DECEMBER 2022 **P/ID 37505/PMA1E**

Time : Three hours Maximum : 80 marks

SECTION A — (10 × 2 = 20 marks)

Answer any TEN questions.

1. Define Lattice homomorphism.

2. Define a totally ordered set.

3. Define n-pole circuit.

4. Define Boolean polynomial.

5. Define a primitive element.

6. Define triangle circuit.

7. Define Möbius function.

8. Define Frobenius automorphism.

9. Define a linear code.

10. Write the additive form of Mobius inversion formula.

11. Define an error word.

12. Define a canonical generator matrix.

SECTION B — (5 × 6 = 30 marks)

Answer any FIVE questions.

13. Let $(L,\leq)$ be a lattice ordered set. Define

$x \wedge y := \inf(x,y),\ x \vee y := \sup(x,y)$.

Prove that $(L,\wedge,\vee)$ is an algebraic lattice.

14. Let $(\mathcal{A}, P)$ be a probability space. For all $b_1, b_2, b \in \mathcal{A}$, prove that

(a) $b_1, b_2 = 0 \Rightarrow P(b_1 + b_2) = P(b_1) + P(b_2)$;

(b) $P(b_1 + b_2) = P(b_1) + P(b_2) - P(b_1 b_2)$;

(c) $b_1 \leq b_2 \Rightarrow P(b_1) \leq P(b_2)$;

(d) $P(b) \in [0,1]$;

(e) $P(b') = 1 - P(b)$.

15. Let p be a prime and let m, n be natural numbers

(a) If $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n}$ then prove that $m \mid n$.

(b) If $m \mid n$ then prove that $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$. Also, prove that there is exactly one subfield of $\mathbb{F}_{p^n}$ with p^m elements.

16. Prove that an irreducible polynomial f over $\mathbb{F}_q$ of degree k divides $x^{q^n} - x$ if and only if k divides n.

17. Let G be a generator matrix of a linear code C. Prove that the rows of G form a basis of C.

18. Let $G = \langle g \rangle$ be cyclic of order m. Prove that all generators of G are given by g^k with $\gcd(k,m) = 1$.

19. Let L be a lattice. Prove that the implications hold:

    (a) L is a Boolean algebra $\Rightarrow$ L is relatively complemented.

    (b) L is relatively complemented $\Rightarrow$ L is sectionally complemented.

    (c) L is finite and sectionally complemented $\Rightarrow$ every nonzero element a of L is a join of finitely many atoms.

SECTION C — (3 × 10 = 30 marks)

Answer any THREE questions.

20. State and prove the Representation theorem.

21. Explain the addition of three one-digit binary numbers using full-adders.

22. Determine the elements of $\mathbb{F}_{2^3}$.

23. Prove the following:

(a) $f = \prod_{s \in \mathbb{F}_q} \gcd(f, h - s)$

(b) The number of monic distinct irreducible factors f_i of f is equal to the dimension of the null space of the matrix $\mathbf{Q} - \mathbf{I}$.

24. Let C be an ideal $\neq \{0\}$ of V_n. Prove that there exists a unique $g \in V_n$ with the following properties:

(a) $g \mid x^n - 1$ in $\mathbb{F}_q[x]$;

(b) $C = (g)$;

(c) g is monic.
