(Pages : 4) **T – 5612**

Reg. No. : .....

Name : .....

Fourth Semester M.Sc. Degree Examination, July 2024

Mathematics

Elective I

MM 243.4 : CODING THEORY

(2020 Admission Onwards)

Time : 3 Hours Max. Marks : 75

PART – A

Answer any **five** questions. Each question carries **3** marks.

1. Define a communication channel. Give an example.

2. Show that a code C is u-error-detecting if and only if $d(C) \geq u+1$.

3. Find the zeros of the polynomial $p(x) = x^4 + 2x^6 \in \mathbb{Z}_3[x]$.

4. Show that every finite field has atleast one primitive element.

5. Show that all the binary Hamming codes of a given length are equivalent.

6. Show that there is a unique monic polynomial of the least degree in every nonzero ideal of $F_q[x]/(x^n - 1)$.

7. Find the reciprocal of the polynomial $h(x) = 1 + 2x + 3x^5 + x^7 \in F_5[x]$.

8. Consider the 7-ary RS code of length 6 with generator polynomial $g(x) = (x-3)(x-3^2)(x-3^3)$. Find a parity check matrix for this code.

($5 \times 3 = 15$ Marks)

P.T.O.

PART – B

Answer **all** questions. Each question carries **12** marks.

9. (A) (a) Prove that a finite field F of characteristic p contains p^n elements for some integer $n \geq 1$. **6**

(b) Show that for a Binary symmetric channel with probability $p < \frac{1}{2}$, the maximum likelyhood decoding rule is the same as the nearest neighbour decoding rule. **3**

(c) Suppose the codewords C = {0000, 0011, 1000, 1100, 0001, 1001} from the binary code are being sent over a BSC. If $x = 0111$ is received, decode x using nearest neighbour decoding. **3**

OR

(B) (a) Show that a code with distance d is an exactly $\left[\frac{d-1}{2}\right]$-error correcting code. **3**

(b) Prove that the characteristic of a field is either zero or a prime. **3**

(c) Discuss maximum likelyhood decoding. **3**

(d) Suppose that the codewords from the code $C = \{000, 111\}$ are being sent over a BSC with crossover probability p = 0.05. Suppose that 110 is received, find the more likelyhood codeword sent by computing the forward channel probabilities.

$P(110\ received \mid 111\ sent) = 0.045125.111$ is morelikely to be the codeword sent. **3**

10. (A) (a) Find the cyclotomic cosets of 2 modulo 15. **3**

(b) Consider a linear code C, and H as a parity-check matrix for C. Show that C has distance $\geq d$ if and only if any $d-1$ columns of H are linearly independent. **6**

(c) Let C be a linear code over F_q. Show that $d(C) = \omega t(C)$. **3**

OR

(B) (a) Show that the dimension of a self-orthogonal code of length n must be $\leq \frac{n}{2}$ and the dimension of a self-dual code of length n is $\frac{n}{2}$. **3**

(b) Consider the code $C = \{0000, 1010, 0101, 1111\}$ over F_2. Check whether this code is self-dual. **3**

(c) Suppose V is a vector space over F_q. Show that V has $\frac{1}{k!}\prod_{k=0}^{k-1}(q^k - q^i)$ different bases if the $\dim(V) = k$. **6**

11. (A) (a) Let $q \geq 2$ be a prime power. Show that $B_q(n,n) = A_q(n,n) = q$. **6**

(b) State and prove the sphere-covering bound. **6**

OR

(B) (a) Explain sphere-packing bound. **6**

(b) Explain the properties of the binary Hamming codes. **6**

12. (A) (a) Let I be a nonzero ideal in $F_q[x]/(x^n - 1)$ and let $g(x)$ be a nonzero monic polynomial of the least degree in I. Show that $g(x)$ is a generator of I and divides $x^n - 1$. **6**

(b) Show that each monic divisor of $x^n - 1$ is the generator polynomial of some cyclic code in F_q^n. **4**

(c) Find all the monic divisors of $x^6 - 1 \in F_2[x]$. **2**

OR

(B) (a) Consider the linear map $\pi : F_q^n \to F_q[x]/(x^n - 1)$ defined by $(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$. Show that a nonempty subset C of F_q^n is a cyclic code if and only if $\pi(C)$ is an ideal of $F_q[x]/(x^n - 1)$. **6**

(b) Show that the dual code $\mathcal{R}(1,m)^{\perp}$ is equivalent to the extended binary Hamming code $\overline{Ham(m,2)}$. **6**

13. (A) (a) Show that the polynomial $x^{15} - 1 \in F_2[x]$ is divisible by $(1 + x + x^2)(1 + x + x^4)(1 + x^3 + x^4)$. **3**

(b) Show that a $q-$ary BCH code of length $q^m - 1$ with designed distance δ has dimension at least $q^m - 1 - m(\delta - 1)$. **6**

(c) Show that any root of $1 + X + X^4 \in F_2[x]$ is primitive in F_{16}. **3**

OR

(B) (a) Show that a BCH code with designed distance δ has minimum distance at least δ. **6**

(b) Let C be a $q-$ary RS code generated by $g(x) = \prod_{i=1}^{\delta-1} (x - \alpha^i)$ with $2 \le \delta \le q - 1$. Show that the extended code $\overline{C}$ is still MDS. **6**

($5 \times 12 = 60$ Marks)

———————