THE UNIVERSITY OF SYDNEY

FACULTIES OF ARTS, ECONOMICS, EDUCATION,

ENGINEERING AND SCIENCE

MATH2969

Discrete Mathematics and Graph Theory (Advanced)

PAPER 1

June 2005 Lecturer: David Easdown

Time allowed: one and a half hours

Instructions to candidates

This paper examines Discrete Mathematics and comprises seven questions split into two sections.

There are two questions in **Section A**, each worth 10 marks.

There are five questions in **Section B**, worth 10, 10, 15, 15 and 10 marks respectively.

The total number of marks available is 80.

Both sections should be attempted.

Write your answers to **Section A** in the places indicated on the green question sheet. Write your name and student number on that sheet.

Write your answers to **Section B** in the answer booklet provided.

Place your completed answers for **Section A** (on the green sheet) inside the answer booklet, to be returned together to the examiner.

No notes or books are allowed. A University supplied calculator is permitted.

Section B

Write your answers to this section in the answer booklet.

B1.

(a) Use the Euclidean Algorithm (forwards then backwards) to find 34^{-1} in $\mathbb{Z}_{57}$, and then solve the following for x:

$$34x = 25 \pmod{57} .$$

(b) We know, from the Euclidean Algorithm, that if m and n are positive integers then

$$\text{g.c.d.}\,(m,n) = am + bn$$

for some integers a and b. Prove further that we can arrange things so that a is positive. (This is a handy fact in cryptography.)

(c) Suppose m and n are positive integers. Prove that if k divides both m and n then k also divides g.c.d. (m,n) .

[$4+3+3=10$ marks]

B2.

(a) Find a simple expression for the generating function of the sequence

$$-1,\ 2,\ -3,\ 4,\ -5,\ 6,\ \ldots$$

(b) Write down the sequence associated with the generating function

$$G(z) = \frac{2z-1}{(1+z)^2} .$$

(c) Let $G(z)$ be the generating function for the sequence defined by $a_0 = 4$ and $a_n = 2a_{n-1} - 1$ for $n \geq 1$. Verify that

$$G(z)(1-2z) = \frac{4-5z}{1-z}$$

and use partial fractions to deduce the formula $a_n = 3(2^n) + 1$.

[$1+3+6=10$ marks]

B3.

(a) Define the floor and ceiling functions and prove that if α and β are real numbers such that $\alpha + \beta = 1$ then

$$N = \lfloor \alpha N \rfloor + \lceil \beta N \rceil$$

for any positive integer N.

(b) Describe (without proof) a divide and conquer algorithm for multiplying integers with $N = 2^k$ digits which has running time

$$T(N) = 3T(N/2) + O(N)$$

for $N > 1$. Find an explicit solution for the running time using Big-Oh notation.

[$5+10=15$ marks]

B4. Suppose throughout that $f(N)$ and $g(N)$ are positive functions of a positive variable N. You may take logarithms to any base.

(a) Prove that if $f(N) = O(g(N))$ then

$$\log f(N) \ = \ O(\log g(N)) \ .$$

(b) If $f(N) = O(g(N))$, does it follow that $2^{f(N)} = O(2^{g(N)})$? Explain.

(c) Verify that, for $k = 1, \ldots, N$,

$$k(N - k + 1) \ \geq \ N \ .$$

Deduce that $(N!)^2 \geq N^N$ and $N \log N = O(\log N!)$.

(d) Consider the following conditions, where K is a positive constant:

$$\text{(i)} \ \lim_{N\to\infty} \frac{f(N)}{g(N)} = \infty \qquad \text{(ii)} \ \lim_{N\to\infty} \frac{f(N)}{g(N)} = 0 \qquad \text{(iii)} \ \lim_{N\to\infty} \frac{f(N)}{g(N)} = K$$

Which of the following (possibly more than one)

$$\text{(iv)} \quad g(N) = \Omega(f(N)) \qquad \text{(v)} \quad g(N) = O(f(N))$$

$$\text{(vi)} \quad f(N) \neq O(g(N)) \qquad \text{(vii)} \quad f(N) \neq \Omega(g(N))$$

are implied by each of (i), (ii), (iii)? (There is no need to supply proofs.)

(e) Suppose $\mathcal{A}$ and $\mathcal{B}$ are algorithms with running times $T_{\mathcal{A}}(N)$ and $T_{\mathcal{B}}(N)$ respectively such that $T_{\mathcal{A}}(N) \ = \ \Omega(N^2)$ and

$$T_{\mathcal{A}}(N) \ = \ T_{\mathcal{B}}(N) + O(N) \ .$$

Prove that $T_{\mathcal{B}}(N) \ = \ \Omega(N^2)$. You may assume that limits of quotients exist in order to apply criteria from the previous part.

[2 + 2 + 4 + 3 + 4 = 15 marks]

B5.

(a) We will invent a logical connective called $\triangle$. The truth table for $\triangle$ is

P	Q	$P \triangle Q$
T	T	T
T	F	F
F	T	X
F	F	Y

for some truth values X and Y . We stipulate further that

$$Q \triangle P \qquad \text{and} \qquad \sim Q \triangle \sim P$$

are logically equivalent. Prove that $X = F$ and $Y = T$. How does $\triangle$ relate to usual implication?

(b) Determine the validity of the following argument, by first setting up appropriate propositional symbols and connectives:

If Superman were able and willing to prevent evil, he would do so. If Superman were unable to prevent evil, he would be impotent; if he were unwilling to prevent evil, he would be malevolent. Superman does not prevent evil. If Superman exists, he is neither impotent nor malevolent. Therefore Superman does not exist.

[4 + 6 = 10 marks]

THIS IS THE LAST PAGE OF THE EXAMINATION PAPER