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

$$\gcd(m, n) = am + bn$$

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 $\gcd(m, n)$.

[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 $\alpha$ and $\beta$ are real numbers such that $\alpha + \beta = 1$ then

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

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 \( f(N) = \mathcal{O}(g(N)) \) then
\[
\log f(N) = \mathcal{O}(\log g(N))
\]

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

(c) Verify that, for \( k = 1, \ldots, N \),
\[
k(N - k + 1) \geq N
\]

Deduce that \( (N!)^2 \geq N^N \) and \( N \log N = \mathcal{O}(\log N!) \).

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

\[
\begin{align*}
(i) \quad & \lim_{N \to \infty} \frac{f(N)}{g(N)} = \infty \\
(ii) \quad & \lim_{N \to \infty} \frac{f(N)}{g(N)} = 0 \\
(iii) \quad & \lim_{N \to \infty} \frac{f(N)}{g(N)} = K
\end{align*}
\]

Which of the following (possibly more than one)

\[
(iv) \quad g(N) = \Omega(f(N)) \quad \text{(v)} \quad g(N) = \mathcal{O}(f(N))
\]
\[
(vi) \quad f(N) \neq \mathcal{O}(g(N)) \quad \text{(vii)} \quad f(N) \neq \Omega(g(N))
\]

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
\[
T_\mathcal{A}(N) = T_\mathcal{B}(N) + \mathcal{O}(N)
\]

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 \text{ marks}]
B5.

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

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \triangle Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$X$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$Y$</td>
</tr>
</tbody>
</table>

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

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

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$]$