**UNIVERSITY OF MALTA**
**FACULTY OF SCIENCE**
**Department of Mathematics**
**B.Sc.(Hons.) Year IV**
**June 2003 Examination Session**

**Mathematics Elective Paper II — MAT4403** **16 June 2003**

*0900–1200*

*Answer FOUR questions: TWO questions from each section*

---

## Section A: Graph Theory and Combinatorics I

**1.** (a) Let $C$ be a $q$-ary code of length $n$ and minimum Hamming distance $\delta$. Prove the Singleton Bound, namely that

$$|C| \leq q^{n-\delta+1}.$$

(b) Suppose that $C$ is a binary code of length $n$ and size $|C| = N$. Suppose also that the probability $p < 1/2$ that any single digit is transmitted wrongly is the same for all digits and that these probabilities are mutually independent. Suppose also that all codewords in $C$ are equally likely to be transmitted. Let $d(a, b)$, for any $a, b \in \mathbb{Z}_2^n$, be the usual Hamming distance. Suppose a codeword has been transmitted and the word $w_0$ has been received. Show that,

(i) For any $c \in C$, $P(c \text{ has been transmitted}) = 1/N$.

(ii) For any $c \in C$, $P(w_0 \text{ received}|c \text{ transmitted}) = p^e(1-p)^{n-e}$ where $e = d(w_0, c)$.

(iii) $P(w_0 \text{ received})$

$$= \sum_{i=0}^{N} P(c_i \text{ transmitted}).P(w_0 \text{ received}|c_i \text{ transmitted}),$$

(where $C = \{c_1, c_2, \ldots, c_r\}$) and that this expression is some constant, $K$ say, independent of which $c$ is sent.

(iv) $P(c \text{ transmitted}|w_0 \text{ received})$ equals

$$p^e(1-p)^{n-e} \cdot \frac{K}{N},$$

and that this probability is maximum when $e$ is minimum.

What does this result say about the relationship between most-likely decoding and nearest-neighbour decoding?

Comment briefly on some of the assumptions used to obtain this result.

(c) Let $C$ be the binary code with generator matrix

$$G = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Find a check matrix for $C$, and deduce that this code is not 1-error correcting.

[In (c), any results relating the check matrix of $C$, the minimum distance in $C$ and the error-correcting capabilities of $C$ need not be proved but must be clearly stated.]

**2.** (a) Let $(X, \mathcal{B})$ be a $t$-design for which $|X| = v$, the size of each block is $k$, and every $t$-set of $X$ appears in exactly $\lambda_t$ blocks (where $t < k < v$ and $\lambda_t > 0$).

(i) Show that the number of blocks of this design is equal to

$$\lambda_t \binom{v}{t} / \binom{k}{t}.$$

(ii) Show that the design is also a $(t-1)$-design. Find $\lambda_{t-1}$ in terms of $\lambda_t$ and the other parameters of $(X, \mathcal{B})$.

(b) Show that the set

$$\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$$

is a difference set in $\mathbb{Z}_{19}$, and use it to construct a symmetric 2-design. What are the parameters of this design?

**3.** (a) Suppose that the edges of an infinite complete graph $G$ are coloured red or blue. Show that $G$ contains an infinite complete subgraph whose edges are all of the same colour.

Deduce that an infinite sequence of real numbers contains an infinite monotonic subsequence.

(b) Let the generalised Ramsey number $r(p_1, p_2, \ldots, p_n)$ denote the least positive integer $N$ such that if the edges of the complete graph $K_N$ on $N$

vertices are coloured with any of the colours $c_1, c_2, \ldots, c_n$ then, for some $1 \leq i \leq n$, $K_N$ contains a complete graph on $p_i$ vertices all of whose edges are coloured $c_i$. Let $r_n$ denote $r(p_1, p_2, \ldots, p_n)$ when all the $p_i$ are equal to 3. Show that

$$r_n \leq n(r_{n-1} - 1) + 2.$$

**4.** (a) Let $s = (1\ 2\ 3 \ldots\ n)$ be the cyclic permutation of the set $D = \{1, 2, \ldots, n\}$. Show that the cycles of $s^i$ are all of the same length. Hence obtain, in terms of Euler's $\phi$-function, the cycle index of the cyclic group of permutations of $D$ generated by $s$.

(b) Prove that $19^2$ divides

$$11^{19^2} + 18 \cdot 11^{19} + 3762.$$

[*Hint.* Consider colouring a necklace using 11 colours. Any form of "Burnside's" Counting Lemma may be used without proof, but its use must be clearly indicated.]