MAY 2022 **P/ID 37505/PMA1E**

Time : Three hours Maximum : 80 marks

PART A — ($10 \times 2 = 20$ marks)

Answer any TEN questions.

1. State Zorn's Lemma.

2. Define star circuit.

3. Define input variables.

4. Write duality principle.

5. Define a primitive element.

6. Define Möbius function.

7. Define triangle circuit.

8. Define zero-ring.

9. Define maximum distance separable.

10. Define Boolean polynomial function.

11. Define an error word.

12. Define a linear code.

PART B — ($5 \times 6 = 30$ marks)

Answer any FIVE questions.

13. 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.

14. Find the symbolic representation of a simple circuit for which the binary polynomial function f in four variables is defined as follows : f is 0 at (0, 0, 1, 0), (0, 0, 1, 1), (0, 1, 1, 0), (0, 1, 1, 1), (1, 0, 0, 0), (1, 0, 0, 1), (1, 1, 0, 0), (1, 1, 0, 1), (1, 1, 1, 1), and has value 1 otherwise.

15. Let F be a finite field and let $\alpha_1, \cdots, \alpha_k$ be algebraic over F. Prove that $F(\alpha_1, \cdots, \alpha_k) = F(\alpha)$ for some α in $F(\alpha_1, \cdots, \alpha_k)$.

16. Let $f \in \mathbb{F}_q [x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree $m \geq 2$. Prove that order f is equal to the order of any root of f in $\mathbb{F}^*_{q^m}$.

17. Let h be a check polynomial of a cyclic code $C \subseteq V_n$ with generator polynomial g and $v \in V_n$. Then prove that $v \in C \Leftrightarrow v * h = 0$.

18. Let F be a finite field of characteristic p. Prove that F contains p^n elements, where $n = [F : \mathbb{Z}_p]$.

19. Let $(L, \wedge, \vee)$ be an algebraic lattice. Define $X \leq y \Leftrightarrow x \wedge y = x$. Prove that $(L, \leq)$ is a lattice ordered set.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

20. Prove that a polynomial $p \in P_n$ is equivalent to the sum of all prime implicants of p.

21. Explain the addition of two binary numbers using half-adders.

22. Prove the following :

(a) Any finite field F is of order p^n where $p = char\ F$ is a prime and n is a positive integer.

(b) For any prime p and any $n \in \mathbb{N}$ there is a field of order p^n.

(c) Any field of order p^n is (up to isomorphism) the splitting field of $x^{p^n} - x$ and also of $x^{p^{n-1}} - 1 \in \mathbb{Z}_p[x]$.

(d) Any two fields of order p^n are isomorphic.

23. State and prove the Chinese Remainder theorem for polynomials.

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.
