**MAY 2025** **P/ID 37505/PMA1E**

Time : Three hours Maximum : 80 marks

PART A — (10 × 2 = 20 marks)

Answer any TEN questions.

1. Define totally ordered set.

2. Define Boolean ring.

3. Draw the NOR-gate.

4. Give the Minimal forms of the polynomials $p_7, p_8, p_9$ and $p_{10}$.

5. Define star-circuit.

6. Define primitive element.

7. Define Mobius function.

8. Find the irreducible polynomial of degree 4 over $\mathbb{F}_2$.

9. Find the number of all monic, irreducible polynomials of degree k over $\mathbb{F}_q$.

10. Define parity-check matrix of the code $C$.

11. Define error vector.

12. Define sphere of radius $r$ about $x \in \mathbb{F}_q^n$.

PART B — (5 × 6 = 30 marks)

Answer any FIVE questions.

13. Let $V$ be a lattice. Prove the following implications:

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

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

14. (a) Prove that every atom of a lattice with zero is join-irreducible.

    (b) Suppose $V$ is a distributive lattice with $p \in V$ join-irreducible and $p \leq a \sqcup b$. Prove that $p \leq a$ or $p \leq b$.

15. Simplify $p_{12}$ using the rules of a Boolean algebra.

16. Let $p$ be a prime and let $m$, $n$ be natural numbers, then prove the following:

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

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

17. Prove that $x^{q^n} - x = \prod_i f_i$, where the product is extended over all distinct. monic. irreducible polynomials over $\mathbb{F}_q$, with degree $a$ divisor of $n$.

18. Prove the following:

(a) The characters of $\mathbb{F}_q$ form a group which is isomorphic to the group $(\mathbb{F}_q, +)$.

(b) For any $a, b \in \mathbb{F}_q$, $a \neq b$, we have $\sum \chi(a)\chi(b) = 0$ where the summation runs through all characters of $\mathbb{F}_q$.

19. Let $h$ be a check polynomial of a cyclic code $C \subset V_n$ with generator polynomial g and $v \in V_n$. Prove that $v \in C \Leftrightarrow V * h = 0$.

PART C — (3 × 10 = 30 marks)

Answer any THREE questions.

20. State and prove representation theorem.

21. (a) Prove: The general solution of $x \sqcup y = c$ is of the form $x = c \sqcap (u \sqcup v')$, $y = c \sqcap (u' \sqcup v')$.

(b) Show that the equation $a \sqcup x = b$ has a solution if and only if $a \leq b$, and if this condition holds show that the general solution is of the form $x = (u \sqcup a') \sqcap b$.

22. Prove the following properties of cyclotomic polynomials:

(a) If $p$ is prime and $p \nmid m$ then $Q_{mp^k}(x) = Q_{pm}(x^{p^{k-1}})$.

(b) If $p$ is prime and $p \nmid m$ $q_{pm}(x) = \dfrac{Q_m(x^p)}{Q_m(x)}$.

(c) If $n \geq 2$, $Q_n(x) = \prod_{d|n}(1 - x^{n/d})^{\mu(d)}$.

(d) If $n \geq 3$, $n$ odd, then $Q_{2n}(x) = Q_n(-x)$.

(e) If $n \geq 2$, $Q_n(x^{-1})x^{\phi(n)} = Q_n(x)$.

23. Prove the following

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

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

24. Let $C$ be a binary (7, 3) code with generator matrix

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$ Show that $C$ is self-orthogonal. Find its dual code.

---