UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2000

MEng Honours Degree in Mathematics and Computer Science Part IV
MEng Honours Degrees in Computing Part IV
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 C438

COMPLEXITY

Thursday 11 May 2000, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions

1a Let L, L_1, L_2 be languages.

i) What does it mean for L_1 to be *p-time reducible* to L_2 ($L_1 \leq L_2$)?

ii) What does it mean for L to be *NP-complete*?

iii) Outline in general terms how to show that a problem is NP-complete using the fact that other problems are already known to be NP-complete.

b Describe four NP-complete problems. Your chosen four should include at least one problem from each of the three areas of graphs, logic and combinatorics/ operations research. You should not include the Travelling Salesman Problem.

c i) Show that TSP(D), the decision version of the Travelling Salesman Problem, is NP-complete, assuming the NP-completeness of one of the problems you described in answer to (b) above.

ii) The Figure of Eight (F8) problem is as follows: Given an undirected graph G, can G be traversed in a figure of eight, so that every node is visited exactly once, apart from a single node which is visited twice (the crossover point of the figure of eight).

Show that F8 is NP-complete, assuming the NP-completeness of one of the problems you described in answer to (b) above.

The three parts carry, respectively, 30%, 20%, 50% of the marks.

2a i) Define LOGSPACE and NLOGSPACE (henceforth abbreviated to L and NL respectively), being careful about space usage.

ii) State (without proof) Savitch's Theorem.

b The problem EO is as follows: Given an undirected graph G, is every even node of G connected to at least one odd node? (The *degree* of a node is the number of nodes adjacent to it. A node is *even* if it has even degree, *odd* if it has odd degree.)

Give an informal argument that EO is in L.

c The problem EP is as follows: Given a directed graph G with n nodes, and two nodes x and y of G, is there an even path from x to y of length less than n? (Here an *even* path is a path of even length.)

Give an informal argument that EP is in NL.

d The problem APE is as follows: Given a directed graph G with n nodes, and two nodes x and y of G, are all paths from x to y of length less than n (if any exist) even?

Show that APE is in NL. State (without proof) any theorems you need.

The four parts carry, respectively, 30%, 25%, 20%, 25% of the marks.

3a What is a *primality certificate* (in the sense of Pratt)? Illustrate with an example. Explain the significance of primality certificates for the complexity of the problem PRIME (given a number, is it prime?).

b i) What is a *Fermat witness* to the compositeness of a number? Give an illustrative example, with brief justification.

ii) Briefly explain why the truth of the extended Riemann hypothesis (ERH) would imply that PRIME $\in$ P. Explain why nonetheless the truth of ERH is of limited significance for practical primality testing.

c In the RSA public-key cryptosystem,

i) what form do the public and private keys take, how do the parties encrypt and decrypt messages, and why does decryption invert encryption?

ii) how could a fast (P-time) algorithm to factorise the product of two primes be used to compromise the system?

iii) what problems arise when the system is used to encrypt short (one-bit) messages, and what practical solution can be offered?

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

4a i) Define the classes RP and ZPP of languages $\subseteq \{0,1\}^*$.

ii) Let $L \subseteq \{0,1\}^*$ be a language and M a P-time precise Turing machine such that for any $w \in \{0,1\}^*$ of length n,

- if $w \in L$ and there are N computations of M on w, at least $N(1-2^{-1/n})$ of them are accepting,
- if $w \notin L$ then all computations of M on w are rejecting.

Show that $L \in$ RP.

b i) Outline the definitions of the classes BPP, IP of languages $\subseteq \{0,1\}^*$.

ii) State the known inclusions between the classes NP, RP, BPP.

c Outline arguments to show that

i) NP $\subseteq$ IP,

ii) BPP $\subseteq$ IP,

iii) IP = co-IP.

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