MAS3004

UNIVERSITY OF EXETER

SCHOOL OF ENGINEERING, COMPUTER SCIENCE & MATHEMATICS

DEPARTMENT OF MATHEMATICAL SCIENCES

CODING THEORY

June 2002

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 $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c} \in (Z_p)^n$. Define the *Hamming distance* $d(\mathbf{a}, \mathbf{b})$ and the weight $w(\mathbf{c})$. Show that $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} - \mathbf{b})$.

   Let C be a code over the alphabet Z_p. Define the *minimum distance* and the *minimum weight* of C, and show that they are equal. (10)

   (b) Let $\mathbf{a}$, $\mathbf{b} \in (Z_p)^n$. Define the dot product $\mathbf{a} \cdot \mathbf{b}$ of $\mathbf{a}$ and $\mathbf{b}$. For $p = 2$ and for $p = 3$, show that $\mathbf{a} \cdot \mathbf{a} = 0$ if and only if $w(\mathbf{a})$ is a multiple of p. Show however, that the corresponding statement for $p = 5$ is false. (8)

   (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

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

   Complete the following ISBNs (which are of real books):
   (i) 074755099?; (ii) 009943511?; (iii) 184?154652. (9)

   (d) Let C be a linear code over Z_p with parity-check matrix H. What is the *syndrome* of a word $\mathbf{a} \in (Z_p)^n$? 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 $(Z_p)^n$.

   Consider the binary linear code with parity-check matrix

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

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

   (i) 01101110;
   (ii) 10011010;
   (iii) 10011001.

(13)

[40]

SECTION B

2. Let Ω denote an alphabet with q letters.

   (a) Let C be a (n, M, d) code over Ω. Prove the *Singleton bound*:

   $$M \leq q^{n-d+1}.$$

   (3)

   (b) Let C be a $(n, M, 2e+1)$ code over Ω. Prove the *sphere packing bound*:

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

   (7)

   (c) Determine whether (n, M, d)-codes exist over $\Omega = \{0, 1\}$ for the following values of (n, M, d). In each case either give a code or prove that no such code exists.

   (i) $(n, M, d) = (8, 16, 4)$;

   (ii) $(n, M, d) = (10, 32, 5)$;

   (iii) $(n, M, d) = (16, 16, 8)$.

   [If a code you give is linear, you may give its generating matrix or parity-check matrix instead of listing its words.] (10)

   [**20**]

3. (a) Give the definition of the *Hamming codes* over Z_p. Describe how to decode a Hamming code, on the assumption that no more that one error can occur in each word.

Let C_1 be the Hamming code over Z_5 with parity-check matrix

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Decode the following words

(i) 102030;

(ii) 334121. (10)

(b) Consider the linear code C_2 over Z_{11} with parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 \\ 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 \end{pmatrix}.$$

Decode the following words, if possible, on the assumption that no more than two errors occur in each word. [Here X denotes the "digit" 10. For convenience the syndrome, with respect to the matrix H, is also given.]

(i) 37202XX with syndrome $(1\,9\,3\,2)^t$;

(ii) 5729643 with syndrome $(3\,4\,9\,1)^t$. (10)

[20]

4. (a) What is a *cyclic code* over Z_p? Describe the correspondence between $(Z_p)^n$ and the truncated polynomial ring $Z_p[x]_n$ and show that this correspondence takes cyclic codes to ideals of $Z_p[x]_n$. What is the *generator polynomial* of a cyclic code, and show that the generator polynomial of a cyclic code of length n is a factor of $x^n - 1$ in $F_p[x]$. (10)

(b) Let $f(x) = 1 + x + x^2 + \cdots + x^{n-1}$ and let $g(x) \in Z_p[x]$. Regarded as elements of $Z_p[x]_n$, show that $g(x)f(x) = g(1)f(x)$. Deduce that if C is a binary cyclic code having a word of odd weight then C contains the all-one word $111\cdots 1$. (4)

(c) Factorize $x^8 - 1$ into irreducible factors over Z_3. Hence determine, by listing the generator polynomial of each, all cyclic $[8, 5]$ codes over Z_3. (6)

[20]

5. (a) Let C be a linear code of length n over Z_2. Define the *weight enumerator* $W_C(z)$ of C. Show that $W_C(z) = z^n W_C(1/z)$ if and only if C contains the all-one word $111\cdots1$. (4)

(b) The MacWilliams identity states that

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

where C is a binary linear $[n,k]$-code and $C^\perp$ is its dual.

Use the MacWilliams identity to calculate the number of words of weight 2 in the binary linear code with generator matrix

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

(6)

(c) A binary *self-dual* code C of length n is a binary linear $[n, n/2]$-code satisfying $C = C^\perp$. Show that if C is a binary self-dual code then all its words have even weight and that C contains the all-one word $111\cdots1$.

Now suppose that C is a binary self-dual $[12,6,4]$-code. Using the MacWilliams identity find $W_C(z)$. [You may find the formula $(1+z)^{12-k}(1-z)^k = 1 + (12-2k)z + (2k^2 - 24k + 66)z^2 + \cdots$ useful.] (10)

[20]