IMPERIAL COLLEGE LONDON

EE4-07
EE9-CS7-23
EE9-SO11

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2018

MSc and EEE/EIE PART IV: MEng and ACGI

Corrected copy

CODING THEORY

Tuesday, 8 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

Instructions for Candidates

Answer all five questions. Each question carries 20 marks.

1. (Finite Fields)

(a) Let $f(x) = x^3 + 1 \in \mathbb{F}_3[x]$ and $g(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$.

i Find the greatest common divisor $h(x)$ of $f(x)$ and $g(x)$, i.e., $h(x) = \gcd(f(x), g(x))$. Write $h(x)$ as a *monic* polynomial. [4]

ii Find the polynomials $a(x) \in \mathbb{F}_3[x]$ and $b(x) \in \mathbb{F}_3[x]$ such that $h(x) = a(x) f(x) + b(x) g(x)$. [4]

(b) Given the finite field $\mathbb{F}_{16} = \mathbb{F}_2[x]/x^4 + x + 1$ as follows

	$\mathbb{F}_2[x]/x^4+x+1$		$\mathbb{F}_2[x]/x^4+x+1$
0	0	x^7	$x^3 + x + 1$
1	1	x^8	$x^2 + 1$
x	x	x^9	$x^3 + x$
x^2	x^2	x^{10}	$x^2 + x + 1$
x^3	x^3	x^{11}	$x^3 + x^2 + x$
x^4	$x + 1$	x^{12}	$x^3 + x^2 + x + 1$
x^5	$x^2 + x$	x^{13}	$x^3 + x^2 + 1$
x^6	$x^3 + x^2$	x^{14}	$x^3 + 1$

i Find the polynomial f_1 in $\mathbb{F}_2[x]/x^4 + x + 1$ such that $(x^2 + 1) \cdot f_1 = x^3 + x + 1$. [4]

ii Let f_1 be the solution of the previous sub-problem. Find the polynomial f_2 in $\mathbb{F}_2[x]/x^4 + x + 1$ such that $x \cdot f_1 + (x^3 + x^2 + x) \cdot f_2 = x + 1$. [4]

In other words, the linear inverse problem below is solved

$$\begin{bmatrix} x^2+1 & 0 \\ x & x^3+x^2+x \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = \begin{bmatrix} x^3+x+1 \\ x+1 \end{bmatrix}.$$

(c)

i Find whether $x^2+x+1 \in \mathbb{F}_2[x]$ is irreducible or not. Prove your answer. [2]

ii Find whether $x^2+x+1 \in \mathbb{F}_3[x]$ is irreducible or not. Prove your answer. [2]

2. (Cryptography)

(a) In Caesar cipher, each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet (cyclic shift of alphabets). Decrypt the following sentence which is encrypted by using Caesar cipher (only consider capital letters).

RYZO PYB DRO LOCD LED ZBOZKBO PYB DRO GYBCD [5]

Hint: The five most commonly used three letter words are THE, AND, FOR, ARE, and BUT. The English alphabet is given in the table below for your convenience.

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

(b) Let $p = 311$. It is a prime number. Fermat's little theorem states that for all $a \in \mathbb{F}_p^*$, $a^{p-1} = a^{310} = 1$.

i Compute $17^x \bmod 311$ for $x = 64, 65, 66$. Based on your results, find $\log_{17} 8 \bmod 311$. [7]

Hint: When you compute $a^x \bmod p$ where both a and x are large, direct calculation could result in integer overflown or inaccurate result.

ii Prove that $\mathrm{ord}(a) | 310$, i.e., $\mathrm{ord}(a)$ divides 310, for all $a \in \mathbb{F}_{311}^*$. [3]

iii Prove that for all $a \in \mathbb{F}_{311}^*$, $\mathrm{ord}(a)$ can only be one of eight possible values. Find the eight possible values. [3]

iv It holds that the number 2 is not a primitive element in $\mathbb{F}_{311}$ while the number 17 is. Explain how to efficiently demonstrate these two claims. A roadmap is sufficient. Detailed computations are not required. [2]

3. (Linear Codes)

(a) Let $C \subset \mathbb{F}_2^7$ be a linear code. Its the parity check matrix is given by

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

i Use Gaussian elimination to change the parity matrix into the form of $\boldsymbol{H} = [\boldsymbol{I}\ \boldsymbol{A}]$ where $\boldsymbol{I}$ is the identity matrix. [2]

ii Find the corresponding generator matrix $\boldsymbol{G}$ in the systematic form $[\boldsymbol{B}\ \boldsymbol{I}]$. [2]

iii Assume that a message $\boldsymbol{m}_1$ is encoded into a codeword $\boldsymbol{c}_1$ using $\boldsymbol{G}$. The codeword $\boldsymbol{c}_1$ is transmitted over an binary symmetric channel. Let the received word be $\boldsymbol{y}_1 = [0\ 0\ 1\ 1\ 1\ 1\ 0]$. Compute the syndrome vector $\boldsymbol{s}_1$. Find the output of the minimum (Hamming) distance decoding, say $\hat{\boldsymbol{c}}_1$, and the corresponding transmitted message $\hat{\boldsymbol{m}}_1$. [3]

iv Assume that a message $\boldsymbol{m}_2$ is encoded into a codeword $\boldsymbol{c}_2$ using $\boldsymbol{G}$ The codeword $\boldsymbol{c}_2$ is transmitted over an binary erasure channel. Let the received word be $\boldsymbol{y}_2 = [0\ 1\ ?\ ?\ 0\ 1\ 0]$. Set the question marks in $\boldsymbol{y}_2$ to zero and compute the corresponding syndrome vector $\boldsymbol{s}_2$. Find the transmitted codeword $\boldsymbol{c}_2$ and the message $\boldsymbol{m}_2$. [3]

(b)

i Find the distance of the code C in Problem 3.(a). (No proof is required.) [1]

ii Prove that the distance of a linear code C is the minimum weight of nonzero codewords, i.e., $d(C) = \min_{c \in C \setminus \{0\}} \mathrm{wt}(\boldsymbol{c})$. [2]

(c) Using the code C in Problem 3.(a), we define the following two codes

$$C_a = \{[\boldsymbol{c}, \boldsymbol{c}] : \boldsymbol{c} \in C\},$$
$$C_b = \{[\boldsymbol{c}_1, \boldsymbol{c}_2] : \boldsymbol{c}_1 \in C,\ \boldsymbol{c}_2 \in C\},$$

where $[\boldsymbol{a}, \boldsymbol{b}]$ denotes the concatenation of two vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ into a vector.

i Find the parameters n (codeword length), k (dimension), and d (distance) of the codes C_a and C_b. Justify your answers. [3]

ii Find the generator matrices $\boldsymbol{G}_a$ and $\boldsymbol{G}_b$ for C_a and C_b respectively. [2]

iii Find the parity-check matrices $\boldsymbol{H}_a$ and $\boldsymbol{H}_b$ for C_a and C_b respectively. [2]

4. (Cyclic and BCH Codes)

Define the generating function of a codeword $\mathbf{c} = [c_0, \cdots, c_{n-1}]$ as $c(x) = \sum_{i=0}^{n-1} c_i x^i$. A *linear* code $\mathcal{C}$ is called a cyclic code if for all $c(x) \in \mathcal{C}$ and arbitrary $u(x) \in \mathbb{F}_p[x]$. it holds that $u(x)\,c(x) \mod x^n - 1$ is in $\mathcal{C}$. For a cyclic code $\mathcal{C}$, choose its generator polynomial $g(x) \in \mathcal{C}$ as the nonzero monic polynomial of least degree.

(a) Prove that for all $c(x) \in \mathcal{C}$, it holds that $c(x) = u(x)\,g(x)$ for some $u(x)$. [2]

(b) Prove that $g(x) \mid (x^n - 1)$. [2]

(c) Now construct a BCH code on $\mathbb{F}_3$ with $n = 26$ and $d \geq 7$ by finding an appropriate generator polynomial $g(x)$.

i Find the corresponding cyclotomic cosets C_i, $i = 0, 1, \cdots, 8$. [4]

ii Let α be a primitive element in $\mathbb{F}_{27}$. For a given cyclotomic coset C_i, write the corresponding minimal polynomial $M^{(i)}(x)$. [1]

iii Find a generator polynomial $g(x)$ to guarantee $d \geq 7$. Write it using minimal polynomials. [3]

iv Prove that the cyclic code generated by the generator polynomial has distance $d \geq 7$. [4]

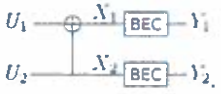
(d) To show a minimal polynomial $M^{(i)}(x) \in \mathbb{F}_p[x]$, one needs the following result.

Lemma. *Let p be the characteristic of $\mathbb{F}_q$. It holds that $(x+y)^p = x^p + y^p$.*

Prove this lemma. [4]

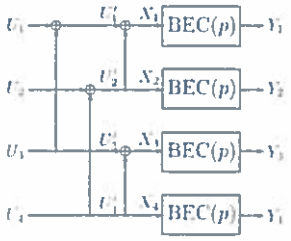
5. (Polar Codes)

Consider the basic building block of polar codes:



Consider a BEC channel with erasure probability p. The mutual information between the input and output of the channel, e.g. $I(X_1; Y_1)$, is $1-p$. The mutual information between the inputs of the basic building block and the outputs is given by $I(U_1; \boldsymbol{Y}) = 1 - 2p + p^2 = (1-p)^2$ and $I(U_2; U_1\boldsymbol{Y}) = 1 - p^2$.

The following two level diagram can be constructed using the basic building block.



(a) In the basic building block, let $[X_1, X_2] = [U_1, U_2]\,\boldsymbol{G}_1$. Write the specific form of $\boldsymbol{G}_1$.

In the two level diagram, let $[X_1, \cdots, X_4] = [U_1, \cdots, U_4]\,\boldsymbol{G}_2$. Write the specific form of $\boldsymbol{G}_2$. [2]

(b) Let $p = 0.1$. In the two level diagram, compute the mutual information at node U_i, denoted by I_i, $i = 1, 2, 3, 4$. Explain your computation process. [4]

(c) Let question mark ? denote the corresponding symbol is erased/unknown. Consider the basic building block. Suppose that one of the output symbols is erased by the channel, that is, the outputs have only two possible forms $[?, y_2]$ or $[y_1, ?]$. Find the corresponding decoded word $[u_1, u_2]$ (in terms of $y_1, y_2, ?$). Based on your decoding, find the most and least reliable input symbols. [4]

(d) Consider the two level diagram. Suppose that one of the output symbols is erased by the channel, that is, the outputs have four possible forms $[?, y_2, y_3, y_4]$, $[y_1, ?, y_3, y_4]$, $[y_1, y_2, ?, y_4]$, or $[y_1, y_2, y_3, ?]$. Find the corresponding decoded word $[u_1, u_2, u_3, u_4]$ (in terms of $y_1, y_2, y_3, y_4, ?$). Based on your decoding, find the most and least reliable input symbols. [5]

(e) Consider the two level diagram. Suppose that one of the output symbols is erased by the channel, that is, the outputs have four possible forms $[?, y_2, y_3, y_4]$, $[y_1, ?, y_3, y_4]$, $[y_1, y_2, ?, y_4]$, or $[y_1, y_2, y_3, ?]$. Also assume that $u_1 = 0$. Find the corresponding decoded word $[u_1, u_2, u_3, u_4]$ (in terms of $0, y_1, y_2, y_3, y_4, ?$). [5]