

**M.Sc. 3rd Semester Examination, 2023**

**APPLIED MATHEMATICS OCEANOLOGY  
AND COMPUTER PROGRAMMING**

PAPER – MTM-303(New)

*Full Marks : 50*

*Time : 2 hours*

*The figures in the right hand margin indicate marks*

*Candidates are required to give their answers in  
their own words as far as practicable*

**PAPER—MTM-303(Unit-1)**

[ *Marks : 20* ]

*(Stochastic Process and Regression)*

1. Answer any *two* questions : 2 × 2

(a) Define the Markov chain with an example.  
Also, define its order.

- (b) Define multiple correlation and partial correlation and indicate how they differ from simple correlation.
- (c) Define the state space in the context of a Birth and Death process.
- (d) Define the following states : periodic, closed, persistent and transient.

2. Answer any *two* questions : 4 × 2

- (a) Write a transition matrix for the problem of random walk between reflecting barriers.
- (b) State and prove the Chapman-Kolmogorov equation. Write its significance with a suitable example.
- (c) Show that the generating function  $P_n(s)$  for the branching process satisfies the following relations
- (i)  $P_n(s) = P_{n-1}(p(s))$

$$(ii) P_n(s) = P(P_{n-1}(s)),$$

where  $P_1(s) = P(s)$ .

(d) Prove that

$$1 - r_{1.23}^2 = (1 - r_{12}^2)(1 - r_{13.2}^2).$$

Use this relation to show that the multiple correlation coefficient is numerically greater than any of the total or partial correlation coefficients of  $x_1$  with the other variables.

3. Answer any *one* question : 1 × 8

(a) Obtain the multiple regression equation of  $x_1$  on  $x_2, x_3, \dots, x_p$  in terms of the means, the standard deviations and the inter-correlations of the variables.

(b) Deduce the forward diffusion equation for the Wiener process. Also, write the backward diffusion equation from the deduced equation.

**PAER—MTM-303(Unit-2)**

[ Marks : 20 ]

(Cryptography)

4. Answer any *two* of the following questions : 2 × 2
- (a) Define the terms 'cipher' and 'public key certificate'.
  - (b) Write down the three independent dimensions to characterize cryptographic systems.
  - (c) Write down a short note on "Block ciphers".
  - (d) What is the meaning of 'digital signature' to use in public-key cryptosystem ?
5. Answer any *two* of the following questions : 2 × 4
- (a) Explain the concepts "Brute-force attacks" and "Monoalphabetic ciphers".

- (b) Write down the algorithm of Data encryption standard (DES) and draw the scheme of Data encryption standard (DES).
- (c) Define Public-key encryption. Describe the six ingredients for Public-key encryption.
- (d) Explain "Play-fair cipher" for substitution technique and write down its working rules.

6. Answer any *one* of the following questions : 1 × 8

(a) (i) Explain the term "One-Time Pad". 2

(ii) Define Hill cipher. Write down the algorithm of Hill cipher and explain it with an example. 1 + 3 + 2

(b) Write down the statement of "Feistel cipher". Describe Feistel cipher struc-

ture and draw its graphical representation to encrypt the data. Hence, write down its all parameters and design features.

2+3+3

[ Internal Assessment – 10 Marks ]

---