Imperial College London

UNIVERSITY OF LONDON

BSc and MSci EXAMINATIONS (MATHEMATICS)

May-June 2006

This paper is also taken for the relevant examination for the Associateship.

M3P17/M4P17

Discrete Mathematics

Date: Tuesday, 30th May 2006 Time: 10 am – 12 noon

Credit will be given for all questions attempted but extra credit will be given for complete or nearly complete answers.

Calculators may not be used.

1. Let $\mathbb{Z}_2 = \{0,1\}$ be the field of order 2 and $\mathbb{Z}_2^n = \{x := (x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}_2\}$ be an n-dimensional vector space over $\mathbb{Z}_2$. For $x, y \in \mathbb{Z}_2^n$ define the Hamming distance $d(x,y)$ and the weight $wt(x)$.

   Prove the following:

   (i) $d(x+z, y+z) = d(x,y)$ and $d(x,y) = wt(x+y)$ for all $x, y, z \in \mathbb{Z}_2^n$;

   (ii) if σ is a permutation of $\{1, 2, \ldots, n\}$ and $x^\sigma = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ then $d(x^\sigma, y^\sigma) = d(x,y)$ for all $x, y \in \mathbb{Z}_2^n$;

   (iii) given $0 \leq i, j, k \leq n$ and $x, y \in \mathbb{Z}_2^n$ with $d(x,y) = k$ then the number p_{ij}^k of $z \in \mathbb{Z}_2^n$ satisfying $d(x,z) = i$, $d(y,z) = j$ is independent of the choice of x and y.

   What is meant by a code C of length n which corrects e errors?

   Define the minimal distance $d(C)$ of C, and state a result linking $d(C)$ and e.

2. Prove the Gilbert-Varshamov bound: if n, m and e are positive integers which satisfy

$$1 + (n-1) + \binom{n-1}{2} + \cdots + \binom{n-1}{e-2} < 2^{n-m}$$

   then there exists a linear code C of length n, dimension m, with $d(C) \geq e$.

   Consider linear codes C of length 10 which correct 2 errors.

   (i) Prove that there exists such a code C with $\dim(C) = 2$.

   (ii) Is there such a code with $\dim(C) = 5$? (Justify your answer.)

3. Let $v > k > \lambda_2$ be positive integers.

   What is meant by a 2-design with parameters (v, k, λ_2)?

   Let $(X, \mathcal{B})$ be a 2-design with parameters (v, k, λ_2). Show that every element of X lies in the same number λ_1 of blocks. Show also that if b is the number of blocks then

$$b\,k = v\,\lambda_1 \quad \text{and} \quad \lambda_1\,(k-1) = \lambda_2\,(v-1)\,.$$

   When is $(X, \mathcal{B})$ said to be symmetric?

   Let A be a $v \times v$ matrix with all entries 0 and 1 (treated as integers) such that

$$JA = kJ$$

$$AA^T = (\lambda_1 - \lambda_2)I + \lambda_2 J$$

   (where I is the identity matrix and J is the matrix with all entries 1). Prove that there exists a symmetric 2-design with parameters (v, k, λ_2) having A as its incidence matrix.

   Deduce from the above that in a symmetric 2-design any two distinct blocks have the same number of elements in common.

4. Let G be a 3-perfect linear code of length 23.

Let $G_m = \{g \in G \mid wt(g) = m\}$.

Calculate the numbers of codewords in G_m for $m = 0, 1, 2, 3, 4, 5, 6, 7$ and 8.

For $g = (g_1, g_2, \ldots, g_{23}) \in G$ define the support of g as $sp(g) = \{i \mid g_i = 1\}$.

Let $X = \{1, 2, \ldots, 23, 24\}$ and let

$$\mathcal{B} = \{sp(g) \mid g \in G_8\} \cup \{sp(g) \cup \{24\} \mid g \in G_7\}.$$

Prove that $(X, \mathcal{B})$ is a 5-design with parameters $(24, 8, 1)$.

5. Explain what is meant by a strongly regular graph with parameters (v, k, a, b).

Let U be a 4-dimensional vector space over $\mathbb{Z}_2$. Let $\Gamma = (V, E)$ be a graph such that V is the set of 2-dimensional subspaces in U and

$$E = \{(x, y) \mid x, y \in V,\ \dim(x \cap y) = 1\}.$$

Show that Γ is strongly regular and calculate the parameters of Γ.

What are the eigenvalues of the adjacency matrix of Γ?

You may use the following standard result.

If A is the adjacency matrix of a strongly regular graph with parameters (v, k, a, b) then A has just 3 distinct eigenvalues k, r, s, where r and s are the roots of

$$x^2 - (a - b)x - (k - b) = 0.$$