

MSc and EEE/EIE PART IV: MEng and ACGI

Time allowed: 3:00 hours

Answer ALL questions.

All the questions carry equal marks.

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. (Linear Codes and Error Probability) Consider a linear code \mathcal{C} over \mathbb{F}_3 defined by the parity check matrix

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

- (a) Find the minimum distance of \mathcal{C} . Prove your answer. [4]
- (b) Find the generator matrix of \mathcal{C} in systematic form. [4]
- (c) A codeword in \mathcal{C} is transmitted through a ternary symmetric channel and the word $\mathbf{y} = [1 \ 1 \ 2 \ 2]$ is received.
 - i). Find the syndrome vector of \mathbf{y} . [2]
 - ii). Find the codeword in \mathcal{C} that is produced by applying the minimum distance decoder. [2]
- (d) A codeword in \mathcal{C} is transmitted through an erasure channel. Let $\mathbf{y} = [? \ ? \ 2 \ 2]$ be the received word, where the question marks denote that the corresponding symbols have been erased. Find the most plausible correction of \mathbf{y} . [4]
- (e) Consider the case where a code $\mathcal{C} \subset \mathbb{F}_q^n$ is used for the memoryless q -ary symmetric channel with crossover probability p :

$$\Pr(y_i \text{ received} | c_i \text{ transmitted}) = \begin{cases} 1 - p & \text{if } y_i = c_i, \\ p/(q - 1) & \text{otherwise.} \end{cases}$$

Find the relationship between p and q such that the minimum distance decoder (MDD) is equivalent to the maximum likelihood decoder (MLD). [4]

2. (Linear Codes) Let \mathcal{C}_1 and \mathcal{C}_2 be two linear codes over \mathbb{F}_q of the same length n . Let \mathbf{G}_i , \mathbf{H}_i , k_i , and d_i be the generator matrix, the parity-check matrix, the dimension, and the minimum distance of \mathcal{C}_i , $i = 1, 2$, respectively. Define

- $\mathcal{C}_3 = \{[\mathbf{c}_1, \mathbf{c}_2] : \mathbf{c}_1 \in \mathcal{C}_1, \mathbf{c}_2 \in \mathcal{C}_2\}$.
- $\mathcal{C}_4 = \mathcal{C}_1 \cup \mathcal{C}_2$.

- (a) Show that \mathcal{C}_3 is a linear code. [5]
- (b) Write the generator matrix \mathbf{G}_3 and the parity-check matrix \mathbf{H}_3 for the code \mathcal{C}_3 in terms of \mathbf{G}_1 , \mathbf{G}_2 , \mathbf{H}_1 , and \mathbf{H}_2 . [5]
- (c) Determine the dimension k_3 and the minimum distance d_3 of the code \mathcal{C}_3 in terms of k_1 , k_2 , d_1 , and d_2 . Prove your results. [5]
- (d) *Suppose that $k_1 < k_2$. Show that \mathcal{C}_4 is a linear code if and only if $\mathcal{C}_1 \subset \mathcal{C}_2$. [5]

3. (Finite Field)

- (a) Consider finite fields $\mathcal{F}_1 = \mathbb{F}_2[x] / (x^3 + x^2 + 1)$ and $\mathcal{F}_2 = \mathbb{F}_2[y] / (y^3 + y + 1)$. Consider the mapping φ from \mathcal{F}_1 to \mathcal{F}_2 defined by $\varphi(x) = y + 1$. Consider two polynomials $f_1(x) = x^2 + 1$ and $f_2(x) = x^2 + x + 1$ taken from \mathcal{F}_1 . Compute the following: [10]

- i). $f_1(x) \cdot f_2(x)$,
- ii). $\varphi(f_1(x) \cdot f_2(x))$,
- iii). $\varphi(f_1(x))$,
- iv). $\varphi(f_2(x))$, and
- v). $\varphi(f_1(x)) \cdot \varphi(f_2(x))$.

(b)

- i). Find all the cyclotomic cosets of 2 mod 7. [3]
- ii). Let α be a primitive element of \mathbb{F}_8 . Find the irreducible polynomials in $\mathbb{F}_2[x]$ that factor $x^7 - 1$. [3]
- iii). *Count the number of distinct cyclic codes in \mathbb{F}_2 of length 7. [4]

4. (Reed-Solomon, cyclic, and BCH codes)

Let α be a primitive element of \mathbb{F}_9 . Define $\mathbf{A} \in \mathbb{F}_9^{4 \times 8}$ by

$$\mathbf{A} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{21} \\ 1 & \alpha^4 & \alpha^8 & \cdots & \alpha^{28} \end{bmatrix}.$$

- (a) Let \mathcal{C} be a code over \mathbb{F}_9 and its parity-check matrix be the matrix \mathbf{A} . What are the parameters, $[n, k, d]$, of \mathcal{C} ? Find the number of errors that this code can correct. [4]
- (b) Suppose that a codeword $\mathbf{c} \in \mathcal{C}$ is transmitted and a word $\mathbf{y} = \mathbf{c} + \mathbf{e}$ is received where $\mathbf{e} \in \mathbb{F}_9^8$ is the error vector. Define the set of error positions $\mathcal{I} = \{0 \leq i \leq 7 : e_i \neq 0\}$. Define the error locator polynomial as

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

Prove that

$$\begin{cases} L(\alpha^{-k}) = 0 & \text{if } 0 \leq k \leq 7 \text{ and } k \in \mathcal{I}, \\ L(\alpha^{-k}) \neq 0 & \text{if } 0 \leq k \leq 7 \text{ and } k \notin \mathcal{I}. \end{cases} \quad [4]$$

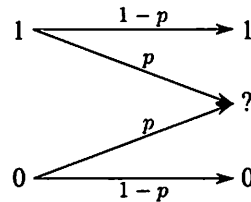
- (c) Suppose that $\mathcal{I} \neq \emptyset$. Fix an $i \in \mathcal{I}$. Find $\frac{d}{dz} L(z)$ when $z = \alpha^{-i}$. [4]
- (d) The syndrome vector is defined via $\mathbf{s} = [s_0, \dots, s_3] = \mathbf{e} \mathbf{A}^T$. The syndrome polynomial is defined as $S(z) = \sum_{j=0}^3 s_j z^j$. Prove that

$$S(z) = \sum_{i \in \mathcal{I}} \frac{e_i \alpha^i}{1 - \alpha^i z} \text{ mod } z^4. \quad [4]$$

- (e) Define a cyclic code $\mathcal{C}' = \{\mathbf{c} \in \mathbb{F}_3^8 : \mathbf{c} \mathbf{A}^T = \mathbf{0}\} \subset \mathbb{F}_3^8$. Find its generator polynomial $g(x)$. [4]

5. (Decoding on graphs with the application of erasure correction)

Consider the following binary erasure channel:



- (a) Assume that $\Pr(x=0) = \Pr(x=1) = 1/2$. Find $\Pr(x|y)$ when x varies in $\{0, 1\}$ and y varies in $\{0, 1, ?\}$. [5]
- (b) Draw the Tanner graph that corresponds to the parity-check matrix

$$\mathbf{H} = \begin{bmatrix} & x_1 & x_2 & x_3 & x_4 & x_5 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{matrix} c_1 \\ c_2 \end{matrix}.$$

(Notations in the Tanner graph are required to be consistent with the above ones.) [5]

- (c) Assume conditional independence, i.e., $\Pr(\mathbf{x}|\mathbf{y}) = \prod_i \Pr(x_i|y_i)$. Assume that $\mathbf{y}_{3:5} = [y_3, y_4, y_5] = [?, 1, 1]$. Decode x_3 by computing $\Pr(x_3|\mathbf{y}_{3:5})$. [5]
- (d) * Consider a code \mathcal{C} which may or may not be linear. Assume that the minimum distance of \mathcal{C} is d . Prove that it can correct $d-1$ erasures. (Note that the “up to” part is not required in your solution, in order to simplify the problem.) [5]

Solution of Question 1.

(a) Since every pair of columns of \mathbf{H} are linearly independent, one has $d \geq 3$.

On the other hand, there exist three columns in \mathbf{H} , for example, columns 1, 2 and 3, linearly dependent, $d \leq 3$. Hence, $d(\mathcal{C}) = 3$. [4]

(b) The generator matrix in the systematic form is given by

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & -1 & 0 \\ 2 & 1 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{bmatrix}. \quad [4]$$

(c)

i). $\mathbf{s} = \mathbf{y}\mathbf{H}^T = [1 \ 2]$. [2]

ii). Since $\mathbf{s} = (\mathbf{c} + \mathbf{e})\mathbf{H}^T = \mathbf{e}\mathbf{H}^T$, it is clear that $\hat{\mathbf{e}} = [0 \ 0 \ 0 \ 2]$. As a result, $\hat{\mathbf{c}} = \mathbf{y} - \hat{\mathbf{e}} = [1 \ 1 \ 2 \ 0]$. [2]

(d) The only codeword of which the last two symbols are both 2 is given by $[2 \ 2] \cdot \mathbf{G} = [0 \ 2 \ 2 \ 2]$. Hence the decoding result is $\hat{\mathbf{c}} = [0 \ 2 \ 2 \ 2]$. [4]

(e) For any given $\mathbf{c} \in \mathcal{C} \subset \mathbb{F}_q^n$ and $\mathbf{y} \in \mathbb{F}_q^n$, let $d = d_H(\mathbf{y}, \mathbf{c})$. Then

$$\Pr(\mathbf{y}|\mathbf{c}) = \left(\frac{p}{q-1}\right)^d (1-p)^{n-d} = (1-p)^n \left(\frac{p}{1-p} \cdot \frac{1}{q-1}\right)^d.$$

The sufficient and necessary condition for the equivalence is that

$$\frac{p}{1-p} \cdot \frac{1}{q-1} < 1.$$

Simple algebra shows that this is equivalent to $q > \frac{1}{1-p}$ or $p < 1 - \frac{1}{q}$. [4]

Solution of Question 2.

(a) For any $\mathbf{c}, \mathbf{c}' \in \mathcal{C}_3$ and $\lambda, \lambda' \in \mathbb{F}_q$, one has

$$\begin{aligned}\lambda \mathbf{c} + \lambda' \mathbf{c}' &= \lambda [\mathbf{c}_1, \mathbf{c}_2] + \lambda' [\mathbf{c}'_1, \mathbf{c}'_2] \\ &= [\lambda \mathbf{c}_1 + \lambda' \mathbf{c}'_1, \lambda \mathbf{c}_2 + \lambda' \mathbf{c}'_2] \\ &= [\mathbf{c}''_1, \mathbf{c}''_2] \in \mathcal{C}_3,\end{aligned}$$

for some $\mathbf{c}''_1 \in \mathcal{C}_1$ and $\mathbf{c}''_2 \in \mathcal{C}_2$, where the last equality follows from the linearity of \mathcal{C}_1 and \mathcal{C}_2 . [5]

(b) It holds that

$$\mathbf{G}_3 = \begin{bmatrix} \mathbf{G}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{G}_2 \end{bmatrix}, \text{ and } \mathbf{H}_3 = \begin{bmatrix} \mathbf{H}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_2 \end{bmatrix} \quad [5]$$

(c) Note that the size of \mathcal{C}_3 is $q^{k_1} \cdot q^{k_2}$. It is clear that $k_3 = k_1 + k_2$. The same conclusion can be derived from the form of the generator matrix \mathbf{G} as well. The computation of the distance of \mathcal{C}_3 relies on the fact that \mathcal{C}_3 is linear. It holds that

$$\begin{aligned}d(\mathcal{C}_3) &= \min_{\mathbf{c} \in \mathcal{C}_3} \text{wt}(\mathbf{c}) \\ &= \min_{\mathbf{c}_1 \in \mathcal{C}_1, \mathbf{c}_2 \in \mathcal{C}_2} \text{wt}([\mathbf{c}_1, \mathbf{c}_2]) \\ &= \min(d_1, d_2).\end{aligned}$$

[5]

(d) The “if” part: $\mathcal{C}_1 \subset \mathcal{C}_2 \Rightarrow \mathcal{C}_4 = \mathcal{C}_1 \cup \mathcal{C}_2 = \mathcal{C}_2 \Rightarrow \mathcal{C}_4$ is linear.

The “only if” part: Suppose that $\mathcal{C}_1 \not\subset \mathcal{C}_2$. It follows that $\mathcal{C}_1 \setminus \mathcal{C}_2 \neq \emptyset$ and $\mathcal{C}_2 \setminus \mathcal{C}_1 \neq \emptyset$ where the second inequality holds as $|\mathcal{C}_1| < |\mathcal{C}_2|$. Hence, there exist $\mathbf{c}_1 \in \mathcal{C}_1 \setminus \mathcal{C}_2 \subset \mathcal{C}_4$ and $\mathbf{c}_2 \in \mathcal{C}_2 \setminus \mathcal{C}_1 \subset \mathcal{C}_4$. We claim that $\mathbf{c}_1 + \mathbf{c}_2 \notin \mathcal{C}_1$ because otherwise $\mathbf{c}_2 = (\mathbf{c}_1 + \mathbf{c}_2) - \mathbf{c}_1$ will be in \mathcal{C}_1 , which contradicts the choice of \mathbf{c}_2 . Similarly, $\mathbf{c}_1 + \mathbf{c}_2 \notin \mathcal{C}_2$. Hence, $\mathbf{c}_1 + \mathbf{c}_2 \notin \mathcal{C}_1 \cup \mathcal{C}_2 = \mathcal{C}_4$. Therefore, \mathcal{C}_4 is not linear. The above arguments show that if \mathcal{C}_4 is linear, then $\mathcal{C}_1 \subset \mathcal{C}_2$. The “only if” part is therefore proved. [5]

Solutions of Question 3.

(a)

$$\begin{aligned}
 f_1(x) \cdot f_2(x) &= (x^2 + 1)(x^2 + x + 1) \\
 &= x^4 + x^3 + x^2 + x^2 + x + 1 \\
 &= x^4 + x^3 + x + 1 \\
 &= x(x^2 + 1) + x^3 + x + 1 \\
 &= 1,
 \end{aligned}$$

$$\varphi(f_1(x) \cdot f_2(x)) = \varphi(1) = 1,$$

$$\varphi(f_1(x)) = (y + 1)^2 + 1 = y^2,$$

$$\begin{aligned}
 \varphi(f_2(x)) &= (y + 1)^2 + (y + 1) + 1 \\
 &= y^2 + y + 1,
 \end{aligned}$$

and

$$\begin{aligned}
 \varphi(f_1(x)) \cdot \varphi(f_2(x)) &= y^2(y^2 + y + 1) \\
 &= y^4 + y^3 + y^2 \\
 &= y(y + 1) + y + 1 + y^2 \\
 &= 1.
 \end{aligned}$$

[10]

(b)

$$\text{i). } C_0 = \{0\}, C_1 = \{1, 2, 4\}, C_3 = \{3, 6, 5\}. \quad [3]$$

$$\text{ii). } x^7 - 1 \text{ can be factored into three irreducible polynomials: } x - 1, (x - \alpha) \cdot (x - \alpha^2) \cdot (x - \alpha^4) \text{ and } (x - \alpha^3) \cdot (x - \alpha^5) \cdot (x - \alpha^6). \quad [3]$$

iii). Note that the generator polynomial $g(x)$ of a cyclic code of length 7 has to satisfy that $g(x) \in \mathbb{F}_2[x]$ and $g(x) \mid x^7 - 1$. From the factorization of $x^7 - 1$, the number of distinct cyclic codes are given by $\binom{3}{0} + \binom{3}{1} + \binom{3}{2} + \binom{3}{3} = 2^3 = 8$, where $\binom{3}{0}$ and $\binom{3}{3}$ are included as the constant

polynomial 1 (corresponding to the code $\mathcal{C} = \mathbb{F}_2^7$) and the polynomial $x^7 - 1$ (corresponding to the trivial code $\mathcal{C} = \{0\}$) generate cyclic codes as well. [4]

Solutions of Question 4.

- (a) $[n, k, d] = [8, 4, 5]$: It is clear that $n = 8$ and $k = n - (n - k) = 8 - 4 = 4$. Note that every four columns of \mathbf{A} forms a Vandemonde matrix, every four columns of \mathbf{A} are linearly independent, i.e., $d \geq 5$. Furthermore, every five columns of \mathbf{A} must be linearly dependent and hence $d = 5$.

The number of errors that this code can correct is $\lfloor \frac{d-1}{2} \rfloor = 2$. [4]

- (b) Given $0 \leq k \leq 7$, it holds that $\alpha^i \alpha^{-k} = 1$ if and only if $k = i$.

When $k \notin \mathcal{I}$, $L(z)$ is a product of nonzero elements and hence nonzero.

When $k \in \mathcal{I}$, there exists an $i \in \mathcal{I}$ such that $(1 - z^i z^{-k}) = 0$ and therefore $L(z) = 0$. [4]

- (c) Elementary algebra shows that

$$\frac{d}{dz} L(z) = \sum_{j \in \mathcal{I}} (-\alpha^j) \prod_{\ell \in \mathcal{I}, \ell \neq j} (1 - \alpha^\ell z).$$

Let $z = \alpha^{-i}$. Then the term

$$\prod_{\ell \in \mathcal{I}, \ell \neq j} (1 - \alpha^\ell z) = \begin{cases} 0 & \text{if } j \neq i \\ \prod_{\ell \in \mathcal{I}, \ell \neq i} (1 - \alpha^{\ell-i}) & \text{if } j = i \end{cases}.$$

Hence,

$$\left. \frac{d}{dz} L(z) \right|_{z=\alpha^{-i}} = -\alpha^i \prod_{\ell \in \mathcal{I}, \ell \neq i} (1 - \alpha^{\ell-i}).$$
 [4]

- (d) It is straightforward to see that $s_j = \sum_{i \in \mathcal{I}} e_i \alpha^{i(j+1)}$ and

$$\begin{aligned} S(z) &= \sum_{j=0}^3 z^j \sum_{i \in \mathcal{I}} e_i \alpha^{i(j+1)} \\ &= \sum_{i \in \mathcal{I}} e_i \alpha^i \sum_{j=0}^3 \alpha^{ij} z^j \\ &\equiv \sum_{i \in \mathcal{I}} e_i \alpha^i \sum_{j=0}^{\infty} (\alpha^i z)^j \pmod{z^4} \\ &= \sum_{i \in \mathcal{I}} e_i \alpha^i \frac{1}{1 - \alpha^i z}. \end{aligned}$$

[4]

- (e) Let $g(x) = \sum_{i=0}^{\ell} g_i x^i$ where $g_i \in \mathbb{F}_3$. Since $\mathbf{g} = [g_0, \dots, g_7] \in \mathcal{C}$, it holds $\mathbf{g}\mathbf{A}^T = \mathbf{0}$. Hence, $\alpha, \alpha^2, \alpha^3$, and α^4 are roots of $g(x)$. The corresponding cyclotomic cosets (of 3 mod 8) are given by $\mathcal{C}_1 = \{1, 3\}$, $\mathcal{C}_2 = \{2, 6\}$, and $\mathcal{C}_4 = \{4\}$. Therefore,

$$\begin{aligned} g(x) &= \text{lcm}(M^{(1)}(x), M^{(2)}(x), M^{(3)}(x), M^{(4)}(x)) \\ &= \text{lcm}(M^{(1)}(x), M^{(2)}(x), M^{(4)}(x)) \\ &= M^{(1)}(x) \cdot M^{(2)}(x) \cdot M^{(4)}(x), \end{aligned}$$

where

$$\begin{aligned} M^{(1)}(x) &= (x - \alpha)(x - \alpha^3), \\ M^{(2)}(x) &= (x - \alpha^2)(x - \alpha^6), \\ M^{(4)}(x) &= (x - \alpha^4). \end{aligned}$$

[4]

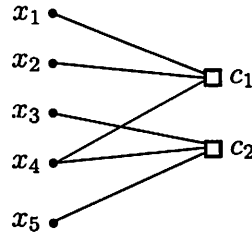
Solutions of Question 5.

(a) It is straightforward to compute that

$$\begin{aligned}\Pr(x = 0|y = 0) &= 1, \Pr(x = 1|y = 0) = 0, \\ \Pr(x = 0|y = 1) &= 0, \Pr(x = 1|y = 1) = 1, \\ \Pr(x = 0|y = ?) &= \frac{1}{2}, \Pr(x = 1|y = ?) = \frac{1}{2},\end{aligned}$$

by using the Bayes' theorem $\Pr(x|y) = \Pr(y|x) \Pr(x) / \Pr(y)$ and the fact that $\Pr(y) = \sum_x \Pr(y|x) \Pr(x)$. [5]

(b) The Tanner graph is given by



[5]

(c) Note that

$$\begin{aligned}\Pr(x_3 = 0|\mathbf{y}_{3:5}) &= \Pr(x_3 = 0, x_4 + x_5 = 0|\mathbf{y}_{3:5}) \\ &= \Pr(x_3 = 0|y_3) \Pr(x_4 + x_5 = 0|y_4 y_5) \\ &= \frac{1}{2} (\Pr(x_4 = 1|y_4) \Pr(x_5 = 1|y_5) \\ &\quad + \Pr(x_4 = 0|y_4) \Pr(x_5 = 0|y_5)) \\ &= \frac{1}{2} (1 + 0) = \frac{1}{2},\end{aligned}$$

and

$$\begin{aligned}\Pr(x_3 = 1|\mathbf{y}_{3:5}) &= \Pr(x_3 = 1, x_4 + x_5 = 1|\mathbf{y}_{3:5}) \\ &= \Pr(x_3 = 1|y_3) \Pr(x_4 + x_5 = 1|y_4 y_5) \\ &= \frac{1}{2} (0 + 0) = 0.\end{aligned}$$

We decode x_3 as 0. [5]

(d) Let \mathcal{I} denote the index set containing the locations of the erased bits and \mathcal{I}^c be its complement. Assume that $|\mathcal{I}| \leq d - 1$. For any two different

codewords \mathbf{c} and \mathbf{c}' from the codebook \mathcal{C} , it holds

$$\begin{aligned} d &\leq d_H(\mathbf{c}, \mathbf{c}') = d_H(\mathbf{c}_I, \mathbf{c}'_I) + d_H(\mathbf{c}_{I^c}, \mathbf{c}'_{I^c}) \\ &\leq d - 1 + d_H(\mathbf{c}_{I^c}, \mathbf{c}'_{I^c}), \end{aligned}$$

which implies that $d_H(\mathbf{c}_{I^c}, \mathbf{c}'_{I^c}) \geq 1$. In other words, the mapping that maps a codeword \mathbf{c} to \mathbf{c}_{I^c} is one to one. The inverse mapping is well defined. The erasures can be corrected. [5]