THE AUSTRALIAN NATIONAL UNIVERSITY

Mid-Semester Quiz
Second Semester, 2014

COMP2600
(Formal Methods for Software Engineering)

Writing Period: 1 hour duration
Study Period: 10 minutes duration
Permitted Materials: One A4 page with hand-written notes on both sides

Answer questions Q1, Q2, (Q3 exor Q4) Q5, Q6
Total marks: 45
That is, either do Q3 or do Q4. If you do parts of Q3 and parts of Q4 then we will choose the one that gives you most marks, but you will not get marks for both parts.

The questions are followed by labelled blank spaces into which your answers are to be written.
Additional answer panels are provided at the end of the paper should you wish to use more space for an answer than is provided in the associated labelled panels.

Student Number:

Q1 Mark | Q2 Mark | Q3 Mark | Q4 Mark | Q5 Mark | Q6 Mark | Total Mark
QUESTION 1 [10 marks]

Structural Induction

Here is the usual Haskell definition of a binary tree:

\[
\text{data Tree } a = \text{Nil} \mid \text{Node } a \ (\text{Tree } a) \ (\text{Tree } a)
\]

Given these function definitions:

- \(\text{sumT Nil} = 0\)  \hspace{1cm} \text{(ST1)}
- \(\text{sumT} \ (\text{Node } a \ t1 \ t2) = a + \text{sumT} \ t1 + \text{sumT} \ t2\)  \hspace{1cm} \text{(ST2)}
- \(\text{sumL} \ [] = 0\)  \hspace{1cm} \text{(SL1)}
- \(\text{sumL} \ (x:xs) = x + \text{sumL} \ xs\)  \hspace{1cm} \text{(SL2)}
- \(\text{flatten Nil} = []\)  \hspace{1cm} \text{(F1)}
- \(\text{flatten} \ (\text{Node } a \ t1 \ t2) = \text{flatten} \ t1 ++ (a : \text{flatten} \ t2)\)  \hspace{1cm} \text{(F2)}
- \([] ++ ys = ys\)  \hspace{1cm} \text{(A1)}
- \((x:xs) ++ ys = x : (xs ++ ys)\)  \hspace{1cm} \text{(A2)}

and the following lemma:

- \(\text{sumL} \ (xs ++ ys) = \text{sumL} \ xs + \text{sumL} \ ys\)  \hspace{1cm} \text{(L1)}

Prove the following property using structural induction:

\(\text{sumT} \ t = \text{sumL} \ (\text{flatten} \ t)\)

(a) State and prove the base case goal.
(b) State the induction hypotheses.

QUESTION 1(b) [2 marks]

(c) State and prove the step case goal.

QUESTION 1(c) [6 marks]
QUESTION 2 [10 marks]

Logic

(a) Use truth tables to determine whether the following proposition is valid, or is a contradiction, or is a contingency:

\[(p \rightarrow (q \lor r)) \iff (p \rightarrow q) \lor (p \rightarrow r)\]

In addition to giving the truth table, your answer needs to explicitly state whether the proposition is valid, or is a contradiction, or is a contingency.

For brevity, the truth table template below uses the abbreviations:

\[R_1 \equiv (p \rightarrow q) \lor (p \rightarrow r)\]
\[R_2 \equiv (p \rightarrow (q \lor r)) \iff (p \rightarrow q) \lor (p \rightarrow r)\]

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>r</th>
<th>q \lor r</th>
<th>p \rightarrow (q \lor r)</th>
<th>p \rightarrow q</th>
<th>p \rightarrow r</th>
<th>R_1</th>
<th>R_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

COMP2600 (Formal Methods for Software Engineering) Page 4 of 20
(b) This question discusses a computer system where a number of processes may be running. Each process consists of a number of threads. The following predicates are given:

- \( T(x) \) - \( x \) can be terminated
- \( R(x) \) - \( x \) is running
- \( B(x, y) \) - \( x \) belongs to \( y \)

Translate the following sentence into First-Order Logic: *Any process can be terminated unless some thread belonging to the process is running.*

**QUESTION 2(b)** [3 marks]

(c) Give a natural deduction proof of \( (\forall x. P(x)) \land (\exists y. P(y) \rightarrow Q(y)) \rightarrow \exists z. Q(z) \)

You may only use the introduction and elimination rules given in Appendix 1. Number each line and include justifications for each step.

**QUESTION 2(c)** [5 marks]
QUESTION 3 [11 marks]

Hoare Logic

Consider the following code fragment \textit{Square}, in which all variables are typed integer:

\begin{verbatim}
i := 0;
s := 0;
while (i \neq n) do
    s := s + n;
i := i + 1
\end{verbatim}

This code takes an integer \( n \), and is intended to calculate \( n^2 \) and assign that value to \( s \). To confirm this, we wish to use the rules of Hoare Logic (Appendix 3) to show that

\[
\{ \text{True} \} \text{Square} \{ s = n^2 \}.
\]

In the questions below (and your answers), we may refer to the loop code as \textit{Loop}, and the body of the loop as \textit{Body}. \textit{Make sure that every step of your proof is numbered, and is justified by citing the rule, and any previous proof steps, that you are using.}

(a) We will need an invariant for \textit{Loop}. We suggest

\[
\text{Inv} \equiv (s = i \times n).
\]

Prove that

\[
\{ \text{Inv} \} \text{Body} \{ \text{Inv} \}.
\]
(b) Using the result of part (a), prove that

\(\{\text{Inv}\} \text{ Loop } \{s = n^2\}\).

QUESTION 3(b) [3 marks]

(c) Using the result of part (b), prove that

\(\{\text{True}\} \text{ Square } \{s = n^2\}\).

QUESTION 3(c) [3 marks]

(d) The code fragment \textit{Square} would get stuck in an infinite loop for some initial values of \(n\). Explain why it is not necessary to consider this possibility when choosing a precondition for this code.

QUESTION 3(d) [1 mark]
QUESTION 4 [11 marks]

Weakest Precondition Calculus

As with the previous question, we will consider the code fragment *Square*:

\[
\begin{align*}
  i &:= 0; \\
  s &:= 0; \\
  &\text{while } (i \neq n) \\
  &\quad \{ s := s + n; \\
  &\quad \quad i := i + 1 \} \\
\end{align*}
\]

We will use the rules of the weakest precondition calculus (Appendix 4) to calculate \( wp(Square, s = n^2) \).

As in the previous question we will use the abbreviations *Loop* and *Body* for the indicated parts of the code. *Remember to simplify your answers wherever possible, and show all your working when you do so.*

(a) We will need to calculate \( wp(\text{Loop}, s = n^2) \).

First, state \( P_0 \) (the predicate expressing success for this weakest precondition after zero loop iterations).
(b) We claim that the general format for $P_k$ (expressing success after $k$ loop iterations for $k \geq 0$) is

$$ P_k \equiv (i + k = n \land s = i^2 + k \times i) $$

Suppose that this holds for some $k$. Then prove that

$$ P_{k+1} \equiv (i + (k + 1) = n \land s = i^2 + (k + 1) \times i) $$
(c) Given parts (a) and (b), state

\[ wp(\text{Loop}, \ s = n^2). \]

Do not attempt any simplification at this stage.

(d) Hence find

\[ wp(\text{Square}, \ s = n^2). \]

State this result in the simplest form possible.
QUESTION 5 [10 marks]

Separation Logic

Prove the following Separation Logic triples by instantiating $P$ and $Q$ using the appropriate axiom from the Separation Logic rules given in the appendix. As your solution, write out the whole triple on one line. You do not need any other rules of Separation Logic or Hoare Logic. You can use multiple lines if you want to do it piece by piece, but justify each step. Please use an abbreviation which uses the first three letters from each word in the name of the axiom, but ending in Axm as shown in the example. Please use the axioms as they are shown in the Appendix as this will make it easier to mark such questions in the quiz, assignment and exam: that is, do not use re-namings of these axioms.

(a) $\{P\} \ x := \text{cons}(y + x) \ {Q}$

(b) $\{P\} \ dispose(42) \ {Q}$

(c) $\{P\} \ [x - 1] := x + 1 \ {Q}$
(d) \( \{P\} \ x := [x - 1] \ \{Q\} \)

[2 marks]

(e) \( \{P\} \ x := x + x \ \{Q\} \)

[2 marks]
QUESTION 6 [4 marks]

Suppose that we are given some fixed store $St$ which maps $x$ and $y$ to $St(x)$ and $St(y)$, and that these are different locations: that is, $St(x) \neq St(y)$.

Suppose that $dom(Hp1) = St(x)$ and $Hp1(St(x)) = 1$ and $dom(Hp2) = St(y)$ and $Hp2(St(y)) = 2$. That is, each of $Hp1$ and $Hp2$ are singleton heaps, they are disjoint, and $Hp1$ maps the location $St(x)$ to the value 1 and $Hp2$ maps the location $St(y)$ to the value 2.

The notation $Hp1 \cdot Hp2$ means the heap that is formed by combining heaps $Hp1$ and $Hp2$. Let $Hp = (Hp1 \cdot Hp2)$: that is, the heap $Hp$ is the combination of the heaps $Hp1$ and $Hp2$.

For each part, write down all of the heaps from $Hp1$, $Hp2$, $Hp$ that make the condition true, or else write “none” if you think none of these three heaps makes the condition true, and give a reason of two or three lines in plain English.

(a) $x \mapsto 1 \land x \mapsto 1$

(b) $\neg (x \mapsto 1)$
Additional answers. Clearly indicate the corresponding question and part.
Appendix 1 — Natural Deduction Rules

Propositional Calculus

\[ \begin{align*}
(\land I) & \quad \frac{p \quad q}{p \land q} & (\land E) & \quad \frac{p \land q}{p} \quad \frac{p \land q}{q} \\
(\lor I) & \quad \frac{p}{p \lor q} & (\lor E) & \quad \frac{p \lor q}{r} \quad \frac{p \lor q}{r} \\
(\rightarrow I) & \quad \frac{q}{p \rightarrow q} & (\rightarrow E) & \quad \frac{p \quad p \rightarrow q}{q} \\
(\neg I) & \quad \frac{q \land \neg q}{\neg p} & (\neg E) & \quad \frac{q \land \neg q}{p}
\end{align*} \]

Predicate Calculus

\[ \begin{align*}
(\forall I) & \quad \frac{P(a) \quad (a \text{ arbitrary})}{\forall x. P(x)} & (\forall E) & \quad \frac{\forall x. P(x)}{P(a)} \\
(\exists I) & \quad \frac{P(a)}{\exists x. P(x)} & (\exists E) & \quad \frac{\exists x. P(x) \quad q \quad (a \text{ arbitrary})}{q} \quad (a \text{ not free in } q)
\end{align*} \]
Appendix 2 — Truth Table Values

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \lor q$</th>
<th>$p \land q$</th>
<th>$p \rightarrow q$</th>
<th>$\neg p$</th>
<th>$p \leftrightarrow q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>
Appendix 3 — Hoare Logic Rules

- **Precondition Strengthening:**
  \[
  P_s \rightarrow P_w \quad \{P_w\} S \{Q\} \\
  \{P_s\} S \{Q\}
  \]

- **Postcondition Weakening:**
  \[
  \{P\} S \{Q_s\} \quad Q_s \rightarrow Q_w \\
  \{P\} S \{Q_w\}
  \]

- **Assignment:**
  \[
  \{Q(e)\} x := e \quad \{Q(x)\}
  \]

- **Sequence:**
  \[
  \{P\} S_1 \{Q\} \quad \{Q\} S_2 \{R\} \\
  \{P\} S_1; S_2 \{R\}
  \]

- **Conditional:**
  \[
  \{P \land b\} S_1 \{Q\} \quad \{P \land \neg b\} S_2 \{Q\} \\
  \{P\} \text{ if } b \text{ then } S_1 \text{ else } S_2 \{Q\}
  \]

- **While Loop:**
  \[
  \{P \land b\} S \{P\} \\
  \{P\} \text{ while } b \text{ do } S \{P \land \neg b\}
  \]
Appendix 4 — Weakest Precondition Rules

\[
wp(x := e, Q(x)) \equiv Q(e)
\]

\[
wp(S_1; S_2, Q) \equiv wp(S_1, wp(S_2, Q))
\]

\[
wp(\text{if } b \text{ then } S_1 \text{ else } S_2, Q) \equiv (b \rightarrow wp(S_1, Q)) \land (\neg b \rightarrow wp(S_2, Q))
\]

\[
\equiv (b \land wp(S_1, Q)) \lor (\neg b \land wp(S_2, Q))
\]

\(P_k\) is the weakest predicate that must be true before while \(b\) do \(S\) executes, in order for the loop to terminate after exactly \(k\) iterations in a state that satisfies \(Q\).

\[
P_0 \equiv \neg b \land Q
\]

\[
P_{k+1} \equiv b \land wp(S, P_k)
\]

\[
wp(\text{while } b \text{ do } S, Q) \equiv \exists k. (k \geq 0 \land P_k)
\]
Appendix 5: Separation Logic Rules

Floyd Store Axiom for Separation Logic: replaces Hoare (Store) Axiom
\[
\{x = v \land \text{emp}\} \quad x := e \quad \{x = e(v/x) \land \text{emp}\}
\]
where \(v\) is an auxiliary variable which does not occur in \(e\)

Derived Floyd Store Axiom for Separation Logic:
\[
\{\text{emp}\} \quad x := e \quad \{x = e \land \text{emp}\}
\]
where \(x\) does not occur in \(e\)

Fetch Assignment Axiom
\[
\{(x = v_1) \land (e \mapsto v_2)\} \quad x := \llbracket e \rrbracket \quad \{(x = v_2) \land (e(v_1/x) \mapsto v_2)\}
\]
where \(v_1\) and \(v_2\) are auxiliary variables which do not occur in \(e\)

Derived Fetch Assignment Axiom
\[
\{(e \mapsto v_2)\} \quad x := \llbracket e \rrbracket \quad \{(x = v_2) \land (e \mapsto v_2)\}
\]
where \(v_2\) and \(x\) do not occur in \(e\)

Heap Assignment Axiom
\[
\{e \mapsto -\} \quad \llbracket e \rrbracket := e_1 \quad \{e \mapsto e_1\}
\]
where \((e \mapsto -)\) abbreviates \((\exists z. e \mapsto z)\) and \(z\) does not occur in \(e\)

Allocation Assignment Axiom
\[
\{x = v \land \text{emp}\} \quad x := \text{cons}(e_1, e_2, \ldots, e_n) \quad \{x \mapsto e_1(v/x), e_2(v/x), \ldots, e_n(v/x)\}
\]
where \(v\) is an auxiliary variable different from \(x\) and not appearing in \(e_1, e_2, \ldots, e_n\)

Derived Allocation Assignment Axiom
\[
\{\text{emp}\} \quad x := \text{cons}(e_1, e_2, \ldots, e_n) \quad \{x \mapsto e_1, e_2, \ldots, e_n\}
\]
where \(x\) does not appear in \(e_1, e_2, \ldots, e_n\)

Dispose Axiom
\[
\{e \mapsto -\} \quad \text{dispose}(e) \quad \{\text{emp}\}
\]
where \((e \mapsto -)\) abbreviates \((\exists z. e \mapsto z)\) and \(z\) does not occur in \(e\)

The Frame Rule:
\[
\frac{\{P\} S \{Q\}}{\{P \ast R\} S \{Q \ast R\}} \quad \text{where no variable modified by } S \text{ appears free in } R
\]

Other Rules: the Hoare Logic rules from Appendix 3, except the Assignment rule, are also in the calculus for Separation Logic.