PRIFYSGOL CYMRU; UNIVERSITY OF WALES

M.Sc. AND DIPLOMA EXAMINATIONS

JANUARY 2003

SWANSEA

Computer Science

CS M23 Formal Methods for System Reliability

Attempt 2 questions out of 3

Time allowed: 2 hours

Students are permitted to use the dictionaries provided by the University

Students are NOT permitted to use calculators

CS_M23
FORMAL METHODS FOR SYSTEM RELIABILITY
(*Attempt 2 questions out of 3*)

Question 1

(a) The ringmaster of a circus needs to decide which acts will perform in the next performance. He is constrained by the following.

(1) Either the human cannonball or the clowns must perform, as both these acts draw big crowds.

(2) If either the knife thrower or the elephants perform, there won't be time for the trapeze artists to set up and perform.

(3) Either the elephants or the dogs must perform, as there must be at least one animal act for the children in the audience.

(4) If the trapeze artists do not perform, the clowns cannot perform, as the clown act is tied into the trapeze act.

(5) The human cannonball broke his arm in rehearsal and cannot perform.

Let H, C, K, E, T and D denote the following propositions:

H = the human cannonball will perform;

C = the clowns will perform;

K = the knife thrower will perform;

E = the elephants will perform;

T = the trapeze artists will perform;

D = the dogs will perform.

(i) Interpret what the above five conditions say about who will perform as symbolic terms using $\neg$, $\vee$, $\wedge$, $\rightarrow$ and $\leftrightarrow$ (as well as the propositional variables H, C, K, E, T and D). **[5 marks]**

(ii) Write down as symbolic terms the negation of each of the conditions from part (i); do this in such a way that negation $\neg$ is applied only to the propositional variables.

Express each of these as English sentences.

[10 marks]

(iii) Which acts will perform? You can explain your answer informally (in English), but for full marks you must present your reasoning carefully using logical rules.

[5 marks]

(Please turn over.)

(b) Construct a truth table to determine if $(P \leftrightarrow Q) \leftrightarrow R$ is equivalent to $P \leftrightarrow (Q \leftrightarrow R)$, that is, if the operator $\leftrightarrow$ is associative. If $\leftrightarrow$ is associative, then say so; otherwise, indicate in which instances the two formulas give different results.

Your truth table should look as follows.

P	Q	R	$P \leftrightarrow Q$	$Q \leftrightarrow R$	$(P \leftrightarrow Q) \leftrightarrow R$	$P \leftrightarrow (Q \leftrightarrow R)$
F	F	F	.	.	.	.
F	F	T	.	.	.	.
F	T	F	.	.	.	.
F	T	T	.	.	.	.
T	F	F	.	.	.	.
T	F	T	.	.	.	.
T	T	F	.	.	.	.
T	T	T	.	.	.	.

[5 marks]

Question 2

Consider the following process definition.

$$X_1 \stackrel{\text{def}}{=} a.X_1 + b.X_3 \qquad X_4 \stackrel{\text{def}}{=} a.X_4 + b.X_3$$

$$X_2 \stackrel{\text{def}}{=} a.X_3 + a.X_6 + b.X_1 \qquad X_5 \stackrel{\text{def}}{=} a.X_3 + a.X_6 + b.X_1$$

$$X_3 \stackrel{\text{def}}{=} a.X_5 \qquad X_6 \stackrel{\text{def}}{=} a.X_3 + a.X_5 + b.X_4$$

(a) Draw the labelled transition system for the above process.

How many states, actions, and transitions does it have?

[4 marks]

(b) What is a bisimulation colouring?

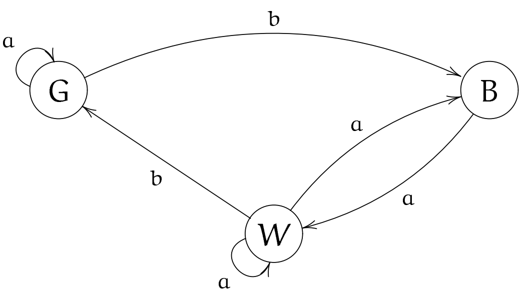
[3 marks]

(c) Carry out the bisimulation colouring algorithm step-by-step.

Explain the steps of the algorithm as you do.

[5 marks]

(d) The following labelled transition system represents the minimal process equivalent to the above process.



Explain in what sense this is true, and how this minimized transition system can be gotten from the above bisimulation colouring algorithm

[4 marks]

(e) Give a process definition for this minimized transition system.

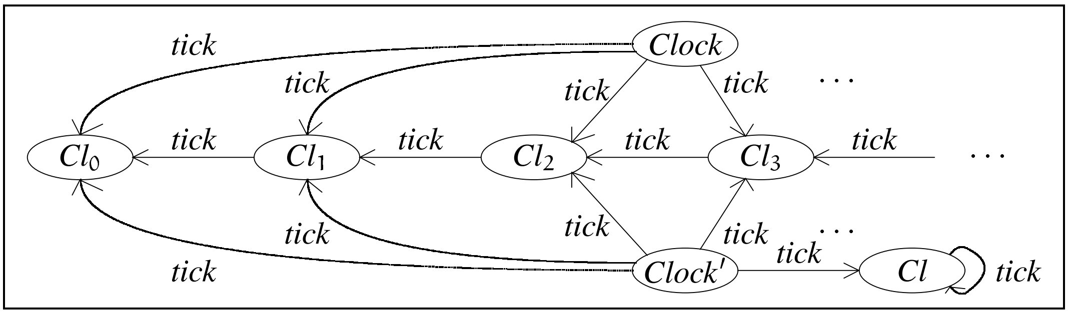
[3 marks]

(f) For each state of the minimized transition system, give a modal formula which is true of it but of no other state in the automaton.

[6 marks]

Question 3

(a) Recall the following clock processes.



(i) Explain why $Clock \sim_n Clock'$ for every $n \in \mathbb{N}$. That is, explain how the second player (Bob) can win any bisimulation game of any length $n \in \mathbb{N}$ which starts with the tokens on *Clock* and *Clock'*.

[4 marks]

(ii) Explain why $Clock \not\sim Clock'$.

[4 marks]

(iii) Explain why no formula of the modal logic M can distinguish between *Clock* and *Clock'*.

[4 marks]

(iv) Prove, by induction on n, that for all $n \in \mathbb{N}$ $Cl_n \sim_n Cl_{n+1}$.

[5 marks]

(b) Consider the following two statements about a computer:

(i) "The computer consists of three parts: a CPU, a memory unit, and a bus for communication with the environment."

(ii) "The emergency button can be pushed; this will halt the computer, which will then not do anything further."

One of these statements can be expressed in the modal logic M; do so.

[4 marks]

The other statement cannot be formalised in M; explain why not.

[4 marks]