Mestrado Integrado em Engenharia Informática e Computação

Métodos Formais em Engenharia de Software 2020/21

TP1. Exercises on Program Verification with Hoare Logic

Notes:

- In exercises 1 to 6, assume that all variables are of type integer.
- At least exercises 1, 2, 3, and 4 should be completed in the first class. If exercise 5 is not completed in the class, it must be completed at home and doubts discussed in the next class.

1. Indicate (by direct inspection) whether the following Hoare triples are true (valid) or false (invalid).

a) {x>5} skip {x>0}

b) {x<6} x := x+1 {x>5}

c) {x = 5 ∧ y = 0} if x > 0 then y := 10 else skip {y = 10}

d) {x=a ∧ y =b} x := y; y := a {x=b ∧ y =a}

e) {x > y} while x > y do x := x -1 {x = y}

2. Indicate (by direct inspection) the weakest precondition (wp) in the following Hoare triples:

a) {wp} x := x+1 {x > 5}

b) {wp} if a > b then x := a else x := b {x > 0}

c) {wp} while x > y do x := x -1 {x = y}

3. Prove or disprove the Hoare triples {P}S{Q} of exercises 1.a to 1.d by calculating wp(S, Q) and proving P ⟹ wp(S, Q) (see slides 16-19).

4. Prove the Hoare triple of 1.e using the proof procedure for loops described in the slides (20-22).
Hint: Use I = (x ≥ y) and V = x-y.

5. Prove the correctness of the following program, using the proof tableau technique (slide 24). Start by selecting an appropriate loop invariant and loop variant.

Inputs: Dividend D (≥0), divisor d (>0).
Outputs: Quotient q and remainder r of integer division.

```
{D ≥ 0  ∧ d > 0}
q := 0;
r := D;
while r ≥ d  do
     q := q + 1;
     r := r - d;
{0 ≤ r < d  ∧  q × d + r = D}
```

6. (Optional, Mini-test 6/11/2019) One wants to prove the correctness of the following Hoare triple, taking as loop invariant I ≡ (z+y=x ∧ z ≥ 0) and as loop variant V ≡ z.

{ x ≥ 0} z := x; y := 0; while z ≠ 0 do (y := y+1; z := z−1) {x = y}

To that end:

a) Complete the proof tableau below, calculating by backward reasoning the weakest preconditions in the points indicated with "?".

```
1:  {x ≥ 0}
2:  {?}
3:  z := x;
4:  {?}
5:  y := 0;
6:  {z + y = x ∧ z ≥ 0}  // I
```

7: **while** $z \neq 0$ **do**
8: $\{z \neq 0 \land z + y = x \land z \geq 0 \land z = V0\}$ // $C \land I \land V = V0$
9: $\{?\}$
10: $y := y+1;$
11: $\{?\}$
12: $z := z-1$
13: $\{z + y = x \land z \geq 0 \land 0 \leq z < V0\}$ // $I \land 0 \leq V < V0$
14: $\{z = 0 \land z + y = x \land z \geq 0\}$ // $\neg C \land I$
15: $\{x = y\}$

b) Prove the implications between consecutive assertions ($1 \Rightarrow 2$, $8 \Rightarrow 9$, $14 \Rightarrow 15$).

7. (Optional) Indicate in natural language preconditions and postconditions for the following operations:

a) calculate the natural logarithm of a real number ln(x) (assuming that exp(x) is defined);

b) obtain a topological sorting of the vertices of a directed graph G=(V, E);

c) obtain an Eulerian circuit in an undirected graph G=(V, E).