 Roll No. ....

18DD1905

M. Sc. EXAMINATION, 2020

(Fourth Semester)

(C Scheme)

(Main Only)

MATHEMATICS

MAT612C

ALGEBRAIC CODING THEORY–II

Time : 3 *Hours*] [*Maximum Marks* : 75

Before answering the question-paper candidates should ensure that they have been supplied to correct and complete question-paper. No complaint, in this regard, will be entertained after the examination.

Note : Attempt *Five* questions in all, selecting *one* question from each Unit. Q. No. **1** is compulsory. All questions carry equal marks.

(Compulsory Question)

1. (a) Write down a parity check matrix for the binary (4, 7) Hamming code.

(b) Find a primitive element of the finite field GF(9).

(c) Obtain the generator polynomial of the ternary cyclic code C = {000, 111, 222}.

(d) Define Reed-Solomon (RS) Code. Show that RS code is a BCH code.

(e) Give an example of a product code. **3×5=15**

Unit I

2. (a) Prove that every cyclic code of length n over finite field $\mathbf{F}_q$ correspondences to an ideal in the ring $\mathbf{F}_q[x]/< x^n - 1 >$. Find the generating polynomial of the ideal in $\mathbf{F}_2[x]/< x^4 - 1 >$ corresponds to the cyclic code C = {0000, 1010, 0101, 1111}. **8**

(b) Show that every cyclic code has an idempotent generator. Find the generating idempotent for the binary [7, 4]-Hamming code. **7**

3. (a) Let C_1 and C_2 be two cyclic codes over $\mathbf{F}_q$ of length n with generating idempotent $e_1(x)$ and $e_2(x)$ respectively. Show that $C_1 + C_2$ and $C_1 \cap C_2$ have generating idemptotents $e_1(x) + e_2(x) - e_1(x)\, e_2(x)$ and $e_1(x)\, e_2(x)$ respectively. **8**

(b) Construct all cyclic codes of length 4 and dimension 2 over finite field $\mathbf{F}_5$. How many errors these codes can detect and correct ? **7**

Unit II

4. (a) Define the cyclotomic coset C_s modulo n over finite field $\mathbf{F}_q$ containing the integer s. If α is a primitive nth root of unity in some extension field of $\mathbf{F}_q$, then show that the minimal polynomial of α^s over $\mathbf{F}_q$ is $\Pi_{j \in C_s}(x - \alpha^j)$. **8**

(b) Show that a binary BCH code of length $n = 2^k - 1$ and the minimum distance at least $d = 2t + 1$ can be constructed with check digits at most kt. **7**

5. (a) Factorize $x^{15} - 1$ over $\mathbf{F}_2$. Hence or otherwie, construct a binary BCH code of length 15 and dimension 8. **8**

(b) Let r be an integer with $0 \le r \le m$. Then prove the following :

(i) The dimensions of Reed-Muller Code $\mathbf{R}(r, m)$ equals

$$\binom{m}{0} + \binom{m}{1} + \ldots\ldots + \binom{m}{r}$$

(ii) The minimum distance of $\mathbf{R}(r, m)$ equals 2^{m-r}. **7**

Unit III

6. (a) Define Quadratic residue codes of prime length and Extended Quadratic residue codes. Also illustrate each one by giving an example. **8**

(b) Prove that $F^{\perp} = \overline{N}$ and $N^{\perp} = \overline{F}$, where quadratic residue codes F and N of length $p \equiv 1 \pmod 4$ over GF(s) generated by $q(x)$ and $n(x)$. **7**

7. (a) Write normalized Hadamard matrix of order 8 and obtain the corresponding Hadamard codes. **8**

(b) If M is a Hadamard matrix of order n and $T = \begin{pmatrix} M & M \\ M & -M \end{pmatrix}$, then prove that T is a Hadamard matrix of order $2n$. Hence or otherwise write down a Hadamard matrix of order 4. **7**

Unit IV

8. (a) If C is an $[n, k, d]$ linear code over GF(q), then prove that C is MDS if and only if every $n - k$ columns of a parity check matrix H of C are linearly independent. **8**

(b) Prove that binary MDS codes are the trivial MDS codes. **7**

9. (a) Let C be an $[n, k]$ linear t-burst-error-correcting code. Then prove the following : **8**

(i) no non-zero burst of length $2t$ or less can be codeword,

(ii) $n - k \geq 2t$.

(b) If C is an $[n, k, d]$ MDS code, then show that any k symbols of the codewords may be taken as message symbols. **7**