Kyle Spence

Mult

```
{y >= 0}
i := y;
ans := 0;
WHILE i != 0 DO
   ans := ans + x;
     i := i-1
LOOP
{ans = x * y}
```

{Sequencing rule
We must now prove the following
('I' represents loop invariant):
1) {I} WHILE i != 0 DO ans := ans + x; i := i-1
   LOOP {ans = x * y}
2) {Q} ans := 0 {I}
3) {y >= 0} i := y {Q} }

1)

```
{I}
WHILE i != 0 DO
   ans := ans + x;
   i := i-1
LOOP
{ans = x * y}
```

{While rule/Postcondition weakening
We must now prove the following:
1.1) {I ∧ i != 0} ans := ans + x;
   i := i-1 {I}
1.2) [I ∧ ¬(i != 0)] ⇒ [ans = x * y] }

1.1)

$\{I \wedge i \mathrel{!}= 0\}$
ans := ans + x;
i := i - 1;
$\{I\}$

{Select loop invariant I:
$I = [(i * x) + ans = x * y]$}

$\{(i * x) + ans = x * y \wedge i \mathrel{!}= 0\}$
ans := ans + x;
i := i - 1
$\{(i * x) + ans = x * y\}$

{Sequencing rule
We must now prove the following:
1.1.1) $\{R\}$ i := i - 1 $\{(i * x) + ans = x * y\}$
1.1.2) $\{(i * x) + ans = x * y \wedge i \mathrel{!}= 0\}$ ans := ans + x $\{R\}$}

1.1.1)

$\{R\}$
i := i - 1
$\{(i * x) + ans = x * y\}$

{Assignment axiom}

$R = ((i * x) + ans = x * y)[i-1/i] = [((i-1) * x) + ans = x * y]$

{We have obtained R}

1.1.2)

$\{(i * x) + ans = x * y \wedge i \mathrel{!}= 0\}$
$ans := ans + x$
$\{((i-1) * x) + ans = x * y\}$

{Assignment axiom}

$(((i-1) * x) + ans = x * y)[ans + x / ans]$

{Expand substitution}

$[((i-1) * x) + ans + x = x * y]$

{Arithmetic}

$[(i * x) + ans = x * y]$

{Precondition strengthening
We must now prove the following:
1.1.2.1) $P = [(i * x) + ans = x * y \wedge i \mathrel{!}= 0]$
$P' = [(i * x) + ans = x * y]$
$P \Rightarrow P'$ }

1.1.2.1)

$[(i * x) + ans = x * y \wedge i \mathrel{!}= 0] \Rightarrow [(i * x) + ans = x * y]$

{Pure logic}

True

1.2)

$[(i * x) + ans = x * y \land \neg(i \; != 0)] \Rightarrow [ans = x * y]$

{Pure logic}

$[ans = x * y] \Rightarrow [ans = x * y]$

{Reflexivity of implication}

True

2)

{Q}
ans := 0
$\{(i * x) + ans = x * y\}$

{Assignment axiom}

$Q = ((i * x) + ans = x * y)\,[0/ans] = [i * x = x * y]$

{We have obtained Q}

3)

$\{y >= 0\}$
$i := y$
$\{i * x = x * y\}$

{Assignment axiom}

$(i * x = x * y)[y/i]$

{Expand substitution}

$y * x = x * y$

{simplify}

True

{Precondition strengthening
We must now prove the following:
3.1) $P = y >= 0$
$P' = \text{True}$
$P \Rightarrow P'$ }

3.1)

$[y >= 0] \Rightarrow [\text{True}]$

{Pure logic}

True

{Q.E.D}

Quot

$\{x >= 0 \wedge y > 0\}$
$r := x;$
$q := 0;$
WHILE $r >= y$ DO
    $q := q + 1;$
    $r := r - y$
LOOP
$\{x = (q * y) + (x \% y)\}$

{Sequencing rule
We must now prove the following
('I' represents loop invariant):
1) $\{I\}$ WHILE $r >= y$ DO $q := q+1;\ r := r-y$
LOOP $\{x = (q*y) + (x\%y)\}$
2) $\{Q\}\ q := 0\ \{I\}$
3) $\{x >= 0 \wedge y > 0\}\ r := x\ \{Q\}$ }

1)

$\{I\}$
WHILE $r >= y$ DO
    $q := q+1;$
    $r := r-y$
LOOP
$\{x = (q*y) + (x\%y)\}$

{While rule/Postcondition Weakening
We must now prove the following:
1.1) $\{I \wedge r >= y\}\ q := q+1;\ r := r-y\ \{I\}$
1.2) $[I \wedge \neg(r >= y)] \Rightarrow [x = (q*y) + (x\%y)]$ }

1.1)

$\{I \wedge r >= y\}$
$q := q+1;$
$r := r-y$
$\{I\}$

{Select loop invariant I:
$I = [x = (q*y) + r]$ }

$\{x = (q*y) + r \wedge r >= y\}$
$q := q+1;$
$r := r-y$
$\{x = (q*y) + r\}$

{Sequencing rule
We must now prove the following:
1.1.1) $\{R\}\ r := r-y\ \{x = (q*y) + r\}$
1.1.2) $\{x = (q*y) + r \wedge r >= y\}\ q := q+1\ \{R\}$ }

1.1.1)

$\{R\}$
$r := r-y$
$\{x = (q*y) + r\}$

{Assignment axiom}

$R = (x = (q*y) + r)[r-y/r] = [x = (q*y) + r - y]$

{We have obtained R}

1.1.2)

$\{x = (q*y) + r \wedge r >= y\}$
$q := q+1$
$\{x = (q*y) + r - y\}$

{Assignment axiom}

$(x = (q*y) + r - y)[q+1/q]$

{Expand substitution}

$[x = ((q+1)*y) + r - y]$

{Arithmetic}

$[x = (q*y) + r]$

{Precondition strengthening
We must now prove the following:
1.1.2.1) $P = [x = (q*y) + r \wedge r >= y]$
$P' = [x = (q*y) + r]$
$P \Rightarrow P'$}

1.1.2.1)

$[x = (q*y) + r \wedge r >= y] \Rightarrow [x = (q*y) + r]$

{Pure logic}

True

1.2)

$[x = (q * y) + r \land \neg(r >= y)] \Rightarrow [x = (q * y)]$

{Pure logic}

$[x = (q * y)] \Rightarrow [x = (q * y)]$

{Reflexivity of implication}

True

2)

$\{Q\}$
$q := 0$
$\{x = (q * y) + r\}$

{Assignment axiom}

$Q = (x = (q * y) + r)[0/q] = [x = r]$

{We have obtained Q}

3)

$\{x >= 0 \land y > 0\}$
$r := x$
$\{x = r\}$

{Assignment axiom}

$(x = r)[x/r]$

{Expand substitution}

$r = r$

{Simplify}

True

{Precondition strengthening
We must now prove the following:
3.1) $P = x >= 0 \land y > 0$
$P' = True$
$P \Rightarrow P'$}

3.1)

$[x >= 0 \land y > 0] \Rightarrow [True]$

{Pure logic}

True

{Q.E.D}

Tri

$\{n >= 0\}$
i := n;
ans := 0;
WHILE i != 0
    ans := ans + i;
    i := i - 1
LOOP
$\{ans = (n * (n+1)) / 2\}$

{Sequencing rule
We must now prove the following
('I' represents loop invariant):
1) {I} WHILE i != 0 DO ans := ans + i; i := i - 1
LOOP {ans = (n * (n+1)) / 2}
2) {Q} ans := 0 {I}
3) {n >= 0} i := n {Q}}

1)

{I}
WHILE i != 0 DO
    ans := ans + i;
    i := i - 1
LOOP
{ans = (n * (n+1)) / 2}

{While rule/Postcondition weakening
We must now prove the following:
1.1) {I ∧ i != 0} ans := ans + i; i := i - 1 {I}
1.2) [I ∧ ¬(i != 0)] ⇒ [ans = (n * (n+1)) / 2] }

1.1)

$\{I \wedge i \mathrel{!}= 0\}$
ans := ans + i;
i := i - 1
$\{I\}$

{Select loop invariant I:
$I = [((i*(i+1))/2) + ans = (n*(n+1))/2]$}

$\{((i*(i+1))/2) + ans = (n*(n+1))/2 \wedge i \mathrel{!}= 0\}$
ans := ans+i;
i := i-1
$\{((i*(i+1))/2) + ans = (n*(n+1))/2\}$

{Sequencing rule
We must now prove the following:
1.1.1) $\{R\}$ i := i-1 $\{((i*(i+1))/2) + ans = (n*(n+1))/2\}$
1.1.2) $\{((i*(i+1))/2) + ans = (n*(n+1))/2 \wedge i \mathrel{!}= 0\}$ ans := ans+i $\{R\}$}

1.1.1)

$\{R\}$
r := r - y
$\{((i*(i+1))/2) + ans = (n*(n+1))/2\}$

{Assignment axiom}

$R = (((i*(i+1))/2) + ans = (n*(n+1))/2)[i-1/i] = [(((i-1)*((i-1)+1))/2) + ans = (n*(n+1))/2]$

{We have obtained R}

1.1.2)

$\{((i*(i+1))/2) + ans = (n*(n+1))/2 \wedge i != 0\}$
$ans := ans + i$
$\{(((i-1)*((i-1)+1))/2) + ans = (n*(n+1))/2\}$

{Assignment axiom}

$((((i-1)*((i-1)+1))/2) + ans = (n*(n+1))/2\ [ans + i/ans]$

{Expand substitution}

$[(((i-1)*((i-1)+1))/2) + (ans+i) = (n*(n+1))/2]$

{Arithmetic}

$[((i*(i+1))/2) + ans = (n*(n+1))/2]$

{Precondition strengthening
We must now prove the following:
1.1.2.1) $P = [((i*(i+1))/2) + ans = (n*(n+1))/2 \wedge i != 0]$
$P' = [((i*(i+1))/2) + ans = (n*(n+1))/2]$
$P \Rightarrow P'$}

1.1.2.1)

$[((i*(i+1))/2) + ans = (n*(n+1))/2 \wedge i != 0] \Rightarrow [((i*(i+1))/2) + ans = (n*(n+1))/2]$

{Pure logic}

True

1.2)

$[((i*(i+1))/2) + ans = (n*(n+1))/2 \land \neg(i != 0)] \Rightarrow (ans = (n*(n+1))/2]$

{Pure logic}

$[ans = (n*(n+1))/2] \Rightarrow [ans = (n*(n+1))/2]$

{Reflexivity of implication}

True

2)

{Q}
ans := 0
$\{((i*(i+1))/2) + ans = (n*(n+1))/2\}$

{Assignment axiom}

$Q = (((i*(i+1))/2) + ans = (n*(n+1))/2\,[0/ans] = [((i*(i+1))/2) = (n*(n+1))/2]$

{We have obtained Q}

3)

$\{n >= 0\}$
$i := n$
$\{((i * (i+1))/2) = (n * (n+1))/2\}$

{Assignment axiom}

$\{((i * (i+1))/2) = (n * (n+1))/2)[n/i]$

{Expand substitution}

$\{((n * (n+1))/2) = (n * (n+1))/2)$

{Simplify}

True

{Precondition strengthening
We must now prove the following:
3.1) $P = n >= 0$
$P' = True$
$P \Rightarrow P'$ }

3.1)

$[n >= 0] \Rightarrow [True]$

{Pure logic}

True

{Q.E.D}