(Pages : 3) **L – 5422**

Reg. No. : ....

Name : ....

Fourth Semester M.Sc. Degree Examination, March 2021

Mathematics

MM 243 Elective : CODING THEORY

(2013 Admission Onwards)

Time : 3 Hours Max. Marks : 75

Instructions :

1) Answer either Part A or Part B of each question.

2) **All** questions carry equal marks.

1. (A) (a) Define the followings : A channel, length of a word, and a block code. Give an example of a binary code. **8**

(b) Define the reliability of a BSC. What can be said about a channel when its reliability is 0 and reliability is 1/2. **7**

(B) (a) If $C = \{01000, 01001, 00011, 11001\}$ and a word $w = 10110$ is received, which codeword is most likely to have been sent? **6**

(b) Let $n = 3$ and $C = \{001, 101\}$. If $v = 001$ is transmitted, when will IMLD conclude this correctly, and when IMLD incorrectly conclude that 101 was sent? **9**

P.T.O.

2. (A) (a) Prove that the distance of a linear code is the weight of the nonzero code of least weight. **5**

(b) For $S = \{1010, 0101, 1111\}$, compute the dual code $C^{\perp}$. **6**

(c) Check whether $S = \{1101, 0111, 1100, 0011\}$ is linearly independent or not? **4**

(B) (a) Using the elementary row operations of a matrix, find a basis for $C = \langle S \rangle$, where $S = \{10101, 01010, 11111, 00011, 10110\}$. **9**

(b) Given is a parity-check matrix for a linear code C. $H = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Find generator matrices for C and $C^{\perp}$. **6**

3. (A) (a) State and prove Gilbert-Varshamov bound. **9**

(b) Is it possible to have a linear code with parameters $(8, 3, 5)$? **3**

(c) Does there exists a (15, 7, 5) linear code? **3**

(B) (a) Define a Hamming code. **3**

(b) Prove the following :

(i) A Hamming code has dimension $2^r - 1 - r$ and contains $2^{2^r - 1 - r}$ code words. **4**

(ii) A Hamming code has distance 3. **4**

(iii) Hamming codes are perfect single-error correcting codes. **4**

4. (A) (a) If $f(x) \equiv g(x)$ mod $h(x)$ then, prove that $f(x)\,p(x) \equiv g(x)\,p(x)\,(\text{mod } h(x))$. **6**

(b) Define a cyclic shift and cyclic code. **4**

(c) Show that the cyclic shift π is a linear transformation. **5**

(B) Let C be a cyclic code of length n and let $g(x)$ be the generator polynomial. Assume $n-k=\text{degree}\,(g(x))$. Prove the following :

(a) C has dimension k.

(b) The codewords corresponding to $g(x)$, $xg(x),\ldots,x^{k-1}g(x)$ form a basis for C. **5**

(c) $c(x) \in C$ if and only if $c(x) = a(x)\,g(x)$ for some polynomial $a(x)$ with degree $(a(x)) < k$. **6**

5. (A) Find all primitive elements in $GF(2^4)$. **15**

(B) Find the minimal polynomial of each element of $GF(2^4)$ constructed using $p(x) = 1 + x^3 + x^4$. **15**

(5 × 15 = 75 Marks)