

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING  
EXAMINATIONS 2003

MSc and EEE/ISE PART IV: M.Eng. and ACGI

**CODING THEORY**

Tuesday, 29 April 10:00 am

Time allowed: 3:00 hours

**There are SIX questions on this paper.**

**Answer FOUR questions.**

**Corrected Copy**

**Any special instructions for invigilators and information for candidates are on page 1.**

Examiners responsible	First Marker(s) :	O.R.L. Pretzel
	Second Marker(s) :	A. Manikas



A table of the field of order 16

log	0	1	12	2	9	13	7	3	4	10	5	14	11	8	6
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	3	4	6	8	10	12	14	9	11	13	15	1	3	5	7
3	2	1	5	12	15	10	9	1	2	7	4	13	14	11	8
4	5	6	7	9	13	1	5	11	15	3	7	2	6	10	14
5	4	7	6	1	8	7	2	3	6	9	12	14	11	4	1
6	7	4	5	2	3	13	11	2	4	14	8	3	5	15	9
7	6	5	4	3	2	1	12	10	13	4	3	15	8	1	6
8	9	10	11	12	13	14	15	15	7	6	14	4	12	13	5
9	8	11	10	13	12	15	14	1	14	12	5	8	1	3	10
10	11	8	9	14	15	12	13	2	3	11	1	5	15	8	2
11	10	9	8	15	14	13	12	3	2	1	10	9	2	6	13
12	13	14	15	8	9	10	11	4	5	6	7	6	10	7	11
13	12	15	14	9	8	11	10	5	4	7	6	1	7	9	4
14	15	12	13	10	11	8	9	6	7	4	5	2	3	2	12
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	3

Below diagonal  $a + b$ , on or above  $a \times b$ ,  
 $0 + a = a$ ,  $a + a = 0$ ,  $0 \times a = 0$

1. We shall say that two linear codes are *equivalent* if they have the same block-length, rank and minimum distance.

a. Let  $C$  be the Triple Check Code introduced in the lectures, which has check matrix

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

Construct the check matrix of the code  $C'$  obtained from  $C$  by adding an overall parity check bit, so that all words have even weight. [4]

Show that  $C'$  has block length 7 and can correct single bit errors in a word, proving any result from the lectures that you quote. Justifying your conclusion carefully, determine whether  $C'$  is equivalent to the Hamming code  $\text{Ham}(3)$ . [7]

b. Let  $C''$  be the code obtained by puncturing  $\text{Ham}(3)$ , that is by deleting the last entry of all code words of  $\text{Ham}(3)$ . Construct a check matrix for  $C''$ . [4]

Find the rank and minimum distance of  $C''$ . Is  $C''$  equivalent to the Triple Check Code? [5]

2. Construct, with justification, a binary linear code of block length 16, minimum distance 4 and largest possible rank, by producing generator and check matrices. What is the rank? construction: [8]  
justification: [8]

Show that your code can correct single bit errors in a block and simultaneously detect double bit errors. [4]

3. The field  $\text{GF}(5)$  consists of the integers  $0, \dots, 4$  with addition and multiplication modulo 5. Find an irreducible polynomial of degree 2 over  $\text{GF}(5)$ , explaining why it is irreducible. [7]

Explain how your polynomial can be used to turn the set of polynomials  $ax + b$  with  $a, b \in \text{GF}(5)$  into a field  $F$ , giving a brief explanation how to perform each of the four operations in  $F$ . [7]

Perform the following calculations in your field:

add  $3x + 2$  and  $2x + 1$ ; [1]

multiply  $2x + 1$  by  $4x + 1$ ; [2]

divide  $4x + 1$  by  $x + 3$ . [3]

4. Define the characteristic of a finite field and prove that it is a prime number. [4]

Prove that in a field of characteristic  $p$  the equation  $(a + b)^p = a^p + b^p$  holds for all  $a$  and  $b$ . [4]

Deduce that an element of a field of characteristic  $p$  cannot have more than one  $p$ th root. [4]

Show that if  $F$  is a finite field of characteristic  $p$ , then every element of  $F$  has a  $p$ th root. [4]

Suppose that  $\alpha$  is a primitive element of a field of order 256, find in the form  $\alpha^n$  all the fourth roots of  $\alpha^7$ . [4]

5. Three polynomial codes  $A, B, C$  of block length 15, have generator polynomials as follows:

$$\begin{aligned} A &: x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1 \\ B &: x^{10} + x^9 + x^8 + x^6 + x^4 + x^2 + x + 1 \\ C &: x^9 + x^8 + x^5 + x^4 + x^3 + 1 \end{aligned}$$

For each of  $A$  and  $B$  determine whether the code is cyclic or not. [4 each]

The code  $C$  is cyclic. Find its check polynomial [4]

Determine for each of the following words whether it is a code word of  $C$ .

$$\begin{array}{cccccccccccccccc} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array} \quad [4 \text{ each}]$$

6. The Reed-Solomon Code RS(4, 3) is used to transmit a message. One received word is

$$14 \ 5 \ 8 \ 14 \ 3 \ 8 \ 14 \ 3 \ 8 \ 5 \ 9 \ 14 \ 3 \ 5 \ 6$$

Assuming that no more than three symbol errors occurred find the transmitted code word. [20]

*To shorten the calculation of the roots of the error locator you may verify that they correspond to the positions in which the received symbol is 5.*

