O P marked from this copy.

Imperial College London

MSc EXAMINATION (COMMUNICATIONS or MATHEMATICS) 2003

E4.07/SO11/SE4.15 Coding Theory

DATE: Thursday 3rd May(?) 2003 2003 TIME: 10 am - 1 pm

There are SIX questions on the paper.

Answer **FOUR** *questions*

A table of the field of order sixteen for use in your calculations is provided at the start of the paper

E4.07/SO11/SE4.15: 3 Pages

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 Ham(3). [7]

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''. [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 GF(5) consists of the integers $0, \ldots, 4$ with addition and multiplication modulo 5. Find an irreducible polynomial of degree 2 over 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, $b \in$ 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 pth root. [4]

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

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]

5. Three polynomial codes A, B, C of block 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 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.

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 [4 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 occured 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.

E4 07

1f9 ISE 4·15

J011

Coding Theory 2003

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

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

There are other valid check matrices, and they will be accepted, but this is the All unseen *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

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. all unseen Thus the maximum possible rank of the code will be 11.

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 3

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 $-(cx+d)/e$.

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

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

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

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

SOLUTION 4

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

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. unseen

SOLUTION 5

all unseen

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 proceeds as follows

$$\begin{array}{cccccccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\
1&0&1&0&0&1&1&0&1&1&1&&&&& \\ \hline
&&1&0&0&1&1&0&1&1&1&0&0&0&0&1 \\
&&1&0&1&0&0&1&1&0&1&1&1&&& \\ \hline
&&&&1&1&1&1&0&1&0&1&1&0&0&1 \\
&&&&1&0&1&0&0&1&1&0&1&1&1& \\ \hline
&&&&&1&0&1&0&0&1&1&0&1&1&1 \\
&&&&&1&0&1&0&0&1&1&0&1&1&1.
\end{array}$$

$$\begin{array}{cccccccccccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\
1&1&1&0&1&0&1&0&1&1&1&&&&& \\ \hline
&1&1&0&1&0&1&0&1&1&1&0&0&0&0&1 \\
&1&1&1&0&1&0&1&0&1&1&1&&&& \\ \hline
&&&1&1&1&1&1&1&0&0&1&0&0&0&1 \\
&&&1&1&1&0&1&0&1&0&1&1&1&& \\ \hline
&&&&&&1&0&1&1&0&0&1&1&0&1.
\end{array}$$

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:

$$\begin{array}{ccccccc|cccccccccccccccc}
&&&&&&&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\
1&0&0&0&0&0&0&1&1&0&0&1&1&1&0&0&1&&&&&& \\ \hline
&&&&&&&&1&0&0&1&1&1&0&0&1&0&0&0&0&0&1 \\
&1&0&0&0&0&0&&1&1&0&0&1&1&1&0&0&1&&&&& \\ \hline
&&&&&&&&&1&0&1&0&0&1&0&1&1&0&0&0&0&1 \\
&&1&0&0&0&0&&&1&1&0&0&1&1&1&0&0&1&&&& \\ \hline
&&&&&&&&&&1&1&0&1&0&1&1&1&1&0&0&0&1 \\
&&&1&0&0&0&&&&1&1&0&0&1&1&1&0&0&1&&& \\ \hline
&&&&&&&&&&&&&1&1&0&0&1&1&1&0&0&1 \\
&&&&&&1&&&&&&&1&1&0&0&1&1&1&0&0&1
\end{array}$$

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.

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

$$\begin{array}{ccccccccccccccccccccc}
1&0&1&1&0&1&1&0&1&0&0&1&1&0&0&&&&&& \\
&1&0&1&1&0&1&1&0&1&0&0&1&1&0&0&&&&& \\
&&1&0&1&1&0&1&1&0&1&0&0&1&1&0&0&&&& \\
&&&1&0&1&1&0&1&1&0&1&0&0&1&1&0&0&&& \\
&&&&&&1&0&1&1&0&1&1&0&1&0&0&1&1&0&0 \\
\hline
1&1&0&1&0&1&0&0&0&1&1&1&1&0&1&1&0&1&1&0&0.
\end{array}$$

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

SOLUTION 6

Received Word:

14 5 8 14 3 8 14 3 8 5 9 14 3 5 6

all unseen

Syndrome Calculation:

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

Syndrome Polynomial:

11 3 5 4 11 13

Euclid's Algorithm:

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

Error Locator and Evaluator:

Locator(V): 2 4 8 3 Evaluator(Rem): 4 8 14

Locations are counted from the right starting with 0. The root β of the error locator corresponding to location k is determined by $k = 15 - \log(\beta)$. Roots of error locator (only those locations with entry 5):

	2	4	8	3
4 :	2	12	10	0
10 :	2	9	4	0
12 :	2	5	6	0

Error Locations:

$$15 - \log(4) = 13 \ 15 - \log(10 = 5 \ 15 - \log(12) = 1$$

Error Evaluator:

	4	8	14
4 :	4	1	10
10 :	4	11	15
12 :	4	10	11

Derivatives of Error Locator:

	2	4	8	3
4 :	2	12	10	0
	2	4	3	
10 :	2	9	4	0
	2	4	7	
12 :	2	5	6	0
	2	4	4	

Error Values:

$$10/3 = 6 \ 15/7 = 12 \ 11/4 = 8$$

Corrected Word:

14 3 8 14 3 8 14 3 8 9 9 14 3 13 6