Software Testing and Verification 2021
Exam
June 28th, 15:15 – 18:15

- Submit your answers via Blackboard. The answers have to be in PDF format, and your name and student number should be stated clearly at the top if the first page.
- You can use the lecture note and existing online resources. You are **not** allowed to communicate about the exam question with anyone, apart from the lecturers, during the exam. This includes posting questions on forums, chats, or the like.
- If you have **questions** during the exam, use MS Teams **direct** message to `g.k.keller@uu.nl`.
- Clarifications and fixes will be posted by Wishnu or Gabriele on the **Exam** MS Teams channel. To keep traffic there low, please **do not post on the Exam channel**.
- If you do copy answers from sources other than course resources (lecture notes, slides), you need to cite your source.
- A maximum of 100 points can be obtained in this exam. They will be scaled to count for a maximum 10 points towards your final marks.

Question	Points	Score
PART I	60	
PART II	40	
Total:	100	

PART I

(a) (10 points) Consider the following two functional programs:

```
(1)   maxAll1  []      = 0
(2)   maxAll1  (x:xs) =  x max (maxAll1 xs)

(3)   maxAll2 n []       = 0 max n
(4)   maxAll2 n (x: xs) =  maxAll2 (n max x) xs
```

Using induction over lists and equational reasoning, show that for all lists of integers `xs`, we have

`maxAll1 xs = maxAll2 0 xs`

You can use the fact that **max** is associative, that is

```
(5)    a max (b max  c) =  (a max b) max c
```

(b) (6 points) Is the following statement correct or incorrect?

For any postcondition Q and program S

$$\{*\ (wp\ S\ Q) \lor Q\ *\}\ S\ \{*\ Q\ *\}$$

is a valid Hoare-triple.

If it is correct, provide a proof. If it is incorrect, provide a counter example.

(c) (8 points) Show that the following theorem holds:

If

$$(P \land \neg P_1) \Rightarrow P_2$$

holds, and

$$\{*\ P_1\ *\}\ S\ \{*\ Q_1\ *\}$$

and

$$\{*\ P_2\ *\}\ S\ \{*\ Q_2\ *\}$$

are valid Hoare-triples, then

$$\{*\ P\ *\}\ S\ \{*\ Q_1 \lor Q_2\ *\}$$

is a valid Hoare-triple as well.

(d) (8 points) What is the weakest precondition of the program S:

```
if (x > y)
  then x := x - 2;
  else y := y + 5;
```

and the post condition `x = y`? Provide the calculation of the weakest precondition, and simplify as much as possible.

(e) (8 points) Given the program S, where al variables are of type `int`

```
x := x + y;
y := x - y;
x := x - y;
```

Is the following Hoare-triple a valid specification?

$$\{*\ x < 15 \Rightarrow x = y\ *\}\ S\ \{*\ y > 10 \vee x = y\ *\}$$

If so, provide the proof. If not, explain why not. In both cases, provide the weakest precondition calculation.

(f) (10 points) Consider the following program S:

```
  a[i] := 2 * a[j];
  a[j] := a[j] - 1;
  a[i] := a[i] + 1;
```

Provide the calculation for (wp S (`a`[`i`] = `a`[`j`])). Simplify as much as possible.

(g) (10 points) Consider the following program S:

```
while (x >= y) do
  if (z > 0)
    then z := z-1;
         x := x+z;
    else y := y+1;
} end;
```

What is the weakest precondition P such that $\{*\ P\ *\}\ S\ \{*\ true\ *\}$ holds for total correctness interpretation? What is a suitable metric m to prove that S terminates, and what is a suitable invariant I? You do not need to provide the proof, just the weakest precondition, m and I.

PART II

(a) (10 points) Given the blackbox specification for the program `foo`:

```
{* low ≤ up *}
Low := low;
foo (up, OUT low, OUT y)
{* (Low ≤ y ≤ up) ∧ y - Low ≤ up - y}
```

What is the weakest precondition of the program

```
a := 2 * b;
A := a;
foo (3* a, a, b);
```

and the postcondition

Q : `b - A ≤ 4`

(b) (15 points) Consider the following program S:

```
i  := 0;
ok := a[0] ≤ a[1]; ;
while  (ok) do {
  i := i + 1;
  ok := a[i] ≤ a[i+1];
 }
```

Show that $\{* \; true \; *\} \; S \; \{* \; Q \; *\}$ for the postcondition

$$Q : (\forall \mathtt{k} : 0 \leq \mathtt{k} < \mathtt{i} : \mathtt{a}[\mathtt{k}] \leq \mathtt{a}[\mathtt{k}+1]) \wedge (\mathtt{a}[\mathtt{i}+1] < \mathtt{a}[\mathtt{i}])$$

holds under partial correctness interpretation.

(c) (5 points) Consider the precondition

$$P : N > 0$$

and the program S

```
i := 0;
while (i < N) do {
   if (a[i] == 0)
      then    i := i + 1
      else a[i] := 0;
} end;
```

Explain briefly in natural language why the S terminates under the precondition P.

(d) (10 points) For the program S from the previous question, find a termination metric m and invariant I, and provide a formal termination proof.

Hint: You can use a conditional expression of the form $(c \rightarrow e_1 \mid e_2)$ as part of your metric.

Note: The proof itself is not very complicated,but the correct metric may not be obvious, so you may want to leave it for last.

- State the metric and loop invariant clearly.
- Every step in your proof should include a justification (the hint/comment part).