MAS3004

UNIVERSITY OF EXETER

SCHOOL OF ENGINEERING, COMPUTER SCIENCE & MATHEMATICS

DEPARTMENT OF MATHEMATICAL SCIENCES

CODING THEORY

June 2004

9:30 a.m. – 11:30 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).

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* $w(\mathbf{c})$. Prove that $d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} - \mathbf{b})$. (7)

   (b) For each of the following parameter systems (n, M, d), determine whether there is a (n, M, d)-code over Z_2. You should justify your answers, but may use standard results without proof provided they are stated clearly.
   (i) $(5, 16, 2)$; (ii) $(9, 4, 6)$; (iii) $(10, 20, 5)$. (13)

   (c) Recall that each word $a_1 a_2 \cdots a_{10}$ in the ISBN code satisfies

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

   Hence complete the following ISBNs:
   (i) 052145761?; (ii) 05213666?X; (iii) 0?87962549.
   Also prove that if two unequal digits are transposed in a valid ISBN then the result is an invalid ISBN. (18)

   (d) Consider the binary linear code C with parity-check matrix

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

   On the assumption that no more than one error has occurred in each word, correct, where possible, the following received words:
   (i) 0000111001;
   (ii) 1110100111;
   (iii) 0011010100.
   (12)

[**50**]

SECTION B

2. (a) What is a *linear code* over Z_p?

   Let C be a linear code over Z_p. What is a *generator matrix* for C? What is the *dual code* $C^{\perp}$ of C?

   Prove that if C is a linear code with generator matrix $G = (I_k\ A)$ where A is a k-by-$(n-k)$ matrix, then $(-A^T\ I_{n-k})$ is a generator matrix for $C^{\perp}$. (9)

   (b) A linear code C over Z_p is *self-dual* if and only if $C = C^{\perp}$. Prove that each self-dual code has even length, and that if C is a self-dual code over Z_p with generator matrix $G = (I_k\ A)$ (where A is a square k-by-k matrix) then $AA^T = -I_k$. (8)

   (c) Prove that if $p = 2$ or $p = 3$ then the weights of all words in a self-dual code C are divisible by p. Give an example of a self dual $[4, 2]$-code over Z_7 and confirm that it has words of weight not divisible by 7. (8)

   [25]

3. (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 prove that this correspondence takes cyclic codes to ideals of $Z_p[x]_n$. What is the *generator polynomial* of a cyclic code? Prove that the generator polynomial of a cyclic code of length n is a factor of $x^n - 1$ in $Z_p[x]$. (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 $Z_p[x]_n$, prove that $g(x)f(x) = g(1)f(x)$. Hence prove that if C is a cyclic code over Z_p then either C contains that all-one word $\mathbf{v} = 111\cdots1$ or that the all-one word is orthogonal to C, that is, $\mathbf{a} \cdot \mathbf{v} = 0$ for all $\mathbf{a} \in C$. (8)

   (c) Factorize $x^{12} - 1$ into irreducible factors over Z_3. Hence determine, by listing the generator polynomial of each, all cyclic $[12, 8]$ codes over Z_3. (You may leave these generator polynomials in factored form.) (7)

   [25]

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

(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 3 in the binary linear code with generator matrix

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

(8)

(c) A binary *self-dual* code C of length n is a linear $[n, n/2]$-code over Z_2 satisfying $C = C^\perp$. Prove 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 $[16,8]$-code, all of whose words have weights divisible by 4. Use the MacWilliams identity to find $W_C(z)$. [You may find the formula $(1+z)^{16-k}(1-z)^k = 1 + (16-2k)z + (2k^2 - 32k + 120)z^2 + \cdots$ useful.] (12)

[25]