Paper Number(s): **E4.07**
SO11
ISE4.15

IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE
UNIVERSITY OF LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2002

MSc and EEE/ISE PART IV: M.Eng. and ACGI

CODING THEORY

Thursday, 2 May 10:00 am

There are SIX questions on this paper.

Answer FOUR questions.

Corrected Copy

Time allowed: 3:00 hours

Examiners responsible:

First Marker(s): Pretzel,O.R.L.

Second Marker(s): Manikas,A.

Special instructions for invigilators: None

Information for candidates:

A table of the field of order ~~12~~ 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 binary linear code with generator matrix

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

Construct a check matrix H for C, stating the definition of a check matrix and proving that your matrix satisfies the conditions of the definition. [5]

Using the check matrix or otherwise find the block length, rank and minimum distance of the code. [7]

Show that the code can correct single errors and simultaneously detect double errors in a block. *If you quote a result that derives this from the minimum distance, you must prove that result.* [5]

Suppose a syndrome/coset leader error correcting table is set up for the code. How many distinct error patterns of weight > 1 will the table correct? [3]

2. Define the term *r–perfect code.* Define (binary) Hamming codes and show that they are 1–perfect. [6]

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. Show that there is no binary perfect code of block length 8. [9]

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. [5]

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. [4]

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. [8]

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

Using your table or otherwise, represent 3^4 as a sum of 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 $\mathbb{B}$ of order 2. [5]

4. Define a *burst* error. Suppose that C is a code of block length n and (odd) minimum distance d. Describe the process of r-fold interleaving and derive from d and r a bound b such that all bursts of length $< b$ can be corrected, but some bursts of length b cannot. [7]

Let $C(k,t)$ be a code defined over GF(2^k) with block length $2^k - 1$ and rank $2^k - 2t - 1$ and minimum distance $2t + 1$. Considering the elements of GF(2^k) as binary k–tuples, calculate the length of the shortest binary burst error that $C(k,t)$ may not be able to correct. [5]

It is proposed to interleave $C(k,t)$ t times in order to improve its burst error capability. What is the shortest burst this interleaved code may not be able to correct? Is the proposal sensible? [4]

In audio CDs a variant form of interleaving is employed. Let the transmitted code words be c_1, c_2, ..., where $c_i = (c_{i1}, \ldots, c_{in})$ (so the block length is n). Then the k–th interleaved block is $(c_{k-1,1}, \ldots, c_{k-n,n})$. Find a bound b', such that all bursts of length $< b'$ can be corrected but some bursts of length b' cannot be corrected when this kind of interleaving is applied to a binary code of block length n and minimum distance d. [4]

5. Suppose that in $BCH(4,3)$ (based on the primitive element $2 \in \mathrm{GF}(16)$) 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. Write down the fundamental equation linking these polynomials in general and verify that your calculated examples satisfy it. [12]

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*). [2]

Correct the following received word:

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

You need not use the full standard algorithm, but in that case you must justify what you do. [6]

6. Find the generator and check polynomials for the Reed-Solomon Code RS(4,4) based on the primitive element $2 \in \mathrm{GF}(16)$. [10]

State the rank r and minimum distance d of the code. [2]

Find a code word of weight d. [4]

What is the code word that starts with the sequence $1, \ldots, r$, where r is defined above? [4]

(Master Solutions)

CODING THEORY 2002

E4.17
SO11
ISE 4.15

1/9

SOLUTION 1

A check matrix is a matrix H such that $Hu = \underline{0}$ if and only if $u \in C$. A possible check matrix is

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

If G is written in standard form as $\begin{pmatrix} I \\ A \end{pmatrix}$ then $H = (A, I)$. For a word v of length 4, $HGv = IAv + AIv = \underline{0}$. Since every code word u has the form Gv, it follows that $Hu = \underline{0}$. Conversely suppose that $w = (x, y)^\top$ is a word, where the constituents x and y have length 4. Then w is a code word if and only if $y = Ax$. If w is not a code word, then $Hw = Ax + Iy$ and $Iy = y \neq Ax$. Therefore $Ax + Iy \neq \underline{0}$.

Application of known book

The matrix G has 8 rows and 4 linearly independent columns. Hence the code has block length 8 and rank 4

unseen

There are obviously code words of weight 4 (for instance any of the columns of G). So the minimum distance of C is at most 4. On the other hand the columns of H have weight 1 or weight 3. It is not possible for the sum of two columns of weight 1 to have either weight 1 or weight 3 so any set of three dependent columns must have at least two columns of weight 3. But again the sum of two columns of weight 3 must have even weight, so it cannot have weight 1 or weight 3. Hence any three columns or less of H are linearly independent.

An error pattern of weight at most three will therefore produce a non-zero syndrome. Hence the code has minimum distance at least 4.

unseen

The syndromes of single errors are the columns of H. A double error will produce a syndrome equal to the sum of two columns of H. As we have just seen these two types of syndrome must be distinct. So the code can correct single errors (by correcting the bit corresponding to the column that is equal to the syndrome), and will still detect double errors.

unseen

Candidates may quote a result from the lectures that a code can correct all error patterns of weight $\leq t$ and simultaneously detect all error patterns of weight $\leq t + k$ if and only if its minimum distance is greater than $2t + k$. If so, they must provide a proof. That was set as an exercise in the course.

The number of syndromes in the decoding table is $2^4 = 16$. Distinct words of weight 1 must lie in distinct cosets (since their difference has weight 2 and is thus not a code word). Therefore 8 syndromes correspond to error patterns of weight 1 (*or observe that these are the columns of H*). There is an additional syndrome $\underline{0}$ corresponding to code words. So 7 syndromes correspond to error patterns of weight greater than 1.

unseen 4

2/9

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

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

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

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)
unseen of each non-zero number in this sequence.

	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
unseen calculation above.

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).

5/9

SOLUTION 4

A burst error is a sequence of k bits of a received word, such that the the errors in the word lie inside this sequence.

r-fold interleaving of a block code consists of rearranging r consecutive code words into blocks of length r such that the i–th block consists of the i–th entries of the code words.

If the number of entries in the burst that come from any code word is at most $(d-1)/2$, then the code will be able to correct all errors. But in some cases, at least, more errors will not be correctable. In order that $(d-1)/2+1$ errors come from the same transmitted code word the burst must intersect that number of interleaved blocks. A burst of length rk has at most k bits from any code word, but some bursts of length $rk+1$ have $k=1$ bits from some code words. So the smallest length for which there exist uncorrectable bursts is $b = r(d-1)/2+1$
Seen in relation to codes correcting t errors rather than the minimum distance

The code correct all error patterns of weight t or less (over GF(2^k)), but not all error patterns of weight $t+1$. For a binary burst to intersect at least $t+1$ entries, it need only have one entry in each of the end blocks, but it must completely cover all the others. Thus the shortest length b such that some errors of length b are not correctable is $k(t-1)+2$.
Seen in relation to Reed-Solomon codes (which have exactly these parameters).

The shortest GF(2^k)–burst the interleaved code may not be able to correct has length t^2+1 by the first part. The shortest binary burst that affects t^2+1 is $k(t^2-1)+2$ by the second. The proposal almost increases the burst capability
unseen by a factor of $t+1$, which is very reasonable.

As in the 'standard' interleaving method we must determine how long a burst must be if it affects more than $(d-1)/2$ bits in a code word. Since each interleaved block contains bits from different code words, the burst must affect more than $n(d-1)/2$ interleaved blocks. So we find precisely the same bound
unseen $b' = n(d-1)/2+1$ as in the standard case with n-fold interleaving.

SOLUTION 5

Definition 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

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

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

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

8/9

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  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