INDIAN STATISTICAL INSTITUTE

Semestral Examination: 2019

Date: 18-11-2019

Subject Name : **Discrete Mathematics**

Course Name : M.Tech. (CrS) I yr. Max Score: 100 Duration: 3 hours

Note: Attempt all questions. Marks are given in brackets. Total score is 130. But the maximum you can score is 100.

1. (a) Let G be a simple graph on n vertices having more than $\frac{n(k-1)}{2}$ edges. Prove that G has a path of length k.

   (b) Let $G = (V, E)$ be a triangle-free simple graph with maximum number of edges. Let $I \subseteq V$ be a maximum-sized independent set of G. Prove that $V \setminus I$ is also an independent set of G.

   $(13 + 7 = 20)$

2. (a) Show that a simple graph on 6 vertices together with its complement contains at least two triangles.

   (b) Let M be a matrix with non-negative entries such that each row and column sum of M is $r > 0$. Show that M can be written as $A = \sum_i r_i P_i$, where P_i are the permutation matrices, and $r_i > 0$ are such that $\sum_i r_i = r$.

   $(8 + 12 = 20)$

3. (a) Let T be a tree with k edges, and G be a simple graph with minimum degree k. Then prove that T is a subgraph of G.

   (b) Let G be a simple graph and $\bar{G}$ be its complement. Prove that if radius of G is at least 3 then radius of $\bar{G}$ is at most 2.

   (c) Prove that a digraph is strongly connected iff for each partition of its vertex set into nonempty sets S and T, there is an edges from S to T.

   (d) Prove that a directed odd cycle is a digraph with no kernel.

   $(7 + 5 + 5 + 3 = 20)$

4. (a) Prove that every tournament has a king vertex (i.e., a vertex from which distance of every other vertex is at most 2). Draw a tournament on 4 vertices that does not have a Hamiltonian cycle (no explanation is needed).

(b) Let $G = (V, E)$ be a simple graph without isolated vertices. Let $D \subset V$ be a minimal dominating set in G. Then show that $V \setminus D$ is also a dominating set.

(c) Given a simple graph G let $\alpha'(G)$ and $\beta(G)$ denote maximum size of a matching and minimum size of a vertex cover in G. We know that $\alpha'(G) = \beta(G)$ if G is bipartite. Now, construct

(i) a simple non-bipartite graph where the above equality holds, and

(ii) a simple graph where the above equality does not hold.

In both the cases the graphs must contain at least one edge. Also, clearly indicate the values of $\alpha'(G)$ and $\beta(G)$ in both the cases (possibly with necessary justification).

$((7 + 3) + 4 + (3 + 3) = 20)$

5. (a) Let $s(m, n)$ be the number of non-negative integer solutions to the following set of equations.

$$x_1 + 2x_3 + 4x_4 = m$$
$$2x_1 + 5x_3 + 7x_4 = n.$$

Find the generating function for the sequence $(s(m, n))_{m \geq 0, n \geq 0}$.

(b) Given a positive integer n, let $d(n)$ denote the number of partitions of n such that each part in a partition is distinct, and $o(n)$ denotes the number of partitions of n such that each part in a partition is odd. Find the generating functions for the sequences $(d(n))_{n \geq 0}$ and $(o(n))_{n \geq 0}$ (with the assumption $d(0) = o(0) = 1$). Hence, or otherwise, show that $d(n) = o(n)$ for $n \geq 0$.

(c) Let a_n be the number of sequences of length n formed by the letters $\{X, Y, Z\}$ such that no X is followed by a Y, and no Y is followed by an X. Then (assuming $a_0 = 1$)

(i) justify the recurrence $a_n = 2a_{n-1} + a_{n-2}, n \geq 2$, and

(ii) solve for a_n.

$(2 + (3 + 2 + 3) + (4 + 6) = 20)$

6. (a) Give an example of a set of 4 well-formed formulas (wffs) such that any subset of 3 wffs is satisfiable but the entire set (of 4 wffs) is unsatisfiable.

(b) Show that any wff is tautologically equivalent to a wff that uses only $\neg, \rightarrow$ as connectives.

(c) Give an example of a wff that is not tautologically equivalent to any wff that uses only $\rightarrow$ and $\wedge$ as connectives. Justify your answer.

$(4 + 5 + (1 + 5) = 15)$

7. Let a deduction system for propositional logic be defined by the following set of axiom schemas:

(a) $(\Phi \rightarrow (\Theta \rightarrow \Phi))$,

(b) $((\Phi \rightarrow (\Theta \rightarrow \Psi)) \rightarrow ((\Phi \rightarrow \Theta) \rightarrow (\Phi \rightarrow \Psi)))$,

(c) $((\neg\Theta \rightarrow \neg\Psi) \rightarrow (\Psi \rightarrow \Theta))$,

and the rule of inference be *modus ponens* (*i.e.*, from Ψ and $\Psi \rightarrow \Theta$ we infer Θ). Then show the following using the *Deduction theorem* or otherwise.

(a) $((\neg(\neg\psi)) \rightarrow \psi)$ is a theorem.

(b) Assume that for any set of wffs Σ it is true that if Σ is consistent then there exists a truth assignment v such that $v(\alpha) = T$ for all $a \in \Sigma$. Also, assume that $(((\neg\phi) \rightarrow \psi) \rightarrow (((\neg\phi) \rightarrow (\neg\psi)) \rightarrow \phi))$ is a theorem. Then show that for a set of wffs Γ and a wff θ, if $\Gamma \models \theta$ then $\Gamma \vdash \theta$.

$(7 + 8 = 15)$

INDIAN STATISTICAL INSTITUTE
M. Tech. (CrS) - I year: 2019–2020
Computing Systems I
Semestral Examination

Date: 20. 11. 2019 Marks: 100 Time: 3 Hours

Answer any five questions.

1. (a) Write down the truth table of a 4-input 1-output Boolean function that cannot be implemented with only 2-input 1-output XOR gates.
   (b) Simplify the Boolean function $f(x, y, z) = \sum(0, 2, 3, 4, 6)$ using Karnaugh map.
   (c) Prove that all n-input m-output Boolean functions can be implemented with two input NOR gates only.
   (d) Design an adder/subtracter circuit which will accept two 4-bit integers and provide the necessary output. Explain with a specific example how the idea of 2's-complement representation is efficiently used in this circuit.

   $4 + 4 + 5 + (4 + 3) = 20$

2. (a) Write down a C program to accept an unsigned integer and then to output the product of its four individual bytes.
   (b) Write down a C program to accept an unsigned integer and then to print the address of its four individual bytes.
   (c) Write down a C program that can catch the signal "ctrl+c".
   (d) Consider that in your directory structure there are several directories and files in the form of a tree. How to write a unix shell script to obtain the list of all the files whose names contain the substring "abcd".
   (e) Explain briefly the application of the unix shell commands "awk" and "grep".

   $5 + 3 + 4 + 4 + (2 + 2) = 20$

3. Consider a 5-bit counter that can count cyclically all the 5-bit integers divisible by 3 in an increasing order (from 00000 to 11110 and then again from 00000) corresponding to every clock pulse.
   (a) Describe each step of your design to implement the counter.
   (b) Draw the complete circuit with Flip-Flops and two-input combinational logic gates of your choice. Credits will be given for implementation with less number of two-input combinational gates.

   $12 + 8 = 20$

PTO

4. (a) What are the important steps in executing an instruction in CPU involving the registers and random access memory?

   (b) Explain the idea of wire and bus in the context of computer organization.

   (c) Explain interleaving of memory with a proper example.

   (d) What is Direct Memory Access and how Bus Arbitrator is related in this context?

   $5 + 5 + 5 + 5 = 20$

5. (a) "In the context of cache memory, write-back is convenient for Single CPU scenario." Do you agree? Briefly comment on this.

   (b) Consider a Fully Associative Cache with 2^8 slots. Each slot contains 2^4 bytes. Considering 32-bit address, identify the bits that will be used for tag. What is the total size of this cache memory?

   (c) Consider an implementation of Set Associative Cache. There are 256 slots, 64 bytes per slot and there are 16 slots per set. Given the address A_{31-0}, how one can locate a specific slot in cache memory, when it is required by the cache?

   $6 + (6 + 2) + 6 = 20$

6. (a) Clearly explain the differences between process and thread.

   (b) Write down snippets of C codes in Unix environment for both cases to identify how the procedure of memory access differs in these two scenarios.

   $8 + (6 + 6) = 20$

7. (a) Explain the idea of Deadlock in the context of operating system.

   (b) How one can relate the processes and resources with a directed graph to identify a deadlock situation?

   (c) Explain the Banker's algorithm in this context with a suitable example.

   $4 + 6 + 10 = 20$

8. With the reference to the Dining Philosophers' problem and with snippets of C codes in Unix environment, explain the ideas of

   (a) creating processes,

   (b) using shared memory, and

   (c) implementing semaphores.

   $4 + 8 + 8 = 20$

INDIAN STATISTICAL INSTITUTE

Semestral Examination: 2019

Subject Name : **Algebra and Number Theory**

Course Name : M.Tech. (CrS) I yr. Max Score: 80 Duration: 3 Hrs

Note: Attempt all questions. Marks are given on the right margin. Total score is 94. Maximum you can score is 80. Use separate Answer Booklets for Section A and Section B. Use of calculator is allowed for Section B.

Section A (Total marks - 50)

1. Prove that the order of 5 in $\mathbb{Z}_{2^e}^*$ is 2^{e-2}, $e \geq 2$. Hence show that $\mathbb{Z}_{2^e}^*$, $e \geq 2$, is not cyclic.

8

2. (a) Prove that in a principal ideal domain an element is prime if and only if it is irreducible.

   (b) Show that the ideal $(13, X)$ is maximal in $\mathbb{Z}[X]$.

$6 + 4 = 10$

3. (a) Let K be a field. Show that a polynomial of degree 3 is irreducible in $K[X]$ if and only if it does not have any root in K.
   Find all irreducible polynomials of degree 3 in $\mathbb{F}_2[X]$.

   (b) Prove that for a polynomial $f(X) \in \mathbb{F}_q[X]$, $\mathbb{F}_q$ a finite field, $(f(X))^q = f(X^q)$.

$(3 + 3) + 4 = 10$

4. (a) List the elements of $\mathbb{F}$, which is the extension field obtained by adjoining a root α of $X^4 + X + 1$ to $\mathbb{F}_2$. What are the multiplicative orders of the elements of $\mathbb{F} \setminus \{0\}$?

   (b) Let α be a primitive element of $\mathbb{F}_{q^n}$ with respect to the finite field $\mathbb{F}_q$.
   Show that for $x = \alpha^s \in \mathbb{F}_{q^n}$, $x^{q^r} = x \iff sq^r \equiv s \mod (q^n - 1)$.
   Compute the 2-cyclotomic cosets modulo 23.

$6 + (3 + 3) = 12$

5. (a) Find a minimal set of vectors that span $\mathbb{C}^3$ over $\mathbb{R}$.

   (b) Let S, T be complementary subspaces of a vector space V. Construct, with justification, a basis of the quotient space V/S from a basis $\{\mathbf{x}_1, \cdots, \mathbf{x}_k\}$ of T.

   (c) Let $f(\mathbf{x}_1, \mathbf{x}_2) = (2\mathbf{x}_1 + 3\mathbf{x}_2, \mathbf{x}_1 - \mathbf{x}_2)$, $g(\mathbf{x}_1, \mathbf{x}_2) = (\mathbf{x}_1, 2\mathbf{x}_1 - 5\mathbf{x}_2)$ be linear operators on $\mathbb{R}^2$. Find the matrix of $f \circ g$ with respect to the canonical basis of $\mathbb{R}^2$.

$2 + 4 + 4 = 10$

P.T.O.

Section B (Total marks - 44)

1. (a) Calculate $|(\mathbb{Z}_n^*)^2|$, $n \in \mathbb{N}$ with explanation.

   (b) Show that if p is an odd prime with $p \equiv 3(\text{mod } 4)$, then $(\mathbb{Z}_p^*)^4 = (\mathbb{Z}_p^*)^2$.

$(3 + 3 = 6)$

2. Use Hensel's Lemma and Chinese remainder theorem to solve the following congruence : $3X^2 - 8X + 4 \equiv 0(\text{mod } 72)$.

(8)

3. (a) By mentioning the result, write the algorithm for the Solovay-Strassen Primality test. What is the failure probability of this test? Explain.

   (b) State and prove the required result and hence write down the algorithm for the Miller-Rabin Primality test.

$(5 + 5 = 10)$

4. (a) Evaluate : $(\frac{1101}{9907})$.

   (b) Does the equation : $X^2 + 2X + 17 \equiv 0(\text{mod } 35)$ have a solution? If yes find the smallest solution $X \geq 0$.

$(3 + 4 = 7)$

5. (a) Prove that for every integer $n > 15$, between n and $2n$ there exists at least one number which is a product of three different primes.

   (b) Describe RSA-cryptography with $n = pq$, $p = 11$, $q = 13$. What is the value of the smallest encoding exponent e ? Taking e to be equal to this value, compute a decoding exponent d. If you want to send the number 29, what will be your encoded message? Suggest ways to make RSA-encryption faster.

$(5 + 8 = 13)$

INDIAN STATISTICAL INSTITUTE

Semestral Examination : Semester I (2019-20)

M. Tech (CrS) I Year

Probability and Statistics

Date: 27.11.2019 Maximum marks: 100 Time: 3 hours

The total mark is 102. Maximum one can score is 100. This test is open notes. Books cannot be used and notes cannot be exchanged. Refer to your notes properly, but do not reproduce derivations from there. Answer Group A and Group B in separate answer-scripts. Simple calculator may be used.

Group A

1. Let X be a random variable following standard normal distribution and Y be another random variable following Chi-square distribution with 1 d.f. Let $P(X < 1)$ be a. Then what is $P(Y < 1)$ in terms of a? [5]

2. There are six similar looking balls of which five have the same weight while the other one is heavier. You are given an ordinary balance with two sides. Here is a method to detect the heavier ball. Draw two balls randomly from the six and compare their weights in the balance. If one side is heavier, the ball is detected. Else draw another two balls randomly from the remaining and follow the same procedure. It is evident that maximum number of weighing is 3. Find out the expected number of weighing. [10]

3. Show that $\bar{X}$ and S^2 based on three independent and identically distributed observations from $\mathcal{N}(0,1)$ are independent. [10]

4. Perform frequency test, block test, autocorrelation test and runs test on the following binary sequence and conclude whether it is pseudo random or not.

   00000 11111 10101 01010 00111 11000 00001 10000 11110 01111 01110 10001 [15]

5. Consider a Markov chain with 3 states. Find a transition probability matrix so that in the steady state all the states are equally likely. [10]

Group B

1. Consider the following data on annual income (in lakhs of Rupees) from 32 individuals.

   1.54, 1.49, 2.31, 6.06, 5.84, 1.96, 1.32, 1.78, 3.48, 24.52, 2.56, 8.72, 4.44, 9.16, 8.04, 1.84, 3.24, 4.16, 5.08, 12.12, 2.20, 20.36, 1.88, 3.20, 28.04, 2.22, 3.92, 4.56, 5.36, 8.66, 14.12, 16.90

   (a) Draw a box-plot of the data (a reasonably rough figure will do) giving full details.

(b) Assume exponential distribution for the above income data.

i. Give an asymptotic 95% confidence interval for the mean annual income.

ii. Obtain maximum likelihood estimates of the third quartile of the income distribution and also the probability that the annual income of a randomly selected individual is greater than Rupees 10 lakhs.

(c) Carry out a non-parametric procedure to test that the median annual income is Rupees 10 lakhs against the two-sided alternative. Use approximation for large sample size.

[12+(8+4)+8=32]

2. It is suspected that sugar level increases after having food. We have sugar level data from 30 individuals measured before lunch and again one hour after lunch. All the 30 individuals are given the same lunch. Assuming normality for the measurements, describe a suitable procedure for testing no effect of lunch on the sugar level against a suitable alternative. [10]

3. We have two groups of 10+2 board examinees, one taking professional tuition and the other not taking any such professional tuition, with size n_1 and n_2, respectively. The number of students achieving first division and above in the board examination in the two groups are f_1 and f_2, respectively. Describe a suitable approximate test for no effect of professional tuition on the 10+2 board result against a suitable alternative.

[10]

Indian Statistical Institute

First Semester Examination 2019
M.Tech.(CrS) Program

Automata Theory, Languages, and Computation
Maximum Marks 50

Date: 22 November, 2019, Duration: 3 hours
[Closed book exam, 4 problems carry total 60 marks]
only precise and to the point answer will get full mark(s)

1. (13 marks)

Let $L = \{ss^{RC} \mid s \in \{0,1\}^*\}$ be a language over alphabet $\{0,1\}$, where s^{RC} describes the **reverse complement** of a string $s \in \{0,1\}^*$, obtained by reversing the order of symbols in s and then exchanging every 0 in s with 1 and every 1 in s with 0. As for example, if $s = 1101$, the reverse order of s is 1011 and the reverse complement s^{RC} is 0100.

(a) State whether there is a string in L with an unequal number of zeros and ones. [2]

(b) Prove that L is a context-free language, but not a regular language. [5+6]

2. (17 marks)

(a) State **three** differences between deterministic and non-deterministic Turing machines. [3]

(b) Prove that the class of decidable languages is closed under complementation. [6]

(c) Let $L = \{\langle R \rangle \mid R$ is a regular expression describing a language containing at least one string w that has 00 as a substring$\}$. Show that L is a decidable language. [8]

3. (11 marks)

(a) If $A \leq_m B$ and B is a regular language, does that imply that A is a regular language? Explain your answer. [3]

(b) Prove that $H_{TM} = \{\langle M, w \rangle \mid M$ is a Turing machine and M halts on input $w\}$ is undecidable. [8]

4. (19 marks)

(a) Prove or disprove the following claims. [3 + 3]

(i) $3^{2n} \in O(2^{3n})$.

(ii) Let L_1 and L_2 be two languages in NP, and assume $P \neq NP$. If $L_1 \leq_P L_2$ and $L_2 \leq_P L_1$, then both L_1 and L_2 are NP-complete.

(b) Let $CNF_H = \{\langle \phi \rangle \mid \phi$ is a satisfiable cnf-formula where each clause contains any number of literals, but at most one negated literal$\}$. Show that $CNF_H \in P$. [5]

(c) Prove that 3-Coloring problem is NP-complete. [8]

— END of the Question Paper —

INDIAN STATISTICAL INSTITUTE

Semestral Examination

M.Tech(CrS)-I Year, 2019-2020 (Semester-I)

Programming and Data Structures

Date: **November 25th, 2019** Maximum Marks: **100** Duration: **3 Hours**

Note: The question paper carries a total of 120 marks. You can answer as much as you can, but the maximum you can score is 100.

---

1. (a) Suppose you are given the inorder and preorder traversal sequences of a binary tree in two arrays A and B. Devise an efficient algorithm to construct the tree from these inorder and preorder traversal sequences.

   (b) Prove that given an open-address hash table with load factor $\alpha < 1$, the expected number of probes in a successful search is at most

   $$\frac{1}{\alpha} ln \frac{1}{1-\alpha} + \frac{1}{\alpha},$$

   assuming uniform hashing and assuming that each key in the table is equally likely to be searched for.

   (15+15=30)

2. (a) An $n \times n$ matrix A is called a $NICE$ matrix, if each row and each column of A has exactly one non-zero element equal to 1. Write a C-program to store a $NICE$ matrix in an $O(n)$ size array.

   (b) Write a bash script program to print the first 10 elements of the Fibonacci series.

   (15+10=20)

3. (a) Suppose you are given two arrays A and B containing $m \geq 1$ and $n \geq 1$ elements respectively. The elements in the arrays A and B are sorted in ascending order. Write an efficient algorithm to merge these two arrays with O(1) extra space so that the elements in the merged array are also sorted in ascending order.

   (b) Given a dictionary and two words **start** and **target** (both of the same length), write an algorithm to find the length of the smallest chain from **start** to **target** if it exists, such that adjacent words in the chain only differ by one character and each word in the chain is a valid word i.e., it exists in the dictionary. It may be assumed that the target word exists in the dictionary and the lengths of all the dictionary words are equal.

   (15+10=25)

4. (a) Write an algorithm using stack to convert an infix expression to the corresponding postfix expression.

   (b) Explain with an example a use case of makefiles.

   (15+10=25)

5. What will be the output of the following codes? Justify your answer.

(a)
```
#include<stdio.h>
int main()
{
    int n,m=10;
    n= -m--;
    printf("n= %d,m= %d",n,m);
    return    0;
}
```

(b)
```
#include <stdio.h>
int main()
{
  static int var = 5;
  printf("%d",var--);
  if(var)
  main();
}
```

(c)
```
#include <stdio.h>
#define  square(x)  x*x
void main()
{
  int i;
  i = 64/square(4);
  printf("%d",i);
}
```

(d)
```
#include <stdio.h>
void main()
{
  int const  p=5;
  printf("%d",++(p));
}
```

(4x5=20)