20000152

20000152

Reg. No.................................

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

M.Sc. DEGREE (C.S.S.) EXAMINATION, MAY 2020

Fourth Semester

Faculty of Science

Branch I (A) : Mathematics

MT 04 E14—CODING THEORY

(2012 Admission onwards)

Time : Three Hours | Maximum Weight : 30

Part A

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

1. Show that the set of all binary words of length n is a vector space.
2. Compute the weight of each of the following words and the distance between each pair of them.
   $V_1 = 1001010$, $V_2 = 0110101$, $V_3 = 0011110$.
3. Show that if C is a binary $[n, (n-1)/2]$ self orthogonal code, for odd n, then C^+ is the $[n, (n+1)/2]$ code generated by C and h.
4. Show that a self dual $\left[n, \frac{n}{2}\right]$ ternary code exists iff n is divisible by 4.
5. Show that the order of any element $g \in G$, divides the order of G, where G is a finite group.
6. Find the minimal polynomials for the elements 0 and 1 in GF (16) constructed using $1 + x + x^3$.
7. Show that if a binary cyclic code with generator polynomial $g(x)$ is self-orthogonal then $1 + x$ must divide $g(x)$.
8. Prove that a Reed-Solomon code C of designed distance d has d as its actual minimum weight. Also show that C is an MDS code.

$(5 \times 1 = 5)$

Turn over

Part B

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

9. Prove that if the rows of a generator matrix G for a binary $[n, k]$ code C have weights divisible by 4 and are orthogonal to each other, then C is self-orthogonal and all weights in C are divisible by 4.

10. Define syndrome. Show that if C is a binary code and e is any vector, the syndrome of e is the sum of those columns of H where e has non-zero components ; where H be a parity check matrix of an $[n, k]$ code.

11. Define Golay code. Find the minimum weight and show that it is triple error correcting code.

12. Show that every monic polynomial over a field F can be expressed uniquely as a product of irreducible monic polynomials over F.

13. Let $x^n - 1 = g(x)h(x)$ over GF (q). Prove that a cyclic code C with generator polynomial $g(x)$ is self-orthogonal iff the reciprocal polynomial of $h(x)$ divides $g(x)$.

14. Find a self-orthogonal length 15 binary cyclic code.

15. Show that in a field of characteristics $\mathrm{P}(x \pm y)^{\mathrm{P}^m} = x^{\mathrm{P}^m} \pm y^{\mathrm{P}^m}$.

16. Show that for any prime p and positive integer m, there is a unique field of p^m elements.

(5 × 2 = 10)

Part C

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

17. (a) If u is a vector in c of weight s, show that there is a dependence relation among s columns of any parity check matrix of c and conversely that any dependence relation among s columns of a parity check matrix of c yields a vector of weight s in c.

    (b) If C has minimum weight d, show that c can detect all errors of weight $\leq d - 1$.

    (c) If C has minimum weight 2 $(t + 1)$, show that we can simultaneously correct all errors of weight t or less and detect all errors of weight $t + 1$.

18. Prove the following :

(a) (i) Given m and d, then there exists a binary code of length n, minimum distance d or more and dimension $k \geq n-m$, whenever

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

(ii) Given m and d, then there exists a code over GF (q) of length n, minimum distance d or more and dimension $k \geq n-m$, whenever

$$(q-1)\binom{n-1}{1}+(q-1)^2\binom{n-1}{2}+.....+(q-1)^{d-2}\binom{n-1}{d-2}<q^m-1.$$

(b) If d is even show that A $(n-1, d-1)$ = A (n, d).

19. (a) Messages are encoded using C_{15}. Determine if possible the location of the errors if w is received with syndrome wH is given by 01000000. The parity check matrix H for C_{15} is given below :

$$H=\begin{bmatrix} 1000 & 1000 \\ 0100 & 0001 \\ 0010 & 0011 \\ 0001 & 0101 \\ 1100 & 1111 \\ 0110 & 1000 \\ 0011 & 0001 \\ 1101 & 0011 \\ 1010 & 0101 \\ 0101 & 1111 \\ 1110 & 1000 \\ 0111 & 0001 \\ 1111 & 0011 \\ 1011 & 0101 \\ 1001 & 1111 \end{bmatrix}$$

(b) Prove that a doubly even $\left[n, \frac{n}{2}\right]$ code exists iff n is divisible by 8.

Turn over

20. (a) Show that $F(x)/(f(x))$ is a field iff $f(x)$ is irreducible. Also show that if $f(x)$ be an irreducible polynomial of degree m over $GF(p)$, then $F' = GF(p)[x]/(f(x))$ is a field with p^m elements.

(b) Prove that every finite field has a primitive element.

21. (a) If $g(x)h(x) = x^n - 1$ in $F[x]$ and $g(x)$ is the generator polynomial of a cyclic code C, show that the reciprocal polynomial of h (x) is the generator polynomial of $C^{\perp}$. Also show that if $h(x) = h_0 + h_1(x) + ... + h_k(x^k)$, then the matrix H given below is a parity check matric of C, and $C^{\perp}$ is cyclic.

$$H = \begin{pmatrix} h_k & h_{k-1} \ldots\ldots & h_0 & 00 \ldots\ldots 0 \\ 0 & h_k \ldots\ldots & h_1 & h_0 0 \ldots\ldots 0 \\ " & " & " & \\ " & " & " & \\ 0 & 0 \ldots\ldots & h_k \ldots\ldots & h_0 \end{pmatrix}$$

(b) Prove that every cyclic [n, k] code C has an idempotent generator e (x).

22. (a) Prove that the minimum weight of a BCH code C of designed distance σ is atleast σ.

(b) Let $f(x)$ be a polynomial with co-efficients in GF (q) and let S be the set of its roots in some field F = GF (q^m). Prove that the weight of is greater then or equal to the size of any set A in a set I_s of subsets of F that is independent with respect to S.

(3 × 5 = 15)