M A/M Sc Applied Mathematics, 3rd-Semester, 2016
End-Semester Examination

Course title: Finite Fields & Coding Theory **Course code:** PGAMT3C003T
Time allowed: 3 hours **Maximum Marks:** 100

Instructions for the candidates:

- *The question paper consist of three sections, namely,* **Section A**, **Section B** *and* **Section C**.
- *The* **section A** *consist of 10 objective type questions, and all the questions are compulsory in this section.*
- *The* **section B** *consist of 10 short answer type questions with 2 questions from each unit, and the candidate has to attempt 5 questions selecting one question from each unit.*
- *The* **section C** *consist of 5 long answer type questions, and the candidate has to attempt any 3 questions.*

Section A

(1) Which of the following is a prime field?
(a) $\mathbb{F}_{5^3}$. (b) $\mathbb{F}_{3^2}$. (c) $\mathbb{F}_3$. (d) None of the above. 1.5

(2) For any prime p the residue class ring $\mathbb{Z}/(p)$ can be identified with
(a) Galois field $\mathbb{F}_p$ of order p. (c) Galois field $\mathbb{F}_p$ of order $p-1$.
(b) may or may not be field . (d) None of the above. 1.5

(3) If p is a prime and n a positive integer, then
(a) n divides $\phi(p^n-1)$. (c) n does not divides $\phi(p^n-1)$.
(b) $\gcd(n, \phi(p^n-1)) = 1$. (d) None of the above. 1.5

(4) Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m}$. Then for the norm function $N_{F/K}$ which of the following statement is false
(a) $N_{F/K}(\alpha\beta) = N_{F/K}(\alpha) \cdot N_{F/K}(\beta)$, for every $\alpha, \beta \in F$.
(b) $N_{F/K}(a) = a^m$, for every $a \in K$.
(c) $N_{F/K}(a^m) = a$, for every $a \in K$.
(d) $N_{F/K}(\alpha^q) = N_{F/K}(\alpha)$, for every $\alpha \in F$. 1.5

(5) Let F be a finite field with q elements, for every $a \in F$
(a) $a^{q-1} = a$. (b) $a^q = a$. (c) $a^{q-1} = 1$. (d) $a^2 = a$.
1.5

(6) Let $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Then the companion matrix of f is given by
(a) $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$. (b) $\begin{pmatrix} 2 & 0 \\ 1 & 0 \end{pmatrix}$. (c) $\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$. (d) $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$. 1.5

(7) If $x = (1110)$ and $y = 1010 \in \mathbb{F}_2^4$, then the Hamming weight of $z = x + y$ is
(a) 1. (b) 5. (c) 2. (d)7. 1.5

(8) For a linear (n, k)-code C, the syndrome $S(y)$ of y is a vector of length
(a) n. (b) k. (c) $n - k$. (d) None of the above. 1.5

(9) A BCH code of length n over $\mathbb{F}_q$ is called a Reed-Solomon code if
(a) $n = q - 1$. (b) $n = q$. (c) $n = q + 1$. (d) None of the above. 1.5

(10) A linear code C is cyclic if and only if C is an ideal of
(a) $F_q[x]/(x^n - 1)$. (c) $(x^n - 1)F_q[x]$.
(b) $F_p[x]/(x^n - 1), q = p^n$, p a prime. (d) None of the above. 1.5

Section - B

Unit - I

(1) If L is a finite extension of K and M is a finite extension of L, then show that M is a finite extension of K with

$$[M : K] = [M : L][L : K].$$

8

(2) Let F_q be the finite field with $q = p^n$ elements. Then every subfield of F_q has order p^m, where m is a positive divisor of n. Conversely, if m is a positive divisor of n, then there exist exactly one subfield of F_q with p^n elements. 8

Unit - II

(3) Prove that the distinct automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are exactly the mappings $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$, defined by $\sigma_i(\alpha) = \alpha^{q^i}$, for $\alpha \in \mathbb{F}_{q^m}$ and $0 \leq i \leq m-1$. 8

(4) Let K be a finite field, F an extension of K of degree m over K, and $\alpha_1, \alpha_2, \ldots, \alpha_m \in F$. Then $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a basis of F over K if and only if $\Delta_{F/K}(\alpha_1, \alpha_2, \ldots, \alpha_m) \neq 0$. 8

Unit - III

(5) Let F be a finite extension of $K = \mathbb{F}_q$ and $\alpha = \beta^q - \beta$ for some $\beta \in F$. Prove that $\alpha = \gamma^q - \gamma$ with $\gamma \in F$ if and only if $\beta - \gamma \in K$. 8

(6) Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree m. Then $f(x)$ divides $x^{q^n} - x$ if and only if m divides n. 8

Unit - IV

(7) If C is a binary $(n, 1)$ repetition code, then prove that the dual code $C^{\perp}$ is the $(n, n-1)$ parity check code.. 8

(8) State and prove Gilbert-Varshamov Bound theorem. 8

Unit - V

(9) Define cyclic code and show that the binary cyclic code of length $n = 2^m - 1$ for which the generator polynomial is minimal polynomial over F_2 of a primitive element of F_{2^m} is equivalent to the binary $(n, n-m)$ Hamming code. 8

(10) Prove that linear code C is cyclic if and only if C is an ideal of $\mathbb{F}_q[x]/(x^n - 1)$. 8

Section C

(11) State and prove existence and uniqueness theorem of finite fields. 15

(12) Prove that for $\alpha \in \mathbb{F}_{q^m}$, $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\}$ is a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if and only if the polynomials $x^m - 1$ and $\alpha x^{m-1} + \alpha^q x^{m-2} + \ldots + \alpha^{q^{m-2}} x + \alpha^{q^{m-1}}$ in $\mathbb{F}_{q^m}[x]$ are relatively prime. 15

(13) Show that the product $I(q, n; x)$ of all monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree $n > 1$ satisfy

$$I(q, n; x) = \prod_{m} Q_m(x),$$

where the product is extended over all positive divisors m of $q^n - 1$ for which n is the multiplicative order of q modulo m, and where $Q_m(x)$ is the mth cyclotomic polynomial over $\mathbb{F}_q$. 15

(14) Construct a standard array for code defined by parity-check matrix

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Use it to decode the vector 110110. 15

(15) Define the BCH code and give the decoding algorithm for the BCH code. 15