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

M836

TMA 02

Covers Units 5-8 **See module website for the cut-off date.**

TMA 02 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.

Question 1 – 25 marks

(a) Show that the matrix

$$H = \begin{pmatrix} 0 & 1 & 2 & 4 & 6 & 4 & 3 & 5 \\ 3 & 2 & 2 & 6 & 1 & 2 & 2 & 0 \end{pmatrix}$$

is a parity-check matrix for a Hamming code $\mathrm{Ham}(2,7)$. *[4]*

(b) Using row operations *only*, transform H to a generator matrix G in standard form for a simplex code $\mathrm{Sim}(2,7)$ and hence obtain a parity-check matrix in standard form for this code. *[5]*

(c) How many cosets does $\mathrm{Sim}(2,7)$ possess? Determine the number of, and describe, the coset leaders in the top part of the Slepian standard array for the $\mathrm{Sim}(2,7)$ code of part (b). Determine the syndromes of each of the vectors $10000000, 01000000, \ldots, 00000001$. Hence correct the received vector 45632036, assuming at most one error. *[6]*

(d) Write down a parity-check matrix $\hat{H}$ for an extended Hamming code $\mathrm{H\hat{a}m}(4,2)$, taking the columns of the corresponding Hamming code in their natural order as indicated on page 81 of **H**. Describe the incomplete decoding algorithm for this code. *[4]*

(e) Apply the algorithm of part (d) to the following received vectors

(i) 0111 0000 0000 0000,

(ii) 0001 1001 1110 0111,

(iii) 1100 0000 0000 0011. *[6]*

Question 2 – 25 marks

The code C over $GF(7)$ is defined by the parity-check matrix

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

(a) What are the dimension and minimum distance of the code? *[2]*

(b) Using the method described on pages 131-4 of **H**, decode the received vector 324664. *[10]*

(c) For which values of a, b, c and d is the vector $11abcd$ a codeword? *[4]*

(d) From your answers to parts (a), (b) and (c), find a generator matrix G in standard form for the code C. *[4]*

(e) It is known that each of the received vectors 324130 and 452066 contains a single error. Use the *generator matrix* G to determine the codewords sent. (Marks will not be awarded for using the same method as in part (b).) *[5]*

Question 3 – 25 marks

(a) The code $C = H * S$ is formed, using Plotkin's $(\mathbf{a}|\mathbf{a}+\mathbf{b})$ construction, from the codes $H = \text{Ham}(3,2)$ and $S = \text{Sim}(3,2)$. Determine the length, dimension and minimum distance of C. Explain why, in constructing a Slepian standard array for C, not all vectors of weight 2 can be coset leaders. [6]

(b) A truth table for the function $f : V(3,2) \to V(1,2)$ is shown below.

v_1	v_2	v_3	$f(v_1, v_2, v_3)$
0	0	0	0
1	0	0	1
0	1	0	1
1	1	0	0
0	0	1	1
1	0	1	0
0	1	1	1
1	1	1	1

Obtain an expression for $f(v_1, v_2, v_3)$ as a Boolean multinomial in three Boolean variables. [6]

(c) A message $\mathbf{a} = a_0a_1a_2a_3a_4$ is encoded using a generator matrix G for $RM(1,4)$ to give the codeword $\mathbf{x} = \mathbf{a}G$, where $\mathbf{x} = x_0x_1 \cdots x_{15}$ and G is as given in Example 7.7 of the Module Notes for Unit 7.

(i) Obtain the equations needed to apply the Reed decoding algorithm. You should give eight equations for each of a_1, a_2, a_3 and a_4, and explain how to get 16 equations for a_0. [7]

(ii) Hence determine the original message word $\mathbf{a}$ from the received vector 1100 1111 0011 1011, assuming that at most three transmission errors have occurred. [6]

Question 4 – 25 marks

(a) Prove that, over $GF(2)$, $x^3 - 1 = (x+1)(x^2+x+1)$. Hence obtain the factorization of $x^9 - 1$ into irreducible monic polynomials over $GF(2)$. [6]

(b) (i) Determine all cyclic codes of length 9 over $GF(2)$ by specifying their generator polynomials and equivalent generator matrices. [5]

(ii) For each of these codes, write down a check polynomial and equivalent parity-check matrix. [5]

(c) One of the codes in part (b) has generator polynomial $g(x) = x^6 + x^3 + 1$.

(i) Determine the minimum distance of this code and the number of codewords. [2]

(ii) A message $m(x) = m_0 + m_1 x + m_2 x^2$ is encoded as $c(x) = m(x)g(x)$. Obtain the codeword corresponding to the message $1 + x + x^2$. [1]

(iii) Given a polynomial $p(x)$ of degree at most 8, the *syndrome* of $p(x)$ is defined to be $p(x)h(x)$ (reduced modulo $x^9 - 1$), where $h(x)$ is the check polynomial corresponding to $g(x)$. Determine the syndrome of each polynomial of weight 1 (i.e. having precisely one nonzero coefficient) and degree at most 8. Hence, assuming at most one error in the received polynomial $1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^8$, determine the original message polynomial. [6]