E4.07
C5.23
SO11
ISE4.15

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2007

MSc and EEE/ISE PART IV: MEng and ACGI

CODING THEORY

Corrected Copy

Friday, 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

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 length, rank and minimal distance.

a. Let C be the triple check code with the check matrix

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

Construct the check matrix of the code C' obtained from C by adding an overall parity check bit.

[5]

Show that C' has length 7 and can correct single bit errors. Justifying your conclusion carefully, determine whether C' is equivalent to the Hamming code $Ham(3)$.

[10]

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

[5]

Find the rank and minimal distance of C''. Is C'' equivalent to the Triple Check Code?

[5]

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 length 8, show that if E can correct all single errors, then it has at most 28 code words. Show that there is no binary perfect code of length 8.

[10]

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

[7]

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 equality $(a+b)^p = a^p + b^p$ holds for every a and b.

[5]

Deduce that an element of a field of characteristic p cannot have more that 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 α^7.

[4]

4. The field $E = GF(16)$ given by the table at the beginning of the paper contains a subfield F of order 4 consisting of the elements $\{0, 1, 10, 11\}$. Show that it does not contain a subfield of order 8, proving any theoretical results that you use.

[9]

Now show that for any element β of E the elements β and β^4 have the same minimal polynomial over F.

[6]

Hence or otherwise determine the minimal polynomials of all the elements of E over F.

[10]

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

$$A : x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

$$B : x^{10} + x^9 + x^8 + x^6 + x^4 + x^2 + x + 1$$

$$C : x^9 + x^8 + x^5 + x^4 + x^3 + 1$$

For each A and B determine whether the code is cyclic or not.

[5 each]

The code C is cyclic. Find its check polynomial.

[5]

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

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

[5 each]

6. Find the generator and check polynomials for the Reed-Solomon Code $RS(4,4)$ based on the primitive element $2 \in GF(16)$.

[12]

State the rank r and the minimal distance d of the code.

[3]

Find a code word of weight d.

[5]

What is the code word that starts with the sequence $1, ..., r$, where r is defined above?

[5]

E407/IH 4.15/

CODING THEORY 2007 . 5011/C5.23

SOLUTION 1

a. If a code word ends with k check bits, then the rows of the check matrix of a code correspond to the equations determining the check bits. and the final k columns give the coefficients of the check bits in these equations. So the check matrix of C' is

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

All unseen

There are other valid check matrices, and they will be accepted, but this is the one the candidates are most likely to produce.

The block length is the length of the words in the code. Since they satisfy $H'u = \underline{0}$, that must be 7.

Any single bit error will produce a syndrome equal to the column of the check matrix H' corresponding to its location. As these are all distinct and non-zero. The code will detect both the presence of such an error and its location. So the code can correct single bit errors.
Some candidates may quote the result from the lectures that a binary code with check matrix with distinct non-zero columns can correct single errors. They should then prove it along the lines given above.

As the rank of H' is 4 (its rows are independent), the rank of the code C' is $7 - 4 = 3$. Ham(3) has rank 4. So the codes are not equivalent.

b. By the same argument as in part (a) we obtain the check matrix H'' of C'' by stripping the last column and last row from the standard form check matrix H_3 of Ham(3).

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad H'' = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

It is important that the matrix H_3 is chosen in standard form, but I shall not penalize candidates for not stating that.

The block length of this code is 6, and since H'' has rank 2, the rank of C'' is $6 - 2 = 4$. Since the columns of H'' are all non-zero the code csan detect single bit errors, but as the second and last column are equal, it cannot determine their location. Hence the code has minimum distance 2, and is not equivalent to the Triple Check Code.

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
seen and Ham(k) is perfect.

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

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

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
unseen cannot be disjoint. Therefore there are no r–perfect codes for $r \geq 4$.

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

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

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

SOLUTION 3

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..*

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 $(a+b)^p = a^p + b^p$.

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 pth root.*

unseen *Consider the pth 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 pth power and so they all have pth roots.*

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.*

4/8

SOLUTION 4

book
unseen

There are several ways to show that there is no field of subfield of order 8. The first is to use the theoretical result that if $F \subseteq E$ for a pair of finite fields then $|E| = |F|^n$ for some n. That is proved by noting that E must be a vector space over F and since it is finite it mustt be finite-dimensional. If its dimension is n then the elements of E correspond to n-tuples of elements of F of which there are $|F|^n$. Thus since $16 \neq 8^n$ for any n there is no subfield of order 8.

A second possibility is to note that the elements 2, 4, 9, 14, 6, 7, 12, 14 are all primitive in the sense that their powers cover all the non-zero elements of the field (that follows because their logarithms given in the table are relatively prime to 15). Hence a field of order 8 cannot contain any of these elements. Thus it must consist of $\{0, 1, 10, 11, 3, 5, 8, 15\}$. But $1 + 3 = 2$ so this set is not closed under addition and so is not a field.
Any valid argument will be accepted.

seen

For the second part we first note that the elements $a \in (F$ satisfy $a^4 = a$ either by direct calculation or from Fermat's Theorem. Hence, since in fields of characteristic 2 $(a + b)^2 = a^2 + b^2$it follows thatif $f(x) \in F[x]$ we have $f(x)^4 = f(x^4)$. Hence $f(\beta) = 0$ iff $f(\beta^4) = 0$.

The minimal polynomial for $\beta \notin F$ is then obtained as $(x - \beta)(x - \beta^4)$ and we get the following list:

unseen

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

These are the minimal polynomials because elements outside F cannot be roots of polynomials in $F[x]$ of degree 1.

SOLUTION 5

The codes are cyclic if and only if their generator polynomials divide $x^{15} - 1$. For the first two codes we do not need to know the quotient. The division
all unseen proceeds as follows

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

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

So this Code A is cyclic while Code B is not. For Code C the quotient will be the check polynomial so the calculation proceeds as follows:

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

So the check polynomial is $x^6 + x^5 + x^4 + x^3 + 1$. To check the words we multiply them by the check polynomial.

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

1	0	1	1	0	1	1	0	1	0	0	1	1	0	0					
	1	0	1	1	0	1	1	0	1	0	0	1	1	0	0				
		1	0	1	1	0	1	1	0	1	0	0	1	1	0	0			
			1	0	1	1	0	1	1	0	1	0	0	1	1	0	0		
						1	0	1	1	0	1	1	0	1	0	0	1	1	0	0
1	1	0	1	0	1	0	0	0	1	1	1	1	0	1	1	0	1	1	0	0.

So the first word is a code word and the second is not.

7/8

SOLUTION 6

The generator is $g(x) = \prod_{k=1}^{8}(x - 2^k)$ and the check polynomial is $h(x) = \prod_{k=9}^{15}(x - 2^k)$. These two polynomials have product $g(x)h(x) = x^{15} - 1$, so it is possible to calculate one and determine the other by division. We shall
definitions determine both by straight multiplication, starting with $g(x)$.
book
calculations
unseen

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

So $g(x) = x^8 + 10x^7 + 2x^6 + 14x^5 + 9x^4 + 4x^3 + 9x^2 + 7x + 15$.

The check polynomial is found similarly.

					1	5	×	1	10
				1	15	9	×	1	13
			1	2	13	1	×	1	3
		1	1	11	15	3	×	1	6
	1	7	13	7	10	10	×	1	12
1	11	2	13	5	15	5	×	1	1
1	10	9	15	8	10	10	5		

So the check polynomial is $h(x) = x^7 + 10x^6 + 9x^5 + 15x^4 + 8x^3 + 10x^+10x + 5$ (*one can check that the polynomials multiply to* $x^{15} + 1$ *but that has not been asked for*).

It follows that the rank of the code is 7, its minimum distance is 9.

unseen Since $g(x)$ represents a code word a code word of weight 9 is

0 0 0 0 0 0 1 10 2 14 9 4 9 7 15

To find a code word beginning (1 2 3 4 5 6 7) we extend this message by zeros,
unseen divide by the generator an add the resulting remainder

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

Therefore the codeword is

1 2 3 4 5 6 7 5 0 7 5 5 3 1 6