Assignment - 1

* Discrete Mathematics

Main Problem

Q1.) A system is designed to automatically verify logical statements used in access control. Each access rule is represented as a propositional formula. Consider the formula:

$$[(p \to q) \land (\neg r \lor q)] \to (p \to r)$$

Where:

- p: user is authenticated
- q: user has a valid token
- r: user can access confidential files

Tasks:

1. construct the truth table for this expression.
2. Determine whether the statement is a tautology, contradiction, or contingency.
3. show how this logic can prevent unauthorized access when q is false.

Soln:-

(1) A system is designed to automaticlly verify logical statements used in access control.

$$[(p \to q) \land (\neg r \lor q)] \to (p \to r)$$

Where:-

- p: user is authenticated
- q: user has a valid token
- r: user can access confidential files

(2) **Truth Table construction**

p	q	r	$p \to q$	$\neg r$	$\neg r \lor q$	$(p \to q) \land (\neg r \lor q)$	$p \to r$	Final Expression
T	T	T	T	F	T	T	T	T
T	T	F	T	T	T	T	F	F
T	F	T	F	F	F	F	T	T
T	F	F	F	T	T	F	F	T
F	T	T	T	F	T	T	T	T
F	T	F	T	T	T	T	T	T
F	F	T	T	F	F	F	T	T
F	F	F	T	T	T	T	T	T

③

Types of statement

- The last column both T_s and F_s.
- Therefore, the formula is a contingency

④

Logical Analysis for Access control (when q is false)

If q ("user has a ~~not~~ valid token") is False:

- The user does not have a valid token.
- The system's logic only grants access to confidential files (r true) if both authentication (p) and token (q) conditions are satisfied.
- If a valid token is missing (q = F), the formula typically evaluates false or restricts access, effectively preventing unauthorized users from accessing confidential files.
- This safeguards the system against unauthorized ~~to~~ access by coupling logical requirements.

(2)

Sub: Problem 1: Propositional Equivalences

Prove that the following propositions are logically equivalent:

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

Tasks:-

1.) Prove the above using truth tables.

2.) use logical identities (e.g., implication, De Morgan's Law) to transform the left-hand side into the right-hand side.

Soln:-

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

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

- columns $\neg(p \Rightarrow q)$ and $p \wedge \neg q$ match for all cases.
- Therefore, the two expression are logically equivalent.

(2) Proof using logical Identities

L.H.S

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

Recall that:

$$p \to q \equiv \neg p \vee q$$

$$\neg(p \to q) \equiv \neg(\neg p \vee q)$$

$\therefore$ (By De Morgan's Law)

$$\neg(\neg p \vee q) \equiv p \wedge \neg q$$

$\therefore$

$$\neg(p \to q) \equiv p \wedge \neg q$$

Both the truth and stepwise identities confirm the equivalence.

Sub-Problem-3:-

Nested Quantifiers & Rules of Inference

Q.) Let:

- $M(x, y)$: "x is a mentor of y"
- $G(x)$ "x is a good mentor"

Given:

1.) $\forall x \ \forall y \ (M(x, y) \rightarrow G(x))$

2.) M (Amit, Reena)

Tasks:-

1.) Using rules of inference, prove that Amit is a good mentor.

2.) Express the above inference chain in steps (Universal Instantiation, Modus Ponens, etc.)

Solution :-

- $M(x,y)$: "x is a mentor of y"
- $G(x)$: "x is a good mentor"

Premises :

1.) $\forall x \forall y \, (M(x,y) \rightarrow G(x))$

2.) $M(\text{Amit}, \text{Reena})$

1.) Proof that Amit is a Good Mentor

Step 1 :

Premise (1):

$\forall x \forall y \, (M(x,y) \rightarrow G(x))$

By universal Instantiation :

$x = \text{Amit}$ and $y = \text{Reena}$:

$M(\text{Amit}, \text{Reena}) \rightarrow G(\text{Amit})$

2.) $M(\text{Amit}, \text{Reena})$

3.) Apply Modus Ponens to the results of step1 and step2 :

$M(\text{Amit}, \text{Reena}) \rightarrow G(\text{Amit})$ is true, and $M(\text{Amit}, \text{Reena})$ is true, then $G(\text{Amit})$ is true

∴ $G(\text{Amit})$ ("Amit is good mentor") is proved by rules of inference.

2.)

step	Statement	Reasoning / Rule
1	$\forall x \forall y (M(x,y) \to G(x))$	Premise
2	$M(\text{Amit}, \text{Reena})$	Premise
3	$M(\text{Amity}, \text{Reena}) \to G(\text{Amit})$	universal Instantiation on (1)
4	$M(\text{Amit}, \text{Reena})$	Restate (2)
5.	$G(\text{Amit})$	Modus Ponens on (3) & (4)

- Universal Instantiation: From a statement that is true for all x and all y it must be true for specific value ($x = \text{Amit}, y = \text{Reena}$) also
- Modus Ponens: If $A \to B$ is true and A is true, then B is true

Sub Problem 4: set theory operations

Q.) Let:

- $A = \{1, 2, 3, 4\}$
- $B = \{2, 4, 6, 8\}$
- $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (universal set)

Tasks:

1.
- A ∪
- A ∩
- A −
- A', B' (complement w.r.t U)

2. verify: $(A \cup B)' = A' \cap B'$

sol • $A = \{1, 2, 3, 4\}$

• $B = \{2, 4, 6, 8\}$

• universal set $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

1)

• union $(A \cup B)$:

$$A \cup B = \{1, 2, 3, 4, 6, 8\}$$

• Intersection $(A \cap B)$:

$$A \cap B = \{2, 4\}$$

• Difference $(A - B)$

$$A - B = \{1, 3\}$$

• complement of A with respect to U (A'):

$$A' = U - A = \{5, 6, 7, 8, 9\}$$

• complement of B with respect to U (B'):

$$B' = U - B = \{1, 3, 5, 7, 9\}$$

2.) verify: $(A \cup B)' = A' \cap B'$

- First, find $(A \cup B)'$:

$$A \cup B = \{1, 2, 3, 4, 6, 8\}$$

so

$$(A \cup B)' = U - (A \cup B) = \{5, 7, 9\}$$

- Now, find $A' \cap B'$

$$A' = \{5, 6, 7, 8, 9\}, \quad B' = \{1, 3, 5, 7, 9\}$$

Intersection:

$$A' \cap B' = \{5, 7, 9\}$$

Hence $(A \cup B)' = A' \cap B'$ is verified.

Sub-Problem 5: Relations - Properties and Matrix Representation:

Let $A = \{1, 2, 3\}$ and define a relation R on A as:

$$R = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}$$

Tasks:

1.) Represent relation R as a 0-1 matrix

2.) Determine whether R is:

- Reflexive
- Symmetric
- Transitive

3. Draw the digraph of R.

Deliverables

Containing all the numericals, truth tables, relation and Proofs.

Criterion	Weight	Excellent / Good / Fair / Poor	Marks Awarded
Truth Table Accuracy	20%	All entries correct / Minor mistakes / Partial logic / Incorrect	5 / 4 / 3 / 2
Logical Proofs + Identities	20 %	~~All~~ complete with step / some gaps / Incomplete / Missing	5 / 4 / 3 / 2

Quantifier Logic	20 %	Accurate symbolic form / Minor flaws / Basic / incorrect	5/4/3/2
Set & Relation Properties	20 %	correct operations & matrix / some mistakes / Few parts done / incomplete	5/4/3/2
Presentation & structure	20 %	Neat, labeled, clear / Minor formatting / unstructured / Poor	5/4 3/2

Sol

$A = \{1, 2, 3\}$

$R = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}$

denfined on set A

1.) Relation R as a 0-1 Matrix

	1	2	3
1	1	1	0
2	0	1	1
3	0	0	1

2.) Properties of Relation R

- Reflexive

Here (1,1), (2,2), (3,3) are in R is reflexive.

- symmetric

  - $(1,2) \in R$ but $(2,1) \notin R$.

  Hence, R is not symmetric

- Transitive:

  - $(1,2), (2,3) \in R$, but $(1,3) \notin R$.

  Hence R is not transitive

3.) Digraph of Relation R

Vertices: 1, 2, 3

Edges:

- Loops on 1, 2, and 3 (for reflexive pairs)
- Directed edge from 1 to 2
- Directed edge from 2 to 3

Property	Is R satisfied?	Reason
Reflexive	Yes	All diagonal pairs (1,1), (2,2), (3,3) are in R.
symmetric	NO	$(1,2) \in R$ but $(2,1) \notin R$.
Transitive	NO	$(1,2), (2,3) \in R$ but $(1,3) \notin R$.

- Accurate 0-1 matrix representation
- clear evaluation of properties based on definitions
- Description for the digraph drawing