IMPERIAL COLLEGE LONDON

EE4-07
EE9-CS7-23
EE9-SO11

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2017

MSc and EEE/EIE PART IV: MEng and ACGI

Corrected copy

CODING THEORY

Tuesday, 23 May 10:00 am

Time allowed: 3:00 hours

11.39am 3b(iv) typo.
Singleton NOT Hamming

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) Prove the following claims:

i $x^2+1 \in \mathbb{F}_2[x]$ is not irreducible. [2]

ii $x^2+1 \in \mathbb{F}_3[x]$ is irreducible. [2]

iii $x^2+1 \in \mathbb{F}_5[x]$ is not irreducible. [2]

(b) Let $f(x) = x^3+x+1 \in \mathbb{F}_5[x]$ and $g(x) = x^2+x+1 \in \mathbb{F}_5[x]$.

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. [3]

ii Find the polynomials $a(x) \in \mathbb{F}_5[x]$ and $b(x) \in \mathbb{F}_5[x]$ such that $h(x) = a(x) f(x) + b(x) g(x)$. [4]

(c) 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 $\mathrm{ord}(x^3+x)$. [2]

ii Find $\mathrm{ord}(x^2+x+1)$. [2]

iii Find $\mathrm{ord}((x^3+x)\cdot(x^2+x+1))$. [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 $b^x = y \bmod p$. If there does not exist x such that $b^x = y \bmod p$, then we say $\log_b y \bmod p$ is not well defined.

i Let $p = 11$ and $a = 2$. Find ord (a) by computing a^x, $x = 1, 2, \cdots$. [2]

ii Let $p = 11$ and $a = 3$. Find ord (a) by computing a^x, $x = 1, 2, \cdots$. [2]

iii Let $p = 11$. Find $\log_2 y \bmod p$ for $y = 2, 3, 4, 5$ respectively. [2]

iv Let $p = 11$. Find $\log_3 y \bmod p$ for $y = 2, 3, 4, 5$ respectively. [2]

(b) Let p be a large prime number. Let b be primitive element of $\mathbb{F}_p$.

i What is the computational complexity to compute $b^x \bmod p$ for an integer $1 < x < p$? Explain your answer. [3]

ii What is the computational complexity in general to compute $\log_b y \bmod p$ for an integer $1 < y < p$? [1]

(c) 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).

G VOIZAXK OY CUXZN G ZNUAYGTJ CUXJY

Hint: English letters are listed below from the most to least in appearance frequency: ETAOINSHRDLCUMWFGYPBVKJXQZ. In the encrypted sentence above, the most frequent used letters include GUXYZ, each of which appeared three times. [4]

(d) Suppose that Bob wants to send some information to Alice using ElGamal Cryptography. Alice keeps her private key a' secret but makes a prime number p, a primitive element $b \in \mathbb{F}_p$, and her public key $a = b^{a'} \in \mathbb{F}_p^*$ publicly available. Bob randomly chooses $t \in \mathbb{N}^+$ and encrypts the message m into (b^t, ma^t).

i How should Alice retrieve the message m? [2]

ii Compared with Caesar cipher, discuss the advantages of ElGammal Cryptography in terms of security. [2]

3. (Linear Codes)

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

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

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

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

iii Assume that a message m_1 is encoded into a codeword c_1 using G. The codeword c_1 is transmitted over an binary symmetric channel. Let the received word be $y_1 = [1\ 1\ 0\ 1\ 1\ 0\ 1]$. Compute the syndrome vector s_1. Find the output of the minimum (Hamming) distance decoding, say $\hat{c}_1$, and the corresponding transmitted message $\hat{m}_1$. [3]

iv Assume that a message m_2 is encoded into a codeword c_2 using G. The codeword c_2 is transmitted over an binary erasure channel. Let the received word be $y_2 = [?\ 1\ 0\ 1\ ?\ 1\ 0]$. Set the question marks in y_2 to zero and compute the corresponding syndrome vector s_2. Find the transmitted codeword c_2 and the message m_2. [3]

(b) Let $C \subset \mathbb{F}_q^n$ be a linear code with distance d.

i State the Hamming bound (also known as sphere packing bound). (No proof is required.) [2]

ii The codes that attain Hamming bound are called perfect codes. Is the code in Part (a) a perfect code? Justify your answer. [3]

iii State the Singleton bound for linear codes. Prove it. [3]

iv The codes that attain Hamming bound are called minimum distance separable (MDS). Is the code in Part (a) MDS? Justify your answer. [2]

Singleton. Corrected at 11.39.

4. (RS, Cyclic, and BCH Codes)

(a) 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 eval (f) by

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

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

i From the definition of the evaluation mapping, show that

$$\boldsymbol{G} = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{k-1} & \cdots & \alpha^{(k-1)(n-1)} \end{bmatrix}$$

is a generator matrix of Reed-Solomon code. [3]

ii Let

$$\boldsymbol{H} = \begin{bmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \cdots & \alpha^{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k} & \cdots & \alpha^{(n-k)(n-1)} \end{bmatrix}.$$

Show that $\boldsymbol{G}\boldsymbol{H}^T = \boldsymbol{0}$. [3]

iii * Let $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$ be the received word, where $\boldsymbol{c}$ is a codeword from a Reed-Solomon code and $\boldsymbol{e} = [e_0, \cdots, e_{n-1}]$ is the error vector introduced by the channel. Define the syndrome vector $\boldsymbol{s} = \boldsymbol{y}\boldsymbol{H}^T = [s_0, \cdots, s_{n-k-1}]$. Define the syndrome polynomial $S(z) = \sum_{j=0}^{n-k-1} s_j z^j$. Prove that $S(z) \equiv \sum_{i \in \mathcal{I}} \frac{e_i \alpha^i}{1 - \alpha^i z} \mod z^{n-k}$ where $\mathcal{I} = \{i :\ e_i \neq 0,\ 0 \le i \le n-1\}$. *Hint*: The first step is to find the expression for the j-th element in $\boldsymbol{s}$, denoted by s_j, $j = 0, 1, \cdots, n-k-1$. [5]

iv Define the error locator polynomial

$$L(z) = \prod_{i \in \mathcal{I}} (1 - \alpha^i z).$$

and the error evaluator polynomial

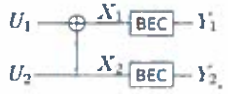
$$E(z) = \sum_{i \in \mathcal{I}} e_i \alpha^i \prod_{j \in \mathcal{I} \setminus \{i\}} (1 - \alpha^j z).$$

Specify the key equation used for Reed-Solomon decoding. [2]

(b) Construct a BCH code on $\mathbb{F}_2$ with $n = 31$ and $d \geq 7$ in the following way. Let α be a primitive element of $\mathbb{F}_{32}$. To make $d \geq 7$, one can choose to have $\alpha, \alpha^2, \cdots, \alpha^6$ as roots of the generator polynomial $g(x)$. Write down the generator polynomial $g(x) \in \mathbb{F}_{32}[x]$ of the constructed BCH code (as a product of minimal polynomials $M^{(i)}(x)$). What is the degree of the generator polynomial $g(x)$? What is the dimension k of the constructed BCH code? *Hint*: Consider cyclotomic cosets of 2 modulo 31. [7]

5. (Polar Codes)

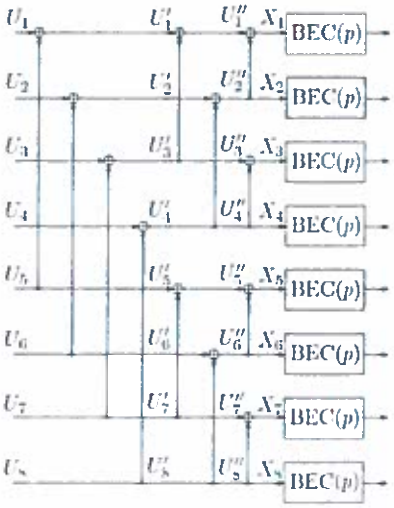
Consider the basic building block of polar codes:



It is clear that $[X_1 X_2] = [U_1 U_2]\, \boldsymbol{G}_1$ where $\boldsymbol{G}_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

For a BEC channel with erasure probability p, it can be calculated that the mutual information $I(U_1; \boldsymbol{Y}) = 1 - 2p + p^2$ and $I(U_2; U_1 \boldsymbol{Y}) = 1 - p^2$.

In particular, let $p = 0.2$. Consider three level of polar code diagram:



The mutual information at U_i'', denoted by I_i'', is given by

$$I_i'' = \begin{cases} 1 - 2 \cdot 0.2 + 0.2^2 = 0.64 & \text{if } i \text{ is odd.} \\ 1 - 0.2^2 = 0.96 & \text{if } i \text{ is even.} \end{cases}$$

(a) Let $[X_1 \cdots X_8] = [U_1 \cdots U_8]\, \boldsymbol{G}_3$. Write the specific form of $\boldsymbol{G}_3$. [3]

(b) Compute the mutual information at U_i', denoted by I_i', $i = 1, 2, \cdots, 8$. [5]

(c) Denote the mutual information at U_i by I_i. It holds that $I_1 < I_5 < I_3 < I_2 < I_7 < I_6 < I_4 < I_8$. Suppose that one constructs a polar code with parameter $n = 8$ and $k = 5$ by setting some of the U_i's to zero. Write the specific form of the generator matrix. [4]

(d) With the code constructed in Part (c), suppose that the received word is [1 0 0 ? 1 0 1 0]. What are the transmitted codeword $\boldsymbol{x}$ and the message $\boldsymbol{m}$? *Hint*: Start with the following matrix presentation

U	U'	U''	X
?	?	?	1
?	?	?	0
?	?	?	0
?	?	?	?
?	?	?	1
?	?	?	0
?	?	?	1
?	?	?	0

apply backward and forward decoding iteratively. [8]