UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2001

BEng Honours Degree in Computing Part III
BSc Honours Degree in Mathematics and Computer Science Part III
MSci Honours Degree in Mathematics and Computer Science Part III
MSc in Advanced Computing
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the Associateship of the City and Guilds of London Institute
This paper is also taken for the relevant examinations for the Associateship of the Royal College of Science

PAPER C378

MATHEMATICAL STRUCTURES IN COMPUTER SCIENCE

Friday 4 May 2001, 14:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators not required

1a Define the term *monotonic* as applied to a function $f:P \to Q$, where P,Q are posets.

A function $g: P \to Q$ will be called *antitone* (i.e. order-reversing) if

$$x \leq y \quad \text{implies} \quad g(y) \leq g(x).$$

Given that D is a poset with at least two elements, state with reasons which, if any, of the following statements is necessarily true (all functions mentioned are of type $D \to D$):

i) if f and $f \circ g$ are monotonic, then g is monotonic

ii) there is at least one function which is both monotonic and antitone

iii) there is at least one function which is *not* both monotonic and antitone.

b i) What is a *homomorphism* of lattices?

ii) Determine how many distinct homomorphisms there are from the lattice of subsets of {a,b} to the two element lattice {0,1}.

iii) Prove or disprove the folowing: for any surjective (onto) homomorphism $h:L \to M$ of lattices, where L has the least element 0, h(0) is the least element of M.

c Define the terms *distributive* (as applied to a lattice) and *Boolean algebra*..

Let B be the Boolean algebra of subsets of {a,b,c}. Show that there are just five distinct Boolean subalgebras of B. (Hint: observe that if a subalgebra contains any two of {a},{b},{c}, then it must be equal to B.) Deduce that the lattice of subalgebras of a Boolean algebra is not necessarily distributive.

2a i) Let Act be the alphabet $\{1,2,3\}$, and $S = \{0,1,..,4\}$ the set of states of a "finite automaton", with next-state function δ: Act $\times$ S $\rightarrow$ S given by

$$\delta(a, \sigma) = (a \times \sigma) \bmod 5$$

(for example, $\delta(3,2) = 6 \bmod 5 = 1$). Let δ^*: Act* $\rightarrow$ [S $\rightarrow$ S] be the usual (transition function) extension of δ to strings of inputs.
Determine $\delta^*(23)$ and $\delta^*(31)$ as maps from S to S. (*Note* : the arguments of δ^* here are strings, not decimal numbers.)
Show that $\delta^*(x)$ is a bijection for any $x \in$ Act*

ii) State the Initial Algebra Theorem for term algebras. State also (very briefly) how the Theorem is relevant to semantics.
The transition function δ^* of a finite automaton may be considered as the "semantics" of the automaton; does this provide an illustration of the Theorem's relevance (to semantics)? Explain.

b i) Define *left inverse* and *inverse*, as applied to elements of a monoid (M,° ,e).

ii) Suppose that the monoid M has (exactly) three elements e,a,b, and that a is a left inverse of b. Prove that M is commutative.

iii) Let Rel be the monoid of binary relations over $\mathbb{N}$, with relational composition as the monoid product. What is the unit of Rel? Find an element of Rel which has a right inverse but no left inverse.

3a What is a *linear code*? What is the *dual* of a linear code?
A subset C of a vector space is cyclic if, for all $(x_1,...,x_n) \in C$, $(x_n,x_1,...,x_{n-1}) \in C$. Prove that if C is a cyclic linear code, then its dual code is cyclic.

b i) Find a 2-dimensional 1-error correcting linear code in the vector space V(5,3). What is the coset of your code that contains the word (2,2,0,0,0)? Does this code have a unique leader, and if so, what is it?

ii) What is a *parity check matrix* of a linear code? What is the *syndrome* of a word with respect to a parity check matrix? Suppose we have stored in a computer a linear code, a parity check matrix for this code, and a list of unique leaders (if they exist) of cosets of the code. Write a simple, efficient decoding algorithm that uses this information and does not rely upon storage of cosets.

c What is a Hamming code? List all the 1-dimensional linear codes in the vector space V(2,3) and, using this list, write down a parity check matrix for the Hamming code H(2,3). In what vector space is H(2,3) a code, and how many codewords does H(2,3) contain?

The three parts carry, respectively, 25%, 50% ,25% of the marks.

4a i) Define *initial* and *terminal*, as applied to objects of a category.

ii) Recall that any (pre-)ordered set may be considered as a category. Let BS be the set of binary strings, taken with the prefix (or left factor) ordering. Describe BS as a category (by specifying its objects and morphisms, and the composition of morphisms), and identify any initial or terminal objects which this category may have.

iii) Two objects A,B of a category **C** are said to be *isomorphic* if there exist morphisms $p:A \to B$, $q:B \to A$ such that $p;q = Id_A$ and $q;p = Id_B$. Show that if **C** has the initial object I and the terminal object T, and there is a morphism from T to I, then T and I are isomorphic.

b Recall that a *finite projective plane* is a finite set S of *points* together with a set L of subsets of S, called *lines* , that satisfy the axioms:

1. For any two distinct points there exists a unique line that contains them;
2. For any two lines there exists a point that lies in both;
3. Any line contains at least three points; there exist at least two lines.

i) Taking care to state at which point in a proof you are using which axiom, prove: for any two distinct lines there is exactly one point that lies in both.

Any finite projective plane has the property that each of its lines contains the same number of points; the *order* of the plane $\wp$ is the number q such that each line contains $q + 1$ points. Prove that, if $\wp$ has order q, then:

ii) For any point P there exist $q + 1$ distinct lines that contain P.

iii) The number of points in $\wp$ is $q^2 + q + 1$.

The two parts carry, respectively, 35%, 65% of the marks.