UNIVERSITY OF LONDON

IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 1996

MEng Honours Degrees in Computing Part IV
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

PAPER 4.38

COMPLEXITY

Friday, May 3rd 1996, 2.00 - 4.00

Answer THREE questions

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

1a Give a program for an input/output multi-tape Turing machine (TM) which takes any string $w \in \{0,1\}^*$ of length n and repeats each character to produce a string of twice the length, so that e.g. 010111 is turned into 001100111111.
Explain any notation you use in your description of the program. Remember that the input tape is read-only and the output tape is write-only.

How much time and space does your TM use as a function of n?

b Outline how the same task as in (a) could be carried out by a single tape TM (there is no need actually to write the program). Obtain an estimate for the amount of time this TM takes.

c Sketch a proof that a k-tape TM ($k \geq 2$) running in time f(n) can be simulated by a 1-tape TM running in time $O((f(n))^2)$.

2a Give definitions for the following:

i) a *language*

ii) polynomial time *reduction* $\leq$

iii) the complexity class P

b Define the *Hamiltonian Path Problem* (HP) and the decision version of the *Travelling Salesman Problem* (TSP(D)), and explain why HP $\leq$ TSP(D).

c The graph isomorphism problem (ISOM) is: given two graphs G_1 and G_2, are they isomorphic? The graph automorphism problem (AUTO) is: given a graph G, does G have a non-trivial automorphism, i.e. is there an isomorphism between G and itself which is not the identity map?

Suppose that ISOM is in P. Show that, if that were the case, then AUTO would also be in P.

The three parts carry, respectively, 30%, 30%, 40% of the marks.

© University of London 1996

3a State the reachability problem for directed graphs RCH, and show that RCH is in the nondeterministic logspace class NL.

b Describe a Boolean circuit C_n which takes inputs of length n and returns true if all the inputs have the same value (i.e. they are all 0 or all 1) and false otherwise. You should aim to keep the depth of C_n as low as possible.

Find the depth and size of your C_n.

c i) What is the Parallel Computation Thesis?

ii) Define the class NC_2.

iii) Sketch a proof that $NL \subseteq NC_2$. You may assume that RCH belongs to NC_2.

4a i) What is meant by a Monte Carlo Turing machine for a language L? Define the class RP.

ii) Show that RP is closed under intersection (i.e. if $L_1, L_2 \in RP$ then $L_1 \cap L_2 \in RP$).

b Explain briefly why the problem of determining whether a natural number is prime (PRIME) is in co-NP

c We are given a system of encryption in which encoding e is deterministic, one-one, and can be done in polynomial time. Show that the following problem is in NP$\cap$co-NP: given some cryptotext c and a word w, does w occur as a substring of the plaintext corresponding to c?

The three parts carry, respectively, 50%, 15%, 35% of the marks.

End of paper

© University of London 1996