PRIFYSGOL CYMRU; UNIVERSITY OF WALES

M.Sc. AND DIPLOMA EXAMINATIONS

May/June 2002

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) Each of the following has one correct answer; indicate the correct answer in each case.

(i) The statement "A if not B" can be written as

- $A \rightarrow \neg B$.
- $\neg B \rightarrow A$.
- $\neg B \vee A$.

(ii) The logical statement "$\neg A \wedge B$" can be read as

- B but not A.
- neither A nor B.
- if A then B.

(iii) If C denotes the statement "The water is clear" and S denotes the statement "The water is safe," then which of the following means "The water is safe if it is clear"?

- $C \rightarrow S$.
- $S \rightarrow C$.
- $C \leftrightarrow S$.

(iv) If D denotes the statement "Donald is a duck" and S denotes the statement "All ducks swim," then which of the following implies that "Donald swims"?

- $D \vee S$.
- $D \rightarrow S$.
- $D \wedge S$.

(v) If $P \rightarrow Q$ is false, then

- P and Q must both be false.
- P may be false.
- P must be true.

[5 marks]

(b) Construct a truth table to determine if $(P \to Q) \to R$ is equivalent to $P \to (Q \to R)$, that is, if the operator $\to$ is associative. If $\to$ 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	$P \to Q$	$Q \to R$	$(P \to Q) \to R$	$P \to (Q \to R)$
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]

(c) Consider the following scenario.

> *Alice, Betty and Carla were planning on going to a party. However, the day before the party, two of the womem had an argument, and the following situation resulted:*
>
> *(1) Carla would not go if Alice went.*
> *(2) Betty would go only if Alice went.*
> *(3) Carla would not go alone.*

Let A, B and C denote the propositions "Alice went to the party," "Betty went to the party," and "Carla went to the party," respectively.

(i) Interpret what the above three conditions say about who went to the party as symbolic terms using $\neg$, $\vee$, $\wedge$, $\to$ and $\leftrightarrow$ (as well as the propositions A, B and C).

[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 A, B and C.

Express each of these as English sentences.

[5 marks]

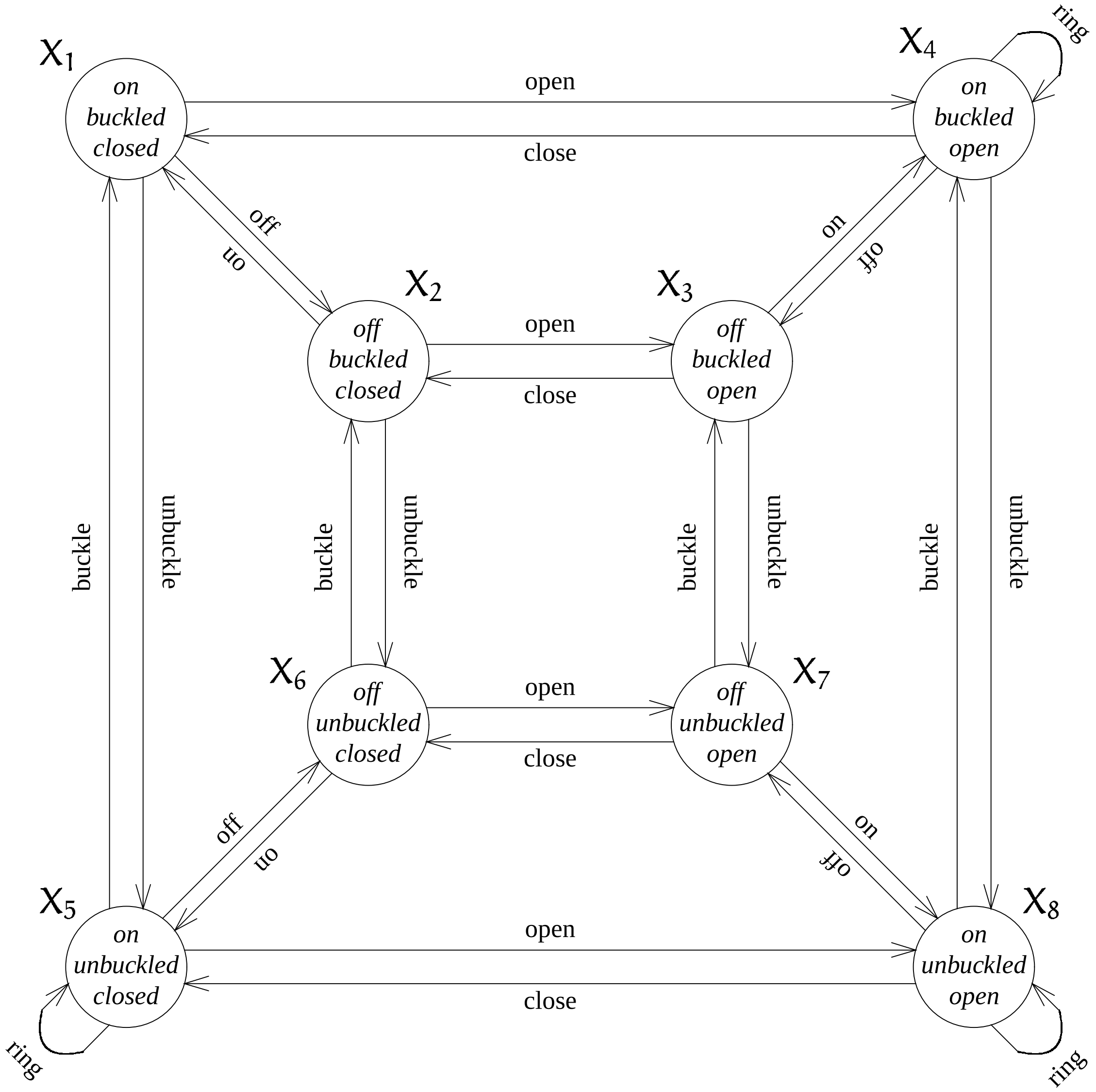
(iii) Did Carla go to the party? You can explain your answer informally (in English), but for full marks you must present your reasoning carefully using logical rules.

[5 marks]

Question 2

In this question, we study the specification of a car safety system, in which a bell rings (repeatedly) whenever the motor is on while the door is open or the seatbelt is unbuckled.

The labelled transition system for this specification may be pictured as follows. In the picture we include within each state X_i the actual state of the motor (*on* or *off*), the seatbelt (*buckled* or *unbuckled*), and the door (*open* or *closed*).



Here we have a system with

- eight states $S = \left\{ X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8 \right\}$, and
- seven actions $A = \left\{ \text{open, close, buckle, unbuckle, on, off, ring} \right\}$.

For example, in state X_4, the motor is on, the seatbelt is buckled, the door is open, and the alarm is ringing.

(a) The eight states in S can be given process definitions, such as

$$X_1 \overset{\text{def}}{=} \text{off}.X_2 \;+\; \text{open}.X_4 \;+\; \text{unbuckle}.X_5$$

Give such a definition for each of the state variables in S.

[4 marks]

(b) Let $D(x)$, $S(x)$, $M(x)$ and $B(x)$ be predicates defined over the states S as follows:

$$\begin{aligned} D(x) &= \text{“the door is open in state } x\text{.”} \\ S(x) &= \text{“the seatbelt is buckled in state } x\text{.”} \\ M(x) &= \text{“the motor is on in state } x\text{.”} \\ B(x) &= \text{“the bell is ringing in state } x\text{.”} \end{aligned}$$

For each of these four predicates, indicate which states satisfy it.

[4 marks]

(c) Express $B(x)$ in the modal logic M in two ways:

(i) one way involving only the action “ring”; and

(ii) another way *not* involving the action “ring”.
(Hint: First express $B(x)$ in terms of $D(x)$, $S(x)$ and $M(x)$.)

[5 marks]

(d) Which states satisfy the following formulas?

(i) $\langle \text{buckle} \rangle \mathit{true} \;\wedge\; \langle \text{close} \rangle \mathit{true}$

(ii) $\langle \text{buckle} \rangle \mathit{true} \;\wedge\; [\text{close}] \mathit{false}$

(iii) $\langle \text{on} \rangle \langle \text{ring} \rangle \mathit{true}$

(iv) $[\text{on}] \langle \text{ring} \rangle \mathit{true}$

(v) $\langle \text{open} \rangle \Big(\langle \text{buckle} \rangle \mathit{true} \;\wedge\; \langle \text{off} \rangle \mathit{true} \Big)$

(vi) $\langle \text{open} \rangle \Big(\langle \text{buckle} \rangle \mathit{true} \;\vee\; \langle \text{off} \rangle \mathit{true} \Big)$

[12 marks]

Question 3

In this question you are to design a candy vending machine which behaves as follows:

1. It accepts (only) 10p and 20p coins.
2. It sells both big candies (for 20p) and little candies (for 10 p).
3. It will allow you to press the “little” candy button if you have inserted (at least) 10p; and to press the “big” candy button if you have inserted (at least) 20p.
4. It will allow you to press the “change” button at any time, and will then return the relevant amount of money to you, as a sequence of 20p coins, terminated if necessary by a single 10p coin.
5. It will never hold more than 30p in credit; if you insert too much money, it will return the coin you most recently inserted.
6. It will allow any sequence of actions which is consistent with the above.

You should not model anything which is not specifically detailed above. For example, do not model a “‘collect” candy event (the machine can be assumed to drop the candy on the floor).

(a) Give a definition of your machine in the language of process expressions.

[8 marks]

(b) Draw your process as a labelled transition system.

[7 marks]

(c) Express each of the following properties in the modal logic $\mathcal{M}$. In each case, state whether or not the property is true of your vending machine, and give a clear justification. If you suspect any ambiguity in any of the statements, then explain these ambiguities, and express any and all properties which you consider to be valid interpretations.

   (i) After inserting two 20p coins, I may get a 20p coin returned to me.

   (ii) After inserting a 10p coin and a 20p coin, in either order, I must either press the “big” candy button or press the “little” candy button.

   (iii) I may insert a 10p coin and get into a state in which I may then either press the “big” candy button or press the “little” candy button.

[10 marks]