IMPERIAL COLLEGE LONDON

EE4-07
EE9-SO11

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2016

MSc and EEE/EIE PART IV: MEng and ACGI

Corrected copy

CODING THEORY

Wednesday, 4 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.

The star notation * right after the sub-question numbering means that the particular sub-question may be difficult to solve.

1. (Finite Fields)

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

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) Use Bézout's identity to prove Euclid's Lemma:

Let $r_1, r_2 \in \mathbb{Z}^+$ and $\gcd(r_1, r_2) = 1$. If $r_1 | (r_2 r)$, then $r_1 | r$. [2]

(c) Let $f(x) = x^2 + 1 \in \mathbb{F}_2[x]$. Is this polynomial irreducible? Justify your answer. [2]

(d) Let $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Is this polynomial irreducible? Justify your answer. [2]

(e) Consider the polynomial ring $\mathcal{R} := \mathbb{F}_p[x] / f(x)$ where $f(x) \in \mathbb{F}_p[x]$ has degree larger than one.

i Prove that if $f(x) \in \mathbb{F}_p[x]$ is irreducible, then $\mathcal{R}$ is a field. [3]

ii Prove that if $\mathcal{R}$ is a field, then $f(x) \in \mathbb{F}_p[x]$ is irreducible. [3]

2. (Cryptography)

(a) Let p be a prime number. For given $b, y \in \mathbb{F}_p^*$, define the discrete logarithmic function $x = \log_b y \bmod p$ if $b^x = y \bmod p$.

i Let $p = 7$ and $\alpha = 3 \in \mathbb{F}_p$. Find $\mathrm{ord}(\alpha)$ by computing α^x, $x = 1, 2, \cdots$. [2]

ii Let $p = 7$ and $b = 3$. Compute $\log_b y \bmod p$ for $y = 1, 2, 3$ respectively. [2]

iii Let $p = 7$ and $\alpha = 2 \in \mathbb{F}_p$. Find $\mathrm{ord}(\alpha)$ by computing α^x, $x = 1, 2, \cdots$.. [2]

iv Let $p = 7$ and $b = 2$. Compute $\log_b y \bmod p$ for $y = 1, 2, 3$ respectively. [2]

v Prove that if b is a primitive element, then $b^{x_1} \neq b^{x_2}$ for all $0 \leq x_1 < x_2 \leq p - 1$. [2]

vi Explain how to choose the base b for the discrete logarithm function so that it is well defined. [2]

(b) Suppose that Alice would like to save her password securely on a server. Denote her user name by i and the raw password by x_i. What information should be stored on the server? [2]

(c) Consider Shamir's Secret Sharing scheme to share a secret $S \in \mathbb{F}_p^*$ among n users:

Randomly choose $k - 1$ integers $a_1, \cdots, a_{k-1} \in \mathbb{F}_p^*$. Set $a_0 = S$. Set $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$. Evaluate $f(x)$ at n distinct points to obtain $(t_i, f(t_i))$. $t_i \in \mathbb{F}_p^*$ and $i = 1, \cdots, n$.

i How many pairs $(t_i, f(t_i))$ are needed in order to uniquely recover the secret S? [2]

ii Given ℓ pairs $(t_{i_1}, f(t_{i_1})), (t_{i_2}, f(t_{i_2})), \cdots, (t_{i_\ell}, f(t_{i_\ell}))$, a linear system $\boldsymbol{a}\boldsymbol{M} = \boldsymbol{f}$ can be used to find the polynomial coefficients, where $\boldsymbol{a} = [a_0, \cdots, a_{k-1}]$ and $\boldsymbol{f} = [f(t_{i_1}), f(t_{i_2}), \cdots, f(t_{i_\ell})]$. Write the explicit form of the matrix $\boldsymbol{M}$. [2]

iii Use your result for the Problem 2.(c)-ii to justify your answer to Problem 2.(c)-i. You are allowed to use the properties of Vandermonde matrix. [2]

3. (Linear Codes)

(a) Let $C \subset \mathbb{F}_q^n$ be a linear code with distance d. State the relationship between d and the weights of the codewords in the code. (No proof is needed.) [2]

(b) Let $C \subset \mathbb{F}_q^n$ be a linear code with distance d. Let $\boldsymbol{H}$ be its parity-check matrix. State the relationship between d and the linear dependence (or independence) of the columns of $\boldsymbol{H}$. (No proof is needed.) [2]

(c) Let $C \subset \mathbb{F}_2^7$ be a linear code generated by the matrix

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

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

ii Find the corresponding parity-check matrix $\boldsymbol{H}$ in the systematic form. [2]

iii Assume that a message $\boldsymbol{m}_1$ is encoded into a codeword $\boldsymbol{c}_1$ using $\boldsymbol{G}'$. Let the received word be $\boldsymbol{y}_1 = [1\ 1\ 0\ 1\ 1\ 0\ 1]$. 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 erasure channel and the received word is given by $\boldsymbol{y}_2 = [1\ ?\ 0\ ?\ 0\ 0\ 1]$. 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]

(d) * Define

$$C_2 = \left\{ \left(c_1, \cdots, c_n, \sum_{i=1}^{n} c_i \right) : (c_1, \cdots, c_n) \in C \right\},$$

where C is the code defined in Problem 3.(c).

i Find the length of the codewords in C_2, denoted by n_2. [1]

ii Find the dimension of C_2 defined as $k_2 := \log_2 |C_2|$ where $|C_2|$ gives the number of codewords in C_2. [1]

iii Find the generator matrix $\boldsymbol{G}_2$ of C_2 using the $\boldsymbol{G}$ from Problem (c). (No proof is needed.) [2]

iv Find the distance of $\mathcal{C}_2$. Prove your answer using the result for Problem 3.(a). [2]

4. (RS, Cyclic, and BCH Codes)

(a) Consider a linear code with parameters $[n, k, d]$. The Singleton bound states that $d \leq n - k + 1$. Prove it. [3]

(b) A Reed-Solomon code can be defined as follows. Let $\mathbb{F}_q$ be a finite field and α be a primitive element. Let $n = q - 1$. For a given polynomial $f(x) \in \mathbb{F}_q[x]$, define the evaluation mapping $\text{eval}(f)$ by

$$\mathbb{F}_q[x] \to \mathbb{F}_q^n$$
$$f \mapsto \boldsymbol{c} = [c_0, c_1, \cdots, c_{n-1}], \text{ where } c_i = f(\alpha^i).$$

An $[n, k]$ Reed-Solomon code is defined as $\mathcal{C} = \{\text{eval}(f),\ 0 \leq \deg(f) \leq k - 1\}$.

i Prove that Reed-Solomon codes are linear codes. [3]

ii Prove that Reed-Solomon codes achieve the Singleton bound. [3]

(c) Let $q = 3$ and $n = 26$. Construct a BCH code in the following way.

i Write down the cyclotomic cosets $C_0, C_1, \cdots, C_8$ of 3 modulo 26. [4]

ii Let α be a primitive element of $\mathbb{F}_{27}$. Define $M^{(i)}(x) = \prod_{j \in C_i} (x - \alpha^j)$. Let $g(x) = \text{lcm}\left(M^{(1)}(x), \cdots, M^{(8)}(x)\right)$. Consider the cyclic code $\mathcal{C}$ generated by $g(x)$.

A. Find the degree of $g(x)$. [2]

B. Decide the dimension k of the generated code $\mathcal{C}$. [2]

C. Find the tightest lower bound on the distance d of the code $\mathcal{C}$. Prove your result. You are allowed to use the properties of Vandermonde matrix. [3]

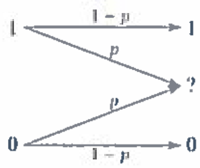
5. (Channel Polarization)

Recall the definition

$$H(X) := -\sum_{x\in\mathcal{X}} p_X(x)\log_2 P_X(x),$$
$$H(X|y) := -\sum_{x\in\mathcal{X}} p_{X|Y}(x|y)\log_2 p_{X|Y}(x|y),$$
$$H(X|Y) := -\sum_{y\in\mathcal{Y}} p_Y(y) H(X|y).$$
$$I(X;Y) := H(Y) - H(Y|X) = H(X) - H(X|Y).$$

Define $H(p) := -p\log_2 p - (1-p)\log_2(1-p)$. Note that $0\log_2 0 = 0$.

(a) Consider the BEC channel:



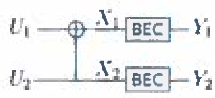
Assume that $p_X(0) = p_X(1) = \frac{1}{2}$.

i Find $p_Y(y)$ for $y \in \{0,1,?\}$. [3]

ii Find the cases that $H(X|y) = 0$ and $H(X|y) = 1$ respectively. [2]

iii Find $I(X;Y)$. [2]

(b) * Consider the following channel of which the input $u_1u_2 \in \{0,1\}^2$ and the output $y_1y_2 \in \{0,1,?\}^2$:



Assume that U_1, U_2 are independent with distribution $p_U(0) = p_U(1) = \frac{1}{2}$.

i Find $p_{Y_1Y_2}(y_1y_2)$ when y_1y_2 varies in $\{0,1,?\}^2$. [3]

ii It is straightforward to see that $H(U_1|y_1y_2)$ can only take two values 0 and 1. Find the cases that $H(U_1|y_1y_2) = 0$ and $H(U_1|y_1y_2) = 1$ respectively. [3]

iii Find $I(U_1;Y_1Y_2)$. [2]

iv It is straightforward to see that $H(U_2|y_1y_2u_1)$ can only take two values 0 and 1. Find the cases that $H(U_2|y_1y_2u_1) = 0$ and $H(U_2|y_1y_2u_1) = 1$ respectively. [3]

v Find $I(U_2; Y_1 Y_2 U_1)$. [2]