EE4-07
EE9-CS7-23
EE9-SO11

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING
EXAMINATIONS 2014

MSc and EEE/EIE PART IV: MEng and ACGI

Corrected Copy

CODING THEORY

Wednesday, 21 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. The star notation * right after the sub-question numbering means that the particular sub-question may be difficult to solve.

1. (Euclidean Algorithm, Finite Fields, and Irreducible Polynomials)

   (a) List all the elements in the polynomial rings $\mathbb{F}_3[y]/y^2+2$ and $\mathbb{F}_3[y]/y^2+1$. [4]

   (b) Use Euclidean algorithm to find the multiplicative inverse of $y+1$ in both polynomial rings. [6]

   (c) Let α be the primitive element in $\mathbb{F}_9$ satisfying $\alpha^2+\alpha+2=0$.

      i). Find out all the cyclotomic cosets of 3 mod 8. [4]

      ii). Find the minimal polynomial of α^2. Write the expression in terms of the product of irreducible polynomials in $\mathbb{F}_9[x]$. [2]

      iii). Rewrite the minimal polynomial of α^2 in terms of an irreducible polynomial in $\mathbb{F}_3[x]$. (Coefficients have to be in $\mathbb{F}_3$.) [4]

2. (Euler's Theorem and RSA Cryptography)

Let p_1, p_2 be two distinct prime numbers. Let $n = p_1 p_2$ and $t = (p_1 - 1)(p_2 - 1)$. Define the set

$$\mathcal{S} = \{1 \leq a \leq p_1 p_2 - 1 : \gcd(a, n) = 1\}.$$

(a) It is a fact that for any two positive integers x and y, $x^{-1} \bmod y$ exists if and only if $\gcd(x, y) = 1$. Using this fact to prove that for any $a \in \mathcal{S}$ and $b \in \mathcal{S}$, it holds $ab \bmod n \in \mathcal{S}$. [4]

(b) For any $a \in \mathcal{S}$, define

$$a \cdot \mathcal{S} = \{a \cdot \ell \bmod n : \ell \in \mathcal{S}\}.$$

Prove that $a \cdot \mathcal{S} = \mathcal{S}$. [5]

(c) Prove that for all $a \in \mathcal{S}$, it holds that $a^t \equiv 1 \bmod n$. [5]

(d) * (An alternative proof of the RSA cryptography) In this part, with slight abuse of definition, we say $x \equiv y \bmod z$ if the three integers x, y, z satisfy the relation $z | (y - x)$. For example it holds that $3 \equiv 9 \bmod 2$ and $3 \equiv -1 \bmod 2$.

i). Show that for any two integers x and y, if $x \equiv y \bmod p_1$ and $x \equiv y \bmod p_2$, then $x \equiv y \bmod p_1 p_2$. [3]

ii). Use Fermat's Little Theorem and the claim in Question 2(d)i) to show that for any $a \in \{0, 1, 2, \cdots, p_1 p_2 - 1\}$, it holds that $a^{kt+1} \equiv a \bmod p_1 p_2$ where k is a positive integer. (Hint: you may first show that $a^{kt+1} \equiv a \bmod p_1$) [3]

3. (Linear Codes)

(a) Let $C \subset \mathbb{F}_3^4$ be a linear code generated by

$$G = \begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

i). Find the systematic generator matrix of C. [2]

ii). Find the corresponding parity check matrix H in the systematic form. [2]

iii). Compute the minimum distance of C and verify your computation. [3]

(b) Let $C = \{c \in \mathbb{F}_3^n : \text{weight}(c) \text{ is even.}\}$ where $n \geq 3$. Is C a linear code? Verify your answer. [3]

(c) Let $H \in \mathbb{F}_q^{m \times n}$ with $m < n$. Define the linear mapping

$$\begin{aligned} \varphi : \mathbb{F}_q^n &\to \mathbb{F}_q^m \\ v &\mapsto s = \varphi(v) = vH^T. \end{aligned}$$

For every $s \in \mathbb{F}_q^m$, the preimage of s under φ is defined as the set

$$\varphi^{-1}(s) = \left\{ v \in \mathbb{F}_q^n : \varphi(v) = s \right\}.$$

i). Show that $\varphi^{-1}(0)$ is a linear code. [2]

ii). Suppose that $\varphi(v) = s$. Show that $v + \varphi^{-1}(0) \subset \varphi^{-1}(s)$. [2]

iii). Prove that $\forall w \in \varphi^{-1}(s)$ it holds that $w \in v + \varphi^{-1}(0)$. This, together with Part 3(c)ii), establish that $v + \varphi^{-1}(0) = \varphi^{-1}(s)$. [3]

iv). Let $s_1, s_2 \in \mathbb{F}_q^m$ be such that $s_1 \neq s_2$. Prove that $\varphi^{-1}(s_1) \bigcap \varphi^{-1}(s_2) = \phi$. [3]

4. (Encoding and decoding)

(a) The parity-check matrix of the binary Hamming code $\mathcal{H}_3$ can be written as

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

i). Assume that the received vector is $\boldsymbol{y} = [0\,1\,0\,1\,1\,1\,1]$. Find the most plausible correction of $\boldsymbol{y}$ from the syndrome vector. Show the main steps of the computation. [3]

ii). Find the generator matrix of *the dual code* of $\mathcal{H}_3$. [2]

(b) Consider a cyclic code $\mathcal{C}$ with codeword length n. Define the generating function of a codeword $\boldsymbol{c} = [c_0, c_1, \cdots, c_{n-1}]$ as the polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$.

i). Prove that $x \cdot c(x) \mod x^n - 1$ is the generating function of a codeword in the $\mathcal{C}$. [3]

ii). Among all the generating functions, how to find the generator polynomial $g(x)$ for the cyclic code? (Proof is not required) [2]

iii). Prove that the generator polynomial $g(x)$ satisfies $g(x) \mid (x^n - 1)$. [5]

iv). How to construct a cyclic code over $\mathbb{F}_q$ with codeword length $n = q^m - 1$ and distance $d \geq \delta$? Here, $\delta < n$ is the designed distance. Prove that $d \geq \delta$ in your construction. [5]

5. (Applications)

(a) *(Primitive elements) To employ the discrete logarithm function for encryption, one needs a finite field $\mathbb{F}_q$ and a primitive element $b \in \mathbb{F}_q$. Given an element, say $a \in \mathbb{F}_q$, the naive way to check whether a is primitive or not is to check a^x for all $x = 1, 2, \cdots, q-1$. This is often computationally impractical when q is large. Smarter methods are needed. Now suppose that $q = 2^6 = 64$. How can you bring down the computational complexity in figuring out whether a given element $a \in \mathbb{F}_q$ is primitive or not? Explain why your method works. [7]

(b) (Interpolation by polynomials) Let $x_1, x_2, \cdots, x_n$ be n *distinct real numbers.* Let $y_1, y_2, \cdots, y_n$ be n arbitrarily chosen *real numbers.* One is asked to construct a polynomial $P(x)$ with degree at most $n-1$ such that $P(x_i) = y_i$, $i = 1, 2, \cdots, n$.

i). Show that the polynomial

$$P(x) = \sum_{\ell=1}^{n} y_\ell \prod_{\substack{1 \le j \le n \\ j \neq \ell}} \frac{x - x_j}{x_\ell - x_j}$$

satisfies the requirement. [6]

ii). *Prove that the polynomial that satisfies the requirement is unique. [7]