EE4-07
EE9SO11

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2012

MSc and EEE/ISE PART IV: MEng and ACGI

Corrected Copy

CD

CODING THEORY

Monday, 14 May 10:00 am

Time allowed: 3:00 hours

There are FIVE questions on this paper.

Answer ALL questions.

All the questions carry equal marks.

Any special instructions for invigilators and information for candidates are on page 1.

Examiners responsible First Marker(s) : W. Dai
Second Marker(s) : C. Ling

EE4-07 Coding Theory

Information for Candidates

This paper contains five questions. Each question carries 20 marks. The total marks are 100. The star notation * right after the sub-question numbering means that the particular sub-question may be difficult to solve.

Problem 1. (Hamming code)

(a) Find the minimum distance of the binary Hamming code $\mathcal{H}_3$ with the parity-check matrix

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Prove your answer. [5]

(b) Assume that the received vector is $\boldsymbol{y} = [0\,1\,0\,1\,1\,1\,0]$. Find the most plausible correction of $\boldsymbol{y}$. Show the computation details. [5]

(c) What are the parameters for a general binary Hamming code $\mathcal{H}_r$ ($r \geq 2$)? Write your answers as functions of r. Prove your answer. [5]

(d) * An extended code of $\mathcal{C}$, denoted by $\overline{\mathcal{C}}$, is defined as follows:

$$\overline{\mathcal{C}} = \left\{ \left(c_1, \cdots, c_n, \sum_{i=1}^{n} c_i \right) : (c_1, \cdots, c_n) \in \mathcal{C} \right\}.$$

Consider the extended binary Hamming code $\overline{\mathcal{H}_r}$. What are the codeword length and the dimension, i.e., $[n, k]$, of $\overline{\mathcal{H}_r}$? [2]

What is the distance of $\overline{\mathcal{H}_r}$? [3]

Write your answers as functions of r. Prove your answer.

Problem 2. (Finite Field)

(a) Consider the finite field $\mathbb{F}_8$ given by

0	1	α	α^2	α^3	α^4	α^5	α^6
000	001	010	100	011	110	111	101

where α is a primitive element of $\mathbb{F}_8$, and the second line of the table is a binary representation of the elements in $\mathbb{F}_8$.

(i) Let $a(x) = x^4$, $b(x) = \alpha^4 x^2 + \alpha^4 x + \alpha^3$ be polynomials in $\mathbb{F}_8[x]$. Find the polynomials $q(x)$ and $r(x)$ so that $a(x) = q(x)\,b(x) + r(x)$ and $0 \leq \deg(r(x)) < \deg(b(x))$. [5]
(Show the details of the polynomial long division. Write your final results in the standard form $c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0$, where $c_i \in \mathbb{F}_8$ are powers of α.)

(ii) Let $a(x) = \alpha^5 x^2 + \alpha^5 x + 1$. Find the value of $a(\alpha^4)$. (Show the steps of computations.) [5]

(b) Let $\mathbb{F}_q$ be a finite field ($q \in \mathbb{Z}^+$).

(i) Prove that $\text{ord}(\beta) \mid (q-1)$ for all $\beta \in \mathbb{F}_q \setminus \{0\}$. You are allowed to use the fact that $\beta^{q-1} = 1$ for all $\beta \in \mathbb{F}_q \setminus \{0\}$. [5]

(ii) * Prove that when $q = 32$, every $\beta \in \mathbb{F}_q \setminus \{0, 1\}$ is a primitive element of $\mathbb{F}_q$. [5]

Problem 3. (Subspaces and linear codes) In this question, $0 < k < n$.

(a) Let $\mathcal{C}$ be a linear subspace of $\mathbb{F}_q^n$ (in other words, a linear code of length n over $\mathbb{F}_q$). Suppose that $\dim(\mathcal{C}) = k$. Prove that $\mathcal{C}$ contains exactly q^k elements. [5]

(b)

(i) How many different choices of a nonzero vector $\boldsymbol{v}_1 \in \mathbb{F}_q^n$ are there? Why? [4]

(ii) Now assume that we have picked a nonzero vector $\boldsymbol{v}_1 \in \mathbb{F}_q^n$. We are asked to pick another vector $\boldsymbol{v}_2 \in \mathbb{F}_q^n$ so that $\boldsymbol{v}_2$ is linearly independent of $\boldsymbol{v}_1$. How many distinct choices are there for $\boldsymbol{v}_2$? Why? [5]

(c) * Let $\boldsymbol{G} \in \mathbb{F}_q^{k \times n}$ contain k linearly independent rows (that is, $\boldsymbol{G}$ is the generator matrix of some linear code $\mathcal{C}[n, k]$ over $\mathbb{F}_q$). How many distinct $\boldsymbol{G}$'s are there? Why? (Hint: The method used to solve the previous sub-question should be useful here.) [3]

(d) * Let $\mathcal{C}$ denote a linear code with parameters $[n, k]$ over $\mathbb{F}_q$. How many distinct $\mathcal{C}$ are there? Why? [3]

Problem 4. (Reed-Solomon codes, BCH codes and related)

Consider the finite field $\mathbb{F}_{16}$. Let α be a primitive element of $\mathbb{F}_{16}$. Define $\boldsymbol{A} \in \mathbb{F}_{16}^{4\times 15}$ by

$$\boldsymbol{A} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{28} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{42} \\ 1 & \alpha^4 & \alpha^8 & \cdots & \alpha^{56} \end{bmatrix}.$$

This matrix is often called a Vandermonde matrix. It has been proved that every four columns of $\boldsymbol{A}$ are linearly independent. Define $\boldsymbol{B} \in \mathbb{F}_{16}^{2\times 15}$ by keeping the first and the third rows of $\boldsymbol{A}$ and erasing all others, i.e.,

$$\boldsymbol{B} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{42} \end{bmatrix}.$$

In this question, we consider two linear codes defined by $\boldsymbol{A}$ and $\boldsymbol{B}$ respectively.

(a) Let $\mathcal{C}'$ be a code over $\mathbb{F}_{16}$ and its parity-check matrix be the matrix $\boldsymbol{A}$. What are the parameters, $[n, k, d]$, of $\mathcal{C}'$? Why? [5]

(b) Let $\mathcal{C}$ be a code over $\mathbb{F}_2$ and its parity-check matrix be the matrix $\boldsymbol{B}$. What are the parameters, $[n, k]$, of $\mathcal{C}$? Why? (The computation of d is not required in this sub-question.) [4]

(Hint: View any element in $\mathbb{F}_{16}$ as a column vector of length 4 over $\mathbb{F}_2$.)

(c) * For any $\boldsymbol{c} = [c_0, c_1, \cdots c_{14}] \in \mathcal{C}$, let $\boldsymbol{c}(x) \in \mathbb{F}_2[x]$ be the corresponding polynomial defined by $\boldsymbol{c}(x) = \sum_{i=0}^{14} c_i x^i$. What are the values of $\boldsymbol{c}(\alpha)$ and $\boldsymbol{c}(\alpha^3)$? Explain your answers. (Hint: Use the definition of $\mathcal{C}$ to get a quick answer.) [4]

(d) * Find as many roots of $\boldsymbol{c}(x)$ as possible. You may use the fact that $\boldsymbol{c}(\alpha^i) = 0$ implies $M^{(i)}(x) \,|\, \boldsymbol{c}(x)$ where $M^{(i)}(x)$ is the minimal polynomial of α^i. [4]

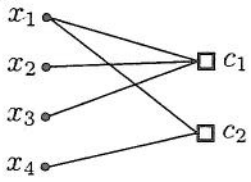
(e) * How many errors can the code $\mathcal{C}$ correct? Prove your results. [3]

Problem 5. (Decoding on graphs)

Assume that $x_1, x_2, x_3, x_4 \in \mathbb{F}_2$ are transmitted code symbols. Let y_i denote the received signals. Assume the conditional independence, i.e., $\Pr(x_1 \cdots x_4 | y_1 \cdots y_4) = \prod_{i=1}^{4} \Pr(x_i|y_i)$. Suppose that the conditional probabilities $\Pr(x_i|y_i)$, $i = 1, \cdots, 4$, are known.

(a) Write down the general formula to compute the marginal probability $\Pr(x_1 = 1 | y_1 \cdots y_4)$ in terms of $\Pr(x_i|y_i)$'s, $i = 1, \cdots, 4$. Count how many additions and multiplications need to be carried out. [5]

(b) Consider the Tanner graph below



(i) Find the parity-check matrix of the corresponding code. [5]

(ii) Using the Tanner graph, write down the explicit formula to compute the conditional probability $\Pr(x_1 = 1 | y_2 y_3)$ in terms of $\Pr(x_i|y_i)$'s, $i = 2, 3$. [5]

(iii) Using the Tanner graph, write down the explicit formula to compute the conditional probability $\Pr(x_1 = 1 | y_1 \cdots y_4)$ in terms of $\Pr(x_i|y_i)$'s, $i = 1, \cdots, 4$. Count how many additions and multiplications in total need to be carried out in this case. [5]

EE4-07

CODING THEORY 2012 - EE9-SO11

SOLUTIONS

Solutions of Question 1:

(a) Since every pair of columns of $\boldsymbol{H}$ are linearly independent, one has $d \geq 3$. On the other hand, there exist three columns in $\boldsymbol{H}$, for example, columns 1,2 and 4, linearly dependent, $d \leq 3$. Hence, $d(\mathcal{H}_3) = 3$. [5]

(b) We first compute the syndrome vector

$$\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^T = [0\ 1\ 0]\,.$$

Hence the 2nd bit of $\boldsymbol{y}$ is erroneous and $\hat{\boldsymbol{x}} = [0\ 0\ 0\ 1\ 1\ 1\ 0]$. [5]

(c) For binary Hamming codes, the parity-check matrix $\boldsymbol{H}_r$ contains all nonzero binary vectors of length r. Hence, the codeword length is $n = 2^r - 1$. The code dimension k is computed by $n-(n-k) = 2^r - 1 - r$. Therefore, the parameters are given by $[2^r - 1, 2^r - 1 - r, 3]$. [5]

(d) The parameters are given by $[2^r, 2^r - 1 - r, 4]$.

It is clear that the codeword length of $\overline{\mathcal{H}}_r$ is one more than that of $\mathcal{H}_r$, and the code size of $\overline{\mathcal{H}}_r$ is the same as that of $\mathcal{H}_r$. Hence, $n = 2^r$ and $k = 2^r - 1 - r$. [2]

Now we prove $d\left(\overline{\mathcal{H}}_r\right) = 4$. Note that $d\left(\overline{\mathcal{H}}_r\right) = \min\ \mathrm{wt}\,(\overline{\boldsymbol{c}})$ where $\overline{\boldsymbol{c}} \in \overline{\mathcal{H}}_r$. For any $\overline{\boldsymbol{c}} \in \overline{\mathcal{H}}_r$, there exists a $\boldsymbol{c} \in \mathcal{H}_r$ such that $\boldsymbol{c} = \overline{\boldsymbol{c}}\,(1 : 2^r - 1)$ (coincide in the first $2^r - 1$ bits). Note that $\mathrm{wt}\,(\overline{\boldsymbol{c}}) = \mathrm{wt}\,(\boldsymbol{c}) + \mathrm{wt}\left(\sum_{i=1}^{2^r-1} c_i\right) \geq \mathrm{wt}\,(\boldsymbol{c})$. Hence, it can be easily verified that

$$\begin{cases} \mathrm{wt}\,(\overline{\boldsymbol{c}}) = 0 & \text{if } \boldsymbol{c} = \boldsymbol{0} \\ \mathrm{wt}\,(\overline{\boldsymbol{c}}) = 4 & \text{if } \mathrm{wt}\,(\boldsymbol{c}) = 3 \\ \mathrm{wt}\,(\overline{\boldsymbol{c}}) \geq \mathrm{wt}\,(\boldsymbol{c}) \geq 4 & \text{if } \mathrm{wt}\,(\boldsymbol{c}) \geq 4 \end{cases}.$$

Note that $d(\mathcal{H}_r) = 3$. We conclude that $d\left(\overline{\mathcal{H}}_r\right) = 4$. [3]

Solutions of Question 2:

(a)

(i) $q(x) = \alpha^3 x^2 + \alpha^3 x + \alpha^5$ and $r(x) = x + \alpha$.

$$
\begin{array}{r|l}
\alpha^4 x^2 + \alpha^4 x + \alpha^3 & \alpha^3 x^2 + \alpha^3 x + \alpha^5 \\
\hline
x^4 & \\
x^4 + x^3 + \alpha^6 x^2 & \\
\hline
x^3 + \alpha^6 x^2 & \\
x^3 + x^2 + \alpha^6 x & \\
\hline
\alpha^2 x^2 + \alpha^6 x & \\
\alpha^2 x^2 + \alpha^2 x + \alpha & \\
\hline
x + \alpha &
\end{array}
$$

[5]

(ii)

$$
\begin{aligned}
a(\alpha^4) &= \alpha^5 \alpha^8 + \alpha^5 \alpha^4 + 1 \\
&= \alpha^6 + \alpha^2 + 1 \\
&= 0.
\end{aligned}
$$

[5]

(b)

(i) Suppose that $\operatorname{ord}(\beta) \nmid (q-1)$. Then $q - 1 = a \cdot \operatorname{ord}(\beta) + r$ for some integers a and $0 < r < \operatorname{ord}(\beta)$. Note that

$$1 = \beta^{q-1} = \beta^{\operatorname{ord}(\beta)\cdot a + r} = \beta^r.$$

Contradicts with the definition of the order of an element. Hence, $\operatorname{ord}(\beta) \mid (q-1)$.

[5]

(ii) For all $\beta \neq 0$, $\operatorname{ord}(\beta) \mid (q-1)$. Since $q - 1 = 31$ is a prime number, $\operatorname{ord}(\beta)$ can take only two values, either $\operatorname{ord}(\beta) = 1$ or $\operatorname{ord}(\beta) = q - 1$. Note that $\operatorname{ord}(\beta) = 1$ implies that $\beta = \beta^1 = 1$. For all $\beta \in \mathbb{F}_q \setminus \{0, 1\}$, the order of β has to be $q - 1$. The desired claim is therefore proved. [5]

Solutions of Question 3:

(a) Since $\dim(\mathcal{C}) = k$, $\mathcal{C}$ can be represented by its basis $\{\boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_k\}$, where $\boldsymbol{b}_i \in \mathbb{F}_q^n$, $i = 1, \cdots, k$, are linearly independent vectors over $\mathbb{F}_q$. Because

$$\mathcal{C} = \left\{ \sum_{i=1}^{k} \lambda_i \boldsymbol{b}_i : \ \lambda_1, \cdots, \lambda_k \in \mathbb{F}_q \right\},$$

we have $|\mathcal{C}| \leq q^k$. As the basis vectors are linear independent, all these vectors are different. Hence, $|\mathcal{C}| = q^k$. [5]

(b)

(i) There are $q^n - 1$ many choices for $\boldsymbol{v}_1$. For a vector over $\mathbb{F}_q$ of length n, there are q^n choices. Since $\boldsymbol{v}_1$ is non-zero, we need to take the zero vector out, hence $q^n - 1$ choices in total. [4]

(ii) There are $q^n - q$ many choices for $\boldsymbol{v}_2$. Among all possible q^n distinct vectors in $\mathbb{F}_q^n$, to choose a vector linearly independent of $\boldsymbol{v}_1$, we need to take all possible "linear combinations" of $\boldsymbol{v}_1$ out, i.e., $\boldsymbol{v}_2 \neq a\boldsymbol{v}_1$ for $a = 0, 1, \cdots, q-1$. Therefore, there are $q^n - q$ choices in total. [5]

(c) The $\boldsymbol{G}$ matrix contains k many linearly independent row vectors $\boldsymbol{v} \in \mathbb{F}_q^n$. Using the same argument for the previous sub-question, there are $q^n - 1$ many choices for the 1^{st} row of $\boldsymbol{G}$, $q^n - q$ many choices for the 2^{nd} row of $\boldsymbol{G}$, $\cdots$, and $q^n - q^{k-1}$ many choices for the k^{th} row of $\boldsymbol{G}$. Hence, there are $\prod_{i=0}^{k-1}(q^n - q^i) = q^{\frac{k(k-1)}{2}} \prod_{i=0}^{k-1}(q^{n-i} - 1)$ many $\boldsymbol{G}$'s. [3]

(d) Note that $\text{span}(\boldsymbol{G}) = \text{span}(\boldsymbol{RG})$ for any $\boldsymbol{R} \in \mathbb{F}_q^{k \times k}$ such that $\boldsymbol{R}$ contains k many linearly independent rows. There are $\prod_{i=0}^{k-1}(q^k - q^i) = q^{\frac{k(k-1)}{2}} \prod_{i=0}^{k-1}(q^{k-i} - 1)$ distinct $\boldsymbol{R}$'s over $\mathbb{F}_q$. Hence, there are

$$\frac{\prod_{i=0}^{k-1}(q^{n-i} - 1)}{\prod_{i=0}^{k-1}(q^{k-i} - 1)}$$

many distinct linear subspaces, i.e., linear codes. [3]

Solutions of Question 4:

(a) From the parity-check matrix $\boldsymbol{A}$, n is clearly 15 and $k = n - (n-k) = 15 - 4 = 11$. Since every four columns of $\boldsymbol{A}$ are linearly independent, $d \geq 5$. Note that every five columns of $\boldsymbol{A}$ must be linearly dependent because the length of the columns is 4. We conclude $d = 5$. (The upper bound can be derived by other methods, for example, the Singleton bound.) [5]

(b) From the parity-check matrix $\boldsymbol{B}$, n is clearly 15. View every symbol in $\boldsymbol{B}$ as a column vector of length 4, $n - k = 8$. Hence, $k = 7$. [4]

(c) Note that $\boldsymbol{c}(\alpha^j) = \sum_{i=0}^{14} c_i \alpha^{ij}$. By the parity check matrix $\boldsymbol{B}$ of $\mathcal{C}$, it is clear that $\boldsymbol{c}(\alpha) = 0$ and $\boldsymbol{c}(\alpha^3) = 0$. [4]

(d) Note the following cyclotomic cosets of 2 mod 15: $C_1 = \{1, 2, 4, 8\}$ and $C_3 = \{3, 6, 12, 9\}$. We have $M^{(1)}(x) = \prod_{i \in C_1} (x - \alpha^i)$, $M^{(3)} = \prod_{i \in C_3} (x - \alpha^i)$. Since $\boldsymbol{c}(\alpha) = \boldsymbol{c}(\alpha^3) = 0$, one has $M^{(1)}(x) \,|\boldsymbol{c}(x)$ and $M^{(2)}(x) \,|\boldsymbol{c}(x)$. Hence, α^i's, $i \in C_1 \bigcup C_3$, are roots of $\boldsymbol{c}(x)$. [4]

(e) The code $\mathcal{C}$ can correct two errors. Using the same argument for part (a), $d(\mathcal{C}) \geq 5$. The number of errors correctable is then give by $\geq \lfloor \frac{5-1}{2} \rfloor = 2$. [3]

Solutions of Question 5:

(a)

$$\begin{aligned}
&\Pr(x_1 = 1|y_1 \cdots y_4) \\
&= \sum_{a_2=0}^{1} \sum_{a_3=0}^{1} \sum_{a_4=0}^{1} \Pr(x_1 = 1, x_2 = a_2, x_3 = a_3, x_4 = a_4|y_1 \cdots y_4) \\
&= \sum_{a_2=0}^{1} \sum_{a_3=0}^{1} \sum_{a_4=0}^{1} \Pr(x_1 = 1|y_1) \prod_{i=2}^{4} \Pr(x_i = a_i|y_i) .
\end{aligned}$$

Hence, there are 8 additions and $8 \times 3 = 24$ multiplications involved. [5]

(b)

(i) $\boldsymbol{H} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$ [5]

(ii) According to the Tanner graph, $x_1 = 1 \Leftrightarrow x_2 + x_3 = 1$. One has

$$\begin{aligned}
&\Pr(x_1 = 1|y_2 y_3) \\
&= \Pr(x_1 = 1, x_2 + x_3 = 1|y_2 y_3) \\
&= \Pr(x_2 + x_3 = 1|y_2 y_3) \\
&= \Pr(x_2 = 0, x_3 = 1|y_2 y_3) + \Pr(x_2 = 1, x_3 = 0|y_2 y_3) \\
&= \Pr(x_2 = 0|y_2) \Pr(x_3 = 1|y_3) + \Pr(x_2 = 1|y_2) \Pr(x_3 = 0|y_3) .
\end{aligned}$$

[5]

(iii) According to the Tanner graph, one has $x_1 = 1 \Leftrightarrow x_2 + x_3 = 1$, and $x_1 = 1 \Leftrightarrow x_4 = 1$. Hence,

$$\begin{aligned}
&\Pr(x_1 = 1|y_1 \cdots y_4) \\
&= \Pr(x_1 = 1, x_2 + x_3 = 1, x_4 = 1|y_1 \cdots y_4) \\
&= \Pr(x_1 = 1|y_1) \Pr(x_2 + x_3 = 1|y_2, y_3) \Pr(x_4 = 1|y_4) ,
\end{aligned}$$

where $\Pr(x_2 + x_3 = 1|y_2, y_3)$ has been computed in the solution of the previous sub-question.

As a result, there are 1 addition and 4 multiplications involved. [5]