第 10 周练习：

1．主要是计算最弱宽松前断言和证明前后断言。参考如下。

$[T](a=s4)$
$= (a=s3 \rightarrow s4=s4) \wedge$
$(a=s1\wedge\neg(x<n) \rightarrow s3=s4) \wedge$
$(a=s2 \rightarrow s1=s4) \wedge$
$(a=s1\wedge(x<n) \rightarrow s2=s4) \wedge$
$(a=s0 \rightarrow s0=s4)$
$= \neg(a=s1\wedge\neg(x<n)) \wedge \neg(a=s2) \wedge \neg(a=s1\wedge(x<n)) \wedge \neg(a=s0)$
$= \neg(a=s1) \wedge \neg(a=s2) \wedge \neg(a=s0)$

$(a=s3)\rightarrow X(a=s4)$
IFF $(a=s3)\rightarrow[T+](a=s4)$
IFF $(a=s3)\rightarrow[T](a=s4)$ and $(a=s3)\rightarrow(E(T)\vee a=s4)$
IFF $(a=s3)\rightarrow[T](a=s4)$
IFF $(a=s3)\rightarrow \neg(a=s1) \wedge \neg(a=s2) \wedge \neg(a=s0)$
IFFtrue

2．主要是两种证明方法的应用。参考如下。

2(a)
只需证明：$(a=s0 \wedge n>=0) \Rightarrow G(a=s4 \rightarrow y=n*n*n-n)$

使用推理规则

$$\begin{array}{l} \phi \Rightarrow \varphi' \\ \varphi' \Rightarrow [T]\, \varphi' \\ \varphi' \Rightarrow \varphi \\ \text{------------} \\ \phi \Rightarrow G\varphi \end{array}$$

设
$\phi=$ $(a=s0 \wedge n>=0)$
$\varphi=$ $(a=s4 \rightarrow y=n*n*n-n)$
$\varphi'=$ $(a=s0 \wedge n>=0) \vee (a=s1 \wedge y=(x*x*x-x)/3 \wedge x<=n) \vee$
$(a=s2 \wedge y=(x*x*x-x)/3 \wedge x<n) \vee (a=s3 \wedge 3y=n*n*n-n) \vee (a=s4 \wedge y=n*n*n-n)$

通过计算和推理，我们有

$$\begin{array}{l} \phi \Rightarrow \varphi' \\ \varphi' \Rightarrow [T]\, \varphi' \\ \varphi' \Rightarrow \varphi \end{array}$$

根据推理规则，我们有$(a=s0 \wedge n>=0) \Rightarrow G(a=s4 \rightarrow y=n*n*n-n)$
因而$(T,\Theta) \models_I n>=0 \rightarrow G(a=s4 \rightarrow y=n*n*n-n)$

2(b).

只需证明：$(a=s0 \wedge n>=0) \quad => \quad F(a=s4)$

使用推理规则

$$\begin{array}{l} \phi \Rightarrow (\psi \vee \varphi) \\ \varphi \Rightarrow (w(t/x) \wedge (E(T) \vee \psi) \\ (\varphi \wedge t=v) \Rightarrow [T](\psi \vee (\varphi \wedge t<v)) \\ \text{--------------------} \\ \phi \Rightarrow F\psi \end{array}$$

设 f(a,n,x) 为具有以下性质的函数。

$I(f(s0,n,x))(\sigma) = \quad I(2n+3)(\sigma)$

$I(f(s1,n,x))(\sigma) = \quad I(2(n-x)+2)(\sigma)$

$I(f(s2,n,x))(\sigma) = \quad I(2(n-x)+1)(\sigma)$

$I(f(s3,n,x))(\sigma) = \quad 0$

$I(f(s4,n,x))(\sigma) = \quad 0$

设

w=	(w>=0)
W=	NAT
t=	f(a,n,x)
ϕ=	$(a=s0 \wedge n>=0)$
ψ=	$(a=s4)$
φ=	$(a=s0 \wedge n>=0) \vee (a=s1 \wedge 0<=x<=n) \vee (a=s2 \wedge 0<= x<n) \vee (a=s3 \wedge 0<=x=n)$

假定 $\varphi \Rightarrow ((E(T) \vee \psi)$ 已根据证明安全性质的方法证明。

通过计算和推理，我们有

$$\begin{array}{l} \phi \Rightarrow (\psi \vee \varphi) \\ \varphi \Rightarrow w(t/x) \\ (\varphi \wedge t=v) \Rightarrow [T](\psi \vee (\varphi \wedge t<v)) \end{array}$$

关于第三个条件的验证，我们有：

$(\varphi \wedge t=v)$为$(a=s0 \wedge n>=0) \vee (a=s1 \wedge 0<=x<=n) \vee (a=s2 \wedge 0<= x<n) \vee (a=s3 \wedge 0<=x=n) \wedge f(a,n,x)=v$

五条迁移分别验证如下

$(\varphi \wedge t=v) \rightarrow [t1] (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi) \rightarrow (a=s0 \rightarrow (0<=n) \wedge f(s1,n,0)< f(s0,n,x))$ iff true

$(\varphi \wedge t=v) \rightarrow [t2] (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi) \rightarrow ((a=s1 \wedge x<n) \rightarrow (0<=x<n) \wedge f(s2,n,x)< f(s1,n,x))$ iff true

$(\varphi \wedge t=v) \rightarrow [t3] (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi) \rightarrow ((a=s2) \rightarrow (0<=x<n) \wedge f(s1,n,x+1)< f(s2,n,x))$ iff true

$(\varphi \wedge t=v) \rightarrow [t4] (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi) \rightarrow ((a=s1 \wedge \neg x<n) \rightarrow (0<=x=n) \wedge f(s3,n,x)< f(s1,n,x))$ iff true

$(\varphi \wedge t=v) \rightarrow [t5] (\psi \vee (\varphi \wedge t<v))$ iff $(\varphi \wedge t=v) \rightarrow ((a=s3) \rightarrow (s4=s4 \vee (f(s4,n,x)< f(s3,n,x)))$ iff true

根据推理规则，我们有$(a=s0 \wedge n>=0) \quad => \quad F(a=s4)$

因而$(T,\Theta) \models_I \quad n>=0 \rightarrow F(a=s4)$

第 11 周练习：

1. 同样是计算最弱宽松前断言和证明前后断言。参考如下。

$[l1,l3,end](y=n*n*n-n)$
$=[l1,l3]\ (3y=n*n*n-n)$
$=\neg(x<n)\rightarrow(3y=n*n*n-n)$

$\{x<=n\wedge 3y=x*x*x-x\}(l1,l3,end)\{(y=n*n*n-n)\}$
IFF $(x<=n\wedge 3y=x*x*x-x)\rightarrow [l1,l3]\ (3y=n*n*n-n)$
IFF $(x<=n\wedge 3y=x*x*x-x)\rightarrow(\neg(x<n)\rightarrow(3y=n*n*n-n))$
IFF true

2．主要是两种证明方法的应用。参考如下。

2(a).

选择 C={beg,l1,end}
选择 q_beg = $(n>=0)$
q_l1 = $(0<=x<=n)\wedge(3y=x*x*x-x)$
q_end = $(y=n*n*n-n)$

枚举相关路径如下： (beg,l1), (l1,l2,l1), (l1,l3,end)

证明路径正确性如下：

$\{0<=n\}(beg,l1)\{(0<=x<=n)\wedge(3y=x*x*x-x)\}$
IFF $(0<=n)[beg,l1]((0<=x<=n)\wedge(3y=x*x*x-x))$
IFF $(0<=n\rightarrow 0<=n\wedge 0=0)$
IFF true

$\{0<=x<=n\wedge 3y=x*x*x-x\}(l1,l2,l1)\{0<=x<=n\wedge 3y=x*x*x-x\}$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow[l1,l2,l1)](0<=x<=n\wedge 3y=x*x*x-x)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow [l1,l2]\ (0<=x+1<=n\wedge 3(y+x*(x+1)=(x+1)*(x+1)*(x+1)-x-1)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow (x<y\rightarrow (0<=x+1<=n\wedge 3(y+x*(x+1)=(x+1)*(x+1)*(x+1)-x-1))$
IFF true

$\{0<=x<=n\wedge 3y=x*x*x-x\}(l1,l3,end)\{(y=n*n*n-n)\}$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)[l1,l3,end](y=n*n*n-n)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow [l1,l3]\ (3y=n*n*n-n)$
IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow(\neg(x<n)\rightarrow(3y=n*n*n-n))$
IFF true

2(b)

选择 C={beg,l1}

选择 q_beg = (n>=0)

q_l1 = $(0<=x<=n)\wedge(3y=x*x*x-x)$

枚举相关路径如下：

(beg,l1),

(l1,l2,l1)

证明路径正确性如下：

$\{0 <=n \}(beg,l1)\{(0<=x<=n)\wedge(3y=x*x*x-x)\}$

IFF $(0 <=n)[beg,l1]((0<=x<=n)\wedge(3y=x*x*x-x))$

IFF $(0<=n\rightarrow 0<=n\wedge 0=0)$

IFF true

$\{0<=x<=n \wedge 3y=x*x*x-x \}(l1,l2,l1) \{0<=x<=n \wedge 3y=x*x*x-x \}$

IFF $(0<=x<=n \wedge 3y=x*x*x-x)\rightarrow[l1,l2,l1)](0<=x<=n \wedge 3y=x*x*x-x)$

IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow [l1,l2] (0<=x+1<=n \wedge 3(y+x*(x+1)=(x+1)*(x+1)*(x+1)-x-1)$

IFF $(0<=x<=n\wedge 3y=x*x*x-x)\rightarrow (x<n\rightarrow (0<=x+1<=n \wedge 3(y+x*(x+1)=(x+1)*(x+1)*(x+1)-x-1))$

IFF true

选择 C’={l1}

选择 W=NAT, w=(x>=0).

我们有 W={σ(x) | I(w)(σ)=true }

选择 t_l1 = (n-x)

我们有 q_l1 $\rightarrow$ (n-x)>=0.

枚举相关路径如下：(l1,l2,l1)

证明路径正确性如下：

$vc(0<=x<=n\wedge(n-x=v), (l1,l2,l1),(n-x<v))$

IFF $(0<=x<=n\wedge(n-x=v))\rightarrow (x<n\rightarrow (n-x-1<v)$

IFF true.

第 12 周练习：

1. 同样是计算最弱宽松前断言和证明前后断言。参考如下。

a.

我们有

$[T]\ (x=i*a+j*b)=$

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

b.

我们有

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

因而$\{ y=k*a+l*b \wedge (x=i*a+j*b) \}\ T\ \{ x=i*a+j*b\}$。

2．主要是两种证明方法的应用。参考如下。

2(a)

设φ为 $gcd(x,y)=gcd(a,b) \wedge (y=k*a+l*b) \wedge (x=i*a+j*b)$

我们有

$\{\varphi\wedge \neg(x=y)\}$ if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j $\{ \varphi \}$

且

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

根据推理规则，我们有

$\{\varphi\}$

while (¬(x=y)) do if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j od

$\{ x=gcd(a,b) \wedge (x=i*a+j*b) \}$

我们有

$\{x=a\wedge y=b\wedge a>=0\wedge b>=0\}$ i:=1; j:=0; k:=0; l:=1 $\{\varphi\}$

根据推理规则，我们有

$\{x=a\wedge y=b\wedge a>=0\wedge b>=0\}$

i:=1; j:=0; k:=0; l:=1;

while (¬(x=y)) do if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j od

$\{ x=gcd(a,b) \wedge (x=i*a+j*b) \}$

因此我们有 $\{x=a\wedge y=b\wedge a>=0\wedge b>=0\}T\{ x=gcd(a,b) \wedge (x=i*a+j*b) \}$

2(b)

设 W=NAT, w=(x>=0). 我们有 W={σ(x) | I(w)(σ)=true}

设 t= (x+y)

设φ为 gcd(x,y)=gcd(a,b) ∧(y=k*a+l*b) ∧(x=i*a+j*b) ∧x>0∧y>0

我们有
φ∧ ¬(x=y) → t>=0
且
[φ∧ ¬(x=y)∧t=v] if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j [φ∧t<v]
且
φ∧ (x=y)→ x=gcd(a,b) ∧ (x=i*a+j*b)

根据推理规则，我们有
[φ]
while (¬(x=y)) do if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j od
[x=gcd(a,b) ∧ (x=i*a+j*b)]

我们有
[x=a∧y=b∧a>0∧b>0] i:=1; j:=0; k:=0; l:=1 [φ]

根据推理规则，我们有
[x=a∧y=b∧a>0∧b>0]
i:=1; j:=0; k:=0; l:=1;
while (¬(x=y)) do if (x>y) then x:=x-y; i:=i-k; j:=j-l; else y:=y-x; k:=k-i; l:=l-j od
[x=gcd(a,b) ∧ (x=i*a+j*b)]

因此我们有 [x=a∧y=b∧a>0∧b>0]T[x=gcd(a,b) ∧ (x=i*a+j*b)]