

QP CODE: 26019097



Reg No :
Name :

M.Sc DEGREE (CSS) EXAMINATION, MARCH 2026

Fourth Semester

M Sc MATHEMATICS

ELECTIVE - ME810403 - CODING THEORY

2019 Admission Onwards

A3E88160

Time: 3 Hours

Weightage: 30

Part A (Short Answer Questions)

Answer any **eight** questions.

Weight **1** each.

1. Suppose we have a BSC with $q=0.90$ and $p=0.10$. We have messages consisting of 3 digits. What is the probability of correctly decoding a received message using Hamming code?
2. Define a self orthogonal code with an example
3. What is the probability P of correctly decoding a message using syndrome decoding in terms of the number of cosets.
4. Write the necessary condition for the existence of a self dual $[n, \frac{n}{2}]$ ternary code.
5. Define divisor of zero. Show that a field doesnot have any divisor of zero.
6. If $a(x) = x^4 + x^3 + 1$ and $b(x) = x^2 + x$, then find $s(x)$ and $r(x)$ in the division algorithm.
7. Define ring of polynomials. Which are the operations in a ring of polynomials.
8. Let ϕ be a mapping from one finite set into another finite set of the same size. Prove that ϕ is onto if and only if ϕ is one-one.
9. Give a cyclic code of length 15 and a parity check matrix for it.
10. Define a BCH code of designed distance δ .

(8×1=8 weightage)





Part B (Short Essay/Problems)

Answer any **six** questions.

Weight **2** each.

11. Prove that the general Hamming $[(q^r - 1)/(q - 1) = n, n - r, 3]$ codes over $GF(q)$ are perfect single-error-correcting codes.
12. If C has minimum weight d , then prove that C can detect all errors of weight $\leq d - 1$.
13. Show that if an irreducible polynomial $f(x)$ divides $g(x)h(x)$, then either $f(x)$ divides $g(x)$ or $f(x)$ divides $h(x)$.
14. Using the double error correcting BCH code, decode the received vector $y = 11101111111111$.
15. State and prove the Langrange's theorem.
16. Let $S = \{s | 0 \leq s < p^m - 1\}$. Show that every element in S is in exactly one cyclotomic coset.
17. Prove that if C is an ideal in R_n , the unique monic generator, $g(x)$, of C of smallest degree divides $x^n - 1$, and conversely, if a polynomial $g(x)$ in C divides $x^n - 1$, then $g(x)$ has the lowest degree in $\langle g(x) \rangle$.
18. If C is a cyclic code over F whose generator polynomial $g(x)$ has roots $\beta, \beta^2, \dots, \beta^{\delta-1}$ in some extension field of F , then prove that the minimum weight of C is $\geq \delta$.

(6×2=12 weightage)

Part C (Essay Type Questions)

Answer any **two** questions.

Weight **5** each.

19. (a) Check whether the codes $C_1 = \{100011, 010101, 001110\}$ and $C_2 = \{011100, 101010, 110001\}$ are equivalent.
(b) Give a parity check matrix for a $[7, 4]$ Hamming code.
20. a) Construct a finite field of 16 elements
b) Show that for each polynomial $a(x)$, there is a unique polynomial $c(x)$ of degree less than the degree of $f(x)$ such that $a(x) \equiv c(x) \pmod{f(x)}$





21. Let $m(x)$ be the minimal polynomial of an element α in a finite field $GF(p^r)$. Then prove the following:
- (i) $m(x)$ is irreducible.
 - (ii) If α is a root of a polynomial $f(x)$ with coefficients in $GF(p)$, then $m(x)$ divides $f(x)$.
 - (iii) $m(x)$ divides $x^{p^r} - x$
 - (iv) If $m(x)$ is primitive, its degree is r . In any case the degree of $m(x)$ is $\leq r$.
22. Let C_1 and C_2 be cyclic codes with generator polynomials $g_1(x)$ and $g_2(x)$ and idempotent generators $e_1(x)$ and $e_2(x)$. Then prove that $C_1 \cap C_2$ has as generator polynomial *l. c. m.* $(g_1(x), g_2(x))$ and as idempotent generator $e_1(x)e_2(x)$, and $C_1 + C_2$ has as generator polynomial *g. c. d.* $(g_1(x), g_2(x))$ and as idempotent generator $e_1(x) + e_2(x) - e_1(x)e_2(x)$.

(2×5=10 weightage)

