National University of Computer & Emerging Sciences, Karachi
Summer - 2021 CS-Department

Mid Exam

11th August, 2021 11:30pm-2pm

Course Code: CS211	Course Name: Discrete Structures
Instructor Name: Mubashra Fayyaz	
Student Roll No:	Section:

Instructions:

- Return the question paper.
- Return the question paper with the answer sheet.
- Read each question completely before answering it.
- Make sure both sides of the paper are printed.
- In case of any ambiguity, you may make assumptions. But your assumption should not contradict any statement in the question paper.

Time: 90 min. Max Marks: 80(weight-age: 30)

Question # 01: [5x3=15 points]

A. Let Q(x, y) be the statement "student x has been a contestant on quiz show y." Express each of these sentences in terms of Q(x, y), quantifiers, and logical connectives, where the domain for x consists of students and the domain for y consists of quiz shows.

a. There is a student who has been a contestant on a quiz show.

$\exists x \; \exists y \; Q(x, y)$

b. No student has ever been a contestant on a quiz show.

$\neg \exists x \; \exists y \; Q(x, y)$

B. Show that these compound propositions are tautologies.

a) $(\neg q \land (p \rightarrow q)) \rightarrow \neg p$

$$(\neg q \land (p \rightarrow q)) \rightarrow \neg p$$

$$\equiv (\neg q \land (\neg p \lor q)) \rightarrow \neg p$$

$$\equiv \neg((\neg q \land (\neg p \lor q))) \lor \neg p$$

$$\equiv ((\neg(\neg q)) \lor (\neg(\neg p \lor q))) \lor \neg p$$

$\equiv ((q) \lor (\neg(\neg p)) \land (\neg q)) \lor \neg p$

$\equiv (q \lor (p \land \neg q)) \lor \neg p$

$\equiv ((q \lor p) \land (q \lor \neg q)) \lor \neg p$

$\equiv ((q \lor p) \land T) \lor \neg p$

$\equiv ((q \lor p) \lor \neg p$

$\equiv q \lor (p \lor \neg p)$

$\equiv q \lor T$

$\equiv T$

b) $((p \lor q) \land \neg p) \to q$

$((p \lor q) \land \neg p) \to q$

$\equiv(\neg p \land (p \lor q)) \lor q$

$\equiv \neg (\neg p \land (p \lor q)) \lor q$

$\equiv (\neg (\neg p) \lor \neg(p \lor q)) \lor q$

$\equiv (p \lor \neg(p \lor q)) \lor q$

$\equiv (p \lor (\neg p \land \neg q)) \lor q$

$\equiv ((p \lor \neg p) \land (p \lor \neg q)) \lor q$

$\equiv (T \land (p \lor \neg q)) \lor q$

$\equiv ((p \lor \neg q) \land T) \lor q$

$\equiv (p \lor \neg q) \lor q$

$\equiv p \lor (\neg q \lor q)$

$\equiv p \lor (q \lor \neg q)$

$\equiv p \lor T$

≡ T

C. Give the converse, the contrapositive, and the inverse of these conditional statements.

a) If it rains today, then I will drive to work.

Converse: If I will drive to work, then it rains today.

Contrapositive: If I will not drive to work then it does not rain today.

Inverse: If it does not rain today, then I will not drive to work.

b) If $|x| = x$, then $x \geq 0$.

Converse: If $x \geq 0$, then $|x| = x$.

Contrapositive: If $x < 0$, then $|x| \neq x$.

Inverse: If $|x| \neq x$, then $x < 0$.

c) If n is greater than 3, then n2 is greater than 9.

Converse: If n2 is greater than 9, then n is greater than 3.

Contrapositive: If n2 is not greater than 9, then n is not greater than 3

Inverse: If n is not greater than 3, then n2 is not greater than 9

Question # 02: [5x2=10 points]

A. Proof that: - [r V (Q ^ (- r -> - p))] = - r ^ (p V - q)

Prove that $\neg[r \vee (q \wedge (\neg r \rightarrow \neg p))] \equiv \neg r \wedge (p \vee \neg q)$

$\neg[r \vee (q \wedge (\neg r \rightarrow \neg p))]$

$\equiv \neg r \wedge \neg(q \wedge (\neg r \rightarrow \neg p))$, De Morgan's law

$\equiv \neg r \wedge \neg(q \wedge (\neg\neg r \vee \neg p))$, Conditional rewritten as disjunction

$\equiv \neg r \wedge \neg(q \wedge (r \vee \neg p))$, Double negation law

$\equiv \neg r \wedge (\neg q \vee \neg(r \vee \neg p))$, De Morgan's law

$\equiv \neg r \wedge (\neg q \vee (\neg r \wedge p))$, De Morgan's law, double negation

$\equiv (\neg r \wedge \neg q) \vee (\neg r \wedge (\neg r \wedge p))$, Distributive law

$\equiv (\neg r \wedge \neg q) \vee ((\neg r \wedge \neg r) \wedge p)$, Associative law

$\equiv (\neg r \wedge \neg q) \vee (\neg r \wedge p)$, Idempotent law

$\equiv \neg r \wedge (\neg q \vee p)$, Distributive law

$\equiv \neg r \wedge (p \vee \neg q)$, Commutative law

B. Use rules of inference to show that the three hypotheses Imply the conclusion:

(i) "If it does not rain or if it is not foggy, then the sailing race will be held and the lifesaving demonstration will go on."

(ii) "If the sailing race is held, then the trophy will be awarded."

(iii) "The trophy was not awarded."

conclusion : (iv) "It rained."

. Let R stand for it rains, F for it's foggy, S for the sailing race being held, L for the lifesaving demonstration, and T for the trophy being awarded. Write the four statements (i) through (iv) in terms of R, F, S, L, and T. (i). $(\neg R \vee \neg F) \rightarrow (S \wedge L)$. (ii). $S \rightarrow T$. (iii). $\neg T$. (iv). R. b. Show that (iv) follows from (i), (ii), and (iii). Break down the steps in the argument into the smallest pieces you can. You don't have to explicitly name the rules such that you use, such as "modus ponens", but each step needs to be as simple as you can make it. There are various proofs. Here are two. I'll include the justifications although they're not required for your answers. First proof: The contrapositive of (i) says $\neg(S \wedge L) \rightarrow \neg(\neg R \vee \neg F)$. Using De Morgan's laws, that can be rewritten as $\neg S \vee \neg L \rightarrow R \wedge F$. From (ii) and (iii) by modus tollens, therefore $\neg S$. By the addition rule, therefore $\neg S \vee \neg L$. From $\neg S \vee \neg L \rightarrow R \wedge F$ and $\neg S \vee \neg L$, we get $R \wedge F$ by modus ponens. Then by simplification, R. q.e.d. Second proof: From (ii) and (iii) by modus tollens, therefore $\neg S$. Since $\neg S$, therefore $\neg(S \wedge L)$. This is actually the contrapositive of the rule of simplification $S \wedge L \rightarrow S$. From that statement and (ii), therefore, by modus tollens, $\neg(\neg R \vee \neg F)$. That's equivalent to $R \wedge F$ by De Morgan's laws. Therefore, R, by simplification again.

Question # 3 (Functions and Set theory) [5x3=15 points]

A. Let f : R → R be defined by the formula f(x) = 4x-1 ∀x ∈ R. Is f a bijective function? If not, give a reason why? If yes, find its inverse.

Solution:

Then f is bijective, therefore f^{-1} exists. By definition of f^{-1},

$$f^{-1}(y) = x \Leftrightarrow f(x)=y$$

Now solving $f(x) = y$ for x

$$\Leftrightarrow \quad 4x-1 = y \qquad \text{(by definition of f)}$$

$$\Leftrightarrow \quad 4x = y + 1$$

$$\Leftrightarrow \quad x = \frac{y+1}{4}$$

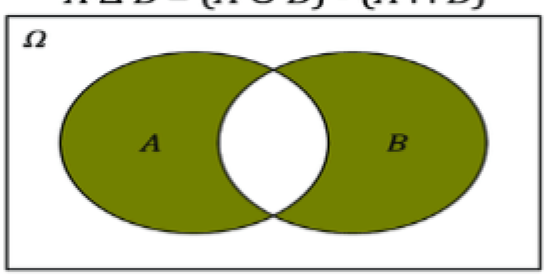
Hence, $f^{-1}(y) = \dfrac{y+1}{4}$ is the inverse of f(x)=4x-1 which defines f^{-1}: R→R.

B. Draw Venn Diagram of the following relationships between the sets:

a) (A U B) – (A ∩ B)

b) U

$A \,\Delta\, B = (A \cup B) - (A \cap B)$



C. Give an example of a function from N to N that is

a) one-to-one but not onto.

b) onto but not one-to-one.

c) both onto and one-to-one.

d) neither one-to-one nor onto

Question # 04: [5x4=20 points]

A. Decide whether each of these integers is congruent to 5 modulo 17. (show steps)

a) 80

b) 103

c) −29

d) −122

Problem 1. Determine whether each of these integers is congruent to 3 modulo 7.

(a) 37; (b) 66; (c) -17; (d) -67.

Solution. (a) $37-3=34$ is not divisible by 7, hence $37 \not\equiv 3 (\bmod 7)$.

(b) $66-3=63=7 \cdot 9$, hence $66 \equiv 3 (\bmod 7)$.

(c) $-17-3=-20$ is not divisible by 7, hence $-17 \not\equiv 3 (\bmod 7)$.

(d) $-67-3=-70=7 \cdot (-10)$, hence $-67 \equiv 3 (\bmod 7)$.

B. a) Use Fermat's little theorem to compute 3^302 mod 11.

b) Use your results from part (a) and the Chinese remainder theorem to find 3^302 mod 385. (Note that 385 = 5 · 7 · 11.)

24a $3^4 \equiv 1 \pmod 5$, $3^6 \equiv 1 \pmod 7$, $3^{10} \equiv 1 \pmod{11}$

$$\begin{array}{llllll} 3^{302} & \bmod 5 & = 3^{300} \cdot 3^2 \bmod 5 & = (3^4)^{75} \cdot 9 \bmod 5 & = 9 \bmod 5 & = 4 \\ 3^{302} & \bmod 7 & = 3^{300} \cdot 3^2 \bmod 7 & = (3^6)^{50} \cdot 9 \bmod 7 & = 9 \bmod 7 & = 2 \\ 3^{302} & \bmod 11 & = 3^{300} \cdot 3^2 \bmod 11 & = (3^{10})^{30} \cdot 9 \bmod 11 & = 9 \bmod 11 & = 9 \end{array}$$

24b One can see that 9 is solution: $9 \equiv 3^{302} \pmod 5$, $9 \equiv 3^{302} \pmod 7$ and $9 \equiv 3^{302} \pmod{11}$. $x \equiv 3^{302} \pmod{5 \cdot 7 \cdot 11}$ has a unique solution modulus 385, which has to verify the three previous relations. Those three have a unique solution modulus 385, (which is 9) due to the Chinese Remainder Theorem. Therefore, 9 is solution of $x \equiv 3^{302} \pmod{5 \cdot 7 \cdot 11}$.
If one is not convinced, there exists integers λ_1, λ_2, λ_3 such that $3^{302} - 9 = 5 \cdot \lambda_1 = 7 \cdot \lambda_2 = 11 \cdot \lambda_3 = \lambda$. Because 5,7 and 11 are relatively primes, $385 = 5 \cdot 7 \cdot 11 \mid \lambda$
and $3^{302} \bmod 385 = 9 + \lambda \bmod 385 = 9$.

If not, one can construct $x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$ with $a_1 = 4$, $a_2 = 2$, $a_3 = 9$, $M_1 = 7 \cdot 11 = 77$, $M_2 = 5 \cdot 11 = 55$, $M_3 = 5 \cdot 7 = 35$, and y_k such that $M_k y_k \equiv 1 \pmod{m_k}$. Be careful not to consider another formula for y_k. The only simplification you can do is the following: $(M_k \bmod m_k) y_k \equiv 1 \pmod{m_k}$

For y_1: $77 \bmod 5 = 2$, $2 \cdot 3 = 6 \equiv 1 \pmod 5$ and $y_1 = 3$
For y_2: $55 \bmod 7 = 6$, $6 \cdot 6 = 36 \equiv 1 \pmod 7$ and $y_2 = 6$
For y_3: $35 \bmod 11 = 2$, $2 \cdot 6 = 12 \equiv 1 \pmod{11}$ and $y_3 = 6$

$x = 4 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 9 \cdot 35 \cdot 6 = 924 + 660 + 1890 = 3474 \equiv 9 \pmod{385}$

C. A message has been encrypted using the function f(x) = (x + 5) mod 26. If the message in encrypted form is VZJXYNTS UFUJW, decrypt the message.

(a) A message has been encrypted using the function f(x) = (x + 5) mod 26. If the message in encrypted form is ***VZJXYNTS UFUJW***, decrypt the message.
Solution:
QUESTION PAPER is the encrypted message.

D. The first nine digits of the ISBN-10 of the European version of the fifth edition of a book are 0-07-119881. What is the check digit for that book?

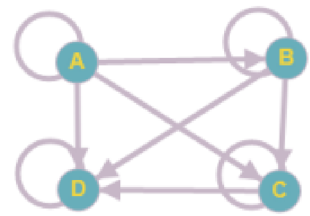
(c) The first nine digits of the ISBN-10 of the European version of the fifth edition of a book are 0-07-119881. What is the check digit for that book?
Solution:
1*0 + 2*0 + 3*7 + 4*1 + 5*1 + 6*9 + 7*8 + 8*8 + 9*1 + x_{10} = 0 mod 11
0 + 0 + 21 + 4 + 5 + 54 + 56 + 64 + 9 + x_{10} = 0 mod 11
213 + x_{10} = 0 mod 11
Check digit, x_{10} = 4.

Question # 05: [5x4=20 points]

(a) Draw the digraph of the following matrix.

$$R = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Solution:

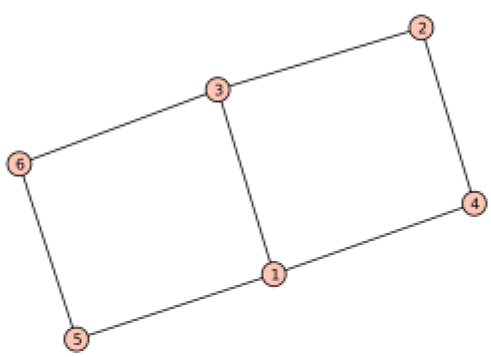


(b) Determine whether the relation in part (a) is an equivalence relation? Show all of your steps.
Solution:
No, it is not an equivalence relation. Since it is Reflective and Transitive but not Symmetric.

(c) Find the composition of relations R1 and R2, Where R1 is the relation from {1,2,3} to {2,4,6,8} with R1 = {(1, 2), (1, 6), (2, 4), (3, 4), (3, 6), (3, 8)} and R2 is the relation from {2,4,6,8} to {s,t,u} with R2 = {(2, u), (4, s), (4, t), (6, t), (8, u)}.
Solution:
R2 ∘ R1 = {(1, u), (1, t), (2, s), (2, t), (3, s), (3, t), (3, u)}.

(d) Determine whether the given relation(R) is a partial-order relation on A= {1, 2, 3, 4, 5}? Show all of your steps.
R= {(x, y) ∈ A | 3 divides x + y}
Solution:
R= {(1,2),(1,5),(2,1),(2,4),(3,3),(4,2),(4,5),(5,1),(5,4)}. It is not a Partial-order relation as it not holds Reflexive, Antisymmetric and Transitive property.

A. Determine if the following graph G is bipartite. If so, state the vertex sets V1 and V2 which partition the vertices of G.



Yes,

V1: 1,2,6

V2: 3,4,5