Homework 6

CIS-623 STRUCTURED PROGRAMMING & FORMAL METHODS

PROF. MEHMET KAYA

2/24/2022

Anthony Redamonti
SYRACUSE UNIVERSITY

Assignment 6

Give total correctness proofs of the following programs.

<u>Question 1:</u>

```
[ T ]
x = 5;
while (x > 0) {
      x = x - 1;
}
[ x = 0 ]
```

$[T]$ precondition

$[(0 \le 5 \le 5) \& (0 \le 5)]$

$x = 5;$

$[(0 \le x \le 5) \& (0 \le x)]$ Inv. & $0 \le$ Variant

while $(x > 0)$ {

$[(0 \le x \le 5) \& (x > 0) \& (0 \le x = E_0)]$ Inv. & guard & $0 \le Var = E_0$

$[(0 \le x-1 \le 5) \& (0 \le x-1 < E_0)]$

$x = x - 1;$

$[(0 \le x \le 5) \& (0 \le x < E_0)]$ Inv. & $0 \le$ Variant $< E_0$

}

$[(0 \le x \le 5) \& \neg(x > 0)]$ Inv. & $\neg$ gaurd

$[x = 0]$ postcondition

- - - - - - - - - - - - - - - - - - - -

$\begin{bmatrix} \text{Variant} = x \\ \text{Invariant} = (0 \le x \le 5) \end{bmatrix}$

$[T] \rightarrow [(0 \le 5 \le 5) \& (0 \le 5)]$ True (Yes)

$[(0 \le x \le 5) \& (x > 0) \& (0 \le x = E_0)] \rightarrow [\underbrace{(0 \le x-1 \le 5)}_{\text{True, } x \le 5 \,\&\, x > 0} \& \underbrace{(0 \le x-1 < E_0)}_{\text{True, } x = E_0 \,\&\, x > 0}]$

True (Yes)

$[(0 \le x \le 5) \& \neg(x > 0)] \rightarrow \underbrace{[x = 0]}_{\text{True } \neg(x>0) \,\&\, x \ge 0}$

True (Yes)

Question 2:

```
[ n > 0 ]
while (n > 0) {
      n = n - 2;
}
n = n + 4;
[ n > 1 ]
```

Variant = $n+1 = E_0$

Invariant = $n > -2$

$[n>0]$ precondition

$[(n>-2) \wedge (0 \le n+1)]$ Invariant $\wedge$ (Variant ≥ 0)

while $(n>0)$ {

$[(n>-2) \wedge (n>0) \wedge (0 \le n+1 = E_0)]$ Invariant $\wedge$ guard $\wedge$ $0 \le$ Variant $= E_0$

$[(n-2>-2) \wedge (0 \le n-2+1 < E_0)]$

$n = n-2;$

$[(n>-2) \wedge (0 \le n+1 < E_0)]$ Invariant $\wedge$ $0 \le n+1 < E_0$

}

$[(n>-2) \wedge (\neg(n>0))]$ Invariant $\wedge$ $\neg$ guard

$[n>-3]$

$n = n+4;$

$[n>1]$ postcondition

$[n>0] \rightarrow [(n>-2) \wedge (0 \le n+1)]$ ~~Invariant~~

Valid

$[(n>-2) \wedge (n>0) \wedge (0 \le n+1 = E_0)] \rightarrow [\underbrace{(n-2>-2)}_{\text{True } (n>0)} \wedge (\underbrace{0 \le n-2+1 < E_0}_{0 \le n-1 < E_0})]$

Valid

$[(n>-2) \wedge \neg(n>0)] \rightarrow \underbrace{[n>-3]}_{\text{True } (n>-2)}$

Valid

Question 3:

```
[ x > y ]
while (x > y) {
        x = x - 1;
        y = y + 1;
}
if (x < y)
        x = x + 1;
[ x = y ]
```

x	y
10	5
9	6
8	7
7	8

Variant: $x - y + 1$

Invariant:

```
[x > y]                  precondition
[0 ≤ (x - y + 1)]        0 ≤ Variant
while (x > y) {                              Variant = E₀ ∧ guard
    [(x > y) ∧ (0 ≤ (x - y + 1) = E₀)]
    [0 ≤ (x - 1 - y) < E₀]
    x = x - 1;
    [0 ≤ (x - y) < E₀]
    y = y + 1;
    [0 ≤ (x - y + 1) < E₀]
}
(¬(x > y))
(x < y) → (x + 1 = y) ∧ ¬(x < y) → (x = y)
if (x < y) {
    [x + 1 = y]
    x = x + 1;
    [x = y]
else { }

[x = y]                  postcondition
```

$[x > y] \rightarrow 0 \leq (x - y + 1)$ Valid

$[(x > y) \wedge (0 \leq (x - y + 1) = E_0)] \rightarrow [0 \leq (x - 1 - y) < E_0]$ Valid

$[\neg (x > y)] \rightarrow [(x < y \rightarrow (x+1 = y)) \wedge (\neg (x < y) \rightarrow (x = y))]$ Valid

Question 4:

$[\ k \geq 0]$

```
n = 0;
x = 1;
while (n != k) {
        x = x + x;
        n = n + 1;
}
```

$[\ x = 2^k]$

Variant: $K - n$

Invariant: $X = 2^n$

n	X	K
0	1	3
1	2	3
2	4	3
3	8	3

$X = 2^n$

$[K \geq 0]$ precondition

$[(1 = 2^0) \wedge (K - 0 \geq 0)]$

$n = 0;$

$[(1 = 2^n) \wedge (K - n \geq 0)]$

$X = 1;$

$[(X = 2^n) \wedge (K - n \geq 0)$

while $(n != K)$ {

$[(X = 2^n) \wedge (n != K) \wedge (0 \leq K - n = E_0)]$

$[(X + X = 2^{n+1}) \wedge (0 \leq K - (n+1) < E_0)]$

$X = X + X;$

$[(X = 2^{n+1}) \wedge (0 \leq K - (n+1) < E_0)]$

$n = n + 1;$

$[(X = 2^n) \wedge (0 \leq K - n < E_0)]$

}

$[(X = 2^n) \wedge (\neg(n != K))]$ invariant $\wedge$ $\neg$ guard

$[X = 2^K]$ post condition

$[K \geq 0] \rightarrow [(1 = 2^0) \wedge (K - 0) \geq 0)]$ Valid

~~$[(X + X = 2^{n+1}$~~

$[(X = 2^n) \wedge (n != K) \wedge (0 \leq K - n = E_0)] \rightarrow [\underbrace{(X + X = 2^{n+1})}_{2X = 2^{n+1} \text{ True}} \wedge \underbrace{(0 \leq K - (n+1) < E_0)}_{\text{True } (n != K)}]$

Valid

$[(X = 2^n) \wedge \neg(n != K)] \rightarrow [X = 2^K]$

Valid