

IMPERIAL COLLEGE LONDON

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING  
EXAMINATIONS 2015

MSc and EEE/EIE PART IV: MEng and ACGI

**CODING THEORY**

Corrected Copy

Monday, 11 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. (Fundamentals)

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

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. [5]

ii Find the polynomials  $a(x)$  and  $b(x)$  such that  $h(x) = a(x)f(x) + b(x)g(x)$ . [5]

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

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

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

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

iii Assume that a message  $m_1$  is encoded into a codeword  $c_1$  using  $G'$ . Let the received word be  $y_1 = [1 \ 0 \ 0 \ 1 \ 1 \ 1 \ 0]$ . Compute the syndrome vector. 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  $m$  is encoded into a codeword  $c$  using  $G'$ . The codeword  $c$  is transmitted over an erasure channel and the received word is given by  $y = [0 \ 0 \ 0 \ 0 \ ? \ ? \ 1]$ . Set the question marks in  $y$  to zero and compute the corresponding syndrome vector. Find the transmitted codeword  $c$  and the message  $m$ . [3]

2. (Linear Codes) Let  $\mathcal{C} \subset \mathbb{F}_q^n$  be a linear code with parameters  $[n, k, d]$ . Denote its generator and parity-check matrices by  $\mathbf{G}$  and  $\mathbf{H}$  respectively.

(a) Prove that the code distance  $d$  is the minimum weight of the nonzero code-words, i.e.,  $d = \min_{\mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}} \text{wt}(\mathbf{c})$ . [2]

(b) Prove that the code distance is  $d$  if and only if

- i every  $d - 1$  columns of  $\mathbf{H}$  are linearly independent;
- ii there exist  $d$  columns of  $\mathbf{H}$  that are linearly dependent. [6]

(c) Based on the statements in Part (b), prove the singleton bound  $d \leq n - k + 1$ . The codes that attain the singleton bound are called maximum distance separable (MDS). [2]

(d) Let  $\alpha$  be the primitive element of  $\mathbb{F}_q$ . Show that the code with the parity-check matrix

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k} & \alpha^{(n-k) \cdot 2} & \dots & \alpha^{(n-k) \cdot (n-1)} \end{bmatrix}$$

is MDS. You may use the fact that the standard Vandermonde matrix

$$\mathbf{V}_L = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \beta_1 & \beta_2 & \dots & \beta_L \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^{L-1} & \beta_2^{L-1} & \dots & \beta_L^{L-1} \end{bmatrix}$$

satisfies  $|\mathbf{V}_L| = \prod_{\ell < m} (\beta_m - \beta_\ell)$ . [2]

(e) Let  $\mathcal{C}$  be an arbitrary MDS code and  $\mathcal{C}^\perp$  be its dual code. Write the parameters  $[n', k']$  of  $\mathcal{C}^\perp$  in terms of  $n$  and  $k$ . Write the generator matrix  $\mathbf{G}'$  and the parity-check matrix  $\mathbf{H}'$  of  $\mathcal{C}^\perp$  in terms of  $\mathbf{G}$  and  $\mathbf{H}$ . [2]

(f) Prove that the dual code  $\mathcal{C}^\perp$  is also MDS. [6]

### 3. (Cryptography)

- (a) Let  $p_1, p_2$  be two distinct prime numbers. Let  $n = p_1 p_2$ . Let  $1 < d < n$  and  $1 < e < n$  be two properly chosen integers. Let  $1 \leq m < n$  be a message to be encrypted. The RSA cryptography scheme is described below.

**Public key:**  $(n, e)$   
**Private key:**  $d$   
**Encryption:** The message  $m$  is encrypted into  $c$  via  $c = m^e \bmod n$ .  
**Decryption:**  $\hat{m} = c^d \bmod n$ .

- i How would you choose the integers  $d$  and  $e$  in order that  $\hat{m} = m$ . (A proof is not required.) [2]
  - ii If the factorisation  $n = p_1 p_2$  is known, which method can be used to find the private key  $d$  and hence crack the RSA scheme? [2]
- (b) Let  $p$  be a prime number and  $b$  be a primitive element in  $\mathbb{F}_p$ . Let  $1 \leq d \leq p-1$  and  $e$  be two properly chosen integers. Let  $m \in \mathbb{F}_p^*$  be a message to be encrypted. The ElGamal encryption process is given as follows.

**Public key:**  $e$   
**Private key:**  $d$   
**Encryption:** Randomly generate an integer  $t$ . The message  $m$  is encrypted into  $(x, y)$  by evaluating  $(x, y) = (b^t, me^t)$ .

- i Denote the mapping that maps  $d$  to  $e$  by  $\tau$ . Identify the mapping  $\tau$  and describe the decryption process. [4]
- ii Prove that the mapping  $\tau$  is invertible by showing
  - A. that  $1 \leq e = \tau(d) \leq p-1$ ; (You may use Euclid's Lemma: if  $p|ab$  then  $p|a$  or  $p|b$ .) [3]
  - B. that the mapping  $\tau$  is one-to-one; and [3]
  - C. that the mapping  $\tau$  is onto. [2]
- iii Generally speaking it is computationally challenging to check whether a given element  $\beta \in \mathbb{F}_p^*$  is a primitive element or not. One way to simplify the computation is to use the fact that  $\text{ord}(\beta) \mid (p-1)$ ,  $\forall \beta \in \mathbb{F}_p^*$ . Prove this fact. You may use Fermat's little theorem stating that  $\beta^{p-1} = 1$ ,  $\forall \beta \in \mathbb{F}_p^*$ . [4]

4. (Cyclic and BCH codes)

- (a) Let  $\mathcal{C} \subset \mathbb{F}_q^n$  be a cyclic code. Let  $g(x) \in \mathcal{C}$  be the nonzero polynomial of the lowest degree. Assume that  $g(x)$  is monic. Show that for all  $c(x) \in \mathcal{C}$  the relation  $g(x) \mid c(x)$  holds. Furthermore, prove the uniqueness of  $g(x)$ . [5]
- (b) Let  $q = 2$  and  $n = 15$ . Construct a BCH code with distance  $d \geq 7$  in the following way.
- i Write down all the cyclotomic cosets of 2 modulo 15. [5]
  - ii Let  $\alpha$  be a primitive element of  $\mathbb{F}_{16}$ . Write down the generator polynomial  $g(x) \in \mathbb{F}_{16}[x]$  of the constructed BCH code (as a product of minimal polynomials). [5]
  - iii Let  $x^{15} - 1 = h(x)g(x) + q(x)$ , where  $g(x)$  is the generator polynomial of the constructed BCH code and all the polynomials are in  $\mathbb{F}_{16}[x]$ . What are  $h(x)$  and  $q(x)$  respectively? [2]
  - iv It can be shown that both  $g(x)$  and  $h(x)$  are polynomials in  $\mathbb{F}_2[x]$ . That is,  $g(x) = g_0 + g_1x + \dots + g_dx^d$  and  $h(x) = h_0 + h_1x + \dots + h_\ell x^\ell$  where the coefficients  $g_i \in \mathbb{F}_2$  and  $h_j \in \mathbb{F}_2$ . Write the form of the generator and parity-check matrices of the constructed BCH code in terms of  $g_i$ 's and  $h_j$ 's. [3]

5. (Reed-Muller codes)

The (first order) Reed-Muller codes  $\mathcal{R}_m$  are binary codes defined, for all integers  $m \geq 1$ , recursively as follows:

- $\mathcal{R}_1 = \mathbb{F}_2^2 = \{00, 01, 10, 11\}$ ;
- for  $m \geq 1$ ,  $\mathcal{R}_{m+1} = \{[u, u] : u \in \mathcal{R}_m\} \cup \{[u, u + 1] : u \in \mathcal{R}_m\}$ , where  $1$  is the all one vector of the proper length.

- (a) Use the definition of linear codes and mathematical induction to prove that  $\mathcal{R}_m$  is a linear code. [5]
- (b) Let  $G_m$  be the generator matrix for  $\mathcal{R}_m$ . Find the generator matrix for  $\mathcal{R}_{m+1}$  in terms of  $G_m$ . [4]
- (c) Find the code length  $n$  and the code dimension  $k$  for  $\mathcal{R}_m$ . [3]
- (d) Use mathematical induction to prove that every codeword in  $\mathcal{R}_m$  except  $0$  and  $1$  has weight  $2^{m-1}$ . This implies that  $d(\mathcal{R}_m) = 2^{m-1}$ . [8]

