MATH-315201

This question paper consists of 2 printed pages, each of which is identified by the reference MATH-3152

Only approved basic scientific calculators may be used.

Mock Examination for the Module MATH-3152

(January 2004)

Coding Theory

Time allowed: 2 hours

Attempt no more than **four** questions. All questions carry equal marks.

1. (a) Let Σ_q be an alphabet of size q and $C \subset \Sigma_q^n$ be a q-ary block code of length n. Define:

   (i) The *Hamming distance* d on Σ_q^n.

   (ii) The *minimum distance* $d(C)$ of the code C.

   (iii) The parameter $A_q(n, d)$.

   (b) State and prove the ball-packing bound on $A_q(n, d)$.

   (c) Prove that $A_q(n, d) \geq A_q(n + 1, d)/q$.

   (d) In each of the following cases *either* construct a code with the specified parameters *or* explain why no such code exists.

   (i) A 7-ary $(5, 550, 3)$ code.

   (ii) A 5-ary $(7, 26, 6)$ code.

   (iii) A 5-ary $(8, 130, 6)$ code.

2. (a) Let C be the ternary linear code with generator matrix

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

   (i) List the codewords of C and find the minimum distance $d(C)$.

   (ii) Construct a standard array for C. Use your array to decode the received vectors 112 and 120

   (b) Suppose that a binary linear $[9, 4, 3]$ code C is transmitted down a binary symmetric channel with symbol error probability $p < \frac{1}{2}$. Show that $P_{\text{corr}}(C)$, the probability of any transmitted codeword being *correctly* decoded, satisfies

$$P_{\text{corr}}(C) \geq (1 - p)^9 + 9p(1 - p)^8 + 13p^7(1 - p)^2 + 9p^8(1 - p).$$

Given that $p = 0.01$, find an upper bound on the word error rate $P_{\text{err}}(C)$ of the code. Compare your answer with $P_{err}(C_0)$, where $C_0 = \mathbb{Z}_2^4$.

3. Let C be the binary linear code with generator matrix

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

   (a) Write down a parity check matrix H for C.

   (b) Explain how the minimum distance of C may be deduced from H. Find $d(C)$.

   (c) How many cosets does C have? How many cosets are led by weight 1 vectors? Does any coset have a weight 2 coset leader?

   (d) Construct a syndrome look-up table for C. Hence, or otherwise, decode the received vectors 100110, 011101 and 101001.

4. (a) Construct the projective equivalence class of the vector $3152 \in \mathbb{Z}_{11}^4$, listing your answer in lexicographical order. [Denote the digit "10" by X, the last digit lexicographically.]

   (b) Write down the parity check matrix for the standard Hamming code $C = \text{Ham}(\mathbb{Z}_3^3)$. Determine the parameters $[n, k, d]$ of C. Decode the received vector $1110 \cdots 0 \in \mathbb{Z}_3^n$.

   (c) Let $\widehat{C}$ be the following subcode of C:

$$\widehat{C} = \{\mathbf{x} \in C \mid \sum_{i=1}^{n} 2^i x_i = 0 \bmod 3\}.$$

   Prove that $\widehat{C}$ is also a linear code. Write down a parity check matrix $\widehat{H}$ for $\widehat{C}$, and determine the parameters $[\widehat{n}, \widehat{k}, \widehat{d}]$ of $\widehat{C}$. Decode the received vector $1110 \cdots 0 \in \mathbb{Z}_3^{\widehat{n}}$.

5. (a) Define the term *cyclic code*.

   (b) Determine whether the following codes are cyclic. Briefly explain your answers.

      (i) The binary code $\{0000, 1010, 0101, 1110, 1101, 1011, 0111\}$.

      (ii) The ternary code $\{000, 011, 101, 110\}$.

      (iii) The 7-ary code $\{\mathbf{x} \in \mathbb{Z}_7^5 \mid \sum_{i=1}^{5} i x_i = 0 \bmod 7\}$.

      (iv) $E_n \subset \mathbb{Z}_2^n$, the set of even weight binary words of length n.

      (v) $O_n \subset \mathbb{Z}_2^n$, the set of odd weight binary words of length n.

   (c) (i) Factorize $p(x) = x^5 - 1$ over $\mathbb{Z}_{31}$ into irreducible factors. (Hint: what is $p(2^n)$?)

      (ii) For each $k \in \{0, 1, 2, \ldots, 5\}$ let N_k denote the number of distinct 31-ary cyclic codes of length 5 and dimension k. Determine the numbers $N_0, N_1, \ldots, N_5$.

      (iii) Choose any one of the cyclic codes of dimension 3 C say. Write down the generator polynomial $g(x)$, the check polynomial $h(x)$, a generator matrix G and a parity check matrix H for C. Determine $d(C)$. Write down the $g^{\perp}(x)$ the generator polynomial of the dual code.