tcg crest

(Deemed to be University u/s 3 of UGC Act, 1956)

Distinct Category - Research

TCG CREST

School of Mathematics and Computer Sciences

Ph.D. Programme
Cryptology and Post-Quantum Cryptology

Academic Session: August 2026

Sample Questions
for the Written Admission Test

Institute for Advancing Intelligence
TCG CREST

Sample Questions

I. Research Methodology

1. Academic research in Science and Technology includes

   A. Research in Humanities.

   B. Research in Psychology.

   C. Research in Basic Science and Technology.

   D. Legal Research.

2. The main characteristic of scientific research is

   A. Empirical.

   B. Theoretical.

   C. Experimental.

   D. All of the above.

3. The prescribed style of supervision is

   A. Laissez-Faire.

   B. Hybrid.

   C. Algorithmic.

   C. Spoon-Feed.

4. A null hypothesis is

   A. When there is no difference between the variables.

   B. The same as research hypothesis.

   C. Subjective in nature.

   D. When there is difference between the variables.

5. A case study is a type of

   A. Experimental research.

   B. Descriptive research.

   C. Correlational research.

   D. Meta-analysis.

II. Technical Section

A. General Mathematics

Basic Algebra

1. (a) Consider the polynomial $x^5 + ax^4 + bx^3 + cx^2 + dx + 4$ where a, b, c, d are real numbers. If $(1 + 2i)$ and $(3 - 2i)$ are two roots of this polynomial then determine the value of a.

   (b) Determine the number of real roots of the equation

   $$2\cos\left(\frac{x^2 + x}{6}\right) = 2^x + 2^{-x}.$$

   (c) If $(1 + x)^n = C_0 + C_1x + C_2x^2 + \ldots + C_nx^n$, n being a positive integer, then determine the value of

   $$\left(1 + \frac{C_0}{C_1}\right)\left(1 + \frac{C_1}{C_2}\right)\ldots\left(1 + \frac{C_{n-1}}{C_n}\right).$$

2. (a) Determine the number of solutions in $1 \leq x \leq 315$ to the following system of congruent equations:

   $$x \equiv 2 \mod 15,\ x \equiv 1 \mod 21.$$

   (b) Find a basis for the following subspace of $\mathbb{R}^4$:

   $$\{(x_1, x_2, x_3, x_4) : x_1 + x_2 + x_3 + 3x_4 = 0, x_1 + x_2 - 2x_3 + x_4 = 0\}.$$

   Argue whether it is possible to compute the dimension of the above subspace without explicitly finding a basis? Justify your answer.

   (c) Consider the following system of equations over a field $\mathbf{F}$.

   $$\begin{aligned} a_1x + b_1y &= c_1 \\ a_2x + b_2y &= c_2, \end{aligned}$$

   where $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbf{F}$. State the conditions for which the above system of equations has (i) no solution, (ii) a unique solution, and (iii) more than one solution.

3. (a) Let G be a finite group of order mn where m and n are relatively prime. Assume there exist $a, b \in G$ such that a has order m and b has order n. Prove that G is cyclic if and only if $ab = ba$.

   (b) Let G be a finite group and $x \in G$ has order k. Prove that for any $m \in \mathbb{Z}$, $x^m = e$ if and only if $k|m$.

   (c) Let $f(z) = z^2 - z + 1$ be defined on the unit disk $D = \{z \in \mathbb{C} : |z| \leq 1\}$. Find the maximum value of $|f(z)|$.

4. (a) Let H be a subgroup of $\mathbb{R}$ under addition. Let

   $$K = \{2^a | a \in H\}.$$

   Prove that K is a subgroup of the group $\mathbb{R}^*$ of non-zero real numbers under multiplication.

   (b) Let G be the set of all real 2×2 matrices of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $a \neq 0$ and $d \neq 0$. (i) Show that$G$ forms a group under matrix multiplication. (ii) Show that $H = \left\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} :\right.$

$b \in \mathbb{R}\Big\}$ is a normal subgroup of G. (iii) Show that G/H is an abelian group.

5. (a) Let S_n be the group of all permutations of $\{1, \ldots, n\}$ under composition. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

be an element of S_6. (i) Find the order of the cyclic subgroup generated by σ. (ii) Find the minimum n such that S_n contains a cyclic subgroup of order 30. Justify your answer. (iii) Let S be a cyclic group of order 6. Show that S has a unique subgroup of order 3. (iv) Let S be a finite cyclic group and K be a subgroup of S oforder m. Show that an element $a \in S$ is an element of K ifand only if $a^m = e$.

(b) Let G be the group of non-zero complex numbers under multiplication and let N be the set of complex numbers of absolute value 1 (i.e., $a + bi \in N$ if $a^2 + b^2 = 1$). Show that G/N is isomorphic to the group of all positive real numbers under multiplication.

6. (a) Let Q be the group (under ordinary matrix multiplication) generated by the Complex matrices

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},$$

where $i^2 = -1$. Prove that

(a) Q is a non-abelian group of order 8.

(b) Each subgroup of Q is normal in Q.

(b) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where a, b, c, d are integers modulo p, p is a prime such that $ad - bc \neq 0$. Prove that G forms a group under matrix multiplication. Assuming $H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid ad - bc = 1 \right\}$, find $o(H)$.

Elementary Linear Algebra

1. (a) Let $\lambda_1, \lambda_2, \lambda_3$ denote the eigenvalue of the matrix

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos t & \sin t \\ 0 & -\sin t & \cos t \end{pmatrix}$$

If $\lambda_1 + \lambda_2 + \lambda_3 = \sqrt{2} + 1$, then determine the set of values of t.

(b) Let $\Theta = 2\pi/67$. Consider the following matrix

$$A = \begin{pmatrix} \cos\Theta & \sin\Theta \\ -\sin\Theta & \cos\Theta \end{pmatrix}$$

Then determine the matrix A^{100}.

2. (a) Let A and B be two $n \times n$ symmetric matrices such that $AB = BA$. Show that if $x \neq 0$ is an eigenvector of A and $Bx \neq 0$, then Bx is also an eigenvector of A corresponding to the same eigenvalue.

(b) Let B be a non-singular matrix. Prove that λ is an eigenvalue of B if and only if λ^{-1} is an eigenvalue of B^{-1}.

3. (a) If $\text{rank}(A) = \text{rank}(A^2)$, then show that $\{x : Ax = 0\} = \{x : A^2x = 0\}$.

   (b) Let A be an $n \times n$ symmetric matrix and let $l_1, l_2, \ldots, l_{r+s}$ be $(r+s)$ linearly independent $n \times 1$ vectors such that for all $n \times 1$ vectors x, $x^{\mathsf{T}}Ax = (l_1^{\mathsf{T}}x)^2 + \ldots + (l_r^{\mathsf{T}}x)^2 - (l_{r+1}^{\mathsf{T}}x)^2 - \ldots - (l_{r+s}^{\mathsf{T}}x)^2$. Prove that $\text{rank}(A) = r + s$.

4. (a) Let V denote the vector space $\mathbb{R}$. Suppose $V \to \mathbb{R}^n$ is a function satisfying

   - $f(v_1, \ldots, v_n) = 0$ whenever $v_i = v_j$ for some $i \neq j$
   - $f(v_1, \ldots, v_{i-1}, \alpha v_i, v_{i+1}, \ldots, v_n) = \alpha f(v_1, \ldots, v_n)$
   - $f(v_1, \ldots, v_{i-1}, v_i + u_i, v_{i+1}, \ldots, v_n) = f(v_1, \ldots, v_n) + f(v_1, \ldots, v_{i-1}, u_i, v_{i+1}, \ldots, v_n)$
   - $f(e_1, \ldots, e_n) = 1$ where e_i is i-th unit vector,

   where $\alpha \in \mathbb{R}$ and $u_i \in \mathbb{R}^n$. Show that for any $n \times n$ matrix A, whose columns are $v_1, \ldots, v_n$, $f(v_1, \ldots, v_n) = \det(A)$.

   (b) If T is an injective homomorphism of a finite dimensional vector space V onto a vector space W, prove that T maps a basis of V onto a basis of W.

5. (a) Let V be the vector space of sequence $(a_n)_{n \geq 1}$ of complex numbers. The shift operator $S : V \to V$ is defined by

$$S(a_1, a_2, a_3, \ldots) = (a_2, a_3, a_4, \ldots).$$

   i. Find the eigen vectors of S.

   ii. Show that the subspace W of V consisting of the sequence (a_n) satisfying $a_{n+2} = a_{n+1} + a_n$ is two-dimensional and $S(W) \subseteq W$.

   (b) Find the null space of the following matrix:

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -2 & 0 \\ 4 & 2 & 0 & 0 & 3 \\ 1 & 1 & 1 & -2 & 1 \\ 2 & 2 & 0 & 0 & 2 \\ 1 & 1 & 2 & -4 & 1 \end{bmatrix}.$$

Statistics

1. (a) Let $f(k) = \frac{1}{k(K+1)}$ for integers $k \geq 1$. Show that f is a probability mass function and find the corresponding cumulative density function. What are its mean and median?

   (b) A coin (need not be fair) is tossed till the kth head shows up. Let X be the number of tosses required. Find the probability mass function of X.

2. (a) Find the mode of $Gamma(\alpha, 1)$ density and the mode of $Poi(\lambda)$ distribution.

   (b) Throw r distinguishable balls into m labelled bins, independently and with probabilities $p_1, \ldots, p_m$ $(p_1 + \ldots + p_m = 1)$. Let X be the number of empty bins. Find the expectation and variance of X.

   (c) For a random variable X, show that :

   i. $\mathbb{E}[(X - a)^2]$ is minimized when $a = \mathbb{E}[X]$.

   ii. $\mathbb{E}[|X - a|]$ is minimized at the medians of X.

3. (a) A box contains p balls carrying label 1, another p balls carrying label 2 and so on up to p coupons labelled N. Draw two balls uniformly at random without replacement and note their labels as X and Y. Find the mean and variance of X and of Y and the covariance of X and Y. What would be the co-variance, when $p \to \infty$?

   (b) From a box of N balls labelled $1, 2, \ldots, N$, we draw three balls one after another, uniformly at random. Let X_1, X_2, X_3 be the numbers on the balls. Find the mean and variance of $X_1 + X_2 + X_3$ in the following two situations: (i) the balls are drawn with replacement, (ii) the balls are drawn without replacement.

4. (a) For $X \sim Exp(\lambda)$, find the moments of X. Also find the mean and variance of $\log X$. Can you justify (without calculations) why the variance of $\log X$ should be independent of λ?

   (b) For independent random variables X and Y, find the distribution of $Z = T(X, Y)$ for

      i. X, Y are i.i.d $N(0, 1)$ and $T(x, y) = x/y$.

      ii. X, Y are i.i.d $Unif[0, 1]$ and $T(x, y) = x + y$.

5. (a) If X and Y are Bernoulli random variables, then show that X and Y independent if and only if they are uncorrelated.

   (b) Let U be a random variable and let $X = f(U)$ and $Y = g(U)$ where $f, g : \mathbb{R} \to \mathbb{R}$ are non-decreasing functions. Show that $Cov(X, Y) \geq 0$.

6. Suppose that $X_1, \ldots, X_n$ is a random sample from a standard normal distribution and define the random variable

$$Y_n = \sum_{i=1}^{n} X_i^2.$$

   (a) Show that $\sqrt{n/2}\,[\frac{1}{n}Y_n - 1]$ converges in distribution to the standard normal random variable Z.

   (b) Let $U_n = (2n^2)^{-1/4}\sqrt{Y_n}$. Show that $\sqrt{n}\,[U_n - 2^{-1/4}]$ converges in distribution to a normal random variable with mean zero and variance $2^{-3/2}$.

7. Let $X_1, \ldots, X_n$ $(n \geq 2)$ be a random sample of a normal distribution with mean zero and variance σ^2. Define

$$W_n = \frac{1}{\binom{n}{2}} \sum_{i=2}^{n} \sum_{j=1}^{i-1} |X_i - X_j|.$$

   (a) For $n = 4$, find b_1, b_2, b_3, b_4 such that $W_4 = b_1 Y_1 + b_2 Y_2 + b_3 Y_3 + b_4 Y_4$, where $Y_1 \geq Y_2 \geq Y_3 \geq Y_4$ is the order statistics of X_1, X_2, X_3, X_4.

   (b) Show that $V_n = \frac{\sqrt{\pi}}{2} W_n$ is an unbiased estimator of σ.

Discrete Mathematics

1. (a) Find the number of permutations of the letters FRIENDS containing

      i. the string DIE?

      ii. the strings RED and FIR?

      iii. the strings FIN and END?

   (b) We consider a decimal digit string a *valid* codeword if it has an even number of zeros. As an example, 1220987078 is a valid codeword, but 67099032024 is not a valid codeword. Let s_n be the number of valid n-digit codewords. Write down a recurrence relation for s_n with the initial conditions. Solve the recurrence to find out the number of valid n-digit codewords.

(c) Consider a shop that has six different flavors of soft drink bottles, with eleven bottles of each flavor. These bottles are stored in five crates. Prove that at least one of the crates contains at least three bottles of one flavor and at least three bottles of another flavor.

2. (a) Let $X \subseteq \{1, 2, \ldots, 99\}$ such that $|X| = 10$. Prove that there always exists two disjoint non-empty proper subsets of X (say X_1 and X_2) such that

$$\sum_{x \in X_1} x = \sum_{x \in X_2} x.$$

As an example, for the set $X = \{12, 33, 38, 42, 54, 66, 71, 72, 85, 90\}$, take $X_1 = \{12, 33, 42, 71\}$ and $X_2 = \{38, 54, 66\}$.

(b) A message is a sequence of bits, that is, 0s and 1s. Transmitting the bit 0 takes one unit of time while sending the bit 1 takes two units of time. Now transmitting different messages might incur the same time; for example, the messages 000, 01, or 10 will take exactly three units of time. Obtain the number of messages that can be sent in exactly T units of time.

3. (a) You are given a circle with a set of n points lying on the circumference of the circle. Suppose you draw lines connecting every point to every other point. Let I be the set of all points of intersection of the lines in the interior of the circle. Assume that no three lines intersect in a single point inside the circle.

i. Find the cardinality of I for $n = 4$ and $n = 5$.

ii. Extend your result to find the cardinality of the set I for general n.

(b) Consider a country where the only available currency notes are 7-rupee and 13-rupee notes. Show that it is impossible to make exactly 71 rupees using these notes, however, any amount greater than 71 rupees can be made.

4. (a) Show that there are exactly $(n + 1)$ way so that one can fill a bag with n fruits subject to the following constraints:

- The number of apples must be even.
- The number of bananas must be a multiple of 5.
- There can be at most 4 oranges.
- There can be at most 1 pear.

(b) Consider a building having a staircase with n stairs. In how many ways can a person climb the staircase, if she can climb by 1 or by 2 stairs in each step? Find out a closed form expressionin terms of n.

5. (a) A car odometer can display any six-digit combination from 000000 to 999999, both inclusive.

i. If it runs through its entire range, how many such combinations will have at least one digit 1 in them?

ii. What is the total number of times the digit i will be displayed? (For example, 101111 contributes five towards the total count of 1's and the next reading 101112 adds four more)

(b) Prove that if $n^2 + 1$ points are placed in an equilateral triangle (the region inside as well as the perimeter) of side length 1, then there are two points whose distance is at most $1/n$.

6. (a) A function $f : \{0, 1\}^n \to \{0, 1\}$ is called self-dual if $f(x_1, x_2, \ldots, x_n) = f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})$, for all $x_1, x_2, \ldots, x_n$, where $\overline{x_i}$ is complement of the bit x_i. Compute the number of self dual functions that are present over n tuples.

(b) A 4×4 S-box is a permutation that takes 4-bit input and produces a 4-bit output. An S-box is called good if the S-box contains no fixed points (i.e. $\forall x \in \{0,1\}^4$, $S(x) \neq x$). Count the number of 4×4 good S-boxes.

Elementary Probability

1. (a) Given a biased coin with probability of head being $p \neq 1/2$, how can you generate a uniformly random bit string (i.e., you need to prove that the probability of each bit being 0 or 1 is 1/2).

   (b) A multiple choice examination has 4 choices for each question, with exactly one correct answer. A student has prepared in the following way:

   - the probability that he knows the exact answer to a question is 0.5;
   - the probability that he is able to eliminate one wrong choice is 0.25;
   - otherwise, all the four choices seem equally plausible.

   If the student knows the answer, he will get the question right. If not, he has to guess from three or four choices depending on whether he could elimimate one wrong choice, or not. Now, if the student answers a question correctly, find out the probability that he actually knew the answer.

2. (a) What is the probability that 1 succeeds n and 2 succeeds $(n-1)$ in a randomly selected permutation over $\{1, \ldots, n\}$?

   (b) Let X be the result of rolling a fair 4-sided die and Y be the result of rolling a fair 6-sided die. Consider the following gambling game: You win $2X$ dollars if $X > Y$ and lose 1 dollar, otherwise. After playing this game 120 times, what is your expected total gain or loss?

   (c) Let X and Y be independent Poisson random variables with respective means λ_1 and λ_2. Calculate the conditional expected value of X given that $X + Y = n$.

3. (a) Consider an one-dimensional X axis of length w units, i.e. the starting co-ordinate is $(0, 0)$ and the end co-ordinate is $(w, 0)$. A drunk guy is placed on the island at location $(n, 0)$ where $n < w$. He then randomly walks on the island along the X-axis: at each step, he either moves to the left or to the right from its current position each with probability 1/2. If he stands either on the location $(0, 0)$ or on the location $(w, 0)$, then he will immediately falls off. Can he surive?

   (b) Consider the above problem with X-axis is infinitely extended to the right direction and the drunk guy is placed at location $(1, 0)$. Then what is the probability that he will survive?

4. (a) A line of 100 airline passengers is waiting to board a plane. They each hold a ticket to one of the 100 seats on that flight (for convenience, let's say that the nth passenger in line has a ticket for the seat number n). Unfortunately, the first person in line is crazy, and will ignore the seat number on his ticket, picking a random seat to occupy. All of the other passengers are quite normal, and will go to their proper seat unless it is already occupied. if it is occupied, they will then find a free seat to sit in, at random. What is the probability that the i^{th} person to board the plane will sit in his proper seat?

   (b) You are given three biased coins. For the first two coins, the probability of getting a head is 2/3, whereas the probability of getting a head for the third coin is 7/8. Design an unbiased coin that uses exactly one toss of each of these three coins. [Note: Essentially you have to define an event whose probability is 1/2.]

5. (a) A man has ten coins. Nine ordinary and one with heads on both sides. He selects a coin at random, tosses it six times, and it always comes up heads. Compute the probability that he selected the double headed coin.

(b) Two teams (Team A and Team B) play 5 match ODI series. Team A has a probability $\frac{3}{4}$ winning a single game. What is the probability Team A wins the series?

6. Suppose you and your friend have a two-sided coin each. Your coin lands Heads with probability $\frac{1}{6}$, while your friend's coin lands Heads with probability $\frac{3}{4}$. The two coins are independent of one another. Suppose you play a game where you both flip your coins once, and if they both land on the same side (i.e., both Heads or both Tails) you get x dollars from your friend, but if they land on different sides, then your friend gets 2 dollars from you. What is the minimum integer value of x for which your expected total winnings after 3 rounds of this game are positive (i.e., you are expected to make money rather than lose some)?

Number Theory

1. (a) If $n \geq 1$ is an integer, show that among $n,\ n+1,\ n+2$ and $n+3$, there is one which is co-prime to the other three.

   (b) Let $k > 1$ and $2^k - 1$ is a prime. Show that $n = 2^{k-1}(2^k - 1)$ is a perfect number. A perfect number is a positive integer that is equal to the sum of its positive divisors, excluding itself.

2. (a) Let p and q are large primes and $N = pq$. We choose a number e such that e is co-prime to $\phi(n)$ and $d = e^{-1} \mod \phi(n)$. Now we consider two functions $f_{N,e} : \mathbb{Z}_N \to \mathbb{Z}_N$, defined as $f_{N,e}(m) = m^e \mod N$ and $g_{N,d} : \mathbb{Z}_n \to \mathbb{Z}_N$ defined as $g_{N,e}(c) = c^d \mod N$. Prove that for $g_{N,e} \circ f_{N,e}$ is an identity function.

   (b) Let $\phi_2(n)$ is the number of positive integers a such that both a and $a+1$ are co-prime to n. Find out the formula for $\phi_2(n)$. (You can assume $\phi_2(n)$ is a multiplicative function, i.e., if m and n are relatively prime then $\phi_2(mn) = \phi_2(m)\phi_2(n)$).

3. (a) There are n people numbered 1 to n standing in a circle. Starting the count with person number 1, every second person is eliminated until only one person is left. Where in the circle should a person stand to remain the last person standing?

   (b) Suppose there are 100 doors labelled with 1 to 100 and there are 100 persons labelled with 1 to 100. Initially each door is closed. For $1 \leq i \leq 100$, i-th person flips the state of the doors whose labels are multiple of i. Determine how many doors will remain open after 100-th person completes the task.

Calculus

1. Consider the function $f(x) = \begin{cases} px + q, & x > 0 \\ \cos 2x, & x \leq 0 \end{cases}$

   (a) Find the values of the constants p and q for which the above function is differentiable, but not continuous.

   (b) Find the values of the constants p and q for which the above function is continuous, but not differentiable.

2. (a) Find the values of the constants a, b and c for which the following function is differentiable. (Give a and b in terms of c.)

$$f(x) = \begin{cases} cx^2 + 4x + 1, & x \geq 1 \\ ax + b, & x < 1 \end{cases}$$

(b) Find all values of a, b such that $f'(x)$ is continuous:

$$f(x) = \begin{cases} ax + b, & x \geq 1 \\ x^2, & x < 1 \end{cases}$$

3. (a) Let a be a positive number. Then find out the value of

$$\lim_{n\to\infty} \left[\frac{1}{a+n} + \frac{1}{2a+n} + \ldots + \frac{1}{na+n} \right].$$

(b) Find out the value of

$$\lim_{n\to\infty} \left\{ \left(1 + \frac{1}{n}\right)^n - \left(1 + \frac{1}{n}\right) \right\}^{-n}.$$

(c) Find out the value of

$$\lim_{n\to\infty} \sum_{i=1}^{n} \frac{1}{n} \left[\sqrt{4i/n}. \right],$$

where $[x]$ denotes the greatest integer which is less than or equal to x.

4. (a) Find out the value of the integral

$$\int_0^{\pi/4} \left[3 \tan^2 x \right] dx.$$

(b) Prove that the integrals

$$\int_0^{\infty} \cos x^2 dx, \quad \text{and} \quad \int_0^{\infty} \sin x^2 dx$$

converges.

(c) Show that the derivative of an even function is odd and that the derivative of an odd function is even.

B. Technical Topics in Computer Science

Graph Theory

1. (a) A tree T is called an $(1, 4)$-tree if all of it's vertices have degree either 1 or 4. If T has n leaves, find the number of vertices with degree 4.
   (b) A k-tree is defined as a tree with each of it's non-leaf nodes containing exactly k children. Obtain the minimum and maximum height of a k-tree with n nodes.
   (c) Prove or Refute: You are given an undirected graph G with unique positive weights and a Minimum Spanning Tree (MST) T. If we square the value of all the edge weights and compute the MST again, we will obtain the same tree structure again.

2. (a) What can be the maximum number of edges in a bipartite graph with 2023 vertices?
   (b) Let G be a forest with 123 vertices and 111 edges. How many disconnected components will be there in G?
   (c) Show that if a graph has $2n$ vertices and all of them have degree at least n, then the graph is connected.

3. (a) Let G be a simple graph of 8 vertices with exactly 3 components. Find the minimum and maximum number of edges of G. Can you generalize this result for n vertices with k components?
   (b) In a graph G with 10 vertices, among any three vertices of G, at least two are adjacent. Find the least number of edges that G can have. Can you draw such a graph?
   (c) Let G be a simple graph with 19 edges, and degree of each vertex is greater than 3. Knowing nothing else about G, find (i) the maximum number of vertices that G could have, (ii) the maximum number of vertices that G could have for which one can conclude whether G is planar or not.

4. Let $A = (A_{i,j})_{n\times n}$ be an adjacency matrix of a simple (having no self loop or multiple edges) undirected graph G with n vertices.
   (a) Prove that $A^k_{i,j}$ is the number of k-length walks between the vertices i and j.
   (b) Prove or Refute: G is connected if and only if all the entries of $A + A^2 + \cdots + A^{n-1}$ are positive.
   (c) Let $\texttt{tr}(A)$ denotes the trace of matrix A, which is the sum of all its diagonal entries. Prove that $\texttt{tr}(A^2) = 2|E(G)|$, where $E(G)$ denotes the set of undirected edges of G.

5. (a) Consider the process of coloring the vertices of a graph. We need to assign colours to the vertices such that any pair of neighbouring vertices do not share the same colour. What is the minimum number of distinct colours you need to colour the following graphs?
   (i) $K_{m,n}$ (the complete bi-partite graph with partite size m and n), (ii) $\overline{K}_{m,n}$ (complement of $K_{m,n}$). Justify your answers.
   (b) If G is a graph with 10 vertices and 30 edges, then show that the (vertex) chromatic number of G is at least 3.

Elements of Computing

1. (a) Given an array $A = \{a_1, a_2, \ldots, a_n\}$ of unsorted distinct integers, write a program in pseudo-code for the following problem: given an integer u, arrange the elements of the array A such that all the elements in A which are less than or equal to u are at the beginning of the array, and the elements which are greater than u are at the end of the array. You may use at most 5 extra variables apart from the array A.

(b) How many asterisks ($*$) in terms of k will be printed by the following C function, when called as $count(m)$, where $m = 3^k$? Assume that 4 bytes are used to store an integer in C and k is such that 3^k can be stored in 4 bytes.

```
void count(int n)
{
   printf("*");
   if(n>1)
   {
       count(n/3);
       count(n/3);
       count(n/3);
   }
}
```

2. (a) Consider the pseudo-code given below.

Input: integers b and c.

```
1. a_0 = max(b,c),a_1 = min(b,c)
2. i = 1.
3. Divide a_{i-1} by a_i.
4. Let q_i be the quotient and r_i be the remainder.
5. If r_i==0 then go to Step 9.
6. a_{i+1} = a_{i-1}-q_i*a_i.
7. i = i + 1
8. Go to Step 3.
9. Print a_i.
```

What is the mathematical relation between the output a_i and the two inputs b and c.

(b) You are given the following file abc.h:

```
#include <stdio.h>
#define SQR(x) (x*x)
#define ADD1(x) (x=x+1)
#define BeginProgram int main(int argc,char *argv[]){
#define EndProgram return 1;}
```

For each of the following code fragments, what will be the output?

```
(i)  #include "abc.h"
main()
{
    int y = 4;
    printf("%d\n", SQR(y+1));
}
```

```
(ii)  #include "abc.h"
BeginProgram
int y=3;
```

```
printf("%d\n", SQR(ADD1(y)));
EndProgram
```

3. (a) Consider the following program:

```
void g(char *s, int len)
{
    if(len == 0)
         return;
    char temp = s[0]; s[0] = s[len-1]; s[len-1] = temp;
    g(s+1, len-2);
}


int main()
{
    char s[] = "hello";
    g(s, strlen(s));
    printf("%s", s);
}
```

What will be the output of the above program ?

(b) Let A be an integer array of size N. The function max returns the maximum of its two arguments. The two code fragments shown below are equivalent (i.e., n, r, s have the same value at the end) if we fill the blank with (i).

```
n = 0, r = 0, s = 0;
while (n != N)
{
    s =  max(s + A[n], 0);
    r = max(r, s);
    n = n+1;
}
```

```
n = -1, r = 0, s = 0;
while (n != N)
{
    r = max(r, s);
    n = n+1;
    if(____(i)____)
    s =  max(s + A[n], 0);
}
```

(c) When called with $x = 10! + 9!$ and $y = 8!$, what does the function f below return?

```
int f(x,y)
{
    int count=0;
    while(x > y)
    {
```

```
            x=x-y;
            count++;
        }
        while(y > x)
        {
            y=y-x;
            count++;
        }
        return count;
    }
```

Data Structures

1. You are given k sorted lists, each containing m integers in ascending order. Assume that (i) the lists are stored as singly-linked lists with one integer in each node, and (ii) the head pointers of these lists are stored in an array.

   (a) Write an efficient algorithm that merges these k sorted lists into a single sorted list using $\Theta(k)$ additional storage.

   (b) Next, write an efficient algorithm that merges these k sorted lists into a single sorted list using $\Theta(1)$ additional storage.

   (c) Analyse the time complexity of your algorithm for both the cases.

2. Suppose you are given a data structure D of n elements that maintains an ordering and supports the following operations:

   - D.set_value(x, i): Set the value x to the i-th element of D.
   - D.get_value(i): Get the value of i-th element of D.

   Answer the following assuming the first operation can be done in $O(n)$ and the second operation can be performed in $O(1)$ time. Marks will be alloted according to the efficiency of your algorithms.

   (a) Describe an algorithm to report an element in D which is neither maximum nor minimum.

   (b) Write an algorithm swap(D, i, j) that swaps the i^{th} and j^{th} elements in D. What is the time complexity of your algorithm?

   (c) Write an algorithm find_min(D) that reports the value of the minimum element in D. What is the time complexity of your algorithm?

   (d) Write down an algorithm sort(D) to sort the elements in D using the operations given above. Justify the time complexity of your algorithm. Assume that any comparison operation $(<, =, >, \leq, \geq)$ in D takes $O(1)$ time. [Hint: You may use the algorithms corresponding to (b) and (c) to sort efficiently in time $O(n^2)$.]

3. (a) Consider a sorted array $A = [a_1, \ldots, a_n]$ of n integers. Write an efficient algorithm that reports one index i such that $A[i] = i$, if it exists. Justify the time complexity of your algorithm.

   (b) Let Q be a non-empty queue and S be an empty stack. Using only the temporary variable X, and the four standard operations Push(S, X), Pop(S), EnQueue(Q, X), DeQueue(Q), and two tests IsEmpty(Q) and IsEmpty(S), write an algorithm to reverse the order of the elements in Q.

(c) A max-heap data structure is a complete binary tree that satisfies the max-heap property, i.e., the value of any given node is always greater than the values of its child nodes, and the value of the root node is the largest among all the nodes. Given a max-heap data structure with n distinct elements, report the third highest element with as few comparisons as possible.

4. (a) Consider a linked list containing n nodes, where each node contains two pointers ptr1 and ptr2. For each node, ptr1 points to the next node of the list. Describe how pointer ptr2 should be set up for each node so that you will be able to locate the i-th node from the start node in the list traversing no more than $\lceil \log i \rceil + \lceil i/2 \rceil$ nodes.

   (b) Give an efficient implementation for a data structure STACK_MIN to support an operation Min that reports the current minimum among all elements in the stack. Usual stack operations (Create, Push, Pop) are also to be supported.

5. (a) Let H_1 and H_2 be two complete binary trees that are heaps as well. Assume H_1 and H_2 are max-heaps, each of size n. Design and analyze an efficient algorithm to merge H_1 and H_2 to a new max-heap H of size $2n$.

   (b) Let B be a rooted binary tree of n nodes. Two nodes of B are said to be a sibling pair if they are the children of the same parent. Design an $O(n)$ time algorithm that prints all the sibling pairs of B.

6. Given an airport with a single runway, design an efficient runway reservation system of that airport. Each reservation request comes with requested landing time let's say t. Landing can go through if there is no landing scheduled within k minutes of requested time, that means t can be added to the set of scheduling landings. For example, suppose the reservation request comes with landing time 6:30 PM. Assuming k to be 15 minutes, the request will be approved if and only if there is no reservations between 6:15 PM to 6:45 PM. This system helps with reservations for the future landings. Once the plane lands safely, you have to remove the plane for landing sets.

   (a) Suggest a data structure to implement the above system so that new reservations can be done in $O(\log n)$ times, where n is the cardinality of the current set of scheduling landings.

   (b) How can you modify your data structure to report the number of planes scheduled between t_1 to t_2 in $O(\log n)$ time?

Design and Analysis of Algorithms

1. (a) Give a strategy to sort four distinct integers a, b, c, d in increasing order that minimizes the number of pairwise comparisons needed to sort any permutation of a, b, c, d.

   (b) The vertices of a triangle T are given. For an arbitrary point P in the plane, give an algorithm to test if P belongs to the interior of T. (The interior of T does not include its edges).

   (c) Let A be a sequence of n non-negative distinct integers in increasing order. Propose an efficient algorithm that reports s many closest integers of x in A. For example, if $A = \langle 03, 08, 11, 17, 18, 21, 25, 29, 33, 44, 47, 65, 71, 73, 89 \rangle$, $s = 5$, and $x = 33$, then the algorithm should return $21, 25, 29, 44, 47$. You will fetch full credit if your proposed algorithm runs in $O(s + \log n)$ time.

2. Suppose you are given n points on the curve $y = x^2 + 1$, sorted according to their X co-ordinate values.

(a) Report the maximum Y co-ordinate value.

(b) Write a *logarithm time* algorithm to report the point with the minimum Y co-ordinate value.

(c) Design a *linear-time* algorithm that sorts the n points according to their Y co-ordinate values.

3. Consider an array $A = [a_1, \ldots, a_n]$ of n integers.

(a) What is the minimum number of comparisons required to report an element that is not the i^{th} $(1 \leq i \leq n)$ minimum?

(b) Write an algorithm to find the maximum and the minimum element of the array simultaneously with approximately $3n/2$ many comparisons.

(c) Assume A contains integers in the range $1, \ldots, n^2$. A number i is called dominating in A if i occurs in A at least $n/2$ times. Give an efficient (linear) algorithm that finds all the dominating numbers in A. Justify the time complexity of your algorithm.

4. The Fibonacci sequence is a sequence in which each element is the sum of the two elements that precede it. The Fibonacci series is given by $0, 1, 1, 2, 3, 5, 8, 13, \ldots$. Given an integer n, the objective is to find F_n, the n-th fibonacci number in the above series. We consider $F_0 = 0$.

(a) Write down a simple recursive function Fib(n) to report the n-th Fibonacci number. What is the time-complexity of this algorithm?

(b) Prove that $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$, where F_n is the n-th fibonacci number.

(c) Given two integers x and n, write an efficient algorithm to compute x^n.

(d) Design an algorithm to find the n-th fibonacci number in $O(\log n)$ time? [Hint: You may use (b) and (c)]

5. Given an array A of length n, the counting inversion problem reports the number of pair of indexes (i, j) such that $i < j$ and $A[i] > A[j]$.

(a) Suppose you are given an array such that both $A[1 \ldots \lfloor n/2 \rfloor]$ and $A[\lceil n/2 \rceil \ldots n]$ are sorted in ascending order (similar as used in the example array). Can you count the number of inversions in such an array in $O(n)$ time?

(b) Use the above result to report all number of inversions in any array of n elements in $O(n \log n)$ time.

For simplicity, you may assume that all the elements in the given array are distinct.

Circuits and Systems

1. (a) Consider the multiplication of two 2-bit integers a_1a_0 and b_1b_0 to get a 4-bit output $c_3c_2c_1c_0$. Assuming that the right most bit is the least significant bit, derive Boolean functions for c_0 and c_3.

(b) Design a combinational logic circuit that takes an unsigned 2-bit integer as input and computes its square.

2. (a) You are given a logic block L that takes two inputs A and B, and produces $\overline{A} + B$ as output. Realize a two-input XOR gate using only the logic block L. You can use as many pieces of block L as you need, and the constant function 0; but no other type of gate.

(b) A binary sting $a_n a_{n-1} \dots a_0$ is called palindrome if $a_n a_{n-1} \dots a_0 = a_0 a_1 \dots a_n$. Design a combinatorial circuit over 4-bit inputs that outputs 1 if and only if the input is a palindrome.

3. (a) You are required to design a 4-bit prime number checker. Note that 0 and 1 are not prime. Design the circuit using a single 4×1 multiplexer and a minimal number of AND, OR or NOT gates.

   (b) Consider you have a number of comparator circuits. Design a digital circuit that takes n inputs, each of which is a 4 bit number and output the minimum number. You may use basic combinatorial gates in addition to the comparator circuit.

   (c) A Boolean function g is said to be the dual of another Boolean function f if g is obtained from f by interchanging the operations + and ., and the constants 0 and 1. A Boolean function f is self-dual if $f = g$. Given $f(a, b, c) = a\overline{b} + \overline{b}c + x$, find the Boolean expression x such that f is self-dual.

4. (a) Let $a_{n-1}a_{n-2} \dots a_0$ and $b_{n-1}b_{n-2} \dots b_0$ denote the two's complement representation of two integers A and B respectively. Addition of A and B yields a sum $S = s_{n-1}s_{n-2} \dots s_0$. The outgoing carry generated at the most significant bit position, if any, is ignored. Show that an overflow (incorrect addition result) will occur only if the following Boolean condition holds: $\overline{s}_{n-1} \oplus (a_{n-1}s_{n-1}) = b_{n-1}(s_{n-1} \oplus a_{n-1})$.

   (b) Design a digital circuit to compare two three bit numbers $A(A_2A_1A_0)$ and $B(B_2B_1B_0)$; the circuit should have three output terminals indicating $A = B$, $A < B$ and $A > B$. Draw the corresponding circuitry.

5. A choke coil connected across a 500 V, 50 Hz supply takes 1 A current at a power factor of 0.8.

   (a) Determine the capacitance that must be placed in series with the choke coil so that it resonates at 50 Hz.

   (b) An additional capacitor is now connected in parallel with the above combination in (a) to change the resonant frequency. Obtain an expression for the additional capacitance in terms of the new resonant frequency.

6. (a) An arc lamp requires a direct current of 10 A at 80 V to function. Prove that if it is connected to a 220 V (rms), 50 Hz AC supply, the series inductor needed for it to work is close to 0.065 H.

   (b) A parallel plate capacitor is charged to 75 μC at 100 V. After removing the 100 V source, the capacitor is immediately connected to an uncharged capacitor with capacitance twice that of the first one. Determine the energy of the system before and after the connection is made. Assume that all capacitors are ideal.

Formal Language and Automata Theory

1. (a) Let $\mathcal{L}$ be a regular language. Then prove that $\mathcal{L}_1 = \{w \in \mathcal{L} : \text{ no proper prefix of } w \in \mathcal{L}\}$ is regular. (Note: A proper prefix of a string w is a string x such that $w = xy$ for some non-empty string y)

   (b) Prove that the language $\mathcal{L} = \{w : w = x_1\|\#\|x_2\|\#\| \dots \|x_k : k \geq 1, x_i \in \{a, b\}^*, x_i \neq x_j\}$ is non-regular. (You may use Pumping Lemma).

   (c) Given two DFA M_1 and M_2, how do you determine whether $\mathcal{L}(M_1) \subseteq \mathcal{L}(M_2)$?

2. (a) Prove that the language $\mathcal{L} = \{a^{pq} : p, q \text{ are primes } \}$ is not context free language.

   (b) Show that $\mathcal{L} = \{a^n b^n : n \text{ is not a multiple of } 5\}$ is context free.

(c) If L_1 is a context free language and L_2 is an infinite regular language, then how do you determine whether $L_1 \cap L_2 = \phi$ or not.

3. (a) Justify whether the following languages are context-free or not:

   i. $\mathcal{L}_1 = \{a^n b^n c^m d^m \ : \ n \geq 1, m \geq 1\}$,

   ii. $\mathcal{L}_2 = \{a^n b^m c^n d^m \ : \ n \geq 1, m \geq 1\}$.

   (b) Let $\mathsf{trans}(\mathcal{L}) = \{zyx \mid x, y, z \in \Sigma^\star, \ xyz \in \mathcal{L}\}$. Suppose $\mathcal{L}$ is a context-free language. Show that $\mathsf{trans}(\mathcal{L})$ is **not** a context-free language. [Hint: Can you use the previous result?]

C. Quantum Computation and Quantum Information

1. (a) Consider that one has to design a unitary operation U that transforms

$$|0\rangle \to |\psi\rangle\,, \quad |1\rangle \to \left|\psi^{\perp}\right\rangle, \quad |+\rangle \to |\phi\rangle\,, \quad |-\rangle \to \left|\phi^{\perp}\right\rangle,$$

where $|\psi\rangle\,, |\phi\rangle$ can be chosen independently. Is it possible to design such an U? Then provide a concrete example. Else, what would be the relationship between $|\psi\rangle$ and $|\phi\rangle$?

(b) Assuming an universal cloning machine exists in quantum paradigm, explain how the security of BB84 protocol would have been compromised under this scenario.

2. Consider a three variable Boolean function $f(x_1, x_2, x_3) = x_3 \oplus x_1x_2$.

(a) Is it constant or balanced? Explain.

(b) How this function can be plugged in Deutsch-Jozsa algorithm as a quantum gate?

(c) Prove that the all zero state can not be observed as an outcome of the Deutsch-Jozsa algorithm for this function.

3. (a) Consider the following qubits:

$$\frac{\sqrt{7}}{2\sqrt{3}}\,|0\rangle - \frac{2+i}{2\sqrt{3}}\,|1\rangle\,, \qquad \frac{(1+i)}{2}\,|0\rangle + \frac{1-i}{2}\,|1\rangle\,.$$

Measure the states in the $\{|+\rangle, |-\rangle\}$ basis, and calculate the probabilities to obtain $|+\rangle$ and $|-\rangle$.

(b) Describe the unitary matrix that is equivalent to consecutive applications of Pauli-X and Pauli-Z gates.

(c) Consider the following operations:

$$|01\rangle \to H^{\otimes 2} \to CNOT \to H^{\otimes 2} \to |\psi\rangle\,.$$

Show the step-by-step calculations to obtain $|\psi\rangle$.

(d) Justify whether the following 2-qubit state is entangled:

$$|\psi\rangle = \frac{i}{\sqrt{30}}\,|00\rangle - \sqrt{\frac{2}{15}}\,|01\rangle - \frac{1-3i}{2\sqrt{15}}\,|10\rangle - \frac{3+i}{\sqrt{15}}\,|11\rangle\,.$$

4. (a) Let $|x_0\rangle$ be the marked element in the initial state of Grover's algorithm as follows:

$$|\psi\rangle = \frac{1}{2\sqrt{2}}\,|x_0\rangle + \frac{\sqrt{7}}{2\sqrt{2}} \sum_{x \neq x_0} |x\rangle\,.$$

How many Grover iterations are required to obtain $|x_0\rangle$ having a probability greater than $\frac{1}{2}$?

(b) Show that $H^{\otimes n}(2\,|0^{\otimes n}\rangle\,\langle 0^{\otimes n}| - I)H^{\otimes n} = 2\,|\psi\rangle\,\langle\psi| - I$, where $|\psi\rangle$ is the equal superposition of all possible n-bit states and I is the identity matrix.