MAS3034

UNIVERSITY OF EXETER

SCHOOL OF ENGINEERING, COMPUTER SCIENCE & MATHEMATICS

DEPARTMENT OF MATHEMATICAL SCIENCES

DIRECTED READING

June 2001

9:30 a.m. – 12:30 p.m.
Duration: 2 hours

Examiner: Robin Chapman

Answer Section A (50%) and any TWO of the three questions in Section B (25% for each).

Marks shown in questions are merely a guideline.

Calculators labelled as approved by the Department of Mathematical Sciences may be used.

SECTION A

1. (a) Let F^n denote the set of length n words over the finite alphabet F. Define the *Hamming distance* $d(\mathbf{a}, \mathbf{b})$ for $\mathbf{a}$, $\mathbf{b} \in F^n$, and show that

$$d(\mathbf{a}, \mathbf{c}) \leq d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c})$$

whenever $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c} \in F^n$.

In the case where $F = GF(q)$ is a finite field define the *weight* $w(\mathbf{a})$ of $\mathbf{a} \in F^n$ and show that when $F = GF(2)$ then

$$w(\mathbf{a} + \mathbf{b}) \equiv w(\mathbf{a}) + w(\mathbf{b}) \pmod 2.$$

(12)

(b) Let C be a $(n, M, 2e+1)$ code over an alphabet F of size q. Prove the *sphere packing bound*:

$$q^n \geq M \sum_{j=0}^{e} \binom{n}{j} (q-1)^j. \qquad (*)$$

(10)

(c) Recall that each word in the ISBN code has the form $a_1 a_2 \cdots a_{10}$ where the digits a_j satisfy

$$\sum_{j=1}^{10} j a_j \equiv 0 \pmod{11}.$$

Show that if one entry is altered or two unequal entries are interchanged in an ISBN code word, the resulting word no longer lies in the ISBN code. (10)

(d) Let C be a linear code over $GF(q)$ with parity-check matrix H. What is the *syndrome* of a word $\mathbf{a} \in V(n, q)$? Show that two words $\mathbf{a}$ and $\mathbf{b}$ have the same syndrome if and only if they lie in the same coset of C in $V(n, q)$.

Consider the binary linear code with parity-check matrix

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

On the assumption that no more than one error has occurred in each word, correct, where possible, the following received words:

(i) 01101100,

(ii) 00011110.

(8)

[**40**]

SECTION B

2. (a) Define the *dual* $C^{\perp}$ of a linear code C over $GF(q)$. Show that $C^{\perp}$ is also a linear code. (5)

   (b) What is a *parity-check* matrix of a linear code C. Prove that if the $[n, k]$ linear code C has generator matrix $(I_k \mid A)$ then $(-A^T | I_{n-k})$ is a parity-check matrix for C. (8)

   (c) Let H be a parity-check matrix for the linear code C. Suppose that for some number k, each set of k columns of H is linearly independent. Prove that the minimum weight of C is at least $k + 1$.

   Find the minimum weight of the linear code C over $GF(3)$ with parity-check matrix

$$H = \begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 1 & 2 \end{pmatrix}.$$

   (7)

   [**20**]

3. (a) Consider the linear code C over $GF(7)$ with parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 \\ 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 \end{pmatrix}.$$

   Show that C is a double-error correcting $[6, 2]$-code. (You may assume standard facts concerning Vandermonde determinants provided these are stated clearly). (5)

   (b) Describe a decoding method for the code C defined in part (a). Use it to correct the following received words, where possible, on the assumption that no more than two errors occur in each. For convenience the syndrome, with respect to the matrix H, is also given.

   (i) (4,5,2,3,3,2) with syndrome (5,3,6,5);

   (ii) (4,6,1,1,1,4) with syndrome (3,3,5,5). (15)

   [**20**]

4. (a) What is a *cyclic code* over the finite field $GF(q)$? Describe the correspondence between words in cyclic codes and polynomials. Let C be a cyclic code of length n and $f(x)$ be the polynomial corresponding to a word of C. Show that if

$$g(x) \equiv xf(x) \pmod{x^n - 1}$$

where $g(x)$ has degree at most $n-1$, then $g(x)$ also corresponds to a word in C. (7)

(b) Let $g(x)$ and $h(x)$ be, respectively, the generator polynomial and the parity-check polynomial of a cyclic code C of length n over $GF(q)$. What is the relation between $g(x)$ and $h(x)$? Explain how to construct generator and parity-check matrices for C from the coefficients of $g(x)$ and $h(x)$. Express the dimension of C in terms of the degree of $g(x)$. (6)

(c) Factorize $x^6 - 1$ into irreducible factors over $GF(5)$. Hence determine, for each k, how many cyclic $[6, k]$ codes over $GF(5)$ there are. (7)

[**20**]

5. The MacWilliams identity for a binary linear code states that

$$W_{C^\perp}(z) = \frac{(1+z)^n}{2^k} W_C\left(\frac{1-z}{1+z}\right)$$

where C denotes an $[n, k]$ binary linear code, $W_C(z)$ its weight enumerator and $C^\perp$ its dual.

(a) Use the MacWilliams identity to calculate the number of weight 3 words in the binary linear code with generator matrix

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

(5)

(b) Let C be a *self-dual* binary linear code of length n, that is, C is an $[n, n/2]$ binary linear code with $C = C^\perp$. Show that the weight of each word in C is even. Deduce that the all-one word $111\cdots1$ lies in C, and conclude that $A_k = A_{n-k}$ for each k, where A_k denotes the number of weight k words in C. (7)

(c) The extended binary Golay code $\mathcal{G}_{24}$ is a $[24, 12]$ binary linear code which is self-dual, all its words have weights divisible by 4, and its minimum weight is 8. Use these properties, together

with the MacWilliams identity, to calculate the weight enumerator of $\mathcal{G}_{24}$.
(Hint: One only needs to compare the constant and z^2 terms on both sides of the MacWilliams identity.) (8)

[**20**]