UNIVERSITY OF LONDON

IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 1996

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

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

PAPER 3.78 / 4.78

MATHEMATICAL STRUCTURES IN COMPUTING SCIENCE

Tuesday, May 14th 1996, 3.00 - 5.00

Answer THREE questions

For admin. only: paper contains
4 questions
4 pages (excluding cover page)

Section A *(Use a separate answer book for this Section)*

1a i) Define the terms *lower bound, greatest lower bound* (glb), as applied to a subset S of a poset (partially ordered set) P. Prove that, if $x,y \in P$, then $x \leq y$ if and only if x is the glb of $\{x,y\}$.

ii) Define the term *lattice* (notions concerning partial order can be presupposed). Prove that, if L is a lattice with a greatest element 1, then every finite subset of L has a glb.

b What is a *homomorphism* of lattices? (Do not assume that a homomorphism preserves 0 or 1.)

i) How many distinct homomorphisms are there from the lattice of subsets of $\{0,1\}$ to the two-element lattice $\{0,1\}$? (Explain your calculation.)

ii) Prove or disprove the following: for any surjective (onto) homomorphism $h{:}L \rightarrow M$ 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 a *weak negation* on a lattice L be defined as a unary operation $\sim$ on L such that

$$x \leq {\sim}y \quad \Leftrightarrow \quad y \leq {\sim}x \quad \text{(for all } x,y \in L).$$

Show that a distributive lattice, in which a weak negation is defined, need not be a Boolean algebra.

2a i) Briefly state Kruskal's Algorithm for finding a minimal cost spanning tree of a connected graph. Give an example of a graph (having at least five edges and two cycles) to illustrate the working of the algorithm.

ii) Define the term *matroid,* and explain how the edge-sets of a graph give rise to a matroid. (No proofs are required.)

iii) In what way is the matroid of edge-sets relevant to the validity of Kruskal's Algorithm? Refer as appropriate to your example in part i).

b 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 $\delta\colon \mathrm{Act} \times S \to S$ given by

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

(for example, $\delta(3,2) = 6 \bmod 5 = 1$). Let $\delta^*\colon \mathrm{Act}^* \to [S \to S]$ be the usual (transition function) extension of δ to strings of inputs.
Determine $\delta^*(23)$ and $\delta^*(33)$ as maps from S to S. (*Note* : the arguments of δ^* here are strings, not decimal numbers.)
Show that $\delta^*(\sigma)$ is always a bijection.

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.

The two parts carry, respectively, 60%, 40% of the marks.

Turn over ...

Section B *(Use a separate answer book for this Section)*

3a Let M be a monoid, and U a subset of it.

i) Give a definition of the submonoid (M', say) of M *generated by U.* Prove that this is indeed a submonoid of M.

ii) From your definition, prove that for any submonoid N of M, $M \subseteq N$ if and only if $U \subseteq N$.

b Let X be a set, and let M be the monoid $(X^*)^3$ (the corresponding Miranda notation would be ([X], [X], [X])).

We define *Merge* to be the submonoid of M generated by the set

$$U = \{([x], [], [x]) : x \in X\} \cup \{([], [x], [x]) : x \in X\}$$

(Intuitively, (xs,ys,zs) $\in$ Merge if zs can be made by interleaving the elements of xs with those of ys.)

i) If X is the set of natural numbers, show that

$$([1, 3], [53, 53, 49], [53, 1, 53, 49, 3]) \in \text{Merge}$$

ii) Show that if (xs, ys, zs) $\in$ Merge, then #zs = #xs+#ys, where #xs is the length of xs. (Hint: consider the set N of triples (xs, ys, zs) such that #zs = #xs+#ys.)

iii) Deduce that if (xs, ys, []) $\in$ Merge, then xs = ys = [].

iv) Show that if (xs, ys, z:zs) $\in$ Merge, then either xs = z:xs' with (xs', ys, zs) $\in$ Merge, or ys = z:ys' with (xs, ys', zs) $\in$ Merge.

The two parts carry, respectively, 30%, 70% of the marks.

4a If P is a poset (equipped with a partial order $\leq$), there is a natural way of considering it as a category F(P), in which the objects are the elements of P and the morphisms are the instances of the $\leq$ relation (so if $x \leq y$, then the pair (x,y) is a morphism from x to y).

i) Define the identity morphisms and composition in F(P). Why are the unit and associativity laws trivial in this case?

ii) If x and y are elements of P, show that $x \cong y$ in F(P) (i.e. x and y are isomorphic) iff $x = y$.

iii) Suppose C is a category, and H, H': $C \to F(P)$ are functors. Show that if H and H' agree on all objects then they are equal.

iv) Describe how to extend F to a functor (also written F) from **Pos** to **Cat**. (**Pos** is the category whose objects are posets and whose morphisms are monotone functions; **Cat** is the category whose objects are categories and whose morphisms are functors.)

b A *preorder* is a set P equipped with a binary relation $\leq$ that is reflexive and transitive: in other words, it is just like a poset except that the antisymmetry law may fail. The construction of part a can also be applied to preorders, giving a functor F: **Preo** $\to$ **Cat** where in **Preo** the objects are preorders, the morphisms are monotone functions. Property a iii) will still hold for the preorders, but a ii) will not in general.

If C is a category, we define G(C) = obj(C), and define a relation $\leq$ on G(C) by $X \leq Y$ iff $C(X,Y) \neq \emptyset$.

i) Show that $\leq$ is a preorder on G(C). Why is it not a partial order in general?

ii) Show that if C is any category and P is any preorder, then monotone functions from G(C) to P are equivalent to functors from C to F(P).

The two parts carry, respectively, 60%, 40% of the marks.

End of paper