3.3.9.21) Consider the code segment that adds the elements in a(1 : n) to b(1 : n) storing the result in c(1 : n):

{0≤n}

i:=1

{ Pinv :1≤i≤n+1∧(∀j|1≤ j<i:c(j)=a(j)+b(j)) }

{t : n − i}

while i ≤ n

c(i) := a(i) + b(i)

i:=i+1

endwhile

(∀j|1 ≤ j ≤ n : c(j) = a(j)+b(j))

{Q}SI{Pinv}:

{ (0≤n) } “i:=1” {1 ≤ i ≤ n+1 ∧ ( ∀j | 1≤ j<i : c(j) = a(j)+b(j) )) }

<definition of Hoare Triple>

(0≤n) => wp( “i:=1” , 1 ≤ i ≤ n+1 ∧ ( ∀j | 1≤ j<i : c(j) = a(j)+b(j) ))

<definition of := >

(0≤n) => ( 1 ≤ 1 ≤ n+1 ∧ ( ∀j | 1≤ j<1 : c(j) = a(j)+b(j) ))

< algebra; ∀ over empty range >

(0≤n) => ( 1 ≤ 1 ≤ n+1 ∧ T)

< ∧*-simplification ; p* => *p ; algebra*>

T

{Pinv ∧ G}S{Pinv}:

<Definition of Hoare Triple>

( 1 ≤ i ≤ n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n ) =>

wp(“c(i) := a(i) + b(i) , i:=i+1 “ , 1 ≤ i ≤ n+1 ∧ ( ∀j | 1≤ j<i : c(j) = a(j)+b(j) )))

<Definition of wp>

( 1 ≤ i ≤ n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n ) =>

wp(“c(i) := a(i) + b(i) “ , wp( “i:=i+1 “ , 1 ≤ i ≤ n+1 ∧ ( ∀j | 1≤ j<i : c(j)=a(j)+b(j) )))

<Definition of := >

( 1 ≤ i ≤ n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n ) =>

wp(“c(i) := a(i) + b(i) “ , 1 ≤ i+1 ≤ n+1 ∧ ( ∀j | 1≤ j<i+1 : c(j)= a(j)+b(j) ))

<split range >

( 1 ≤ i ≤ n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n ) =>

wp(“c(i) := a(i) + b(i) “ , 1 ≤ i+1 ≤ n+1 ∧ ( ∀j | 1≤ j<i+1 : c(j)= a(j)+b(j) ) ∧ c(i) := a(i) + b(i) ))

<definition of :=>

( 1 ≤ i ≤ n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n ) =>

( 1 ≤ i+1 ≤ n+1 ∧ ( ∀j | 1≤ j<i : c(j)= a(j)+b(j) ) ∧ a(i) + b(i) := a(i) + b(i) )

<definition of := / p => p>

( 1 ≤ i ≤ n+1 ∧ i ≤ n ) => ( 1 ≤ i+1 ≤ n+1 )

< ∧-simplification / algebra>

T

Pinv ∧ ¬G => R:

( 1≤i≤n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ ¬(i ≤ n)) ) => (∀j|1 ≤ j ≤ n : c(j) = a(j)+b(j))

< ^*-simplification; algebra; commutativity; associativity* >

( 1≤i≤n+1 ∧ (i≤n+1 ∧ i≥n+1) ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ ¬(i ≤ n)) ) => (∀j|1 ≤ j ≤ n : c(j) = a(j)+b(j))

< definition of =>

( 1≤i≤n+1 ∧ (i=n+1) ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ ¬(i ≤ n)) ) => (∀j|1 ≤ j ≤ n : c(j) = a(j)+b(j))

<algebra>

( 1≤i≤n+1 ∧ (∀j|1≤ j≤ n:c(j)=a(j)+b(j)) ∧ ¬(i ≤ n)) ) => (∀j|1 ≤ j ≤ n : c(j) = a(j)+b(j)) <weakening-strengthening>

T

3.3.9.22) Consider the following program that computes the quotient *q* and remainder *r* of the integer division of *x* by *y*:

{0≤*x*∧0<*y*}

*q* := 0; *r* := *x*

{*Pinv* :0<*y*∧0≤*r*∧*q*∗*y*+*r*=*x*}

{*t* : *r*}

while *r* ≥ *y*

*r* := *r* − *y*

*q*:=*q*+1

Endwhile

(qy+r=x)∧(r<y)

Give all *fully instantiated* conditions that must be proved *true* to establish partial correctness, but do not prove them.

{Q}SI{Pinv}:

(0≤x ∧ 0<y) => wp( “q := 0; r := x” , 0<y ∧ 0≤r ∧ q∗y + r = x)

{Pinv ∧ G}S{Pinv}:

( 0<y ∧ 0≤r ∧ q∗y + r = x ∧ r ≥ y) =>

wp( “r := r − y ; q := q+1“ , 0<y ∧ 0≤r ∧ q∗y + r = x )

Pinv ∧ ¬G => R:

( (0<y ∧ 0≤r ∧ q∗y + r = x) ∧ ¬( *r* ≥ *y*) ) => ((qy+r=x)∧(r<y))

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3.3.9.23) Prove the partial correctness of the problem in the last homework.

{Q}SI{Pinv}:

(0≤x ∧ 0<y) => wp( “q := 0; r := x” , 0<y ∧ 0≤r ∧ q∗y + r = x)

<definition of wp >

(0≤x ∧ 0<y) => wp( “q := 0”, wp(“ r := x” , 0<y ∧ 0≤r ∧ q∗y + r = x))

<definition of :=>

(0≤x ∧ 0<y) => wp( “q := 0”, 0<y ∧ 0≤x ∧ q∗y + x = x)

<definition of :=>

(0≤x ∧ 0<y) => ( 0<y ∧ 0≤x ∧ 0 + x = x)

<Identity Law and p => p>

T

{Pinv ∧ G}S{Pinv}:

( 0<y ∧ 0≤r ∧ q∗y + r = x ∧ r ≥ y) =>

wp( “r := r − y ; q := q+1“ , 0<y ∧ 0≤r ∧ q∗y + r = x )

<definition of wp>

( 0<y ∧ 0≤r ∧ q∗y + r = x ∧ r ≥ y) =>

wp( “r := r − y” , wp(q := q+1 , 0<y ∧ 0≤r ∧ (q)∗y + r = x ))

<definition of :=>

( 0<y ∧ 0≤r ∧ q∗y + r = x ∧ r ≥ y) => wp( “r := r − y” , 0<y ∧ 0≤r ∧ (q+1)∗y + r = x )

<definition of :=>

( 0<y ∧ 0≤r ∧ q∗y + r = x ∧ r ≥ y) => ( 0<y ∧ 0≤(r - y) ∧ (q+1)∗y + (r - y) = x )

<algebra>

( 0<y ∧ 0≤r ∧ q∗y + r = x ∧ r ≥ y) => ( 0<y ∧ y≤r ∧ q∗y + r = x )

<weakening-strengthening>

T

Pinv ∧ ¬G => R:

( (0<y ∧ 0≤r ∧ q∗y + r = x) ∧ ¬( *r* ≥ *y*) ) => ((q\*y+r=x) ∧ (r<y))

<Negation Law>

( 0<y ∧ 0≤r ∧ q∗y + r = x ∧ r<y ) => ((q\*y+r=x) ∧ (r<y))

<weakening-strengthening>

T

3.3.9.24) Prove that the loop in the last two homeworks terminates.

*Pinv* ∧ *G* => (*t* ≥ 0):

<Instantiation>

(1≤i≤n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n) => (n − i ≥ 0)

<algebra>

(1≤i≤n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n) => (n ≥ i)

<weakening-strengthening>

T

{*Pinv* ∧ *G*} *t*0:=*t*; *S*{*t* < *t*0}:

<instantiation - Hoare Triple Definition>

(1≤i≤n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n) => wp(“*t*0:=n − i *,* c(i) := a(i) + b(i) , i:=i+1” , n − i< *t*0)

<definition of wp>

(1≤i≤n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n) => wp(“*t*0:=n − i *,* c(i) := a(i) + b(i)” ,

wp( i:=i+1 , n − i< *t*0)

<definition of := / definition of wp>

(1≤i≤n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n) => wp(“t0:=n − i” , wp( c(i) := a(i) + b(i) , n − i +1 < t0)

<definition of :=>

(1≤i≤n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n) => (n − i +1 < n - i)

<algebra>

(1≤i≤n+1 ∧ (∀j|1≤ j<i:c(j)=a(j)+b(j)) ∧ i ≤ n) => T

<implication Law>

T

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

{0≤*x*∧0<*y*}

*q* := 0; *r* := *x*

{*Pinv* :0<*y*∧0≤*r*∧*q*∗*y*+*r*=*x*}

{*t* : *r*}

while *r* ≥ *y*

*r* := *r* − *y*

*q*:=*q*+1

Endwhile

(qy+r=x)∧(r<y)

*Pinv* ∧ *G* => (*t* ≥ 0):

(0<y∧ 0≤r ∧ q∗y+r=x ∧ *r* ≥ *y*) => (*r* ≥ 0)

<weakening-strengthening>

T

{*Pinv* ∧ *G*} *t*0:=*t*; *S*{*t* < *t*0}:

<instantiation>

(0<y∧ 0≤r ∧ q∗y+r=x ∧ r ≥ y) => wp (“t0:=r , r := r − y, q:=q+1 ” , r < t0)

< definition of wp>

(0<y∧ 0≤r ∧ q∗y+r=x ∧ r ≥ y) => wp (“t0:=r , r := r − y” , wp(q:=q+1 , r < t0))

<definition of wp>

(0<y∧ 0≤r ∧ q∗y+r=x ∧ r ≥ y) => wp (“t0:=r” , wp( r := r − y , r < t0))

<definition of wp / definition of :=>

(0<y∧ 0≤r ∧ q∗y+r=x ∧ r ≥ y) => wp (“t0:=r”, r - y < t0)

<definition of := , algebra>

(0<y∧ 0≤r ∧ q∗y+r=x ∧ r ≥ y) => T

<Implementation Law>

T