M.Sc. (MATHEMATICS WITH APPLICATIONS IN COMPUTER SCIENCE)

M.Sc. (MACS)

Term-End Examination

December, 2022

MMTE-005 : CODING THEORY

Time : 2 hours *Maximum Marks : 50*

Note :

*(i) Answer any **four** questions from questions no. 1 to 5.*

*(ii) Question no. **6** is **compulsory**.*

(iii) All questions carry equal marks.

(iv) Use of calculator is not allowed.

1. (a) Define the weight of a binary code. Give an example of a binary linear code with minimum weight 3. *2*

(b) State the sphere packing bound carefully explaining all the terms in the bound. *2*

(c) Define a primitive element in a finite field. Find all the primitive elements in $\mathbb{F}_7$. *3*

(d) Define a cyclic code and give an example. Write down the parity check matrix of the cyclic code of length 4 with generator matrix $x^2 + x + 1$. *3*

2. (a) For a linear code, define the syndrome of a message. Find the syndrome of the message (1, 1, 0, 1) if a parity check matrix of the binary code is $\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$. *3*

(b) Define a self-dual code and give an example. *3*

(c) Check whether the polynomial $x^3 - x + 3$ is irreducible over $\mathbb{F}_5$. *2*

(d) Define a convolutional code. *2*

3. (a) Find all the codewords of the code $\mathcal{C}$ with generator matrix

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

How many errors can it detect ? How many errors can it correct ? *6*

(b) Construct the addition table of a field with 8 elements. *4*

4. (a) Let $\mathcal{C}$ be [15, 7] narrow sense binary BCH code of designed distance $\delta = 5$ which has a defining set T = {1, 2, 3, 4, 6, 8, 9, 12}.

Let $\alpha^4 = 1 + \alpha$, where α is a primitive 15^{th} root of unity, and generator polynomial $\mathcal{C}$ is $g(x) = 1 + x^4 + x^6 + x^7 + x^8$.

If $y(x) = 1 + x + x^5 + x^6 + x^9 + x^{10}$ is received, find the transmitted codeword. You may find the following table useful.

0000	0	1000	α^3	1011	α^7	1110	α^{11}
0001	1	0011	α^4	0101	α^8	1111	α^{12}
0010	α	0110	α^5	1010	α^9	1101	α^{13}
0100	α^2	1100	α^6	0111	α^{10}	1001	α^{14}

$\alpha^4 = 1 + \alpha$ 5

(b) Prove that in a linear code, the minimum distance is the same as the minimum weight. 3

(c) Prove that a BCH code with designed distance δ has minimum weight at least δ. 2

5. (a) Let $\mathcal{C}$ be a cyclic code over $\mathbb{F}_q$ with generating idempotent e(x). Prove that the generator polynomial of $\mathcal{C}$ is $g(x) = \gcd(e(x), x^n - 1)$ computed in $\mathbb{F}_q[x]$. 5

(b) Let $\mathcal{C}$ be any self-dual [12, 6, 6] ternary code. Prove that the weight enumerator of $\mathcal{C}$ is $W_C(x, y) = y^{12} + 264\, x^6y^6 + 440\, x^9y^3 + 24\, x^{12}$ 5

6. Which of the following statements are *True* and which are *False* ? Justify your answer with a short proof or a counter example. *5×2=10*

(a) $5^{10} \equiv 1 \pmod{10}$

(b) If C is an (n, k)-code with parity check matrix P, then any two words x, y ∈ $\mathcal{C}$ have the same syndrome only if x = y.

(c) If x and y are two codewords in an LDPC code, with distance between them being less than 1, then x and y will differ in only one component.

(d) The dimension of a code $\mathcal{C}$ is the same as the dimension of the dual code of $\mathcal{C}$.

(e) The number of errors a code $\mathcal{C}$ can correct is the same as the minimum distance of $\mathcal{C}$.