Research School of Computer Science, Australian National University
COMP2600 — Formal Methods in Software Engineering
Semester 2, 2015

Assignment 3 : Hoare Logic, WP Calculus and Separation Logic

Due 11:59 pm Friday 30th of October 2015

The submission of your assignment must be done via the assignment boxes in the student foyer. Failure to submit by the due date will result in late penalties of five percent per **weekday** for the whole assignment. Since Saturday 31st of October and Sunday 1st of November are not weekdays, I will not check the submission boxes until 1700 on Monday 2nd of November!

Other arrangements that are required because of truly exceptional circumstances need to be negotiated before your deadline. Your submission must be well-presented on clean A4 paper with a fully completed standard cover page, including your tutor's name and your tutorial group. Failure to follow this instruction will result in a penalty. The COMP2600 Assignments page has a link to an appropriate cover page. You may *not* collaborate with others on this assignment and we will penalise and report any suspected collusion or plagiarism to the appropriate authorities. Attending the CSSA study sessions is okay.

Questions about the assignment should be posted to the COMP2600-2015 Piazza forum. If you email me with a general question about the assignment then I will reply via the forum as this saves my having to answer the same question multiple times. If you email me from a non-ANU account, such as gmail or yahoo, I will ignore your email.

Assignment 3 as a whole is worth 60 marks and this constitutes 13.5 % of your final mark since the material took 9 out of 24 lectures of assessable material i.e. 13.5 = (9/24)*36: see `http://cs.anu.edu.au/courses/COMP2600/outline.html`

If any of this is unclear then post a question to the Piazza forum.

Why the delay? Because one of our guest speakers is going to talk about primality testing so I wanted to use primality testing in this assignment. However, a simple web search turns up this:
`http://se.inf.ethz.ch/courses/2010b_fall/sv/exercises/Hoare-recap.pdf`
which uses primality testing as the example (with solutions)!

You are free to look at the ethz solution if you wish. But I have spent the last three days changing my initial version so that the ethz solution will not help you much. In fact, it may confuse you. I am also trying to show you the pitfalls of "formal verification".

Please complain officially via SELTS if you think that my delay has harmed your studies!

An algorithm for determining whether a number is prime.

A natural number $a > 1$ is a prime if it has no factors others than 1 and itself.

Let *Prog* be the program below where $y \; != \; 1$ means $y \neq 1$:

```
1   x := 1;
2   y := 0
3   while (y != 1) & (x < a) do
4         x := x + 1            (* so now x >= 2 *)
5         if (a mod x) = 0 then y := 1
```

where the while loop (lines 3-5) is W, the loop body (lines 4-5) is B, and the initialisation assignments (lines 1-2) is I, and $a \; mod \; x$ is the modulus function that returns 0 when x divides a without any remainder i.e. when x is a factor of a.

Thus, intuitively, the program repeatedly increments x and sets y to the value 1 if the original number a can be divided by x with a zero remainder. It stops when x reaches the value a or when $y = 1$

Question 1. Hoare Logic: 20 marks.

The Aim. To establish a vacuous precondition (**true**) for the postcondition

$$(y = 1) \Rightarrow \exists z.(a \ mod \ z = 0)$$

since this postcondition guarantees that a has a factor $z \neq 1$.

Let Q be the postcondition $(y = 1) \Rightarrow \exists z.(a \ mod \ z = 0)$.

Our aim is to prove: $\{\mathbf{true}\}$ `Prog` $\{Q\}$

That is: $\{\mathbf{true}\}$ `I;W` $\{Q\}$

The proof will have this structure where P is the loop-invariant:

$$\dfrac{\dfrac{\vdots}{\{\mathbf{true}\}\ \texttt{I}\ \{P\}} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\{b \wedge P\}\ \texttt{x := x + 1}\ \{R\}}{\{b \wedge P\}\ \texttt{x := x + 1; if a mod x = 0 then y := 1}\ \{P\}} \qquad \dfrac{\{R \wedge a \ mod \ x = 0\}\ \texttt{y := 1}\ \{P\} \qquad R \wedge a \ mod \ x \neq 0 \Rightarrow P}{\{R\}\ \texttt{if a mod x = 0 then y := 1}\ \{P\}}}{\{b \wedge P\}\ \texttt{B}\ \{P\}}}{\{P\}\ \texttt{while b do B}\ \{P \wedge \neg b\}}\ \text{While}}{\{P\}\ \texttt{while b do B}\ \{Q\}}\ \text{PostCondWk}}{\{\mathbf{true}\}\ \texttt{I;while b do B}\ \{Q\}}\ \text{Seq}$$

Note: B is the S part of the while rule. The while rule uses a b which is the formula $(y \neq 1) \wedge (x < a)$, and so $\neg b$ is $(y = 1) \vee (x \geq a)$.

Loop Invariant. The first task is to find the loop invariant but to make life easier for you, one loop invariant that suffices is the following:

$$P \;\equiv\; 1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \; mod \; z = 0)$$

.

We are going to construct a line by line proof of: $\{\textbf{true}\}$ `Prog` $\{P\}$ but we will do the left hand sub-proof first and then do the right hand sub-proof to make marking easier.

Make sure every step of your proofs carry full and correct justifications. If you need to prove an intermediate result, do so in a separate lemma.

Prove: $\{\textbf{true}\}$ `I` $\{P\}$ (**5 marks**)

Solution

1. $\{1 \leq 1 \wedge 1 < a\}$ `x` := `1` $\{1 \leq x \wedge 1 < a\}$ (Asst)
2. $\{\textbf{true}\}$ `x` := `1` $\{1 \leq x \wedge 1 < a\}$ (PreConEqv)
3. deliberately left blank
4. $\{1 \leq x \wedge 1 < a \wedge (0 = 1 \Rightarrow \exists z.a \; mod \; z = 0)\}$ `y` := `0` $\{$
   $1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \; mod \; z = 0)\}$ (Asst)
5. $\{1 \leq x \wedge 1 < a\}$ `y` := `0` $\{1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \; mod \; z = 0)\}$ (PreConEqv)
6. deliberately left blank
7. $\{\textbf{true}\}$ `x` := `1` ; `y` := `0` $\{1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \; mod \; z = 0)\}$ (Seq 2, 5)
8. $\{\textbf{true}\}$ `I` $\{P\}$

Prove: $\{b \wedge P\}$ `x := x + 1` $\{R\}$ where

$$R \equiv y \neq 1 \wedge x \leq a \quad \wedge \quad 2 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)$$

3 marks

Solution

a. $\{y \neq 1 \wedge x < a \quad \wedge \quad 1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)\}$ `x := x + 1` $\{$
$y \neq 1 \wedge x - 1 < a \quad \wedge \quad 1 \leq x - 1 \quad \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)\}$ (Asst)

b. $\{y \neq 1 \wedge x < a \quad \wedge \quad 1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)\}$ `x := x + 1` $\{$
$y \neq 1 \wedge x < a+1 \quad \wedge \quad 2 \leq x \quad \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)\}$ (PostConEq)

c. $\{y \neq 1 \wedge x < a \quad \wedge \quad 1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)\}$ `x := x + 1` $\{$
$y \neq 1 \wedge x \leq a \quad \wedge \quad 2 \leq x \quad \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)\}$ (PostConEq)

Prove: $\{R \wedge a \ mod \ x = 0\}$ `y := 1` $\{P\}$ **3 marks**

Solution

a. $\{1 \leq x \quad \wedge 1 < a \wedge (1 = 1 \Rightarrow \exists z.a \ mod \ z = 0)\}$ `y := 1` $\{$
$1 \leq x \quad \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)\}$ (Asst)

b. $\{y \neq 1 \wedge x \leq a \wedge 2 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0) \wedge a \ mod \ x = 0\}$ `y := 1` $\{$
$1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)\}$ (PreConStr)

Prove: $(R \wedge a \ mod \ x \neq 0) \Rightarrow P$ **3 marks**

Solution Suppose

$$y \neq 1 \wedge x \leq a \wedge 2 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0) \wedge \ a \ mod \ x \neq 0$$

is true. We have to show that so is

$$1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0)$$

But $2 \leq x$ implies $1 \leq x$ and $y \neq 1$ implies $(y \neq 1 \vee \exists z.a \ mod \ z = 0)$, which is logically equivalent to $(y = 1 \Rightarrow \exists z.a \ mod \ z = 0)$. Thus P holds as required.

Prove: $P \wedge \neg b \Rightarrow Q$ **2 marks**

Solution Suppose $(1 \leq x \wedge 1 < a \wedge (y = 1 \Rightarrow \exists z.a \ mod \ z = 0) \wedge \neg(y \neq 1 \wedge x < a))$. Thus $(y = 1 \Rightarrow \exists z.a \ mod \ z = 0)$ holds trivially.

Thus we have met our aim.

Suppose we now wanted to add a final extra line to output an answer as follows:

```
7 If C then print(``a is not prime'')
```

What should C be ? **4 marks**

Solution $C \equiv (x \neq a)$ because if $x = a$ then $y = 1$ and $a \ mod \ a = 0$ but a is prime! That is, for this program, our Q is made vacuously true by prime numbers so it is not a good measure of success! Lesson: make sure that your Q really does what you think it does! This is why Hoare now says that testing is also an important part of ensuring correctness!

Once again, every step of your proofs must carry full and correct justifications.
If you need to prove an intermediate result, do so in a separate lemma.

Question 2. Weakest Precondition 20 marks

In the previous question, we assumed that $1 < a$: that is, a was a natural number greater than 1. Let us drop this assumption and calculate the weakest precondition required to guarantee Q:

$$wp(Prog, Q)$$

Find P_k. The first step in the proof is to determine the sequence $P_0, P_1, P_2 \ldots$ from the definitions given for these in the weakest precondition calculus. This can be done by (careful) calculation using the *wp* definition for *While*.

Instruction: write out the definition for each P_i and work inwards from the far right hand side as it is easy to get confused if you substitute for the various expressions too early. To make marking easier I have given a plan of the solution so please follow the plan.

Solution

$$
\begin{aligned}
P_0 &\equiv \neg b \wedge\ Q \\
&\equiv\ \neg(y \neq 1 \wedge x < a) \wedge Q \\
&\equiv\ (y = 1 \vee x \geq a) \wedge (y = 1 \Rightarrow a\ mod\ x = 0)
\end{aligned}
$$

(2 marks)

$$
\begin{aligned}
P_1 &\equiv\ b \wedge\ wp(B, P_0) \\
&\equiv\ b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}\ ;\ \texttt{if a mod x} = \texttt{0 then y} := \texttt{1}, P_0) \\
&\equiv\ b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, wp(\texttt{if a mod x} = \texttt{0 then y} := \texttt{1}, P_0)) \\
&\equiv\ b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, P_1^1)
\end{aligned}
$$

$$
\begin{aligned}
P_1^1 &\equiv wp(\texttt{if a mod x} = \texttt{0 then y} := \texttt{1}, P_0) \\
&\equiv (a\ mod\ x = 0 \wedge wp(\texttt{y} := \texttt{1}, P_0)) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_0) \\
&\equiv (a\ mod\ x = 0 \wedge P_1^2) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_0)
\end{aligned}
$$

$$
\begin{aligned}
P_1^2 &\equiv wp(\texttt{y} := \texttt{1}, P_0) \\
&\equiv\ (1 = 1 \vee x \geq a) \wedge (1 = 1 \Rightarrow a\ mod\ x = 0) \\
&\equiv\ a\ mod\ x = 0
\end{aligned}
$$

$$
\begin{aligned}
P_1^1 &\equiv (a\ mod\ x = 0 \wedge P_1^2) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_0) \\
&\equiv (a\ mod\ x = 0 \wedge a\ mod\ x = 0) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_0) \\
&\equiv (a\ mod\ x = 0) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_0) \\
&\equiv a\ mod\ x = 0 \quad \vee \quad P_1^3
\end{aligned}
$$

$$
\begin{aligned}
P_1^3 &\equiv a\ mod\ x \neq 0 \wedge P_0 \\
&\equiv a\ mod\ x \neq 0 \wedge ((y = 1 \vee x \geq a) \wedge (y = 1 \Rightarrow a\ mod\ x = 0)) \\
&\equiv a\ mod\ x \neq 0 \wedge (y = 1 \vee x \geq a) \wedge (y \neq 1 \vee a\ mod\ x = 0) \\
&\equiv a\ mod\ x \neq 0 \wedge (y = 1 \vee x \geq a) \wedge y \neq 1 \\
&\equiv a\ mod\ x \neq 0 \wedge x \geq a \wedge y \neq 1
\end{aligned}
$$

$$
P_1^1 \equiv a\ mod\ x = 0 \quad \vee \quad a\ mod\ x \neq 0 \wedge x \geq a \wedge y \neq 1
$$

$$
\begin{aligned}
P_1 &\equiv\ b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, P_1^1) \\
&\equiv\ b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, a\ mod\ x = 0 \quad \vee \quad a\ mod\ x \neq 0 \wedge x \geq a \wedge y \neq 1) \\
&\equiv\ b \wedge \quad (a\ mod\ x + 1 = 0 \quad \vee \quad a\ mod\ x + 1 \neq 0 \wedge x + 1 \geq a \wedge y \neq 1) \\
&\equiv\ (y \neq 1 \wedge x < a) \wedge \quad (a\ mod\ x + 1 = 0 \quad \vee \quad a\ mod\ x + 1 \neq 0 \wedge x + 1 \geq a \wedge y \neq 1) \\
&\equiv\ (y \neq 1 \wedge x < a) \wedge \quad (a\ mod\ x + 1 = 0 \quad \vee \quad a\ mod\ x + 1 \neq 0 \wedge x + 1 \geq a)
\end{aligned}
$$

(3 marks)

$$
\begin{aligned}
P_2 \equiv\ & b \wedge\ wp(B, P_1) \\
\equiv\ & b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}\ ;\ \texttt{if a mod x} = \texttt{0 then y} := \texttt{1}, P_1) \\
\equiv\ & b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, wp(\texttt{if a mod x} = \texttt{0 then y} := \texttt{1}, P_1)) \\
\equiv\ & b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, P_2^1)
\end{aligned}
$$

$$
\begin{aligned}
P_2^1 \equiv & wp(\texttt{if a mod x} = \texttt{0 then y} := \texttt{1}, P_1) \\
\equiv & (a\ mod\ x = 0 \wedge wp(\texttt{y} := \texttt{1}, P_1)) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_1) \\
\equiv & (a\ mod\ x = 0 \wedge P_2^2) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_1)
\end{aligned}
$$

$$
\begin{aligned}
P_2^2 \equiv & wp(\texttt{y} := \texttt{1}, P_1) \\
\equiv\ & (1 \neq 1 \wedge x < a) \wedge \quad (a\ mod\ x + 1 = 0 \quad \vee \quad a\ mod\ x + 1 \neq 0 \wedge x + 1 \geq a) \\
\equiv\ & False
\end{aligned}
$$

$$
\begin{aligned}
P_2^1 \equiv & (a\ mod\ x = 0 \wedge P_2^2) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_1) \\
\equiv & a\ mod\ x \neq 0 \wedge P_1 \\
\equiv & a\ mod\ x \neq 0 \wedge y \neq 1 \wedge x < a \wedge \quad (a\ mod\ x + 1 = 0 \quad \vee \quad a\ mod\ x + 1 \neq 0 \wedge x + 1 \geq a)
\end{aligned}
$$

$$
\begin{aligned}
P_2 \equiv\ & b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, P_2^1) \\
\equiv\ & b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, \\
& a\ mod\ x \neq 0 \wedge y \neq 1 \wedge x < a \wedge \quad (a\ mod\ x + 1 = 0 \quad \vee \quad a\ mod\ x + 1 \neq 0 \wedge x + 1 \geq a) \\
\equiv\ & (y \neq 1 \wedge x < a)\ \wedge \\
& (a\ mod\ x + 1 \neq 0 \wedge x + 1 < a \wedge \quad (a\ mod\ x + 2 = 0 \quad \vee \quad a\ mod\ x + 2 \neq 0 \wedge x + 2 \geq a))
\end{aligned}
$$

(4 marks)

Assuming that

$$
\begin{aligned}
P_1 \equiv\ & y \neq 1\ \wedge x < a \\
& \qquad \wedge (a\ mod\ x + 1 \neq 0 \Rightarrow x + 1 \geq a) \\
P_2 \equiv\ & y \neq 1 \wedge x < a \\
& \wedge a\ mod\ x + 1 \neq 0 \wedge x + 1 < a \\
& \qquad \wedge (a\ mod\ x + 2 \neq 0 \Rightarrow x + 2 \geq a))
\end{aligned}
$$

and assuming that

$$
\begin{aligned}
P_k \equiv\ & y \neq 1 \wedge x < a \\
& \wedge a\ mod\ x + 1 \neq 0 \wedge x + 1 < a \\
& \wedge a\ mod\ x + 2 \neq 0 \wedge x + 2 < a \\
& \cdots \\
& \wedge a\ mod\ x + k - 1 \neq 0 \wedge x + k - 1 < a \\
& \qquad \wedge (a\ mod\ x + k \neq 0 \Rightarrow x + k \geq a))
\end{aligned}
$$

follow the solution skeletons shown for P_1 and P_2 to compute the analogues P_k^1, P_k^2 to

prove that

$$
\begin{aligned}
P_{k+1} &\equiv\ b \wedge\ wp(B, P_k) \\
&\equiv\ b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}\ ;\ \texttt{if a mod x} = \texttt{0 then y} := \texttt{1}, P_k) \\
&\equiv\ b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, wp(\texttt{if a mod x} = \texttt{0 then y} := \texttt{1}, P_k)) \\
&\equiv\ b \wedge wp(\texttt{x} := \texttt{x} + \texttt{1}, P_k^1)
\end{aligned}
$$

$$
\begin{aligned}
P_k^1 &\equiv wp(\texttt{if a mod x} = \texttt{0 then y} := \texttt{1}, P_k) \\
&\equiv (a\ mod\ x = 0 \wedge wp(\texttt{y} := \texttt{1}, P_k)) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_k) \\
&\equiv (a\ mod\ x = 0 \wedge P_k^2) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_k)
\end{aligned}
$$

$$
\begin{aligned}
P_k^2 &\equiv wp(\texttt{y} := \texttt{1}, P_k) \\
&\equiv\ 1 \neq 1 \wedge x < a \\
&\qquad \wedge\ a\ mod\ x + 1 \neq 0 \wedge x + 1 < a \\
&\qquad \wedge\ a\ mod\ x + 2 \neq 0 \wedge x + 2 < a \\
&\qquad \cdots \\
&\qquad \wedge\ a\ mod\ x + k - 1 \neq 0 \wedge x + k - 1 < a \\
&\equiv\ False
\end{aligned}
$$

$$
\begin{aligned}
P_k^1 &\equiv (a\ mod\ x = 0 \wedge P_k^2) \quad \vee \quad (a\ mod\ x \neq 0 \wedge P_k) \\
&\equiv a\ mod\ x \neq 0 \wedge P_k \\
&\equiv a\ mod\ x \neq 0\ \wedge \\
&\qquad y \neq 1 \wedge x < a \\
&\qquad \wedge\ a\ mod\ x + 1 \neq 0 \wedge x + 1 < a \\
&\qquad \wedge\ a\ mod\ x + 2 \neq 0 \wedge x + 2 < a \\
&\qquad \cdots \\
&\qquad \wedge\ a\ mod\ x + k - 1 \neq 0 \wedge x + k - 1 < a \\
&\qquad\qquad\qquad \wedge\ (a\ mod\ x + k \neq 0 \Rightarrow x + k \geq a))
\end{aligned}
$$

$$
\begin{aligned}
P_{k+1} \equiv\ & b \wedge wp(\mathtt{x} := \mathtt{x} + \mathtt{1}, P_k^1) \\
\equiv\ & b \wedge wp(\mathtt{x} := \mathtt{x} + \mathtt{1}, \\
& \quad a \ mod \ x \neq 0 \wedge \\
& \quad y \neq 1 \wedge x < a \\
& \quad \wedge a \ mod \ x + 1 \neq 0 \wedge x + 1 < a \\
& \quad \wedge a \ mod \ x + 2 \neq 0 \wedge x + 2 < a \\
& \quad \cdots \\
& \quad \wedge a \ mod \ x + k - 1 \neq 0 \wedge x + k - 1 < a \\
& \qquad \wedge (a \ mod \ x + k \neq 0 \Rightarrow x + k \geq a)) \\
\equiv\ & y \neq 1 \wedge x < a \\
& \quad \wedge a \ mod \ x + 1 \neq 0 \wedge x + 1 < a \\
& \quad \wedge a \ mod \ x + 2 \neq 0 \wedge x + 2 < a \\
& \quad \wedge a \ mod \ x + 3 \neq 0 \wedge x + 3 < a \\
& \quad \cdots \\
& \quad \wedge a \ mod \ x + k \neq 0 \wedge x + k < a \\
& \qquad \wedge (a \ mod \ x + k + 1 \neq 0 \Rightarrow x + k + 1 \geq a)
\end{aligned}
$$

(6 marks)

Weakest precondition of the loop. Calculate

$$wp(W, Q) = \exists k.\ k \geq 0 \wedge P_k$$

Solution

$$\begin{aligned}
wp(W, Q) &\equiv P_0 \vee \exists k.\ k \geq 1 \wedge P_k \\
&\equiv\ (y = 1 \vee x \geq a) \wedge (y = 1 \Rightarrow a\ mod\ x = 0) \vee \\
&\quad \exists k.\ k \geq 1 \wedge\ \ y \neq 1 \wedge x < a \\
&\quad \wedge\, a\ mod\ x + 1 \neq 0 \wedge x + 1 < a \\
&\quad \wedge\, a\ mod\ x + 2 \neq 0 \wedge x + 2 < a \\
&\quad \cdots \\
&\quad \wedge\, a\ mod\ x + k - 1 \neq 0 \wedge x + k - 1 < a \\
&\qquad\qquad \wedge\, (a\ mod\ x + k \neq 0 \Rightarrow x + k \geq a))
\end{aligned}$$

(3 marks)

Finalise the proof. Complete the proof of the program by showing that

$$\begin{aligned}
wp(I; W, Q) \equiv (1 \geq a) \vee \\
\exists k.\ k \geq 1 \wedge\ \ 1 < a \\
\wedge\, a\ mod\ 2 \neq 0 \wedge 2 < a \\
\wedge\, a\ mod\ 3 \neq 0 \wedge 3 < a \\
\cdots \\
\wedge\, a\ mod\ k \neq 0 \wedge k < a \\
\qquad\qquad \wedge\, (k \neq a \Rightarrow a\ mod\ 1 + k = 0))
\end{aligned}$$

(2 marks)

Once again, every step of your proofs must carry full and correct justifications.
If you need to prove an intermediate result, do so in a separate lemma.

Question 3. Separation Logic. 5 marks

a. Consider the allocation axiom:

$$\{x = v \wedge \texttt{emp}\}\ \texttt{x} := \texttt{cons}(\texttt{e}_1, \texttt{e}_2, \cdots, \texttt{e}_\texttt{n})\ \{x \mapsto e_1(v/x), e_2(v/x), \cdots, e_n(v/x)\}$$

where v is an auxilliary variable different from x and not appearing in $e_1, e_2, \cdots, e_n$ and where

$$x \mapsto e_1(v/x), e_2(v/x), \cdots, e_n(v/x)$$

abbreviates the formula

$$x \mapsto e_1(v/x)\ *\ (x{+}1) \mapsto e_2(v/x)\ *\ (x{+}2) \mapsto e_3(v/x) \cdots\ *\ (x{+}n{-}1) \mapsto e_n(v/x)$$

(1) What is the size of the heap after this instruction completes?
Solution n

(2) How many variables are given a value in the store by this instruction?
Solution 1

(3) If there is not enough memory to allocate, does this instruction fault?
Solution no, it does not fault by definition!

(4) Why are the allocated memory locations contiguous?
Solution Because the left hand sides of the points-to formulae form are x, $x + 1$, ..., $x + n - 1$ which means that the respective heaps are each of size 1 but form a contiguous chain.

(5) Why do we insist that the pre-condition contains `emp`?
Solution To enforce our goal to reason about the smallest possible heap at all times.

5 marks (1 mark each)

Question 4. Separation Logic. 15 marks

Let Π be the following program:

```
x := cons(1,2) ;
dispose(x)
```

Our goal is to prove

$\{\texttt{emp}\}\ \Pi\ \{(x+1) \mapsto 2)\}$

You may need the following properties of separation logic:

Purity: $(A \wedge B)\ *\ C \Leftrightarrow A \wedge (B\ *\ C)$ if A contains no occurrences of `emp`, $*$ and $\mapsto$

Commutativity of $*$: $(A\ *\ B) \Leftrightarrow (B\ *\ A)$

Commutativity of $\wedge$: $(A \wedge B) \Leftrightarrow (B \wedge A)$

Unit Property: $(\texttt{emp}\ *\ B) \Leftrightarrow B$

a. Prove $\{\texttt{emp}\}\ \texttt{x} := \texttt{cons}(1,2)\ \{x \mapsto 1\ *\ (x+1) \mapsto 2\}$

Set out the proof as a linear sequence of numbered lines with justifications on the right hand side as usual. Do *not* use the frame rule. My solution is three lines long but any proper proof without the frame rule will do. **(2 marks)**

Solution

(1) $\{\texttt{emp}\}\ \texttt{x} := \texttt{cons}(1,2)\ \{x \mapsto 1, 2\}$ (DerAllAssAxm)

(2) $(x \mapsto 1, 2) \Leftrightarrow x \mapsto 1\ *\ (x+1) \mapsto 2$ (Abbreviation)

(3) $\{\texttt{emp}\}\ \texttt{x} := \texttt{cons}(1,2)\ \{x \mapsto 1\ *\ (x+1) \mapsto 2\}$ (a1, a2 PostConEq)

b. Prove $\{x \mapsto 1\}\ \texttt{dispose}(\texttt{x})\ \{\texttt{emp}\}$

Set out the proof as a linear sequence of numbered lines with justifications on the right hand side as usual. My solution is three lines long but any proper proof will do.

(3 marks)

Solution

(1) $\{x \mapsto -\}\ \texttt{dispose}(\texttt{x})\ \{\texttt{emp}\}$ (DisposeAxm)

(2) $\{\exists z.x \mapsto z\}\ \texttt{dispose}(\texttt{x})\ \{\texttt{emp}\}$ (b1 Abbrev)

(3) $\{x \mapsto 1\}\ \texttt{dispose}(\texttt{x})\ \{\texttt{emp}\}$ (b2 PreConStr)

c. Using (a) and (b) prove $\{\texttt{emp}\}\ \texttt{x} := \texttt{cons}(1,2)\ ;\ \texttt{dispose}(\texttt{x})\ \{(x+1) \mapsto 2\}$

Set out the proof as a linear sequence of numbered lines with justifications on the right hand side as usual. My solution has first line (a) and second line (b), and then five more lines, but any proper proof will do.

(10 marks)

Solution

(1) $\{\texttt{emp}\}\ \texttt{x} := \texttt{cons}(1,2)\ \{x \mapsto 1\ *\ (x+1) \mapsto 2\}$ a

(2) $\{x \mapsto -\}\ \texttt{dispose}(\texttt{x})\ \{\texttt{emp}\}$ b

(3) $\{x \mapsto -\ *\ (x+1) \mapsto 2\}\ \texttt{dispose}(\texttt{x})\ \{\texttt{emp}\ *\ (x+1) \mapsto 2\}$ (c2 Frame Rule)

(4) $(\texttt{emp}\ *\ (x+1) \mapsto 2) \Leftrightarrow (x+1) \mapsto 2$ (Unit Property)

(5) $\{x \mapsto -\ *\ (x+1) \mapsto 2\}\ \texttt{dispose}(\texttt{x})\ \{(x+1) \mapsto 2\}$ (c3, c4 PostConEqv)

(6) $\{\texttt{emp}\}\ \texttt{x} := \texttt{cons}(1,2)\ \{x \mapsto -\ *\ (x+1 \mapsto 2\}$ (c1 PostConWk)

(7) $\{\texttt{emp}\}\ \texttt{x} := \texttt{cons}(1,2)\ ;\ \texttt{dispose}(\texttt{x})\ \{(x+1) \mapsto 2\}$ (c6, c5 Seq)

I know that some of you understand separation logic very well so you might be tempted to give a direct short solution to (c) without doing parts (a) and (b). Please don't do this as it makes it harder for us to mark your assignment. I am more than happy to discuss such ideas over the forum so that we get a good discussion going. That is, please do the sub-parts of this question as stated.