RV College of Engineering®
Mysore Road, RV Vidyaniketan Post,
Bengaluru - 560059, Karnataka, India

Go, change the world®

USN										

Academic year 2024-2025 (ODD Sem)

DEPARTMENT OF

INDUSTRIAL ENGINEERING & MANAGEMENT

Date	**25-11-2024**	**Maximum Marks**	**10 + 50**
Course Code	**HS251TA**	**Duration**	**30 + 90 Min**
Sem	**V**	**CIE – I Scheme & Solution**	
Principles of Management and Economics			

Note:

1. Answer all the Questions.

Sl. No.	Questions	M	BT	CO
	Part – A			
1	Directing.	01	1	1
2	Effectiveness in management refers to the degree to which an organization successfully achieves its goals and objectives. It involves doing the right tasks and ensuring that activities align with strategic aims to produce desired outcomes.	01	1	1
3	Quantitative.	01	1	1
4	The specific situation and environment	01	1	2
5	Henri Fayol	01	1	1
6	TQM relies on quantitative methods to assess and improve quality continuously, ensuring that customer needs are met through data-driven decision-making and process optimization.	01	1	2
7	Fiscal policy stimulates the economy by increasing government spending or reducing taxes to boost aggregate demand.	01	1	4
8	The government collects taxes from households and businesses and provides goods and services in return.	01	1	4
9	GDP, inflation, unemployment	02	1	5
	Part –B			
1 a	**Findings of the Hawthorne Studies:** • **Hawthorne Effect:** Demonstrated that employees' productivity increases when they know they are being observed. • **Social and Psychological Factors:** Revealed that factors such as attention from management, group dynamics, and employee recognition significantly impact productivity. **Reshaping Management Practices:** • **Shift from Mechanical to Human-Centric Management:** Managers began to focus more on employee relations, recognizing the importance of addressing workers' social and psychological needs. • **Increased Emphasis on Communication:** Open lines of communication between managers and employees became a priority to foster trust and collaboration. • **Focus on Employee Well-being:** Organizations started implementing practices aimed at improving job satisfaction, such as better working conditions, recognition programs, and opportunities for personal growth. **Influence on Modern Employee Motivation:**	06	4	1

	• **Motivation Theories:** The Hawthorne Studies laid the groundwork for theories like Maslow's Hierarchy of Needs and Herzberg's Two-Factor Theory, which emphasize the importance of fulfilling psychological and self-fulfillment needs. • **Employee Engagement:** Modern management practices stress the importance of engaging employees through meaningful work, autonomy, and opportunities for advancement. • **Recognition and Reward Systems:** Organizations implement various reward systems to acknowledge and incentivize employee contributions, boosting morale and productivity. **Influence on Teamwork Strategies:** • **Team-Based Structures:** Encouraging teamwork and collaborative efforts became integral to organizational design, promoting a sense of belonging and shared responsibility. • **Group Dynamics Understanding:** Managers are trained to understand and manage group dynamics, facilitating effective teamwork and conflict resolution. • **Empowerment and Participation:** Employees are given more autonomy and are encouraged to participate in decision-making processes, enhancing teamwork and collective problem-solving. **Conclusion:** The Hawthorne Studies fundamentally shifted management focus from purely physical and mechanical aspects to the human and social dimensions of work. This transformation has led to more holistic management practices that prioritize employee motivation and effective teamwork, thereby enhancing overall organizational performance and employee satisfaction.			
1 b	**Contingency Theory:** Management practices must adapt to situational factors like organizational size, culture, or external conditions. The **Contingency Theory** of management suggests that there is no universal set of principles or practices that work effectively in all situations. It recognizes that organizations, their environments, and the problems they face are diverse and dynamic, making it necessary to tailor management practices to fit specific circumstances. This theory refutes the idea of a "one-size-fits-all" approach by emphasizing the need for flexibility and adaptability in managerial decision-making. **Examples:** • A hierarchical structure works well in manufacturing but not in creative industries. • Flexible leadership styles are needed during a crisis compared to routine operations. It highlights the need for tailored approaches based on specific circumstances.	04	3	2
2	**Classical Approach:** • **Focus:** Emphasizes organizational structure, efficiency, and productivity through rational processes. • **Key Theories:** Scientific Management (Taylor), Administrative Theory (Fayol), Bureaucracy (Weber). • **Productivity Enhancement:** Achieved by optimizing workflows, standardizing tasks, and implementing strict hierarchical structures.	10	2	1

	• **Strengths:** Improves efficiency, clarifies roles, and establishes clear authority lines.
	Behavioral Approach:
	• **Focus:** Centers on human relations, employee motivation, and the social aspects of work.
	• **Key Studies:** Hawthorne Studies, Organizational Behavior (OB) theories.
	• **Productivity Enhancement:** Achieved by improving employee satisfaction, fostering teamwork, and addressing psychological needs.
	• **Strengths:** Enhances employee morale, encourages creativity, and reduces turnover.
	Comparison:
	• **View of Employees:** Classical views employees as parts of a machine to be optimized, while Behavioral views them as individuals with needs and motivations.
	• **Management Style:** Classical favors top-down, authoritarian management; Behavioral supports participative and democratic styles.
	• **Primary Concern:** Classical is concerned with "how" tasks are done efficiently; Behavioral focuses on "why" employees behave a certain way and how to motivate them.
	Limitations in Modern Workplaces:
	• **Classical Approach:**
	  o **Rigid Structure:** May stifle creativity and adaptability in dynamic environments.
	  o **Employee Disengagement:** Overemphasis on control can lead to low morale and high turnover.
	• **Behavioral Approach:**
	  o **Less Focus on Efficiency:** May neglect the need for structured processes and clear hierarchies.
	  o **Subjectivity:** Relies on understanding complex human behaviors, which can be less predictable and harder to manage systematically.
	Conclusion:
	While the Classical Approach effectively enhances efficiency and organizational structure, it often overlooks the human element, leading to potential employee dissatisfaction. Conversely, the Behavioral Approach prioritizes employee well-being and motivation, fostering a more engaged workforce but may sometimes lack the necessary focus on process optimization. Modern workplaces benefit from integrating both approaches to balance efficiency with employee satisfaction.			

3	**POSDCORB** stands for **Planning, Organizing, Staffing, Directing, Coordinating, Reporting, and Budgeting**, representing the key functions of management. Each component plays a crucial role in ensuring both **efficiency** (doing things right) and **effectiveness** (doing the right things): • **Planning:** Establishes goals and outlines the steps to achieve them, providing direction and reducing uncertainties. • **Organizing:** Arranges resources and tasks in a structured manner, ensuring optimal resource utilization.	10	3	1

	• **Staffing:** Involves recruiting and training the right people, which is vital for executing plans effectively. • **Directing:** Guides and motivates employees, fostering a productive work environment. • **Coordinating:** Ensures all departments and activities are aligned, preventing overlaps and conflicts. • **Reporting:** Provides feedback and information flow, enabling timely adjustments and informed decision-making. • **Budgeting:** Allocates financial resources efficiently, ensuring that funds are available for essential activities. **Ensuring Efficiency and Effectiveness:** • **Efficiency** is achieved through organized resource allocation, minimizing waste, and optimizing processes. • **Effectiveness** is ensured by aligning activities with organizational goals, selecting the right personnel, and adapting to changes. **Challenges if a Function is Underperformed:** • **Neglecting Planning:** Leads to unclear objectives, misaligned activities, and inefficient use of resources. • **Poor Organizing:** Causes resource misallocation, duplication of efforts, and operational bottlenecks. • **Inadequate Staffing:** Results in skill mismatches, low employee morale, and reduced productivity. • **Weak Directing:** Causes lack of motivation, unclear instructions, and decreased employee engagement. • **Faulty Coordinating:** Leads to departmental silos, conflicts, and inconsistent outcomes. • **Incomplete Reporting:** Hinders performance tracking, delaying problem identification and resolution. • **Ineffective Budgeting:** Results in financial constraints, inability to fund critical projects, and overspending. **Conclusion:** Each POSDCORB function interrelates to create a cohesive management framework. Underperformance in any one area disrupts the entire system, undermining both efficiency and effectiveness. Managers must balance all functions to maintain organizational health and achieve strategic objectives.			
4	**Relevance of Systems Theory:** • **Holistic View:** Systems Theory views an organization as a complex set of interrelated and interdependent parts working together toward a common goal. • **Open Systems:** Emphasizes that organizations interact with their external environment, adapting to changes and influences from outside factors. **Emphasis on Interdependence:** • **Integration of Functions:** Encourages the integration of various departments and functions, ensuring that changes in one area consider impacts on others. • **Collaboration:** Promotes cross-functional collaboration, leading tomore cohesive and unified organizational efforts.	10	4	1

	• **Resource Optimization:** Recognizes that resources are interconnected, leading to more efficient and effective utilization across the organization. **Emphasis on the Environment:** • **Adaptability:** Encourages organizations to be flexible and responsive to external changes such as market trends, technological advancements, and regulatory shifts. • **Proactive Decision-Making:** Managers anticipate external factors and incorporate environmental scanning into their strategic planning. • **Sustainability:** Focuses on long-term viability by considering environmental, social, and economic factors in decision-making. **Benefits to Decision-Making:** • **Comprehensive Analysis:** Decisions are made with a thorough understanding of how different parts of the organization and external factors interact. • **Enhanced Problem-Solving:** By recognizing interdependencies, managers can identify root causes of issues and implement more effective solutions. • **Strategic Alignment:** Ensures that decisions align with both internal objectives and external opportunities or threats, fostering strategic coherence. • **Risk Management:** Facilitates the identification and mitigation of risks arising from environmental changes, enhancing organizational resilience. **In summary:** Systems Theory remains highly relevant in modern organizations by providing a framework that accounts for the complexity and dynamism of both internal and external environments. Its emphasis on interdependence and environmental interaction enables managers to make more informed, strategic, and adaptive decisions, ultimately leading to sustainable organizational success.			
5	The circular flow model links microeconomics, macroeconomics, and economic systems, showing how their interaction drives economic activity. 1. **Microeconomics in the Circular Flow:** o Households and firms engage in the exchange of goods, services, and factors of production. o Example: Firms pay wages (micro) to households, who spend it on goods, creating demand. 2. **Macroeconomics in the Circular Flow:** o Government policies (e.g., fiscal stimulus) influence overall spending and production. o Example: Tax cuts increase disposable income, boosting aggregate demand. 3. **Economic Systems in the Circular Flow:** o The structure of the economy determines the roles of markets and governments in regulating the flow. o Example: In a mixed economy, subsidies might support businesses during downturns, while in capitalism, market corrections occur without intervention. **Challenges When Components Fail to Work in Harmony:** • **Mismatch Between Policies and Market Dynamics:**	10	4	5

	○ Over-regulation in capitalist systems may stifle growth, while under-regulation in mixed systems can lead to market failures (e.g., financial crises). • **Imbalance in Resource Allocation:** ○ Inefficiencies arise when resources are not directed to where they are needed most, leading to unemployment or shortages. • **Inequality and Economic Disruptions:** ○ A focus on micro-level profitability can lead to macro-level instability, such as wealth inequality and social unrest. **Conclusion:** Microeconomics, macroeconomics, and economic systems must align within the circular flow to ensure stability and growth. Failure to coordinate these components can disrupt the flow of money, goods, and services, hindering economic progress.			

BT-Blooms Taxonomy, CO-Course Outcomes, M-Marks

Marks Distribution	Particulars		CO1	CO2	CO3	CO4	CO5	L1	L2	L3	L4	L5	L6
	Quiz	Max Marks	04	02	-	2	2	10	-	-	-	-	-
	Test		36	04	-	0	10	-	10	14	26		

****

Academic year 2024-2025 (Odd Sem)

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING

SCHEME AND SOLUTION

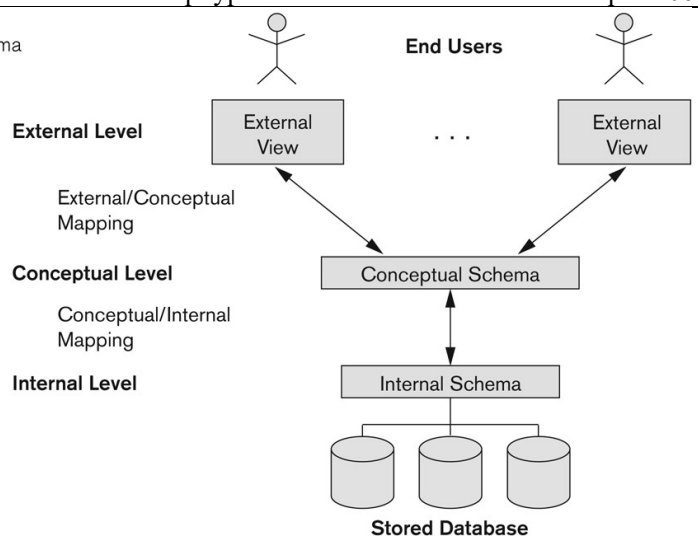
Date	24th November 2024	**Maximum Marks**	10+50
Course Code	CD252IA	**Duration**	90 Minutes
Sem	V	Faculty:	

CIE-I

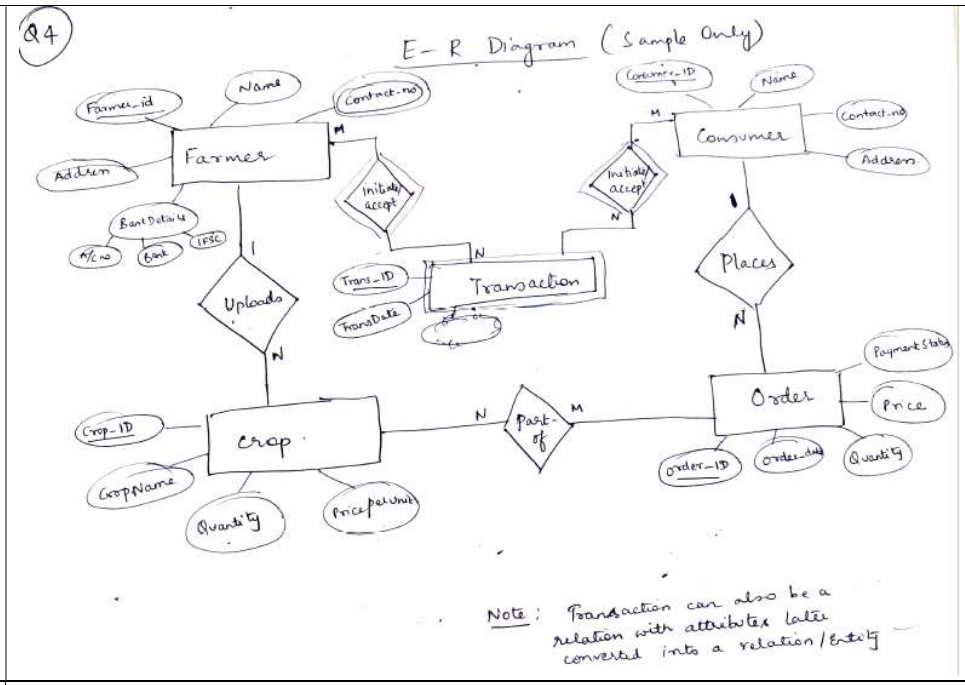
Database Management Systems (Common to CS, IS, CD, AI & CY)

Sl.No	PART-A	M	BT	CO
1.	**Tasks of Actors on the Scene:** 1. Querying the database for specific information (e.g., retrieving customer data). 2. Updating or modifying records in the database (e.g., editing employee information). Examples: Data Analysts, Bank Clerks, Sales Executives. **Tasks of Workers Behind the Scene:** 1. Ensuring the database system is running efficiently (e.g., tuning database performance). 2. Implementing security measures to protect the database (e.g., setting user access permissions). Examples: Database Administrators (DBAs), System Engineers, Security Specialists.	**2**	**L3**	**1**
2.	**Representational (or Implementation) Data Model**. Example: Model which organizes data into tables (relations) with rows and columns, allowing users to query and manipulate data using SQL.	**2**	**L3**	**1**
3.	It depends on the combination of the **Member ID** (from the **Member** entity) and the **Book ID** (from the **Book** entity) for its identification.	**2**	**L3**	**2**
4.	Composite attributes can be divided into smaller subparts, which represent more basic attributes with independent meanings. Multivalued attributes are those for which different users may have different values for the same attribute. It may have lower and upper bounds to constrain the number of values allowed for each individual entity. – 1 mark Representation for both: 1 mark	**2**	**L2**	**2**
5.	In some cases, a particular entity may not have an applicable value for an attribute. For such situations, a special value called NULL is created. An address of a single-family home would have NULL for its Apartment_number attribute, and a person with no college degree would have NULL for College_degrees. NULL can also be used if we do not know the value of an attribute for a particular entity.	**2**	**L2**	**1**

Sl. No.		PART-B	M	BT	CO
1		A relationship type R among n entity types E1, E2, ..., En defines a set of associations—or a relationship set—among entities from these entity types. Mathematically, the relationship set R is a set of relationship instances ri, where each ri associates n individual entities (e1, e2, ..., en), and each entity ej in ri is a member of entity set Ej, $1 \leq j \leq n$. Hence, a relationship set is a mathematical relation on E1, E2, ..., En; alternatively, it can be defined as a subset of the Cartesian product of the entity sets E1 × E2 × ... × En. Each of the entity types E1, E 2, ..., En is said to participate in the relationship type R; similarly, each of the individual entities e1, e2, ..., en is said to participate in the relationship instance ri = (e1, e2, ..., en). – 040 marks iii) An example of a ternary relationship is SUPPLY, where each relationship instance ri associates three entities—a supplier s, a part p, and a project j—whenever s supplies part p to project j. Relationships can generally be of any degree, but the ones most common are binary relationships. iv) Relationships as Attributes: Consider the WORKS_FOR relationship type. One can think of an attribute called Department of the EMPLOYEE entity type, where the value of Department for each EMPLOYEE entity is (a reference to) the DEPARTMENT entity for which that employee works. Hence, the value set for this	**10**	**L2**	**1**

		Department attribute is the set of all DEPARTMENT entities, which is the DEPARTMENT entity set. v) Role names are not technically necessary in relationship types where all the participating entity types are distinct, since each participating entity type name can be used as the role name. However, in some cases the same entity type participates more than once in a relationship type in different roles. In such cases the role name becomes essential for distinguishing the meaning of the role that each participating entity plays. Such relationship types are called recursive relationships. – 06 marks			
2	(a)	**Figure 2.2** The three-schema architecture.  Fig -2 marks, Expln: 4 marks	06	L2	1
	(b)	**Logical data independence** is the capacity to change the conceptual schema without having to change external schemas or application programs. We may change the conceptual schema to expand the database (by adding a record type or data item), to change constraints, or to reduce the database (by removing a record type or data item). **Physical data independence** is the capacity to change the internal schema without having to change the conceptual schema. Hence, the external schemas need not be changed as well. Changes to the internal schema may be needed because some physical files were reorganized—for example, by creating additional access structures—to improve the performance of retrieval or update. 2X2 =4	04	L2	1
3	(a)	List -2M Explanation 4M • Self-describing nature of a database system • ■ Insulation between programs and data, and data abstraction • ■ Support of multiple views of the data • ■ Sharing of data and multiuser transaction processing	06	L2	1
	(b)	Participation Constraints Definition 2M Example 2M Total Participation Partial Participation	04	L2	1
4	(a)	**Entities and Attributes** 1. **Farmer** ○ **Attributes**: ▪ FarmerID (Primary Key) ▪ Name ▪ ContactNumber	10	L4	2

		▪ Address ▪ BankDetails 2. **Consumer/Wholesaler** o **Attributes**: ▪ ConsumerID (Primary Key) ▪ Name ▪ ContactNumber ▪ Address 3. **Crop/Produce** o **Attributes**: ▪ CropID (Primary Key) ▪ CropName ▪ QuantityAvailable ▪ PricePerUnit 4. **Order** o **Attributes**: ▪ OrderID (Primary Key) ▪ OrderDate ▪ QuantityOrdered ▪ TotalPrice ▪ PaymentStatus 5. **Transaction** o **Attributes**: ▪ TransactionID (Primary Key) ▪ TransactionDate ▪ FarmerID (Foreign Key) ▪ ConsumerID (Foreign Key) ▪ OrderID (Foreign Key)			
		Relationships 1. **Farmer uploads Crop/Produce** o **Relationship**: One Farmer can upload multiple Crops, but each Crop belongs to one Farmer. o **Type**: One-to-Many 2. **Consumer places Order** o **Relationship**: One Consumer can place multiple Orders, but each Order is placed by one Consumer. o **Type**: One-to-Many 3. **Crop is part of Order** o **Relationship**: One Order can contain multiple Crops, and each Crop can be part of multiple Orders. o **Type**: Many-to-Many (resolved through an associative entity, e.g., **OrderDetails**) 4. **Farmer and Consumer/Wholesaler involved in Transaction** o **Relationship**: Each Transaction involves one Farmer and one Consumer. o **Type**: Many-to-Many (can be resolved using the **Transaction** entity). **ER Diagram – 07 marks** **Cardinality ratio – 03 marks**			

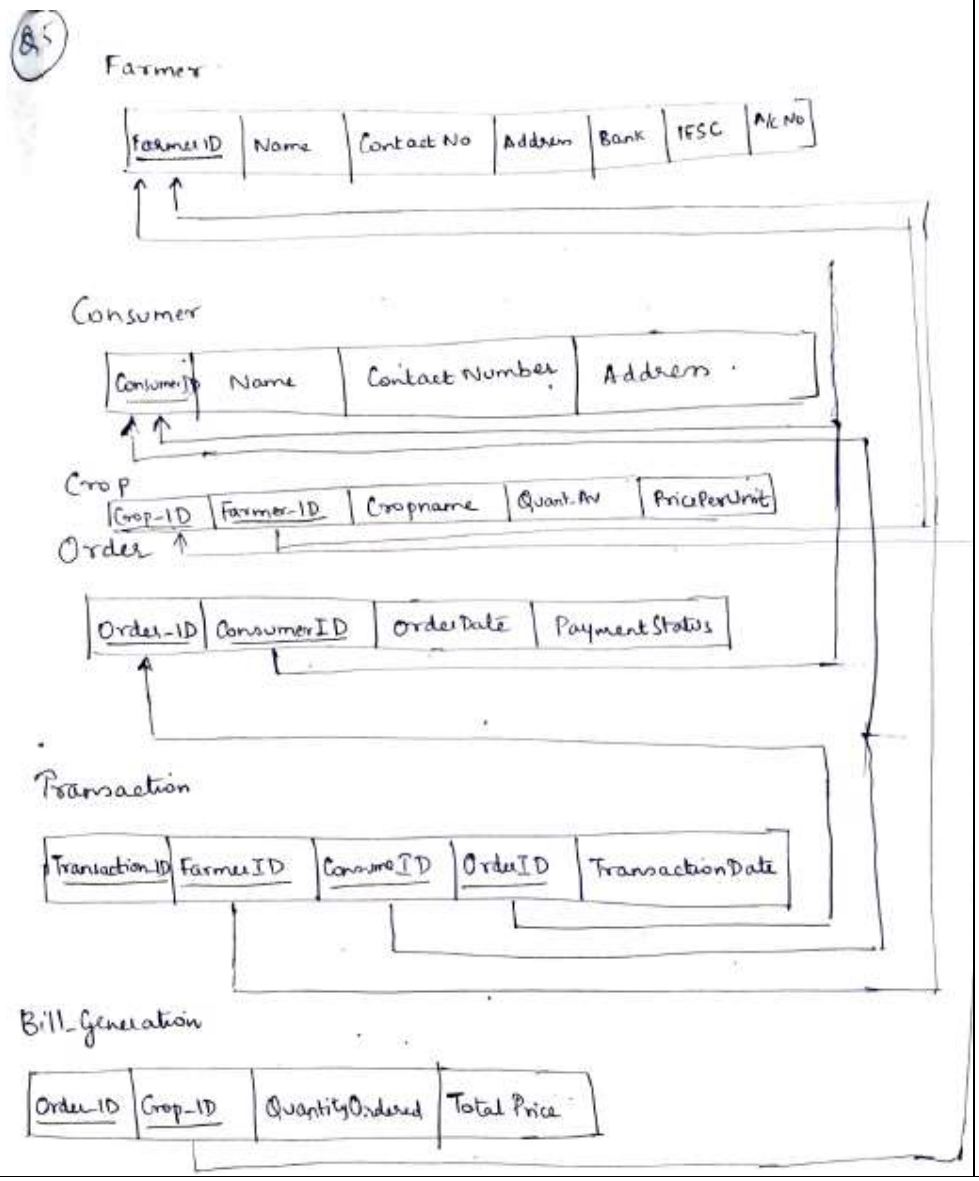
					
5	(a)	**Relational Tables – 07 marks** 1. **Farmer** o FarmerID (Primary Key) o Name o ContactNumber o Address o BankDetails 2. **Consumer** o ConsumerID (Primary Key) o Name o ContactNumber o Address 3. **Crop** o CropID (Primary Key) o FarmerID (Foreign Key, references Farmer.FarmerID) o CropName o QuantityAvailable o PricePerUnit 4. **Order** o OrderID (Primary Key) o ConsumerID (Foreign Key, references Consumer.ConsumerID) o OrderDate o PaymentStatus 5. **OrderDetails** (Associative table for Many-to-Many relationship between Order and Crop) o OrderID (Foreign Key, references Order.OrderID) o CropID (Foreign Key, references Crop.CropID) o QuantityOrdered o TotalPrice 6. **Transaction** o TransactionID (Primary Key) o FarmerID (Foreign Key, references Farmer.FarmerID) o ConsumerID (Foreign Key, references Consumer.ConsumerID) o OrderID (Foreign Key, references Order.OrderID)	10	4	L2

- TransactionDate

Relational Schema Diagram Representation – 03 marks

- **Primary Keys (PK)**: Underlined in each table.
- **Foreign Keys (FK)**: Marked as references to their respective tables.
- Relationships are shown using lines/arrows connecting FK columns to their referenced PK columns.

Representation of the above diagram step by step as per algorithm



RV College of Engineering®
Mysore Road, RV Vidyaniketan Post,
Bengaluru - 560059, Karnataka, India

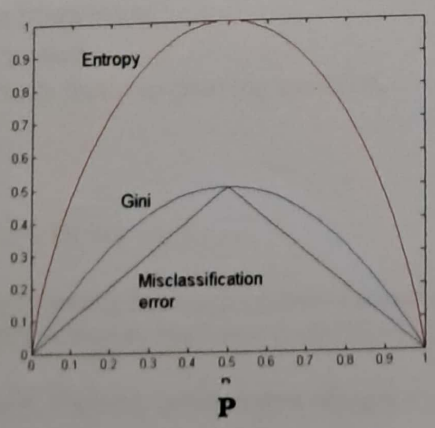
Go, change the world

Academic year 2024-2025 (Odd Sem)

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

Date	26 November 2024	Maximum Marks	60
Course Code	IS353IA	Duration	120 min
Sem	V	CIE-1	
UG/PG	UG	Faculty:	

Artificial Intelligence and Machine Learning
<(Common to AIML/CSE/ISE) >

Sl. No.	Quiz Questions	M	L	CO
1	Justify whether the following sentence(s) hold true or false for Turing test in context AI. Marks are awarded for justification only. i. The Turing Test requires the machine to be able to convincingly simulate human intelligence to pass. *TRUE- The Turing Test, proposed by Alan Turing, evaluates a machine's ability to exhibit behavior indistinguishable from that of a human during a conversation.* ii. The Turing Test guarantees that a machine that passes it is intelligent. *FALSE- The Turing Test only measures a machine's ability to mimic human-like responses but does not guarantee genuine intelligence or understanding.*	02	L3	CO1
2	The _____ algorithm uses Entropy as a measure for constructing decision trees, while the _____ algorithm employs the Gini Index for splitting criteria. *ID3, CART*	02	L1	CO1
3	Draw observations from the graph below  At p=0.5, all measures are at their maximum (highest impurity).	02	L3	CO1

1a - 8
1b 6
14

2a - 12
2b - 6
18

3a - 10
3b - 8
18.

Scanned with OKEN Scanner

	• As p approaches 0 or 1 (classes become more pure), all measures decrease. • Entropy drops faster than Gini, and Misclassification Error drops the slowest, reflecting their sensitivity to changes in p.			
4	List the key stopping criteria used in constructing a decision tree (any two) • *Maximum depth reached* *No significant information gain* *Pure node (homogeneous labels)* *all attribute same value*	**02**	L2	CO1
5	Differentiate Rationality and perfection in AI decision making with an example. *Rationality: Making the best decision given the available information, computational limitations, and environmental constraints.* *Perfection: Making an ideal decision with complete and perfect information and unlimited computational power.*	**02**	L2	CO1

Sl. No.	Test Questions	M	L	CO
1a	Analyze each of the following agent environments and determine whether they are fully or partially observable, deterministic or stochastic, static or dynamic, and discrete or continuous. Justify your classification with appropriate reasoning for each environment. i. autonomous Mars rover. ii. playing tic-tac-toe. iii. mathematician's theorem-proving assistant. **2.5*2+3=8M** **i. Autonomous Mars Rover** • **Observability:** Partially Observable (limited sensor range and obstructions). • **Deterministic/Stochastic:** Stochastic (unpredictable elements like dust storms). • **Static/Dynamic:** Dynamic (environment changes over time).	**08**	L3	CO1

Scanned with OKEN Scanner

- **Discrete/Continuous:** Continuous (real-world terrain and movements).

ii. Playing Tic-Tac-Toe

- **Observability:** Fully Observable (entire board is visible).
- **Deterministic/Stochastic:** Deterministic (outcomes depend solely on player moves).
- **Static/Dynamic:** Static (game state doesn't change without player action).
- **Discrete/Continuous:** Discrete (finite moves and board states).

iii. Mathematician's Theorem-Proving Assistant

- **Observability:** Fully Observable (complete problem description available).
- **Deterministic/Stochastic:** Deterministic (logical rules ensure predictable outcomes).
- **Static/Dynamic:** Static (problem doesn't change during solving).
- **Discrete/Continuous:** Discrete (steps involve logical, finite reasoning).

1b — **06** — L3 — CO1

For the following examples, find the PEAS (Performance measure, Environment, Actuators, Sensors) framework and describe each component:

1. Washing Machine
2. Autonomous Drone
3. Smart Home Thermostat

2.5*2+3=8M

Example	Performance Measure	Environment	Actuators	Sensors
Washing Machine	Cleanliness of clothes, minimal water and energy usage, adherence to time settings	Laundry load, type of clothes, water supply, detergent	Drum motor, water inlet valve, detergent dispenser, heater	Water level sensor, temperature sensor, load sensor, speed sensor
Autonomous Drone	Safe navigation, task completion (e.g., delivery, surveillance), energy efficiency	Airspace, obstacles, GPS location, weather conditions	Motors, rotors, camera gimbals, control surfaces	GPS, gyroscope, accelerometer, camera, lidar, altimeter
Smart Home Thermostat	Maintaining desired	Room temperature,	Heating or cooling	Temperature sensor, humidity

Scanned with OKEN Scanner

	temperature with minimal energy consumption	external weather, occupancy, HVAC system	system control, fan control	sensor, occupancy sensor			

4.

Consider the following data set:

price	maintenance	capacity	airbag	profitable
low	low	2	no	yes
low	med	4	yes	no
low	low	4	no	yes
low	high	4	no	no
med	med	4	no	no
med	med	4	yes	yes
med	high	2	yes	no
med	high	5	no	yes
high	med	4	yes	yes
high	high	2	yes	no
high	high	5	yes	yes

3a Suppose we decide to construct a decision tree using binary splits and the Gini index impurity measure. Which feature and split point combinations would be the best to use as the root node assuming that we consider each of the input features to be unordered? **12** L3 CO2

Feature	P	Gini Index
price	price = low	0.3961
maintenance	maintenance = low	0.3961
capacity	capacity = 4	0.3879
airbag	airbag = no	0.4909

Capacity is best feature

3b Discuss the approaches for splitting based on continuous attributes? Demonstrate the same using the following dataset: 3+3=6M **06** L3 CO2

Record	Age	Purchased (Yes/No)
1	22	No
2	25	Yes
3	28	Yes

Scanned with OKEN Scanner

4	35	No
5	40	Yes

Binary split:

Threshold = 28: Split into Age ≤ 28 and Age > 28.

- Age ≤ 28: Records 1, 2, 3 (Yes: 2, No: 1)
- Age > 28: Records 4, 5 (Yes: 2, No: 0)
- **Gini for Age ≤ 28:**

$$Gini = 1 - \left(\left(\frac{2}{3}\right)^2 + \left(\frac{1}{3}\right)^2\right) = 0.4444$$

- **Gini for Age > 28:**

$$Gini = 1 - \left(\left(\frac{2}{2}\right)^2 + \left(\frac{0}{2}\right)^2\right) = 0$$

- **Weighted Gini for Threshold = 28:**

$$Gini_{split} = \frac{3}{5} \times 0.4444 + \frac{2}{5} \times 0 = 0.2667$$

Discrtization approach

Scanned with OKEN Scanner

Step 2: Calculate Gini Index for Each Interval

1. **Interval 1 ($\text{Age} \leq 25$):**
   - Records: 1, 2, 3
   - Purchased: Yes = 2, No = 1
   - Gini Index:

$$Gini = 1 - \left(\frac{2}{3}\right)^2 - \left(\frac{1}{3}\right)^2 = 1 - 0.4444 - 0.1111 = 0.4444$$

2. **Interval 2 ($25 < \text{Age} \leq 35$):**
   - Record: 4
   - Purchased: Yes = 0, No = 1
   - Gini Index:

$$Gini = 1 - \left(\frac{0}{1}\right)^2 - \left(\frac{1}{1}\right)^2 = 0$$

3. **Interval 3 ($\text{Age} > 35$):**
   - Record: 5
   - Purchased: Yes = 1, No = 0
   - Gini Index:

$$Gini = 1 - \left(\frac{1}{1}\right)^2 - \left(\frac{0}{1}\right)^2 = 0$$

4a Compare and contrast the types of intelligent agents—simple reflex, model-based reflex, goal-based, and utility-based—based on their rationality, memory use, ability to handle dynamic or partially observable environments, and computational complexity. Use examples like a robot vacuum or a virtual assistant to illustrate their differences and applications. Present your answer in a tabular format with the following columns: 2*5=10M **10** L3 CO1

Agent Type	Rationality	Memory Usage	Handling Dynamic/Partially Observable Environments	Computational Complexity	Example/Use Case
Simple Reflex Agent	Acts solely based on current percepts without	Minimal	Cannot handle dynamic or partially observable environments effectively	Low (simple condition-action rules)	Robot vacuum cleaning a static, fully observable

Scanned with OKEN Scanner

		considering history or future; rational in simple tasks				room			
	Model-Based Reflex Agent	Rational with the inclusion of an internal model to track the environment state	Moderate (needs to store model)	Can handle partially observable environments to some extent	Moderate (requires model maintenance)	Robot vacuum navigating around moving obstacles			
	Goal-Based Agent	Rational by choosing actions aimed at achieving defined goals	High (stores model and goals)	Can handle dynamic and partially observable environments with goal evaluation	High (requires planning and search algorithms)	Virtual assistant scheduling appointments based on user goals			
	Utility-Based Agent	Rational by selecting actions that maximize utility or satisfaction	Very High (tracks model, goals, and utility)	Best suited for complex, dynamic, and partially observable environments	Very High (requires optimization algorithms)	Self-driving car ensuring safety, efficiency, and passenger comfort			
4b 3	With the help of examples describe the potential causes and solutions of model overfitting in decision trees. 1. Overfitting Due to Presence of Noise 2. Overfitting Due to Lack of Representative Samples 3. High model complexity (Multiple Comparison Procedure) 2.5*2+3=8M						**08**	L2	CO1

****

BT-Blooms Taxonomy, CO-Course Outcomes

Marks Distribution	Particulars		CO1	CO2	CO3	CO4	CO5	L1	L2	L3	L4	L5	L6
	Test	Max Marks	42	18				2	12	46			

Scanned with OKEN Scanner

Gini Index

I

$$Gini(Price(low)) = 1-\left(\frac{2}{4}\right)^2-\left(\frac{2}{4}\right)^2 = 1-0.25-0.25 = 0.5$$

$$Gini(Price(med)) = 1-\left(\frac{2}{4}\right)^2-\left(\frac{2}{4}\right)^2 = 0.5$$

$$Gini(Price(high)) = 1-\left(\frac{2}{3}\right)^2-\left(\frac{1}{3}\right)^2 = 1-0.44-0.11 = 0.45$$

$$Gini\ Index(Price) = \frac{4}{11}*0.5 + \frac{4}{11}*0.5 + \frac{3}{11}*0.45$$

$$= 0.181 + 0.181 + 0.1227$$

$$= \underline{0.484}$$

II

$$Gini(Maintainance(low)) = 1-\left(\frac{2}{2}\right)^2-\left(\frac{0}{2}\right)^2 = 0$$

$$Gini(Maintainance(med)) = 1-\left(\frac{2}{4}\right)^2-\left(\frac{2}{4}\right)^2 = 0.5$$

$$Gini(Maintainance(high)) = 1-\left(\frac{3}{5}\right)^2-\left(\frac{2}{5}\right)^2$$

$$= 1-0.36-0.16 = 0.48$$

$$Gini\ Index(Maintainance) = \frac{2}{11}*0 + \frac{4}{11}*0.5 + \frac{5}{11}*0.48$$

$$= 0.181 + 0.218 = \underline{0.399}$$

III.

$$Gini(\text{airbag}(yes)) = 1-\left(\frac{3}{6}\right)^2-\left(\frac{3}{6}\right)^2 = 0.5$$

$$Gini(airbag(no)) = 1-\left(\frac{3}{5}\right)^2-\left(\frac{2}{5}\right)^2 = 0.48$$

$$Gini(airbag) = \frac{6}{11}*0.5 + \frac{5}{11}*0.48 =$$

$$= 0.27 + 0.218 = \underline{0.488}$$

Scanned with OKEN Scanner

Capacity	Profitable.	
2	Yes.	2
2	NO	
2	NO.	
4	NO	4
4	Yes	
4	NO.	
4	NO	4.
4	Yes.	
4	Yes.	
5	Yes.	
5	Yes.	

$$\text{Gini}(\text{Capacity}(2)) = 1 - \left(\frac{1}{3}\right)^2 - \left(\frac{2}{3}\right)^2 = 0.78 \quad 0.44$$

$$\text{Gini}(\text{Capacity}(4)) = 1 - \left(\frac{3}{6}\right)^2 - \left(\frac{3}{6}\right)^2 = 0.5$$

$$\text{Gini}(\text{Capacity}(5)) = 1 - \left(\frac{0}{2}\right)^2 - \left(\frac{2}{2}\right)^2 = 0.$$

$$\text{Gini Indp}(\text{Capacity}) = \frac{3}{11} * 0.78 + \frac{6}{14} * 0.5$$

$$= 0.212 + 0.2727$$

$$= 0.4847 \quad 0.39$$

Scanned with OKEN Scanner

2b

Record.	Age	Purchased (Yes/No)	
1	22	NO	23.5
2	25	Yes	
3	28	Yes	31.5
4	35	NO	37.5
5	40	Yes	

$$\text{Gini}(<23.5) = 1-\left(\frac{1}{1}\right)^2-\left(\frac{0}{1}\right)^2 = 0$$

I $$\text{Gini}(\geq 23.5) = 1-\left(\frac{3}{4}\right)^2-\left(\frac{1}{4}\right)^2 =$$

$$= 1-0.562-0.0625 = \underline{0.375}$$

$$\text{Gini Index (Split Pt (23.5))} = \frac{1}{5}*0+\frac{4}{5}*0.375 = 0.3$$

II $$\text{Gini}(<31.5) = 1-\left(\frac{2}{3}\right)^2-\left(\frac{1}{3}\right)^2$$

$$= 1-0.044-0.11 = \underline{0.45}$$

$$\text{Gini}(\geq 31.5) = 1-\left(\frac{1}{2}\right)^2-\left(\frac{1}{2}\right)^2 = \underline{0.5}$$

$$\text{Gini Index (Split Pt (31.5))} = \frac{3}{5}*0.45+\frac{2}{5}*0.5$$

$$= 0.27+0.2$$

$$= 0.47$$

III $$\text{Gini}(<37.5) = 1-\left(\frac{2}{4}\right)^2-\left(\frac{2}{4}\right)^2 = 0.5$$

$$\text{Gini}(\geq 37.5) = 0.$$

$$\text{Gini Index (Split Pt (37.5))} = \frac{4}{5}*0.5 = 0.47$$

Scanned with OKEN Scanner

CIE - I

Date: 26-11-24

Scheme and Solutions

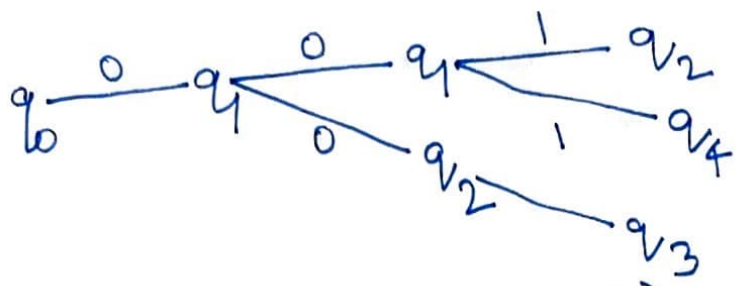
Subject : TOC

Sub. Code: CS354TA

Marks : 60

PART- A

1.0 $\delta^*(q_0, 001)$



q_4 – final state ∴ accept — 2

2.0 ϵ-closure({3, 5, 12})

$= \epsilon$-closure(3) ∪ ϵ-closure(5) ∪ ϵ-closure(12)

= {3, 6, 7, 8, 10} ∪ {5, 6, 7, 8, 10} ∪ {1, 2, 4, 12, 13} — 2

= {1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13} — 1

3.0 i) aba or any other string — 1

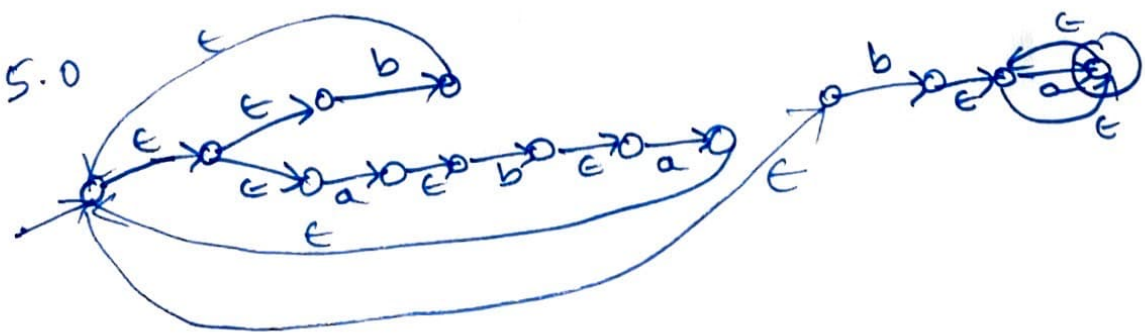
ii) b or any other string

4.0 L = {ab, ac, c}, $L \cdot L = L^2$ = {abab, abac, abc, acab, acac, acc, cab, cac, cc}

$L^2 \cdot L = L^3$ = {ababab, ababac, ababc, abacab, abacac, abacc, abcab, abcac, abcc, acabab, acabac, acabc, acacab, acabac, acacc, accab, accac, accc, cabab, cabac, cabc, cacab, cacac, cacc, ccab, ccac, ccc} — 2

$L^4 = L^3 \cdot L$ = { . . . } $|L^4| = 81$.

5.0



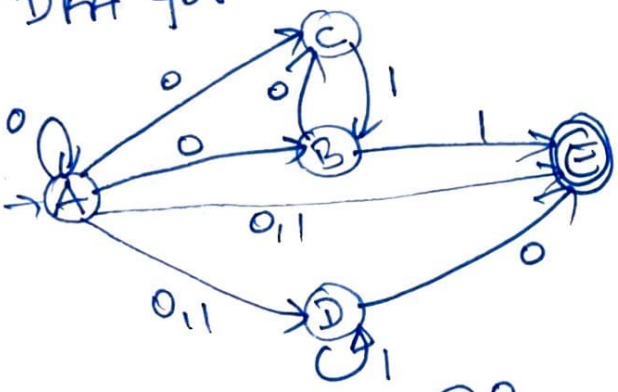
— 2

PART - B

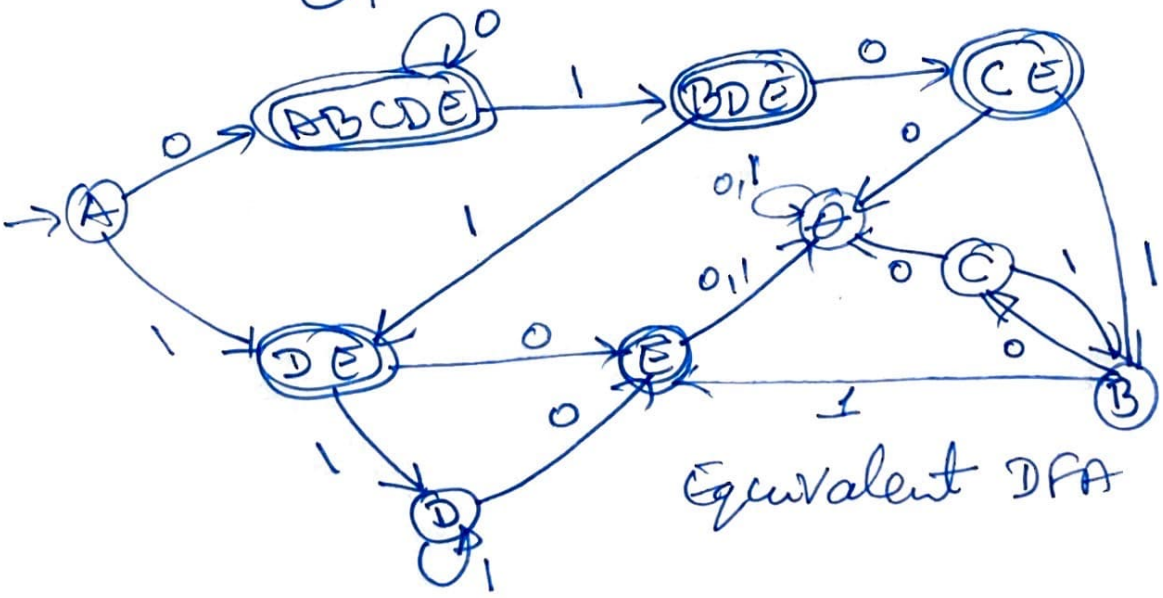
1.a Definition of regular expression — 2
R.E for (i) — 2
R.E for (ii) — 2

1.b ε-NFA definition — 1
Extended transition fn of ε-NFA — 2
Language acceptance of ε-NFA — 1

2. Equivalence of ε-NFA to NFA — 2
Equivalence of NFA to DFA — 2
Equivalent NFA for the given ε-NFA — 3
DFA for the NFA found — 3



Equivalent NFA.



Equivalent DFA

3.a) i) Equivalent DFA for $(a+b)^* ab (a+b)^*$ — 2

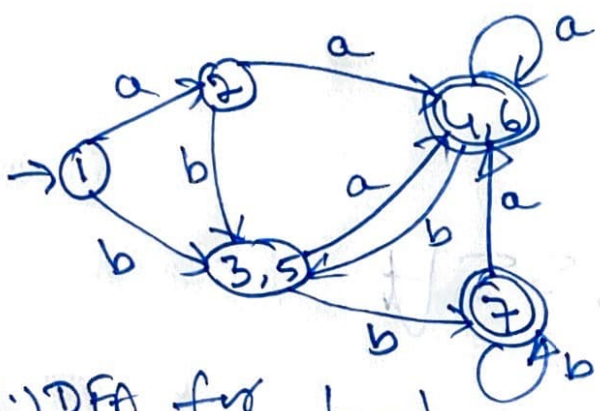
ii) Equivalent DFA for $(a+b)^* (ab + bba)$ — 2

3.b

	1	2	3	4	5	6
2	✓					
3	✓	✓				
4	✓	✓	✓			
5	✓	✓		✓		
6	✓	✓	✓		✓	
7	✓	✓	✓	✓	✓	✓

— 4

$3 \equiv 5$ & $4 \equiv 6$



— 2

4.a) i) DFA for $L_1 - L_2$ — 2

ii) DFA for $L_1 \cap L_3$ — 2

iii) DFA for $L_2 \cup L_3$ — 2

4.b) Decision algorithm for (i) — 2

Decision algorithm for (ii) — 2

5.a) pumping lemma statement — 1
proof of the lemma — 2
To show the given language is not regular — 3

5.b) a) NO. It won't work — 1
example — 1

b) NO. It won't work — 1
example. — 1

TOC CIE-1:

PART A-

Q1. $\delta^*(q_0, 001)$.

$\delta^*(\delta(q_0, 0), 01)$

$\delta^*(q_1, 01)$

$\delta^*(\delta(q_1, 0), 1)$.

$\delta^*((q_1, q_2), 1)$

~~$\delta^*(\delta(q_1, 1)$~~

$\delta(q_1, 1) \cup \delta(q_2, 1)$.

$\{q_2, q_3, q_4\}$.

Q2. ε-closure $(3) = \{3, 6, 7, 8, 10\}$

ε-closure $(5) = \{5, 6, 7, 8, 10\}$

ε-closure $(12) = \{12, 13, 1, 2, 4\}$.

$\therefore$ ε-closure $(3, 5, 12) = \{1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13\}$.

Q3. i) bbbaa.

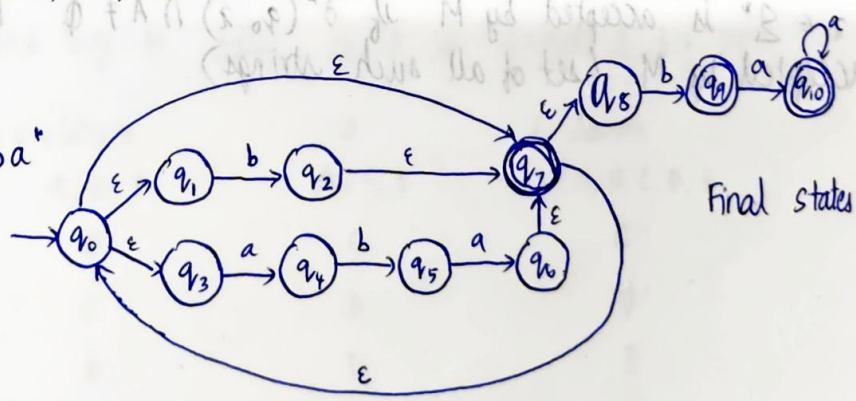
ii) a.

Q4. $L^2 = \{ab, ac, c, abac, abc, acc, acab, cab, cac\}$.

$L^4 = (L^2)^2 = \{ab, ac, c, \ldots\ldots$ 81 elements.

Q5. $(b+aba)^* ba^*$.

For $(b+aba)^* ba^*$



Final states: q_9, q_{10}.

PART-B:

Q1.

a) Regular expression is recursively defined as the formula for expressing regular languages. If Σ is an alphabet, the set R of regular languages if the language ϕ is an element of R and for every $a \in \Sigma$, $\{a\}$ is in R. For any 2 languages L_1, L_2 in R, $L_1 + L_2$, $L_1 L_2$ and L_1^* is in R.

i) $(0+1)^* (00+10+11) + 0 + 1 + \varepsilon$.

ii) $(1+01)^* (0+\varepsilon)$.

Q1.

b) 5-tuple machine: $M = (Q, \Sigma, \delta, q_0, F)$.

Q: set of all states (finite, non-empty).

Σ: alphabet (finite set).

q_0: start states

F: set of final states.

δ: transition function.

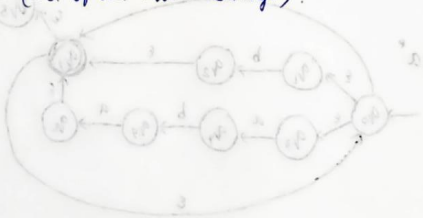
Extended transition function - $\delta^* : Q \times \Sigma^* \to 2^Q$.

For every $q \in Q$, $\delta^*(q, \varepsilon) = \varepsilon$-closure$(q)$.

For every $q \in Q$ and $y \in \Sigma^*$, $\sigma \in \Sigma$:

$$\delta^*(q, y\sigma) = \varepsilon\text{-closure}\left(\bigcup \delta(p, \sigma) \mid p \in \delta^*(q, y)\right)$$

A string $x \in \Sigma^*$ is accepted by M if $\delta^*(q_0, x) \cap A \neq \phi$ language L(M) is thus accepted by M. (set of all such strings).



Q2. ε-NFA: $M = (Q, \Sigma, q_0, A, \delta)$.

DFA: $M_1 = (Q_1, \Sigma, q_1, A_1, \delta_1)$.

$Q_1 = 2^Q$.

Initial state q_1 of Q_1 is $\{q_0\}$.

For every $q \in Q_1$, every $\sigma \in \Sigma$,

$$\delta_1(q, \sigma) = \bigcup \{\delta(p, \sigma) \mid p \in q\}.$$

$$A_1 = \{q \in Q_1 \mid q \cap A \neq \phi\}$$

They accept the same language only if for every $x \in \Sigma^*$,

$$\delta_1^*(q_1, x) = \delta^*(q_0, x).$$

when $x = \varepsilon$, $\delta_1^*(q_1, x) = \delta_1^*(q_1, \varepsilon) = q_1 = \{q_0\}$
$= \delta^*(q_0, \varepsilon) = \delta^*(q_0, x)$.

Base case of induction satisfied.

Assume for x, $\delta_1^*(q_1, x) = \delta^*(q_0 x)$. For every $\sigma \in \Sigma$,

To prove: $\delta_1^*(q_1, x\sigma) = \delta^*(q_0, x\sigma)$.

$$\begin{aligned}
\delta_1^*(q_1, x\sigma) &= \delta_1(\delta_1^*(q_1, x), \sigma) \\
&= \delta_1(\delta^*(q_0, x), \sigma) \\
&= \bigcup \{\delta(p, \sigma) \mid p \in \delta^*(q_0, x)\} \\
&= \delta^*(q_0, x\sigma).
\end{aligned}$$

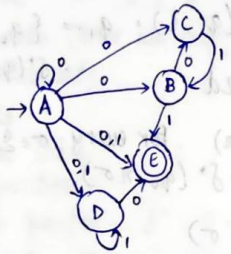
$\therefore$ x is accepted by M_1 only if it is accepted by M.

	ε-closure	0	ε-closure
A	A, B, D	A, C, E	A, B, C, D, E
B	B	C	C
C	C	ϕ	ϕ
D	D	E	E
E	E	ϕ	ϕ

	ε-closure	1	ε-closure
A	A, B, D	D, E	D, E
B	B	E	E
C	C	B	B
D	D	D	D
E	E	ϕ	ϕ

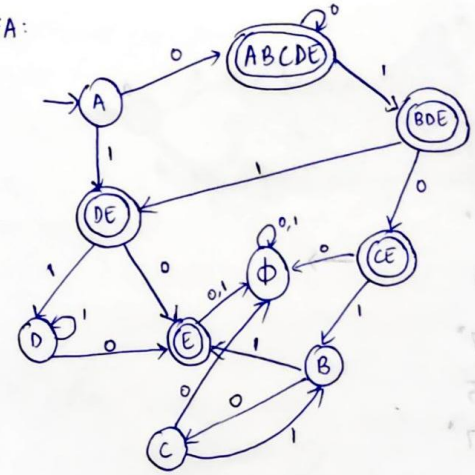
	0	1
→ A	A, B, C, D, E	D, E
B	C	E
C	ϕ	B
D	E	D
* E	ϕ	ϕ

NFA:



	0	1
→ A	ABCDE	DE
* ABCDE	ABCDE	BDE
* BDE	CE	DE
* CE	ϕ	B
* DE	E	D
B	C	E
* E	ϕ	ϕ
C	ϕ	B
D	E	D
ϕ	ϕ	ϕ

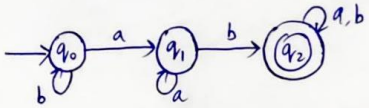
DFA:



Q3. DFA:

a)

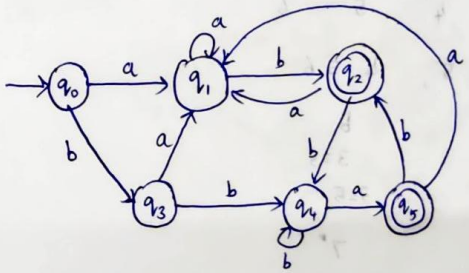
i)



Q3.

a)

ii)



Q3.

b)

	a	b
→ 1	2	3
2	4*	5
3	6*	7*
4*	4*	5
5	6*	7*
6*	4*	5
7*	6*	7*

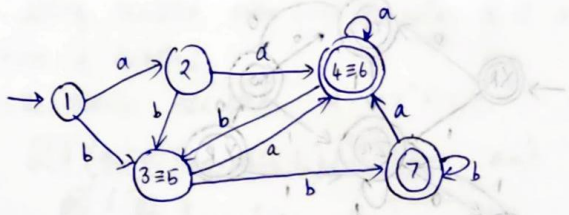
2	×				
3	×	×			
4*	×	×	×		
5	×	×		×	
6*	×	×	×		×
7*	×	×	×	×	×	×
	1	2	3	4*	5	6*

$\therefore$ $3 \equiv 5$, $4 \equiv 6$.

Table:

	a	b
→ 1	2	$3 \equiv 5$
2	$4^* \equiv 6^*$	$3 \equiv 5$
$3 \equiv 5$	$4^* \equiv 6^*$	7*
$4^* \equiv 6^*$	$4^* \equiv 6^*$	$3 \equiv 5$
7*	$4^* \equiv 6^*$	7*

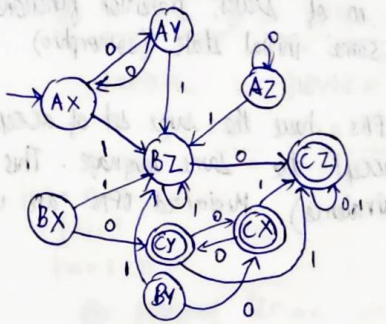
TD:



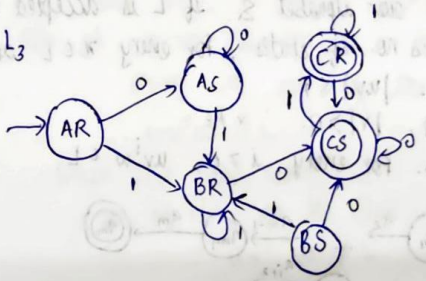
Q4.

a)

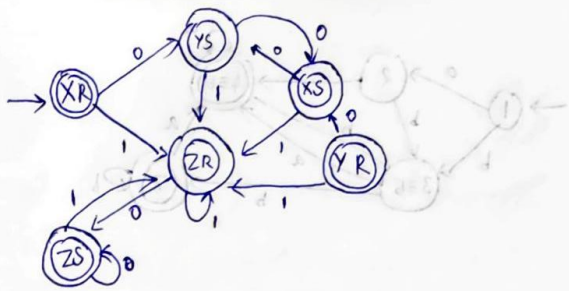
a) $L_1 - L_2$



b) $L_1 \cap L_3$



c) $L_2 \cup L_3$

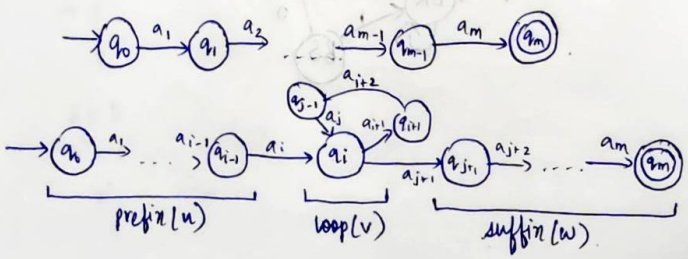


Q4. b) i) Both minimized DFA's of the DFA M and regular expression converted should have same no. of states, transition functions, same set of accepting states and same initial state. (isomorphic).

ii) If it's equivalent minimized DFAs have the same set of accepting states for given values, then they accept the same language. This is an NP-complete decision problem. (equivalence). Minimized DFAs are isomorphic.

Q5.

a) Suppose L is a language over alphabet Σ. If L is accepted by machine $M = (Q, \Sigma, q_0, A, \delta)$, n is no. of states, for every $x \in L$ and $|x| \geq n$, $x = uvw$ such that:
1. $|uv| \leq n$.
2. $|v| > 0$. $v \neq \varepsilon$.
3. For every $i \geq 0$, $uv^iw \in L$.



Minimum string accepted when $i = 0$ is $uv^0w = uw$ as it reaches q_m.

$i = 1$, uvw is accepted.

when $i = 2$, uvvw accepted as $uv^iw \in L$.

$\delta(\delta(q_0, a_1 a_2 \ldots a_{i-1} a_i), a_{j+1}, a_{j+2} \ldots a_m)$

$\delta(\delta(q_i, a_{j+1}, a_{j+2} \ldots a_m))$.

$\delta(q_k, a_{k+1}, \ldots a_m)$.

q_m. Thus, uv^iw is accepted. Hence, proved.

ww or ww^r is not regular.

$$x = \overbrace{\underbrace{1\ldots1}_{n}\ \underbrace{0\ldots0}_{n}}^{w}\ \overbrace{\underbrace{0\ldots0}_{n}\ \underbrace{1\ldots1}_{n}}^{w^r}$$

$|x| \geq n$, let $|uv| \leq n$ $|v| \geq 1$.

$$x = \underbrace{1\ldots}_{u}\ \underbrace{1}_{v}\ \underbrace{0\ldots0\,0\ldots01\ldots1}_{w}$$

$|u| = n - 1$.

$|v| = 1$.

$|uv| = n$.

For pumping lemma $uv^iw \in L$.

when $i = 0$, v doesn't appear.

$\therefore$ No. of zeros on left is 1 less than on the right

$\therefore$ string is not of the form ww^r.

$\therefore uv^0w \notin L$

When $i = 2$ and more,

no. of 1's on the left increases more than right

$\therefore uv^{i \geq 2}w \notin L$.

Similarly for ww:

Q5.

a) ~~No~~.

$$x = \overbrace{\underbrace{1\ldots1}_{n}\underbrace{0\ldots0}_{n}}^{w}\ \overbrace{\underbrace{1\ldots1}_{n}\underbrace{0\ldots0}_{n}}^{w}$$

$$x = \underbrace{1\ldots1\,0\ldots}_{u}\ \underbrace{0}_{v}\ \underbrace{1\ldots1\,0\ldots0}_{w} \rightarrow \underbrace{1\ldots1}_{u}\underbrace{0}_{v}\underbrace{0\ldots0\,1\ldots10\ldots0}_{w}$$

$|uv| = n$.

$|v| \geq 1$

when $i=0$, v doesn't appear

1's on left less than right.

$ww \notin L$.

when $i \geq 2$, 1's on left increases.

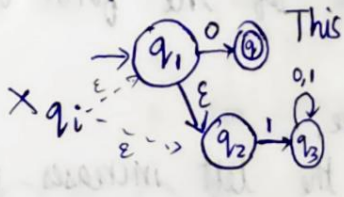
$ww \notin L$.

$\therefore$ ww and $ww^r \notin L$

The language is not regular.

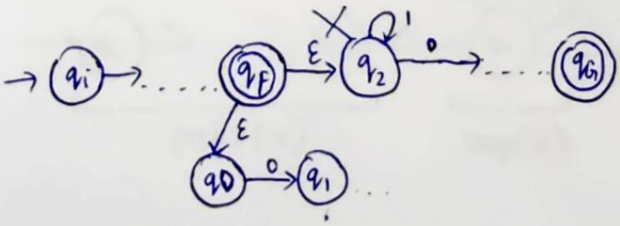
Q5.

b) a) No.



This doesn't work as ε-transition is only from q_i to q_1 and q_2 respectively. There is no ε-transition from q_1 to q_2.

b) No.



If we merge the two states, the ε-closure of the states will change and may accept wrong strings.

TOC - Retest Paper - CS354TA

PART-A

1.1 $r = 0^* + 1^*$, $s = 01^* + 10^* + 1^*0 + (0^*1)^*$, $t = 1^*(01)^*0^*$

a) str. of min. length not in language corresponding to R.E 't' (excluding ϵ).

$\Rightarrow$ 001, 011

b) corresponding to 's' not in 't'

$\Rightarrow$ 001, 011,

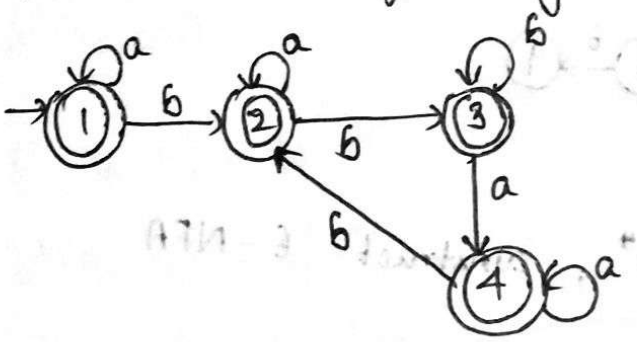
c) Both r and s

$\Rightarrow \epsilon, 0, 1,$

d) neither 'r' and 's'

$\Rightarrow$ 101, 010

1.2 Minimize the following DFA



When all states in a DFA are accepting, the minimized DFA will always have a single state with self-loops for all inputs

$\therefore$

where $q_f = \{1, 2, 3, 4\}$

$\therefore$ No of states = 1

1.3 Deterministic Finite Automata

- A DFA is defined by the 5-tuple:-

$$\{Q, \Sigma, q_0, F, \delta\}$$

where

$Q \Rightarrow$ a finite set of states

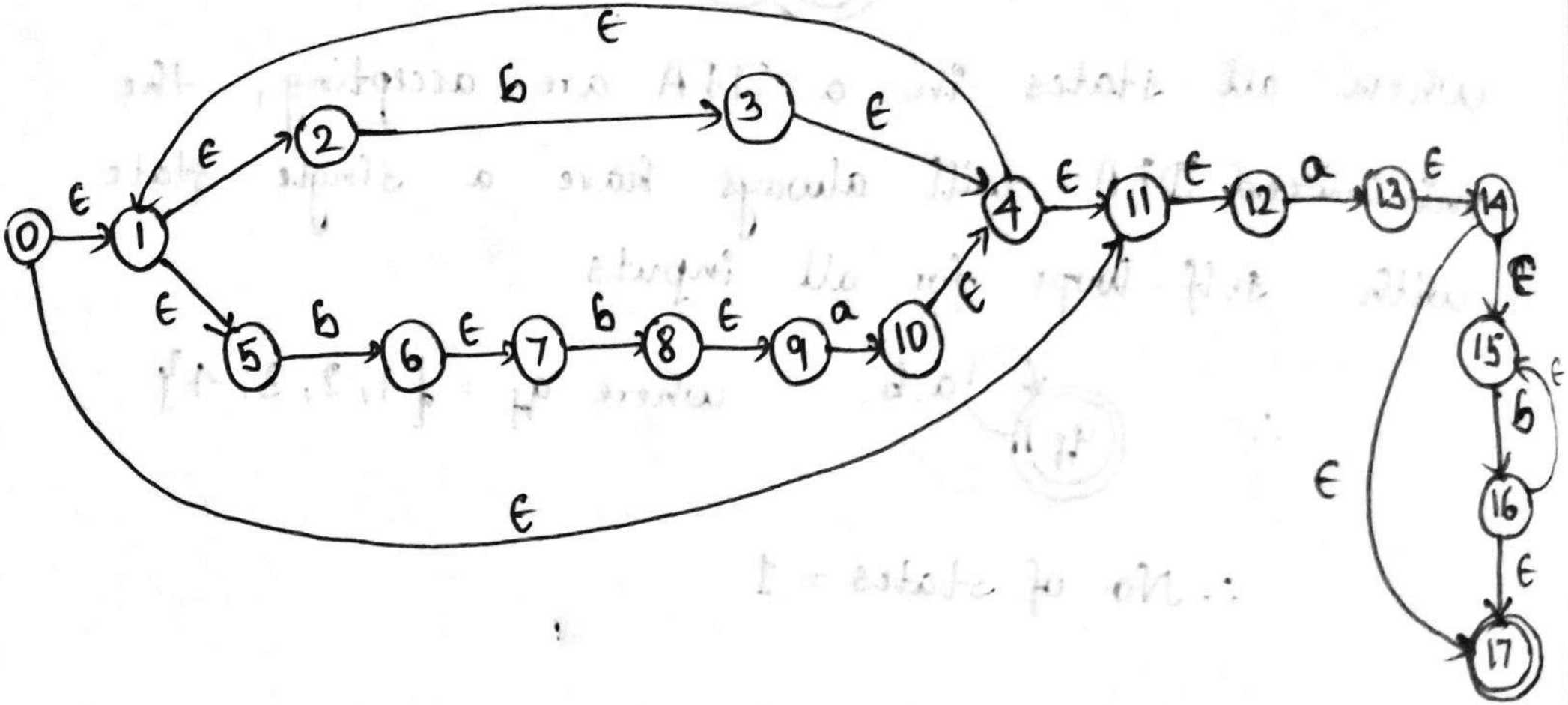
$\Sigma \Rightarrow$ a finite set of i/p symbols [alphabet]

$q_0 \Rightarrow$ start state

$F \Rightarrow$ set of accepting states

$\delta \Rightarrow$ transition function which is a mapping between $Q \times \Sigma \Rightarrow Q$

1.4 $R = (b + bba)^* ab^*$, construct ϵ-NFA

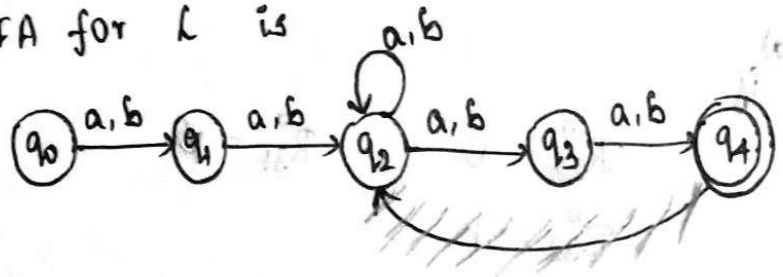


1.5 $L = \{vwv : v, w \in \{a,b\}^*, |v| = 2\}$ is regular

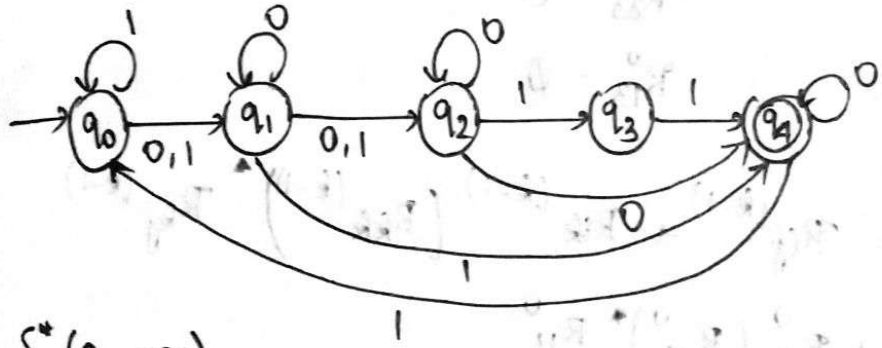
$\Rightarrow$ If we can come up with

- DFA
- NFA
- Regular Expression, for some Language L, then L is regular

$\therefore$ NFA for L is



1.6



$\delta^*(q_0, 001)$

$\delta^*(q_0, \epsilon) = q_0$

$\delta^*(q_0, 0) = \delta(\delta^*(q_0, \epsilon), 0) = \delta(q_0, 0) = q_1$

$\delta^*(q_0, 00) = \delta(\delta^*(q_0, 0), 0) = \delta(q_1, 0) = \{q_1, q_2\}$

$\delta^*(q_0, 001) = \delta(\delta^*(q_0, 00), 1) = \delta(q_1, 1) \cup \delta(q_2, 1)$

$= \{q_2, q_4\} \cup \{q_3\}$

$= \{q_2, q_4, q_3\}$

1.7 Two decision properties of Regular Languages

i) Emptiness test

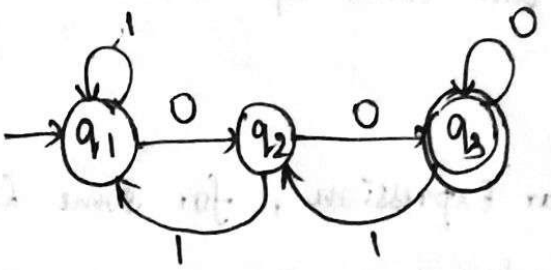
ii) Membership test

iii) Finiteness test

PART - B

2) DFA

	0	1
$\rightarrow q_1$	q_2	q_1
q_2	q_3	q_1
$* q_3$	q_3	q_2



⇒ transition diagram

a) R.E of $R^{(0)}_{ij}$

$R^0_{11} = 1$ $\quad R^0_{23} = 0$ $\quad R^0_{31} = \emptyset$

$R^0_{12} = 0$ $\quad R^0_{32} = 1$

$R^0_{21} = 1$ $\quad R^0_{33} = 0$

$R^0_{22} = \epsilon$ $\quad R^0_{13} = \emptyset$

b) $R_{ij}^{(k)} = R_{ij}^{(k-1)} + R_{ik}^{(k-1)} \left(R_{kk}^{(k-1)}\right)^* R_{kj}^{(k-1)}$

$R^1_{11} = R^0_{11} + R^0_{11} (R^0_{11})^* R^0_{11}$

$= 1 + 1(1)^* 1 = 11^*$

$R^1_{12} = R^0_{12} + R^0_{11} (R^0_{11})^* R^0_{12}$

$= 0 + 1(1)^* 0 = 1^* 0$

$R^1_{21} = R^0_{21} + R^0_{21} (R^0_{11})^* R^0_{11}$

$= 1 + 1(1)^* 1 = 11^*$

$R^1_{22} = R^0_{22} + R^0_{21} (R^0_{11})^* R^0_{12}$

$= \epsilon + 1(1)^* 0 = \epsilon + 1(1)^* 0$

$R^1_{23} = R^0_{23} + R^0_{21} (R^0_{11})^* R^0_{13}$

$= 0 + 1(1)^* \emptyset = 0$

$R^1_{32} = R^0_{32} + R^0_{31} (R^0_{11})^* R^0_{12} = 1 + \emptyset(\cdots)$

$= 1$

$$R_{33}^{1} = R_{33}^{0} + R_{31}^{0}\left(R_{11}^{0}\right)^{*} R_{13}^{0}$$

$$= 0 + \emptyset\,(\cdots)$$

$$= 0$$

$$R_{13}^{1} = R_{13}^{0} + R_{11}^{0}\left(R_{11}^{0}\right)^{*} R_{13}^{0}$$

$$= \emptyset + 1\,(1)^{*}\,\emptyset \quad = \emptyset$$

$$R_{31}^{1} = R_{31}^{0} + R_{31}^{0}\left(R_{11}^{0}\right)^{*} R_{11}^{0}$$

$$= \emptyset + \emptyset\,(\cdots) \quad = \emptyset$$

c) Regular expression for language

$$= R_{13}^{3} = R_{13}^{2} + R_{13}^{2}\left(R_{33}^{2}\right)^{*} R_{33}^{2}$$

$$R_{13}^{2} = R_{13}^{1} + R_{12}^{1}\left(R_{22}^{1}\right)^{*} R_{23}^{1}$$

$$= \emptyset + 1^{*}0\,(\epsilon + 1(1)^{*}0)^{*}\,0$$

$$= 1^{*}0\,(1(1)^{*}0)^{*}\,0$$

$$R_{33}^{2} = R_{33}^{1} + R_{32}^{1}\left(R_{22}^{1}\right)^{*} R_{23}^{1}$$

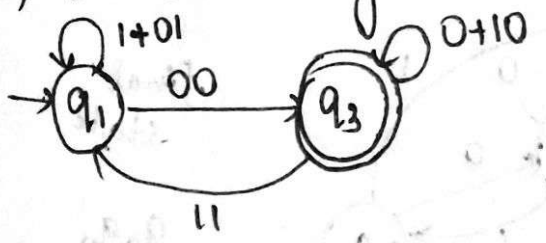
$$= 0 + 1\,(\epsilon + 1(1)^{*}0)^{*}\,0$$

$$= 0 + 1\,(1(1)^{*}0)^{*}\,0$$

$$\therefore R_{13}^{3} = 1^{*}0(1(1)^{*}0)^{*}0 + 0 + 1(1(1)^{*}0)^{*}0$$

$$= 0 + (1^{*}0 + 1)(1(1)^{*}0)^{*}0$$

d) On eliminating state 2



$R = 1 + \epsilon + 01$

$S = 00$

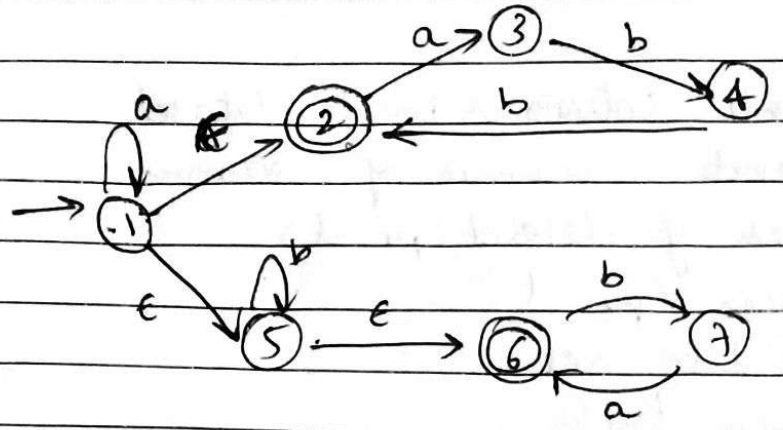
$U = 0 + \epsilon + 10$

$T = 11$

$$R.E = (R + SU^{*}T)^{*}SU^{*} = \left(\left(\begin{matrix}1+\epsilon\\+01\end{matrix}\right) + (00)(0+10+\epsilon)^{*}11\right)^{*}00\,(0+10+\epsilon)^{*}$$

$$= \left((1+01+\epsilon) + 00(0+10)^{*}11\right)^{*}00\,(0+10)^{*}$$

3)



ⓐ find closure of each state

$\epsilon\text{-close}(1) = \{1, 2, 5, 6\}$
$\epsilon\text{-close}(2) = \{2\}$
$\epsilon\text{-close}(3) = \{3\}$
$\epsilon\text{-close}(4) = \{4\}$
$\epsilon\text{-close}(5) = \{5, 6\}$
$\epsilon\text{-close}(6) = \{6\}$
$\epsilon\text{-close}(7) = \{7\}$

ⓑ ε-NFA to DFA

$\epsilon\text{-close}(1) = \{1, 2, 5, 6\} \Rightarrow$ start state
$\delta_d(\{1,2,5,6\}, a) = \epsilon\text{-close}(1, 3) = \{1, 2, 3, 5, 6\}$
$\delta_d(\{1,2,5,6\}, b) = \epsilon\text{-close}(5, 7) = \{5, 6, 7\}$
$\delta_d(\{1,2,3,5,6\}, a) = \epsilon\text{-close}(1, 3) = \{1, 2, 3, 5, 6\}$
$\delta_d(\{1,2,3,5,6\}, b) = \epsilon\text{-close}(4, 5, 7) = \{4, 5, 6, 7\}$
$\delta_d(\{5,6,7\}, a) = \epsilon\text{-close}(6) = 6$
$\delta_d(\{5,6,7\}, b) = \epsilon\text{-close}(5, 7) = \{5, 6, 7\}$
$\delta_d(\{4,5,6,7\}, a) = \epsilon\text{-close}(6) = \{6\}$
$\delta_d(\{4,5,6,7\}, b) = \epsilon\text{-close}(2, 5, 7) = \{2, 5, 6, 7\}$
$\delta_d(6, a) = \phi$
$\delta_d(6, b) = \epsilon\text{-close}(7) = 7$
$\delta_d(\{2,5,6,7\}, a) = \epsilon\text{-close}(3, 6) = \{3, 6\}$
$\delta_d(\{2,5,6,7\}, b) = \epsilon\text{-close}(5, 7) = \{5, 6, 7\}$
$\delta_d(7, a) = 6$
$\delta_d(7, b) = \phi$

$\delta_d(\{3,6\}, a) = \phi$

$\delta_d(\langle 3,6\}, b) = \epsilon\text{-close}(4,7) = \langle 4,7\}$

$\delta_d(\langle 4,7\}, a) = \epsilon\text{-close}(6) = 6$

$\delta_d(\langle 4,7\}, b) = \epsilon\text{-close}(2) = 2$

$\delta_d(2, a) = 3$

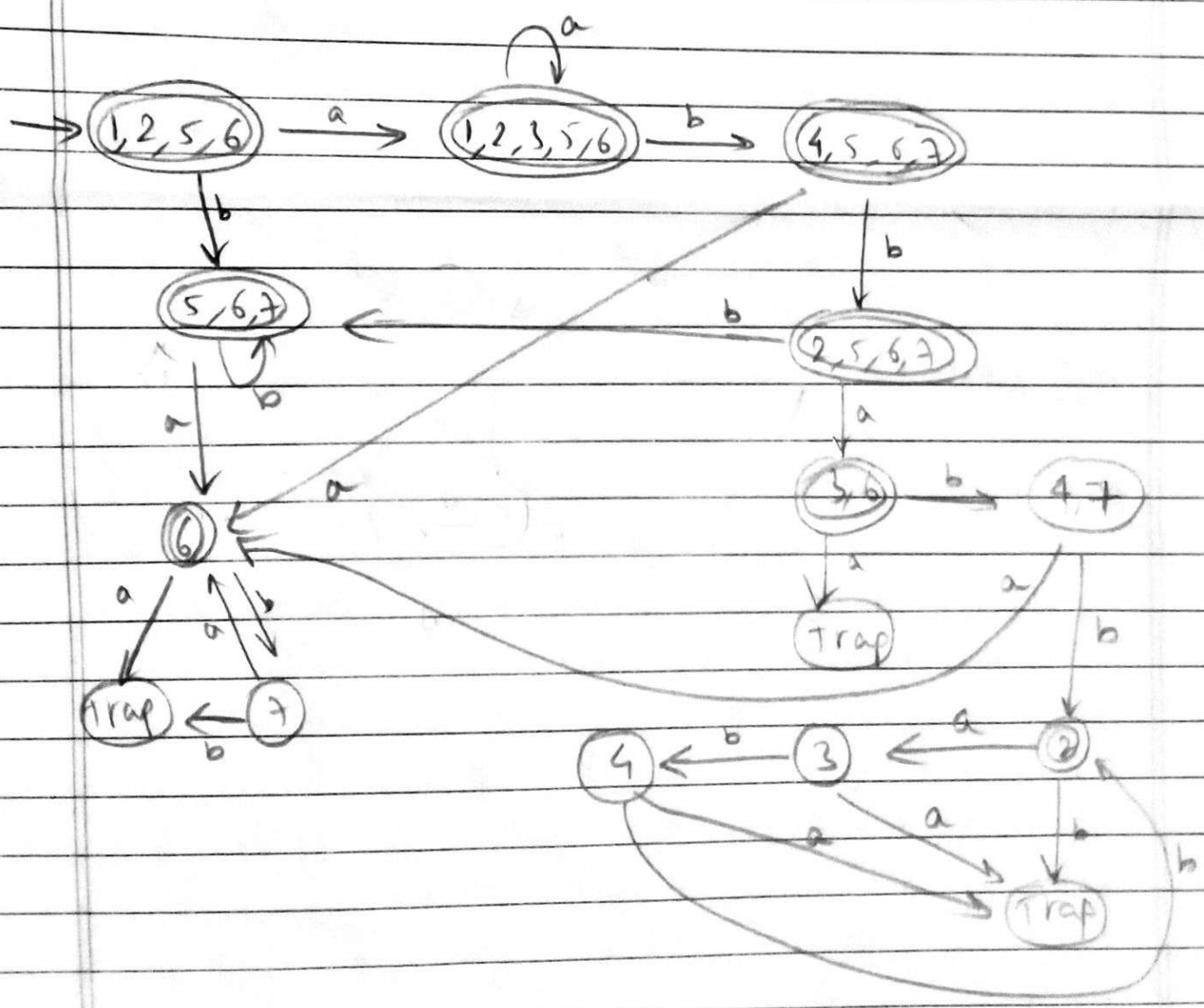
$\delta_d(2, b) = \phi$

$\delta_d(3, a) = \phi$

$\delta_d(3, b) = 4$

$\delta_d(4, a) = \phi$

$\delta_d(4, b) = 2$



4)

a) <u>Pumping Lemma</u>

- It is a property of all regular languages and a technique that is used to show that a given language is not regular.

- <u>Theorem</u> - Let L be a regular language - there exists some constant N, such that for every string $w \in L$, $|w| \geq N$, there exists a way to ~~shee~~ break w into 3 parts,

  $w = xy^{k}z$ such that

  i) $y \neq \epsilon$ ii) $|xy| \leq N$ iii) for all $k \geq 0$, all strings of the form $xy^{k}z \in L$

- This property should hold for all regular languages. N is called 'Pumping Lemma Constant'

Purpose:- To prove some languages cannot be regular

eg:- $L = \{a^n b^n \mid n \geq 0\}$

Proof: i) Let L be regular

ii) so $y \neq \epsilon$, $|y| \geq 1$

Let $M = xy^i z$, $|xy| \leq n$

$i = 0, 1, \ldots$

where $x = a$

$y = a$

$z = a^{n-2} b^n$

Let $i = 0$: $M = a a^i a^{n-2} b^n$

$= a a^{n-2} b^n = a^{n-1} b^n$

We know that $a^{n-1} b^n \notin a^n b^n$

$M \notin L$

$\therefore$ L is not a regular language

$\therefore$ Hence proved by pumping lemma

4.6) Applications of Regular Expression:-

i) In compiler design, it is used for lexical analysis Ex:- To identify and extract tokens (eg:- keywords, identifiers) from code.

ii) Regular expression is used in Data Extraction and Parsing. Ex:- extracting names, addresses/dates from a document

iii) Regular expression is used in network security significantly. Ex:- pattern matching with network traffic logs, to detect common type of malicious payload in network traffic

iv) Command line operations. Ex:- 'grep' commond supports regular exp. to filter & extract specific lines from files

5. * 2 states p & q of a DFA are said to be <u>Indistinguishable</u> if, for all $w \in \Sigma^*$ (w is a string);

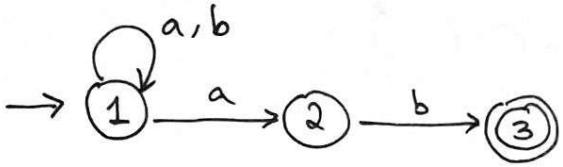
$\delta^*(p, w) \in F$ implies $\delta^*(q, w) \in F$

$\delta^*(p, w) \notin F$ implies $\delta^*(q, w) \notin F$

* 2 states p & q of a DFA are said to be <u>'Distinguishable'</u> by a string 'w' if there exists some string $w \in \Sigma^*$ such that $\delta^*(p, w) \in F$ and $\delta^*(q, w) \notin F$ or vice versa.

Given: NFA

To obtain: Minimised DFA.



$\Sigma = \{a, b\}$

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

δ_N	a	b
→ 1	{1, 2}	{1}
2	ϕ	{3}
* 3	ϕ	ϕ

To DFA by Lazy creation of subsets:

$\delta_D(1, a) = \{1, 2\}$

$\delta_D(1, b) = \{1\}$

$\delta_D(\{1,2\}, a) = \delta_N(1, a) \cup \delta_N(2, a) = \{1, 2\}$

$\delta_D(\{1,2\}, b) = \delta_N(1, b) \cup \delta_N(2, b) = \{1, 3\}$

$\delta_D(\{1,3\}, a) = \{1, 2\}$

$\delta_D(\{1,3\}, b\} = \{1\}$

So,

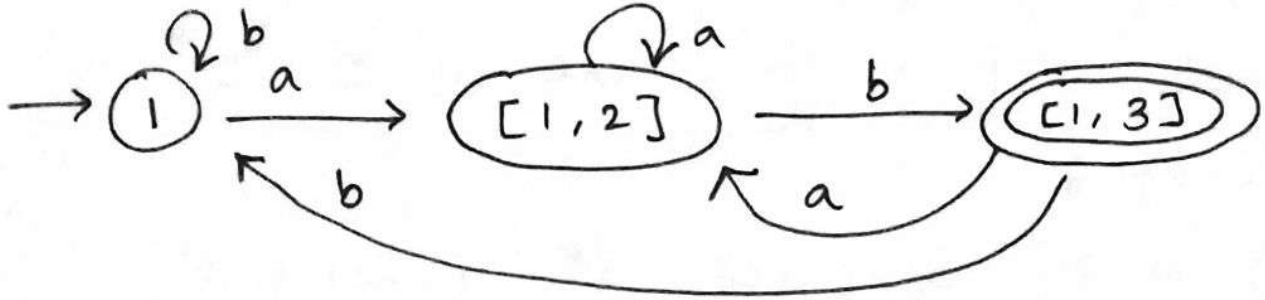
δ_D	a	b
→ 1	{1, 2}	{1}
{1, 2}	{1, 2}	{1, 3}
* {1, 3}	{1, 2}	{1}

So, equivalent DFA:

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

$F = \{(1,3)\}$

$q_0 = \{1\}$



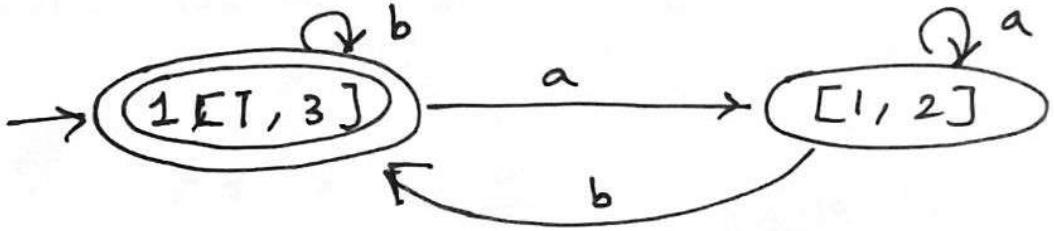
Minimization of DFA:

δ_D	a	b
→ 1	{1, 2}	{1}
{1, 2}	{1, 2}	{1, 3}
* {1, 3}	{1, 2}	{1}

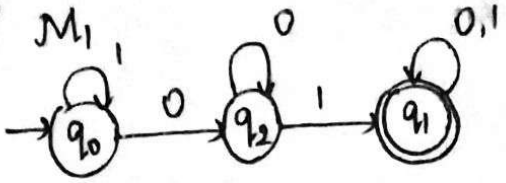
	1	{1,2}	{1,3}
1	=		
{1,2}	×	=	
{1,3}	=	×	=

States '1' & '{1, 3}' are indistinguishable

∴ Minimized DFA:

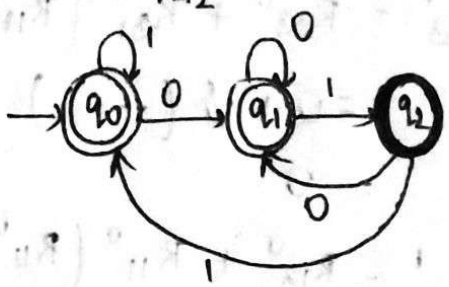


6) M_1



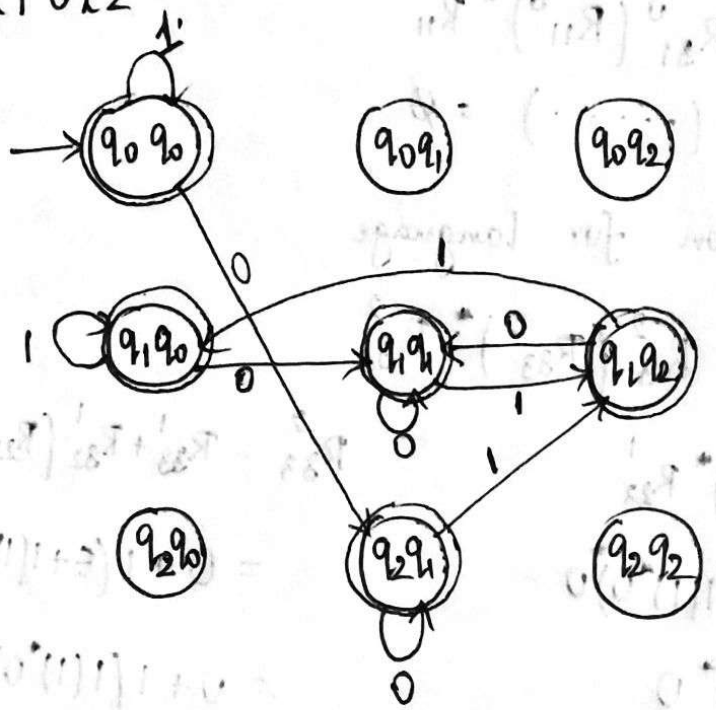
accepts $L1$

M_2



accepts $L2$

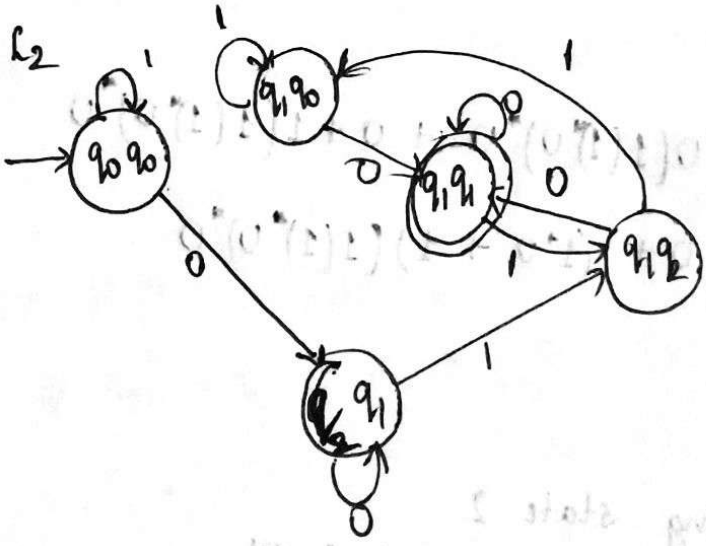
i) $L1 \cup L2$



Final states

q_0q_0
q_1q_0
q_1q_1
q_1q_2
q_2q_1

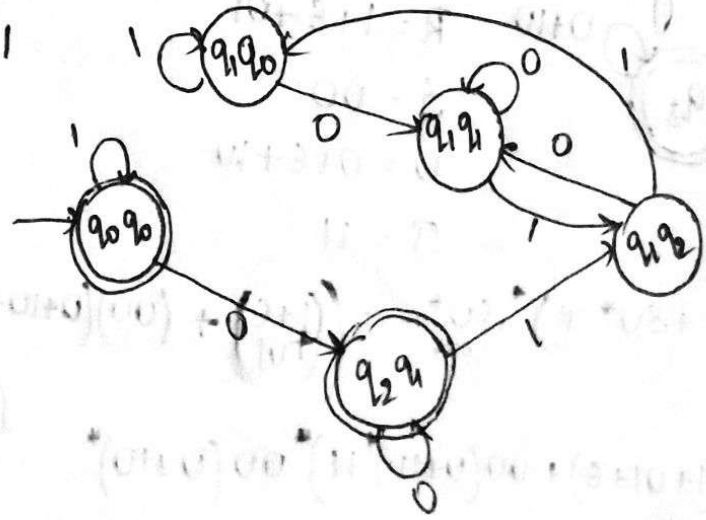
ii) $L_1 \cap L_2$



final state

q_1q_1

iii) $L2 - L1$

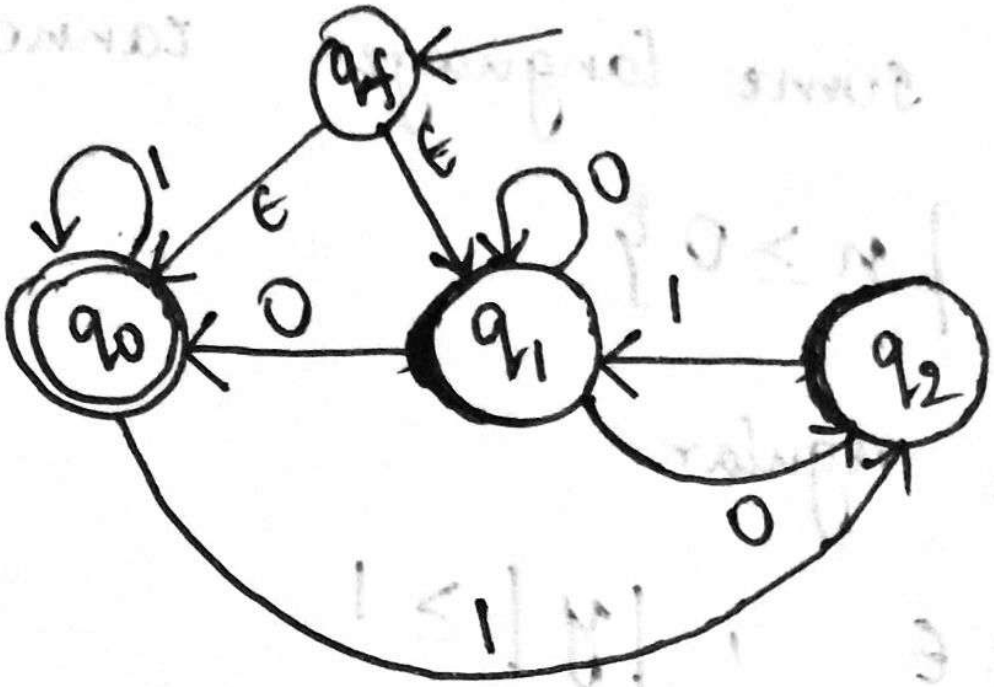


final state

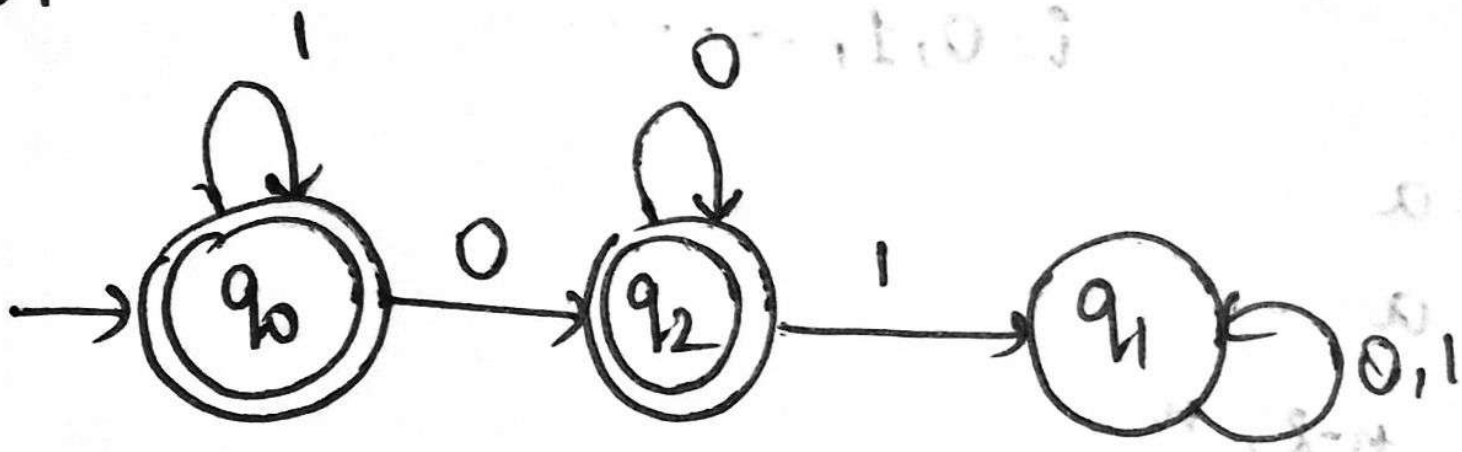
q_0q_0

q_2q_1

iv) L_2^R



v) $\overline{L_1}$



	RV College of Engineering® **Department of Computer Science and Engineering** **CIE - I**		
Course & Code	**Vulnerability Assessment & Penetration Testing (CY255TBD)** **Professional Core Course Elective-I**		**Semester: V**
Date: 27/11/2024	**Duration:**120 minutes	**Max.Marks** : 10 Marks (Quiz) + 50 Marks (Test)	
Scheme and Solution			

Sl.no.	Part A Quiz	Marks
1	CVSS - common vulnerability scoring system	01
2	Human Emotion	01
3	Meet-in-the-Middle Attack or The Meeting attack	01
4	Detection: Actively monitoring for signs of exploitation and staying informed through threat intelligence feeds. Mitigation: Implementing temporary controls, such as access restrictions, disabling vulnerable features, or using web application firewalls, until a permanent fix is available. Patch Management: Applying patches or updates as soon as they are released by the vendor. Incident Response: Having an incident response plan in place to quickly address any exploitation attempts. Communication: Informing stakeholders about the vulnerability and the steps being taken to mitigate the risk.	02
5	FTP (port 20, 21) SSH (port 22) Telnet (port 23) SMTP (port 25) HTTP (port 80) NTP (port 123) HTTPS (port 443	02
6	John the Ripper is a computer security tool (password cracking) used by penetration testers to test the security of a computer system. It is a command-line tool that can be used to test the security of various file formats. It can also be used to extract data from a target computer.	01
7	A black box test is a simulation of an attack from an external attacker, a white box test is a comprehensive review of an application's source code, and a grey box test is a combination of black box and white box testing.	02

<table>
<tr><th>Sl.no.</th><th>Part B Test</th><th>Marks</th></tr>
<tr><td>1.a</td><td>
<table>
<tr><th>S.No.</th><th>Penetration Testing</th><th>Vulnerability Assessments</th></tr>
<tr><td>1.</td><td>This is meant for critical real-time systems.</td><td>This is meant for non-critical systems.</td></tr>
<tr><td>2.</td><td>This is ideal for physical environments and network architecture.</td><td>This is ideal for lab environments.</td></tr>
<tr><td>3.</td><td>It is non-intrusive, documentation and environmental review and analysis.</td><td>Comprehensive analysis and through review of the target system and its environment.</td></tr>
<tr><td>4.</td><td>It cleans up the system and gives final report.</td><td>It attempt to mitigate or eliminate the potential vulnerabilities of valuable resources.</td></tr>
<tr><td>5.</td><td>It gathers targeted information and/or inspect the system.</td><td>It allocates quantifiable value and significance to the available resources.</td></tr>
<tr><td>6.</td><td>It tests sensitive data collection.</td><td>It discovers the potential threats to each resource.</td></tr>
<tr><td>7.</td><td>It determines the scope of an attack.</td><td>It makes a directory of assets and resources in a given system.</td></tr>
<tr><td>8.</td><td>The main focus is to discovers unknown and exploitable weaknesses in normal business processes.</td><td>The main focus is to lists known software vulnerabilities that could be exploited.</td></tr>
<tr><td>9.</td><td>It is a simulated cyberattack carried out by experienced ethical hackers in a well-defined and controlled environment.</td><td>It is an automated assessment performed with the help of automated tools.</td></tr>
<tr><td>10.</td><td>This is a goal-oriented procedure that should be carried out in a controlled manner.</td><td>This cost-effective assessment method is often considered safe to perform.</td></tr>
<tr><td>11.</td><td>It only identifies the exploitable security vulnerabilities.</td><td>It identifies, categorizes, and quantifies security vulnerabilities.</td></tr>
</table>
</td><td>06</td></tr>
<tr><td>1.b</td><td>False Positives/Negatives: Scans can sometimes report incorrect vulnerabilities, requiring further validation.
Prioritization: With hundreds or thousands of vulnerabilities, deciding which to address first can be complex.
Continuous Updating: New vulnerabilities are discovered regularly, so assessments must be ongoing.
Any four challenges with brief explanation- 4marks</td><td>04</td></tr>
<tr><td>2.a</td><td>1. Injection Attacks
SQL Injection: Attackers insert malicious SQL code into a query to access or manipulate databases.
Command Injection: Executing arbitrary commands on a server, leading to unauthorized access or system control.
Cross-Site Scripting (XSS): Injecting malicious scripts into web pages viewed by other users, allowing attackers to impersonate users or steal information.
2. Broken Authentication and Session Management
Weak Passwords: Easily guessable passwords or poor password management practices.
Session Hijacking: Attacking active user sessions to gain unauthorized access.
Exposed Session IDs: Using exposed session tokens to impersonate users.
3. Sensitive Data Exposure
Unencrypted Data: Storing or transmitting data without encryption, allowing attackers to intercept sensitive information.</td><td>06</td></tr>
</table>

	Insufficient Encryption Standards: Using weak or outdated encryption algorithms that can be cracked 4.Security Misconfiguration Default Configurations: Using default settings or passwords, which attackers can exploit. Unpatched Software: Failing to apply updates or security patches, making systems vulnerable to known attacks. 5. Cross-Site Request Forgery (CSRF) CSRF Attacks: Trick users into performing unwanted actions on authenticated websites, like transferring funds or changing settings. 6. Broken Access Control Excessive Privileges: Users or applications have more permissions than necessary. Directory Traversal: Attackers access restricted files or directories by manipulating URL paths. 7. Insecure Deserialization Malicious Object Injection: Exploiting deserialization to insert malicious objects or commands that compromise applications. 8. Insufficient Logging and Monitoring No Auditing: Failure to log actions and monitor systems can delay detection of breaches. Inadequate Monitoring: Lack of alerts for suspicious activities can lead to prolonged data breaches. 9. Outdated Components Legacy Systems: Using outdated software or hardware with known vulnerabilities. Unsupported Software: No longer receiving security patches, which makes systems easy targets. 10. Insufficient Transport Layer Protection Unencrypted Connections: Using HTTP instead of HTTPS, which can expose data to interception. Weak TLS Configurations: Using older TLS/SSL protocols vulnerable to attacks like BEAST or POODLE.	
2.b	• Actually teach security professionals what the bad guys already know and are doing. • Why do militaries all over the world study their enemies' tactics, tools, strategies, technologies. • Most countries' militaries carry out various scenario-based fighting exercises. • Base is so dependent upon technology and Software-Communication channels • different type of "security police" is required to cover and monitor all of these entry points into and out of the base. • An interesting aspect of the hacker community is that it is changing. • Thrill of figuring out how to exploit vulnerabilities to figuring out how to make revenue from their actions and getting paid for their skills. • Gaining financial benefits from their activities. • joy riding to hacking as an occupation. Examples: • hack, pump, and dump scheme, Russian hacking group called the Russian Business Network (BSN) stole tens of millions of dollars from Citibank etc. • Criminals are also using online scams in a bid to steal donations • Malware is still one of the main culprits that costs companies the most amount of money. • The commands and logic within the malware are the same components that attackers used to have to carry out manually.	04

3	1. Form two or three teams:
	• Red team—The attack team
	• White team—Network administration, the victim
	• Blue team—Management coordinating and overseeing the test (optional)
	2. Establish the ground rules:
	• Testing objectives
	• What to attack, what is hands-off
	• Who knows what about the other team (Are both teams aware of the other? Is the testing single blind or double blind?)
	• Start and stop dates
	• Legal issues
	  • Just because a client asks for it, doesn't mean that it's legal.
	  • The ethical hacker must know the relevant local, state, and federal laws and how they pertain to testing procedures.
	• Confidentiality/Nondisclosure
	• Reporting requirements
	• Formalized approval and written agreement with signatures and contact information
	  • Keep this document handy during the testing. It may be needed as a "get out of jail free" card
		10

	3. Passive scanning: Gather as much information about the target as possible while maintaining zero contact between the penetration tester and the target. Passive scanning can include interrogating. The company's website and source code • Social networking sites • Whois database • Edgar database • Newsgroups • ARIN, RIPE, APNIC, LACNIC databases • Google, Monster.com, etc. • Dumpster diving **4. Active scanning** Probe the target's public exposure with scanning tools, which might include: Commercial scanning tools • Banner grabbing • Social engineering • War dialing • DNS zone transfers • Sniffing traffic • Wireless war driving **5. Attack surface enumeration** Probe the target network to identify, enumerate, and document each exposed device: • Network mapping • Router and switch locations • Perimeter firewalls • LAN, MAN, and WAN connections **6. Fingerprinting** Perform a thorough probe of the target systems to identify: • Operating system type and patch level • Applications and patch level • Open ports • Running services • User accounts **7. Target system selection** Identify the most useful target(s). **8. Exploiting the uncovered vulnerabilities** Execute the appropriate attack tools targeted at the suspected exposures. • Some may not work. • Some may kill services or even kill the server. • Some may be successful. **9. Escalation of privilege** Escalate the security context so the ethical hacker has more control. • Gaining root or administrative rights • Using cracked password for unauthorized access • Carrying out buffer overflow to gain local versus remote control **10. Documentation and reporting** Document everything found, how it was found, the tools that were used, vulnerabilities that were exploited, the timeline of activities, and successes, etc.	
4	• simulating cyberattacks to identify vulnerabilities in a system. • Larger penetration test, we'll only cover the social engineering portion of the attack. **Attacks:** • The Good Samaritan • The Meeting attack • Join the Company attack **1.The Good Samaritan:** • Attackers exploit human emotions and trust to bypass technical security measures. • Target's willingness to help others. • both digital and physical contexts to bypass security or extract sensitive information. Steps: 1. Creating a Scenario of Need 2. Exploiting the Victim's Trust 3. Executing the Exploit Examples of the Good Samaritan Attack • Malicious USB Drives	10

- Fake Customer in Retail
- Tech Support Ruse

Defending Against Good Samaritan Attacks

- Employee Awareness
- Technical Safeguards
- Clear Security Policies
- Encourage Reporting
- Organizations must balance technological defenses with comprehensive employee education to mitigate this and other social engineering threats

2. The Meeting attack

- ***Meet-in-the-Middle Attack.***
- *cryptographic attack primarily used against encryption algorithms (Ex.* ***block ciphers*** *and* ***hash functions****)*
- *It reduces the effort needed to break the encryption by exploiting trade-offs between* ***time*** *and* ***memory****.*

Working:

1.Target*: The attack is typically used against encryption schemes that employ multiple encryption layers, such as double encryption (e.g., Double DES).*

2. Approach*:*

The attacker tries to compute both the encryption and decryption of the message until a match is found, reducing the effective security of the system.

Double DES, which encrypts a plaintext twice using two keys (K1 and K2)

- *Compute all possible encryptions of the plaintext with K1 and store the results.*
- *Compute all possible decryptions of the ciphertext with K2.*
- *Compare these two sets to find a match, significantly reducing the number of brute force operations.*

2. Approach*:*

The attacker tries to compute both the encryption and decryption of the message until a match is found, reducing the effective security of the system.

Double DES, which encrypts a plaintext twice using two keys (K1 and K2)

- *Compute all possible encryptions of the plaintext with K1 and store the results.*
- *Compute all possible decryptions of the ciphertext with K2.*
- *Compare these two sets to find a match, significantly reducing the number of brute force operations.*

Applications of the Attack:

- ***Block Ciphers****: Common against ciphers that use multiple encryption layers, such as 2DES or 3DES.*
- ***Cryptographic Protocols****: To test weaknesses in multi-stage encryption systems.*
- ***Hash Functions****: To find collisions in hash algorithms using similar methods.*

Mitigation Techniques:

- ***Use Larger Keys****: Increase key sizes to make brute-force attacks infeasible.*
- ***Use More Complex Designs****: Adopt encryption systems like AES, which are resistant to Meet-in-the-Middle attacks due to single encryption stages with strong mixing.*
- ***Key Management****: Avoid using algorithms that are vulnerable to this attack.*

3.Join the Company attack

Insider threat.

Attacker infiltrates an organization by gaining employment or physical access to the company.

Once inside, they exploit their access privileges to steal sensitive data, disrupt operations, or compromise security systems.

Key Features of the Attack:

- ➢ Entry Point:

The attacker applies for a job within the organization and gets hired.

Alternatively, they gain access through contractors, interns, or temporary positions.

- ➢ Execution:

Once inside, the attacker exploits their legitimate access to gather sensitive information, plant malware, or create backdoors.

They may blend in with employees to avoid detection while exfiltrating data or sabotaging systems.

- ➢ Motivation:

	Stealing intellectual property. Gaining access to trade secrets. Sabotaging the organization for financial gain, personal vendetta, or competitive advantage. ***Example Scenarios:*** ➢ Corporate Espionage: An attacker joins a rival company to steal proprietary designs, product plans, or customer data. ➢ Data Breach: A malicious insider plants malware or copies sensitive databases for personal or financial gain. ➢ Nation-State Attacks: A state-sponsored actor joins a defense or technology firm to obtain classified information. ***Detection and Mitigation Strategies:*** ➢ Background Checks: Perform thorough checks on all employees and contractors before hiring. ➢ Access Control: Implement least privilege policies to restrict access to only what is necessary for each role. ➢ Activity Monitoring: Monitor employee activity, especially on critical systems, for unusual behavior. ➢ Data Encryption: Encrypt sensitive data to minimize the impact of potential breaches. ➢ Regular Audits: Conduct frequent audits of access logs, security policies, and employee roles. ➢ Awareness Training: Educate employees about insider threats and the importance of reporting suspicious behavior.	
5.a	Risk Analysis and Penetration Testing are both important aspects of information security, however, they have some key differences. Risk Analysis is the process of identifying, quantifying, and assessing the potential risks associated with a security vulnerability, system, or process. Penetration Testing is the process of testing a system's vulnerability to attack by trying to exploit discovered vulnerabilities. Penetration Testing can be used to find vulnerabilities that could be harmful if exploited. When it comes to security, many organizations have a tendency of neglecting the perimeter. While this is understandable in the vast majority of cases, due to breaches that often originate from outside sources such as phishing and malware attacks, failing to properly secure your internal network can be shut down. A third-party penetration testing firm can help alleviate some of these problems by providing reliable and accurate information about vulnerabilities present in your organization's systems or networks. Additionally, they can provide guidance on how best to address them – whether through vulnerability assessment or remediation.	05
5.b	To strengthen its defenses against potential threats, Visma adopted the Qualys Cloud Platform for in-depth security scans. Qualys Vulnerability Management allowed the firm to automatically scan its development infrastructures and place the scan results in the same backlog with vulnerability reports on the company's code. It also provided the firm with a 360-degree view of vulnerabilities on its network that trickled down to individual devices. "We now have a comprehensive map of all 4,000 servers and 6,000 clients across our global IT infrastructure and an accurate view of all the vulnerabilities and their severity," says Hans Petter Holen, CISO, Visma. "We can perform scans in the background, even when a device is offline, and deliver the results as soon as it is reconnected to the network. When we detect a vulnerability, we deliver the findings to whoever is responsible for the machine — either via email to the local IT department or via Jira to the developer who owns the device." **Industry:** IT services **Vulnerability scanning provider:** Qualys **Outcomes:** • Vulnerability detection across more than 10,000 connected devices • Functions on minimal external management • Quarterly patching cycles accelerated up to 80%	05

	RV College of Engineering® **Department of Computer Science and Engineering** **CIE - I**		
Course & Code	**Vulnerability Assessment & Penetration Testing (CY255TBD)** **Professional Core Course Elective-I**		**Semester: V**
Date: 27/11/2024	**Duration:**120 minutes	**Max.Marks** : 10 Marks (Quiz) + 50 Marks (Test)	
USN :	**Name :**		

NOTE: ***Answer all the questions***

Sl.no.	Part-A Quiz	Marks	BT	CO
1	_____ is an industry-standard that vendors used to determine the severity of a vulnerability.	1	L1	CO5
2	_____ is the heart of every social engineering attack without which the attacks will not work.	1	L1	CO1
3	_____Attack reduces the effort needed to break the encryption by exploiting trade-offs between time and memory.	1	L2	CO3
4	How do you handle zero-day vulnerabilities?	2	L2	CO1
5	List the commonly targeted ports during penetration testing. Give example.	2	L2	CO1
6	What is John the ripper tool and how penetration testers are using it?	1	L1	CO1
7	Differentiate between a black box, white box, and grey box penetration test.	2	L1	CO1
	Part-B Test			
1.a	Differentiate between Vulnerability Assessment and Penetration Testing.	06	L2	CO2
1.b	List and briefly explain the common challenges in vulnerability assessment.	04	L2	CO1
2.a	Describe the most common vulnerabilities affecting organizations today. Discuss their causes, potential impacts, and strategies to mitigate these vulnerabilities.	06	L3	CO3
2.b	Why is it important to understand an attacker's tactics and how can this knowledge help to strengthen their defenses against potential threats?	04	L2	CO4
3	Outline the 10 steps involved in the penetration testing process. Explain the significance of each step and how it contributes to identifying and mitigating security vulnerabilities.	10	L3	CO2
4	Discuss any two common types of attacks used in penetration testing. Explain the purpose of each attack and their role in identifying vulnerabilities in an organization's security posture.	10	L3	CO5

5.a	Explain how risk analysis and penetration testing are different from each other. Why should penetration testing be carried out by a third party?	05	L2	CO4
5.b	With over one million customers across Europe and Latin America, Visma is a leading provider of accounting, procurement, and payroll solutions. Visma employs over 5,500 professionals and includes 200 companies spanning over 20 countries across the world. As the firm transformed into a software-as-a-service (SaaS) provider, newer challenges related to security emerged. Visma not only needs to ensure the security of its own systems, but it has the responsibility of safeguarding customer data as well. With a larger attack surface, Visma wanted to gain increased protection against potential cyberattacks by effectively detecting and remediating vulnerabilities. To strengthen its defenses against potential threats, Visma adopted the Qualys Cloud Platform for in-depth security scans. **Analyze how Visma addressed the cybersecurity challenges arising from its transformation into a SaaS provider. Discuss the role of the Qualys Cloud Platform in enhancing Visma's security infrastructure, focusing on the benefits achieved through its implementation. Include specific examples from the case study to support your answer.**	05	L3	CO5

BTL,CO	**L1**	**L2**	**L3**	**L4**	**L5**	**L6**	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	05	24	31	***	***	***	12	16	07	09	16