PRIFYSGOL CYMRU; UNIVERSITY OF WALES

DEGREE EXAMINATIONS MAY/JUNE 2003

SWANSEA

Computer Science

CS 411 Critical Systems

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_411
CRITICAL SYSTEMS

(*Attempt* **2** *questions out of 3*)

Question 1.

(a) Define briefly the notions safety critical system, business critical system and mission critical system.

[3 marks]

(b) The fire doors in the department of Computer Science in Swansea are kept open by electromagnets. If a fire alarm is activated, the electromagnets are switched off, and the doors are closed. In order to save energy, it was suggested to modify this mechanism, so that the doors are closed when the electromagnets are switched on, and otherwise are kept open. What would be the disadvantage of such a change?

[3 marks]

(c) Give a fault tree analysis of the system of brakes of a bicycle. You can assume that the system consists of two independent brakes, and that under normal circumstances, the failure of one brake will not cause an accident. Start with the failure of both brakes. Consider as causes for the failure of an individual brake that the cable connecting the handle with the brake is broken or that the brake shoe (the rubber part in contact with the wheel) has fallen off. Your fault tree analysis should contain at least one or-gate and one and-gate.

[5 marks]

(d) Assume two versions of a telephone exchange server. Version A fails on average once per calendar month (30 days) for 1 second, version B fails once per year (365 days) for 1 minute. Determine the availability of both systems. It suffices to write down your result as a formula. Which of the two systems is more available and which is more reliable? Explain your result.

[8 marks]

(e) Determine 3 advantages and 3 disadvantages for the use of Java as a language for writing safety-critical software.

[6 marks]

Question 2.

(a) In type theory, one uses dependent types in order to express properties of a system expressible by a formula. Why can the same not be done in Haskell, which has only non-dependent types? Indicate how to express the formulae $\forall x : \mathrm{N}.A(x)$ and $B \wedge C$ as types in dependent type theory, provided this has been done already for the formulae $A(x)$, B and C.

[7 marks]

In the following, consider the situation of a pedestrian crossing, controlled by traffic lights and pedestrian lights. For simplicity we assume that both the traffic and the pedestrian lights have only two states, red, meaning that the vehicles or pedestrians have to wait, and green, meaning that they can proceed. All traffic lights controlling the road traffic will have at any time the same state. The same applies to all pedestrian lights. The goal is to model this system in such a way, that it is never allowed for both the pedestrians to cross the street and the vehicles to proceed at the same time.

(b) Introduce in Agda the set of states of the traffic/pedestrian lights, and the set of states of the complete system.

[4 marks]

(c) Introduce in Agda a predicate expressing that the system is safe, i.e. that it is not the case that both the pedestrian and the traffic lights are green.

[4 marks]

(d) Introduce in Agda a set of control states representing all possible states in which the system is safe and compute for each control state the corresponding state of the system.

[7 marks]

(e) What would one have to show in order to guarantee that each control state is safe? You don't have to carry out this proof.

[3 marks]

Question 3.

(a) For each type construction in dependent type theory there are four groups of rules. Name each of these groups and explain briefly what they are used for.

[6 marks]

(b) Prove using the rules of dependent type theory the following judgement:

$$A : \mathrm{Set}, f : A \to A, a : A \Rightarrow f\ a : A \ .$$

[7 marks]

(c) Introduce in Agda the set N of natural numbers and for $n, m : \mathrm{N}$ the relations $\mathrm{Eq}\ n\ m$, expressing that n and m are equal and the relation $\mathrm{LessEq}\ n\ m$ expressing that $n \leq m$ holds. Both $\mathrm{Eq}\ n\ m$ and $\mathrm{LessEq}\ n\ m$ should be sets.

[6 marks]

(d) Show in Agda that the relation LessEq introduced in (b) is antisymmetric, i.e. that $\mathrm{LessEq}\ n\ m$ and $\mathrm{LessEq}\ m\ n$ implies $\mathrm{Eq}\ n\ m$.

[6 marks]