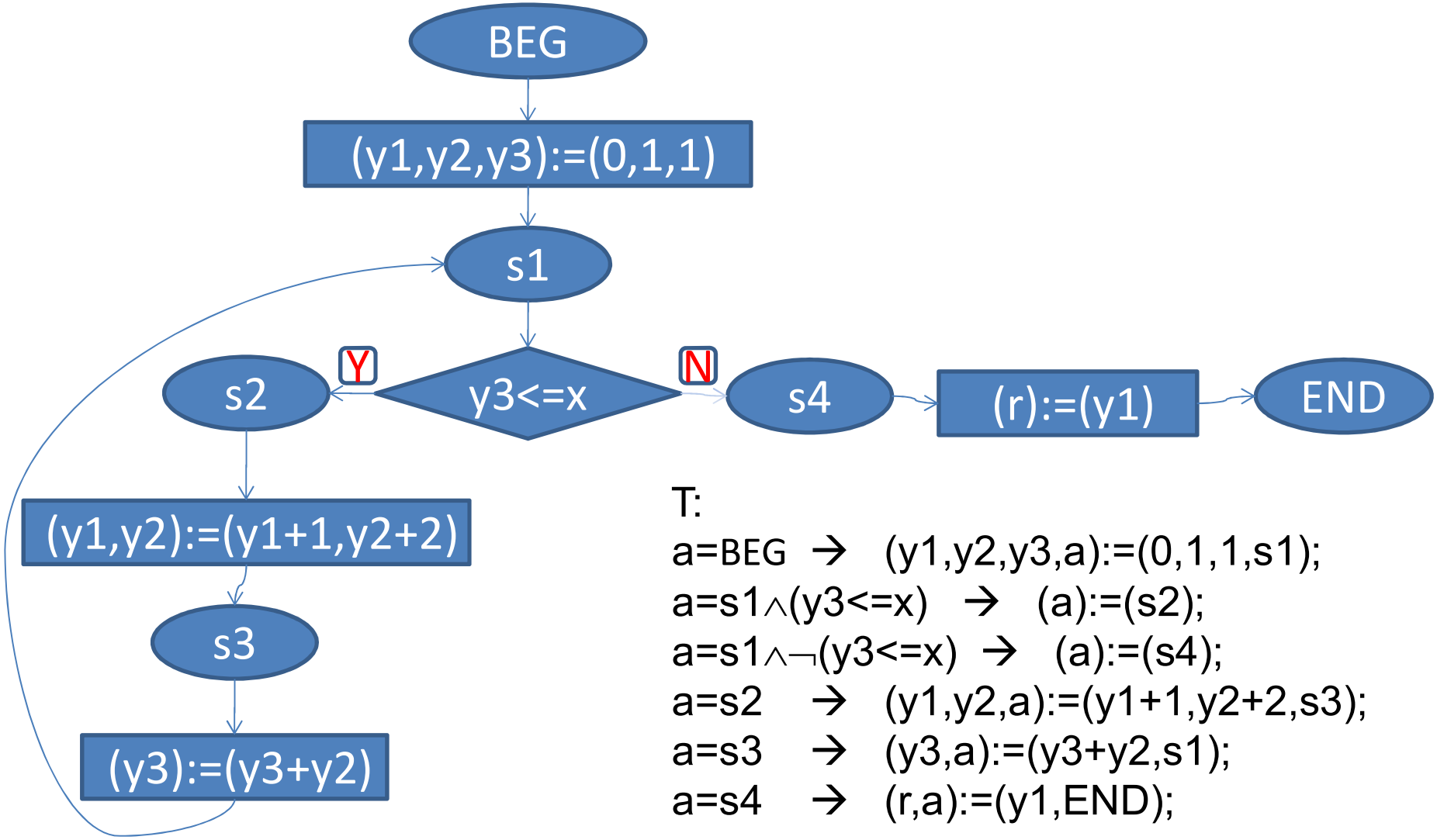
T:		Θ
a=s0$\rightarrow$	(y,t,a):=(1,1,s1);	x=0 $\wedge$
a=s1$\wedge$(x=0 $\vee$ t=0) $\rightarrow$	(a):=(s2);	y=0 $\wedge$
a=s2 $\rightarrow$	(y,a):=(0, s3);	a=s0 $\wedge$
a=s3$\rightarrow$	(y,t,a):=(1,1,s1);	b=t0
b=t0$\rightarrow$	(y,t,b):=(1,0,t1);	
b=t1$\wedge$(y=0 $\vee$ t=1) $\rightarrow$	(b):=(t2);	
b=t2 $\rightarrow$	(y,b):=(0, t3);	
b=t3$\rightarrow$	(y,t,b):=(1,0,t1);	

Integer Square Root



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

Integer Square Root



T:

a=BEG → (y1,y2,y3,a):=(0,1,1,s1);

a=s1∧(y3<=x) → (a):=(s2);

a=s1∧¬(y3<=x) → (a):=(s4);

a=s2 → (y1,y2,a):=(y1+1,y2+2,s3);

a=s3 → (y3,a):=(y3+y2,s1);

a=s4 → (r,a):=(y1,END);

Θ: a=BEG

Guarded Transition Systems

- B=(F,P)
- V
- I=(D,I_0)
- Σ

- I: Term → (Σ→D)
- I: WFF → (Σ→ {0,1})

M=(T,Θ)

(I) Correctness

Specification: FOLTL

DEFINITION

$M \models \phi$, iff

$\pi \models \phi$, for every computation π of M

Correctness

M |= G(q): p is a safety property of M

M |= F(q): p is an inevitability property of M

G(q), (p)R(q), G(p→(q R r))

F(q), (p)U(q), G(p→(qU r))

$\varphi \Rightarrow \psi$: G(φ→ψ)

(II) Assertions

t: $p \rightarrow (x_1,\ldots,x_n) := (e_1,\ldots,e_n)$

$\sigma \rightarrow^t \sigma'$: $\sigma \models p$ and $\sigma' = \sigma[x_1/I(e_1)\sigma]\ldots[x_n/I(e_n)\sigma]$

$\sigma \rightarrow^S \sigma'$: $\exists\, t \in S.(\sigma \rightarrow^t \sigma')$

DEFINITION

$\models \{ \varphi \}\, S\, \{ \psi \}$: $I(\varphi)(\sigma) \rightarrow \forall \sigma'.((\sigma \rightarrow^S \sigma') \rightarrow I(\psi)(\sigma'))$

φ and ψ are called the pre- and post-condition of S

EX

$\models \{ \varphi \}\ S\ \{ \psi \}$: $I(\varphi)(\sigma) \rightarrow \forall \sigma'.((\sigma \rightarrow^{S} \sigma') \rightarrow I(\psi)(\sigma'))$

t1: true → x:=x+1;

t2: y=1 → x:=x+2;

{ x>1 }	{ t1 }	{ x>2}
{y=1 → x>1 }	{ t2 }	{ x>2}
{x>1 }	{t1,t2}	{ x>2 }

Weakest Liberal Precondition

DEFINTION

ϕ is the weakest liberal precondition of (S,ψ),

denoted $\phi = wlp(S,\psi)$,

if $I(\phi)(\sigma)$ iff $\forall\sigma'.((\sigma \rightarrow^S \sigma') \rightarrow I(\psi)(\sigma'))$

PROPOSTION

If $(X \subseteq Y)$, then $wlp(Y,\varphi) \rightarrow wlp(X,\varphi)$

PROPOSTION

$\models \{ \varphi \} S \{ \psi \}$ iff $\varphi \rightarrow wlp(S, \psi)$

EX

$I(wlp(S,\psi))(\sigma)$ iff $\forall\sigma'.((\sigma \rightarrow^{S} \sigma') \rightarrow I(\psi)(\sigma'))$

t1: true → x:=x+1;
t2: y=1 → x:=x+2;

{ x>1 }	{ t1 }	{ x>2}
{y=1 → x>1 }	{ t2 }	{ x>2}
{x>1 }	{t1,t2}	{ x>2 }

wlp({t1},x>2) = (x>1)
wlp({t1},x>2) = (y=1 → x>0)
wlp({t1,t2},x>2) = (x>1)

Computation of wlp(S,ψ)

$I(\ wlp(S,\psi)\ )(\sigma) \leftrightarrow \forall\sigma'.((\sigma \rightarrow^{S} \sigma') \rightarrow I(\psi)(\sigma')\ )$

Define $[S]\psi$:

$[\{\}]\psi$ = true

$[\{t\}]\psi$ = $p \rightarrow \psi(e_1/x_1,\ldots, e_n/x_n)$

$[X \cup Y]\psi$ = $[X]\psi \wedge [Y]\psi$

PROPOSITION

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

EX

t1: true → x:=x+1;
t2: y=1 → x:=x+2;

{ x>1 }	{ t1 }	{ x>2}
{y=1 → x>1 }	{ t2 }	{ x>2}
{x>1 }	{t1,t2}	{ x>2 }

wlp({t1},x>2) = (x>1)
wlp({t1},x>2) = (y=1 → x>0)
wlp({t1,t2},x>2) = (x>1)

[{t1}](x>2) = (x>1)
[{t1}](x>2) = (y=1 → x>0)
[{t1,t2}](x>2) = (x>1)

Consequences

COROLLARY

$\models \{ \varphi \} S \{ \psi \}$ iff $\varphi \rightarrow [S]\psi$

The Next Operator

$M=(T,\Theta)$

$\varphi \Rightarrow X\psi$ iff
for all reachable σ, $I(\varphi)(\sigma) \rightarrow \forall\sigma'.((\sigma \rightarrow^{M} \sigma') \rightarrow I(\psi)(\sigma'))$

Suppose: $T = \{t_1,\ldots,t_n\} = \{p_1 \rightarrow a_1,\ldots,p_n \rightarrow a_n\}$

DEF: $E(T)=(p_1 \vee \ldots \vee p_n)$

DEF: $T^{+} = T \cup \{\neg E(T) \rightarrow (x):=(x)\}$

$\varphi \Rightarrow X\psi$ iff
for all reachable σ, $I(\varphi)(\sigma) \rightarrow \forall\sigma'.((\sigma \rightarrow^{T+} \sigma') \rightarrow I(\psi)(\sigma'))$

The Next Operator

$\varphi \Rightarrow X\psi$ iff $\varphi \Rightarrow wlp(T^+,\psi)$

$\varphi \Rightarrow X\psi$ iff $\varphi \Rightarrow [T^+]\psi$

$[T^+]\psi \equiv [T]\psi \wedge (E(T) \vee \psi))$

$\varphi \Rightarrow X\phi$ iff $\varphi \Rightarrow [T^+]\phi$

iff $\varphi \Rightarrow [T]\phi$ and $\varphi \Rightarrow (E(T) \vee \phi)$

iff $\varphi \Rightarrow [t_1]\phi$,…, $\varphi \Rightarrow [t_n]\phi$ and $\varphi \Rightarrow (E(T) \vee \phi)$

Proof Rule for X

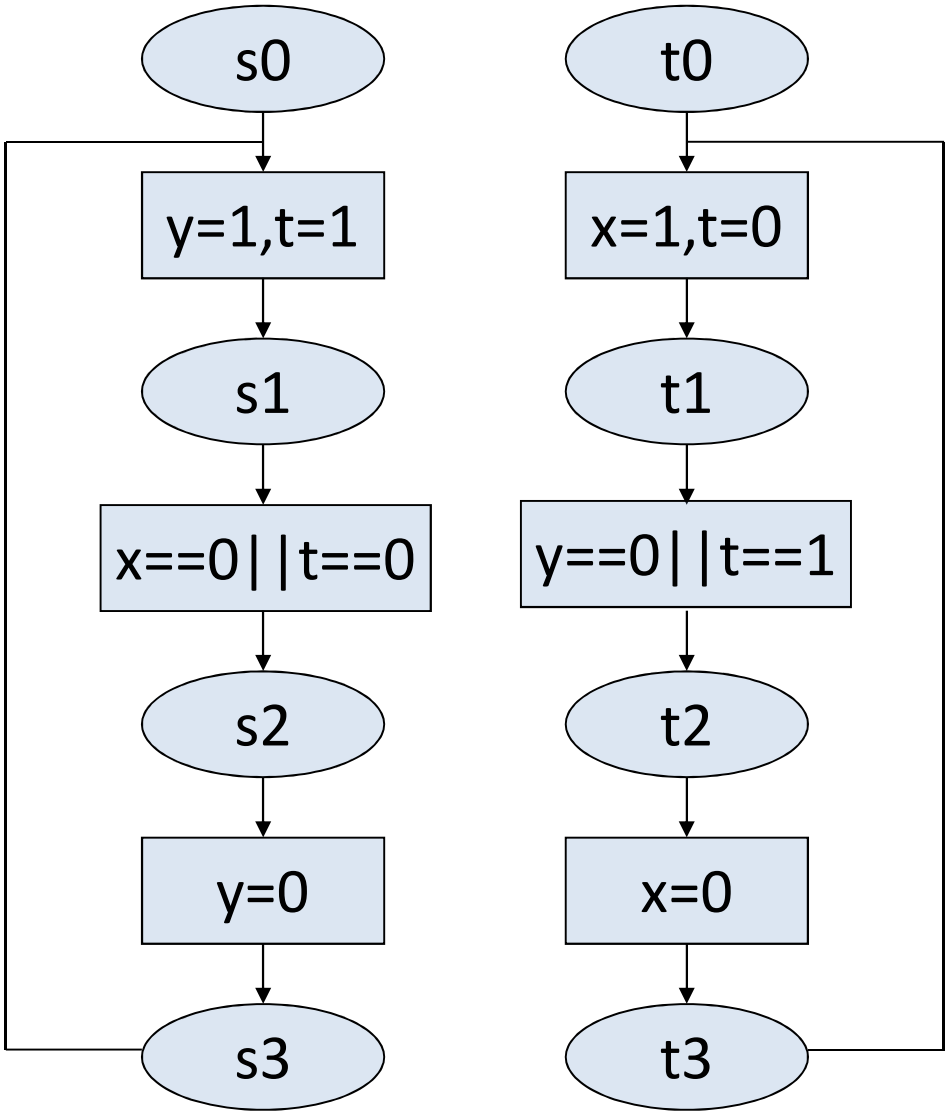
$$\frac{\varphi \Rightarrow [T^+]\psi}{\varphi \Rightarrow X\psi}$$

$$\frac{\varphi \Rightarrow E(T) \vee \psi \qquad \varphi \Rightarrow [T]\psi}{\varphi \Rightarrow X\psi}$$

$M=(T,\Theta)$

$I(\varphi)(\sigma) \rightarrow ((\sigma \rightarrow^M \sigma') \rightarrow I(\psi)(\sigma'))$

Mutual Exclusion



Initial States

s0
t0
x=0
y=0

Mutual Exclusion

T:		Θ
a=s0$\rightarrow$	(y,t,a):=(1,1,s1);	x=0 $\wedge$
a=s1$\wedge$(x=0 $\vee$ t=0) $\rightarrow$	(a):=(s2);	y=0 $\wedge$
a=s2 $\rightarrow$	(y,a):=(0, s3);	a=s0 $\wedge$
a=s3$\rightarrow$	(y,t,a):=(1,1,s1);	b=t0
b=t0$\rightarrow$	(y,t,b):=(1,0,t1);	
b=t1$\wedge$(y=0 $\vee$ t=1) $\rightarrow$	(b):=(t2);	
b=t2 $\rightarrow$	(y,b):=(0, t3);	
b=t3$\rightarrow$	(y,t,b):=(1,0,t1);	

Examples

1. Compute: wlp(T,b!=t2)

2. Prove: $(b!=t1 \wedge b!=t2) \Rightarrow X(b!=t2)$

Compute wlp(T,b!=t2)

wlp(T,b!=t2) = [T](b!=t2)

T:

t1:	a=s0$\rightarrow$	(y,t,a):=(1,1,s1);
t2:	a=s1$\wedge$(x=0 $\vee$ t=0) $\rightarrow$	(a):=(s2);
t3:	a=s2 $\rightarrow$	(y,a):=(0, s3);
t4:	a=s3$\rightarrow$	(y,t,a):=(1,1,s1);
t5:	b=t0$\rightarrow$	(y,t,b):=(1,0,t1);
t6:	b=t1$\wedge$(y=0 $\vee$ t=1) $\rightarrow$	(b):=(t2);
t7:	b=t2 $\rightarrow$	(y,b):=(0, t3);
t8:	b=t3$\rightarrow$	(y,t,b):=(1,0,t1);

[T](b!=t2)

t1:	$a=s0 \rightarrow$	(y,t,a):=(1,1,s1);
t2:	$a=s1 \wedge (x=0 \vee t=0) \rightarrow$	(a):=(s2);
t3:	$a=s2 \rightarrow$	(y,a):=(0, s3);
t4:	$a=s3 \rightarrow$	(y,t,a):=(1,1,s1);
t5:	$b=t0 \rightarrow$	(y,t,b):=(1,0,t1);
t6:	$b=t1 \wedge (y=0 \vee t=1) \rightarrow$	(b):=(t2);
t7:	$b=t2 \rightarrow$	(y,b):=(0, t3);
t8:	$b=t3 \rightarrow$	(y,t,b):=(1,0,t1);

[t1](b!=t2) =	$a=s0 \rightarrow$ (b!=t2)
[t2](b!=t2) =	$a=s1 \wedge (x=0 \vee t=0) \rightarrow$ (b!=t2)
[t3](b!=t2) =	$a=s2 \rightarrow$ (b!=t2)
[t4](b!=t2) =	$a=s3 \rightarrow$ (b!=t2)

[T](b!=t2)

t1:	$a=s0 \rightarrow$	(y,t,a):=(1,1,s1);
t2:	$a=s1 \wedge (x=0 \vee t=0) \rightarrow$	(a):=(s2);
t3:	$a=s2 \rightarrow$	(y,a):=(0, s3);
t4:	$a=s3 \rightarrow$	(y,t,a):=(1,1,s1);
t5:	$b=t0 \rightarrow$	(x,t,b):=(1,0,t1);
t6:	$b=t1 \wedge (y=0 \vee t=1) \rightarrow$	(b):=(t2);
t7:	$b=t2 \rightarrow$	(x,b):=(0, t3);
t8:	$b=t3 \rightarrow$	(x,t,b):=(1,0,t1);

[t5](b!=t2) =	$b=t0 \rightarrow$ (t1!=t2)
[t6](b!=t2) =	$b=t1 \wedge (y=0 \vee t=1) \rightarrow$ (t2!=t2)
[t7](b!=t2) =	$b=t2 \rightarrow$ (t3!=t2)
[t8](b!=t2) =	$b=t3 \rightarrow$ (t1!=t2)

[T](b!=t2)

=

$[t1](b!=t2) \wedge [t2](b!=t2) \wedge [t3](b!=t2) \wedge [t4](b!=t2) \wedge$
$[t5](b!=t2) \wedge [t6](b!=t2) \wedge [t7](b!=t2) \wedge [t8](b!=t2)$

=

$(a=s0 \rightarrow (b!=t2)) \wedge$
$(a=s1 \wedge (x=0 \vee t=0) \rightarrow (b!=t2)) \wedge$
$(a=s2 \rightarrow (b!=t2)) \wedge$
$(a=s3 \rightarrow (b!=t2)) \wedge$
$(b=t0 \rightarrow (t1!=t2)) \wedge$
$(b=t1 \wedge (y=0 \vee t=1) \rightarrow (t2!=t2)) \wedge$
$(b=t2 \rightarrow (t3!=t2)) \wedge$
$(b=t3 \rightarrow (t1!=t2))$

Simplification

[T](b!=t2)

=

$[t1](b!=t2) \wedge [t2](b!=t2) \wedge [t3](b!=t2) \wedge [t4](b!=t2) \wedge$
$[t5](b!=t2) \wedge [t6](b!=t2) \wedge [t7](b!=t2) \wedge [t8](b!=t2)$

=

$(a=s0 \rightarrow (b!=t2)) \wedge$
$(a=s1 \wedge (x=0 \vee t=0) \rightarrow (b!=t2)) \wedge$
$(a=s2 \rightarrow (b!=t2)) \wedge$
$(a=s3 \rightarrow (b!=t2)) \wedge$
$\neg(b=t1 \wedge (y=0 \vee t=1))$

Prove (b!=t1 $\wedge$b!=t2) $\Rightarrow$ X(b!=t2)

We have the proof rule:

$\varphi \Rightarrow$ E(T)$\vee$ ψ
$\varphi \Rightarrow$ [T]ψ

$\varphi \Rightarrow$ Xψ

Need to prove
(b!=t1 $\wedge$b!=t2) $\Rightarrow$ E(T) $\vee$ (b!=t2) and
(b!=t1 $\wedge$b!=t2) $\Rightarrow$ [T](b!=t2)

$(b!=t1 \wedge b!=t2) \Rightarrow [T](b!=t2)$

$(b!=t1 \wedge b!=t2) \Rightarrow [T](b!=t2)$

iff $(b!=t1 \wedge b!=t2) \Rightarrow$
$(a=s0 \rightarrow (b!=t2)) \wedge$
$(a=s1 \wedge (x=0 \vee t=0) \rightarrow (b!=t2)) \wedge$
$(a=s2 \rightarrow (b!=t2)) \wedge$
$(a=s3 \rightarrow (b!=t2)) \wedge$
$\neg(b=t1 \wedge (y=0 \vee t=1))$

iff $(b!=t1 \wedge b!=t2) \Rightarrow \neg(b=t1 \wedge (y=0 \vee t=1))$

iff true

Current-Time

$M=(T,\Theta)$

$$M \models \Theta \rightarrow \varphi$$

$$M \models \varphi$$

Summary

Given $M=(T,\Theta)$:

$$\varphi \Rightarrow E(T) \vee \psi$$

$$\varphi \Rightarrow [T]\psi$$

$$\varphi \Rightarrow X\psi$$

$$M \models \Theta \rightarrow \varphi$$

$$M \models \varphi$$

(III) Verification Techniques

(III.a) Proof Rule (for R) - FOLTL

$$\phi \Rightarrow \varphi'$$

$$\varphi' \wedge \neg\psi \Rightarrow X\varphi'$$

$$\varphi' \Rightarrow \varphi$$

$$\phi \Rightarrow (\psi R \varphi)$$

Proof Rule (for R)

$$\varphi \Rightarrow \mathsf{E}(\mathsf{T}) \vee \psi$$
$$\varphi \Rightarrow [\mathsf{T}]\,\psi$$

$$\varphi \Rightarrow \mathsf{X}\,\psi$$

$$\phi \Rightarrow \varphi'$$
$$\varphi' \wedge \neg\psi \Rightarrow \mathsf{X}\varphi'$$
$$\varphi' \Rightarrow \varphi$$

$$\phi \Rightarrow (\psi \mathsf{R} \varphi)$$

$$\varphi' \wedge \neg\psi \Rightarrow \mathsf{E}(\mathsf{T}) \vee \varphi'$$
$$\varphi' \wedge \neg\psi \Rightarrow [\mathsf{T}]\,\varphi'$$

$$\varphi' \wedge \neg\psi \Rightarrow \mathsf{X}\,\varphi'$$

Proof Rule (for R)

$$\phi \Rightarrow \varphi'$$

$$\varphi' \wedge \neg\psi \Rightarrow [T]\, \varphi'$$

$$\varphi' \Rightarrow \varphi$$

$$\phi \Rightarrow (\psi R \varphi)$$

Proof Rule (for G)

$$\phi \Rightarrow \varphi'$$

$$\varphi' \Rightarrow [T]\, \varphi'$$

$$\varphi' \Rightarrow \varphi$$

$$\phi \Rightarrow G\varphi$$

例子

Mutual Exclusion (P1)

$B = (\{s_0, s_1, s_2, s_3, t_0, t_1, t_2, t_3, 0, 1\}, \{=\})$, $V = \{a, b, x, y, t\}$
$M = (T, \Theta)$ over (B, V) as follows, with the usual interpretation I.

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	$(a = s_0 \wedge b = t_0 \wedge x = 0 \wedge y = 0 \wedge t = 0)$		

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

Proof Rule

Proof Rule:

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

We have:

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

Attempt 1

Proof Rule:

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

We have:

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

Remain to prove:

$$\varphi' \wedge \neg\psi \rightarrow [T]\varphi'$$

Attempt 1

(1)
t_1: $a = s_0 \longrightarrow (y, t, a) := (1, 1, s_1)$
$[t_1]\varphi' = (a = s0 \rightarrow \varphi'(1/y, 1/t, s_1/a)) = (a = s0 \rightarrow b \neq t_2)$
$\varphi' \wedge \neg\psi \rightarrow [t_1]\varphi'$: $(b \neq t_2) \wedge \neg(a = s_2) \rightarrow [t_1](b \neq t_2)$
OK.

...
(6)
t_6: $b = t_1 \wedge (y = 0 \vee t = 1) \longrightarrow (b) := (t_2)$
$[t_6]\varphi' = (b = t_1 \wedge (y = 0 \vee t = 1) \rightarrow t_2 \neq t_2)$
$\varphi' \wedge \neg\psi \rightarrow [t_6]\varphi'$: $(b \neq t_2) \wedge \neg(a = s_2) \rightarrow [t_6](b \neq t_2)$
FAIL.

NEED to strengthen φ'.

Attempt 2

Proof Rule:

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

We have:

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

Remain to prove:

$$\varphi' \wedge \neg\psi \rightarrow [T]\varphi'$$

Attempt 2

Try to prove $\varphi' \wedge \neg\psi \rightarrow [t_6]\varphi'$

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

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

$$
\begin{array}{l}
((a = s_1 \wedge ((b = t_1 \wedge x = 1 \wedge t = 0))) \wedge (y = 0) \\
\rightarrow (a = s_2)
\end{array}
$$

FAIL.

Solution

Proof Rule:

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

We have:

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

Remain to prove:

$$\varphi' \wedge \neg\psi \rightarrow [T]\varphi'$$

Solution OK

Try to prove $\varphi' \wedge \neg\psi \rightarrow [t_6]\varphi'$

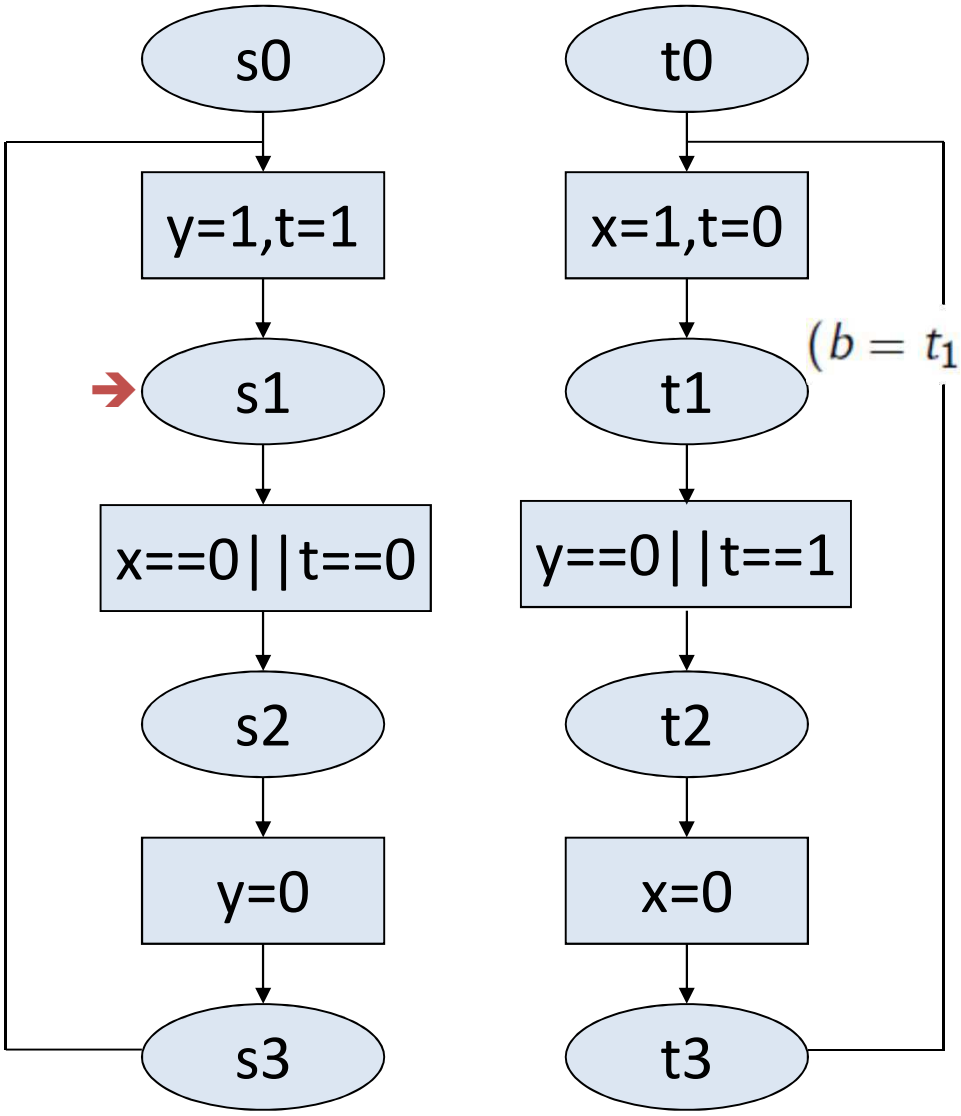
$$
\begin{array}{l}
((a = s_1 \wedge (b = t_0 \vee b = t_3 \vee (b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1))) \vee \\
(a = s_2 \wedge b \neq t_2)) \wedge (a \neq s_2) \wedge (b = t_1 \wedge (y = 0 \vee t = 1)) \\
\rightarrow (a = s_1 \wedge (t_2 = t_0 \vee t_2 = t_3 \vee (t_2 = t_1 \wedge x = 1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

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

$$
\begin{array}{l}
((a = s_1 \wedge ((b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1)))) \wedge (y = 0) \\
\rightarrow \mathit{false}
\end{array}
$$

OK.

Mutual Exclusion



$(b = t_1 \wedge x = 1 \wedge t = 0 \wedge y = 1)$

Initial States

s0
t0
x=0
y=0

Further Thinking

$$a = s_1 \wedge b \neq t_1 \wedge b \neq t_2 \Rightarrow (a = s_2 R b \neq t_2)$$

$$a = s_1 \wedge (b = t_0 \vee b = t_3) \Rightarrow (a = s_2 R b \neq t_2)$$

$a = s_1 \wedge (b = t_0) \Rightarrow (a = s_2 R b \neq t_2)$ and
$a = s_1 \wedge (b = t_3) \Rightarrow (a = s_2 R b \neq t_2)$

May be easier to prove the last two properties.

$$\frac{\zeta_0 \Rightarrow \psi R \varphi \qquad \zeta_1 \Rightarrow \psi R \varphi}{\zeta_0 \vee \zeta_1 \Rightarrow \psi R \varphi}$$

Integer Square Root (P1)

Given $M = (T, \Theta)$, and the usual interpretation I over integers.

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	$(a = s_0)$		

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

Preparation

Proof Rule:

$$\frac{\begin{array}{l}\zeta \Rightarrow \varphi' \\ \varphi' \rightarrow [T]\varphi' \\ \varphi' \Rightarrow \varphi\end{array}}{\zeta \Rightarrow G\varphi}$$

Suppose that we have
$(T, \Theta) \models_I G(a = s_0 \wedge x > 0 \rightarrow G(a = s_4 \rightarrow y_1 = \sqrt{x}))$

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

In addition, we have $(T, \Theta) \models_I a = s_0$.

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

Proof Rule

Proof Rule:

$$\frac{\begin{array}{l}\zeta \Rightarrow \varphi' \\ \varphi' \rightarrow [T]\varphi' \\ \varphi' \Rightarrow \varphi\end{array}}{\zeta \Rightarrow G\varphi}$$

We have:

$$\begin{array}{lcl}\zeta & \equiv & (x > 0 \wedge a = s_0) \\ \varphi & \equiv & (a = s_4 \rightarrow y_1 = \sqrt{x}) \\ \varphi' & \equiv & ?\end{array}$$

Solution

Let

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

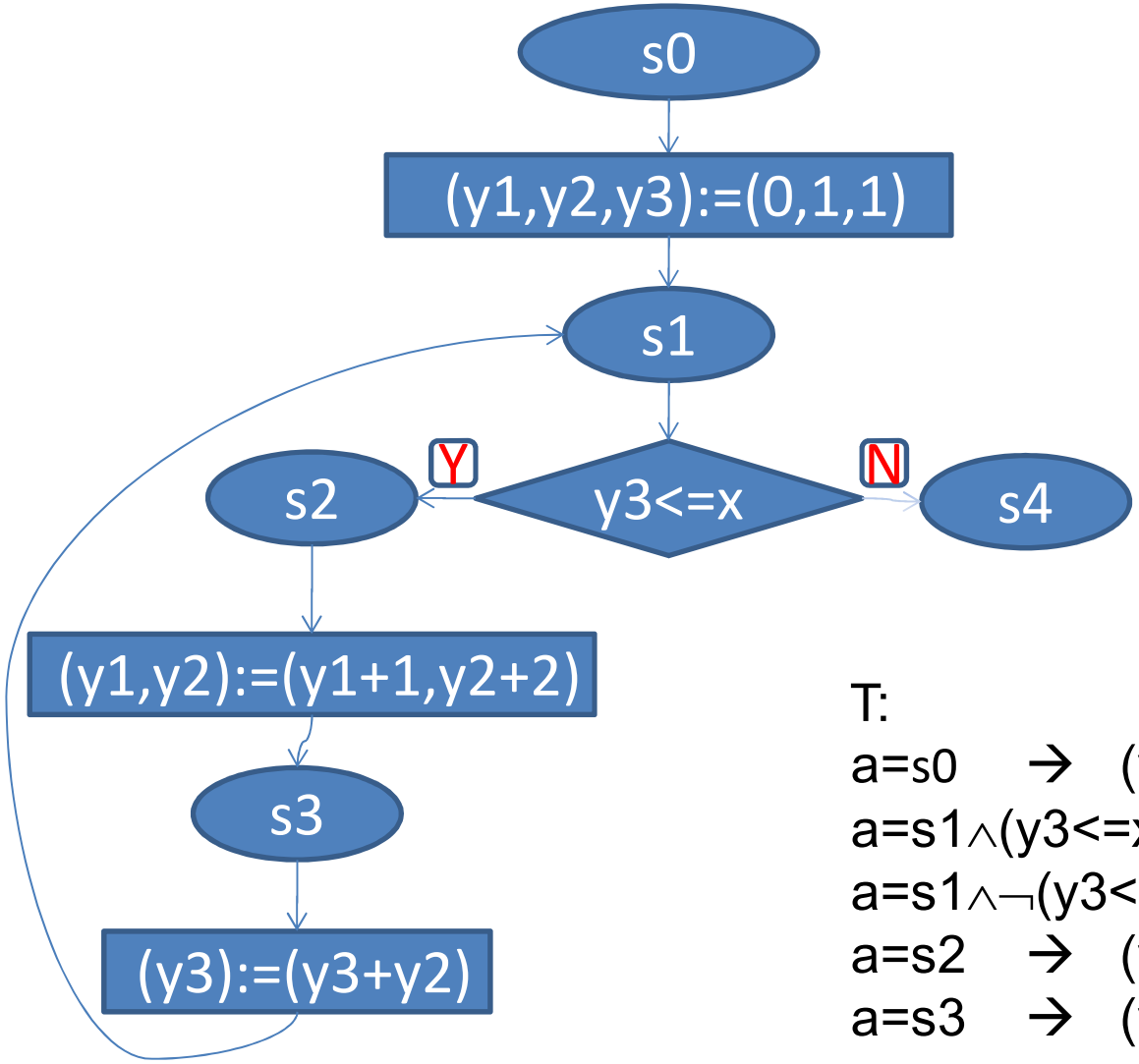
where

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

Remain to prove:

$$\varphi' \rightarrow [T]\varphi'$$

Integer Square Root



T:

a=s0 → (y1,y2,y3,a):=(0,1,1,s1);

a=s1∧(y3<=x) → (a):=(s2);

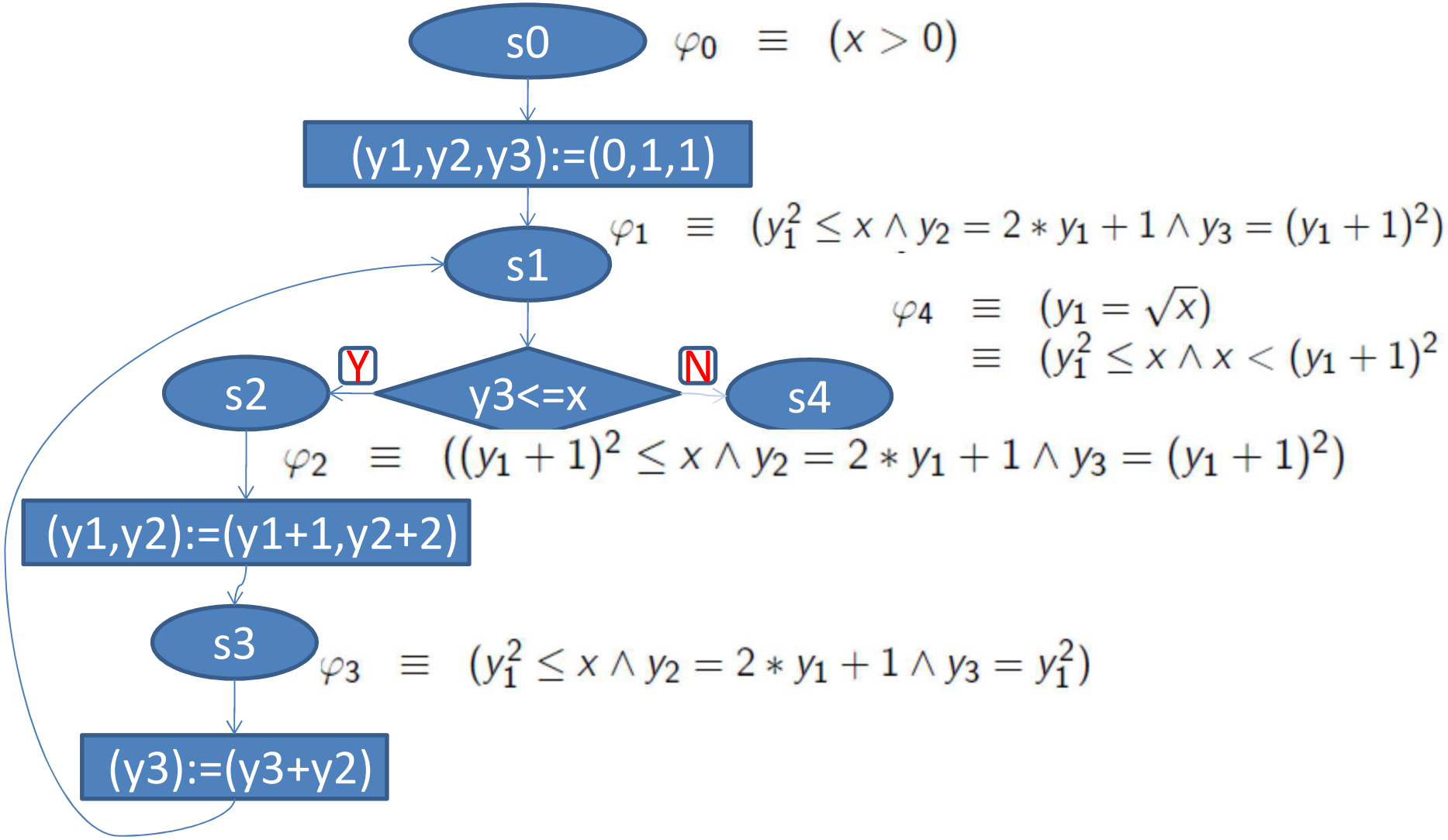
a=s1∧¬(y3<=x) → (a):=(s4);

a=s2 → (y1,y2,a):=(y1+1,y2+2,s3);

a=s3 → (y3,a):=(y3+y2,s1);

Θ: a=s0

Integer Square Root



(III.b) Proof Rule (for U)

$$\phi \Rightarrow (\psi \vee \varphi)$$

$$\varphi \Rightarrow (\varphi_0 \wedge w(t/x))$$

$$(\varphi \wedge t=v) \Rightarrow X(\psi \vee (\varphi \wedge t<v))$$

$$\phi \Rightarrow (\varphi_0 U \psi)$$

(III.b) Proof Rule (for U)

$$\phi \Rightarrow (\psi \vee \varphi)$$

$$\varphi \Rightarrow (\varphi_0 \wedge w(t/x))$$

$$(\varphi \wedge t=v) \Rightarrow X(\psi \vee (\varphi \wedge t<v))$$

$$\phi \Rightarrow (\varphi_0 U \psi)$$

$$(\varphi \wedge t=v) \Rightarrow (E(T) \vee (\psi \vee (\varphi \wedge t<v)))$$

$$(\varphi \wedge t=v) \Rightarrow [T](\psi \vee (\varphi \wedge t<v))$$

$$(\varphi \wedge t=v) \Rightarrow X(\psi \vee (\varphi \wedge t<v))$$

(III.b) Proof Rule (for U)

$$\phi \Rightarrow (\psi \vee \varphi)$$

$$\varphi \Rightarrow (\varphi_0 \wedge w(t/x))$$

$$(\varphi \wedge t=v) \Rightarrow X(\psi \vee (\varphi \wedge t<v))$$

$$\phi \Rightarrow (\varphi_0 U \psi)$$

$$(\varphi \wedge t=v) \Rightarrow (E(T) \vee (\psi))$$

$$(\varphi \wedge t=v) \Rightarrow [T](\psi \vee (\varphi \wedge t<v))$$

$$(\varphi \wedge t=v) \Rightarrow X(\psi \vee (\varphi \wedge t<v))$$

(III.b) Proof Rule (for U)

$$\phi \Rightarrow (\psi \vee \varphi)$$

$$\varphi \Rightarrow (\varphi_0 \wedge w(t/x))$$

$$(\varphi \wedge t{=}v) \Rightarrow X(\psi \vee (\varphi \wedge t{<}v))$$

$$\phi \Rightarrow (\varphi_0 U \psi)$$

$$(\varphi) \Rightarrow (E(T) \vee (\psi))$$

$$(\varphi \wedge t{=}v) \Rightarrow [T](\psi \vee (\varphi \wedge t{<}v))$$

$$(\varphi \wedge t{=}v) \Rightarrow X(\psi \vee (\varphi \wedge t{<}v))$$

Proof Rule (for U)

$$\phi \Rightarrow (\psi \vee \varphi)$$

$$\varphi \Rightarrow (\varphi_0 \wedge w(t/x)) \wedge (E(T) \vee \psi)$$

$$(\varphi \wedge t=v) \Rightarrow [T](\psi \vee (\varphi \wedge t<v))$$

$$\phi \Rightarrow (\varphi_0 U \psi)$$

Proof Rule (for F)

$$\phi \Rightarrow (\psi \vee \varphi)$$

$$\varphi \Rightarrow (w(t/x) \wedge (E(T) \vee \psi))$$

$$(\varphi \wedge t=v) \Rightarrow [T](\psi \vee (\varphi \wedge t<v))$$

$$\phi \Rightarrow F\psi$$

例子 EE

Mutual Exclusion (P2)

Given $M = (T, \Theta)$, and the usual interpretation I.

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	$(a = s_0 \wedge b = t_0 \wedge x = 0 \wedge y = 0 \wedge t = 0)$		

Prove: $(T, \Theta) \models_I G(a = s_1 \rightarrow F(a = s_2))$

Proof Rule

Proof Rule:

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

We have:

$$\begin{array}{lcl}\varphi & \equiv & (a = s_1) \\ \psi & \equiv & (a = s_2) \\ \zeta & \equiv & ? \\ w & \equiv & ? \\ e & \equiv & ?\end{array}$$

We may assume $(T, \Theta) \models_I G(E(T))$

Attempt 1

Define f such that:

$$I(f(t_0,0)) = 1 \quad I(f(t_1,0)) = 0 \quad I(f(t_2,0)) = 2 \quad I(f(t_3,0)) = 1$$
$$I(f(t_0,1)) = 1 \quad I(f(t_1,1)) = 3 \quad I(f(t_2,1)) = 2 \quad I(f(t_3,1)) = 1$$

Let

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

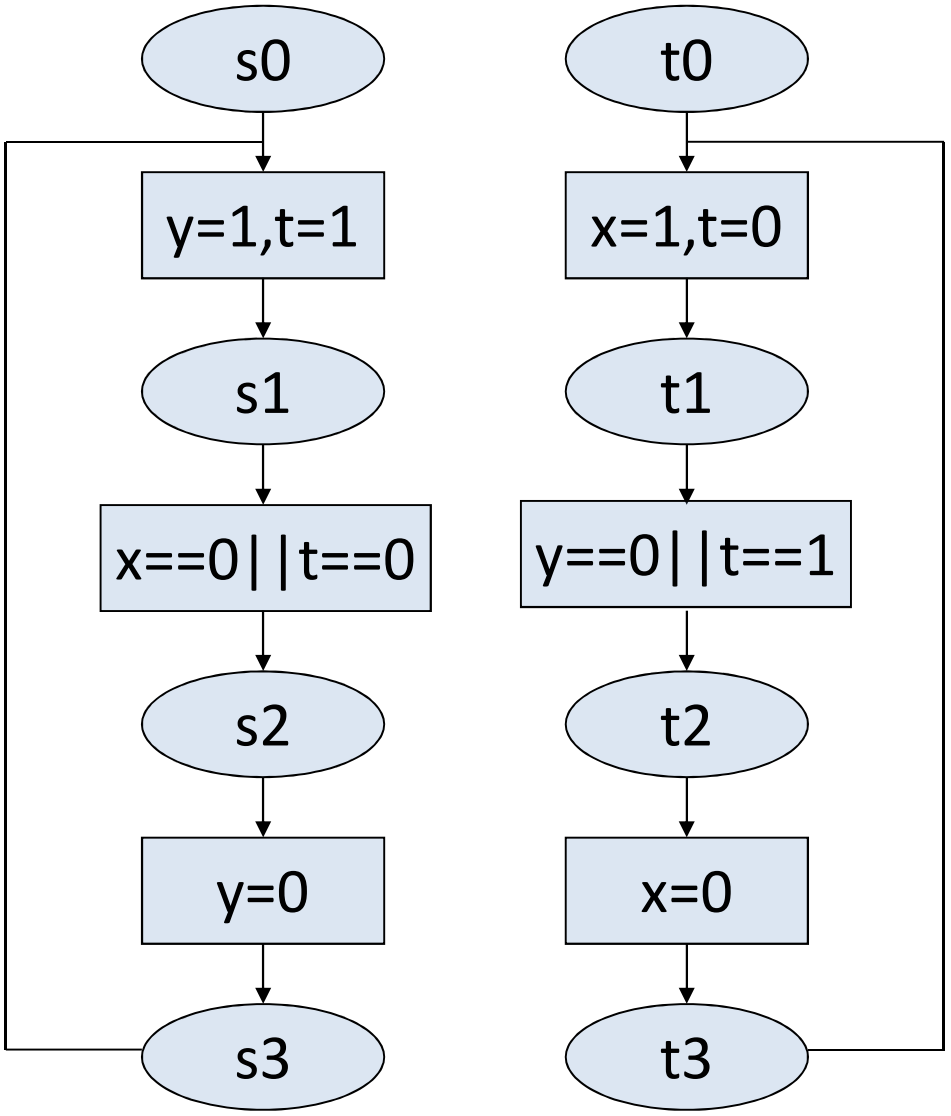
Need

$$\varphi \Rightarrow (\psi \vee \zeta)$$
$$\zeta \Rightarrow w_x^e \wedge (\psi \vee E(T))$$
$$\zeta \wedge e = v \rightarrow [T](\psi \vee (\zeta \wedge e < v))$$

Remain to prove:

$$\zeta \wedge e = v \rightarrow [T](\psi \vee (\zeta \wedge e < v))$$

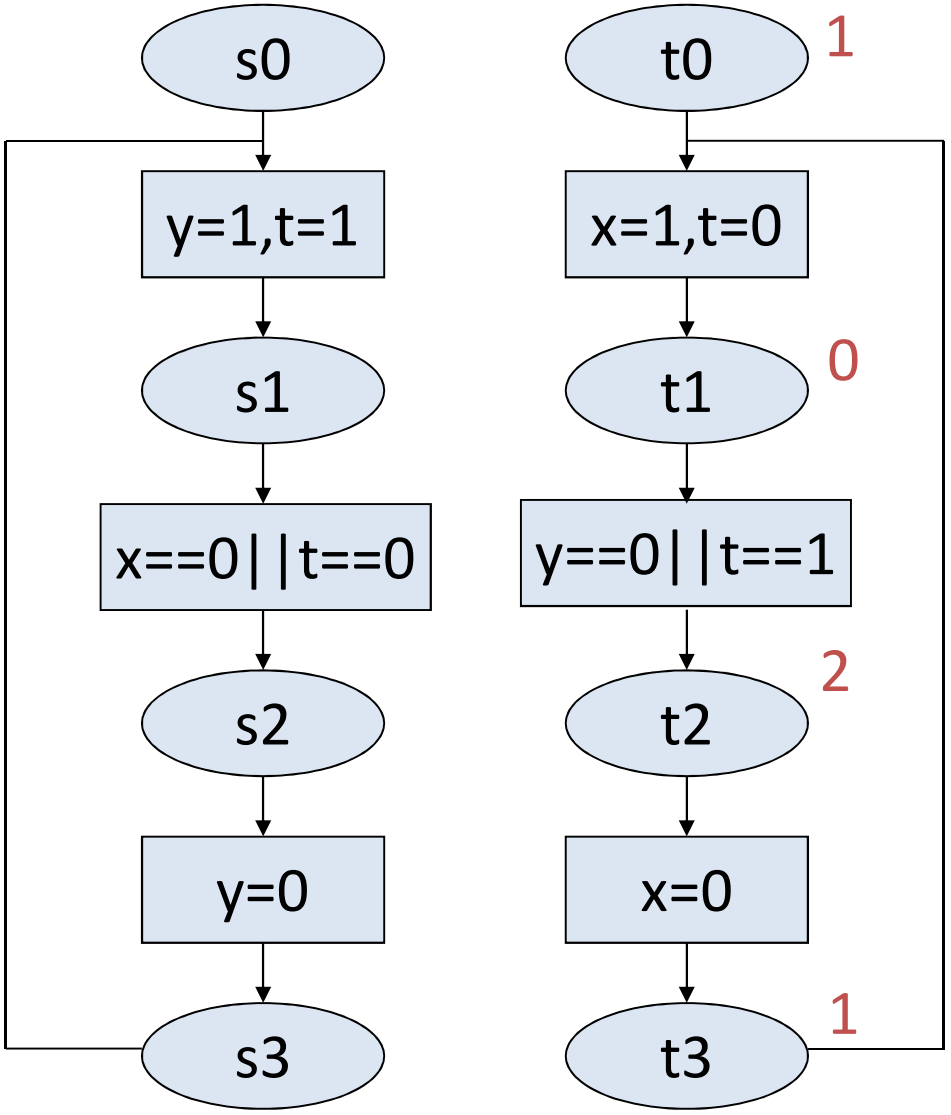
Mutual Exclusion



Initial States

s0
t0
x=0
y=0

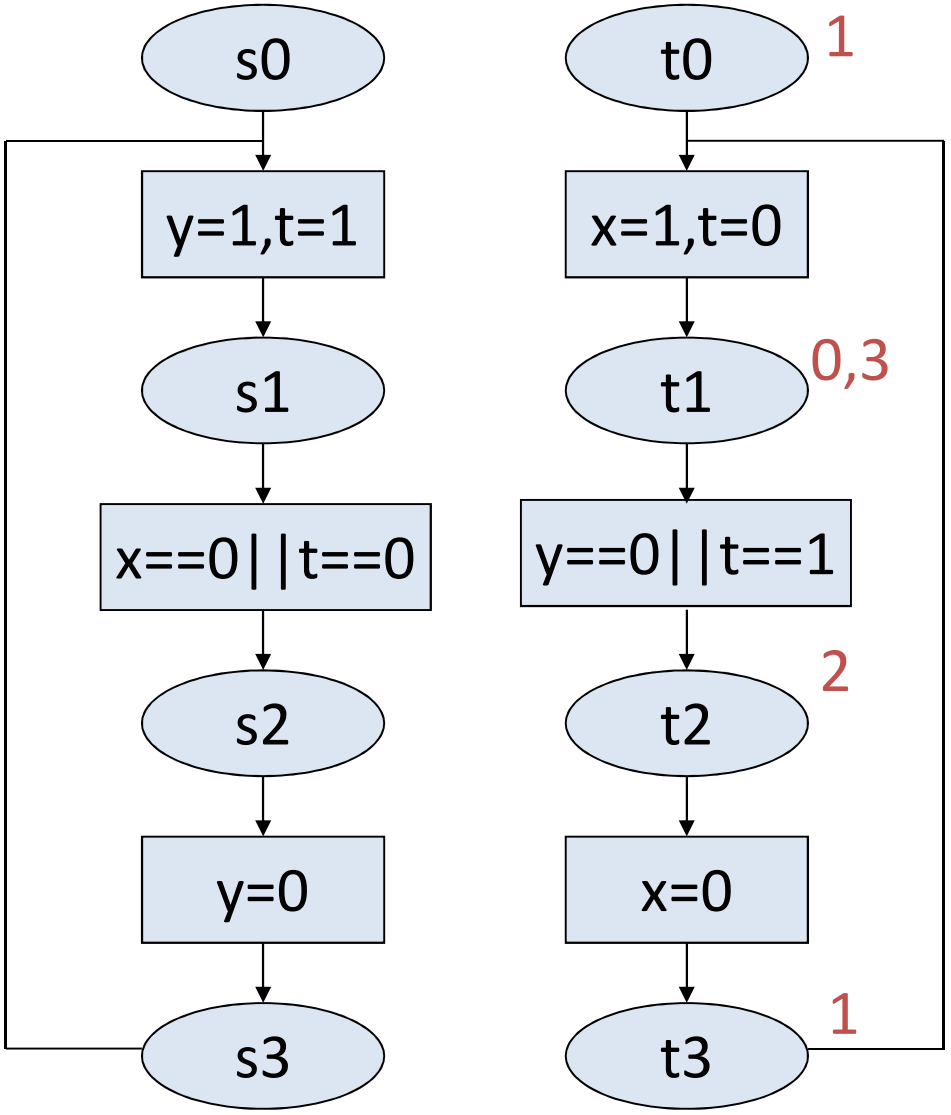
Mutual Exclusion



Initial States

s0
t0
x=0
y=0

Mutual Exclusion



Initial States

s0
t0
x=0
y=0

Attempt 1

t_6: $b = t_1 \wedge (y = 0 \vee t = 1) \longrightarrow (b) := (t_2)$

$$((a = s_1 \wedge f(b, t) = v) \wedge b = t_1 \wedge (y = 0 \vee t = 1))$$
$$\rightarrow (a = s_2 \vee (a = s_1 \wedge f(t_2, t) < v))$$

$$((a = s_1 \wedge f(t_1, t) = v) \wedge b = t_1 \wedge (y = 0 \vee t = 1))$$
$$\rightarrow (a = s_2 \vee (a = s_1 \wedge f(t_2, t) < v))$$

$$((a = s_1) \wedge b = t_1 \wedge (y = 0 \vee t = 1))$$
$$\rightarrow (a = s_2 \vee (a = s_1 \wedge f(t_2, t) < f(t_1, t)))$$

FAIL.

Need to strengthen $\zeta = (a = s_1)$ with $\zeta = (a = s_1 \wedge y = 1)$.
Then it is ok.

Solution

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

Ok.

Need:
$\varphi \Rightarrow (\psi \vee \zeta)$, i.e., $a = s_1 \Rightarrow (a = s_2 \vee (a = s_1 \wedge y = 1))$.
It is ok, since we have the following (can be proved separately).
$(T, \Theta) \models G(a = s_1 \rightarrow y = 1)$.

Integer Square Root (P2)

Given $M = (T, \Theta)$, and the usual interpretation I over natural numbers (!).

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	$(a = s_0)$		

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

Preparation

Proof Rule:

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

Suppose that we have $(T, \Theta) \models_I G(a = s_0 \wedge x > 0 \rightarrow F(a = s_4))$

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

Proof Rule

Proof Rule:

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

We have:

$$\begin{array}{lcl}\varphi & \equiv & (a = s_0 \wedge x > 0) \\ \psi & \equiv & (a = s_4) \\ \zeta & \equiv & ? \\ w & \equiv & ? \\ e & \equiv & ?\end{array}$$

We may assume $(T, \Theta) \models_I G(\psi \vee E(T))$

Solution

Define f such that:

$$I(f(s_0, x, y_3)) = 3x + 1$$
$$I(f(s_i, x, y_3)) = 3(x + 1 - y_3) + 1 - i \quad (i = 1, 2, 3)$$
$$I(f(s_4, x, y_3)) = 0$$

Let

$$\begin{array}{lcllcl} W & = & (NAT, \leq) & \varphi & = & (x > 0 \wedge a = s_0) \\ w & = & true & \psi & = & (a = s_4) \\ e & = & f(a, x, y_3) & \zeta & = & \varphi' \end{array}$$

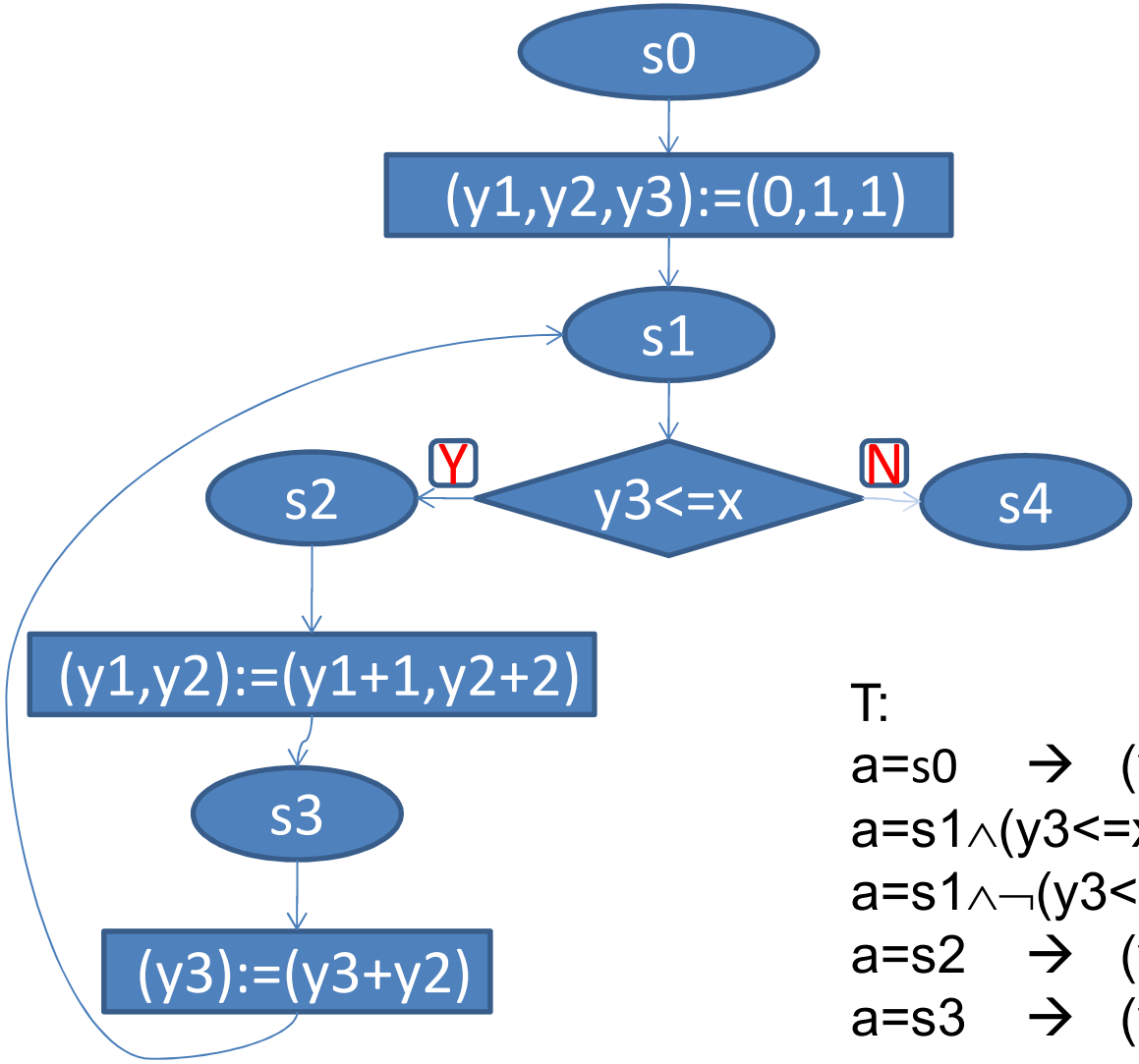
Need

$$\varphi \Rightarrow (\psi \vee \zeta)$$
$$\zeta \Rightarrow w_x^e \wedge (\psi \vee E(T))$$
$$\zeta \wedge e = v \rightarrow [T](\psi \vee (\zeta \wedge e < v))$$

Remain to prove:

$$\zeta \wedge e = v \rightarrow [T](\psi \vee (\zeta \wedge e < v))$$

Integer Square Root



T:

a=s0 → (y1,y2,y3,a):=(0,1,1,s1);

a=s1∧(y3<=x) → (a):=(s2);

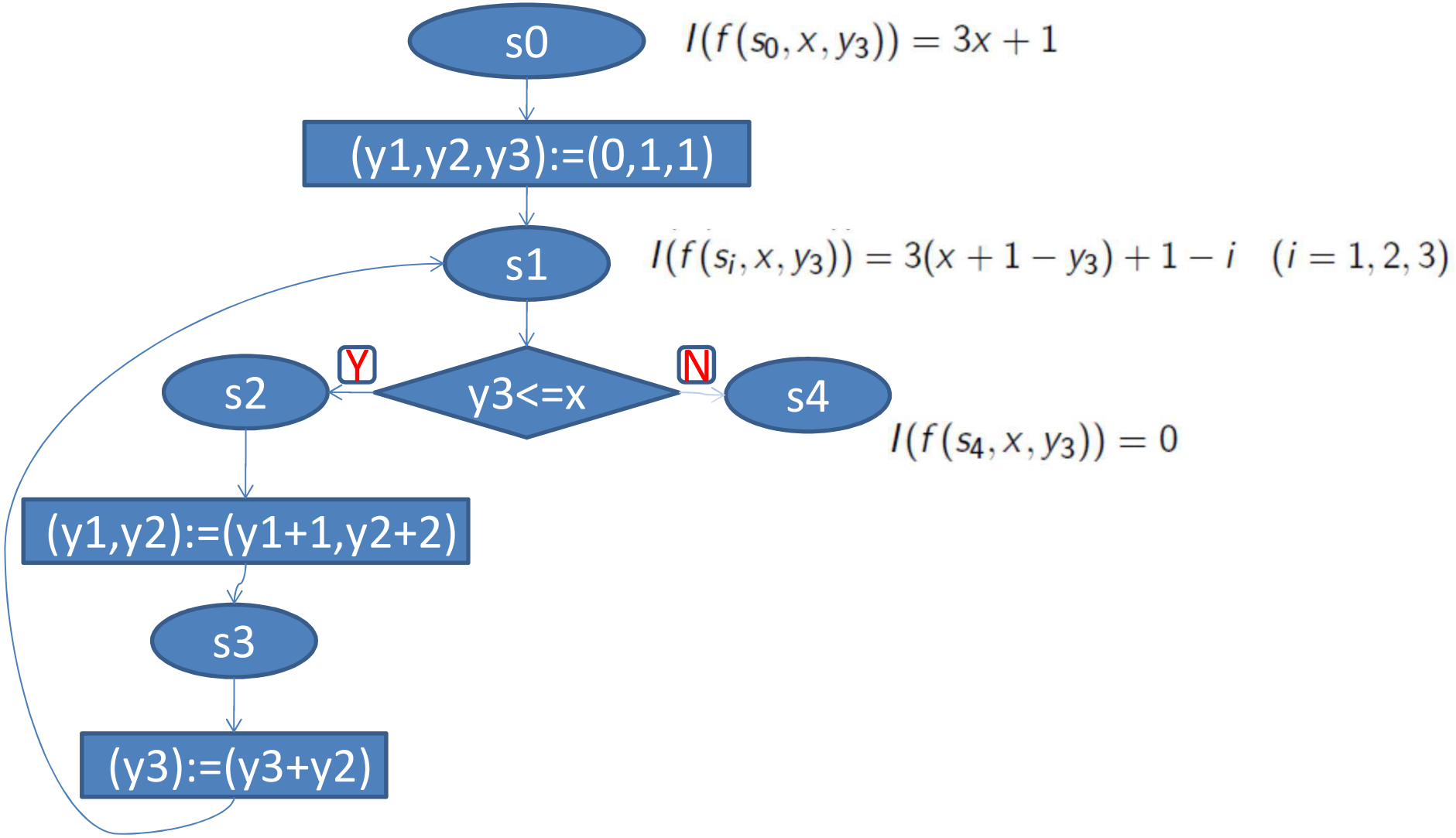
a=s1∧¬(y3<=x) → (a):=(s4);

a=s2 → (y1,y2,a):=(y1+1,y2+2,s3);

a=s3 → (y3,a):=(y3+y2,s1);

Θ: a=s0

Integer Square Root



Solution, Ok with some Modification

$(\zeta \wedge e = v) \equiv (\zeta \wedge f(a, x, y_3) = v)$.
Focus on the part related to the ranking function.

t_1: $a = s_0 \rightarrow f(s_1, x, 1) < v$,
i.e., $a = s_0 \rightarrow 3(x + 1 - 1) < 3x + 1$.

t_2: $a = s_1 \wedge y_3 \leq x \rightarrow f(s_2, x, y_3) < v$,
i.e., $a = s_1 \wedge y_3 \leq x \rightarrow 3(x + 1 - y_3) - 1 < 3(x + 1 - y_3)$. [ok]

t_3: $a = s_1 \wedge \neg(y_3 \leq x) \rightarrow (f(s_4, x, y_3) < v) \vee (s_4 = s_4)$. (ok)

t_4: $a = s_2 \rightarrow f(s_3, x, y_3) < v$,
i.e., $a = s_2 \rightarrow 3(x + 1 - y_3) - 2 < 3(x + 1 - y_3) - 1$.
[need $y_3 \leq x$, also ok, implied by ζ]

t_5: $a = s_3 \rightarrow f(s_1, x, y_3 + y_2) < v$,
i.e., $a = s_3 \rightarrow 3(x + 1 - (y_3 + y_2)) < 3(x + 1 - y_3) - 2$.
(need $y_2 \geq 1$ and $y_3 \leq x$, we need to add $y_2 \geq 1$ to ζ, ok)

Integer Square Root (P2a)

Given $M = (T, \Theta)$, and the usual interpretation I over integers.

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	$(a = s_0)$		

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

Preparation

Proof Rule:

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

Suppose that we have $(T, \Theta) \models_I G(a = s_0 \wedge x > 0 \rightarrow F(a = s_4))$

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

Proof Rule

Proof Rule:

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

We have:

$$\begin{array}{lcl}\varphi & \equiv & (a = s_0 \wedge x > 0) \\ \psi & \equiv & (a = s_4) \\ \zeta & \equiv & ? \\ w & \equiv & ? \\ e & \equiv & ?\end{array}$$

We may assume $(T, \Theta) \models_I G(\psi \vee E(T))$

Attempt 1

Define f such that:

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

Let

$$
\begin{array}{lcllcl}
W & = & (NAT, \leq) & \varphi & = & (x > 0 \wedge a = s_0) \\
w & = & x \geq 0 & \psi & = & (a = s_4) \\
e & = & f(a, x, y_3) & \zeta & = & \varphi'
\end{array}
$$

Need

$$
\begin{aligned}
&\varphi \Rightarrow (\psi \vee \zeta) \\
&\zeta \Rightarrow w_x^e \wedge (\psi \vee E(T)) \qquad ??? \\
&\zeta \wedge e = v \rightarrow [T](\psi \vee (\zeta \wedge e < v))
\end{aligned}
$$

Solution

Define f such that:

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

Let

$$\begin{array}{lllllll} W & = & (NAT,\leq) & \varphi & = & (x>0 \wedge a=s_0) \\ w & = & x \geq 0 & \psi & = & (a=s_4) \\ e & = & f(a,x,y_3) & \zeta & = & \varphi' \end{array}$$

Need

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

Remain to prove:

$$\zeta \wedge e = v \rightarrow [T](\psi \vee (\zeta \wedge e < v))$$

Solution, Ok with some Modification

$(\zeta \wedge e = v) \equiv (\zeta \wedge f(a, x, y_3) = v)$

t_1: $a = s_0 \rightarrow f(s_1, x, 1) < v$,
i.e., $a = s_0 \rightarrow 3(x + 1 - 1) < 3x + 1$, or $a = s_0 \rightarrow 0 < 3x + 1$.

t_2: $a = s_1 \wedge y_3 \leq x \rightarrow f(s_2, x, y_3) < v$,
i.e., $a = s_1 \rightarrow 3(x + 1 - y_3) - 1 < 3(x + 1 - y_3)$.

t_3: $a = s_1 \wedge \neg(y_3 \leq x) \rightarrow (f(s_4, x, y_3) < v) \vee (s_4 = s_4)$. [ok]

t_4: $a = s_2 \rightarrow f(s_3, x, y_3) < v$,
i.e., $a = s_2 \rightarrow 3(x + 1 - y_3) - 2 < 3(x + 1 - y_3) - 1$, or $-2 < -1$.

t_5: $a = s_3 \rightarrow f(s_1, x, y_3 + y_2) < v$,
i.e., $a = s_3 \rightarrow f(s_1, x, y_3 + y_2) < 3(x + 1 - y_3) - 2$. $[y_3 \leq x]$
Either $f(s_1, x, y_3 + y_2) = 0$,
or $f(s_1, x, y_3 + y_2) = 3(x + 1 - (y_3 + y_2))$ and we add $y_2 \geq 1$ to ζ.

(IV) Summary

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

练习1

设 $B = (\{x, y, n, a\}, \{s_0, s_1, s_2, s_3, s_4, 0, 1, 2, 3, +, -, *\}, \{<, =, >\})$
给定迁移系统 (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。

计算最弱宽松前断言wlp(T,a=s4)即[T](a=s4)
并证明 (a=s3)⇒X(a=s4)。

练习2

设 $B = (\{x, y, n, a\}, \{s_0, s_1, s_2, s_3, s_4, 0, 1, 2, 3, +, -, *\}, \{<, =, >\})$
给定迁移系统 (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。

(1) $(T, \Theta) \vdash_I n \geq 0 \rightarrow \mathsf{G}(a = s_4 \rightarrow y = n * n * n - n)$

(2) $(T, \Theta) \vdash_I n \geq 0 \rightarrow \mathsf{F}(a = s_4)$