(Knowledge for Development)

# KIBABII UNIVERSITY

## UNIVERSITY EXAMINATIONS

## 2019/2020 ACADEMIC YEAR

## FIRST YEAR FIRST SEMESTER

## MAIN EXAMINATION

## FOR THE DEGREE OF MASTER OF SCIENCE IN PURE MATHEMATICS

**COURSE CODE:** MAT 827

**COURSE TITLE:** CODING THEORY I

**DATE:** 18/02/2021 **TIME:** 2 PM -5 PM

---

**INSTRUCTIONS TO CANDIDATES**

Answer Any THREE Questions

TIME: 3 Hours

# MAT ~~843~~ 827 CODING THEORY

## Question One, (20 mks)

a) Define the Hamming code Ham(n,r) (3mks)

b) State without proof the distance theorem for Linear codes (3 mks)

c) Use the distance theorem to find the minimum distance of the binary code with check matrix. (3 mks)

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

d) Generate a $(7,4)$ Hamming code for the Message 1000, (3 mks)

e) A 7 bit Hamming codeword is received as 1010111. Assuming even parity determine whether the received word is wrong or correct and if wrong find the correct codeword. ( 4mks)

f) Find the generator matrix for Ham(3,2). (4 mks)

## Question Two, (20 mks)

a) Define the following terms

   (i) A Linear code (2 mks)

   (ii) The minimum weight of a code (2 mks)

   (iii) The minimum distance of a code (2 mks)

   (iv) Define a dual of a code $C$ (2 mks)

b) Show that, for a Linear code $C$, the minimum distance and the Hamming weight are the same (3 mks)

c) Given a code $C = < S >$ where $S = 11101, 10110, 01011, 11010$. find the basis of this code and the generator matrix of the dual code $C^{\perp}$. (5 mks)

d) List all the codewords of the above code $C$. If this code is used for error detection in a binary symmetric channel with bit error rate $p = 0.1$, calculate $P_{undetect}(C)$, the probability that an error in a recieved vector is not detected. Leave your answer in unsimplified form (3 mks)

e) What is meant by a syndrome of a code (1 mks)

## Question Three (20 mks)

a) Define what is meant by an Ideal $I$ in a commutative ring $R$ (3 mks)

b) Define what is meant by a cyclic code $C$ in $F_p^{(n)}$ ( 3 mks)

c) Show that a set $S$ in $R_n$ corresponds to a cyclic code. (5 mks)

d) iven that over $F_2$,

$$x^7 = (x-1)(x^3+x+1)(x^3+x^2+1)$$

as a product of irreducible polynomials: Construct binary cyclic codes for n = 7. (5 mks)

e) Write down the parity check polynomial of the binary cyclic code generated by $1+x+x^3$ (4 mks)

## Question Four (20 mks)

a) Let $C$ be a binary Linear code given by the generator matrix.

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

i) Determine all the code words of $C$. What can you say about the error detection and correlation ability. (4 mks)

ii) Find the associated parity check matrix $H$. (3 mks)

iii) Use $H$ to decode the following received words. 11011 and 11010 (4 mks)

b) A binary sequence code has probability $P = 0.05$ of incorrect transmission. If the code word $C = 011011101$ is transmitted, without simplfying your answer, what is the probability that,

i) We receive $r = 111011100$ (2 mks)

ii) A double error occurs (3 mks)

c) Prove that a code $C$ of minimum distance $d$ can detect up to $t$ errors in any code word and correct up to t errors in any code word if $d \geq 2t-1$ (4 mks)

## Question Five (20 mks)

a) Define a BCH code. (3 mks)

b) Construct a triple error correcting $BCH$ code with block ength $n = 31$ over $GF(2^5)$ (10 mks)

c) Define a Boolean function (1 mks)

d) Define a Reed-Muller code $R(r, m)$ (3 mks)

e) Find a generator matrix for $R(1, 3)$ (3 mks)