Q1 and Q2

Group 4

Kevin Pettersson - Alice Moss

1 Question 1

1.1 Program statement

$S:\quad \text{if } (x > y) \text{ then } \{a := x, b := y\} \text{ else } \{a := y, b := x\}$

1.2 Post-condition

$R:\quad a > b$

1.3 Weakest pre-condition calculus

$wp(S, R):\ \text{wp(if } (x > y) \text{ then } (a := x, b := y) \text{ else } (a := y, b := x), a > b) =$
(By Conditional Rule)
$(x > y) \Rightarrow wp((a := x, b := y), a > b) \wedge$
$\neg(x > y) \Rightarrow wp((a := y, b := x), a > b) =$
(By Assignment Rule)
$(x > y) \Rightarrow (x > y) \wedge not(x > y) \Rightarrow (y > x)$
(Simplify)
$(true \wedge not(x > y) \Rightarrow (y > x) =$
$(true) \wedge (y \neq x) =$
$(y \neq x)$

1.4 Pre-condition

For the program to satisfy: $R : a > b$, the weakest pre-condition is: $Q : x \neq y$

2 Question 2

2.1 Program statement

$S1: \quad res := 1, \quad i := 2 \quad$ (Before the loop).
$S: \quad res := res * i, \quad i := i + 1 \quad$ (Inside the loop).
$S2: \quad skip \quad$ (After the loop).

2.2 Post-condition

$R: \quad res == fact(n)$

2.3 Pre-condition

$Q: \quad n > 0$

2.4 Invariant

$I: \quad res == fact(i - 1), \quad 2 <= i <= n + 1$
(This holds true before and after the loop terminates).

2.5 Proof (partial correctness)

1. Before the Loop: $\quad Q \implies wp(S1, I)$
$n > 0 \implies wp((res := 1, i := 2), res == fact(i - 1), 2 \leq i \leq n + 1) =$
(Sequential rule)
$n > 0 \implies wp((res := 1), wp(i := 2, res == fact(i - 1), 2 \leq i \leq n + 1) =$
(Assignment rule)
$n > 0 \implies wp((res := 1), res == fact(1), 2 \leq n + 1)$
(Assignment rule)
$n > 0 \implies (1 == fact(1), 2 \leq n + 1)$
(Simplify)
$n > 0 \implies (1 == fact(1) \wedge 2 \leq n + 1)$
Which is true, if n is bigger than 0, n+1 must be equal or bigger than 2 and 1 == fact(1) is trivially true since the factorial of 1 is 1.

2. Inside the loop: $I \wedge B \implies wp(S, I)$
$(res := fact(i-1), 2 \leq i \leq n+1 \wedge i \leq n) \implies$
$wp((res := res * i, i := i+1), res == fact(i-1), 2 \leq i \leq n+1)$
(Sequential rule)
$(res := fact(i-1), 2 \leq i \leq n+1 \wedge i \leq n) \implies$
$wp((res := res * i, wp((i := i+1), res == fact(i-1), 2 \leq i \leq n+1)$
(Assignment rule)
$(res := fact(i-1), 2 \leq i \leq n+1 \wedge i \leq n) \implies$
$wp((res := res * i, res == fact(i), 2 \leq i+1 \leq n+1)$
(Assignment rule)
$(res := fact(i-1), 2 \leq i \leq n+1 \wedge i \leq n) \implies$
$(res * i == fact(i), 2 \leq i+1 \leq n+1)$
(Simplify)
$(res := fact(i-1), 2 \leq i \leq n+1 \wedge i \leq n) \implies$
$(res * i == fact(i), 1 \leq i \leq n)$
(Simplify)
$(res := fact(i-1), 2 \leq i \leq n+1 \wedge i \leq n) \implies$
$(res == fact(i-1) \wedge 1 \leq i \leq n)$
On the left-hand side of the implication, we have: $res := fact(i-1)$ and $2 \leq i \leq n$. The assignment $res := fact(i-1)$ ensures that $res == fact(i-1)$ as well, since $2 \leq i$ it follows that $i \geq 1$ since $2 > 1$. Combining this with $i \leq n$ we can conclude $1 \leq i \leq n$ therefore the right hand side holds.

3. After the loop: $I \wedge \neg B \implies wp(S2, R)$
$(res == fact(i-1), 2 \leq i \leq n+1 \wedge i > n) \implies (skip, res == fact(n))$
(Skip rule)
$(res == fact(i-1), 2 \leq i \leq n+1 \wedge i > n) \implies (res == fact(n))$
(Simplify)
$(res == fact(n), 2 \leq n+1 \wedge n+1 > n) \implies (res == fact(n))$
(Simplify)
$(res == fact(n)) \implies (res == fact(n))$
We know when the loop terminates, $i > n$ therefore since, $i \leq n+1$ is the upper-bound when we combine these, the only possible value for i is $i := n+1$ we can substitute $i := n+1$ into the invariant and we get $res == fact(n)$ then by the skip rule we show that we now satsify the post-condition