U.PORTO
FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

Master in Informatics and Computing Engineering (M.EIC)

M.EIC037 | Formal Methods for Critical Systems 2021/22

Exercises on Program Verification with Hoare Logic

Notes:

- In exercises 1 to 6, assume that all variables are of type integer.

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) $\{x = 5 \wedge y = 0\}$ **if** x > 0 **then** y := 10 **else skip** $\{y = 10\}$
d) $\{x = a \wedge y = b\}$ x := y; y := a $\{x = b \wedge y = a\}$
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 $P \rightarrow$ wp(S, Q) (see slides 22-40).

4. Prove the Hoare triple of 1.e using the proof procedure for loops described in the slides (41-52).
Hint: Use $I \equiv x \geq y$ and $V \equiv x\text{-}y$.

5. Prove the correctness of the following program, using the proof tableau technique (slide 53). 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.

$\{D \geq 0 \wedge d > 0\}$
q := 0;
r := D;
while r ≥ d **do**
    q := q + 1;
    r := r - d;
$\{0 \leq r < d \ \wedge \ q \times d + r = D\}$

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

$\{ x \geq 0\}$ z := x; y := 0; **while** $z \neq 0$ **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: $\{x \geq 0\}$
2: $\{?\}$

```
3:   z := x;
4:    {?}
5:    y := 0;
6:    {z + y = x  ∧  z ≥ 0}                              // I
7:    while z ≠ 0 do
8:          {z ≠ 0  ∧  z+y = x  ∧  z ≥ 0  ∧  z = V0}     // C ∧ I ∧ V = V0
9:          {?}
10:         y := y+1;
11:         {?}
12:         z := z−1
13:         {z+y = x  ∧  z ≥ 0  ∧  0 ≤ z < V0}           // I ∧ 0 ≤ V < V0
14: {z = 0  ∧  z+y = x  ∧  z ≥ 0}                        // ¬ C ∧ I
15: {x = y}
```

b) Prove the implications between consecutive assertions (1 → 2, 8 → 9, 14 → 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).