

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING  
EXAMINATIONS 2008

MSc and EEE/ISE PART IV: MEng and ACGI

**CODING THEORY**

Friday, 16 May 10:00 am

Time allowed: 3:00 hours

Corrected Copy

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

**Answer FOUR questions.**

*All questions carry equal marks*

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

Examiners responsible      First Marker(s) :      A.A. Ivanov

Second Marker(s) :      C. Ling

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. Let  $C$  be the code of block length 8 obtained by extending the binary Hamming code  $\text{Ham}(3)$  by an overall parity check bit (so that all code words of  $C$  have even weight).

Determine the rank (dimension)  $k$  and minimum distance  $d$  of  $C$ , and show that, with the exception of  $\underline{0}$  (the all zeros code word) and the  $\underline{1}$  (the all ones code word), all code words of  $C$  have weight  $d$ .

[10]

Deduce that for any pair of code words  $u, v$  of  $C$

$$u \cdot v = \sum_{i=1}^8 u_i v_i = 0.$$

[10]

Hence or otherwise show that for any  $8 \times k$  generator matrix  $G$  for  $C$ , the matrix  $H = G^T$  is a check matrix for  $C$ .

[5]

*You may use the following version of the Rank and Nullity Theorem without proof:*

**Theorem** *If  $G$  is a generator matrix of a code of block length  $n$  and rank  $m$ , then  $G^T$  is a check matrix for a code of block length  $n$  and rank  $n - m$ .*

2. Define the term *r*-perfect code. Define (binary) Hamming codes and show that they are 1-perfect.

[8]

Let  $E$  be a (not necessarily linear) binary code of block length 8, show that if  $E$  can correct all single errors, then it has at most 28 code words.

[4]

Show that there is no binary perfect code of block length 8.

[4]

Show that the code BCH(4,3), which has block length 15, rank  $\geq 3$  and minimum distance at least 7, is not *r*-perfect for any *r*.

[9]

3. Define the characteristic of a finite field and prove that it is a prime number.

[5]

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

[5]

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

[6]

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

[5]

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]

4. Show that a field of characteristic 2 has  $q = 2^n$  elements for some positive integer  $n$ .

[5]

Show that the roots of  $x^q - x$ , where  $q = 2^n$  and the polynomial is considered as an element of  $\mathbb{B}[x]$ , are all distinct.

*If you use a criterion for distinctness of the roots you must prove it*

[6]

Suppose now that  $F$  is a field of characteristic 2 such that  $x^q - x$  splits into linear factors over  $F$ . Show that the roots of  $x^q - x$  form a subfield of  $F$  containing exactly  $q$  elements.

[7]

Use this method to exhibit a field with 4 elements inside  $\text{GF}(16)$ .

[7]

5. Suppose that the triple error correcting Reed-Solomon code  $RS(4,3)$  defined over  $GF(16)$  is being used and the following word is received;

1 2 1 1 2 1 1 2 1 1 2 1 6 8 7

calculate the syndrome polynomial.

[15]

Assuming that at most three errors have occurred find the transmitted code word.

[10]

6. Define the error locator, error evaluator, and syndrome polynomials,  $l(z)$ ,  $w(z)$  and  $s(z)$ , for a received word with respect to a BCH code,  $BCH(k; t)$  (defined using the primitive element  $\alpha$ ) and state the fundamental relation linking these three polynomials.

[5]

Consider the BCH code,  $BCH(4,3)$  defined using the primitive element 2 of the field  $GF(16)$ . Suppose the error pattern of a received word is

1 0 0 0 0 1 0 0 0 0 1 0 0 0 0

calculate the three polynomials and check the validity of the fundamental relation in this case.

[10]

Now suppose that the received word is

1 0 1 1 0 1 1 0 1 1 0 1 1 0 1

Calculate the syndrome polynomial, and explain why the number of bit errors must be at least 4.

[10]