E4.07
C5.23
SO11
ISE4.15

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2006

MSc and EEE/ISE PART IV: MEng and ACGI

Corrected Copy

CODING THEORY

Thursday, 11 May 10:00 am

Time allowed: 3:00 hours

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) :	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. 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: [10]

justification: [10]

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

[5]

2. Let F and E be finite fields, $F \subseteq E$, and let F have q elements. Let β be an element of E. Define the minimal polynomial $mp_\beta(x)$ of β over F.

[5]

Show that it is irreducible, and that $g(\beta) = 0$ for a polynomial $g(x) \in F[x]$ if and only if $mp_\beta(x)$ divides $g(x)$ exactly.

[5]

Show that $F[\beta] = E$ if and only if E has precisely q^d elements where d is the degree of $mp_\beta(x)$.

[5]

The polynomial $x^3 + x + 1$ is irreducible over the binary field $\mathbb{B}$. Let $E = \mathbb{B}[\alpha]$ where α is a root of $x^3 + x + 1$. Show that α is a primitive element of E.

[10]

3. A field F of order 16 is constructed using the irreducible binary polynomial

$$x^4 + x^3 + x^2 + x + 1.$$

We use the convention that a binary polynomial $ax^3 + bx^2 + cx + d$ is represented by the integer whose binary expansion is $abcd$.

Note that the table at the beginning of this paper does not apply to F.

Calculate $9 + 13$ and 9×13 in F from first principles.

[5]

Calculate the powers of 2 up to 2^5 in F and deduce that 2 is not a primitive element of F. Calculate the powers of 3 up to 3^{15} and deduce that 3 is primitive.

[10]

Write down a table of discrete logarithms for F using 3 as a base (you should give $\log 1 = 0$). Use your table to verify the calculation of 9×13 above.

[4]

Using your table or otherwise, represent 3^4 as a sum lower powers of 3 (including 3^0). Show that this is not possible for 3^3 or 3^2 and hence find the minimal polynomial of 3 over the field $\mathbb{B}$ or order 2.

[6]

4. Define the t-error correcting code $BCH(k,t)$ of block length $2^k - 1$, based on the primitive element α by giving its check matrix.

[10]

Show how the generator polynomial is determined from the check matrix. Then explain how the check polynomial is obtained.

[2]

The minimal polynomials for the elements of $GF(16)$ are given in the table below.

Element(s)	Minimal Polynomial
0	x
1	$x+1$
10, 11	x^2+x+1
6, 7, 12, 13	x^4+x+1
2, 4, 9, 14	x^4+x^3+1
3, 5, 8, 15	$x^4+x^3+x^2+x+1$

Using this, and the table for $GF(16)$, show that the codes $BCH(4,3)$ based on $\alpha = 2, 4, 9,$ and 14 are identical, but that the code $BCH(4,3)$ based on $\alpha = 7$ is distinct from these.

[5]

Use your check polynomials for the two distinct codes to determine whether

10000 10100 11011

lies in either of them.

[8]

5. Suppose that in $BCH(4,3)$ (based on the primitive element $2 \in GF(16)$) a received word v has error pattern

$$1\,0\,0\,0\,0\;\;0\,1\,0\,0\,0\;\;0\,0\,1\,0\,0.$$

Define and calculate the error locator, error evaluator and syndrome polynomials of v.

[10]

Write down the fundamental equation linking these polynomials in general and verify that your calculated examples satisfy it.

[10]

State the properties of the error locator, and evaluator polynomials from which it follows that they are determined by the syndrome polynomial (*You do not need to supply the proof itself*).

[5]

6. The field $GF(5)$ consists of the integers $0, 1, ..., 4$ with addition and multiplication modulo 5. Find an irreducible polynomial of degree 2 over $GF(5)$, explaining why it is irreducible.

[9]

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

[8]

Perform the following calculations in your field:

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

[1]

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

[3]

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

[4]

Master

E4.07/ISE4.15/SO11/C5.23

CODING THEORY

SOLUTIONS 2006

SOLUTION 1

Since the code has minimum distance ≥ 3 the columns of its check matrix must be distinct and non-zero. If we choose a column size of 4 we can get only 15 distinct non-zero binary columns. So we must use a column length of 5. Thus the maximum possible rank of the code will be 11. all unseen

In order to ensure that the minimum distance is 4 we shall firstly make the columns of the check matrix distinct and non-zero, so that the minimum distance is at least 3, and secondly ensure that all code words have even weight, since then no two can be at distance 3. The easiest way to ensure that all code words have even weight is to make the last bit an overall parity check. Thus the fifth row of the check matrix should be the all 1s row and the 16th column should be $(0,0,0,0,1)^{\mathsf{T}}$. The remaining entries of the matrix should be all possible non-zero columns of length 4. Thus our check matrix is

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

There are two ways of constructing a generator matrix, either will do. The first is to construct code wordes stating with each of the unit vectors e_i of length 11 by using the rows of H to determine each of the check bits in turn. The second is to convert H to standard form A, I_5 by row operations. Then the generator $G = (I_{11}, A^{\top})^{\top}$. Both methods are acceptable and produce

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

Suppose this code is used to correct single bit errors, then it will only attempt to correct words of odd weight. If a word contains two bit errors it will have even weight, and it cannot be a code word since the minimum distance is > 2. Hence the error will be detected.

The candidates can also quote a general result, though if they give no indication why that result holds they will not get all 4 marks.

SOLUTION 2

The minimum polynomial of β is the (monic) polynomial $f(x) \in F[x]$ of least degree such that $f(\beta) = 0$. It is irreducible, for suppose $f(x) = g(x)h(x)$ with $\deg g$, $\deg h < \deg f$. Then by assumption $g(\beta), h(\beta) \neq 0$. But $g(\beta)h(\beta) = f(\beta) = 0$, contradicting the fact that E is a field.

Suppose $g(\beta) = 0$. Then divide g by f in $F[x]$:

$$g(x) = q(x)f(x) + r(x),$$

where $r(x) = 0$ or $\deg r < \deg f$. Now $r(\beta) = g(\beta) - q(\beta)f(\beta) = 0$. Hence the option $\deg(r) < \deg(f)$ is impossible. Thus $g(x) = q(x)f(x)$.

book

Conversely if $g(x) = q(x)f(x)$, then $g(\beta) = q(\beta)f(\beta) = 0$.

$F[\beta]$ consists of the values $g(\beta)$ where g ranges over $F[x]$. From the above $g(\beta) = h(\beta)$ if and only if $f(x)$ exactly divides $g(x) - h(x)$ in $F[x]$. Hence the number of elements in $F[\beta]$ is precisely the number of residues of $mp - \beta(x)$ in $F[x]$. The residues are 0 and all polynomials of degree $< d$ in $F[x]$. Identifying these polynomials with their sequences of coefficients, one sees that there are exactly q^d of them. Hence $|F[\beta]| = q^d$. As $F[\beta] \subseteq E$, they will be equal if they have the same number of elements.

seen

Given the facts above we know that E has 8 elements. Now we calculate the powers of α successively substituting $\alpha^3 = \alpha + 1$ at each step we get

$$1,\, \alpha,\, \alpha^2,\, \alpha+1,\, \alpha^2+\alpha,\, \alpha^2+\alpha+1,\, \alpha^2+1,\, 1,\, \ldots$$

unseen

thus the powers of α cover all the non-zero elements of E and α is primitive.

SOLUTION 3

unseen Addition is ordinary polynomial addition (=XOR) so $9 + 13 = 4$.
To calculate 9×13 we first multiply the polynomials and then calculate the remainder mod $x^4 + x^3 + x^2 + x + 1$. Using binary positional notation we have

$$1001 \times 1101 = 1101 + 1101000 = 1100101.$$

The division goes as follows

```
10011)1100101(101
      11111
      ------
       011001
        11111
       ------
         0110
```

So the product is 6.

Multiplying by 2 is just a left shift in binary so the successive powers of 2 can be calculated by shifting left and subtracting (adding) 11111 corresponding to $x^4 + x^3 + x^2 + x + 1$ if necessary to make the left hand bit zero. This gives the following sequence (starting with $2^0 = 1$)

$$0001,\ 0010,\ 0100,\ 1000,\ 1111,\ 0001$$

unseen Since $2^5 = 1$, 2 is not primitive.

Multiplying by 3 corresponds to a left shift followed by addition of 11111 if necessary followed by addition of the original 4-tuple. This gives the sequence

$$\begin{array}{lllll} 0001, & 0011, & 0101, & 1111, & 1110, \\ 1101, & 1000, & 0111, & 1001, & 0100, \\ 1100, & 1011, & 0010, & 0110, & 1010 \end{array}$$

Since these powers produce in sequence all the elements of the field, 3 is a primitive element. The table of logarithms gives the position (starting at 0) of each non-zero number in this sequence.
unseen

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

From the table 9 has logarithm 8 and 13 has logarithm 5. Their product is thus the number with logarithm $8 + 5 = 13$, which is 6, confirming the calculation above.
unseen

$\frac{5}{10}$

From the table we have $3^0 = 1$, $3^1 = 3$, $3^2 = 5$ and $3^3 = 15$. Certainly $14 = 15 + 1$, but no combination of $1, 3$, and 5 yield 15 and no combination of 1 and 3 yields 5. Thus the 3 is a root of $x^4 + x^3 + 1$ and of no non-zero binary polynomial of lower degree. Hence that is its minimal polynomial over GF(2).

SOLUTION 4

a. The check matrix $H_{k,t}$ of BCH(k,t) with entries in GF(2^k) has $2^k - 1$ columns and t rows. The entry in the (i,j) position is

$$\alpha^{(2^k-j)(2i-1)}.$$

Thus the first row consists of the powers of α in descending order, and the other rows are the odd powers of elements in the first row up to the $2t-1$st power. It follows that a polynomial $f(x)$ represents a code word iff $f(\alpha^r) = 0$ for all odd powers of α up to $r = 2t-1$. Hence the generator polynomial $g(x)$ of the code is the product of the distinct minimal polynomials of these powers. book

The check polynomial $h(x)$ is the product of the remaining irreducible minimal polynomials of non-zero elements of GF(2^k) so that $g(x)h(x) = x^n - 1$, where $n = 2^k - 1$. book

b. The generator polynomial is the product of the distinct minimal polynomials of α, $\alpha^3 = 5$, and $\alpha^5 = 11$. For the $\alpha = 2$, 4, 9, 14 these are $x^4 + x^3 + 1$, $x^4 + x^3 + x^2 + x + 1$, and $x^2 + x + 1$ and their product is

$$g_1(x)x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1.$$

For $\alpha = 7$ they are $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$, and $x^2 + x + 1$ and their product is

$$g_2(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Since $g_1(x)$ is a code word of the first code and not a code word of the second because it is not divisible by $x^4 + x + 1$. The two codes are distinct. unseen

The check polynomial is the product of the remaining minimal polynomials of non-zero elements of GF(16): In the first case:

$$h_1(x) = (x^4 + x + 1)(x + 1) = x^5 + x^4 + x^2 + 1.$$

In the second:

$$h_2(x) = (x^4 + x^3 + 1)(x + 1) = x^5 + x^3 + x + 1.$$

We multiply the test word by the two check polynomials first by $h_1(x)$:

```
          1 0 0 0 0 1 0 1 0 0 1 1 0 1 1
      1 0 0 0 0 1 0 1 0 0 1 1 0 1 1
  1 0 0 0 0 1 0 1 0 0 1 1 0 1 1
1 0 0 0 0 1 0 1 0 0 1 1 0 1 1
---------------------------------------
1 1 0 1 0 0 1 1 0 0 1 0 0 0 1 0 0 1 1 1
```

This is not a multiple of $x^{15}-1$ and so the word does not belong to the first code. unseen

Now we multiply with $h_2(x)$:

$$
\begin{array}{cccccccccccccccccccc}
 & & & & & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
 & & & & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & \\
 & & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & & & \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & & & & & \\
\hline
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1
\end{array}
$$

unseen This is a multiple of $x^{15}-1$ so the word does belong to the second code.

SOLUTION 5

The error locator is $l(z) = \prod(1 - \alpha^i z)$, where α is the element the code is
book based on and i runs over the error locations (counting from the right starting
calculations at 0). In our case this is
unseen

$$(1 - 2^2 z)(1 - 2^8 z)(1 - 2^{14} z) = 5z^3 + 15z^2 + 6z + 1$$

The error evaluator is $w(z) = \sum \alpha^i \prod_{j \neq i}(1 - \alpha^j z)$ where again α is the element the code is based on and i and j run over the error locations. In our case this is

$$4(1 - 2^8 z)(1 - 2^{14} z) + 14(1 - 4z)(1 - 12z) + 12(1 - 4z)(1 - 14z) = 5z^2 + 6$$

The syndrome polynomial is $S(z) = \sum_{i=1}^{2t} S_i z^{i-1}$, where $S_i = v(\alpha^i)$. For the BCH code we have $S_{2i} = S_i^2$ which saves some calculation effort. We have

$$\begin{aligned} S_1 = &\quad 2^{14} + 2^8 + 2^2 = 12 + 14 + 4 &= 6 \\ S_3 = &\quad 8^{14} + 8^8 + 8^2 = 3 + 5 + 15 &= 9 \\ S_5 = &\ 11^{14} + 11^8 + 11^2 = 10 + 10 + 10 &= 10 \end{aligned}$$

So the syndrome polynomial is $14z^5 + 10z^4 + 7z^3 + 9z^2 + 13z + 6$.

book The fundamental equation is $l(z)S(z) \equiv w(z) \bmod z^{2t}$.

We verify this in tabular form (omitting the powers of z.

			14	10	7	9	13	6	×	5	15	6	1
		15	14	11	4	5	13						
	12	2	6	10	4	9							
4	9	2	6	11	7								
4	5	15	0	0	0	5	0	6					

unseen which confirms the congruence.

The properties that ensure that $S(z)$ determines $l(z)$ and $w(z)$ are the following (a) $\deg(w(z) < \deg(l(z) \leq t$, (b) $l(z)$ and $w(z)$ are relatively prime and
book (c) the constant term of $l(z)$ is 1.

We calculate the syndromes of the received word using Horner's scheme

	1	1	1	0	0	1	1	1	0	0	0	0	0	1	1
2	1	3	7	14	5	11.	14	4	8	9	11	15	7	15	6
8	1	9	6	2	9	6	3	0	0	0	0	0	0	1	9
11	1	10	0	0	0	1	10	0	0	0	0	0	0	1	10

$\frac{9}{10}$

These syndromes agree with those of the error pattern above. So this word has the same syndrome polynomial as that error word. As a consequence of the uniqueness of the error locator and evaluator guaranteed by their properties, it follows that the error pattern is the one given at the start of the question.

Thus the corrected word is

$$0\,1\,1\,0\,0\,1\,0\,1\,0\,0\,0\,0\,1\,1\,1$$

$\frac{10}{10}$

SOLUTION 6

Since we can always divide by any non-zero constant we can assume that all polynomials we consider have highest coefficient 1 (ie. that they are *monic*). We write out the products of pairs of monic polynomials of degree 1 and get the following list.

	x	$x+1$	$x+2$	$x+3$	$x+4$
x	x^2	x^2+x	x^2+2x	x^2+3x	x^2+4x
$x+1$	x^2+x	x^2+2x+1	x^2+3x+2	x^2+4x+3	x^2+4
$x+2$	x^2+2x	x^2+3x+2	x^2+4x+4	x^2+1	x^2+x+3
$x+3$	x^2+3x	x^2+4x+3	x^2+1	x^2+x+3	x^2+2x+2
$x+4$	x^2+4x	x^2+4	x^2+x+3	x^2+2x+1	x^2+3x+1

Any of the monic quadratic polynomials absent from this list will do (as it is not a product of polynomials of lower degree). For instance, we can choose
All Unseen x^2+x+1.

Now we add and subtract polynomials of degree one in the normal way by adding and subtracting their coefficients mod 5, but in multiplying we substitute $x^2 = -x-1$. To find the inverse of a polynomial $ax+b$ we divide x^2+x+1 by $ax+b$ obtaining an equation

$$x^2+x+1 = (cx+d)(ax+b)+e$$

then division by $ax+b$ is multiplication by $-(cx+d)/e$.

$$(3x+2)+(2x+1) = 3$$

$$(2x+1)(4x+1) = 3x+3$$

$$(4x+1)/(x+3) = 3x+3$$

(By a fluke, $(2x+1)(x+3) = 2x^2+2x+3 \equiv 1$).