19001152

19001152

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

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

M.Sc. DEGREE (C.S.S.) EXAMINATION, APRIL 2019

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. What are equivalent codes ? Find a generator matrix G' in standard form for a code equivalent to the code with the generating matrix $G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$.
2. Find the dual code C^+ for the code C = < S >, where S = {1010, 0101, 1111}
3. If C is a self dual code with generator matrix $(I|A)$, show that C also has $(-A'|I)$ as a generator matrix.
4. Show that every monic polynomial over a field F can be expressed uniquely as a product of irreducible monic polynomials over F.
5. If an element g has order r, show that $g^s = e$ iff s is a multiple of r.
6. If F is a field of characteristic P, show that the mapping ϕ defined by $\phi(\alpha) = \alpha^p$ is an automorphism of F.
7. If C_1 and C_2 are cyclic codes with generator polynomials $g_1(x)$ and $g_2(x)$, show that $C_1 \leq C_2$ iff $g_2(x)$ divides $g_1(x)$.

Turn over

8. Define Reed-Solomon code.

   Show that a Reed-Solomon code C of designed distance d has d as its actual minimum weight.

(5 × 1 = 5)

Part B

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

9. 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, show that C is self-orthogonal and all weights in C are divisible by 4.
10. Find a parity check matrix for the code C = {0000, 1001, 0110, 1111}.
11. Define Golay Code. Show that it is a triple error correcting code.
12. Define a field. Give an example of a finite field.
13. If $f(x)$ is a polynomial with co-efficients in $\mathrm{GF}\left(p^v\right)$, show that $f\left(x^{p^v}\right) = \left(f(x)\right)^{p^v}$.
14. Show that $\mathrm{GF}\left(p^s\right) < \mathrm{GF}\left(p^v\right)$ iff $x^{p^s - 1} - 1$ divides $x^{p^r - 1} - 1$.
15. Show that C is an ideal in $\mathbb{R}_n$, 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 $< g(x) >$.
16. Write the parity check matrix for a Hamming code of length 7.

(5 × 2 = 10)

Part C

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

17. (a) Prove that every vector in a fixed coset has the same syndrome and vectors in different cosets have different syndromes. Also show that all possible q^{n-k} syndromes occur as syndromes of some vectors.

    (b) Prove that the packing radius t has the following properties :—

      (i) If C has minimum weight d, then $t = [(d - 1)/2]$.

      (ii) t is the largest among the numbers s so that each vector of weight $\leq s$ is a unique coset leader.

18. (a) Prove that if C is an $[n, k, d]$ code, then every $(n - d + 1)$ Co-ordinate positions contain an information set. Also show that d is the largest number with this property.

(b) Prove that the dual of an MDS code C is again an MDS code.

19. (a) Using the double-error-correcting BCH code decode the received vector.

$x = (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$

The parity check matrix H is given by

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

(b) Messages are encoded using C_{15} whose parity check matrix is given above : Determine if possible the location of the errors if w is received and syndrome WH is 11101000.

20. (a) Show that if a field of $q = p^m$ elements exists, then it is unique upto isomorphism.

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

21. (a) Prove that if C is an ideal in $\mathbb{R}_n = {}^{F(x)}\!\big/\!{}_{(x^n - 1)}$ and $g(x)$ be the monic polynomial of smallest degree in C, then $g(x)$ is uniquely determined and C = $\langle g(x) \rangle$.

Turn over

(b) Suppose that $a(x)=(a_0,a_1,.....a_{n-1})$ and $b(x)=(b_0,b_1,.....b_{n-1})$. Prove that $a(x)b(x)=0$ in $\mathbb{R}_n$ iff $a(x)$ is orthogonal to the vector $(b_{n-1},........b_0)$ and every cyclic shift of this vector.

22. (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 $e_2(x)$. Prove that $C_1 \cap C_2$ has as generator polynomial l.c.m ($g_1(x)$, $g_2(x)$) and as idempotent generator $e_1(x).e_2(x)$. Also show that C_1+C_2 has as generator polynomial g.c.d. ($g_1(x)$, $g_2(x)$) and as idempotent generator $e_1(x)+e_2(x)-e_1(x)\,e_2(x)$.

(b) Describe a Reed-Solomon [7, 3] code over GF (8) by giving its generator polynomial. How many errors will it correct ?

(3 × 5 = 15)