Discrete Mathematics, CSE 121 : Mid-Semester Exam, Monsoon 2022

General Instructions:

(a) Maximum marks = 25; Duration: 2 hours.

(b) This is a closed-book exam. The exam paper is self-contained. Any attempt to use any source during the exam will be dealt with according to the Academic Dishonesty Policy of the institute.

(c) In every proof/derivation clearly state your assumptions and give details of each step.

(d) You will be evaluated for your attempt and approach. Therefore, you are encouraged to attempt the questions even if you can not complete an answer. The Academic Dishonesty Policy of the institute is equally applicable even for partial answers.

Questions:

1. What are the sets in the partition of the integers arising from congruence modulo 4? [1 mark]

   Solution. Both fine: either $[0]_4, [1]_4, [2]_4, [3]_4$ or $\{4k\}, \{4k+1\}, \{4k+2\}, \{4k+3\}$.

   (If $[0], [1], [2], [3]$ are written without subscripts $[]_4$ or without mentioning that these are congruent modulo 4, deduce 0.5 marks) ■

2. There are two quotes written on a wall: (a) Good grades are not easy, and (b) Easy grades are not good. Prove or disprove the equivalence of the two. [3 marks]

   Solution. Take the propositions as G: "Grades are good" and E: Grades are easy. Show that the propositions $G \implies \neg E$ and $E \implies \neg G$ are equivalent. One can use truth table for this for various combinations of truth values of G and E.

   (One must be careful with other proof methods such as contrapositive. I had a look at a couple of such solutions who used contrapositive; they were incorrect.) ■

3. If f and $f \circ g$ are one-to-one, show that g is one-to-one. [3 marks]

   Solution. (Unless someone has been too innovative, the proof is by contradiction and uses contrapositive. If the use of contrapositive is not indicated, deduce 1 mark)

   Suppose g is not one-to-one. Let $g : A \to B$ and $f : B \to C$.

   By assumption, since g is not one-to-one, there exist 2 distinct elements $x_1, x_2 \in A$ such that $g(x_1) = g(x_2) = y$ where $y \in B$. Let $f(y) = z$ for some $z \in C$.

Thus, $f \circ g(x_1) = f \circ g(x_2) = z$. Hence $f \circ g$ cannot be one-to-one.

Take P as the proposition that "f and $f \circ g$ are one-to-one" and Q as the proposition that "g is one-to-one". Using contrapositive, $\neg Q \implies \neg P \equiv P \implies Q$. ■

4. Define a relation R on the set of positive integers by $(x, y) \in R$ if the greatest common devisor of x and y is 1. Determine whether R is reflexive, symmetric, antisymmetric, transitive, and partial order. [4 marks]

   Solution. It is not reflexive, as for every positive integer $z \in Z^+$, $gcd(z, z) = z \neq 1$. It is symmetric because $gcd(a, b) = gcd(b, a)$, so $gcd(a, b) = 1$ iff $gcd(b, a) = 1$ for every $a, b \in Z^+$. Not antisymmetric — proving by a counterexample, $gcd(5, 7) = 1$ and $gcd(7, 5) = 1$, i.e. $(5, 7) \in R$ and $(7, 5) \in R$, however, $gcd(5, 5) = 5$, i.e. $(5, 5) \notin R$. Not transitive — proving by counterexample, $gcd(5, 7) = 1$, and $gcd(7, 10) = 1$, but $gcd(5, 10) = 5$, i.e. $(5, 7) \in R$ and $(7, 10) \in R$, however, $(5, 10) \notin R$. Because not transitive, it is not a partial order.

   (50% marks for proving each of the determinations i.e. is/isn't reflexive, etc.) ■

5. Prove that given a non-negative integer n, there is a unique non-negative integer m such that $m^2 \leq n < (m + 1)^2$. [4 marks]

   Solution. First prove that there exists a unique non-negative integer m such that $m \leq \sqrt{n} < (m + 1)$ for every non-negative integer n. This proof could be by cases: (a) $\sqrt{n} \in Z^+$ (b) $\sqrt{n} \in Q^+$. It could also potentially be done by contradiction and contrapositive.

   From here deduce the original proposition as using algebraic manipulation, etc.

   (For first part 3 marks, for deduction 1 mark. I have seen a couple of attempts to prove it by mathematical induction which were wrong.) ■

6. Let λ denote the empty string. Let A be any finite non-empty set. A palindrome over A can be defined as a string that reads the same forward and backward. For example, "mom" and "dad" are palindromes over the set of English alphabets. We define a set S as follows: (a) $\lambda \in S$, (b) $\forall a \in A,\ a \in S$, (c) $\forall a \in A \text{ and } x \in S,\ axa \in S$, and (d) all the elements in S must be generated by the rules (a), (b), and (c). Using structural induction show that S is the set of all palindromes over A. [5 marks]

   Solution. Given A is a finite non-empty set.

   (The elements of A, denoted $a \in A$, could be anything. We treat them as individuals similar to characters in English alphabet. For example, in the set $A = \{2, 20, Man\}$, the elements are essentially similar to those in the set $A' = \{a, b, c\}$. Thus, a palindrome over A could be $20Man20$.)

   Let A^P denote the set of all palindromes over A, including the empty string $\lambda \in A^P$. Consider the proposition $P(s) : (s \in S \iff s \in A^P)$.

- Basis step: By the definitions of S and palindrome, $\lambda \in S$ and it is a palindrome. Thus, $P(\lambda)$ is true.
- Inductive step: We assume that $P(a)$ is true for $a \in A^P$. Because a is a palindrome, axa is a palindrome for every $x \in S$. Thus we have shown that $P(axa)$ is true for $a \in A^P$ and $x \in S$, i.e. the set constructed by the recursive definition of S is the set of all palindromes over A. ■

7. Prove the generalization of one of De Morgan's laws: [5 marks]

$$\overline{\cup_{1\leq i\leq n} A_i} = \cap_{1\leq i\leq n}\bar{A}_i$$

Solution. Consider the proposition $P(n) : \overline{\cup_{1\leq i\leq n} A_i} = \cap_{1\leq i\leq n}\bar{A}_i$.

- Basis step: The case for $n = 1$ is vacuously true. Take $n = 2$ and prove the standard De Morgan's law for two sets. (One can do that by using the method $\overline{A_1 \cup A_2} \subseteq \bar{A}_1 \cap \bar{A}_2$ and $\overline{A_1 \cup A_2} \supseteq \bar{A}_1 \cap \bar{A}_2$ or even by Venn diagram for this.) Thereby $P(b)$ is true.
- Inductive step: Apply mathematical induction here.
  Assume that $P(k)$ is true i.e. $\overline{\cup_{1\leq i\leq k} A_i} = \cap_{1\leq i\leq k}\bar{A}_i$.
  With that,

$$\begin{aligned}
\cup_{1\leq i\leq k+1} A_i &= \overline{\cup_{1\leq i\leq k} A_i \cup A_{k+1}} && (algebra) \\
&= \overline{\cup_{1\leq i\leq k} A_i} \cap \overline{A_{k+1}} && (using\ the\ Basis\ step\ P(2)\ is\ true) \\
&= \cap_{1\leq i\leq k}\bar{A}_i \cap \overline{A_{k+1}} && (using\ the\ assumption\ P(k)\ is\ true) \\
&= \overline{\cap_{1\leq i\leq k+1} A_i} && (algebra)
\end{aligned}$$

(50% marks for proving the base case, deduct that if base case has not been proved) ■