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 (Resolution)

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 or false. **[Selected]**

a) {x>5} **skip** {x>0}
R: True

b) {x<6} x := x+1 {x>5}
R: False (counter example: x_{ini}=0)

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

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

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

2. Indicate (by direct inspection) the weakest precondition (*wp*) in the following Hoare triples. **[Selected]**

a) {*wp*} x := x+1 {x > 5}
R: x > 4

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

c) {*wp*} **while** x > y **do** x := x-1 {x = y}
R: 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 22-40). **[Selected]**

a) i) wp(skip, x>0) = x>0
ii) (P ⇒ wp(S,Q)) ⇔ (x>5 ⇒x>0) ⇔ true

b) i) wp(x:=x+1, x>5) = (x+1>5) = (x>4)
ii) (P ⇒ wp(S,Q)) ⇔ (x<6 ⇒x>4) ⇔ (x ≥ 6 ∨ x>4) ⇔ (x>4)
Since this does not reduce to true (does not always hold), the triple is not valid.

c) i) wp(if x > 0 then y := 10 else skip, y = 10)
= [(x > 0 ∧ wp(y:=10, y=10)) ∨ (x ≤ 0 ∧ wp(skip, y=10))]
= [(x > 0 ∧ 10=10) ∨ (x ≤ 0 ∧ y=10)]
= [(x > 0) ∨ (x ≤ 0 ∧ y=10)]
= (x > 0 ∨ y=10)
ii) (P ⇒ wp(S, Q)) ⇔ (x=5 ∧ y =0 ⇒x>0 ∨ y=10) ⇔ true

d) i) wp((x := y; y := a), x=b ∧ y =a)
= wp(x := y, wp(y := a, x=b ∧ y =a))
= wp(x := y, x=b ∧ a=a)
= wp(x := y, x=b)
= (y=b)
ii) (P ⇒ wp(S,Q)) ⇔ (x=a ∧ y =b ⇒ y=b) ⇔ true

4. Prove the Hoare triple of 1.e using the proof procedure for loops described in the slides (41-52). **[Selected]**

Hint: Use $I \equiv x \geq y$ and $V \equiv$ x-y.

(i) $(P \Rightarrow I) \Leftrightarrow (x > y \Rightarrow x \geq y) \Leftrightarrow$ true

(ii) $(I \wedge \neg C \Rightarrow Q)$

$\Leftrightarrow (x \geq y \wedge x \leq y \Rightarrow x = y)$

$\Leftrightarrow (x = y \Rightarrow x = y)$

$\Leftrightarrow$ true

(iii) $\{I \wedge C \wedge V{=}V_0\}$ S $\{I \wedge 0 \leq V{<}V_0\}$

$\Leftrightarrow \{x \geq y \wedge x > y \wedge x\text{-}y{=}V_0\}$ x:=x-1 $\{x \geq y \wedge 0{\leq}\, x\text{-}y{<}V_0\}$

$\Leftrightarrow \{x > y \wedge x\text{-}y{=}V_0\}$ x:=x-1 $\{x \geq y \wedge x\text{-}y{<}V_0\}$

$\Leftrightarrow (x > y \wedge x\text{-}y{=}V_0 \Rightarrow x\text{-}1 \geq y \wedge x\text{-}1\text{-}y{<}V_0)$

$\Leftrightarrow (x > y \wedge x\text{-}y{=}V_0 \Rightarrow x \geq y{+}1 \wedge x\text{-}y{\leq}V_0)$

$\Leftrightarrow (x > y \wedge x\text{-}y{=}V_0 \Rightarrow x > y \wedge x\text{-}y{\leq}V_0)$

$\Leftrightarrow$ true

So the given triple is valid (true).

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. **[Selected]**

Inputs: Dividend D ($\geq$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;
$\{0 \leq r < d \wedge q{\times}d{+}r = D\}$

R:

i) Select loop invariant and loop variant

$I = r \geq 0 \wedge d > 0 \wedge q \times d + r = D$

$V = r$

Note: d>0 is needed in the loop invariant to prove loop termination

Note: $r \geq 0$ is needed in the loop invariant to prove the post-condition

ii) inject the corresponding assertions in the code

$\{D \geq 0 \wedge d > 0\}$
q := 0;
r := D;
$\{r \geq 0 \wedge d > 0 \wedge q \times d + r = D\}$ // I
while r ≥ d do
    $\{r \geq 0 \wedge d > 0 \wedge q \times d + r = D \wedge r \geq d \wedge r = V0\}$ // $I \wedge C \wedge V{=}V0$
    q := q + 1;
    r := r - d;
    $\{r \geq 0 \wedge d > 0 \wedge q \times d + r = D \wedge 0 \leq r < V0\}$ // $I \wedge 0 \leq V < V0$
$\{r \geq 0 \wedge d > 0 \wedge q \times d + r = D \wedge r < d\}$ // $I \wedge \neg C$
$\{0 \leq r < d \wedge q \times d + r = D\}$

iii) compute weakest pre-conditions

$\{D \geq 0 \wedge d > 0\}$
$\{D \geq 0 \wedge d > 0 \wedge 0 \times d + D = D\}$
q := 0;
$\{D \geq 0 \wedge d > 0 \wedge q \times d + D = D\}$
r := D;

$\{r \geq 0 \land d > 0 \land q \times d + r = D\}$ // I
while $r \geq d$ do
$\{r \geq 0 \land d > 0 \land q \times d + r = D \land r \geq d \land r = V0\}$ // I $\land$ C $\land$ V=V0
$\{r - d \geq 0 \land d > 0 \land (q+1) \times d + (r - d) = D \land 0 \leq r - d < V0\}$
$q := q + 1;$
$\{r - d \geq 0 \land d > 0 \land q \times d + (r - d) = D \land 0 \leq r - d < V0\}$
$r := r - d;$
$\{r \geq 0 \land d > 0 \land q \times d + r = D \land 0 \leq r < V0\}$ // I $\land$ $0 \leq V < V0$
$\{r \geq 0 \land d > 0 \land q \times d + r = D \land r < d\}$ // I $\land$ $\neg C$
$\{0 \leq r < d \land q \times d + r = D\}$

iv) prove implications between pairs of consecutive assertions
$(D \geq 0 \land d > 0 \Rightarrow D \geq 0 \land d > 0 \land 0 \times d + D = D)$
$\Leftrightarrow (D \geq 0 \land d > 0 \Rightarrow D \geq 0 \land d > 0)$
$\Leftrightarrow$ true

$(r \geq 0 \land d > 0 \land q \times d + r = D \land r \geq d \land r = V0 \Rightarrow r - d \geq 0 \land d > 0 \land (q+1) \times d + (r - d) = D \land 0 \leq r - d < V0)$
$\Leftrightarrow (d > 0 \land q \times d + r = D \land r \geq d \land r = V0 \Rightarrow r \geq d \land d > 0 \land q \times d + r = D \land r < V0 + d)$
$\Leftrightarrow$ true

$(r \geq 0 \land d > 0 \land q \times d + r = D \land r < d \Rightarrow 0 \leq r < d \land q \times d + r = D)$
$\Leftrightarrow$ true

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

$$\{x \geq 0\}\ z := x;\ y := 0;\ \text{while } z \neq 0 \text{ do } (y := y+1;\ z := z-1)\ \{x = y\}$$

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

01. $\{x \geq 0\}$
02. $\{x + 0 = x \land x \geq 0\} \Leftrightarrow \{x \geq 0\}$
03. $z := x;$
04. $\{z + 0 = x \land z \geq 0\}$
05. $y := 0;$
06. $\{z + y = x \land z \geq 0\}$
07. while $z \neq 0$ do
08. $\{z \neq 0 \land z + y = x \land z \geq 0 \land z = V0\} \Leftrightarrow \{z + y = x \land z > 0 \land z = V0\}$
09. $\{z - 1 + y + 1 = x \land z - 1 \geq 0 \land z - 1 < V0\} \Leftrightarrow \{z + y = x \land z > 0 \land z - 1 < V0\}$
10. $y := y+1;$
11. $\{z - 1 + y = x \land z - 1 \geq 0 \land z - 1 < V0\}$
12. $z := z-1$
13. $\{z + y = x \land z \geq 0 \land 0 \leq z < V0\} \Leftrightarrow \{z + y = x \land z \geq 0 \land z < V0\}$
14. $\{z = 0 \land z + y = x \land z \geq 0\} \Leftrightarrow \{z = 0 \land z + y = x\} \Leftrightarrow \{z = 0 \land y = x\}$
15. $\{x = y\}$

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

i) $(x \geq 0 \Rightarrow x \geq 0) \Leftrightarrow$ true

ii) $(z + y = x \land z > 0 \land z = V0 \Rightarrow z + y = x \land z > 0 \land z - 1 < V0)$
$\Leftrightarrow (z + y = x \land z > 0 \land z = V0 \Rightarrow z + y = x \land z > 0 \land V0 - 1 < V0)$

$\Leftrightarrow \quad (z + y = x \wedge z > 0 \wedge z = V0 \Rightarrow z + y = x \wedge z > 0)$
$\Leftrightarrow$ true.

iii) $(z = 0 \wedge y = x \Rightarrow x = y)$
$\Leftrightarrow$ True

7. 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);
   pre: $x > 0$
   post: exp(result) = x

b) obtain a topological sorting of the vertices of a directed graph G=(V, E);
   pre: G is acyclic
   post: the resulting sequence $s_1, \ldots, s_n$ is a permutation of V, and
   there are no two elements s_i, s_k with $i < k$ such that (s_i, s_k) in E

c) obtain an Eulerian circuit in an undirected graph G=(V, E).
   pre: G is connected, and
   all the vertices in G have even degree (number of incident edges)
   post: the resulting circuit $(s_1, \ldots, s_{n+1})$ is such that:
   (i) $s_1 = s_{n+1}$
   (ii) $(s_1, \ldots, s_n)$ is a permutation of V
   (iii) $\forall i \in \{1,\ldots,n\} \cdot (s_i, s_{i+1}) \in E$