PAPER CODE NO. **COMP313**	EXAMINER : Michael Fisher DEPARTMENT : Computer Science Tel. No. 54262

UNIVERSITY OF LIVERPOOL

MAY 2007 EXAMINATIONS

Bachelor of Arts : Year 3
Bachelor of Engineering : Year 3
Bachelor of Science : Year 3
Bachelor of Science : Year 4
No qualification aimed for : Year 1

Formal Methods

TIME ALLOWED : Two and a Half Hours

INSTRUCTIONS TO CANDIDATES

Answer FOUR questions.

If you attempt to answer more questions than the required number of questions (in any section), the marks awarded for the excess questions answered will be discarded (starting with your lowest mark).

1. This question concerns the basic structures used within Z specifications.

(a) What is the representation of the sequence

$$\langle 1, 3, 5, 7, 9 \rangle$$

when given in terms of a function (i.e., as a set of maplets)? **[4 marks]**

(b) If A and B are both sets of the same type, then under what circumstances (if any) will

$$(A \setminus B) = (B \setminus A)$$

be true? Give examples and counter examples to illustrate your answer. **[6 marks]**

(c) If B is a bag of elements from the set $\{w, x, y, z\}$, then what will be the result of each of these expressions?

i. $B \oplus \{x \mapsto 2\}$
ii. $B \uplus \{y \mapsto 3, z \mapsto 1\}$
iii. $B \oplus \{w \mapsto 0\}$ **[9 marks]**

(d) Consider the following sets: $A == \{1, 9\}$, $B == \{1, 3\}$, and $C == \{1, 5, 9\}$.
What is the value of $\#((A \times B) \cap (A \times C))$? **[6 marks]**

2. We wish to specify the relationship between exam marks and students, and already have the following state space schema (N.B., *PERSON* is the set of all people):

$$
\begin{array}{|l}
\hline
\textit{MarkRecord} \\
\textit{students} : \mathbb{P}\,\textit{PERSON} \\
\textit{marks} : \textit{PERSON} \mathrel{+\!\!\!\!\rightarrow} 0 \,..\, 100 \\
\hline
\operatorname{dom} \textit{marks} \subseteq \textit{students} \\
\hline
\end{array}
$$

(a) Write a Z specification for the operation

$$\textit{AddStudent}(\textit{name}? : \textit{PERSON})$$

which adds a new student (i.e. *name*?) to *MarkRecord*, but does not assign the student a mark. **[5 marks]**

(b) Write a Z specification for the operation

$$\textit{AddMark}(\textit{name}? : \textit{PERSON}, \textit{mark}? : 0 \,..\, 100)$$

which assigns the mark (*mark*?) to the student (*name*?) in the *MarkRecord*.**[5 marks]**

(c) Write a Z specification for the operation

$$\textit{CheckMark}(\textit{name}? : \textit{PERSON}, \textit{mark}! : 0 \,..\, 100)$$

which returns the mark (*mark*!) associated with the student (*name*?).

Note: the operation should be undefined if the given student has not already been assigned a mark. **[5 marks]**

(d) Write a Z specification for the operation

$$\textit{Unmarked}(\textit{names}? : \mathbb{P}\,\textit{PERSON})$$

which returns the set of students that have not yet been assigned marks. **[5 marks]**

(e) How would you modify the *CheckMark* operation above so that it is robust (i.e. it will be defined for any student name supplied)? Assume that a *REPORT* type exists for reporting errors. **[5 marks]**

3. This question concerns the fundamentals of Temporal Logic.

(a) What type of structure is typically used to provide a model for propositional, discrete, linear temporal logic, with finite past, and why? **[5 marks]**

(b) Is the following valid, i.e. true in all possible models?

$$\Box\Diamond\varphi \;\Rightarrow\; \Diamond\bigcirc\varphi$$

Justify your answer, either informally or by appealing to the formal semantics. **[7 marks]**

(c) How do *branching* temporal logics differ from linear temporal logics, and what additional operators do they typically provide? **[5 marks]**

(d) We can conjoin together next-formulae such as

$$p \wedge \bigcirc p \wedge \bigcirc\bigcirc p \wedge \bigcirc\bigcirc\bigcirc p \wedge \ldots$$

How many such formulae would we have to conjoin together to give the same behaviour as $\Box p$? **[3 marks]**

(e) Given $\Box(\varphi \Rightarrow \Diamond\psi)$, then if we also know that $\Box\varphi$ is true, how many times will ψ be forced to occur? **[5 marks]**

4. How is temporal logic useful in the formal specification of reactive systems?

Write an essay on this, bringing in as many elements as appropriate, and giving examples where relevant. **[25 marks]**

5. This question concerns the foundations of model checking.

(a) Given a finite state structure, M, represented as a finite-state automaton, and a temporal formula, φ, how would we use the *automata-theoretic* approach to model checking to establish $M \models \varphi$? **[10 marks]**

(b) Describe two problems with the standard model checking approach and explain what techniques are being developed to tackle these. **[10 marks]**

(c) If the model checking process fails then what information is returned? What does this say about the execution of the system being modelled? **[5 marks]**

6. Consider the following Promela code.

```
proctype G (chan out)
{
         int num;
         num = 0;
G1:      num = ((num*2)+1);
         out!num;
         if
         :: (num < 20) -> goto G1;
         :: (num >= 20) -> goto G2;
         fi
G2:      num = num -1;
         out!num;
         if
         :: (num > 0) -> goto G2;
         fi }

proctype S (chan in, outB, outL)
{
         int num;
S1:      in?num;
         if
         :: (num <= 10) -> outL!num; goto S1;
         :: (num > 10) -> outB!num; goto S1;
         fi }

proctype B (chan in)
{
         int num;
B1:      in?num;
         assert(num > XXX);
         goto B1 }

proctype L (chan in)
{
         int num;
L1:      in?num;
         assert(num <= XXX);
         goto L1 }

init {   chan g2s = [0] of { int };
         chan s2b = [0] of { int };
         chan s2l = [0] of { int };
         atomic { run G(g2s); run S(g2s, s2b, s2l);
                  run B(s2b); run L(s2l) }
     }
```

(a) What is the communication structure between the four processes G, S, B, and L, i.e. which channels link the processes and in which direction does information flow between them? **[6 marks]**

(b) What is the sequence of numbers generated and sent down the out channel in process G? **[6 marks]**

(c) In order for the assertions in processes B and L to succeed, which single integer should be used in place of 'XXX' in both processes? Explain your answer.**[6 marks]**

(d) If we wanted to verify that all the numbers seen by process B were bigger than any of the numbers seen by process L, how might we do this? What additional aspects might we add to the program and what temporal formula would we check?**[7 marks]**