**MMTE-005**

# ASSIGNMENT BOOKLET

**M.Sc. (Mathematics with Applications in Computer Science)**

**CODING THEORY**

**(Valid from July 1, 2021– June 30, 2022)**

**It is compulsory to submit the assignment before filling in the exam form.**

**School of Sciences**
**Indira Gandhi National Open University**
**Maidan Garhi, New Delhi 110068**
**2021-2022**

Dear Student,
Please read the section on assignments in the Programme Guide that we sent you after your enrolment. As you may know already from the programme guide, the continuous evaluation component has 20% weightage. This assignment is for the continuous evaluation component of the course.

**Instructions for Formating Your Assignments**

Before attempting the assignment please read the following instructions carefully.

1) On top of the first page of your answer sheet, please write the details exactly in the following format:

---

**ROLL NO. :** .....

**NAME :** .....

**ADDRESS :** .....

.....

.....

**COURSE CODE :** ..... .....

**COURSE TITLE :** .....

**STUDY CENTRE :** ..... **DATE** .....

---

**PLEASE FOLLOW THE ABOVE FORMAT STRICTLY TO FACILITATE EVALUATION AND TO AVOID DELAY.**

2) Use only foolscap size writing paper (but not of very thin variety) for writing your answers.

3) Leave 4 cm margin on the left, top and bottom of your answer sheet.

4) Your answers should be precise.

5) While solving problems, clearly indicate which part of which question is being solved.

6) Write all the answers in your own words. Do not copy from the internet, from your fellow students or from any other source. If your assignment is found to be copied, it will be rejected.

7) This assignment is valid only up to 30th June, 2022. If you fail in this assignment or fail to submit it by 30th June, 2022, then you need to get the assignment for 2022-23 and submit it as per the instructions given in the Programme Guide.

8) It is **compulsory** to submit the assignment before you submit your examination form.

9) For any doubts, clarifications and corrections, write to `svenkat@ignou.ac.in`.

We **strongly** suggest that you retain a copy of your answer sheets.

Wish you good luck.

# Assignment

**Course Code: MMTE-005**
**Assignment Code: MMTE-005/TMA/2021-22**
**Maximum Marks: 100**

**Note:** In this assignment, the notations, symbols, definitions and conventions will be as in the prescribed book 'Fundamentals of Error-Correcting Codes' by Huffman and Pless. Also, 'the book' will always mean the prescribed book.

1) a) Define the generator matrix and parity check matrix of an $[n,k]$ linear code. Consider the linear code

$$\mathscr{C} = \{ (x_1,x_2,x_3,x_4,x_5) \in \mathbf{F}_2^n | x_1+x_2+x_3 = 0, x_2+x_4+x_5 = 0\}$$

Find a generator matrix and a parity check matrix of the code. What is the dimension of the code? (6)

b) Prove Theorem 1.4.12. (**Hint:** Consider the kernel and the image of the map $f\colon \mathscr{C} \to \mathbf{F}_q$ given by $(x_1,x_2,\ldots,x_n) \to x_1+x_2+\cdots+x_n$.) (4)

2) The aim of this exercise is to give a step by step solution of exerise 35, page 20 of the book.

a) Let $P$ be an $n \times n$permutation matrix and $\mathbf{x}, \mathbf{y} \in \mathbf{F}_q^n$.

i) Prove that

$$\mathbf{e_i}P \cdot \mathbf{e_j}P = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{Otherwise} \end{cases}$$

where $\mathbf{e_i}$ is the row vector with 1 in the i$^{\text{th}}$ position and 0 elsewhere. (**Hint:** Each row of $P$ is $\mathbf{e_i}$ for some $i$. (Why?))

ii) Prove that $\mathbf{x} \cdot \mathbf{y} = \mathbf{x}P \cdot \mathbf{y}P$. (Hint: Use the fact that $P$ is linear and the dot product is bilinear.) (4)

b) Suppose $\mathscr{C}_1$ and $\mathscr{C}_2$ are permutation equivalent codes where $\mathscr{C}_1 P = \mathscr{C}_2$ for some permutation matrix $P$. Prove that

i) $\mathscr{C}_1^{\perp} P = \mathscr{C}_2^{\perp}$.

ii) If $\mathscr{C}_1$ is self dual, $\mathscr{C}_2$ is also self dual. (6)

3) a) i) What is the smallest field of characteristic 3 that contains a primitive seventh root unity?

ii) What is the smallest field of characteristic 11 that contains a primitive seventh root of unity? (4)

b) Find the 3-cyclotomic cosets modulo 26. (2)

c) Let $\alpha$ be a root of $f(x) = x^3+x+1$ which is in $\mathbf{F}_8$. The table elements of $\mathbf{F}_8$ is given in example 3.4.3. Compute the following elements of $\mathbf{F}_8$, both as polynomials in $\alpha$ and powers of $\alpha$:

i) $$\frac{\left(\alpha^2+\alpha^6-\alpha+1\right)\left(\alpha^3+\alpha\right)}{\left(\alpha^4+\alpha\right)}$$

ii) $$\frac{\left(\alpha^5+\alpha^3+\alpha^2+1\right)\left(\alpha^4+\alpha^3+1\right)}{\left(\alpha^3+\alpha^2+1\right)}$$

(**Hint:** See examples 3.4.2 and 3.4.3 in the book.) (6)

d) In this exercise, we work out the details of example 3.7.8. As given in the table, the 2-cyclotomic sets modulo 15 are $\{0\}$, $\{1,2,4,8\}$, $\{3,6,9,12\}$, $\{5,10\}$, $\{7,1,13,14\}$. The example gives the irreducible factor of $x^{15}-1$ corresponding a coset. To explaing this method, we compute the irreductible factor corresponding to the cyclotomic coset $\{1,2,4,8\}$. Let $\alpha^4=\alpha+1$ be a root of the irreducible polynomial $x^4+x+1$. For computation we use the Table 5.1 on page 184.

The irreducible polynomial corresponding to the cyclotomic coset $\{1,2,4,8\}$ is

$$\begin{aligned}(x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right)\left(x-\alpha^8\right) = x^4 &- \left(\alpha+\alpha^2+\alpha^4+\alpha^8\right)x^3 \\ &+ \left(\alpha\alpha^2+\alpha\alpha^2+\alpha\alpha^2+\alpha^2\alpha^4+\alpha^2\alpha^8+\alpha^4\alpha^8\right)x^2 \\ &+ \left(\alpha\alpha^2\alpha^4+\alpha\alpha^2\alpha^8+\alpha\alpha^4\alpha^8+\alpha^2\alpha^4\alpha^8\right)x \\ &+ \alpha\alpha^2\alpha^4\alpha^8\end{aligned}$$

The coefficient of $x^3$ is

$$\begin{array}{rr} \alpha = & 0010 \\ \alpha^2 = & 0100 \\ \alpha^4 = & 0011 \\ \alpha^8 = & 0101 \\ \hline & 0000 \end{array}$$

So, the coefficient of $x^3$ is 0.

The proces of addition is simple. We count the number of 1s in a column. If it even, we put 0 as the answer. If it is odd, we put 1 as the answer. Similarly, the coefficient of $x^2$ is

$$\begin{array}{rr} \alpha\alpha^2=\alpha^3 = & 1000 \\ \alpha\alpha^4=\alpha^5 = & 0110 \\ \alpha\alpha^8=\alpha^9 = & 1010 \\ \alpha^2\alpha^4=\alpha^6 = & 1100 \\ \alpha^2\alpha^8=\alpha^{10} = & 0111 \\ \alpha^4\alpha^8=\alpha^{12} = & 1111 \\ \hline & 0000 \end{array}$$

So, the coefficient of $x^2$ is 0.

The coefficient of $x$ is

$$\begin{array}{rr} \alpha\alpha^2\alpha^4=\alpha^7 = & 1011 \\ \alpha\alpha^2\alpha^8=\alpha^{11} = & 1110 \\ \alpha\alpha^4\alpha^8=\alpha^{13} = & 1101 \\ \alpha^2\alpha^4\alpha^8=\alpha^{14} = & 1001 \\ \hline & 0001 \end{array}$$

So, the coefficient of $x$ is one.

The constant term is $\alpha\alpha^2\alpha^4\alpha^8=\alpha^{15}=1$. Therefore,

$$(x-\alpha)\left(x-\alpha^2\right)\left(x-\alpha^4\right)\left(x-\alpha^8\right) = x^4+x+1$$

Simlarly, compute the polynomials for the cyclotomic cosets

i) $\{3,6,9,12\}$

ii) $\{7,11,13,14\}$ (8)

4) a) Solve exercise 208, page 128. (**Hint:** If a code $\mathscr{C}$ has dimension $k$, it dual code has dimension $n-k$.) (2)

b) Let $\mathscr{C}$ be a binary cyclic code of length 9 with generator polynomial $g(x) = \left(1+x^3+x^6\right)$. Find the parity check matrix of the code and the generator matrix of the dual code $\mathscr{C}^{\perp}$ using Theorem 4.2.7. (3)

c) In this exercise, we ask you to solve exercise 213 in page 129. We illustrate the procedure using a simple example. We consider the binary cyclic code of length three with generator polynomial $g(x) = \left(1+x^3+x^6\right)$ with message $m(x) = 1+x^2$. Here $n = 9$, $k = 3$.

**Method 1** This is a non-systematic encoding method. Constructing the generator matrix from the generator polynomial, we get

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

The vector corresponding to $1+x^2$ is $(1,0,1)$. Multiplying by the generator matrix, we get

$$(1,0,1)\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} = [1,0,1,1,0,1,1,0,1]$$

The codeword is $[1,0,1,1,0,1,1,0,1]$

**Method 2** This is a systematic method. We multiply the message polynomial $m(x)$ by $x^{n-k}$. Here, we multiply $1+x^2$ by $x^6$ to get $m(x)x^{n-k} = x^6+x^8$.

We then find the remainder $r(x)$ on division of $x^{n-k}m(x)$ by $g(x)$. Here we find the remainder on divsion of $x^8+x^6$ by $g(x) = 1+x^3+x^6$. The remainder is $r(x) = x^5+x^3+x^2+1$.

Subtracting the remainder $r(x)$ from $x^{n-k}m(x)$ we get $c(x) = x^{n-k}m(x) - r(x)$. $c(x)$ is the code word. Here
$x^8+x^6-(x^5+x^3+x^2+1) = x^8+x^6+x^5+x^3+x^2+1 = c(x)$ is the codeword.

**Method 3** This is also a systematic method. From part b) of this exercise,
$h(x) = 1+x^3 = h_0+h_1x+h_2x^2+h_3x^3$ with $h_0 = 1$, $h_1 = 0$, $h_2 = 0$ and $h_3 = 1$.
Writing down the parity check matrix as given in (4.1), page 128, we get

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

We calculate the codeword $c_0, c_2, c_1, \ldots, c_{n-1}$ as follows: Let $(m_0, m_1, \ldots, m_{k-1})$ be the message polynomial written as a vector. We let $c_i = m_i$ for $0 \leq i \leq k-1$. So, $c_0 = m_0 = 1$, $c_1 = m_1 = 0$, $c_2 = m_2 = 1$. So, the codeword is $\mathbf{c} = (1,0,1,c_3,c_4,c_5,c_6,c_7,c_8)$. We calculate $c_3$, $c_4$, …, $c_8$ by setting $H\mathbf{c}^t = \mathbf{0}$:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \\ c_8 \end{bmatrix} = \begin{bmatrix} c_3+1 \\ c_4 \\ c_5+1 \\ c_3+c_6 \\ c_4+c_7 \\ c_5+c_8 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

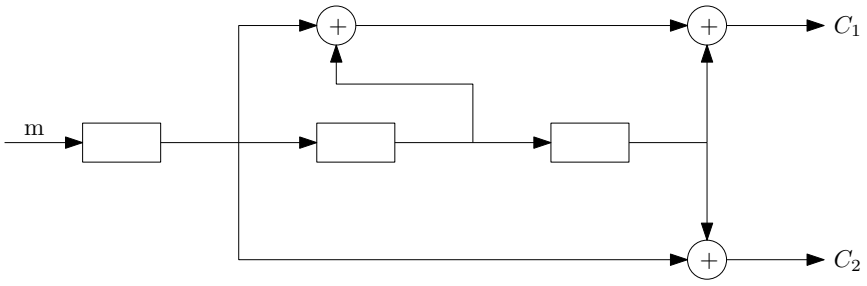


Figure 1: Encoder for convolutional code.

Comparing the first columns, we get $c_3 + 1 = 0$ or $c_3 = 1$. Comparing the second columns, we get $c_4 = 0$. From the third column, we get $c_5 = 1$. From the fourth column, we get $c_3 + c_6 = 0$ or $c_6 = c_3 = 1$. Similarly, we get $c_7 = 0$ and $c_8 = c_5 = 1$. So,the final code word is $\mathbf{c} = (1,0,1,1,0,1,1,0,1)$.

Solve exercise 213 in page 129 similarly. (11)

d) Find the generating idempotent of the cyclic code of length nine with generator polynomial $x^6 + x^3 + 1$. (**Hint:** See the discussion after Theorem 4.3.2 in page 133.) (4)

5) a) Which of the following binary codes are linear?

i) $\mathscr{C} = \{(0,0,0,0),(1,0,1,0),(0,1,1,0),(1,1,1,0)\}$

ii) $\mathscr{C} = \{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}$

Justify your answer. (3)

b) Find the minimum distance for each of the codes. (4)

c) For each of the linear codes, find the degree, a generator matrix and a parity check matrix. (3)

6) a) In this exercise, we will use the data in Example 5.4.3. However, we ask you to decode a different received code word. Let $\mathscr{C}$ be the $[15,7]$ narrow-sense binry BCH code of designed distance $\delta = 5$, which has defining set $T = \{1,2,3,4,6,8,9,12\}$. The generator polynomial of $\mathscr{C}$ is

$$g(x) = 1 + x^4 + x^6 + x^7 + x^8$$

Suppose that $\mathscr{C}$ is used to transmit a codeword and the received codeword is $x^{11} + x^{10} + x^8 + x^5 + x^4 + x^2 + 1$. Find the transmitted code word. (7)

b) Let $\mathscr{C}$ be the [5, 2] ternary code generated by

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

Find the weight enumerator $W_{\mathscr{C}}(x,y)$ of $\mathscr{C}$. (3)

c) Find the convolutional code for the message 11011. The convolutional encoder is given in Fig. 1. (5)

d) Draw the Tanner graph of the code $\mathscr{C}$ with parity check matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}. \quad (5)$$

7) Which of the following statements are true and which are false? Justify your answer with a short proof or a counterexample. (10)

i) If two codes $\mathscr{C}_1$ and $\mathscr{C}_2$ are permutation equivalent, then the punctured codes $\mathscr{C}_1^*$ and $\mathscr{C}_2^*$ obtained from $\mathscr{C}_1$ and $\mathscr{C}_2$, respectively, are also permutation equivalent.

ii) There is no linear self orthogonal code of odd length.

iii) There is no 3-cyclotomic coset modulo 121 of size 25.

iv) There is no duadic code of length 15 over $\mathbf{F}_2$.

v) There is no LDPC code with parameters $n = 16$, $c = 3$ and $r = 5$.