THE AUSTRALIAN NATIONAL UNIVERSITY

Mid-Semester Quiz
Second Semester, 2011

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

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	Total Mark

QUESTION 1 [11 marks]

Natural Deduction

(a) Use truth tables to determine whether the following inference is (always) valid or not; if not, give a counterexample (values of p, q, r for which it is not valid).

$$\frac{(p \to q) \lor (q \to r)}{(p \land q) \to r}$$

QUESTION 1(a) **[3 marks]**

p	q	r	$p \to q$	$q \to r$	$(p \to q) \lor (q \to r)$	$p \land q$	$(p \land q) \to r$
T	T	T					
T	T	F					
T	F	T					
T	F	F					
F	T	T					
F	T	F					
F	F	T					
F	F	F					

(b) Give a natural deduction proof of $\frac{(p \to r) \lor (q \to r)}{(p \land q) \to r}$ (may be continued next page)

QUESTION 1(b) **[4 marks]**

QUESTION 1(b), continued

(c) Give a natural deduction proof of $\dfrac{(\exists\, x.\ P(x)) \rightarrow Q}{\forall\, x.\ P(x) \rightarrow Q}$, that is, $\dfrac{(\exists\, x.\ P(x)) \rightarrow Q}{\forall\, x.\ (P(x) \rightarrow Q)}$

(where x does not appear free in Q)

QUESTION 1(c) **[4 marks]**

QUESTION 2 [10 marks]

Structural Induction

Given these function definitons:

```
sum []       = 0                              -- (S1)
sum (x:xs)   = x + sum xs                     -- (S2)

[]     ++ ys  = ys                            -- (A1)
(x:xs) ++ ys  = x : (xs ++ ys)                -- (A2)
```

We would like to prove the following property using structural induction.

```
sum (xs ++ ys) = sum xs + sum ys
```

You may need to include an explicit ∀ in the goals and the inductive hypothesis. If so, in your answers indicate where you need to make use of this.

(i) State and prove the base case goal.

QUESTION 2	**[3 marks]**

(ii) State the induction hypothesis.

QUESTION 2	**[2 marks]**

(iii) State and prove the step case goal.

QUESTION 2 **[5 marks]**

QUESTION 3 [11 marks]

Finite State Machines

(a) Give a Non-deterministic Finite State Automaton (NFA) on the alphabet $\Sigma = \{0, 1\}$ which accepts the language L of even binary numerals written without superfluous leading 0, that is, L consists of non-empty strings which either

- consist of a single 0, or
- start with 1 and end with 0

If possible, find an NFA with only three states.

QUESTION 3(a)	**[3 marks]**

(b) Give a regular expression for the language L.

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

(c) Find a Deterministic Finite State Automaton (DFA) for L. (Hint: this requires five states).

QUESTION 3(c)	**[3 marks]**

(d) Explain why a Deterministic Finite State Automaton for L must have more than one final state.

QUESTION 3(d)	**[3 marks]**

QUESTION 4 [7 marks]

Context-free Languages and Parsing

Consider the following grammar with non-terminal (and start symbol) S, and terminals a, b.

$$S \rightarrow a\ b \qquad\qquad S \rightarrow a\ S\ b$$

(a) Describe the language L generated by this grammar.

QUESTION 4(a)	**[2 marks]**

(b) The PDA derived naturally from this grammar has the following transitions:
With q_0 as start state, and q_2 as final state:

$$\delta(q_0, \epsilon, Z) \mapsto q_1/SZ \qquad \delta(q_1, a, a) \mapsto q_1/\epsilon$$
$$\delta(q_1, \epsilon, Z) \mapsto \underline{q_2}/\epsilon \qquad \delta(q_1, b, b) \mapsto q_1/\epsilon$$

plus two more transitions omitted from the above. What are they?

QUESTION 4(b)	**[1 mark]**

(c) We want to do top-down parsing of the language using this PDA. But allowing one symbol lookahead in the input is not sufficient to make this parser deterministic. Explain why.

QUESTION 4(c)	**[2 marks]**

(d) We can change the grammar, to avoid this problem. Give a grammar such that

- it generates the same language L, and
- looking ahead one symbol of the input *is* sufficient to determine the next transition of the corresponding PDA

Hint: one possible solution has, as one of its productions, $S \to a\ T$.

QUESTION 4(d)	**[2 marks]**

QUESTION 5 [11 marks]

Specification using Z

A technical college has students; they enrol, take courses and, if their collection of completed units satisfies certain rules, they graduate.

The bare bones of the system is captured in the following Z specification.

$[Person]$
$[Unit]$

$Status ::= Incomplete \mid Graduated$

$$
\begin{array}{|l}
preRequisites : Unit \leftrightarrow Unit \\
advancedUnits : \mathbb{P}\, Unit \\
\hline
\forall u : Unit \bullet u \in advancedUnits \Rightarrow \\
\quad \exists p : Unit \bullet (p \mapsto u) \in preRequisites
\end{array}
$$

College

$$
\begin{array}{|l}
status : Person \nrightarrow Status \\
courses : Person \nrightarrow \mathbb{P}\, Unit \\
unitsCompleted : Person \leftrightarrow Unit \\
\hline
\mathrm{dom}\ unitsCompleted \subseteq \mathrm{dom}\ courses \\
\mathrm{dom}\ courses \subseteq \mathrm{dom}\ status \\
\forall p : Person, u : Unit \bullet \\
\quad (p \mapsto u) \in unitsCompleted \Rightarrow \\
\qquad u \in courses(p)
\end{array}
$$

$StudentAdmission_o$

$$
\begin{array}{|l}
\Delta College \\
p? : Person \\
\hline
p? \notin \mathrm{dom}\, status \\
status' = status \cup \{p? \mapsto Incomplete\} \\
courses' = courses \cup \{p? \mapsto \varnothing\} \\
unitsCompleted' = unitsCompleted
\end{array}
$$

$UnitEnrolment_o$

$$
\begin{array}{|l}
\Delta College \\
p? : Person \\
u? : Unit \\
\hline
status(p?) = Incomplete \\
u? \notin courses(p?) \\
\forall c : Unit \bullet ((c \mapsto u?) \in preRequisites) \\
\qquad \Rightarrow ((p? \mapsto c) \in unitsCompleted) \\
status' = status \\
courses' = courses \setminus \{p? \mapsto courses(p?)\} \\
\qquad \cup \{p? \mapsto (courses(p?) \cup \{u?\})\} \\
unitsCompleted' = unitsCompleted
\end{array}
$$

$Graduation_o$

$$
\begin{array}{|l}
\Delta College \\
p? : Person \\
\hline
(p? \mapsto Incomplete) \in status \\
\#(\{p?\} \lhd unitsCompleted) \geq 8 \\
\#(\mathrm{ran}(\{p?\} \lhd unitsCompleted) \\
\qquad \cap advancedUnits) \geq 4 \\
status' = status \setminus (p? \mapsto Incomplete) \\
\qquad \cup (p? \mapsto Graduated) \\
courses' = courses \\
unitsCompleted' = unitsCompleted
\end{array}
$$

(a) Give, in plain English, the constraint on the constant set *advancedUnits*.

QUESTION 5(a)	**[2 marks]**

(b) Describe, in English the global variable (state variable) *unitsCompleted*. How is it different from the state variable *courses*?

QUESTION 5(b)	**[2 marks]**

(c) Give (in English) the preconditions for the operation $UnitEnrolment_o$.

QUESTION 5(c)	**[1 mark]**

(d) Give (in English) the postconditions for the operation $UnitEnrolment_o$.

QUESTION 5(d)	**[2 marks]**

(e) Give (in English) the three preconditions for the operation $Graduation_o$.

QUESTION 5(e)	**[2 marks]**

(f) Write a schema for a query called $Graduates_o$ which has an output variable *graduates*! which will be the set of students who have graduated.

QUESTION 5(f)	**[2 marks]**

Additional answers. Clearly indicate the corresponding question and part.

Additional answers. Clearly indicate the corresponding question and part.

Additional answers. Clearly indicate the corresponding question and part.

Additional answers. Clearly indicate the corresponding question and part.

Appendix 1 — Natural Deduction Rules

Propositional Calculus

$$(\wedge I)\quad \frac{p \qquad q}{p \wedge q} \qquad\qquad (\wedge E)\quad \frac{p \wedge q}{p} \qquad \frac{p \wedge q}{q}$$

$$(\vee I)\quad \frac{p}{p \vee q} \qquad \frac{p}{q \vee p} \qquad\qquad (\vee E)\quad \frac{p \vee q \qquad \begin{matrix}[p]\\ \vdots \\ r\end{matrix} \qquad \begin{matrix}[q]\\ \vdots \\ r\end{matrix}}{r}$$

$$(\to I)\quad \frac{\begin{matrix}[p]\\ \vdots \\ q\end{matrix}}{p \to q} \qquad\qquad (\to E)\quad \frac{p \qquad p \to q}{q}$$

$$(\neg I)\quad \frac{\begin{matrix}[p]\\ \vdots \\ q \wedge \neg q\end{matrix}}{\neg p} \qquad\qquad (\neg E)\quad \frac{\begin{matrix}[\neg p]\\ \vdots \\ q \wedge \neg q\end{matrix}}{p}$$

Predicate Calculus

$$(\forall I)\quad \frac{P(a) \qquad (a \text{ arbitrary})}{\forall x.\ P(x)} \qquad\qquad (\forall E)\quad \frac{\forall x.\ P(x)}{P(a)}$$

$$(\exists I)\quad \frac{P(a)}{\exists x.\ P(x)} \qquad\qquad (\exists E)\quad \frac{\exists x.\ P(x) \qquad \begin{matrix}[P(a)]\\ \vdots \\ q\end{matrix} \qquad (a \text{ arbitrary})}{q \quad (a \text{ is not free in } q)}$$

Appendix 2 — Truth Table Values

p	q	$p \vee q$	$p \wedge q$	$p \rightarrow q$	$\neg p$	$p \leftrightarrow q$
T	T	T	T	T	F	T
T	F	T	F	F	F	F
F	T	T	F	T	T	F
F	F	F	F	T	T	T