G 2022 (Pages : 3) Reg. No...............................

Name...................................

M.Sc. DEGREE (C.S.S.) EXAMINATION, JUNE 2016

Fourth Semester

Faculty of Science

Branch I (A)—Mathematics

MT 04 E14—CODING THEORY

(2012 Admissions—Regular)

Time : Three Hours Maximum Weight : 30

Part A

Answer any **five** *questions.*
Each question has weight 1.

1. Define the distance between two vectors u and v. Describe a sphere of radius r about a vector u with an example.
2. Define covering radius. What are the properties of covering radius ?
3. If $a(x)$ is a binary polynomial, prove that $a(x)^2 = a(x^2)$.
4. Find the primitive elements of GF (16).
5. Prove that $\mathrm{GF}(p^s) \subseteq \mathrm{GF}(p^r)$ if and only if $x^{p^s-1}-1$ divides $x^{p^r-1}-1$.
6. Let F = GF (q). Find an element in $F[x]/(x^3-1)$ that does not have a multiplicative inverse.
7. Find the parity check matrix H for the binary [7, 4] cyclic code C with generator polynomial $f(x) = 1 + x + x^3$.
8. Give multiplication table for the field of five elements.

(5 × 1 = 5)

Part B

Answer any **five** *questions.*
Each question has weight 2.

9. If d is the minimum weight of a code C then prove that C can correct at the most $\left[\frac{d-1}{2}\right]$ errors, and conversely.
10. Show that the general Hamming $\left[\frac{q^r-1}{q-1}=n, n-r, 3\right]$ codes over GF(q) are perfect single-error-correcting codes.
11. Construct a finite field of 16 elements.

Turn over

12. Show that the ternary [12, 6] Golay code has minimum weight 6.
13. Explain Double error correcting BCH code.
14. Use double-error correcting BCH code to find the positions in error of vectors x and y whose syndromes are :

$$syn(x)=\left[\alpha^{11} \quad \alpha^{14}\right]^T \text{ and } syn(y)=\left[\alpha^{6} \quad \alpha^{3}\right]^T$$

15. Prove that the degree of the minimal polynomial $m(x)$ of an element $\alpha \in GF(p^n)$ is the size of a certain cyclotomic coset.
16. Prove that every k successive positions are information positions, if the first k are, in an $[n, k]$ cyclic code.

(5 × 2 = 10)

Part C

Answer any **three** *questions.*
Each question has weight 5.

17. Describe packing radius and covering radius of a code C. Show that :
    (a) If C has minimum weight d, packing radius $t=\left[\frac{d-1}{2}\right]$.
    (b) Covering radius r is the weight of the coset of largest weight.
    (c) Packing radius is the largest among the numbers s so that each vector of weight $\leq s$ is a unique coset leader.
18. (a) Prove that a binary code of length n, minimum distance d or more and dimension $k \geq n-m$ exists if :

$$\binom{n-1}{1}+\binom{n-1}{2}+\ldots\ldots+\binom{n-1}{d-2}<2^m-1.$$

    (b) Compute $1001 \times 1011 + 0101 \div 1100$ and $(1110)^{\frac{1}{2}} + 1101$ in GF (16).
19. (a) Show that a set of elements S in R_n corresponds to a cyclic code C if and only if S is an ideal in R_n.
    (b) How many polynomials of the form $x^2 + ax + b$ with $b \neq 0$ are there over GF (4).
20. (a) Define the binary [24, 12] Golay code. Show that its minimum weight is 8 and corrects triple errors.
    (b) Suppose $x^n - 1 = g(x)\, h(x)$ over GF (q). Prove that a cyclic code C with generator polynomial $g(x)$ is self orthogonal if and only if the reciprocal polynomial of $h(x)$ divides $q(x)$.

21. (a) 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 $e_2(x)$ respectively. Prove that $C_1 \cap C_2$ has generator polynomial $l.c.m.\left(g_1(x), g_2(x)\right)$ and the idempotent generator $e_1(x)\, e_2(x)$.

(b) Explain the method of finding cyclic codes.

22. (a) Let $g(x) = 1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10}$ be a generator polynomial of a [15, 5] BCH code. Determine the correct word that was sent if (101101011001001) is received.

(b) Find a generator polynomial for a double-error-correcting Reed-Solomon code over GF(16). Give its length and dimension.

(3 × 5 = 15)