Birla Institute of Technology and Science, Pilani (Pilani Campus)
First Semester 2022-23

Course Number: MATH F441 (Discrete Mathematical Structures) — Comprehensive Exam
Date of Examination: 19.12.2022 (Monday) — **Part A (Closed Book)**
Maximum Duration: 180 min (9:00 am-12:00 pm)

General Instructions.

1. There are two parts: Part A is Closed Book and for 40 marks. **The maximum time allowed for Part A is 90 minutes.** You will get answer sheet for Part B after you submit your answers for Part A.
2. Calculators are allowed.
3. For a prime p, the symbols $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p$ are used interchangeably.
4. If two or more solutions are written for the same question, only the first one will be graded.

Q1. True or False. Justify your answers.

(i) A $(343, 171, 85)$-BIBD exists. **[2]**

(ii) Let $f(x) \in \mathbb{F}_2[x]$ be irreducible. Then $\alpha = [x]$ is a primitive element for the field $\mathbb{F}_2[x]/f(x)$. **[3]**

Q2. Let $(X, \mathcal{A})$ be a symmetric (v, k, λ)-BIBD with incidence matrix A.

(a) Let $B \in \mathcal{A}$. Determine if $(X \setminus B, \{S \setminus B : S \in \mathcal{A},\ S \neq B\})$ is a BIBD. If so, determine the parameters.

(b) Let $p = \sqrt{\frac{\lambda}{v}}$. Let J denote the $v \times v$ matrix with all entries 1.

(i) Prove that $1/(k-\lambda)(A + pJ)$ is the inverse of $A^t - pJ$, where A^t denotes the transpose of A.

(ii) Prove that $AA^t = A^tA$.

[4+7]

Q3. Use Berlekemp's algorithm to find the number of irreducible factors of the square-free part of the polynomial $f(x) = x^5 + x + 1 \in \mathbb{F}_2[x]$. **[6]**

Q4. Find the 2×2 encryption matrix of a Hill cipher which encrypted the plaintext CEIGEL to the ciphertext NCHYAO. Here, the letters were converted to numbers as:

A	B	C	...	Y	Z
1	2	3	...	25	26

[6]

Q5. Let $n \in \mathbb{N}$ and let $a_1, \ldots, a_n \in \mathbb{Z}$ with $a_i \neq a_j$ if $i \neq j$. Prove that $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) - 1$ is irreducible in $\mathbb{Z}[x]$. **[6]**

Q6. Let $m(x) = x^5 + x^2 + 1 \in \mathbb{F}_2[x]$. Consider the field $\mathbb{F}_2[x]/m(x)$, identified as $\mathbb{F}_2[\alpha]$. The information word $(1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ is to be sent using BCH codes in this field and $t = 2$. Find the word that is sent. Justify all the steps. You may use the table provided on the next page.

[6]

1		$\alpha^{15} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$
α		$\alpha^{16} = 1 + \alpha + \alpha^3 + \alpha^4$
α^2		$\alpha^{17} = 1 + \alpha + \alpha^4$
α^3		$\alpha^{18} = 1 + \alpha$
α^4		$\alpha^{19} = \alpha + \alpha^2$
$\alpha^5 = 1 + \alpha^2$		$\alpha^{20} = \alpha^2 + \alpha^3$
$\alpha^6 = \alpha + \alpha^3$		$\alpha^{21} = \alpha^3 + \alpha^4$
$\alpha^7 = \alpha^2 + \alpha^4$		$\alpha^{22} = 1 + \alpha^2 + \alpha^4$
$\alpha^8 = 1 + \alpha^2 + \alpha^3$		$\alpha^{23} = 1 + \alpha + \alpha^2 + \alpha^3$
$\alpha^9 = \alpha + \alpha^3 + \alpha^4$		$\alpha^{24} = \alpha + \alpha^2 + \alpha^3 + \alpha^4$
$\alpha^{10} = 1 + \alpha^4$		$\alpha^{25} = 1 + \alpha^3 + \alpha^4$
$\alpha^{11} = 1 + \alpha + \alpha^2$		$\alpha^{26} = 1 + \alpha + \alpha^2 + \alpha^4$
$\alpha^{12} = \alpha + \alpha^2 + \alpha^3$		$\alpha^{27} = 1 + \alpha + \alpha^3$
$\alpha^{13} = \alpha^2 + \alpha^3 + \alpha^4$		$\alpha^{28} = \alpha + \alpha^2 + \alpha^4$
$\alpha^{14} = 1 + \alpha^2 + \alpha^3 + \alpha^4$		$\alpha^{29} = 1 + \alpha^3$
		$\alpha^{30} = \alpha + \alpha^4$

Birla Institute of Technology and Science, Pilani (Pilani Campus)
First Semester 2022-23

Course Number: MATH F441 (Discrete Mathematical Structures) | Comprehensive Exam
Date of Examination: 19.12.2022 (Monday) | **Part B (Open Book)**
Maximum Duration: 180 min (9:00 am-12:00 pm)

General Instructions.

1. There are two parts: Part B is Open Book and for 40 marks. The maximum time allowed for Part A is 90 minutes. You will get answer sheet for Part B after you submit your answers for Part A.
2. Calculators are allowed.
3. For a prime p, the symbols $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_p$ are used interchangeably.
4. If two or more solutions are written for the same question, only the first one will be graded.

Q1. Let n be a positive integer, and let p be a prime number that divides $2^n + 1$. Prove that if m is an odd positive integer, then p does not divide $2^m - 1$. **[6]**

Q2. Let $f(x) \in \mathbb{Z}[x]$. Let $\varphi_f(m)$ denote the number of integers a with $1 \leq a \leq m$ such that $\gcd(f(a), m) = 1$. Prove that

$$\varphi_f(m) = m \prod_{p|m} \left(1 - \frac{N(p)}{p}\right),$$

where $N(p)$ equals the number of solutions modulo p of the congruence $f(x) \equiv 0 \pmod{p}$. **[9]**

Q3. Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = p^n$, for an odd prime p and a positive integer n. Prove that for every $x \in \mathbb{F}$, there exist $a, b \in \mathbb{F}$ such that $x = a^2 + b^2$. (*Hint: Consider the number of squares in* $\mathbb{F}$.) **[9]**

Q4. Using Chinese Remainder Theorem, find $f(x)$ in $\mathbb{F}_2[x]$ such that $\deg(f(x)) < 6$ and

$$f(x) \equiv 1 \pmod{x+1},$$
$$f(x) \equiv x \pmod{x^2+x+1},$$
$$f(x) \equiv x^2+x+1 \pmod{x^3+x^2+1}.$$

[8]

Q5. Determine the number of inequivalent colourings of a necklace with five beads, using three colours for the beads. (You may assume that the beads form the vertices of a regular pentagon. Two colourings are considered equivalent if one can be transformed into the other via a rotation or a reflection.)

[8]

ALL THE BEST