Faculty of Science, Technology, Engineering and Mathematics
M836 Coding theory

M836

TMA 03

Covers Units 9-12 **See module website for the cut-off date.**

TMA 03 is a formative assignment that does not count towards your final grade. However, in order to pass the module, you are required to submit at least three TMAs and score at least 30% on at least three of the TMAs submitted.

The substitution rule does not apply to this module.

To be sure of passing this module, you need to achieve a score of at least 50% in the examination and score at least 30% on three out of four TMAs. The final rank score will be completely determined by your overall exam score (OES).

You are strongly encouraged to submit your assignments online using the electronic TMA/EMA service. If you cannot submit an assignment electronically, then, with permission from your tutor, you may submit it by post. Please read the instructions under the 'Assessment' tab of the module website before starting your assignments. The assignment cut-off dates can be found on the module website.

Each TMA of this module examines the work contained in the block to which it relates, but may require knowledge of material in previous blocks. Within each TMA, there is not a one-to-one correspondence between questions and the units forming that block. The number of marks assigned to each part of a question is given in the right-hand margin. There are 100 marks available for each assignment. A high standard of presentation is required. Answers should be written in good English with appropriate explanations. There is no need to word-process your solutions; legible handwriting is perfectly acceptable.

 WEB 09645 7
2.1

Question 1 – 25 marks

An $m \times n$ *Latin rectangle* (with $1 \leq m \leq n$) is an $m \times n$ array with entries $0, 1, \ldots, n-1$ such that each entry appears exactly once in each row and at most once in each column. We will assume that the rows are indexed by $0, 1, \ldots, m-1$ and the columns are indexed by $0, 1, \ldots, n-1$. Two such rectangles $A = [a_{i,j}]$ and $B = [b_{i,j}]$ are said to be *mutually orthogonal* if the mn ordered pairs $(a_{i,j}, b_{i,j})$ are all distinct; in other words, if we superimpose A and B to form a new array with ordered pairs as entries, then these mn entries are all distinct.

(a) Prove that if $1 < m \leq n$, then there cannot exist a set of n mutually orthogonal $m \times n$ Latin rectangles. Determine the maximum possible number of mutually orthogonal $1 \times n$ Latin rectangles. [6]

(b) Suppose that $p > 1$ is prime and that $q > 1$ is an integer having no prime factors less than p. Put $n = pq$. For $\lambda = 1, 2, \ldots, n-1$, define A_λ to be the $p \times n$ array with entries $a_{i,j}^{(\lambda)} = \lambda i + j$ for $i = 0, 1 \ldots, p-1, \quad j = 0, 1, \ldots, n-1$, and with arithmetic in Z_n.

(i) Prove that A_λ is a $p \times n$ Latin rectangle. [4]

(ii) Prove that if $\lambda \neq \mu$, then A_λ and A_μ are mutually orthogonal, so that $\{A_\lambda : \ 1 \leq \lambda \leq n-1\}$ forms a set of $n-1$ mutually orthogonal $p \times n$ Latin rectangles. [4]

(c) A code $C_{p,q}$ is formed from the Latin rectangles A_λ by taking as codewords all vectors of the form $(i, j, a_{i,j}^{(1)}, a_{i,j}^{(2)}, \ldots, a_{i,j}^{(n-1)})$ for $i = 0, 1 \ldots, p-1$ and $j = 0, 1, \ldots, n-1$ (where again $n = pq$).

(i) List the codewords of $C_{2,3}$. [4]

(ii) Determine the minimum distance of $C_{p,q}$ in terms of p and q. [7]

Question 2 – 25 marks

In the course of this question we use the Lloyd polynomial (see Theorem 9.6 of **H**) to prove that there is no nontrivial perfect binary 2-error-correcting code.

(a) Suppose that C is a perfect binary $(n, M, 5)$-code. Prove that $n^2 + n + 2$ is necessarily of the form 2^m, where m is an integer, and that if C is nontrivial (i.e. if $n > 5$), then $m > 5$. [4]

(b) Show that the Lloyd polynomial $L_2(x)$ is given by

$$2L_2(x) = 4x^2 - 4(n+1)x + (n^2 + n + 2).$$

Hence show that if $n > 5$, then neither $L_2(1)$ nor $L_2(2)$ is zero. [6]

(c) Suppose that $L_2(x)$ has two integer roots x_1, x_2 satisfying $3 \leq x_1 < x_2 \leq n$. By considering the product of the roots, show that both x_1 and x_2 must be integer powers of 2. If $x_1 = 2^a$ and $x_2 = 2^b$, show that $(2^{a+1} + 2^{b+1} - 1)^2 = 2^{m+2} - 7$. By considering this equation modulo 16, obtain a contradiction, thereby proving that $L_2(x)$ cannot have two distinct integer roots for $1 \leq x \leq n$ and that, consequently, there is no perfect binary $(n, M, 5)$-code with $n > 5$. [9]

(d) Prove that although there is no binary $(90, 2^{78}, 5)$-code, there is a binary *linear* $(90, 2^{73}, 5)$-code. [6]

Question 3 – 25 marks

(a) By listing the codewords of $RM(1,1)$, $RM(1,2)$ and $RM(1,3)$, give the number of codewords of each weight in each of these codes. [3]

(b) Prove that for $m \geq 1$, $RM(1,m)$ has weight enumerator

$$1 + (2^{m+1} - 2)z^{2^{m-1}} + z^{2^m}.$$ [9]

(c) Using your answer to part (b), or otherwise, show that the weight enumerator of $RM(m-2, m)$ is

$$W(z) = \frac{1}{2^{m+1}} \left[(1+z)^{2^m} + (2^{m+1} - 2)(1-z^2)^{2^{m-1}} + (1-z)^{2^m} \right].$$ [5]

(d) If $C = RM(2,4)$ is used for error detection over a binary symmetric channel with symbol error probability p, determine an expression for $P_{undetec}(C)$, the probability of an incorrect message being received undetected. Show that if p is small, then $P_{undetec}(C) \approx 140p^4$. If $p = 0.01$, give a rough estimate for the average number of received vectors per undetected error. [8]

Question 4 – 25 marks

(a) Let C be the cyclic code in $R_{15} = F_2[x]/(x^{15}-1)$ with generator polynomial $g(x) = 1 + x + x^2 + x^3 + x^6$. By multiplication or otherwise, prove that the corresponding check polynomial is $h(x) = 1 + x + x^4 + x^5 + x^6 + x^9$. Show that the following 56 polynomials in R_{15} are all distinct (it should not be necessary to write down the 56 polynomials explicitly):

$$0, \quad x^k h(x)\ (0 \le k \le 14), \quad x^k(1+x)h(x)\ (0 \le k \le 13),$$

$$x^k(1+x^2)h(x)\ (0 \le k \le 12), \quad x^k(1+x+x^2)h(x)\ (0 \le k \le 12).$$

Hence show that all vectors of burst length at most 3 are in distinct cosets of C and, consequently, that C is 3 burst error-correcting. Prove also that C is *not* 3 error-correcting. [*10*]

(b) Let D be the code $\mathrm{Ham}(3,2)$ with generator matrix

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

(i) The codewords

$$\mathbf{c}_1 = 1100110, \quad \mathbf{c}_2 = 1001100, \quad \mathbf{c}_3 = 0010110,$$
$$\mathbf{c}_4 = 0111100, \quad \mathbf{c}_5 = 1111111, \quad \mathbf{c}_6 = 0001111$$

are transmitted using interleaving to depth 3. Give the sequence of transmitted bits. Determine the maximum length of an error burst that can be assured of correction, assuming a sufficient interval between adjacent error bursts. [*5*]

(ii) Repeat part (i) but using 2-frame interleaving. [*3*]

(c) Let C_1 be the binary $[7,1,7]$ repetition code with generator matrix $G_1 = (1\ 1\ 1\ 1\ 1\ 1\ 1)$, and let C_2 be the binary $[8,4,4]$-code $RM(1,3)$ with generator matrix

$$G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

When C_1 is cross-interleaved with C_2, with C_2 being interleaved to depth 3, the following vector is received:

111	111	000	000	000	000	111	111	
111	111	000	000	111	111	000	111	
100	111	011	000	000	011	111	100	
000	111	111	000	000	111	111	000	
000	110	110	000	000	110	110	000	...

Determine the first 8 message bits, assuming that a single burst of length at most 9 has affected the transmission. [*7*]