Software Testing & Verification 2015/2016
Universiteit Utrecht

30th June 2016, 11:00 - 13:00, EDUC-MEGARON

Lecturer: Wishnu Prasetya

You are allowed to bring along Appendix-A of the LN.

Part I [4pt (8 × 0.5)]

For each question, choose one correct answer.

1. Which of the following is true?
   
   (a) Under the total correctness interpretation, the specification \{* true \} S \{* true \} is always valid.
   
   (b) Under the total correctness interpretation, \{* true \} S \{* true \} implies that S always terminate.
   
   (c) Under the partial correctness interpretation, the specification \{* true \} S \{* false \} is always valid.
   
   (d) Under the partial correctness interpretation, \{* false \} S \{* true \} implies that S does not terminate.

   Answer: b

2. Suppose \{* P \} S \{* Q \} is valid. Which of the following is true?

   (a) \{* Q \Rightarrow P \} S \{* Q \} is also valid.
   
   (b) If additionally \ R \Rightarrow Q \ is valid, then \{* P \} S \{* R \} is also valid.
   
   (c) If additionally \ P \Rightarrow R \ is valid, then \{* R \} S \{* Q \} is also valid.
   
   (d) If additionally \ R \Rightarrow P \ is valid, then \{* R \} S \{* Q \} is also valid.

   Answer: d

3. What is the weakest pre-condition of the following statement with respect to the post-condition Q?

   \{* ? \} if x=y then S else skip \{* Q \}

   (a) \((x=y) \lor \text{wp } S \lor Q \)
   
   (b) \((x=y) \Rightarrow \text{wp } S \lor (x\neq y) \Rightarrow Q \)
(c) \((x=y) \Rightarrow \text{wp S Q}) \land Q\)
(d) \((x=y) \land \text{wp S Q}) \lor ((x\neq y) \land Q)\)

Answer: d

4. What is the weakest pre-condition of the following statement with respect to the given post-condition?

\[
\{\ast \ ? \ast\} \ a[0] := x \ \{\ast \ a[0] = x \ast\}\]

(a) \(a(0 \ \text{repby} \ x)[x] = x\)
(b) \(a[x] = x\)
(c) \(a[a(0 \ \text{repby} \ x)[0]] = x\)
(d) \(a(0 \ \text{repby} \ x)[a[0]] = x\)

Answer: Calculating the \(\text{wp}\):

\(a(0 \ \text{repby} \ x)[a(0 \ \text{repby} \ x)[0]] = x\)

which can be simplified to:

\(a(0 \ \text{repby} \ x)[x] = x\)

So: a

5. What is the weakest pre-condition of the following statement with respect to the given post-condition?

\[
\{\ast \ ? \ast\}
\{\text{var m; assume } (\forall i :: m > a[i]) \ ; \ y := m-1 \} \{\ast \ y > m \ast\}\]

(a) \(m-1 > m\)
(b) \(\forall i :: m > a[i] \Rightarrow m-1 > m'\)
(c) \(\forall m' :: (\forall i :: m' > a[i]) \Rightarrow m'-1 > m\)
(d) \(\forall i :: m' > a[i] \land m'-1 > m\)

Answer: The \(\text{wp}\) is:

\(\forall m' :: (\forall i :: m' > a[i]) \Rightarrow m'-1 > m\)

So: c.
6. Consider the loop below; \( f \) is a pure function (so, it has no side effect) of type \( \text{int} \to \text{int} \).

\[
\text{while } x < y \text{ do } x := f(x)
\]

Which of the properties below implies that the above loop terminates?

(a) \( f(x) > 0 \)
(b) \( x > f(x) \land x > 0 \) is invariant
(c) for all \( a: a > f(a) \)
(d) for all \( a: a < f(a) \)

Answer: d
7. Consider the function \( \text{val} \) defined below. Given a list of digits, e.g. as in \( \text{val} \) \([3, 4, 5]\), it will calculate the integer value of the digits if they would be the string "345". In this case the answer is the integer 345. Notice that the function is tail recursive.

\[
\begin{align*}
\text{val} v [] &= v \\
\text{val} v (x : z) &= \text{val} (10 \times v + x) z
\end{align*}
\]

Below is an imperative implementation of the function. The specification is given.

\[
\begin{align*}
\{ \text{true} \} \\
v := 0; t := s; \\
\text{while } t \neq [] \text{ do } \{ \\
v := 10 \times v + \text{head}(t); \\
t := \text{tail}(t) \\
\} \\
\{ v = \text{val} 0 s \}
\end{align*}
\]

Which of the following is a consistent and good enough invariant to prove the correctness of the above specification?

(a) \( \text{val} v t = \text{val} v s \)
(b) \( \text{val} v t = \text{val} 0 s \)
(c) \( v = \text{val} 0 t \)
(d) \( v = \text{sum}[s_i \times 10^i \mid 0 \leq i < \text{length}(s)] \)

**Answer:** b

8. Consider the loop below; \( i \) is of type \text{int} and \( \text{isPrime}(i) \) is a side-effect-free function that checks if \( i \) is a prime number.

\[
\begin{align*}
\{ \text{true} \} \\
\text{while } i < N \land \neg \text{isPrime}(i) \text{ do } i := i + 1 \\
\{ \text{i} \neq N \Rightarrow \text{isPrime}(i) \}
\end{align*}
\]

Which of the predicates below is a correct invariant of the loop, that is enough to prove that the above specification is valid under the \textit{partial correctness} interpretation?

(a) \( 0 < i \leq N \)
(b) \( 0 < i \leq N \land \neg \text{isPrime}(i) \)
(c) \( \neg \text{isPrime}(i - 1) \lor \text{isPrime}(i) \)
(d) \( \forall k: 0 < k < i : \neg \text{isPrime}(k) \)

**Answer:** a
Part II [6pt]

1. [4 pt] Loop

Consider the following program and its specification. The program checks if every \( j \)-th element of an integer array \( a \) does not exceed \( 10^j \) (10 to the power of \( j \)).

\[
\{ * \ 0 \leq N \ * \} \quad // \text{pre-condition}
\]

\[
p := 1 ; \]
\[
k := 0 ; \]
\[
ok := true ; \]
\[
while \ k \neq N \land ok \ do \ { \]
\[
\quad ok := ok \land a[k] \leq p ;
\]
\[
\quad p := p \times 10 ;
\]
\[
\quad k := k + 1 ;
\}
\]
\[
\{ * \ ok = (\forall j : 0 \leq j < N : a[j] \leq 10^j) \ * \} \quad // \text{post-condition}
\]

Give a formal proof that the program satisfies its specification, under partial correctness.

- Please mention what your chosen invariant is.
- Every step in your proof should include a justification (the hint/comment part).
- Steps involving quantifiers should be done in small steps: each step should refer to a proof rule or a theorem in Appendix A. You can additionally use this theorem:

\[
\vdash P \Rightarrow (P = \text{true})
\]
- You don’t have to show the \( wp \) calculation.

**Answer:** Grading: 0.5 pt Pinit, 2 pt PIC, 1.5 pt EC. No separate point for the invariant; wrong invariant will show up in the proofs anyway.

Bad proof styles (BPS): deduction up to 1 pt.

Incorrect inv: 0.3 pt to maximum.

We'll use this this invariant \( I \):

\[
0 \leq k \\
\land \quad p = 10^k \\
\land \quad ok = (\forall j : 0 \leq j < k : a[j] \leq a^j)
\]

2. [1 pt] Program call

Consider the following specification of a program to find the next distinct element in an array.

\[
\{ * (\exists k : k > i : a[k] \neq a[i]) \ * \} \\
Iold := i; \ \text{findOther(READ a : int[]), OUT i : int}
\]
\[
\{ * i > Iold \land a[i] \neq a[Iold] \ * \} \\
\]
Consider the statement below, that contains a call to \texttt{findOther}. The correctness requirement is expressed as the pre-condition \(P_0\) and post-condition \(P_3\).

\[
\begin{align*}
  \{* \ P_0 : \ \forall i : (\exists k : i < k : a[i] < a[k]) \} & \\
  \{P_1 : \} & \ x := a[2i+1] ; \ i := 2i+1 ; \\
  \{P_2 : \} & \ \text{findOther}(a, i) \\
  \{* \ P_3 : \ a[i] \neq x \} & 
\end{align*}
\]

Calculate intermediate predicates \(P_2\) and \(P_1\), such that from the corresponding positions they guarantee the final post-condition \(P_3\). Use the Black Box reduction rule for program call to calculate \(P_2\), and standard \(wp\) calculation for \(P_1\).

Note that in the above case, the actual parameters passed to the call are literally the same as the formal parameters. Therefore, there is no need to transform the call.

Just give the answers; you do not have to show the calculation. The specification is valid; you can use this fact as a check in your own calculation.

\textbf{Answer:}

\[
\begin{align*}
  2 & : \ (\exists k : k > i : a[k] \neq a[i]) \land ((i' > i \land a[i'] \neq a[i]) \Rightarrow (a[i'] \neq x)) \\
  1 & : \ (\exists k : k > 2i+1 : a[k] \neq a[2i+1]) \land ((i' > 2i+1 \land a[i'] \neq a[2i+1]) \Rightarrow (a[i'] \neq a[2i+1]))
\end{align*}
\]

3. [1 pt, challenging] \textbf{Termination.}

Consider this program, with the given pre-condition:

\[
\begin{align*}
  \{* \ 0 < x < y *\} & \\
  \text{while } x < y \ \text{do } \{ \text{if } y-x=1 \ \text{then } y := y+1 \ \text{else } y := y-2 \ \} & 
\end{align*}
\]

Prove that if the above program starts from the given pre-condition, it will terminate. We do not care in which state the program would terminate. You can skip the proofs of Init, IC, and EC, but do mention your chosen invariant (make sure it is a consistent invariant).

Mention your termination metric, then prove the conditions TC1 and TC2. Do mention the resulting \(wp\) in TC1.

\textbf{Answer:} Using \(\text{odd}(y-x) \rightarrow 2y \mid y\) as the termination metric \(m\). And using \(0 < x\) as invariant will do.

It is not difficult to show that the metric is \(> 0\) at the start of every iteration. To show that that it decreases it decreases, we have to prove this:

\[
x < N \Rightarrow \ wp \ (C := m ; \ \text{body}) \ (m < C)
\]

Calculating the \(wp\) gives:

\[
\begin{align*}
  (y-x=1) \land ((\text{odd}(y+1-x) \rightarrow 2(y+1) \mid y+1) < ((\text{odd}(y-x) \rightarrow 2y \mid y))) & \\
  \lor & \\
  (y-x\neq1) \land ((\text{odd}(y-2-x) \rightarrow 2(y-2) \mid y-2) < ((\text{odd}(y-x) \rightarrow 2y \mid y))) & 
\end{align*}
\]
which can be simplified to:

\[(y-x=1) \land y+1 < 2y \]
\[\lor\]
\[(y-x\neq1) \land ((\text{odd}(y-2-x) \rightarrow 2(y-2) | y-2) < ((\text{odd}(y-x) \rightarrow 2y | y)))\]

The first disjunct is implied by \( y > x \) and \( x > 0 \); therefore \( y > 1 \), therefore \( 2y > y+1 \). The second disjunct is valid.