IMPERIAL COLLEGE LONDON

E4.07
SO11
ISE4.15

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2004

MSc and EEE/ISE PART IV: MEng and ACGI

CODING THEORY

Friday, 14 May 10:00 am

Time allowed: 3:00 hours

There are SIX questions on this paper.

Answer FOUR questions.

Corrected Copy

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. Let C be the code of block length 8 obtained by extending the binary Hamming code 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 ≥ 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 pth root.

[6]

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

[5]

Suppose that α is a primitive element of a field of order 256, find in the form α^n all the fourth roots of a^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 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 α) 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]

SOLUTIONS - CODING THEORY 2004

E4.07 | IE 4.15 | S011

SOLUTION 1

The code Ham(3) has as its check matrix the 3×7 matrix whose columns are all possible non-zero binary triples. Hence it has block length 7, rank 4, and since it can correct all single errors minimum distance at least 3. Since theren are code words of weight 3, that is the precise minimum distance.

Adding a check bit increases the block length to 8, and it leaves the rank unchanged (as the number of code words is unchanged). Since a word of weight 3 becomes a word of weight 4, the minimum distance goes up to 4.

5 unseen

The zero word and the all 1s word are code words of Ham(3) and hence the same holds for the extended zero and all 1s word. Any other word of the code must have at least 4 1s (so that its distance from $\underline{0}$ is 4 and at least 4 zeros so that its distance from the all 1s word is at least 4. Thus it must have exactly 4 1s.

5 unseen

As every codeword has even weight by construction it follows immediately that $u \cdot u = 0$. It also follows immediately that for any code word $u \neq \underline{0}, \underline{1}$ both $u \cdot \underline{0}$ and $u \cdot \underline{1}$ are 0 (the first is the sum of 8 0s and the second is the sum of 4 1s and 4 0s). Now suppose that both u and $v \neq u$ have weight 4. They must differ in four places because their difference is a code word $\neq \underline{01}$. Since they both have weight 4 the number of 1s in u corresponding to 0s in v must be exactly equal to the number of 0s in u corresponding to 1s in v. Hence exactly two 1s of u become 0s in v. Thus $u \cdot v$ is the sum of two 1s which is 0.

10 unssen

Now let G be any generator matrix and let $H = G^{\mathsf{T}}$. the rows of H are code words of C and by the argument we have just given it follows that $Hv = \underline{0}$ for all $v \in C$. So C is contained in the code C' with check matrix H, but by the theorem rank $C' = 4 =$ rank C and so the codes must be equal.

5 unseen

2/6

SOLUTION 2

A code is *r–perfect* if every received word lies with Hamming distance r of exactly one code word.

The code Ham(k) has as its check matrix a binary $k \times 2^k - 1$ matrix whose columns are all non-zero binary k–tuples, each occurring once. A received word has syndrome $\underline{0}$ or its syndrome is equal to a unique column of the check matrix. In the first case it is a code word. In the second changing the bit corresponding to the column equal to its syndrome produces a code word. Changing any other bit adds the corresponding column to the syndrome, which therefore does not become $\underline{0}$. That means it does not produce a code word. Thus every non-code word is at distance 1 from a unique code word and Ham(k) is perfect.

8 seen

For block length 8 the number $N_1 = 1 + 8 = 9$. If a code C of block length 8 can correct single errors, then the disks of Hamming radius 1 around code words must be disjoint. So

$$|C|\, 9 \leq 2^8 = 256.$$

4 unseen

Hence $|C| \leq 256/9 < 29$. Thus $|C| \leq 28$.

The disks of radius 1, 2 and 3 about code words of block length 8 contain 9, $9 + 4 \times 7 = 37$ and $37 + 4 \times 7 \times 2 = 93$ words. None of these numbers exactly divide 256 and therefore there cannot be r–perfect codes for $r = 1, 2, 3$. The greatest possible distance between words in $\mathbb{B}^8$ is 8 and so disks of radius ≥ 4 cannot be disjoint. Therefore there are no r–perfect codes for $r \geq 4$.

4 unseen

If BCH(4,3) were r–perfect, r would have to be at least 3. Let N_r denote the number of words at distance at most r from a code word. For an r–perfect binary linear code C of block length 15 we must have $|C|\, N_k = 2^{15}$ and if the code has rank m, then $|C| = 2^m$. Hence N_r must be 2^{15-m}. Now

$$N_r = 1 + 15 + \binom{15}{2} + \cdots + \binom{15}{r}. \qquad (*)$$

Calculating this value for successive values of r starting with $r = 3$ we get

$$N_3 = 576,\ N_4 = 1941, N_5 = 4946, \ldots$$

6 unseen

None of these are powers of 2, and the last is greater than $2^{15-3} = 2^{12}$. Therefore BCH(4,3) cannot be perfect.

3/1

SOLUTION 3

5 book

The characteristic of a finite field is the smallest number of times that 1 *must be added to itself to produce* 0. *We denote the sum of* n *copies of* 1 *by* $n \circ 1$. *The distributive law implies that* $(m \circ 1)(n \circ 1) = (mn) \circ 1$. *Let* p *be the smallest positive number such that* $p \circ 1 = 0$. *If* $p = mn$ *with* $m, n < p$ *then* $0 = (m \circ 1)(n \circ 1$. *so one of* $m \circ 1$ *and* $n \circ 1$ *must be zero, contradicting the minimality of* p. *Hence* p *has no proper factors and is prime..*

3 book

First note that $p \cdot a = (p \cdot 1)a = 0 \cdot a = 0$. *Next, observe that the binomial theorem allows us to calculate* $(a+b)^p$*:*

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p}b^p.$$

But the formula $\binom{p}{k} = p!/(k!(p-k)!)$ *shows that for* $k \neq 0, p$, $\binom{p}{k}$ *is a multiple of* p. *So all the middle terms of the expansion are 0. Hence* $(a+b)^p = a^p + b^p$.

6 unseen

Suppose that $x^p = y^p = a$. *Then* $x^p - y^p = 0$. *If the characteristic* p *is odd, then* $-y^p = (-y)^p$. *If it is* 2. *then* $-y^p = y^p = (-y)^p$. *In either case we have* $x^p + (-y)^p = 0$ *Hence* $(x + (-y))^p = 0$ *and so* $x - y = 0$ *or* $x = y$. *Thus* a *has at most one* p*th root.*

5 unseen

Consider the p*th powers od the elements of* F. *By what has been just shown they are all distinct and there are exactly* $|F|$ *of them, hence every element of* F *must occur as a* p*th power and so they all have* p*th roots.*

4 unseen

Since square roots are unique and exist, there is exactly one fourth root of any field element in GF(256). *We need to find* n *so that* $4n \equiv 7 \pmod{255}$. *The unique answer is* $n \equiv 193 \pmod{255}$, *which can be found by trial and error or using Euclid's algorithm.*

4/6

SOLUTION 4

F is a vector space over its prime field $\mathbb{B}$. *If F is finite, then the dimension of this space must be finite. Now every vector in a vector space of dimension n over the field* $\mathbb{B}$ *can be represented by a coordinate sequence* $(x_1, \ldots, x_n)$ *and every such sequence determines a unique vector. So the number of vectors is the same as the number of coordinate sequences. We know* $\mathbb{B}$ *has 2 elements.* 8 book *So there are exactly* 2^n *coordinate sequences* $(x_1, \ldots, x_n)$ *with entries in* $\mathbb{B}$.

It is possible to solve the second part using a book work criterion involving the derivative of the polynomial. Here is a neater direct solution.
Let α *be a root of* $x^q - x$. *Then* $(x-\alpha)^q = x^q - \alpha^q = x^q - \alpha$ *since q is a power of the characteristic 2. Thus*

$$\begin{aligned} x^q - x &= (x^q - \alpha) - (x - \alpha) \\ &= (x-\alpha)^q - (x-\alpha) \\ &= (x-\alpha)((x-\alpha)^{q-1} - 1). \end{aligned}$$

8 *Since* α *does not divide the second term, it is not a multiple root of* $x^q - x$.

By the second part there are exactly q roots, so the number of elements is correct. We must show that the set of roots is closed under addition, multiplication, and taking inverses (negatives is unnecessary in characteristic 2). If $\alpha^q = \alpha$ *and* $\beta^q = \beta$ *then* $(\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$ *and* $(\alpha^{-1})^q = (\alpha^q)^{-1} = \alpha^{-1}$. *For addition we use the result of question 3 and find that* $(\alpha+\beta)^q = \alpha^q + \beta^q = \alpha+\beta$. 5 book *So closure holds and the set forms a field.*

The roots of $x^4 - x$ *in* GF(16) *are* 0, 1, 10, 11 *(by inspection. So by the previous result, they form a field of order* 4. 4/ unseen

5/1

SOLUTION 5

Received Word: 1 2 1 1 2 1 1 2 1 1 2 1 6 8 7
Syndrome Calculation:

5 seen

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

Syndrome Polynomial: 13 7 11 6 8 14
Euclid's Algorithm:

10 seen

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

Error Locator: 9 3 12 10.
Horner's scheme: (only rows corresponding to roots of locator shown)

	9	3	12	10
2:	9	8	5	0
4:	9	12	14	0
8:	9	4	7	0

10 unseen

Roots: 2 4 8
Error Locations: 14 13 12
Error Evaluator/x: 1 1 8
Evaluated: 2: 14, 4: 5, 8: 15
Derivative of Error Locator: 2: 3, 4: 2, 8: 6
Error Values: 13 14 14
Corrected Word:12 12 15 1 2 1 1 2 1 1 2 1 6 8 7

6/1

SOLUTION 6

Transmitted Codeword	:	$c(x) = c_m x^m + \cdots + c_0$
Received Word	:	$d(x) = d_m x^m + \cdots + d_0$
Error Word	:	$d(x) - c(x) = e(x) = e_m x^m + \cdots + e_0$
Error Positions	:	$M = \{i : e_i \neq 0\},$
	:	$s = \lvert M \rvert \leq t$
Error Locator Polynomial	:	$l(z) = \prod_{i \in M} (1 - \alpha^i z)$
This has roots	:	$\{\alpha^{-i} : i \in M\}$
Error Evaluator Polynomial	:	$w(z) = \sum_{i \in M} e_i \alpha^i \prod_{j \in M \setminus i} (1 - \alpha^j z)$
Syndromes	:	$d(\alpha^i) = e(\alpha^i) = S_i$ for $i = 1, \ldots, 2t$
Syndrome Polynomial	:	$s(z) = \sum_{i=1}^{2t} S_i z^{i-1}$
Fundamental Equation	:	$l(z)s(z) \equiv w(z) \pmod{z^2 t}.$

5 book

Error Pattern: 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0. Syndrome Calculation:

	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0
2:	1	2	4	8	9	10	13	3	6	12	0	0	0	0	0
8:	1	8	15	5	3	0	0	0	0	0	1	8	15	5	3
11:	1	11	10	1	11	11	10	1	11	10	0	0	0	0	0

Thus $S_1 = 0$ and so $S_2 = S_4 = 0$. $S_3 = 3$ and so $S_6 = 3^2 = 5$, $S_5 = 0$. Syndrome Polynomial: $s(z) = 5z^5 + 3z^2$. The error locations are 14, 9 and 4. Hence the error locator is

$$(1 - 14z)(1 - 9z)(1 - 4z) = 3z^3 + 1.$$

The error evaluator is

$$14(1 - 9z)(1 - 4z) + 9(1 - 14z)(1 - 4z) + 4(1 - 14z)(1 - 9z) = 3z^2$$

10 unseen

Verifying the fundamental equation gives:

$$l(z)s(z) = (3z^3 + 1)(5z^5 + 3z^2) = 15z^8 + 3z^2 \equiv w(z) \pmod{z^6}.$$

Received word: 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1.
Syndrome calculation:

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

10

5 unseen

The syndrome polynomial is $s(z) = 11z^4$. This divides z^6 and $l(z)s(z)$ will be a multiple of z^4 for any polynomial $l(z)$. So it is impossible for the fundamenal equation to hold. Hence there must be more than 3 errors.