Discrete Structures (MA5.101)

End Semester Examination (Monsoon 2022)

International Institute of Information Technology, Hyderabad

Time: 180 Minutes (3 Hours) Total Marks: 180

Instructions: Answer *ALL* questions.

This is a closed books and notes examination.

Write your answers sequentially as given in the question paper and also all the parts of a question at the same place.

No query is allowed during the examination.

Use of Regular Calculator is allowed.

1. Consider the language of propositional logic (without equality). Consider the ordering $\prec$ between propositional formulas. $A \prec B$ iff formula A is an immediate subformula of formula B.

   Apply the principle of induction over the set of propositional formulas ordered according to $\prec$ to show that the valuation of a formula depends only on the assignment of propositional variables occurring in that formula.

   [20]

2. (a) Define precisely what is a partial order.

   (b) Identify which of the following are not partial orders and justify why they not.

   i. The set A along with an arbitrary equivalence relation R.

   ii. The set students in IIIT along with the binary relation sRt iff the height of of student s is not greater than the height of student t.

   iii. The set P (positive integers) along with the binary relation mRn if m and n are co-prime. (Two numbers are coprime if the only number dividing both of them is 1.)

   [10 + 10 = 20]

3. Prove that in an undirected graph (self-loops allowed), the number of vertices whose degree is odd is even.

   [20]

4. Let H and K be two product subgroups of a group $\langle G, \cdot \rangle$. The product set of H and K, denoted by $H \cdot K$, is the set of all products of the form $h \cdot k$, for $h \in H$ and $k \in K$. Under what condition the product set $H \cdot K$ is a normal subgroup of G? Justify your answer.

   [20]

5. Let $f : G \to G'$ be a group epimorphism, and let H be the normal subgroup that is the *kernal* of the epimorphism. Prove that G' is isomorphic to G/H, where $\langle G/H, \circ \rangle$ is a quotient group.

   [20]

6. A non-empty subset S of a ring $(R, +, .)$ will form a sub-ring of R, if and only if, for any two elements x and y of S,

$$x - y \in S \text{ and } x.y \in S, \forall x, y \in S.$$

The center of a ring R is defines to be

$$\{a \in R | ax = xa, \forall x \in R\}.$$

Show that the center of the ring R is a sub-ring of R.

[10]

7. (a) Compute the product of two byes $\{d3\}.\{8f\}$ in the finite (Galois) field $GF(2^8)$ with respect to an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.

(b) Under what condition can you compute the multiplicative inverse of a polynomial $b(x)$ modulo a polynomial $m(x)$ in $GF(2^8)$? Explain the algorithm for computing $b(x)^{-1} \pmod{m(x)}$.

[15 + 15 = 30]

8. (a) With respect to the research paper discussed on the hierarchical access control as an application of partial order relation: **Y. F. Chung, H. H. Lee, F. Lai and T. S. Chen, "Access control in user hierarchy based on elliptic curve cryptosystem", Information Sciences (Elsevier), vol. 178, no. 1, pp. 230-243, 2008**, discuss about the key derivation phase where a legal predecessor security class can derive the secret key of its successor security class(s).

(b) Define syndrome of an n-tuple x with reference of an $r \times n$ parity-check matrix H. Prove that two n-tuples are in the same coset if and only if they have the same syndrome.

[10 + 10 = 20]

9. (a) Define even and odd permutations. Examine whether the following permutation:

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

is odd or even.

(b) Given a set of sixteen natural numbers, none having a prime factor > 7, show that either some number is a perfect square or, the product of some two distinct numbers is a perfect square.

[Use the fundamental theorem of arithmetic and the canonical representation of a number $n > 1$].

[10 + 10 = 20]

********** **End of Question Paper** **********