MAS3004

UNIVERSITY OF EXETER

SCHOOL OF ENGINEERING, COMPUTER SCIENCE & MATHEMATICS

DEPARTMENT OF MATHEMATICAL SCIENCES

CODING THEORY

June 2006 | Andreas Schweizer
Duration: 2 hours

Examiner:

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) For each of the following parameter systems (n, M, d) decide whether there exists a q-ary (n, M, d)-code. Justify your answers.

   (i) $(6, 32, 2)$ for $q = 2$;

   (ii) $(6, 132, 4)$ for $q = 5$;

   (iii) $(5, 27, 3)$ for $q = 3$;

   (iv) $(6, 49, 3)$ for $q = 7$. (16)

   (b) What is the check condition for $a_1 a_2 \ldots a_{10}$ to be an ISBN number?

   Complete the following ISBN numbers

   (i) 03407?6146;

   (ii) 2070387?64. (10)

   (c) Determine the coset leaders and their syndromes for the ternary linear code with parity-check matrix

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

   Using syndrome decoding, decode 0022 and 1201. (15)

   (d) Let $Ham(3, 2)^+$ be the extended binary Hamming code with parity-check matrix

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

   Using incomplete decoding, decode 11100000, 10100101 and 11001100. (9)

[**50**]

SECTION B

2. (a) State and prove the sphere-packing bound for one-error-correcting codes. (10)

   (b) Explain why a one-error-correcting code must have minimum distance at least 3. (5)

   (c) Show that for $q \neq 4$ there are no q-ary perfect one-error-correcting codes of length 5. (10)

   [25]

3. (a) Let C be the linear code over $\mathbb{F}_5$ with parity-check matrix

$$H = \begin{bmatrix} 0 & 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 4 & 0 \\ 0 & 3 & 0 & 2 & 1 \end{bmatrix}.$$

   What is the minimum distance of C? Justify your answer. (10)

   (b) Show that if C is a cyclic code over $\mathbb{F}_p$ of length n and $w(C) = 1$, then $C = \mathbb{F}_p^n$. (5)

   (c) Factorize $x^4 - 1$ into irreducible factors over $\mathbb{F}_7$. Use this to determine all cyclic codes of length 4 over $\mathbb{F}_7$, listing the generator polynomial and a generator matrix for each. (10)

   [25]

4. (a) Let C be the linear code over $\mathbb{F}_5$ with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 1 \end{bmatrix}.$$

If C is used for error detection, and if for each digit the probability that it is corrupted during transmission is p=0.02, what is the probability $P_{undetect}(C)$ that a received word contains an undetectable error? (10)

(b) The MacWilliams identity for binary codes of length n states that

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

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

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

(10)

(c) Let C be a binary linear code. Prove that $C^\perp$ contains the word $1111\ldots1$ if and only if each codeword in C has even weight. (5)

[25]