Discrete Mathematical Structures

CSET106



What is Discrete Mathematics?

- Discrete mathematics is the study of mathematical structures that are countable or otherwise distinct and separable.
- Examples of structures that are discrete are combinations, graphs, and logical statements, integers, etc.
- Discrete structures can be finite or infinite.
- By contrast, discrete mathematics excludes topics in "continuous mathematics" such as real numbers, calculus or Euclidean geometry.
- Discrete objects can often be enumerated by integers; more formally, discrete mathematics has been characterized as the branch of mathematics dealing with countable sets.

Applications of Discrete Mathematics

Areas in which discrete mathematics concepts are applied:

- Formal Languages (computer languages)
- Compiler Design
- Data Structures
- Computability
- Automata Theory
- Algorithm Design
- Relational Database Theory
- Complexity Theory (counting)

Logic

- Introduction:

The universe cannot be read until we have learnt the language and become familiar with the characters in which it is written. It is written in mathematical language... without which means it is humanly impossible to comprehend a single word.

Logic is the bridge between the language the universe is written-in and mathematics.

In this lecture, we shall learn the basic entities of logic:

1. Propositions
2. Boolean Variables
3. Logical (boolean) operators
4. Truth tables

Propositions

Definition

A Proposition is a statement of a fact which is either true or false but not both.

Examples:

1. Today is Saturday.

Propositions

Definition

A Proposition is a statement of a fact which is either true or false but not both.

Examples:

1. Today is Saturday.
2. It is raining today.

Propositions

Definition

A Proposition is a statement of a fact which is either true or false but not both.

Examples:

1. Today is Saturday.
2. It is raining today.
3. If n is an integer, then $(2n+1)^2 = 1 (\text{mod } 8)$.

Propositions

Definition

A Proposition is a statement of a fact which is either true or false but not both.

Examples:

1. Today is Saturday.
2. It is raining today.
3. If n is an integer, then $(2n+1)^2 = 1 (\text{mod } 8)$.
4. There are no positive integers x, y, z satisfying the equality $x^2 + y^2 = z^2$.

Propositions

Definition

A Proposition is a statement of a fact which is either true or false but not both.

Examples:

1. Today is Saturday.
2. It is raining today.
3. If n is an integer, then $(2n+1)^2 = 1 (\text{mod } 8)$.
4. There are no positive integers x, y, z satisfying the equality $x^2 + y^2 = z^2$.
5. There are infinitely many prime numbers q such that $q = 4p + 1$, where p is prime.

Proposition or NOT

1. New Delhi is the capital of India.

Proposition or NOT

1. New Delhi is the capital of India. Yes
2. Read this carefully.

Proposition or NOT

1. New Delhi is the capital of India. Yes
2. Read this carefully. No
3. $x + 1 = 2$

Proposition or NOT

1. New Delhi is the capital of India. Yes
2. Read this carefully. No
3. $x + 1 = 2$ No
4. $2 + 2 = 5$

Proposition or NOT

1. New Delhi is the capital of India. Yes
2. Read this carefully. No
3. $x + 1 = 2$ No
4. $2 + 2 = 5$ Yes
5. Water is made from Oxygen and Nitrogen.

Proposition or NOT

1. New Delhi is the capital of India. Yes
2. Read this carefully. No
3. $x + 1 = 2$ No
4. $2 + 2 = 5$ Yes
5. Water is made from Oxygen and Nitrogen.Yes
6. Do not use your cell phone while driving.

Proposition or NOT

1. New Delhi is the capital of India. Yes
2. Read this carefully. No
3. $x + 1 = 2$ No
4. $2 + 2 = 5$ Yes
5. Water is made from Oxygen and Nitrogen.Yes
6. Do not use your cell phone while driving. No (It's not a fact.)

Logic Operations

- Logic operations and compound propositions were introduced by the English mathematician George Boole in 1848. This lay the foundation of developing the digital computer 100 years later.
- We shall denote propositions by letters: $p, q, r, s, \cdots$, .

Logic Operations

- Logic operations and compound propositions were introduced by the English mathematician George Boole in 1848. This lay the foundation of developing the digital computer 100 years later.
- We shall denote propositions by letters: $p, q, r, s, \cdots$, .

Definition

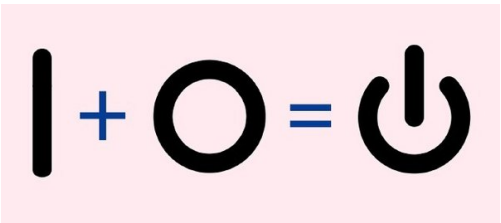
A Boolean Variable is a variable whose domain is propositions and range just two values, commonly denoted by **TRUE**, **FALSE**. Sometimes we also use $\{0, 1\}$.

Note: Almost all programming languages include boolean variables.

0 or 1, only two!

Question: What can be done with a single boolean variable that has only two values?

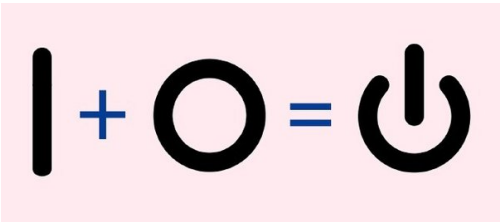
Answer: Not much more than a light switch, it can be off or on.



0 or 1, only two!

Question: What can be done with a single boolean variable that has only two values?

Answer: Not much more than a light switch, it can be off or on.



But combining an array of boolean variables, like 32 in common processors yields 2^{32} different patterns, That is more than $4,000,000,000$ patterns!

Note: Combining boolean variable is done with logic or boolean operators.

Example (Compound Propositions)

1. An elephant is not a bird.

Example (Compound Propositions)

1. An elephant is not a bird.
2. The speed limit in Bhubaneswar-Cuttack road for heavy vehicles is 40 km/hour and for trucks 30 km/hour.

Example (Compound Propositions)

1. An elephant is not a bird.
2. The speed limit in Bhubaneswar-Cuttack road for heavy vehicles is 40 km/hour and for trucks 30 km/hour.
3. If $x = 2$, then $x + 3 = 5$.

Example (Compound Propositions)

1. An elephant is not a bird.
2. The speed limit in Bhubaneswar-Cuttack road for heavy vehicles is 40 km/hour and for trucks 30 km/hour.
3. If $x = 2$, then $x + 3 = 5$.
4. If $x = 1$ or $x = 2$, then $(x - 1)(x - 2) = 0$.

Observe: Each proposition is composed of one or more propositions connected by keywords:

1. `not`: Number 1 has one proposition.
2. `and`: Number 2 has two propositions.
3. `or`: Number 4 has 2 propositions.
4. `if then`: Number 3 has 3 propositions.

Logical Operators

- **Negation**: **not** is a unary operator: $\neg p$ inverts the truth value of p.
- **Conjuction**: **and** is a binary operator: $p \wedge q$ is true only when both p and q are true.
- **Disjunction**: **or** is a binary operator: $p \vee q$ is false only when both p and q are false.
- **Implication**: **implies** (if then) is a binary operator: $p \rightarrow q$ is false only when p is true and q is false.

Truth Tables

Definition

Truth tables are used to describe the truth values of compound propositions.

1. All these operators can be physically implemented electronically.
2. These are the building blocks of micro-processors and many other systems.

Other Binary Operators There are other binary operators. Truth tables will help us understand how to construct them.

Truth Table (Negation)

- Truth Table for Unary Operator $\neg$ (not):

  p: Today is Friday.

  $\neg p$: It is not the case that today is Friday.

  or $\neg p$: Today is not Friday.

  or $\neg p$: It is not Friday today.

p	$\neg p$
T	F
F	T

Truth Table (Conjuction)

- Truth Table for Binary Operator $\wedge$ (and):

  p: Today is Friday.

  q: It is raining today.

  $p \wedge q$: Today is Friday and it is raining today.

  Note: Both p and q must be True.

p	q	$p \wedge q$
T	T	T
F	T	F
T	F	F
F	F	F

Truth Table (Disjuction)

- Truth Table for Binary Operator $\vee$ (or):

p: Today is Friday.

q: It is raining today.

$p \vee q$: Today is Friday or it is raining today.

p	q	$p \vee q$
T	T	T
F	T	T
T	F	T
F	F	F

- **Note**: Only one of p and q must be true. Hence, the inclusive nature.

Truth Table (Exclusive OR)

- Truth Table for Binary Operator $\oplus$ (XOR):

  p: Today is Friday.

  q: It is raining today.

  $p \oplus q$: Today is Friday or it is raining today, but not both.

p	q	$p \oplus q$
T	T	F
F	T	T
T	F	T
F	F	F

- **Note**: p or q, but not both.

Truth Table (Implication $\Longrightarrow$)

- Truth Table for Binary Operator $\rightarrow$ (implies, 'if ... then ...'):

p: I am elected.

q: I will lower taxes.

$p \rightarrow q$: If I am elected, then I will lower taxes.

p	q	$p \rightarrow q$
T	T	T
F	T	T
T	F	F
F	F	T

- **Note**[1]: The implication is false only when P is true and Q is false!
- **Note**[2]: $p \rightarrow q$ has the same truth table as $\neg p \vee q$.

Truth Table for Compound Proposition

- Evaluating compound propositions with truth tables:

  Example: Let's try to build the truth table for the compound proposition: $(p \to q) \wedge (\neg p \to q)$.

p	q	$p \to q$	$\neg p \to q$	$(p \to q) \wedge (\neg p \to q)$
T	T	T	T	T
F	T	T	T	T
T	F	F	T	F
F	F	T	F	F

Thank You.



Discrete Mathematical Structures

CSET106



Truth Table (Implication $\Longrightarrow$)

- Truth Table for Binary Operator $\rightarrow$ (implies, 'if ... then ...'):

p: I am elected.

q: I will lower taxes.

$p \rightarrow q$: If I am elected, then I will lower taxes.

p	q	$p \rightarrow q$
T	T	T
F	T	T
T	F	F
F	F	T

- **Note**[1]: The implication is false only when P is true and Q is false!
- **Note**[2]: $p \rightarrow q$ has the same truth table as $\neg p \vee q$.

Terminologies used to express $p \rightarrow q$

if p, then q	p implies q
p only if q	p is sufficient for q
a sufficient condition for q is p	q if p
q whenever p	q when p
q is necessary for p	a necessary condition for p is q
if p, q	q follows from p

Truth Table (Biconditional $\iff$)

- Truth Table for Binary Operator $\leftrightarrow$ (Bi-implication, 'p if and only if q'):

p: You can take the flight.

q: You buy a ticket.

$p \rightarrow q$: You can take the flight if and only if you buy a ticket.

p	q	$p \leftrightarrow q$
T	T	T
F	T	F
T	F	F
F	F	T

- **Note**[1]: The biconditional statement is true when p and q have the same truth values, and false otherwise.
- **Note**[2]: $p \rightarrow q$ has the same truth table as $(p \rightarrow q) \wedge (q \rightarrow p)$.

Precedence of Logical Operators

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

$p \wedge q \vee r$ means $(p \wedge q) \vee r$ and

~~$p \wedge (q \vee r)$~~

Bit Operations

Truth Value	Bit
T	1
F	0

Definition

A bit string is a sequence of zero or more bits. The length of this string is the number of bits in the string.

Example: Find the bitwise *OR*, bitwise *AND*, and bitwise *XOR* of the bit strings 01 1011 0110 and 11 0001 1101.

$$\begin{array}{l} 01\ 1011\ 0110 \\ 11\ 0001\ 1101 \\ \hline 11\ 1011\ 1111 \text{ bitwise } OR \\ 01\ 0001\ 0100 \text{ bitwise } AND \\ 10\ 1010\ 1011 \text{ bitwise } XOR \end{array}$$

Translating English Sentences into Propositional Logic

Example: 1 You can access the Internet from campus only if you are a computer science student or you are not an outsider.

$$p \rightarrow (q \vee \neg r)$$

where

p You can access the Internet from campus.

q You are a computer science student.

r You are an outsider.

Translating English Sentences into Propositional Logic

Example: 2 You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old.

$$(r \wedge \neg s) \rightarrow \neg q$$

where

q You can ride the roller coaster.

r You are under 4 feet tall.

s You are older than 16 years old.

Propositional Equivalences

- A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it, is called a tautology. Ex. $p \vee \neg p$
- A compound proposition that is always false is called a contradiction. Ex. $p \wedge \neg p$
- A compound proposition that is neither a tautology nor a contradiction is called a contingency.

Logical Equivalences

Definition

The compound propositions p and q are called logically equivalent if $p \leftrightarrow q$ is a tautology. The notation $p \equiv q$ denotes that p and q are logically equivalent.

The symbol $\Longleftrightarrow$ is sometimes used instead of $\equiv$ to denote logical equivalence.

Logical Equivalence Demonstration

Example: Show that $p \vee (q \wedge r)$ and $(p \vee q) \wedge (p \vee r)$ are logically equivalent.

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$	$p \vee r$	$(p \vee q) \wedge (p \vee r)$
T	T	T	T	T	T	T	T
T	T	F	F	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	T	T	T
F	T	T	T	T	T	T	T
F	T	F	F	F	T	F	F
F	F	T	F	F	F	T	F
F	F	F	F	F	F	F	F

distributive law of disjunction over conjunction

Logical Equivalences

Equivalence	Name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws

Logical Equivalences

Equivalence	Name
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation laws

Logical Equivalences Involving Conditional Statements

Equivalence	Logical Equivalence
$p \to q \equiv \neg p \vee q$	Implication law
$p \to q \equiv \neg q \to \neg p$ $p \vee q \equiv \neg p \to q$ $p \wedge q \equiv \neg(p \to \neg q)$ $\neg(p \to q) \equiv p \wedge \neg q$	Contrapositive law
$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$ $(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$ $(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$ $(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$	Distributive law

Logical Equivalences Involving Biconditional Statements

Equivalence	**Expression**
1	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
2	$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
3	$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
4	$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Logical Equivalence Proof

Example: $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent by developing a sequence of logical equivalences.

Proof:

$$\begin{aligned}
\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) && \text{by the second De Morgan law} \\
&\equiv \neg p \wedge (\neg(\neg p) \vee \neg q) && \text{by the first De Morgan law} \\
&\equiv \neg p \wedge (p \vee \neg q) && \text{by the double negation law} \\
&\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) && \text{by the second distributive law} \\
&\equiv F \vee (\neg p \wedge \neg q) && \text{because } \neg p \wedge p \equiv F \\
&\equiv (\neg p \wedge \neg q) \vee F && \text{by the commutative law for disjunct} \\
&\equiv \neg p \wedge \neg q && \text{by the identity law for F}
\end{aligned}$$

Thank You.



Discrete Mathematical Structures

CSET106

Rules of Inferences



Argument

Definition

- An argument in propositional logic is a sequence of propositions. All but the final proposition in the argument are called premises and the final proposition is called the conclusion.
- An argument is valid if the truth of all its premises implies that the conclusion is true.
- An argument form in propositional logic is a sequence of compound propositions involving propositional variables.
- An argument form is valid no matter which particular propositions are substituted for the propositional variables in its premises, the conclusion is true if the premises are all true.

Rules of Inference

- Constructing truth table is a tedious approach. For example, when an argument form involves 10 different propositional variables, to use a truth table to show this argument form is valid requires $2^{10} = 1024$ different rows.
- We do not have to resort to truth tables. Instead, we can first establish the validity of some relatively simple argument forms, called rules of inference.
- These rules of inference can be used as building blocks to construct more complicated valid argument forms.

Common Inference Rules

- These are logical rules used to draw conclusions from given premises.
- Common rules of inferences:
  1. Modus Ponens
  2. Modus Tollens
  3. Hypothetical Syllogism
  4. Disjunctive Syllogism
  5. Addition
  6. Simplification
  7. Conjunction
  8. Resolution

Modus Ponens

derived from Latin and translates to "mode that affirms."

Rule

If $P \to Q$ and P are true, then we can conclude that Q is true.

$$\begin{array}{ll} & P \to Q \\ & P \\ \hline \therefore & Q \end{array}$$

Example

- Premise 1: If it is raining, then the ground is wet. $(R \to W)$
- Premise 2: It is raining. (R)
- Conclusion: Therefore, the ground is wet. (W)

Modus Tollens

derived from Latin and translates to "mode that denies."

Rule

If $P \to Q$ is true and Q is false, then we can conclude that P is false.

$$\begin{array}{l} P \to Q \\ \neg Q \\ \hline \therefore \quad \neg P \end{array}$$

Example

- Premise 1: If it is snowing, then the road is slippery. $(S \to R)$
- Premise 2: The road is not slippery. $(\neg R)$
- Conclusion: Therefore, it is not snowing. $(\neg S)$

Hypothetical Syllogism

Rule

If $P \to Q$ and $Q \to R$ are true, then we can conclude that $P \to R$ is true.

$$\begin{array}{rrcl} & P & \to & Q \\ & Q & \to & R \\ \hline \therefore & P & \to & R \end{array}$$

Example

- Premise 1: If it is sunny, then I go for a run. $(S \to R)$
- Premise 2: If I go for a run, then I feel energized. $(R \to E)$
- Conclusion: Therefore, if it is sunny, then I feel energized. $(S \to E)$

Disjunctive Syllogism

Rule

If $P \vee Q$ is true and $\neg P$ is true, then we can conclude that Q is true.

$$\begin{array}{l} P \vee Q \\ \neg P \\ \hline \therefore \quad Q \end{array}$$

Example

- Premise 1: It is either snowing or raining. $(S \vee R)$
- Premise 2: It is not snowing. $(\neg S)$
- Conclusion: Therefore, it is raining. (R)

Addition

Rule

If P is true, then $P \vee Q$ is also true.

$$\frac{P}{\therefore \quad P \vee Q}$$

Example

- Premise: The sky is blue. (B)
- Conclusion: Therefore, the sky is either blue or cloudy. $(B \vee C)$

Simplification

Rule

If $P \wedge Q$ is true, then both P and Q are true.

$$\frac{P \wedge Q}{\therefore \quad P}$$

Example

- Premise: It is both sunny and warm. $(S \wedge W)$
- Conclusion: Therefore, it is sunny. (S)

Conjunction

Rule

If P and Q are true, then $P \wedge Q$ is true.

$$\begin{array}{ll} & P \\ & Q \\ \hline \therefore & P \wedge Q \end{array}$$

Example

- Premise 1: The cat is black. (B)
- Premise 2: The cat is playful. (P)
- Conclusion: Therefore, the cat is both black and playful. $(B \wedge P)$

Resolution

Rule

If $P \vee Q$ and $\neg P \vee R$ are true, then we can conclude that $Q \vee R$ is true.

$$\begin{array}{rl} & P \vee Q \\ & \neg P \vee R \\ \hline \therefore & Q \vee R \end{array}$$

Example

- Premise 1: It is either sunny or windy. $(S \vee W)$
- Premise 2: It is not sunny or it is rainy. $(\neg S \vee R)$
- Conclusion: Therefore, it is either windy or rainy. $(W \vee R)$

Conclusion

- Rules of inference are essential in logical reasoning.
- These rules provide a systematic way to derive conclusions from given premises.
- Practice using these rules to enhance your logical problem-solving skills.

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism
p $\therefore p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution

Exercise Problem 1

Problem

Use Modus Ponens to derive a conclusion from the following premises:

- Premise 1: If it is Monday, then there is a staff meeting. ($M \rightarrow S$)
- Premise 2: Today is Monday. (M)

What can you conclude?

Exercise Problem 2

Problem

Apply Modus Tollens to infer a conclusion from the following statements:

- Premise 1: If the alarm is working, then there is no burglary. ($A \rightarrow \neg B$)
- Premise 2: There is a burglary. (B)

What can be inferred from these premises?

Exercise Problem 3

Problem

Utilize Hypothetical Syllogism to draw a conclusion based on the following propositions:

- Premise 1: If it is sunny, then the outdoor event will take place. ($S \rightarrow O$)
- Premise 2: If the outdoor event takes place, then there will be live music. ($O \rightarrow L$)

What can you conclude using Hypothetical Syllogism?

Exercise Problem 4

Problem

Employ Disjunctive Syllogism to make an inference from the given statements:

- Premise 1: It is either snowing or raining. $(S \vee R)$
- Premise 2: It is not snowing. $(\neg S)$

What conclusion can you draw using Disjunctive Syllogism?

Exercise Problem 5

Problem

Show that the premises "If you send me an e-mail message, then I will finish writing the program", "If you do not send me an e-mail message, then I will go to sleep early", and "If I go to sleep early, then I will wake up feeling refreshed" lead to the conclusion "If I do not finish writing the program, then I will wake up feeling refreshed".

Hint:

	Step	Reason
(1)	$p \rightarrow q$	Premise
(2)	$\neg q \rightarrow \neg p$	Contrapositive of (1)
(3)	$\neg p \rightarrow r$	Premise
(4)	$\neg q \rightarrow r$	Hypothetical syllogism using (2) and (3)
(5)	$r \rightarrow s$	Premise
(6)	$\neg q \rightarrow s$	Hypothetical syllogism using (4) and (5)

Thank You.



Discrete Mathematical Structures

CSET106

Predicates and Quantifiers



Introduction

Predicate:

A statement with variables that becomes a proposition when specific values are substituted for the variables.

Quantifiers:

Symbols used to express the extent of generality of a proposition.

Predicates

Definition

A **predicate** is a statement parameterized by variables that can be either true or false depending on the values of those variables.

Examples:

1. $P(x)$: "x is a prime number".
2. $Q(x, y)$: "x is less than y".

Quantifiers

Existential Quantifier ($\exists$)

The **existential quantifier** asserts that there exists at least one element in the domain for which the predicate is true.

Example

- $\exists x P(x)$: "There exists a prime number."

Universal Quantifier ($\forall$)

The **universal quantifier** asserts that the predicate is true for every element in the domain.

Example

- $\forall x Q(x, 10)$: "Every number is less than 10."

Quantifiers (contd.)

1. $P(x)$: "x is a prime number".
2. $Q(x, y)$: "x is less than y".

Negation of Quantified Statements

- $\neg\exists x P(x) \equiv \forall x \neg P(x)$: "There is no prime number."
- $\neg\forall x Q(x, 10) \equiv \exists x \neg Q(x, 10)$: "There exists a number greater than or equal to 10."

Nested Quantifiers

- $\forall x \exists y Q(x, y)$: "For every x, there exists a y such that x is less than y."

Examples

Example 1

$P(x)$: "x is an even number"

- $\exists x P(x)$:

Examples

Example 1

$P(x)$: "x is an even number"

- $\exists x P(x)$: "There exists an even number."
- $\forall x \neg P(x)$:

Examples

Example 1

$P(x)$: "x is an even number"

- $\exists x P(x)$: "There exists an even number."
- $\forall x \neg P(x)$: "Every number is not even."

Example 2

$Q(x, y)$: "x is divisible by y"

- $\exists x \forall y Q(x, y)$:

Examples

Example 1

$P(x)$: "x is an even number"

- $\exists x P(x)$: "There exists an even number."
- $\forall x \neg P(x)$: "Every number is not even."

Example 2

$Q(x, y)$: "x is divisible by y"

- $\exists x \forall y Q(x, y)$: "There exists a number divisible by every other number."

Example 3

$R(x, y)$: "x is a factor of y"

- $\forall x \exists y R(x, y)$:

Examples

Example 1

$P(x)$: "x is an even number"

- $\exists x P(x)$: "There exists an even number."
- $\forall x \neg P(x)$: "Every number is not even."

Example 2

$Q(x, y)$: "x is divisible by y"

- $\exists x \forall y Q(x, y)$: "There exists a number divisible by every other number."

Example 3

$R(x, y)$: "x is a factor of y"

- $\forall x \exists y R(x, y)$: "For every x, there exists a y such that x is a factor of y."

Exercise Problems

Problem 1

Define a predicate $S(x, y)$ representing "x is the square of y." Provide examples and negate the quantified statements.

Problem 2

Consider the predicate $G(x, y)$: "x and y are both greater than 5." Express the statement $\exists x \exists y G(x, y)$ in plain English.

Problem 3

Define a predicate $L(x, y)$: "x is less than the cube of y." Express the statement $\forall x \exists y L(x, y)$ in plain English.

Problem 1: Define a predicate $S(x, y)$ representing "x is the square of y." Provide examples and negate the quantified statements.

Solution to Problem 1

- Predicate: $S(x, y)$: "x is the square of y."
- Examples:
  - $S(4, 2)$ is true because 4 is the square of 2.
  - $S(9, 3)$ is true because 9 is the square of 3.
- Negation of quantified statements:
  - Universal quantifier: $\neg(\forall x, y S(x, y))$ - "It is not the case that for all x and y, x is the square of y." equivalent to $(\exists x, y \neg S(x, y))$ - "There exists an x and y such that x is not the square of y".
  - Existential Quantifier: $\neg(\exists x, y S(x, y))$ - "There does not exist x and y such that x is the square of y." equivalent to $\forall x, y \neg S(x, y)$: "For all x and y, x is not the square of y."

Problem 2

Consider the predicate $G(x, y)$: "x and y are both greater than 5." Express the statement $\exists x \exists y G(x, y)$ in plain English.

Solution to Problem 2

The statement $\exists x \exists y G(x, y)$ can be expressed in plain English as "There exist two numbers, x and y, both greater than 5."

Problem 3

Define a predicate $L(x, y)$: "x is less than the cube of y." Express the statement $\forall x \exists y L(x, y)$ in plain English.

Solution to Problem 3

The statement $\forall x \exists y L(x, y)$ can be expressed in plain English as "For every number x, there exists a number y such that x is less than the cube of y."

Problem 4

Prove that there is no greatest prime number.

- We'll use proof by contradiction and the negation of a quantified statement.
- Assume, for contradiction, that there exists a greatest prime number, denoted as P.
- The negation of this assumption is:

$$\neg(\forall p)(p \text{ is a prime number} \implies p \leq P)$$

which is equivalent to

$$(\exists p)(p \text{ is a prime number} \wedge p > P)$$

- Consider a new number Q defined as:

$$Q = 2 \times 3 \times 5 \times \ldots \times P + 1$$

- Q is either prime or composite.
- If Q is prime, then we have found a prime number greater than P.
- If Q is composite, it has a prime factor greater than P.
- We have shown that the assumption of a greatest prime leads to a contradiction.
- Therefore, there is no greatest prime number.

Conclusion

- Predicates allow us to make statements about variables.
- Quantifiers help us express the generality of these statements.
- Careful use of quantifiers is essential for precise mathematical statements.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Predicates and Quantifiers Continue



Precedence of Quantifiers

- Quantifiers bind more strongly than logical connectives.
- The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus, like $\wedge$ (and), $\vee$ (or), and $\Rightarrow$ (implies), etc.
- For example, $\forall x P(x) \vee Q(x)$ means $\big(\forall x P(x)\big) \vee Q(x)$ and not ~~$\forall x \big(P(x) \vee Q(x)\big)$~~.
- $\forall x (P(x) \wedge Q(x))$: The quantifier $\forall x$ binds more strongly than the logical connective $\wedge$.
- $\exists y (R(y) \Rightarrow S(y))$: The quantifier $\exists y$ binds more strongly than the implication $\Rightarrow$.
- **Note:** While precedence rules help in most cases, it's crucial to use parentheses to avoid ambiguities in complex statements.

De Morgan's Laws for Quantifiers

Negation	Equivalent Statement
$\neg\exists x P(x)$	$\forall x \neg P(x)$
$\neg\forall x P(x)$	$\exists x \neg P(x)$

- **Example 1:** What is the negations of the statement "All Indians eat rice"?
- **Ans:**

$R(x)$	"x eats rice"
$\forall x R(x)$	"All Indians eat rice"
$\exists x \neg R(x)$	"There is an Indian who does not eat rice."

- **Example 2:** What is the negations of the statement "There is an honest politician"?
- **Ans:**

$H(x)$	"x is honest"
$\exists x H(x)$	"There is an honest politician"
$\forall x \neg H(x)$	"Every politician is dishonest."

- **Note:** In English, the statement "All politicians are not honest" is ambiguous. In common usage, this statement often means "Not all politicians are honest."

Rules of Inference for Quantified Statements

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\dfrac{\forall x\, P(x)}{\therefore\ P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\ \forall x\, P(x)}$	Universal generalization
$\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some element } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some element } c}{\therefore\ \exists x\, P(x)}$	Existential generalization

Examples

- **Example 1:** Show that the premises "Everyone in this DMS class has taken a course in computer science" and "Neena is a student in this class" imply the conclusion "Neena has taken a course in computer science."
- **Solution:** Let $D(x)$ denote "x is in this DMS class," and let $C(x)$ denote "x has taken a course in computer science." Then the premises are $\forall x(D(x) \rightarrow C(x))$ and $D(\text{Neena})$. The conclusion is $C(\text{Neena})$.

Step	**Reason**
(1) $\forall x(D(x) \rightarrow C(x))$	Premise
(2) $D(\text{Neena}) \rightarrow C(\text{Neena})$	Universal instantiation
(3) $D(\text{Neena})$	Premise
(4) $C(\text{Neena})$	Modus ponens from (2) and (3)

- **Example 2:** Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."
- Let $C(x)$ be "x is in this class," $B(x)$ be "x has read the book" and $P(x)$ be "x passed the first exam."
- The premises are:

- **Example 2:** Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."
- Let $C(x)$ be "x is in this class," $B(x)$ be "x has read the book" and $P(x)$ be "x passed the first exam."
- The premises are:
  - $\exists x(C(x) \wedge \neg B(x))$
  - $\forall x(C(x) \rightarrow P(x))$
- The conclusion is:

- **Example 2:** Show that the premises "A student in this class has not read the book," and "Everyone in this class passed the first exam" imply the conclusion "Someone who passed the first exam has not read the book."
- Let $C(x)$ be "x is in this class," $B(x)$ be "x has read the book" and $P(x)$ be "x passed the first exam."
- The premises are:
  - $\exists x(C(x) \wedge \neg B(x))$
  - $\forall x(C(x) \rightarrow P(x))$
- The conclusion is:
  - $\exists x(P(x) \wedge \neg B(x))$

Logical Steps

1. $\exists x(C(x) \wedge \neg B(x))$ **Premise**
2. $C(a) \wedge \neg B(a)$ **Existential instantiation from (1)**
3. $C(a)$ **Simplification from (2)**
4. $\forall x(C(x) \rightarrow P(x))$ **Premise**
5. $C(a) \rightarrow P(a)$ **Universal instantiation from (4)**
6. $P(a)$ **Modus ponens from (3) and (5)**
7. $\neg B(a)$ **Simplification from (2)**
8. $P(a) \wedge \neg B(a)$ **Conjunction from (6) and (7)**
9. $\exists x(P(x) \wedge \neg B(x))$ **Existential generalization from (8)**

Combining Rules of Inference for Propositions and Quantified Statements

Universal Modus Ponens

$$\frac{\begin{array}{l}\forall x\big(P(x) \to Q(x)\big) \\ P(a), \text{ where } a \text{ is a particular element in the domain}\end{array}}{\therefore Q(a)}$$

Universal Modus Tollens

$$\frac{\begin{array}{l}\forall x\big(P(x) \to Q(x)\big) \\ \neg Q(a), \text{ where } a \text{ is a particular element in the domain}\end{array}}{\therefore \neg P(a)}$$

- **Example:** Assume that "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n " is true. Use universal modus ponens to show that $100^2 < 2^{100}$.

- **Example:** Assume that "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n " is true. Use universal modus ponens to show that $100^2 < 2^{100}$.
- Let $P(n)$ denote "$n > 4$" and $Q(n)$ denote "$n^2 < 2^n$." The statement "For all positive integers n, if n is greater than 4, then n^2 is less than 2^n" can be represented by $\forall n(P(n) \rightarrow Q(n))$, where the domain consists of all positive integers. Note that $P(100)$ is true because $100 > 4$. It follows by universal modus ponens that $Q(100)$ is true, namely that $100^2 < 2^{100}$.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Nested Quantifiers



The Order of Quantifiers

- **Example 1:** Let $P(x, y)$ be the statement "$x + y = y + x$." What are the truth values of the quantifications $\forall x \forall y P(x, y)$ and $\forall y \forall x P(x, y)$ where the domain for all variables consists of all real numbers?

- **Example 2:** Let $Q(x, y)$ denote "$x + y = 0$." What are the truth values of the quantifications $\exists y \forall x Q(x, y)$ and $\forall x \exists y Q(x, y)$, where the domain for all variables consists of all real numbers?

- **Example 2:** Let $Q(x, y)$ denote "$x + y = 0$." What are the truth values of the quantifications $\exists y \forall x Q(x, y)$ and $\forall x \exists y Q(x, y)$, where the domain for all variables consists of all real numbers?
- $\exists y \forall x Q(x, y)$: FALSE!

- **Example 2:** Let $Q(x, y)$ denote "$x + y = 0$." What are the truth values of the quantifications $\exists y \forall x Q(x, y)$ and $\forall x \exists y Q(x, y)$, where the domain for all variables consists of all real numbers?
- $\exists y \forall x Q(x, y)$: FALSE! "There is a real number y such that for every real number x, $Q(x, y)$." No matter what value of y is chosen, there is only one value of x for which $x + y = 0$. Because there is no real number y such that $x + y = 0$ for all real numbers x.

- **Example 2:** Let $Q(x, y)$ denote "$x + y = 0$." What are the truth values of the quantifications $\exists y \forall x Q(x, y)$ and $\forall x \exists y Q(x, y)$, where the domain for all variables consists of all real numbers?
- $\exists y \forall x Q(x, y)$: FALSE! "There is a real number y such that for every real number x, $Q(x, y)$." No matter what value of y is chosen, there is only one value of x for which $x + y = 0$. Because there is no real number y such that $x + y = 0$ for all real numbers x.
- $\forall x \exists y Q(x, y)$: TRUE "For every real number x there is a real number y such that $Q(x, y)$."

- **Example 2:** Let $Q(x, y)$ denote "$x + y = 0$." What are the truth values of the quantifications $\exists y \forall x Q(x, y)$ and $\forall x \exists y Q(x, y)$, where the domain for all variables consists of all real numbers?
- $\exists y \forall x Q(x, y)$: FALSE! "There is a real number y such that for every real number x, $Q(x, y)$." No matter what value of y is chosen, there is only one value of x for which $x + y = 0$. Because there is no real number y such that $x + y = 0$ for all real numbers x.
- $\forall x \exists y Q(x, y)$: TRUE "For every real number x there is a real number y such that $Q(x, y)$." Given a real number x, there is a real number y such that $x + y = 0$; namely, $y = -x$.

- **Example 3:** Let $Q(x, y, z)$ be the statement "$x + y = z$." What are the truth values of the statements $\forall x \forall y \exists z Q(x, y, z)$ and $\exists z \forall x \forall y Q(x, y, z)$, where the domain of all variables consists of all real numbers?

- **Example 3:** Let $Q(x, y, z)$ be the statement "$x + y = z$." What are the truth values of the statements $\forall x \forall y \exists z Q(x, y, z)$ and $\exists z \forall x \forall y Q(x, y, z)$, where the domain of all variables consists of all real numbers?
- "For all real numbers x and for all real numbers y there is a real number z such that $x + y = z$".

  $\therefore \forall x \forall y \exists z Q(x, y, z)$ is TRUE.

- **Example 3:** Let $Q(x, y, z)$ be the statement "$x + y = z$." What are the truth values of the statements $\forall x \forall y \exists z Q(x, y, z)$ and $\exists z \forall x \forall y Q(x, y, z)$, where the domain of all variables consists of all real numbers?
- "For all real numbers x and for all real numbers y there is a real number z such that $x + y = z$".

  $\therefore \forall x \forall y \exists z Q(x, y, z)$ is TRUE.
- "There is a real number z such that for all real numbers x and for all real numbers y it is true that $x + y = z$".

  $\therefore \exists z \forall x \forall y Q(x, y, z)$ is FALSE.

Translating Mathematical Statements into Statements Involving Nested Quantifiers

- **Example 1:** Translate the statement "The sum of two positive integers is always positive" into a logical expression.

Translating Mathematical Statements into Statements Involving Nested Quantifiers

- **Example 1:** Translate the statement "The sum of two positive integers is always positive" into a logical expression.
- Rewrite as "For every two integers, if these integers are both positive, then the sum of these integers is positive."

Translating Mathematical Statements into Statements Involving Nested Quantifiers

- **Example 1:** Translate the statement "The sum of two positive integers is always positive" into a logical expression.
- Rewrite as "For every two integers, if these integers are both positive, then the sum of these integers is positive."
- Again, "For all positive integers x and y, $x + y$ is positive."

Translating Mathematical Statements into Statements Involving Nested Quantifiers

- **Example 1:** Translate the statement "The sum of two positive integers is always positive" into a logical expression.
- Rewrite as "For every two integers, if these integers are both positive, then the sum of these integers is positive."
- Again, "For all positive integers x and y, $x + y$ is positive."
- $\forall x \forall y((x > 0) \wedge (y > 0) \rightarrow (x + y > 0))$, where the domain for both variables consists of all integers.
- **Note:** We could also translate this using the positive integers as the domain. $\forall x \forall y(x + y > 0)$, where the domain for both variables consists of all positive integers.

- **Example 2:** Translate the statement "Every real number except zero has a multiplicative inverse."

- **Example 2:** Translate the statement "Every real number except zero has a multiplicative inverse."
- "For every real number x, if $x \neq 0$, then there exists a real number y such that $xy = 1$."

- **Example 2:** Translate the statement "Every real number except zero has a multiplicative inverse."
- "For every real number x, if $x \neq 0$, then there exists a real number y such that $xy = 1$."
- $\forall x\big((x \neq 0) \rightarrow \exists y(xy = 1)\big)$.

Translating from Nested Quantifiers into English

- **Example 1:** Translate the statement $\forall x\Big(C(x) \vee \exists y\big(C(y) \wedge F(x,y)\big)\Big)$ into English, where $C(x)$ is "x has a computer," $F(x,y)$ is "x and y are friends," and the domain for both x and y consists of all students in your school.

Translating from Nested Quantifiers into English

- **Example 1:** Translate the statement $\forall x\Big(C(x) \vee \exists y\big(C(y) \wedge F(x,y)\big)\Big)$ into English, where $C(x)$ is "x has a computer," $F(x,y)$ is "x and y are friends," and the domain for both x and y consists of all students in your school.
- "For every student x in your school, x has a computer or there is a student y such that y has a computer and x and y are friends."
- "Every student in your school has a computer or has a friend who has a computer."

- **Example 3:** Translate the statement $\exists x \forall y \forall z \Big(\big(F(x,y) \wedge F(x,z) \wedge (y \neq z) \big) \rightarrow \neg F(y,z) \Big)$ into English, where $F(a,b)$ means a and b are friends and the domain for x, y, and z consists of all students in your school.

- **Example 3:** Translate the statement $\exists x \forall y \forall z \Big(\big(F(x,y) \wedge F(x,z) \wedge (y \neq z) \big) \rightarrow \neg F(y,z) \Big)$ into English, where $F(a,b)$ means a and b are friends and the domain for x, y, and z consists of all students in your school.
- "If students x and y are friends, and students x and z are friends, and furthermore, if y and z are not the same student, then y and z are not friends.
- "There is a student none of whose friends are also friends with each other."

Thank You.



Discrete Mathematical Structures

CSET106

Propositional Fallacies



Introduction

- **Definition:** Propositional fallacies are errors in reasoning that occur in the argument's proposition or premises.
- They can lead to invalid or unsound conclusions.
- Recognizing these fallacies is crucial for critical thinking.

Common Propositional Fallacies

1. **Affirming the Consequent**
   - If P, then Q.
   - Q is true.
   - Therefore, P must be true.
2. **Denying the Antecedent**
   - If P, then Q.
   - P is false.
   - Therefore, Q must be false.
3. **False Analogy**
   - Arguing on the basis of a flawed analogy.

Examples

Affirming the Consequent

- *If it's raining, the streets are wet.*
- *The streets are wet.*
- *Therefore, it's raining.*

Denying the Antecedent Example

- *Conditional Statement: If it is raining (P), then the streets are wet (Q).*
- *Denying the Antecedent: It is not raining (not P).*
- *Incorrect Conclusion: Therefore, the streets are not wet (not Q).*

False Analogy

- *Studying for exams is like preparing for a marathon.*
- *Just as marathon runners eat pasta, students should eat pasta.*
- *Therefore, eating pasta will improve exam performance.*

Conclusion

- Recognizing propositional fallacies is essential for effective argument analysis.
- Critical thinking skills help identify and avoid these common pitfalls.
- Practice identifying fallacies to improve your logical reasoning.

Thank You.



Discrete Mathematical Structures

CSET106

Consistent and Inconsistent Propositional Systems



Consistent and Inconsistent Propositional Systems

- Propositional Systems: Collections of propositions and logical connectives.

Definition

A propositional system is consistent if it does not lead to contradictions, i.e. all the propositions must be true in at least one case, or in other words - there is no way to derive a contradiction within the system; otherwise the system is inconsistent.

- **Example 1:** Consider the following propositional system.

  "He is rich or he is happy."

  "He is not rich."

  "If he is rich, then he is happy."

  Check the consistency of the above system of propositions.

  Ans.: Let p: "He is rich", q: "He is happy". So the system is

$$\begin{cases} p \vee q \\ \neg q \\ p \to q \end{cases}$$

  Given $\neg q$ is True $\implies$ p is False

  $\implies$ $p \vee q$ is True if and only if q is True.

  Besides, $p \to q$ is also True when p is False and q is True.

  $\therefore$ The system is consistent for p False and q True.

- **Example 1:** Consider the following propositional system.

  "He is rich or he is happy."

  "He is not rich."

  "If he is rich, then he is happy."

  Check the consistency of the above system of propositions.

  Ans.:

p	q	$\neg p$	$p \vee q$	$p \rightarrow q$
T	T	F	T	T
T	F	F	T	F
F	T	T	T	T
F	F	T	F	T

- **Example 2:** Consider the following propositional system.

  "He is rich or he is happy."

  "He is not rich."

  "If he is rich, then he is happy."

  "He is not happy.

  Check the consistency of the above system of propositions.

  Ans.: Let p: "He is rich", q: "He is happy". So the system is

$$\begin{cases} p \vee q \\ \neg q \\ p \rightarrow q \\ \neg p \end{cases}$$

  Clearly, all cannot be True together.

  $\therefore$ The system is inconsistent.

Conclusion

- Consistent propositional systems do not lead to contradictions.
- Inconsistent systems allow the derivation of contradictory statements.
- Ensuring consistency is essential for the reliability of logical reasoning.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Methods of Proving Theorems



Direct Proof

- A **direct proof** of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.
- **Example 1:** If a and b are even integers, then $a + b$ is even.

Direct Proof

- A **direct proof** of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using rules of inference, with the final step showing that q must also be true.
- **Example 1:** If a and b are even integers, then $a + b$ is even.
- Since a and b are even, they can be expressed as $a = 2k$ and $b = 2m$ for some integers k and m. Then,

$$a + b = 2k + 2m = 2(k + m),$$

where $k + m$ is also an integer. Therefore, $a + b$ is even.

- **Example 2:** Give a direct proof of the theorem "If n is an odd integer, then n^2 is odd."

Proof by Contraposition

- **Proofs by contraposition** make use of the fact that the conditional statement $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$.
- This means that the conditional statement $p \rightarrow q$ can be proved by showing that its contrapositive, $\neg q \rightarrow \neg p$, is true. In a proof by contraposition of $p \rightarrow q$, we take $\neg q$ as a premise, and using axioms, definitions, and previously proven theorems, together with rules of inference, we show that $\neg p$ must follow.

- **Example 1:** If n is an integer and n^2 is even, then n is even.

- **Example 1:** If n is an integer and n^2 is even, then n is even.
- We prove the contrapositive: if n is odd, then n^2 is odd. Assume n is odd, so $n = 2k + 1$ for some integer k. Then,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

which is clearly odd. Therefore, if n^2 is even, then n must be even.

- **Example 2:** Prove that if n is an integer and $3n + 2$ is odd, then n is odd.

- **Example 2:** Prove that if n is an integer and $3n + 2$ is odd, then n is odd.
- **Example 3:** Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Vacuous Proof

- We can quickly prove that a conditional statement $p \rightarrow q$ is true when we know that p is false, because $p \rightarrow q$ must be true when p is false.
- Consequently, if we can show that p is false, then we have a proof, called a **vacuous proof**, of the conditional statement $p \rightarrow q$.
- **Example :** Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.

Vacuous Proof

- We can quickly prove that a conditional statement $p \rightarrow q$ is true when we know that p is false, because $p \rightarrow q$ must be true when p is false.
- Consequently, if we can show that p is false, then we have a proof, called a **vacuous proof**, of the conditional statement $p \rightarrow q$.
- **Example :** Show that the proposition $P(0)$ is true, where $P(n)$ is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.
- Note that $P(0)$ is "If $0 > 1$, then $0^2 > 0$." We can show $P(0)$ using a vacuous proof. Indeed, the hypothesis $0 > 1$ is false. This tells us that $P(0)$ is automatically true.

Trivial Proof

- By showing that q is true, it follows that $p \rightarrow q$ must also be true. A proof of $p \rightarrow q$ that uses the fact that q is true is called a **trivial proof**.
- **Example :** Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that $P(0)$ is true.

Trivial Proof

- By showing that q is true, it follows that $p \rightarrow q$ must also be true. A proof of $p \rightarrow q$ that uses the fact that q is true is called a **trivial proof**.
- **Example :** Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$," where the domain consists of all nonnegative integers. Show that $P(0)$ is true.
- The proposition $P(0)$ is "If $a \geq b$, then $a^0 \geq b^0$." Because $a^0 = b^0 = 1$, the conclusion of the conditional statement "If $a \geq b$, then $a^0 \geq b^0$" is true. Hence, this conditional statement, which is $P(0)$, is true.
- **Note** that the hypothesis, which is the statement "$a \geq b$," was not needed in this proof.

Proof by Contradiction

- Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.

Proof by Contradiction

- Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.
- How can we find a contradiction q that might help us prove that p is true in this way?

Proof by Contradiction

- Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.
- How can we find a contradiction q that might help us prove that p is true in this way?
- The statement $r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove that p is true if we can show that $\neg p \rightarrow (r \wedge \vee r)$ is true for some proposition r. Proofs of this type are called **proofs by contradiction**.

- **Example :** Prove that $\sqrt{2}$ is an irrational number by giving a proof by contradiction.

Proofs of Equivalence

- To prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.
- $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$ is a tautology.
- **Example:** Prove the theorem "If n is an integer, then n is odd if and only if n^2 is odd."

Proof by Mathematical Induction

Principle of Mathematical Induction

To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

1. **Basis Step:** We verify that $P(1)$ is true.
2. **Inductive Step:** We show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

- Expressed as a rule of inference, this proof technique can be stated as

$$\Big(P(1) \wedge \forall k\big(P(k) \rightarrow P(k+1)\big)\Big) \rightarrow \forall n P(n),$$

when the domain is the set of positive integers.

- **Example 1:** Show that if n is a positive integer, then

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

- **Example 2:** Use mathematical induction to show that

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$$

for all nonnegative integers n.

- **Example 3:** Use mathematical induction to prove the inequality $n < 2^n$ for all positive integers n.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Russell's Paradox



Paradox

- A paradox is a logically self-contradictory statement or a statement that runs contrary to one's expectation.
- It is a statement that, despite apparently valid reasoning from true premises, leads to a seemingly self-contradictory or a logically unacceptable conclusion.

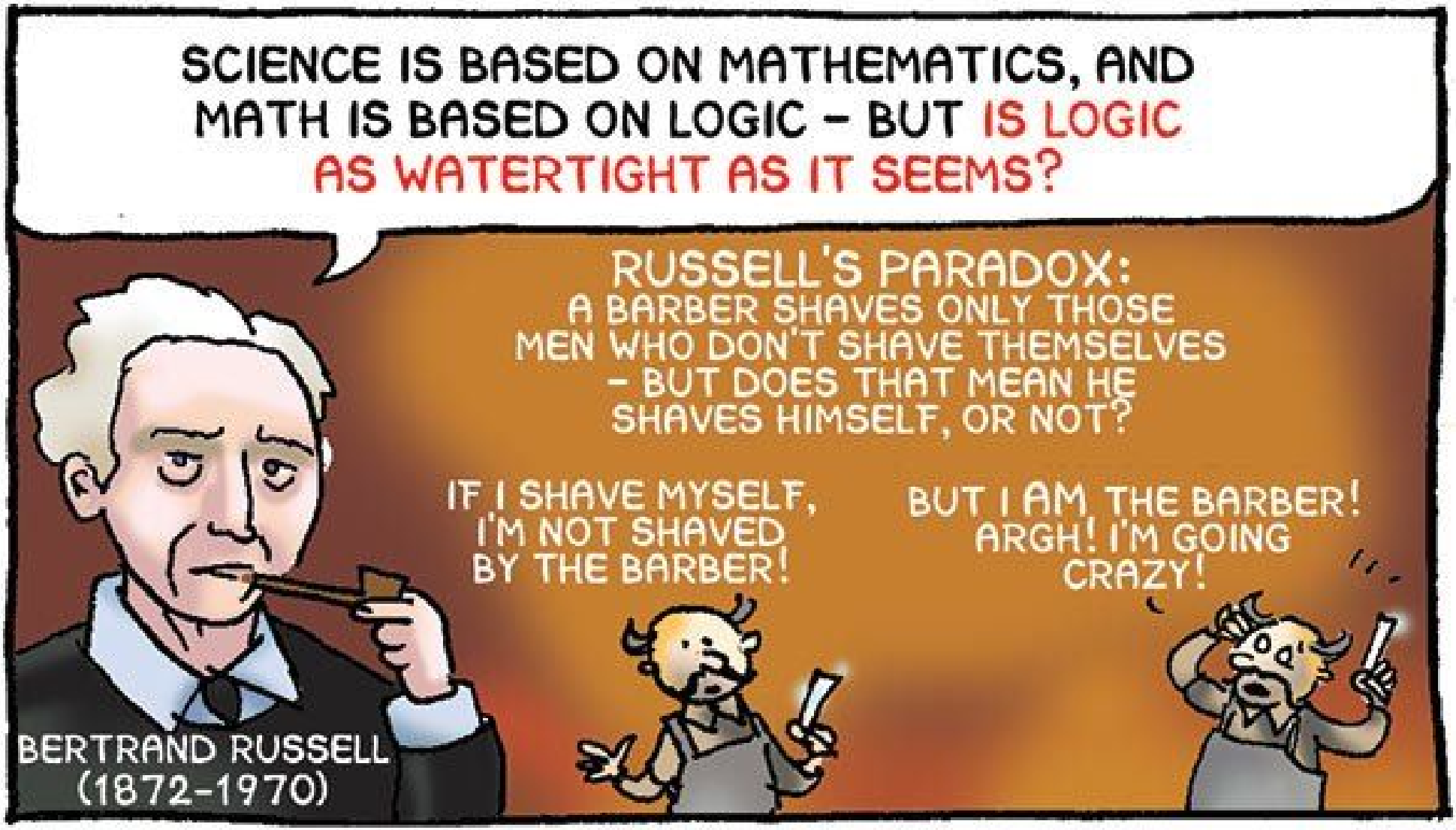
Russell's Paradox

- It shows that naive set theory leads to a contradiction.
- According to set theory any definable collection is a set.
- Let R be the set of all sets that are not members of themselves.
- Symbolically, let $R = \{x \mid x \in x\}$.
- If R is not a member of itself, then its definition dictates that it must contain itself.
- If it contains itself, then it contradicts its own definition as the set of all sets that are not member of themselves.
- Symbolically, $R = \{x \mid x \in x\}$, then $R \in R \iff R \notin R$.

The Barber Paradox

- In a town, the barber shaves everyone who does not shave themselves, but no one else.
- More precisely, in this town every man keeps himself clean-shaven, doing exactly one of these things.
  1. shaving himself
  2. going to the barber
- The question that prompts the paradox is, who shaves the barber? .
- Both the possibilities result in barber shaving himself, but this is not possible since he only shaves the men who do not shave themselves.
- There is no way to solve this pradox, it can only be avoided.
-

$$(\exists x)(\text{person}(x) \wedge (\forall y)(\text{person}(y) \implies (\text{shaves}(x, y) \iff \neg\text{shaves}(y, y))$$


SCIENCE IS BASED ON MATHEMATICS, AND MATH IS BASED ON LOGIC - BUT IS LOGIC AS WATERTIGHT AS IT SEEMS?
RUSSELL'S PARADOX:
A BARBER SHAVES ONLY THOSE MEN WHO DON'T SHAVE THEMSELVES - BUT DOES THAT MEAN HE SHAVES HIMSELF, OR NOT?
IF I SHAVE MYSELF, I'M NOT SHAVED BY THE BARBER!
BUT I AM THE BARBER! ARGH! I'M GOING CRAZY!
BERTRAND RUSSELL (1872-1970)



A version of Russell's paradox, taken from *Logicomix*.

Interesting Number Paradox

- The interesting number paradox is a humorous paradox which arises from the attempt to classify every natural number as either "interesting" or "uninteresting".
- The paradox states that every natural number is interesting.
- The "proof" is by contradiction: if there exists a non-empty set of uninteresting natural numbers, there would be a smallest uninteresting number – but the smallest uninteresting number is itself interesting because it is the smallest uninteresting number, thus producing a contradiction.

Omnipotence Paradox

- The omnipotence paradox is a logical contradiction that arises when an omnipotent being can perform any action, including creating a task that it cannot perform.
- The most well-known version of the paradox is the paradox of the stone: "Could God create a stone so heavy that even S/He could not lift it?" .
- If Yes, then s/he cannot lift it; if No, then s/he cannot create it.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Module 2

Sets



Sets

- A set is an unordered collection of objects, called elements or members of the set.
- A set is said to *contain* its elements.
- We write $a \in A$ to denote that a is an element of the set A.
- The notation $a \notin A$ denotes that a is not an element of the set A.

Methods of Describing a Set

- Roster Method:
  1. The set V of all vowels in the English alphabet can be written as $V = \{a, e, i, o, u\}$.
  2. The set of positive integers less than 100 can be denoted by $\{1, 2, 3, \cdots, 99\}$.
- Set Builder Method: We characterize all those elements in the set by stating the property or properties they must have to be members.
  1. $O = \{x \mid x \text{ is an odd positive integer less than } 10\}$, $O = \{x \in \mathbb{Z}^+ \mid x \text{ is odd and } x < 10\}$.
  2. $\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in Z, \text{ and } q \neq 0\}$, the **set of rational numbers**

Equal Sets

- Two sets are *equal* if and only if they have the same elements.
- Therefore, if A and B are sets, then A and B are equal if and only if

$$\forall x(x \in A \longleftrightarrow x \in B).$$

We write $A = B$ if A and B are equal sets.

- Example: $\{1, 3, 5\} = \{3, 5, 1\} = \{1, 3, 3, 3, 5, 5, 5, 5\}$

Empty Set and Universal Set

- The special set which has no elements is called the empty set, or null set, and is denoted by ϕ
- The set which contains all the objects under consideration is called the universal set and is denoted by U.

  Note: In Venn diagrams the universal set U is represented by a rectangle.

Subsets

- The set A is a subset of B if and only if every element of A is also an element of B. The notation used is $A \subseteq B$ to indicate that A is a subset of the set B. $A \subseteq B$ if and only if

$$\forall x(x \in A \rightarrow x \in B)$$

- When we wish to emphasize that a set A is a subset of a set B but that $A \neq B$, we write $A \subset B$ and say that A is a proper subset of B. That is, A is a proper subset of B if and only if

Subsets

- The set A is a subset of B if and only if every element of A is also an element of B. The notation used is $A \subseteq B$ to indicate that A is a subset of the set B. $A \subseteq B$ if and only if

$$\forall x(x \in A \rightarrow x \in B)$$

- When we wish to emphasize that a set A is a subset of a set B but that $A \neq B$, we write $A \subset B$ and say that A is a proper subset of B. That is, A is a proper subset of B if and only if

$$\forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A).$$

- Prove that for every set A, (i) $\phi \subseteq A$ and (ii) $A \subseteq A$.
- Proof of (i): claim: $\forall x(x \in \phi \rightarrow x \in A)$ is true.

  Hint: $x \in \phi$ is always false. This is an example of a vacuous proof.

The Size of a Set

- Let S be a set. If there are exactly n distinct elements in S where n is a nonnegative integer, we say that S is a finite set and that n is the cardinality of S. The cardinality of S is denoted by $|S|$.
- Let A be the set of odd positive integers less than 10. Then $|A| = 5$.
- A set is said to be infinite if it is not finite.
- The set of positive integers is infinite.

Power Set

- Given a set S, the power set of S is the set of all subsets of the set S. The power set of S is denoted by $\mathcal{P}(S)$.
- $\mathcal{P}(\{0,1,2\}) = \{\phi, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$.
- **Result:**

  If a set has n elements, then its power set has 2^n elements.

Cartesian Product of Sets

- Let A and B be sets. The Cartesian product of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b), where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

- $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}$.
- $A^n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A \text{ for } i = 1, 2, ..., n\}$.
- $\{1, 2\} \times \{a, b, c\} = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$.
- $(\{1, 2\})^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$.
- A subset R of the Cartesian product $A \times B$ is called a **relation** from the set A to the set B.

Set Operations

- Let A and B be sets. The union of the sets A and B, denoted by $A \cup B$, is the set that contains those elements that are either in A or in B, or in both.

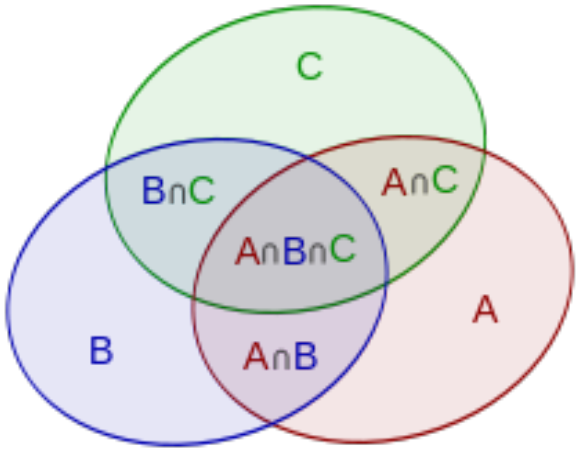
$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

- Example: $\{1, 3, 5\} \cup \{1, 2, 3\} = \{1, 2, 3, 5\}$
- Let A and B be sets. The intersection of the sets A and B, denoted by $A \cap B$, is the set containing those elements in both A and B.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

- Example: $\{1, 3, 5\} \cap \{1, 2, 3\} = \{1, 3\}$.

Principle of Inclusion–Exclusion



- $|A \cup B| = |A| + |B| - |A \cap B|$
- $$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$
- $$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} |A_{i_1} \cap \cdots \cap A_{i_k}| \right)$$

- Let A and B be sets. The difference of A and B, denoted by $A - B$ (or $A \backslash B$), is the set containing those elements that are in A but not in B. The difference of A and B is also called the complement of B with respect to A.
- $A - B = \{x \mid x \in A \wedge x \notin B\}$.
- Example: $\{1, 3, 5\} - \{1, 2, 3\} = \{5\}$.
- Let U be the universal set. The complement of the set A, denoted by $\overline{A}$, is the complement of A with respect to U. Therefore, the complement of the set A is $U - A$.
- $\overline{A} = \{x \in U \mid x \notin A\}$.
- Note: $A - B = A \cap \overline{B}$.

TABLE 1 Set Identities.

Identity	*Name*
$A \cap U = A$ $A \cup \emptyset = A$	Identity laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination laws
$A \cup A = A$ $A \cap A = A$	Idempotent laws
$\overline{(\overline{A})} = A$	Complementation law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement laws

- Prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
- Proof:

$$\overline{A \cap B} = \{x \mid x \notin A \cap B\} \text{ by definition of complement}$$

$$= \{x \mid \neg(x \in (A \cap B))\} \text{ by definition of does not belong symbol}$$

$$= \{x \mid \neg(x \in A \wedge x \in B)\} \text{ by definition of intersection}$$

$$= \{x \mid \neg(x \in A) \vee \neg(x \in B)\}$$

by the first De Morgan law for logical equivalences

$$= \{x \mid x \notin A \vee x \notin B\} \text{ by definition of does not belong symbol}$$

$$= \{x \mid x \in \overline{A} \vee x \in \overline{B}\} \text{ by definition of complement}$$

$$= \{x \mid x \in \overline{A} \cup \overline{B}\} \text{ by definition of union}$$

$$= \overline{A} \cup \overline{B} \text{ by meaning of set builder notation}$$

- Prove that $\overline{A \cup (B \cap C)} = (\overline{C} \cup \overline{B}) \cap A$ for all sets A, B, and C.
- Proof:

$$\begin{aligned}
\overline{A \cup (B \cap C)} &= \overline{A} \cap \overline{(B \cap C)} && \text{by the first De Morgan law} \\
&= \overline{A} \cap (\overline{B} \cup \overline{C}) && \text{by the second De Morgan law} \\
&= (\overline{B} \cup \overline{C}) \cap \overline{A} && \text{by the commutative law for intersections} \\
&= (\overline{C} \cup \overline{B}) \cap \overline{A} && \text{by the commutative law for unions.}
\end{aligned}$$

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Module 2

Relations

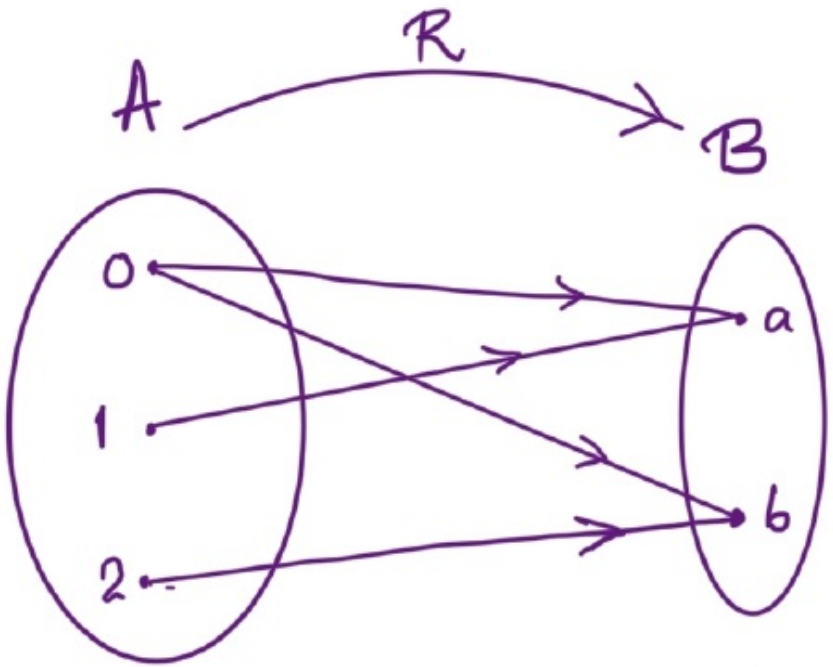


Relation

- Relationships between elements of sets are represented using the structure called a **relation**, which is just a subset of the Cartesian product of the sets.
- Relations can be used to solve problems such as determining which pairs of cities are linked by airline flights in a network, finding a viable order for the different phases of a complicated project, or producing a useful way to store information in computer databases.
- Let A and B be sets. A **binary relation** from A to B is a subset of $A \times B$.
- $a \ R \ b$ is used to denote that $(a, b) \in R$ and $a \not R \ b$ is used to denote that $(a, b) \notin R$.

Relation: Example

Let $A = \{0, 1, 2\}$ and $B = \{a, b\}$. Then $\{(0, a), (0, b), (1, a), (2, b)\}$ is a relation from A to B.



Graphical representation of R

R	a	b
0	✓	✓
1	✓	
2		✓

Tabular representation of R

Relations on a Set

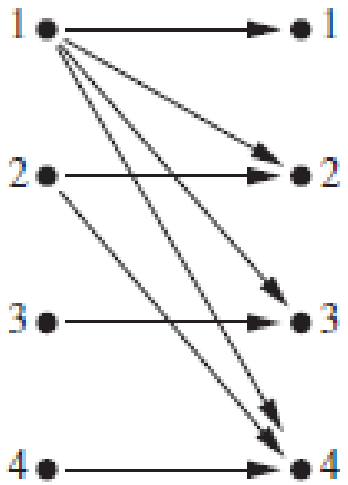
- A relation on a set A is a relation from A to A.
- **Example**: Let A be the set $\{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{(a, b) \mid a \text{ divides } b\}$?

Relations on a Set

- A relation on a set A is a relation from A to A.
- **Example**: Let A be the set $\{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{(a, b) \mid a \text{ divides } b\}$?
- $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$.
- How many relations are there on a set with n elements?

Relations on a Set

- A relation on a set A is a relation from A to A.
- **Example**: Let A be the set $\{1, 2, 3, 4\}$. Which ordered pairs are in the relation $R = \{(a, b) \mid a \text{ divides } b\}$?
- $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$.
- How many relations are there on a set with n elements? Ans. 2^{n^2}



Graphical representaion of R

R	1	2	3	4
1	×	×	×	×
2		×		×
3			×	
4				×

Tabular representation of R

Reflexive Relation

Definition

A relation R on a set A is called **reflexive** if $(a, a) \in R$ for every element $a \in A$.

- The "Greater Than or Equal To" Relation:

  In the set of real numbers, the relation "is greater than or equal to" is reflexive because every real number is greater than or equal to itself.

- The "Less Than or Equal To" Relation:

  Similarly, in the set of real numbers, the relation "is less than or equal to" is reflexive because every real number is less than or equal to itself.

Reflexive Relation

- The "Divides" Relation:

  In the set of integers, the relation "divides" is reflexive because every integer divides itself (e.g., 5 divides 5, -3 divides -3).

- The "Parallel" Relation:

  In the set of lines on a plane, the relation "is parallel to" is reflexive because every line is parallel to itself.

- The "Congruence" Relation:

  In geometry, the relation "is congruent to" is reflexive because every geometric figure is congruent to itself.

Symmetric Relation

Definition

A relation R on a set A is called **symmetric** if $(b, a) \in R$ whenever $(a, b) \in R$, for all $a, b \in A$.

- Equality Relation:

  In the set of real numbers, the relation "is equal to" is symmetric because if $a = b$, then $b = a$ for any real numbers a and b.

- Divisibility Relation:

  In the set of integers, the relation "divides evenly into" is not only reflexive but also symmetric. If a divides b evenly, then b divides a evenly as well. For example, if 2 divides 6 evenly, then 6 divides 2 evenly.

Symmetric Relation

- Set Intersection Relation:

  In the context of sets, the relation "has a non-empty intersection with" is symmetric. If set A has a non-empty intersection with set B, then set B also has a non-empty intersection with set A.

- Distance Relation in Geometry:

  In Euclidean geometry, the relation "is at the same distance as" is symmetric. If point A is at the same distance from point B as point B is from point A, then the relation is symmetric.

Antisymmetric Relation

Definition

A relation R on a set A such that for all $a, b \in A$, if $(a, b) \in R$ and $(b, a) \in R$, then $a = b$ is called **antisymmetric**.

- Strict Inequality Relation:

  In the set of real numbers, the relation "is strictly less than" is antisymmetric. If $a < b$ and $b < a$ are both true, then a and b must be the same number, which satisfies the antisymmetric property.

Antisymmetric Relation

- Subset Relation:

  In the context of sets, the relation "is a proper subset of" is antisymmetric. If A is a proper subset of B and B is a proper subset of A, then A and B must be the same set, satisfying the antisymmetric property.

- Divisibility Relation:

  In the set of integers, the relation "divides evenly into" is antisymmetric. If a divides b evenly and b divides a evenly, then a and b must be the same integer or their absolute values must be equal.

Antisymmetric Relation

- Parent Relation:

  In a set of individuals where the relation "is a parent of" is defined, this relation is often antisymmetric. If A is a parent of B and B is a parent of A, then A and B must be the same individual, satisfying the antisymmetric property.

- Square Root Relation:

  In the set of non-negative real numbers, the relation "is the square root of" is antisymmetric. If a is the square root of b and b is the square root of a, then a and b must be the same non-negative real number.

Transitive Relation

Definition

A relation R on a set A is called **transitive** if whenever $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$, for all $a, b, c \in A$.

- Subset Relation:

  In the context of sets, the relation "is a subset of" is transitive. If set A is a subset of set B and set B is a subset of set C, then set A is also a subset of set C.

Transitive Relation

- Divisibility Relation:

  In the set of integers, the relation "divides evenly into" is transitive. If integer a divides integer b evenly and integer b divides integer c evenly, then integer a divides integer c evenly.

- Less Than Relation:

  In the set of real numbers, the relation "is less than" is transitive. If a is less than b and b is less than c, then a is also less than c.

- Implication Relation:

  In logic, the implication relation "p implies q" is transitive. If p implies q and q implies r, then p implies r.

Transitive Relation

- Successor Relation:

  In the set of natural numbers, the relation "is the successor of" is transitive. If a is the successor of b and b is the successor of c, then a is also the successor of c.

Equivalence Relation

Definition

An **equivalence relation** on a set is a relation which is simultaneously reflexive, symmetric and transitive.

- Equivalence relations are fundamental in mathematics and are used to partition a set into disjoint subsets called **equivalence classes**, where elements within the same class are related to each other, and elements in different classes are not related.

Examples of Equivalence Relation

- Equality Relation:

  In the set of real numbers, the relation "is equal to" is an equivalence relation. It is reflexive, symmetric, and transitive.

- Modular Congruence Relation:

  In number theory, the relation "is congruent to modulo n" is an equivalence relation. It is reflexive, symmetric, and transitive.

- Partition Relation:

  In set theory, a partition of a set S induces an equivalence relation on S. Two elements are related if they belong to the same partition subset. This relation is reflexive, symmetric, and transitive.

Examples of Equivalence Relation

- Rational Equivalence Relation:

  In algebraic geometry, the relation "is rationally equivalent" between algebraic cycles is an equivalence relation. It is reflexive, symmetric, and transitive.

- Geometric Similarity Relation:

  In geometry, the relation "is similar to" between geometric figures (e.g., triangles) is an equivalence relation. It is reflexive, symmetric, and transitive.

Composition of Relations

Definition

Let R be a relation from a set A to a set B and S a relation from B to a set C. The composite of R and S is the relation consisting of ordered pairs (a, c), where $a \in A, c \in C$, and for which there exists an element $b \in B$ such that $(a, b) \in R$ and $(b, c) \in S$. The composite of R and S is denoted by $S \circ R$.

Example

- What is the composite of the relations R and S, where R is the relation from $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$ with $R = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$ and S is the relation from $\{1, 2, 3, 4\}$ to $\{0, 1, 2\}$ with $S = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$?

Example

- What is the composite of the relations R and S, where R is the relation from $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$ with $R = \{(1, 1), (1, 4), (2, 3), (3, 1), (3, 4)\}$ and S is the relation from $\{1, 2, 3, 4\}$ to $\{0, 1, 2\}$ with $S = \{(1, 0), (2, 0), (3, 1), (3, 2), (4, 1)\}$?
- $$S \circ R = \{(1, 0), (1, 1), (2, 1), (2, 2), (3, 0), (3, 1)\}.$$

  $S \circ R$ is constructed using all ordered pairs in R and ordered pairs in S, where the second element of the ordered pair in R agrees with the first element of the ordered pair in S.

  For example, the ordered pairs $(2, 3)$ in R and $(3, 1)$ in S produce the ordered pair $(2, 1)$ in $S \circ R$.

Matrix Representation of a Relation

- A relation between two sets A and B can also be represented using a matrix.
- The matrix representation helps us visualize and analyze the relation.
- Each row corresponds to an element of A, and each column corresponds to an element of B. So, the dimension of the matrix is $|A| \times |B|$.

Matrix Representation

Let $A = \{a, b, c\}$ and $B = \{x, y\}$.

The matrix representation of a relation R from A to B is defined as follows:

$$\text{Matrix } M_R = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \\ r_{31} & r_{32} \end{pmatrix}$$

where $r_{ij} = 1$ if $(a_i, b_j) \in R$, and $r_{ij} = 0$ otherwise.

This matrix helps us understand the relationship between elements of A and B in a clear and concise way.

Example of a Relation

Let's consider a relation R from set $A = \{a, b, c\}$ to set $B = \{x, y\}$.

The relation R is defined as:

$$R = \{(a, x), (b, y), (c, x)\}$$

The matrix representation of this relation is:

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

Matrix Representation of a Relation on a Set

Let $A = \{a, b, c\}$.

The matrix representation of a relation R on A is:

$$\text{Matrix } M_R = \begin{pmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{pmatrix}$$

where $r_{ij} = 1$ if $(a_i, a_j) \in R$, and $r_{ij} = 0$ otherwise.

Example of a Relation

Let's consider a relation R on set $A = \{a, b, c\}$.

The relation R is defined as:

$$R = \{(a, a), (b, b), (c, c), (a, c)\}$$

The matrix representation of this relation is:

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

Procedures to Check Properties

Given the matrix representation M_R of a relation R on set A:

1. **Reflexive**:
   - R is reflexive if all diagonal elements of M_R are 1 or i.e., Trace$(A) = |A|$.
2. **Symmetric**:
   - R is symmetric if M_R is symmetric about the main diagonal.
3. **Antisymmetric**:
   - R is antisymmetric if M_R satisfies $r_{ij} = 1$ and $r_{ji} = 1$ only when $i = j$.

     In other words, if $i \neq j$, then $a_{ij}a_{ji} = 0$.

Example

Let's consider a relation R on set $A = \{a, b, c\}$ with the matrix representation:

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

The matrix M_R represents the relation R on set A.

Reflexive, Anti-symmetric, Transitive

M_R^2:

$$M_R^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Union of Relations

- Let R_1 and R_2 be two relations on sets A and B. The union $R_1 \cup R_2$ of R_1 and R_2 is defined as:

$$(a, b) \in (R_1 \cup R_2) \quad \text{if and only if} \quad (a, b) \in R_1 \text{ or } (a, b) \in R_2$$

- The matrix representation of $R_1 \cup R_2$ is the element-wise maximum of the matrices representing R_1 and R_2 or it is the bit-wise $\vee$ operation.

$$M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2}.$$

Intersection of Relations

- The intersection $R_1 \cap R_2$ of R_1 and R_2 is defined as:

$$(a, b) \in (R_1 \cap R_2) \quad \text{if and only if} \quad (a, b) \in R_1 \text{ and } (a, b) \in R_2$$

- The matrix representation of $R_1 \cap R_2$ is the element-wise minimum of the matrices representing R_1 and R_2 or it is the bit-wise $\wedge$ operation.

$$M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}.$$

Composition of Relations

- Let R_1 be a relation from set A to B and R_2 be a relation from set B to C. The composition $R_2 \circ R_1$ is defined as:

  $(a, c) \in (R_2 \circ R_1)$ if and only if $\exists b \in B : (a, b) \in R_1$ and $(b, c) \in R_2$

- The matrix representation of $R_2 \circ R_1$ can be obtained by multiplying the matrices representing R_1 and R_2 and then replacing each non-zero entries by 1.

$$M_{R_2 \circ R_1} = M_1 \odot M_2.$$

- **Example**: Consider the following two relations R_1 and R_2 on the set $\{1, 2, 3\}$ defined as $R_1 = \{(1, 1), (2, 2), (2, 3)\},\ R_2 = \{(3, 3), (2, 3)\}$.. Then $R_1 \cup R_2 = \{(1, 1), (2, 2), (2, 3), (3, 3)\}$ and $R_1 \cap R_2 = \{(2, 3)\}$.

$$M_{R_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \qquad M_{R_2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

- **Example**: Consider the following two relations R_1 and R_2 on the set $\{1, 2, 3\}$ defined as $R_1 = \{(1, 1), (2, 2), (2, 3)\},\ R_2 = \{(3, 3), (2, 3)\}$.. Then $R_1 \cup R_2 = \{(1, 1), (2, 2), (2, 3), (3, 3)\}$ and $R_1 \cap R_2 = \{(2, 3)\}$.

$$M_{R_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \qquad M_{R_2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$M_{R_1 \cup R_2} = \begin{pmatrix} 1 \vee 0 & 0 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 1 \vee 0 & 1 \vee 1 \\ 0 \vee 0 & 0 \vee 0 & 0 \vee 1 \end{pmatrix}, \ M_{R_1 \cap R_2} = \begin{pmatrix} 1 \wedge 0 & 0 \wedge 0 & 0 \wedge 0 \\ 0 \wedge 0 & 1 \wedge 0 & 1 \wedge 1 \\ 0 \wedge 0 & 0 \wedge 0 & 0 \wedge 1 \end{pmatrix}$$

- **Example**: Consider the following two relations R_1 and R_2 on the set $\{1, 2, 3\}$ defined as $R_1 = \{(1, 1), (2, 2), (2, 3)\},\ R_2 = \{(3, 3), (2, 3)\}$.. Then $R_1 \cup R_2 = \{(1, 1), (2, 2), (2, 3), (3, 3)\}$ and $R_1 \cap R_2 = \{(2, 3)\}$.

$$M_{R_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \qquad M_{R_2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

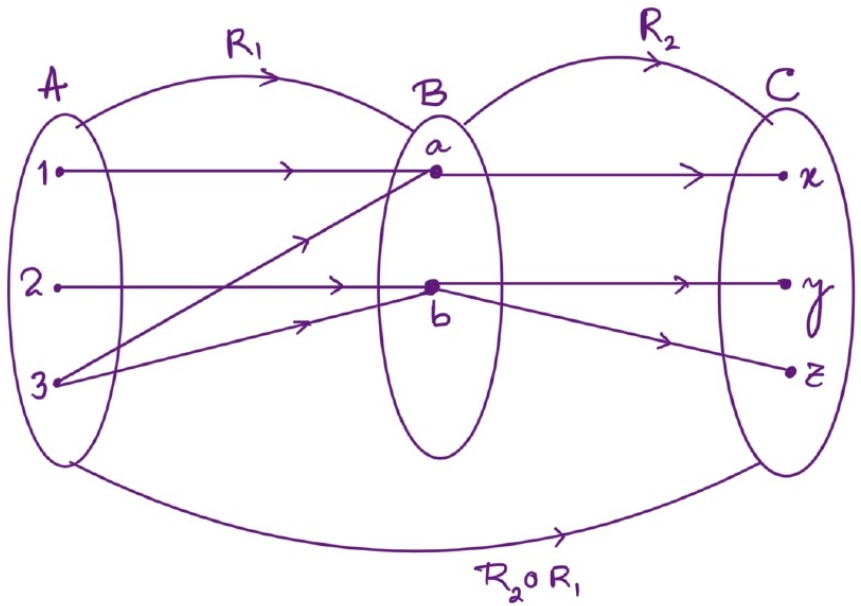
$$M_{R_1 \cup R_2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad M_{R_1 \cap R_2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

One can consider entry-wise maximum and minimum in case of $M_{R_1 \cup R_2}$ and $M_{R_1 \cap R_2}$, respectively.

Example of Composition of Relations

- Consider the relations $R_1 : A \to B$ and $R_2 : B \to C$ defined as $R_1 = \{(1, a), (2, b), (3, a), (3, b)\}$ and $R_2 = \{(a, x), (b, y), (b, z)\}$.
- Then $R_2 \circ R_1 : A \to C$ given by

$$R_2 \circ R_1 = \{(1, x), (2, y), (2, z), (3, x), (3, y), (3, z)\}.$$



Example of Composition of Relations

- Consider the relations $R_1 : A \to B$ and $R_2 : B \to C$ defined as $R_1 = \{(1, a), (2, b), (3, a), (3, b)\}$ and $R_2 = \{(a, x), (b, y), (b, z)\}$.
- Then $R_2 \circ R_1 : A \to C$ given by

$$R_2 \circ R_1 = \{(1, x), (2, y), (2, z), (3, x), (3, y), (3, z)\}.$$

- $M_{R_1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad M_{R_2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad \therefore M_{R_2 \circ R_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

$$M_{R_2 \circ R_1} = M_1 \odot M_2.$$

Closure of a Relation

- Let R be a relation on a set A. The closure of R with respect to a property P is denoted by R_P and is the smallest relation containing R that satisfies property P.
- Let R be a relation on set A. The **reflexive closure** of R, denoted by R_{ref}, is obtained by adding all pairs (a, a) to R for every $a \in A$ such that $(a, a) \notin R$.
- Let R be a relation on set A. The **symmetric closure** of R, denoted by R_{sym}, is obtained by adding (b, a) to R whenever $(a, b) \in R$ and $(b, a) \notin R$.
- Let R be a relation on set A. The **transitive closure** of R, denoted by R_{trans}, is obtained by adding (a, c) to R whenever $(a, b) \in R$ and $(b, c) \in R$.

Example of Closure of a Relation

Let's consider a relation R on set $A = \{1, 2, 3\}$:

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

- The reflexive closure R_{ref} adds $(3, 3)$ to R:

$$R_{\text{ref}} = \{(1, 1), (1, 2), (2, 2), (2, 3), (3, 3)\}$$

- The symmetric closure R_{sym} adds $(2, 1)$ and $(3, 2)$ to R:

$$R_{\text{sym}} = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 2)\}$$

- The transitive closure R_{trans} adds $(1, 3)$ to R:

$$R_{\text{trans}} = \{(1, 1), (1, 2), (2, 2), (2, 3), (1, 3)\}$$

Digraph Representation of a Relation

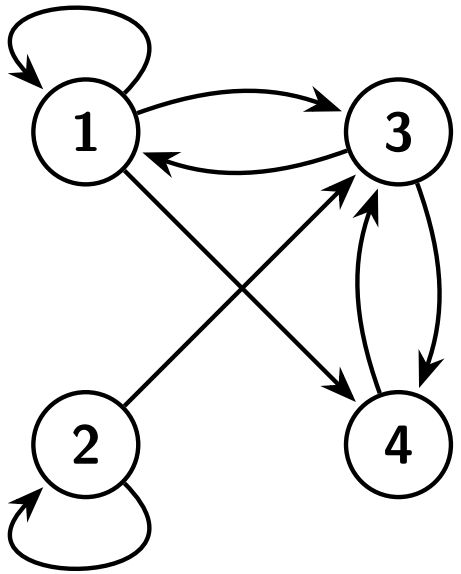
Consider the relation

$$R = \{(1,1),(1,3),(1,4),(2,2),(2,3),(3,1),(3,4),(4,3)\}$$

defined on the set $A = \{1,2,3,4\}$.

Let's consider the matrix of R:

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



Procedures to Check Relation Properties

Given the digraph representation of a relation R on set A:

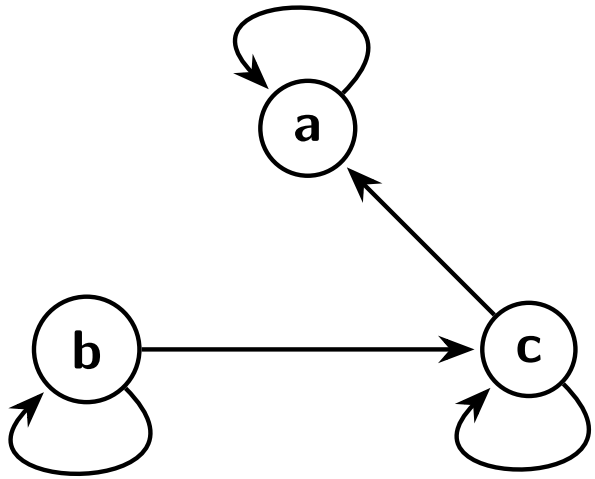
Procedure to Check Properties:

1. **Reflexive**:
   - R is reflexive if every node has a loop to itself.
2. **Symmetric**:
   - R is symmetric if for every directed edge from x to y, there is a directed edge from y to x.
3. **Antisymmetric**:
   - R is antisymmetric if for every pair of distinct nodes x and y, if there is a directed edge from x to y and a directed edge from y to x, then $x = y$.
4. **Transitive**:
   - R is transitive if for every pair of nodes x and y, if there is a directed path from x to y, then there is a direct edge from x to y.

Example: Checking Relation Properties

For the given digraph representation:

1. **Reflexive**:
   - Every node has a loop to itself.
   - $\therefore R$ is reflexive.



2. **Symmetric**:
   - For $b \to c$, there is no $c \to b$.
   - $\therefore R$ is not symmetric.
3. **Antisymmetric**:
   - There are no nodes with both $x \to y$ and $y \to x$ for distinct x and y.
   - $\therefore R$ is antisymmetric.
4. **Transitive**:
   - There is a path from b to a $(b \to c \to a)$, but no direct edge $b \to a$.
   - $\therefore R$ is not transitive.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Module 2

Fuzzy Sets



What are Fuzzy Sets?

- The word "fuzzy" means "vagueness (ambiguity)".
- Introduced by Lotfi Zadeh in 1965.
- Classical set theory allows the membership of the elements in the set in binary terms.
- Fuzzy set theory permits membership function valued in the interval $[0, 1]$.
- Fuzzy sets are a generalization of classical sets where elements have a degree of membership rather than a strict binary classification.
- Fuzzy sets allow for a more flexible representation of uncertainty and vagueness.

Fuzzy Sets

- Words like young, tall, good or high are fuzzy.
- There is no single quantitative value which defines the term young.
- For some people, age 25 is young, and for others, age 35 is young.
- The concept young has no clean boundary.
- Age 35 has some possibility of being young and usually depends on the context in which it is being considered.

  Fuzzy set theory is an extension of classical set theory where elements have **degree of membership**.

Crisp Set vs Fuzzy Set

- **Is 5+2=10?**
  - Crisp Set: Either yes or no (No ambiguity)
- **Is Navi honest?**
  - Fuzzy Set:
    - Extremely honest: 1
    - Very honest: 0.8
    - Honest at times: 0.4
    - Extremely dishonest: 0

Fuzzy Sets: Examples

- **Tallness in Humans:** In a fuzzy set representing "tall humans," the degree of membership could vary for individuals based on their height. Someone who is 6'5" might have a higher degree of membership (closer to 1) compared to someone who is 5'5", whose degree of membership might be lower but still non-zero.
- **Temperature:** Consider a fuzzy set representing "hot water." Water at 100°C might have a high degree of membership (close to 1), while water at 50°C might have a lower degree of membership but still be somewhat considered "hot."
- **Speed Limits:** In a fuzzy set representing "high-speed traffic," cars traveling at 90 mph might have a high degree of membership, while cars traveling at 40 mph might have a lower degree of membership but still be considered as part of the set to some extent.

- **Age Groups:** A fuzzy set representing "old age" might include people in their 60s, 70s, and 80s, with varying degrees of membership depending on how close their age is to these boundaries.
- **Health Levels:** A fuzzy set representing "good health" might include people with different levels of physical fitness, with individuals who exercise regularly having a higher degree of membership compared to those who lead a sedentary lifestyle.

Examples of Fuzzy Sets with Membership Values

- **Tallness in Humans**:
  - John: Membership = 0.8 (John is quite tall)
  - Sarah: Membership = 0.5 (Sarah is of average height)
  - Tom: Membership = 0.2 (Tom is relatively short)
- **Temperature**:
  - Water at 100°C: Membership = 0.9 (Very hot)
  - Water at 50°C: Membership = 0.6 (Warm)
  - Water at 20°C: Membership = 0.3 (Cool)
- **Speed Limits**:
  - Car traveling at 90 mph: Membership = 0.8 (High-speed)
  - Car traveling at 40 mph: Membership = 0.4 (Moderate-speed)
  - Car traveling at 10 mph: Membership = 0.1 (Low-speed)

- **Age Groups**:
  - Person aged 65: Membership = 0.8 (Considered old)
  - Person aged 40: Membership = 0.3 (Considered middle-aged)
  - Person aged 20: Membership = 0.1 (Considered young)
- **Health Levels**:
  - Athlete: Membership = 0.9 (Very healthy)
  - Regular Exerciser: Membership = 0.7 (Fairly healthy)
  - Sedentary Lifestyle: Membership = 0.3 (Not very healthy)

Definition

If X is an universe of discourse and x is a particular element of X, then a **fuzzy set** A is defined on X and can be written as a collection of ordered pairs

$$A = \{\big(x, \mu_A(x)\big) | x \in X, \mu_A(x) : X \to [0, 1]\},$$

where $\mu_A(x)$ is the **membership function** associated with the fuzzy set A.

Example of a Fuzzy Set: Warmth in Weather

- Let W represent the fuzzy set of warmth in weather, where x is the temperature in degrees Celsius.
- The membership function $\mu_W(x)$ can be defined as follows:

$$\mu_W(x) = \begin{cases} 1 & \text{if } x \geq 30 \text{ (Very warm)} \\ \frac{x-20}{10} & \text{if } 20 \leq x < 30 \text{ (Moderately warm)} \\ 0 & \text{if } x < 20 \text{ (Not warm)} \end{cases}$$

- When the temperature is 35°C, $\mu_W(35) = 1$, indicating that it is very warm.
- When the temperature is 25°C, $\mu_W(25) = 0.5$, indicating that it is moderately warm.
- When the temperature is 15°C, $\mu_W(15) = 0$, indicating that it is not warm.

Example of a Fuzzy Set: Membership in a Social Club

- Let M represent the fuzzy set of membership in a social club, where x is the number of social events attended by an individual.
- The membership function $\mu_M(x)$ can be defined as follows:

$$\mu_M(x) = \begin{cases} 1 & \text{if } x \geq 10 \text{ (Very active member)} \\ \frac{x}{10} & \text{if } 0 \leq x < 10 \text{ (Moderately active member)} \\ 0 & \text{if } x = 0 \text{ (Non-member)} \end{cases}$$

- If an individual attends 15 events, $\mu_M(15) = 1$, indicating that they are a very active member.
- If an individual attends 5 events, $\mu_M(5) = 0.5$, indicating that they are a moderately active member.
- If an individual doesn't attend any event, $\mu_M(0) = 0$, indicating that they are not a member.

Example of Fuzzy Set: Smartness of Students

- Let $X = \{$Hritik, Mohit, Alia, Shilpi, Khusi, Virat, Rohit$\}$ be the reference set of students.
- Let A be the fuzzy set of "smart" students, where "smart" is fuzzy term.
- $A = \{(\text{Hritik}, 0.7), (\text{Mohit}, 0.6), (\text{Alia}, 0.4), (\text{Khushi}, 0.9)\}$
- Here A indicates that the smartness of Hritik is 0.7 and so on.

Example: Fuzzy Set of Brilliant Students

- In a certain class, based on the percentage of marks in the final exam, we can define a fuzzy set of brilliant students (B) as follows:

$$\mu_B(x) = \begin{cases} 1 & \text{if } x \geq 75 \\ x/75 & \text{if } x < 75 \end{cases}$$

Student	**Marks**	**Membership**
Stud1	79	1
Stud2	74	0.99
Stud3	50	0.67

Table: Membership function

The grades of membership show the belongingness of the element to the set.

Operations on Fuzzy Sets

- Union
- Intersection
- Complement
- Cardinality

Operations on Fuzzy Sets

Given X to be the universe of discourse and A and B to be fuzzy sets with $\mu_A(x)$ and $\mu_B(x)$ are their respective membership function, the fuzzy set operations are as follows:

Union:	$\mu_{A\cup B}(x) = \max\{\mu_A(x), \mu_B(x)\} \quad \text{for } x \in X.$
Intersection:	$\mu_{A\cap B}(x) = \min\{\mu_A(x), \mu_B(x)\} \quad \text{for } x \in X.$
Complement:	$\overline{\mu_A}(x) = 1 - \mu_A(x) \quad \text{for } x \in X.$

- The fuzzy union of two fuzzy sets A and B, denoted by $A \cup B$, represents the degree to which elements belong to either A or B.
- The fuzzy intersection of two fuzzy sets A and B, denoted by $A \cap B$, represents the degree to which elements belong to both A and B.
- The fuzzy complement of a fuzzy set A, denoted by $\overline{A}$, represents the degree to which elements do not belong to A.

Examples of Fuzzy Operations

- **Example 1**: Consider the fuzzy set $A = \{(x, 0.5), (y, 0.7), (z, 0)\}$ and fuzzy set $B = \{(x, 0.8), (y, 0.2), (z, 1)\}$. Then
- **Union**:

Examples of Fuzzy Operations

- **Example 1**: Consider the fuzzy set $A = \{(x, 0.5), (y, 0.7), (z, 0)\}$ and fuzzy set $B = \{(x, 0.8), (y, 0.2), (z, 1)\}$. Then
- **Union**: $A \cup B = \{(x, 0.8), (y, 0.7), (z, 1)\}$

  Because $\mu_{A \cup B}(x) = \max(\mu_A(x), \mu_B(x)) = \max(0.5, 0.8) = 0.8$;

  $\mu_{A \cup B}(y) = 0.7$ and $\mu_{A \cup B}(z) = 1$.
- **Intersection**:

Examples of Fuzzy Operations

- **Example 1**: Consider the fuzzy set $A = \{(x, 0.5), (y, 0.7), (z, 0)\}$ and fuzzy set $B = \{(x, 0.8), (y, 0.2), (z, 1)\}$. Then
- **Union**: $A \cup B = \{(x, 0.8), (y, 0.7), (z, 1)\}$

  Because $\mu_{A \cup B}(x) = \max(\mu_A(x), \mu_B(x)) = \max(0.5, 0.8) = 0.8$;

  $\mu_{A \cup B}(y) = 0.7$ and $\mu_{A \cup B}(z) = 1$.
- **Intersection**: $A \cap B = \{(x, 0.5), (y, 0.2), (z, 0)\}$
- **Complement**:

Examples of Fuzzy Operations

- **Example 1**: Consider the fuzzy set $A = \{(x, 0.5), (y, 0.7), (z, 0)\}$ and fuzzy set $B = \{(x, 0.8), (y, 0.2), (z, 1)\}$. Then
- **Union**: $A \cup B = \{(x, 0.8), (y, 0.7), (z, 1)\}$

  Because $\mu_{A \cup B}(x) = \max(\mu_A(x), \mu_B(x)) = \max(0.5, 0.8) = 0.8$;

  $\mu_{A \cup B}(y) = 0.7$ and $\mu_{A \cup B}(z) = 1$.
- **Intersection**: $A \cap B = \{(x, 0.5), (y, 0.2), (z, 0)\}$
- **Complement**: $\overline{A} = \{(x, 0.5), (y, 0.3), (z, 1)\}$.

- **Example 2**: Let A represent tallness and B represent shortness of people. Fuzzy sets A and B are defined as follows:

$$A = \{(5\text{ft}, 0.2), (6\text{ft}, 0.8), (7\text{ft}, 0.5)\}$$

$$B = \{(5\text{ft}, 0.8), (6\text{ft}, 0.2), (7\text{ft}, 0.6)\}$$

- The fuzzy set operations are performed as follows:

  Union (A $\cup$ B):

$$A \cup B = \{(5\text{ft}, 0.8), (6\text{ft}, 0.8), (7\text{ft}, 0.6)\}$$

- **Example 2**: Let A represent tallness and B represent shortness of people. Fuzzy sets A and B are defined as follows:

$$A = \{(5\text{ft}, 0.2), (6\text{ft}, 0.8), (7\text{ft}, 0.5)\}$$

$$B = \{(5\text{ft}, 0.8), (6\text{ft}, 0.2), (7\text{ft}, 0.6)\}$$

- The fuzzy set operations are performed as follows:

  Intersection (A $\cap$ B):

$$A \cap B = \{(5\text{ft}, 0.2), (6\text{ft}, 0.2), (7\text{ft}, 0.5)\}$$

- **Example 2**: Let A represent tallness and B represent shortness of people. Fuzzy sets A and B are defined as follows:

$$A = \{(5\text{ft}, 0.2), (6\text{ft}, 0.8), (7\text{ft}, 0.5)\}$$

$$B = \{(5\text{ft}, 0.8), (6\text{ft}, 0.2), (7\text{ft}, 0.6)\}$$

- The fuzzy set operations are performed as follows:

  Complement ($\overline{A}$):

$$\overline{A} = \{(5\text{ft}, 0.8), (6\text{ft}, 0.2), (7\text{ft}, 0.5)\}$$

- **Example 3**: Let X be the universe of discourse representing the temperature in Celsius. Define two fuzzy sets A and B on X as follows:

$$A = \{(0, 0.2), (10, 0.5), (20, 0.8), (30, 0.5), (40, 0.2)\}$$

$$B = \{(0, 0.5), (10, 0.8), (20, 1.0), (30, 0.8), (40, 0.5)\}$$

- The fuzzy set operations yield:

  Union $(A \cup B)$:

$$A \cup B = \{(0, 0.5), (10, 0.8), (20, 1.0), (30, 0.8), (40, 0.5)\}$$

- **Example 3**: Let X be the universe of discourse representing the temperature in Celsius. Define two fuzzy sets A and B on X as follows:

$$A = \{(0, 0.2), (10, 0.5), (20, 0.8), (30, 0.5), (40, 0.2)\}$$

$$B = \{(0, 0.5), (10, 0.8), (20, 1.0), (30, 0.8), (40, 0.5)\}$$

- The fuzzy set operations yield:

  Intersection $(A \cap B)$:

$$A \cap B = \{(0, 0.2), (10, 0.5), (20, 0.8), (30, 0.5), (40, 0.2)\}$$

- **Example 3**: Let X be the universe of discourse representing the temperature in Celsius. Define two fuzzy sets A and B on X as follows:

$$A = \{(0, 0.2), (10, 0.5), (20, 0.8), (30, 0.5), (40, 0.2)\}$$

$$B = \{(0, 0.5), (10, 0.8), (20, 1.0), (30, 0.8), (40, 0.5)\}$$

- The fuzzy set operations yield:

  Complement ($\overline{A}$):

$$\overline{A} = \{(0, 0.8), (10, 0.5), (20, 0.2), (30, 0.5), (40, 0.8)\}$$

Alpha Cut and Strong Alpha Cut in Fuzzy Sets

- An **alpha cut** of a fuzzy set A is a crisp set containing all elements x from the universe of discourse X whose membership degree in A is greater than or equal to α, where α is a specified threshold.

$$\alpha_A = \{x \mid \mu_A(x) \geq \alpha\}$$

- **Example**: Consider a fuzzy set A representing temperature levels:

$$A = \{(0°\text{C}, 0.2), (10°\text{C}, 0.5), (20°\text{C}, 0.8), (30°\text{C}, 0.6), (40°\text{C}, 0.2)\}$$

An alpha cut for $\alpha = 0.5$ would include $(10°\text{C}, 0.5)$, $(20°\text{C}, 0.8)$ and $(30°\text{C}, 0.6)$.

$$\therefore A_{0.5} = \{10°\text{C}, 20°\text{C}, 30°\text{C}\}.$$

Alpha Cut and Strong Alpha Cut in Fuzzy Sets

- A **strong alpha cut** of a fuzzy set A is a crisp set containing all elements x from the universe of discourse X whose membership degree in A is greater than α.

$$\alpha_A^+ = \{x \mid \mu_A(x) > \alpha\}$$

- **Example**: Using the same fuzzy set A as above, the strong alpha cut for $\alpha = 0.5$ would include $(20°\text{C}, 0.8)$, and $(30°\text{C}, 0.5)$.

$$\therefore A_{0.5}^+ = \{20°\text{C}, 30°\text{C}\}.$$

- **Example**: Let A be a fuzzy set on a set $X = \{10, 20, 30, 40, 50\}$ whose membership function is defined as :

$$\mu_A(x) = \frac{x}{x + 10}.$$

Find A_α for $\alpha = 0.6$.

- Fuzzy Set

$$A = \{(10, 0.5), (20, 0.67), (30, 0.75), (40, 0.80), (50, 0.83)\}.$$

- $A_{0.6} = \{20, 30, 40, 50\}$

Support and Crossover Point of a Fuzzy Set

- Given a fuzzy set A, defined on X, **support** of A is the crisp set that contains all the elements of X that have a non-zero grade of membership in A and is denoted by Supp(A).
- It is a strong α-cut of A for $\alpha = 0$, i.e.

$$\text{Supp}(A) = A_0^+ = \{x \in X \mid \mu_A(x) > 0\}.$$

- The element $x \in X$ at which $\mu_A(x) = 0.5$ is called the **crossover point**.
- **Example**: Let $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Fuzzy Set $A = \{(1, 0), (2, 0), (3, 0.2), (4, 0.5), (5, 0.3), (6, 0.4), (7, 0), (8, 0), (9, 0), (10, 0)\}$ Then Supp$(A) = \{3, 4, 5, 6\}$ and $x = 4$ is the Crossover Point.

Core and Height of a Fuzzy Set

- The **core** of a fuzzy set is the α-cut of A for which $\alpha = 1$ and it is denoted by Core(A).

$$\text{Core}(A) = \{x \in X \mid \mu_A(x) = 1\}.$$

- The **height** of a fuzzy set is the highest grade of membership of any element in the set and it is denoted by $h(A)$.

$$h(A) = \max_{x \in X} \mu_A(x).$$

Cardinality of a Fuzzy Set

- In fuzzy set theory, the cardinality of a fuzzy set measures the degree of membership of elements in the set.
- The **cardinality** of a fuzzy set A, denoted $\text{Card}(A)$, is defined as:

$$\text{Card}(A) = \sum_{x \in X} \mu_A(x)$$

where $\mu_A(x)$ represents the degree of membership of element x in the fuzzy set A.

- The cardinality of a fuzzy set provides a measure of its "size" taking into account the varying degrees of membership of its elements.

Example of Cardinality of a Fuzzy Set

Consider a fuzzy set A defined on the universe of discourse $X = \{1, 2, 3, 4, 5\}$ with membership degrees:

$$\mu_A(1) = 0.8$$

$$\mu_A(2) = 0.6$$

$$\mu_A(3) = 0.4$$

$$\mu_A(4) = 0.2$$

$$\mu_A(5) = 0.1$$

The cardinality of A is calculated as:

$$\text{Card}(A) = 0.8 + 0.6 + 0.4 + 0.2 + 0.1 = 2.1$$

Appendix*

Membership Function Types

1. Triangular Membership Function:
   - Defined by three parameters: lower bound, upper bound, and peak.
   - Membership value starts at 0, increases linearly to 1 at the peak, then decreases linearly.
2. Trapezoidal Membership Function:
   - Defined by four parameters: lower bound, upper bound, and two points defining the plateau width.
   - Membership value increases linearly to 1, remains constant within the plateau, then decreases linearly.
3. Gaussian (Normal) Membership Function:
   - Bell-shaped curve resembling the normal distribution.

Membership Function Types

- Defined by mean and standard deviation.

4. Sigmoidal Membership Function:
   - S-shaped curve.
   - Defined by slope and center.
5. Generalized Bell Membership Function:
   - More flexible than Gaussian functions.
   - Defined by width, slope, and center.
6. Singleton Membership Function:
   - Assigns membership value of 1 to a single point and 0 elsewhere.
   - Useful for representing crisp values.

Applications of Fuzzy Sets

- Fuzzy Logic Controllers
- Fuzzy Pattern Recognition
- Fuzzy Expert Systems
- Fuzzy Decision Making

Application: HVAC

Automatic climate control systems for buildings adjust heating, ventilation, and air conditioning (HVAC) settings based on environmental conditions. Fuzzy logic enables these systems to adapt to changing conditions in a flexible and intuitive manner.

Temperature Control

Traditional HVAC systems use crisp thresholds for temperature control. Fuzzy logic allows for more nuanced control by representing temperature preferences as fuzzy sets like “slightly cool,” “comfortable,” and “slightly warm.”

- Fuzzy rules and membership functions are used to adjust heating and cooling levels gradually based on occupants’ comfort preferences.
- Example: If the current temperature is ”slightly warm,” decrease heating gradually to achieve comfort.

Humidity Regulation

Fuzzy logic is also applied to regulate humidity levels. Fuzzy sets like “dry,” “comfortable,” and “humid” represent different humidity levels.

- Fuzzy rules specify how the HVAC system adjusts humidity levels based on sensor readings and occupants’ preferences.
- Example: If the humidity level is ”humid,” increase ventilation to reduce humidity.

Energy Efficiency

Fuzzy logic helps improve energy efficiency by optimizing HVAC system operation based on real-time conditions and occupants' comfort requirements.

- Dynamic adjustment of setpoints and control parameters minimizes energy consumption while maintaining comfort.
- Example: If outdoor temperatures are mild and occupancy is low, reduce heating or cooling output to conserve energy.

Conclusion

Fuzzy sets and fuzzy logic enable HVAC systems to make intelligent decisions about temperature and humidity control, providing comfortable indoor environments while optimizing energy usage and operational efficiency.

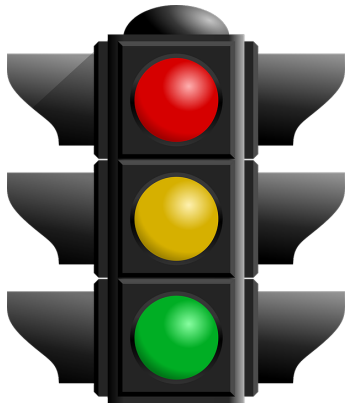
Further Examples of Fuzzy Sets in Decision Making

Appendix**

(not for examination point of view)

Traffic Control Systems

Fuzzy logic optimizes traffic flow at intersections by dynamically adjusting traffic signal timings based on real-time conditions.



- Fuzzy sets represent variables such as vehicle speed, density, and distance to intersection.
- Fuzzy rules adjust traffic signals to reduce congestion and improve traffic efficiency.

Product Quality Assessment

Fuzzy logic assesses product quality in manufacturing industries by combining multiple quality attributes into an overall quality score.

- Fuzzy sets represent dimensions like dimensional accuracy, surface finish, and material strength.
- Fuzzy inference systems help make decisions about product acceptance and process improvement.

Portfolio Management

Fuzzy logic optimizes investment strategies in financial portfolio management by dynamically adjusting portfolio allocations based on market conditions and investor preferences.

- Fuzzy sets represent variables like risk tolerance, return expectations, and asset volatility.
- Fuzzy rules balance risk and return to achieve optimal investment outcomes.

Medical Diagnosis

Fuzzy logic aids medical diagnosis by interpreting clinical data and generating diagnostic hypotheses.

- Fuzzy sets represent symptoms, test results, and patient characteristics.
- Fuzzy inference systems improve diagnostic accuracy by considering uncertainty and imprecision in medical data.

Robotics and Automation

Fuzzy logic controls robotics and automation systems by adapting to uncertain environments and performing tasks with varying precision.

- Fuzzy sets represent sensory inputs like distance measurements and object recognition.
- Fuzzy rules generate control signals for robotic actuators, enabling effective navigation, manipulation, and interaction.

Examples of Fuzzy Sets in Pattern Recognition

Handwritten Character Recognition

Fuzzy sets are used in handwritten character recognition systems to classify ambiguous or distorted characters.

- Fuzzy membership functions represent the similarity between input characters and prototype patterns.
- Fuzzy inference systems determine the most likely character class, even for ambiguous characters.

Face Recognition

Fuzzy sets play a role in facial recognition systems to cope with variations in facial expressions, lighting conditions, and occlusions.

- Fuzzy sets represent facial features and variations using linguistic terms like "round face" or "smiling lips."
- Fuzzy inference mechanisms combine fuzzy features to match and classify faces accurately across diverse conditions.

Object Recognition in Computer Vision

Fuzzy sets are utilized in object recognition tasks to handle uncertainties in object appearance and context.

- Fuzzy membership functions represent object features such as shape, texture, and color with varying degrees of certainty.
- Fuzzy clustering and classification techniques use fuzzy representations to identify objects robustly in complex visual scenes.

Biometric Identification

Fuzzy sets are applied in biometric identification systems to account for variations in biometric data due to aging, environmental conditions, and sensor noise.

- Fuzzy sets represent biometric features such as fingerprint minutiae or iris patterns, capturing inherent uncertainty.
- Fuzzy matching algorithms compare input biometric samples with reference templates, enabling flexible and adaptive identification.

Speech Recognition

Fuzzy sets are used in speech recognition systems to handle variations in speech patterns, accents, and background noise.

- Fuzzy linguistic variables represent phonetic features and acoustic characteristics of speech signals.
- Fuzzy rules and inference mechanisms interpret spoken words accurately even in challenging acoustic environments.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Module 3

Inclusion-Exclusion Principle, Binomial Coefficients, Permutaion, Combination,

Pigeonhole Principle



Inclusion-Exclusion Principle

- Suppose two tasks A and B can occur in n_1 and n_2 ways, where some of the n_1 and n_2 ways may be same. In this case, just $n_1 + n_2$ cannot be considered as it may count the same ways twice. Therefore, in such a case, **inclusion-exclusion principle** is applied.
- Let $|A|$ denote the cardinal number of set A, then it follows immediately that

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Example

- In how many ways can we select an ace or a heart from a pack of cards?
- **Solution:** There are 4 aces and 13 cards of heart in a pack of cards and 1 card is common to both. If A is the event of getting an ace, H is the event of getting an heart, then $|A| = 4, |H| = 13$ and $|A \cap H| = 1$.

  $\therefore$ the number ways one can select an ace or a heart from a pack of cards is given by

$$|A \cup H| = |A| + |H| - |A \cap H| = 4 + 13 - 1 = 16.$$

- **Exercise problem:** There are 70 students in a class. The class teacher decided to organize two competitions – singing and dancing. Every student has to participate in at least one competition. The students who participate in the dance competition, also get a chance to perform during the annual function. The student who participated in both the activities get an additional 10 points in general proficiency, 50 students participate in the singing competition and only 30 students do not get additional points in their general proficiency. Find the number of students who get the chance to perform during the annual function, but do not get additional points.

Permutation

- Permutation of a set is an arrangement of its members into a sequence or linear order, or if the set is already ordered, a rearrangement of its elements.
- For example, there are six permutations (orderings) of the set $\{1, 2, 3\}$: written as tuples, they are $(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2)$, and $(3, 2, 1)$.
- Permutations are used in almost every branch of mathematics and in many other fields of science. In computer science, they are used for analyzing sorting algorithms; in quantum physics, for describing states of particles; and in biology, for describing RNA sequences.

Number of Permutations

- The number of permutations of n distinct objects is n factorial, usually written as $n!$, which means the product of all positive integers less than or equal to n.
- **k-permutations of n:** A k-permutation of n (sometimes called a partial permutation, sequence without repetition, variation, or arrangement) means an ordered arrangement (list) of a k-element subset of an n-set.
- The number of such k-permutations (k-arrangements) of n is denoted by ${}^nP_k$ or $P(n,k)$ and is defined as

$$P(n,k) = \underbrace{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}_{k \text{ factors}} = \frac{n!}{(n-k)!}.$$

Examples

- **Example 1:** In how many ways can five students arrange themselves in a row?

Examples

- **Example 1:** In how many ways can five students arrange themselves in a row?
- Ans. The permutation of n objects taken all at a time is given by $n!$. Thus total number of ways is $5! = 120$.

Examples

- **Example 1:** In how many ways can five students arrange themselves in a row?
- Ans. The permutation of n objects taken all at a time is given by $n!$. Thus total number of ways is $5! = 120$.
- **Example 2:** In how many ways can 5 students arrange themselves in a circle?

Examples

- **Example 1:** In how many ways can five students arrange themselves in a row?
- Ans. The permutation of n objects taken all at a time is given by $n!$. Thus total number of ways is $5! = 120$.
- **Example 2:** In how many ways can 5 students arrange themselves in a circle?
- Ans. The permutation of n objects in a circle is $(n-1)!$. Thus the total number of ways is $4! = 24$.
- **Example 3:** How many different 3 digit numbers can be formed by using the digits 1,2,3,4 and 5 when repetition is not allowed?

Examples

- **Example 1:** In how many ways can five students arrange themselves in a row?
- Ans. The permutation of n objects taken all at a time is given by $n!$. Thus total number of ways is $5! = 120$.
- **Example 2:** In how many ways can 5 students arrange themselves in a circle?
- Ans. The permutation of n objects in a circle is $(n-1)!$. Thus the total number of ways is $4! = 24$.
- **Example 3:** How many different 3 digit numbers can be formed by using the digits 1,2,3,4 and 5 when repetition is not allowed?
- Ans. The total number of ways is $P(5,3) = \frac{5!}{(5-3)!} = 5!/2! = 60$.

- **Exercise Problem 1:** In how many ways can 6 students arrange themselves in a row, if two particular students always sit together?

- **Exercise Problem 1:** In how many ways can 6 students arrange themselves in a row, if two particular students always sit together? Ans. 240
- **Exercise Problem 2:** In how many ways can 7 students arrange themselves in a row if two particular students always take the corner seats.

- **Exercise Problem 1:** In how many ways can 6 students arrange themselves in a row, if two particular students always sit together?

  Ans. 240
- **Exercise Problem 2:** In how many ways can 7 students arrange themselves in a row if two particular students always take the corner seats.

  Ans. 240

Combination

- **Definition:** A **combination** is a selection of items from a set that has distinct members, such that the **order of selection does not matter** (unlike permutations).
- For example, given three fruits, say an apple, an orange and a pear, there are three combinations of two that can be drawn from this set: an apple and a pear; an apple and an orange; or a pear and an orange.

Number of Combinations

- A k-combination of a set S is a subset of k distinct elements of S. So, two combinations are identical if and only if each combination has the same members. (The arrangement of the members in each set does not matter.)
- The number of combinations of n items taken r at a time is denoted by $\binom{n}{r}$ or $C(n,r)$ or ${}^{n}C_{r}$ and is defined as

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

Examples

- **Example 1:** Find the number of ways to choose 2 students out of 5 to form a committee.

Examples

- **Example 1:** Find the number of ways to choose 2 students out of 5 to form a committee.
- Ans. Here, $n = 5$ (total students) and $r = 2$ (committee size).
  $\binom{5}{2} = \frac{5!}{2!(5-2)!} = \frac{5\times4}{2\times1} = 10$ ways.

Examples

- **Example 1:** Find the number of ways to choose 2 students out of 5 to form a committee.
- Ans. Here, $n = 5$ (total students) and $r = 2$ (committee size).
  $\binom{5}{2} = \frac{5!}{2!(5-2)!} = \frac{5\times4}{2\times1} = 10$ ways.
- **Example 2:** How many ways are there to choose 3 colors from 6 colors to paint a room?

Examples

- **Example 1:** Find the number of ways to choose 2 students out of 5 to form a committee.
- Ans. Here, $n = 5$ (total students) and $r = 2$ (committee size).
  $\binom{5}{2} = \frac{5!}{2!(5-2)!} = \frac{5\times4}{2\times1} = 10$ ways.
- **Example 2:** How many ways are there to choose 3 colors from 6 colors to paint a room?
- Ans. Here, $n = 6$ (total colors) and $r = 3$ (colors to choose).
  $\binom{6}{3} = \frac{6!}{3!(6-3)!} = \frac{6\times5\times4}{3\times2\times1} = 20$ ways.

- **Example 3:** A lock has 4 digits (0-9). How many 4-digit codes can be formed using distinct digits?

- **Example 3:** A lock has 4 digits (0-9). How many 4-digit codes can be formed using distinct digits?
- Ans. Here, $n = 10$ (total digits) and $r = 4$ (4-digit code).
  $\binom{10}{4} = \frac{10!}{4!(10-4)!} = \frac{10\times9\times8\times7}{4\times3\times2\times1} = 210$ codes.

Binomial Coefficients

- The binomial coefficients are the positive integers that occur as coefficients in the binomial theorem. Commonly, a binomial coefficient is indexed by a pair of integers $n \geq k \geq 0$ and is written $\binom{n}{k}$. It is the coefficient of the x^k term in the polynomial expansion of the binomial power $(1+x)^n$.
- This coefficient can be computed by the multiplicative formula

$$\binom{n}{k} = \frac{n \times (n-1) \times \cdots \times (n-k+1)}{k \times (k-1) \times \cdots \times 1},$$

which using factorial notation can be compactly expressed as

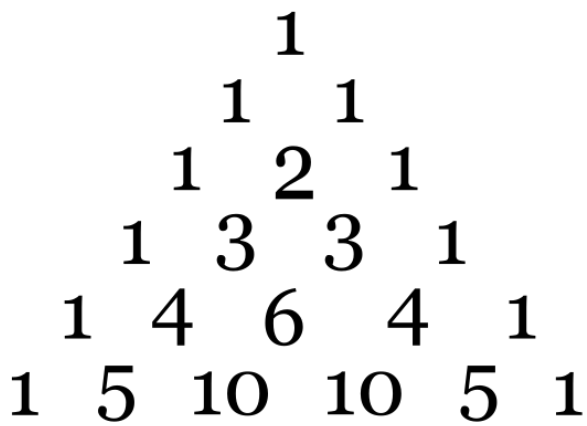
$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Example

For example, the fourth power of $1 + x$ is

$$(1+x)^4 = \binom{4}{0}x^0 + \binom{4}{1}x^1 + \binom{4}{2}x^2 + \binom{4}{3}x^3 + \binom{4}{4}x^4$$
$$= 1 + 4x + 6x^2 + 4x^3 + x^4.$$

Note: The problem with Pascal's triangle procedure is that it is an implicit method, meaning, if you want to find n-th row of the Pascal's triangle, then you need to construct/find all the previous rows.



Pascal's Triangle

Pigeonhole Principle

Pigeonhole Principle

If n items are placed into m containers where $n > m$, then at least one container must contain more than one item.

- The principle is based on the simple idea that if you have more items than containers, some container must have more than one item.
- It is also known as the "box principle" or "dirichlet principle."
- The Pigeonhole Principle is often used in combinatorics, number theory, and computer science.



Pigeons in holes. Here there are $n = 10$ pigeons in $m = 9$ holes. Since 10 is greater than 9, the pigeonhole principle says that at least one hole has more than one pigeon.

Pigeonhole Principle Examples

Example

If there are 13 people in a room, at least how many people have their birthday in the same month?

- There are 12 months in a year, so we have 12 "containers."
- Since there are 13 people, by the Pigeonhole Principle, at least 2 people must share a birthday month.

Pigeonhole Principle Examples

Example

In a chess tournament, 9 games are played. Show that at least two games have been played on the same day.

- There are 7 days in a week, so we have 7 "containers."
- Since 9 games are played, by the Pigeonhole Principle, at least 2 games must have been played on the same day.

Pigeonhole Principle Examples

Example

Suppose you have 8 socks in your drawer, and each sock is either red, blue, or green. Show that there are at least two socks of the same color.

- There are 3 colors, so we have 3 "containers."
- Since there are 8 socks, by the Pigeonhole Principle, at least 2 socks must be of the same color.

Pigeonhole Principle: Hand Shaking Example

- **Example:** If n people can shake hands with one another (where $n > 1$), the pigeonhole principle shows that there is always a pair of people who will shake hands with the same number of people.

Pigeonhole Principle: Hand Shaking Example

- **Example:** If n people can shake hands with one another (where $n > 1$), the pigeonhole principle shows that there is always a pair of people who will shake hands with the same number of people.
- The "hole" to which a person is assigned is the number of hands that person shakes. Since each person shakes hands with some number of people from 0 to $n - 1$, there are n possible holes.
- On the other hand, either the "0" hole, the "$n - 1$" hole, or both must be empty, for it is impossible (if $n > 1$) for some person to shake hands with everybody else while some person shakes hands with nobody. This leaves n people to be placed into at most $n - 1$ non-empty holes, so the principle applies.

Pigeonhole Principle: Hand Shaking Example

- **Example:** If n people can shake hands with one another (where $n > 1$), the pigeonhole principle shows that there is always a pair of people who will shake hands with the same number of people.
- This hand-shaking example is equivalent to the statement that in any graph with more than one vertex, there is at least one pair of vertices that share the same degree. This can be seen by associating each person with a vertex and each edge with a handshake.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Module 3

GCD



BENNETT UNIVERSITY

TIMES OF INDIA GROUP

Fundamental Theorem of Arithmetic

- The fundamental theorem of arithmetic, also called the unique factorization theorem and prime factorization theorem, states that every integer greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors.
- For example 360 can be uniquely expressed as

$$360 = 2^3 \times 3^2 \times 5.$$

Many cryptographic protocols are based on the difficulty of factoring large composite integers or a related problem—for example, the RSA problem. An algorithm that efficiently factors an arbitrary integer would render RSA-based public-key cryptography insecure.

Greatest Common Divisor

- The greatest common divisor (GCD) of two or more integers, which are not all zero, is the largest positive integer that divides each of the integers.
- For two integers x, y, the greatest common divisor of x and y is denoted $\gcd(x, y)$.
- Other name of GCD includes highest common factor (**HCF**).
- For example, the GCD of 8 and 12 is 4, that is, $\gcd(8, 12) = 4$.

Example

- The complete list of divisors of 54 is $1, 2, 3, 6, 9, 18, 27, 54$. Similarly, the divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$. The numbers that these two lists have in common are the common divisors of 54 and 24, that is, $1, 2, 3, 6$. Of these, the greatest is 6, so it is the greatest common divisor:

$$\gcd(54, 24) = 6.$$

Coprime Numbers

Definition

Two numbers are called **relatively prime**, or **coprime**, if their greatest common divisor equals 1.

- For example, 9 and 28 are coprime.

Euclidean Algorithm to Find GCD of Two Numbers

Algorithm

The Euclidean algorithm can be thought of as constructing a sequence of non-negative integers that begins with the two given integers

$$r_{-2} = a \text{ and } r_{-1} = b$$

and will eventually terminate with the integer zero:

$$\{r_{-2} = a,\ r_{-1} = b,\ r_0,\ r_1,\ \cdots,\ r_{n-1},\ r_n = 0\}$$

with $r_{k+1} < r_k$. The integer r_{n-1} will then be the GCD and we can state $\gcd(a, b) = r_{n-1}$.

Pseudocode of the Algorithm

function $\gcd(a, b)$

while $b \neq 0$

$t := b$

$b := a \pmod{b}$

$a := t$

return a

Example 1

- Find GCD of $a = 1071$ and $b = 462$ using Euclidean algorithm.
-

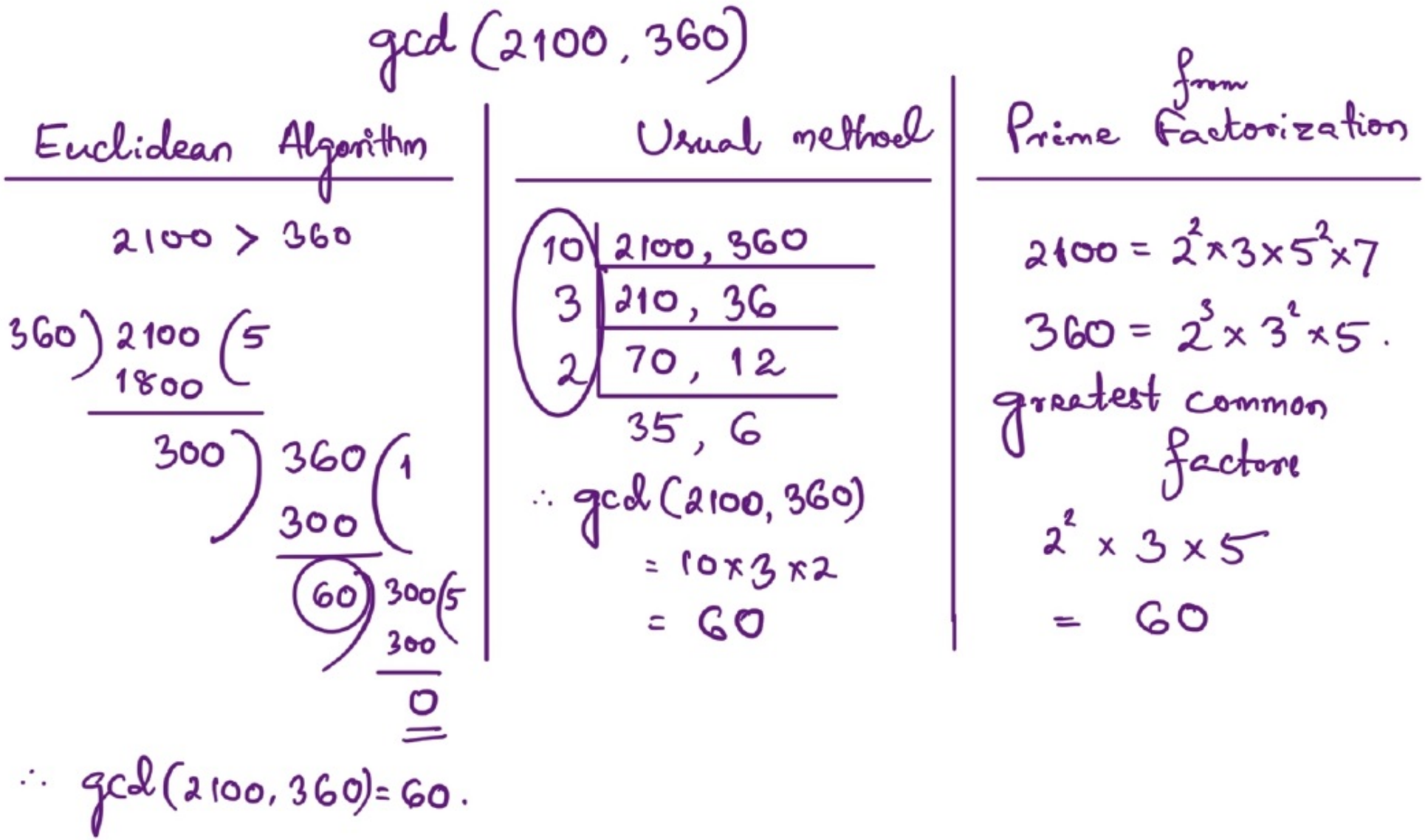
$$1071 = 2 \times 462 + 147$$

$$462 = 3 \times 147 + 21.$$

$$147 = 7 \times 21 + 0.$$

Since the last remainder is zero, the algorithm ends with 21 as the greatest common divisor of 1071 and 462.

Example 2


gcd (2100, 360)
Euclidean Algorithm
2100 > 360
360) 2100 (5
1800
300) 360 (1
300
60) 300 (5
300
0
∴ gcd(2100, 360) = 60.
Usual method
10 | 2100, 360
3 | 210, 36
2 | 70, 12
35, 6
∴ gcd(2100, 360)
= 10 × 3 × 2
= 60
from
Prime Factorization
2100 = 2² × 3 × 5² × 7
360 = 2³ × 3² × 5.
greatest common factor
2² × 3 × 5
= 60

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Module 3

Recurrence Relations and Generating Functions



Recurrence Relations

Recurrence Relation

A recurrence relation is an equation that recursively defines a sequence where each term is defined in terms of previous terms.

- Recurrence relations are often used to model sequences in mathematics and computer science.
- They can describe various phenomena such as growth rates, algorithms, and recursive processes.

Examples of Recurrence Relations

- **Example 1:** The Fibonacci sequence is defined by the recurrence relation:

$$F(n) = F(n-1) + F(n-2) \quad \text{for } n \geq 2$$

with initial conditions $F(0) = 1$ and $F(1) = 1$.

- **Example 2:** The factorial function $n!$ can be defined recursively as:

$$n! = n \cdot (n-1)! \quad \text{for } n \geq 1$$

with initial condition $0! = 1$.

Generating Functions

Generating Function

A generating function is a formal power series that encodes information about a sequence.

- Generating functions provide a powerful tool for analyzing sequences, especially those defined by recurrence relations.
- They can be used to find closed-form expressions, calculate sums, and derive properties of sequences.

"A generating function is a device somewhat similar to a bag. Instead of carrying many little objects detachedly, which could be embarrassing, we put them all in a bag, and then we have only one object to carry, the bag." – George Pólya

Examples of Generating Functions of a Recurrence Relation

- **Example 1:** The generating function for the Fibonacci sequence is:

$$F(x) = \sum_{n=0}^{\infty} F(n)x^n = \frac{1}{1 - x - x^2}$$

This allows us to easily derive properties of the Fibonacci sequence.

- **Example 2:** The generating function for the factorial sequence is:

$$F(x) = \sum_{n=0}^{\infty} n!x^n = e^x$$

This is a result of the Maclaurin series for e^x.

Recurrence Relations and Generating Functions

- **Example 1:** Consider the sequence defined by the recurrence relation:

$$a_n = 2a_{n-1} + 3a_{n-2} \quad \text{for } n \geq 2$$

with initial conditions $a_0 = 1$ and $a_1 = 2$.

- The generating function for this sequence is: $A(x) = \sum_{n=0}^{\infty} a_n x^n$

Multiplying the recurrence relation by x^n and summing over n, we get:

$$A(x) - a_0 - a_1 x = 2x(A(x) - a_0) + 3x^2 A(x)$$

Solving for $A(x)$, we find: $A(x) = \dfrac{1}{1 - 2x - 3x^2}$.

- **Exercise Problem 1:** Consider the sequence defined by the recurrence relation:

$$c_n = 3c_{n-1} - 2c_{n-2} \quad \text{for } n \geq 2$$

with initial conditions $c_0 = 1$ and $c_1 = 3$.

- Ans. $C(x) = \dfrac{1}{1 - 3x + 2x^2}$.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Module 3

Semi-group, Monoid, Group

Algebraic Structures



Algebraic Structures with One Binary Operation

$(X, *)$

Semi-group

Semi-group

A semi-group is a set S equipped with an associative binary operation $\cdot$, i.e., for all $a, b, c \in S$:

$$(a * b) * c = a * (b * c)$$

- **Example 1:** The set of natural numbers $\mathbb{N}$ with addition forms a semi-group:

$$(a + b) + c = a + (b + c) \quad \text{for } a, b, c \in \mathbb{N}$$

- **Example 2:** The set of non-negative integers $\mathbb{Z}_{\geq 0}$ with multiplication forms a semi-group:

$$(a \times b) \times c = a \times (b \times c) \quad \text{for } a, b, c \in \mathbb{Z}_{\geq 0}$$

Semigroup Example: Strings with Concatenation

The set of all strings with the operation of string concatenation forms a semigroup.

- Concatenation of strings is associative.
- For example:

$$(\text{“}Hello\text{”} + \text{“ ”}) + \text{“}World\text{”} = \text{“}Hello\text{”} + (\text{“ ”} + \text{“}World\text{”})$$

Semigroup Example: Matrices under Matrix Multiplication

The set of all square matrices of a fixed size with the operation of matrix multiplication forms a semigroup.

- Matrix multiplication is associative.
- For example, if we have matrices A, B, and C:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

Semigroup Example: Sets with Intersection

The set of all sets with the operation of intersection forms a semigroup.

- Set intersection is associative.
- For example, if we have sets A, B, and C:

$$(A \cap B) \cap C = A \cap (B \cap C)$$

Semigroup Example: Functions under Composition

The set of all functions from a set to itself with the operation of function composition forms a semigroup.

- Function composition is associative.
- For example, if we have functions f, g, and h:

$$(f \circ g) \circ h = f \circ (g \circ h)$$

Monoid

Monoid

A monoid is a semi-group with an identity element e, i.e., for all $a \in S$:

$$e * a = a * e = a$$

- **Example 1:** The set of integers $\mathbb{Z}$ with addition forms a monoid:

$$a + 0 = 0 + a = a \quad \text{for } a \in \mathbb{Z}$$

- **Example 2:** The set of non-negative integers $\mathbb{Z}_{\geq 0}$ with multiplication forms a monoid:

$$a \times 1 = 1 \times a = a \quad \text{for } a \in \mathbb{Z}_{\geq 0}$$

Monoid Example: Matrices under Matrix Multiplication

The set of all square matrices of a fixed size with the operation of matrix multiplication forms a monoid.

- The identity element is the identity matrix of the appropriate size.
- Matrix multiplication is associative.
- For example, if we have matrices A, B, and C:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

Examples of Semigroups but not Monoids

- **Example 1:** The set of positive integers $\mathbb{Z}^+$ with addition is a semigroup: $(a+b)+c = a+(b+c)$ for $a, b, c \in \mathbb{Z}^+$. However, it is not a monoid since it does not have an identity element.
- **Example 2:** The set of skew-symmetric matrices $\mathcal{A}_n(\mathbb{R})$ with matrix addition is a semigroup:

$$(A+B)+C = A+(B+C) \quad \text{for } A, B, C \in \mathcal{A}_n(\mathbb{R}).$$

  But it is not a monoid as it lacks an identity matrix for all $n > 1$.
- **Example 3:** The set of non-empty strings over an alphabet Σ with concatenation is a semigroup:

$$(xy)z = x(yz) \quad \text{for } x, y, z \in \Sigma^*.$$

  It is not a monoid unless the empty string is included.

More Examples

- The set of positive rational numbers $\mathbb{Q}^+$ with addition is a semigroup :
  - Closure property is satisfied since sum of two positive rationls is a positive rational number.
  - Associative property is satisfied since
    $(a+b)+c = a+(b+c)$ for $a, b, c \in \mathbb{Q}^+$.

  It is not a monoid as 0 is not included in the set.
- The set of integers greater than 1, $\mathbb{Z}_{\geq 2}$ with multiplication is a semigroup, but not a monoid.
- The set of $n \times n$ upper triangular matrices with zero diagonal entries and matrix multiplication is a semigroup. It is not a monoid as it lacks an identity matrix for $n > 1$.

Group

Group

A group is a monoid where every element has an inverse, i.e., for every $a \in S$, there exists $a^{-1} \in S$ such that:

$$a * a^{-1} = a^{-1} * a = e$$

- **Example 1:** The set of integers $\mathbb{Z}$ with addition forms a group:

$$a + (-a) = (-a) + a = 0 \quad \text{for } a \in \mathbb{Z}$$

- **Example 2:** The set of non-zero rational numbers $\mathbb{Q}^*$ with multiplication forms a group:

$$a \times \frac{1}{a} = \frac{1}{a} \times a = 1 \quad \text{for } a \in \mathbb{Q}^*$$

Group Example: $\mathbb{Z}_n$ under Addition

The group $\mathbb{Z}_5$ consists of integers modulo 5 with the operation of addition.

- Elements: $\{0, 1, 2, 3, 4\}$.
- Check for closure and associative properties.
- The identity element is 0.
- Inverses:
  - 0 is the inverse of itself
  - $-1 \equiv 4 \pmod 5$
  - $-2 \equiv 3 \pmod 5$
  - $-3 \equiv 2 \pmod 5$
  - $-4 \equiv 1 \pmod 5$

Group Example: $\mathbb{Z}_p^*$ (p: prime) under Multiplication

The group $\mathbb{Z}_5^*$ consists of integers modulo 5 with the operation of multiplication.

- Elements: $\{1, 2, 3, 4\}$.
- Check for closure and associative properties.
- The identity element is 1.
- Inverses:
  - 1 is the inverse of itself
  - $2^{-1} \equiv 3 \pmod 5$ (since $2 \times 3 \equiv 1 \pmod 5$)
  - $3^{-1} \equiv 2 \pmod 5$ (since $3 \times 2 \equiv 1 \pmod 5$)
  - $4^{-1} \equiv 4 \pmod 5$ (since $4 \times 4 \equiv 1 \pmod 5$)

Examples of Monoids but not Groups

- **Example 1:** The set of nonnegative integers $\mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, \ldots\}$ with addition forms a monoid:

$$(a + b) + c = a + (b + c) \quad \text{for } a, b, c \in \mathbb{N}$$

The identity element is 0.

  - Not a Group: Not every natural number has an additive inverse.
  - For example, 1 does not have an inverse since there is no natural number n such that $n + 1 = 0$.

Examples of Monoids but not Groups

- **Example 2:** The set of strings over an alphabet Σ with concatenation forms a monoid:

$$(xy)z = x(yz) \quad \text{for } x, y, z \in \Sigma^*$$

The identity element is the empty string ε.

  - Not a Group: Not every string has a concatenative inverse.
  - For example, there is no string s such that s concatenated with any string t equals the empty string ε.

Examples of Monoids but not Groups

- **Example 3:** The set of all finite subsets of a set X with union forms a monoid:

$$(A \cup B) \cup C = A \cup (B \cup C) \quad \text{for } A, B, C \subseteq X$$

The identity element is the empty set $\emptyset$.

  - Not a Group: Not every subset has a union inverse.
  - For example, if we consider $X = \{1, 2, 3\}$, the set $\{1, 2\}$ does not have an inverse subset that, when unioned with $\{1, 2\}$, gives the identity element $\emptyset$.

Abelian Groups

Abelian Group

An Abelian group, also known as a commutative group, is a group where the group operation is commutative. That is, for all $a, b \in G$:

$$a * b = b * a$$

- **Example 1:** The set of integers $\mathbb{Z}$ with addition form an Abelian group:

$$a + b = b + a \quad \text{for } a, b \in \mathbb{Z}$$

- **Example 2:** The set of real numbers $\mathbb{R}$ with addition also forms an Abelian group.
- **Example 3:** The group $(\mathbb{Z}_n, +)$ where $\mathbb{Z}_n$ is the set of integers modulo n and addition is modulo n addition.

Non-Abelian Groups

Non-Abelian Group

A Non-Abelian group is a group where the group operation is not commutative. That is, there exist elements $a, b \in G$ such that:

$$a * b \neq b * a$$

- **Example 1:** The set of all 2×2 invertible matrices with matrix multiplication forms a Non-Abelian group: $AB \neq BA$. for some matrices A and B.
- **Example 2:** The symmetric group S_n of permutations of n elements, for $n \geq 3$, is a Non-Abelian group.

Example of Non-Abelian Group: Heisenberg Group

The Heisenberg group is a group of 3x3 upper triangular matrices with 1s on the diagonal.

- Elements: Matrices of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ where a, b, and c are real numbers.
- The identity element is $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
- Inverses: $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$
- Matrix multiplication is non-commutative.

Cyclic Group

A cyclic group is a group that can be generated by a single element. That is, there exists an element g in the group such that every element of the group can be expressed as g^n, where n is an integer.

- **Example 1:** The integers $\mathbb{Z}$ under addition form a cyclic group generated by 1: $\langle 1 \rangle = \{..., -2, -1, 0, 1, 2, ...\}$. Every integer can be expressed as a multiple of 1.
- **Example 2:** The group of integers modulo n, denoted $\mathbb{Z}_n$, under addition forms a cyclic group: $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$. It is generated by 1 with addition modulo n.
- **Example 3:** The multiplicative group of integers modulo n, denoted $(\mathbb{Z}_n)^*$, forms a cyclic group if n is prime:

$$(\mathbb{Z}_n)^* = \{1, 2, ..., n-1\}$$

Order of a Group and Properties of Cyclic Groups

- In a cyclic group G, there exists an element a such that $G = \langle a \rangle$. We call it a generator of the cyclic group.
- The order of a group is the number of elements it contains.
- Let a be the generator of a cyclic group G, and e be the identity element. The order of an element a of G, denoted as $|a|$ or $o(G)$, is the smallest positive integer n such that $a^n = e$.
- When $a^n = e$, the cyclic group wraps around and repeats.

Example: Order of an Element of a Cyclic Group $\mathbb{Z}_6$ under Addition

- Consider the cyclic group $\mathbb{Z}_6$ under addition.
- Elements: $\{0, 1, 2, 3, 4, 5\}$. So, order of $\mathbb{Z}_6$ is 6.
- Let's find the order of element 2.
- Calculate: $2^1 = 2$, $2^2 = 4$, $2^3 \equiv 0 \pmod 6$ (wraps around).
- So, the subgroup $\langle 2 \rangle = \{2, 4, 0\} \implies |2| = 3$.
- Note 1: Here 2^3 means $2 + 2 + 2$ or $3 \cdot 2$ because it is addition modulo arithmetic.
- Note 2: Under addition modulo operation in a cyclic group one can write/mean g^n as ng.

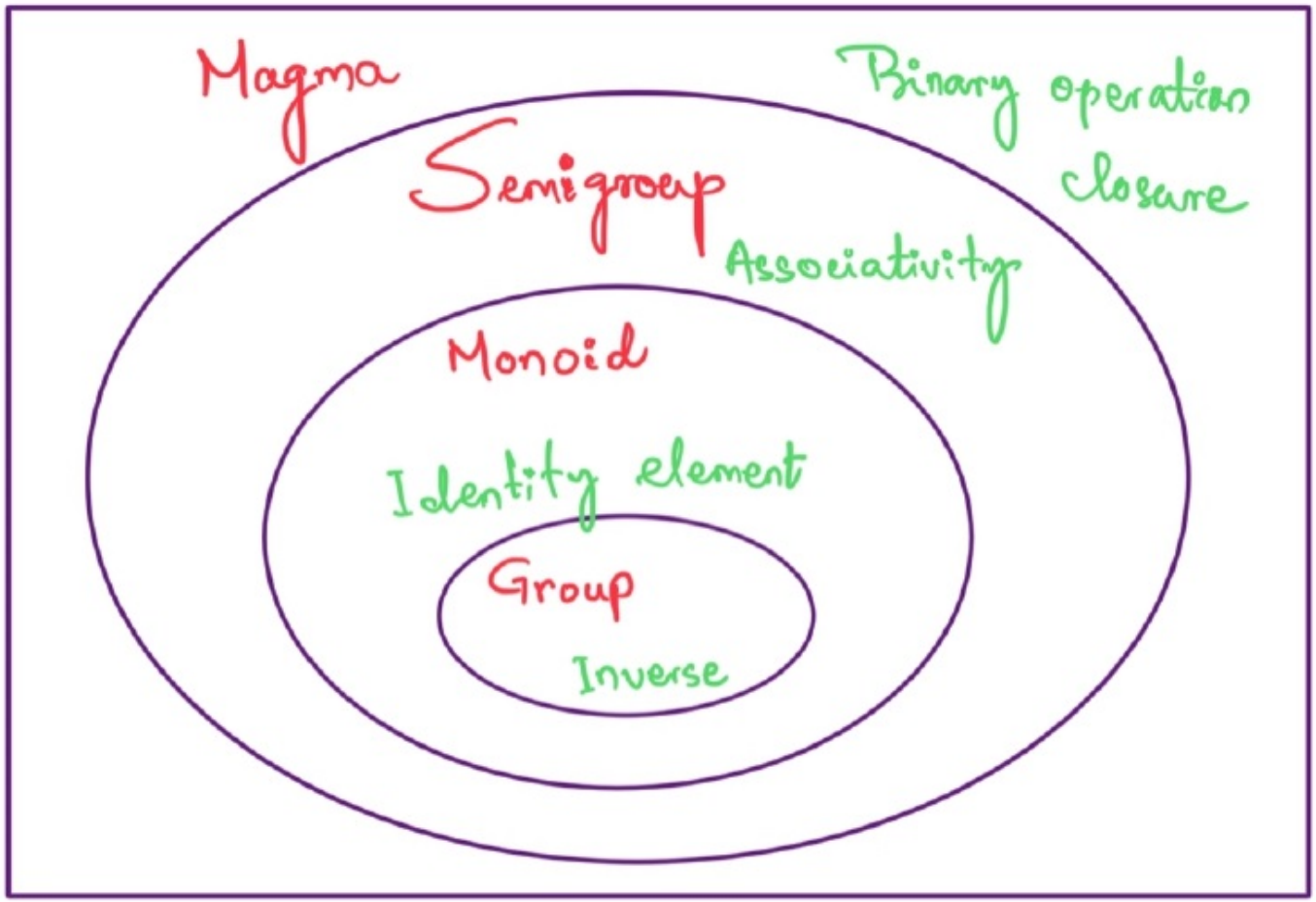
Example: Order of an Element of a Cyclic Group $\mathbb{Z}_6$ under Addition

- Continuing with $\mathbb{Z}_6$ under addition.
- Let's find the order of element 3.
- Calculate: $1 \cdot 3 = 3$, $2 \cdot 3 = 0$ (wraps around).
- So, $|3| = 2$.
- Finally, for $\mathbb{Z}_6$ under addition.
- Let's find the order of element 5.
- Calculate: $1 \cdot 5 = 5$, $2 \cdot 5 = 4$, $3 \cdot 5 = 3$, $4 \cdot 5 = 2$, $5 \cdot 5 = 1$, $6 \cdot 5 = 0$ (wraps around).
- So, $|5| = 6$. Therefore, 5 is also a generator of $\mathbb{Z}_6$.

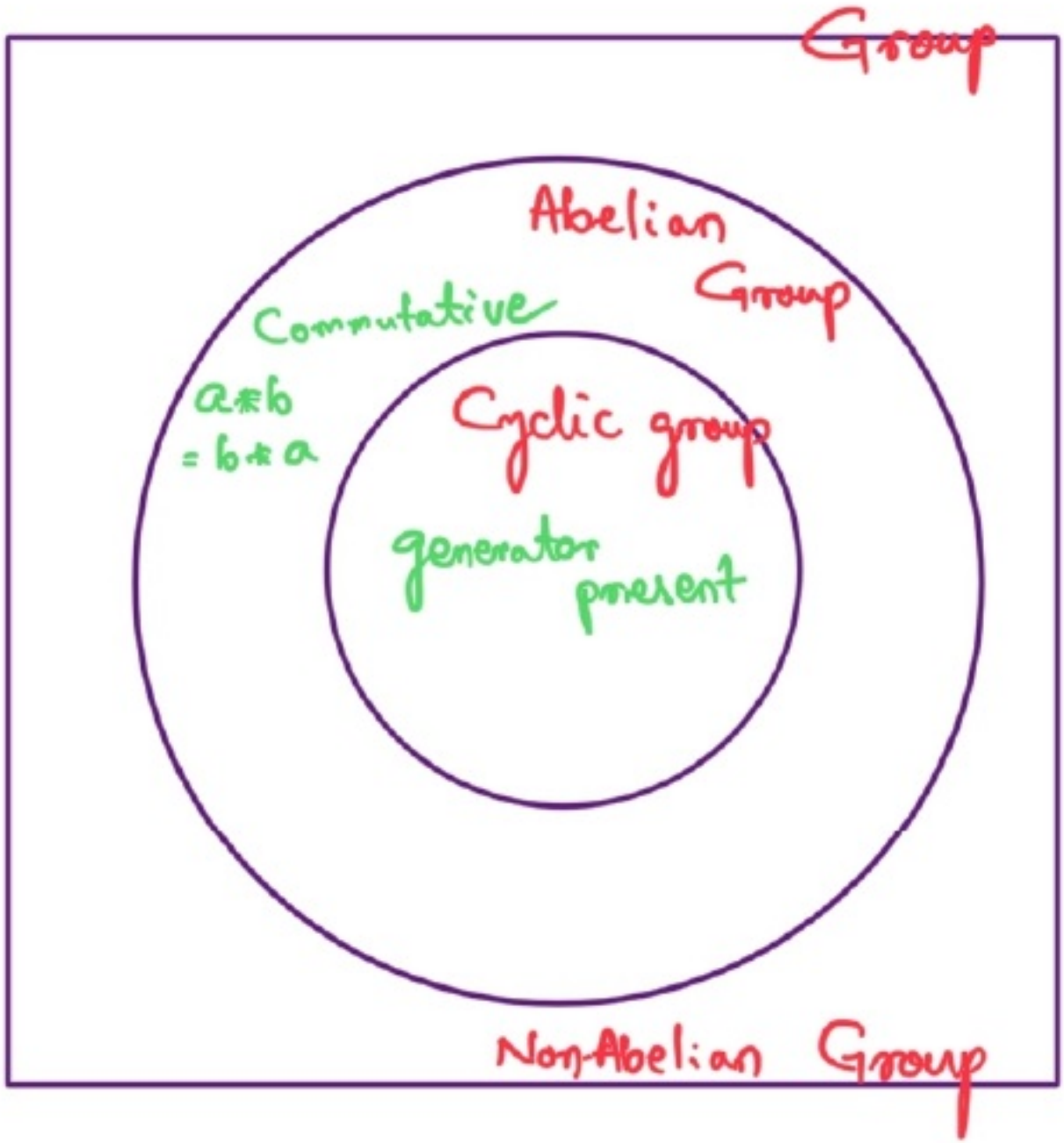
Example: Order of an Element of a Cyclic Group $\mathbb{Z}_5^*$ under Multiplication

- Consider the cyclic group $\mathbb{Z}_5^*$ under multiplication.
- Elements: $\{1, 2, 3, 4\}$. So, order of $\mathbb{Z}_5^*$ is 4. Identity element is 1.
- Let's find the order of element 2.
- Calculate: $2^1 = 2$, $2^2 = 4$, $2^3 \equiv 3 \pmod 5$, $2^4 \equiv 1$.
- So, $\langle 2 \rangle = \{1, 2, 4, 3\} \implies |2| = 3$.
- Similarly, $3^1 = 3, 3^2 \equiv 4, 3^3 \equiv 2, 3^4 \equiv 1 \pmod 5$.

Algebraic Structures: Venn Diagram



Algebraic Structure with respect to one Binary Operation


Group
Abelian
Group
Commutative
a*b
= b*a
Cyclic group
generator
present
Non-Abelian Group

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Module 3

Chinese Remainder Theorem

CRT



BENNETT
UNIVERSITY
TIMES OF INDIA GROUP

Multiplicative Inverse of a Number in $\mathbb{Z}_n$

- **Question:** Find the multiplicative inverses of each nonzero elements of $\mathbb{Z}_5$.
- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
- Multiplicative inverse of 1 in $\mathbb{Z}_5$ is 1.
- Multiplicative inverse of 2 in $\mathbb{Z}_5$ is 3.

  Meaning we need to find $2 \times ? \equiv 1 (\text{mod } 5)$.

  Note: $a \equiv b (\text{mod } n)$ means $n|(a-b)$, i.e. if you divide $a-b$ by n then the remainder is 0.
- Multiplicative inverse of 3 in $\mathbb{Z}_5$ is 2.
- Multiplicative inverse of 4 in $\mathbb{Z}_5$ is 4. $5|(4 \times 4 - 1)$ or $4 \times 4 \equiv 1 (\text{mod } 5)$.

Chinese Remainder Theorem

- The Chinese remainder theorem states that if one knows the remainders of the Euclidean division of an integer n by several integers, then one can determine uniquely the remainder of the division of n by the product of these integers, under the condition that the divisors are pairwise coprime (no two divisors share a common factor other than 1).
- For example, if we know that the remainder of n divided by 3 is 2, the remainder of n divided by 5 is 3, and the remainder of n divided by 7 is 2, then without knowing the value of n, we can determine that the remainder of n divided by 105 (the product of $3, 5$, and 7) is 23.
- Importantly, this tells us that if n is a natural number less than 105, then 23 is the only possible value of n.

CRT

Statement

If the n_i are pairwise coprime, and if $a_1, ..., a_k$ are any integers, then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k}, \end{aligned}$$

has a solution, and any two solutions, say x_1 and x_2, are congruent modulo M, that is, $x_1 \equiv x_2 (\text{mod } M)$.

Solution To Chinese Remainder Theorem

Algorithm

1. Find $M = m_1 \times m_2 \times \cdots \times m_k$. This is the common modulus.
2. Find $M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \cdots, M_k = \frac{M}{m_k}$.
3. Find the multiplicative inverse of $M_1, M_2, \cdots, M_k$ using the corresponding moduli $(m_1, m_2, \cdots, m_k)$. Call the inverses $M_1^{-1}, M_2^{-1}, \cdots, M_k^{-1}$.
4. The solution to the simultaneous equations is

$$x \equiv \left(a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}\right) (\text{mod } M).$$

Example

- **Question:** Find the solution to the simultaneous equations:

$$\begin{cases} x \equiv 2 (\text{mod } 3) \\ x \equiv 3 (\text{mod } 5) \\ x \equiv 2 (\text{mod } 7) \end{cases}$$

- **Solution:**
  1. $M = 3 \times 5 \times 7 = 105.$
  2. $M_1 = 105/3 = 35, M_2 = 105/5 = 21, M_3 = 105/7 = 15.$
  3. The inverses are $M_1^{-1} = 2, M_2^{-1} = 1, M_3^{-1} = 1.$
  4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \text{ mod } 105 \equiv 23 \text{ mod } 105.$

Application of CRT

- In coding theory, detection and correction of errors is done by adding redundancy to data that is sent via a noisy channel or in a computer.
- The CRT remainder techniques are useful in developing code that detects errors.
- In cryptography, the CRT is used in secret sharing through error-correcting code.
- The CRT is itself a secret-sharing scheme without any need for modification

Further Applications

- **Parallel computation:** Suppose you have a huge computation to do that involves adding, multiplying and subtracting integers. Possibly also dividing but, if so, only division by numbers in a finite set S which you already know.

  Choose primes $p_1, p_2, ..., p_r$ which do not divide any element of S, and such that $p_1 p_2 \cdots p_r$ is surely larger than your answer. Split your computation over r processors, the ith of which computes the answer modulo p_i. Use CRT to put your answer back together in the end.

- **Secret sharing:** Suppose we have N people. We want any $k+1$ of them to be able to launch a missile attack, but no k of them to have this power.
- Solution: Choose some large prime p and a random polynomial $f(t)$ of degree k with coefficients in $\mathbb{Z}/p$. Tell person 1 the value of $f(1)$, person 2 the value of $f(2)$ and so forth. (Also, everyone knows what p is.) Set up the missiles to only launch when $f(0)$ is input. Any $k+1$ people can use the Chinese remainder theorem to compute f, and hence $f(0)$; any k people do not have enough data to constrain $f(0)$ in any way.

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

Module 4

Poset, Totally Ordered Set, Hasse Diagram, Lattice



Partially Ordered Sets (Posets)

Definition

A partially ordered set, or poset, is a set P together with a binary relation R that is:

1. **Reflexive**: $(a, a) \in R$ for all $a \in P$.
2. **Antisymmetric**: $(a, b) \in R$ and $(b, a) \in R$ implies $a = b$.
3. **Transitive**: $(a, b) \in R$ and $(b, c) \in R$ implies $(a, c) \in R$.

Note: Instead of writing P with R, now onward, we'll write $(P, \leq)$. So, we'll use the notation $a \leq b$ instead of $(a, b) \in R$.

Examples of Posets

1. Divisibility Poset:
   - Let S be the set of positive integers.
   - Define $a \leq b$ if a divides b.
   - This forms a poset since divisibility is reflexive, antisymmetric, and transitive.
2. Subset Poset:
   - Let X be a set.
   - The power set $\mathcal{P}(X)$ ordered by set inclusion forms a poset.
   - $A \leq B$ if A is a subset of B.

Totally Ordered Sets

Definition

A totally ordered set or toset is a poset where for any two elements a and b in the set, either $a \leq b$ or $b \leq a$ (or both).

Examples of Totally Ordered Sets:

1. Real Numbers with Standard Order:
   - The set of real numbers $\mathbb{R}$ with the standard order $<$ is a totally ordered set.
   - For any two real numbers a and b, either $a < b$ or $b < a$ holds.
2. Alphabetical Order of Words:
   - The set of all words in a language ordered by alphabetical order forms a totally ordered set.
   - For example, "apple" $\leq$ "banana" $\leq$ "cherry".

Well-ordered Set

A set $(X, \leq)$ is called well-ordered if:

1. $(X, \leq)$ is a partially ordered set.
2. For every non-empty subset $Y \subseteq X$, there exists an element $y \in Y$ such that $y \leq x$ for all $x \in Y$.

Examples

Natural Numbers

The set $\mathbb{N} = \{1, 2, 3, \ldots\}$ is well-ordered with respect to the usual "less than or equal to" ordering.

Integers (Absolute Value)

The set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ is not well-ordered with the usual ordering because, for example, the set of negative integers does not have a least element. However, if we consider the set $\mathbb{Z}$ with the absolute value ordering $|a| \leq |b|$ if and only if $a \leq b$, then $\mathbb{Z}$ becomes a well-ordered set.

Alphabetical Ordering of Words

Consider the set of all English words, ordered alphabetically.

Set of Divisors of a Number

Take any positive integer n and consider the set of all positive divisors of n.

Definition of Lexicographic Ordering of Two Posets

Let $(X, \leq_X)$ and $(Y, \leq_Y)$ be two posets. The lexicographic ordering $\leq_{\text{lex}}$ on $X \times Y$ is defined as follows for elements (a, b) and (c, d) in $X \times Y$:

- $(a, b) \leq_{\text{lex}} (c, d)$ if and only if:
  - $a <_X c$, or
  - $a = c$ and $b \leq_Y d$.

Examples of Lexicographic Ordering of Two Posets

Example 1: Lexicographic Ordering of Two Intervals

Consider the posets $([0,2], \leq)$ and $([0,1], \leq)$:

- $(x, y) \leq_{\text{lex}} (u, v)$ if and only if:
  - $x < u$, or
  - $x = u$ and $y \leq v$.

Example: $(1,0) \leq_{\text{lex}} (1,1) \leq_{\text{lex}} (2,0) \leq_{\text{lex}} (2,1)$

Examples of Lexicographic Ordering of Two Posets

Example 2: Lexicographic Ordering of Day and Time

Consider the posets (Days of the Week, $\leq$) and (Time of Day, $\leq$):

- $(\text{day}, \text{time}) \leq_{\text{lex}} (\text{day}', \text{time}')$ if and only if:
  - The days are ordered.
  - If the days are the same, then the times are ordered.

Example:

$(\text{Monday}, 8{:}00\text{AM}) \leq_{\text{lex}} (\text{Tuesday}, 10{:}00\text{AM}) \leq_{\text{lex}} (\text{Tuesday}, 2{:}00\text{PM})$

Examples of Lexicographic Ordering of Two Posets

Example 3: Lexicographic Ordering of Words and Length

Consider the posets $(\text{Words in English}, \leq)$ and $(\mathbb{N}, \leq)$:

- $(\text{word}, \text{length}) \leq_{\text{lex}} (\text{word}', \text{length}')$ if and only if:
  - The words are ordered lexicographically.
  - If the words are the same, then the lengths are ordered numerically.

Example: $(\text{apple}, 5) \leq_{\text{lex}} (\text{banana}, 6) \leq_{\text{lex}} (\text{cat}, 3)$

Examples of Lexicographic Ordering of Two Posets

Example 4: Lexicographic Ordering of Temperatures and Altitudes

Consider the posets $(\mathbb{R}, \leq)$ and $(\mathbb{R}, \leq)$ for temperatures and altitudes:

- $(T_1, A_1) \leq_{\text{lex}} (T_2, A_2)$ if and only if:
  - $T_1 < T_2$, or
  - $T_1 = T_2$ and $A_1 \leq A_2$.

Example: $(20°\text{C}, 1000\text{m}) \leq_{\text{lex}} (20°\text{C}, 2000\text{m}) \leq_{\text{lex}} (25°\text{C}, 1000\text{m})$

Minimal and Maximal Elements

Definition

In a poset $(X, \leq)$:

- **Minimal Element**: An element a is minimal if there is no $b \in X$ such that $b < a$.
- **Maximal Element**: An element a is maximal if there is no $b \in X$ such that $a < b$.

Example

- In a linear ordering $\{a, b, c, d\}$ with the usual ordering:
  - a is minimal.
  - d is maximal.

Greatest Lower Bound (GLB) and Least Upper Bound (LUB)

Definitions

Let $(X, \leq)$ be a poset and $A \subseteq X$:

- **Greatest Lower Bound (GLB)**: An element g is the GLB of A if:
  1. g is a lower bound of A ($g \leq a$ for all $a \in A$).
  2. If l is any other lower bound of A, then $l \leq g$.
- **Least Upper Bound (LUB)**: An element l is the LUB of A if:
  1. l is an upper bound of A ($a \leq l$ for all $a \in A$).
  2. If u is any other upper bound of A, then $l \leq u$.

Greatest Lower Bound (GLB) and Least Upper Bound (LUB)

Examples

- In the poset $\mathbb{Z}$ with the usual ordering:
  - $A = \{1, 2, 3\}$:
    - The GLB of A is 1 (the smallest element of A).
    - The LUB of A is 3 (the largest element of A).
- In the poset $(\mathbb{R}, \leq)$:
  - $A = [0, 1]$:
    - The GLB of A is 0 (the infimum of A).
    - The LUB of A is 1 (the supremum of A).

Hasse Diagrams

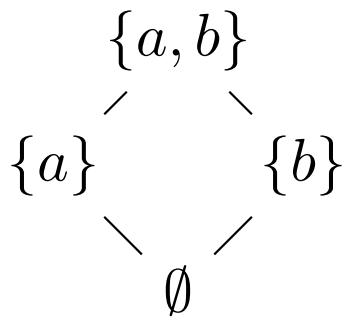
Definition

A Hasse diagram is a graphical representation of a partially ordered set, depicting the elements and the partial order relation.

- Hasse diagrams are used to represent posets visually.
- They remove redundant edges, making the structure easier to understand.
- Useful for studying properties like chains and antichains.

Examples of Hasse Diagrams

1. Divisibility Poset:
   - Let S be the set of positive integers.
   - The relation $a \leq b$ if a divides b forms a poset.
   - Hasse diagram removes redundant edges.
2. Power Set Lattice:
   - Consider the power set $\mathcal{P}(S)$ of a set S.
   - Ordered by set inclusion ($A \subseteq B$), it forms a lattice.



Some Rules for Drawing a Hasse Diagram

1. If $p < q$ in the poset, then the point corresponding to p appears lower in the drawing than the point corresponding to q.
2. The two points p and q will be joined by a line segment if p is related to q.
3. No edge is implied by transitivity.
4. All edges whose orientation is omitted go upward.

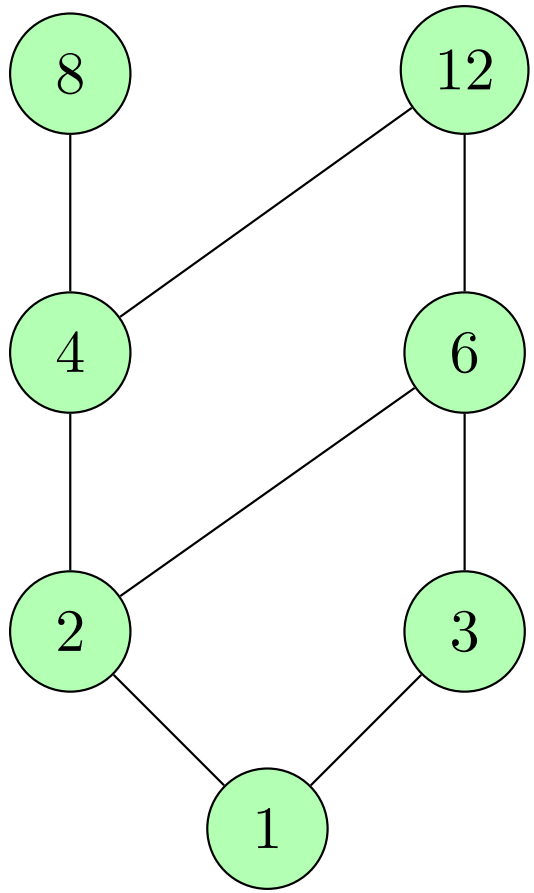
Examples of Hasse Diagrams

Example 1: Divisibility Poset

- Set

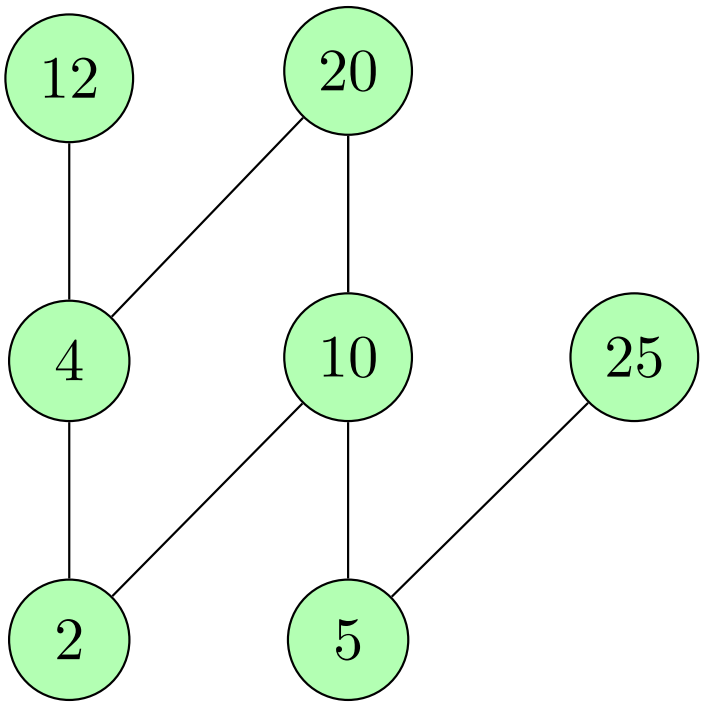
  $S = \{1, 2, 3, 4, 6, 8, 12\}$

- Relation: $a \leq b$ if a divides b



Examples of Hasse Diagrams

Example 2: Hasse Diagram for Poset $(\{2, 4, 5, 10, 12, 20, 25\}, |)$

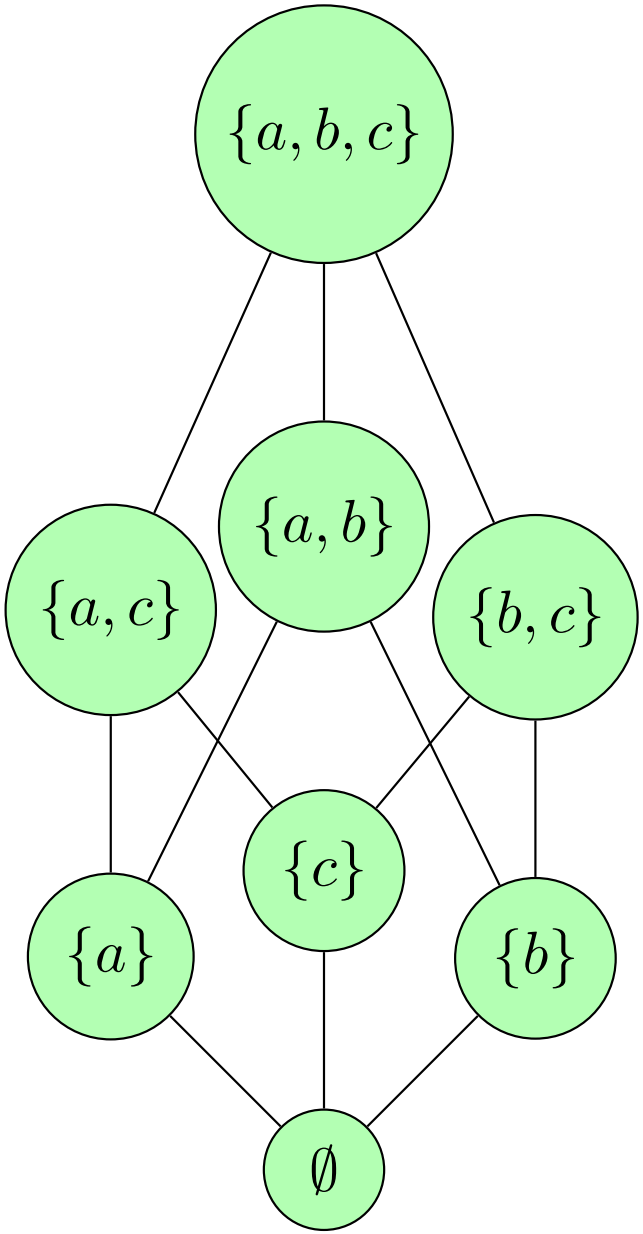


Examples of Hasse Diagrams

Example 3: The Hasse Diagram of

$(\mathcal{P}(\{a, b, c\}), \subseteq)$

- Set $S = \{a, b, c\}$
- Hasse diagram of the power set $\mathcal{P}(S)$ with $\subseteq$ relationship.



Lattices

Definition

A lattice is a partially ordered set in which every two elements have both a supremum (least upper bound) and an infimum (greatest lower bound).

Example: Lattice of Subspaces

- Let V be a vector space over a field F.
- The set of all subspaces of V, denoted $\text{Sub}(V)$, forms a lattice under set inclusion.
- The supremum of two subspaces U and W is their intersection $U \cap W$, and the infimum is their sum $U + W$.

More Examples

- Example 1: Poset of Divisibility
- Example 2: Real Numbers with Standard Order
- Example 3: Hasse Diagram of Power Set
- Example 4: Lattice of Subspaces

Thank You.



Discrete Mathematical Structures

CSET106

Dr. Gopinath Sahoo

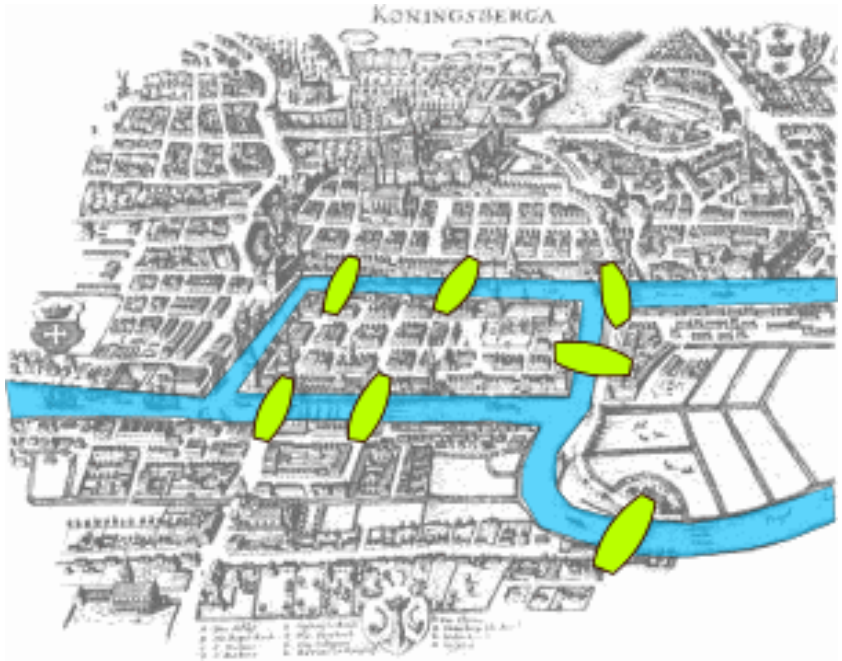
Module 4

Graph Theory



Seven Bridges of Königsberg and Graph Theory

- The city of Königsberg in Prussia (now Kaliningrad, Russia) was set on both sides of the Pregel River, and included two large islands—Kneiphof and Lomse—which were connected to each other, and to the two mainland portions of the city, by seven bridges.



- The problem was to devise a walk through the city that would cross each of those bridges once and only once.

- Leonhard Euler (in 1736) first pointed out that the choice of route inside each land mass is irrelevant and that the only important feature of a route is the sequence of bridges crossed.
- This allowed him to reformulate the problem in abstract terms (laying the foundations of graph theory).



Graphs: Vertices and Edges

Definition

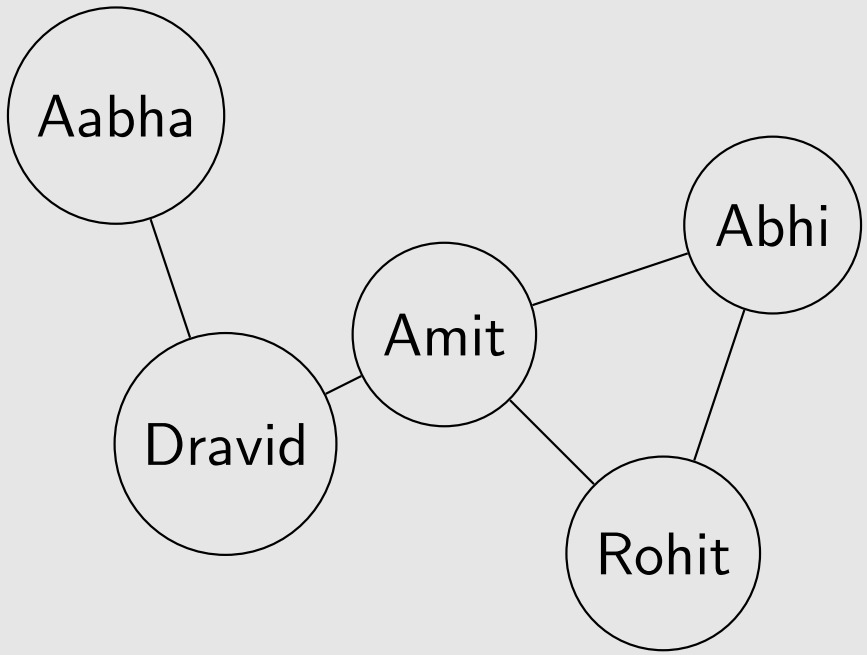
A graph $G = (V, E)$ consists of:

- **Vertices** V: Representing entities or points.
- **Edges** E: Connecting pairs of vertices.

Applications of Graphs

Social Networks

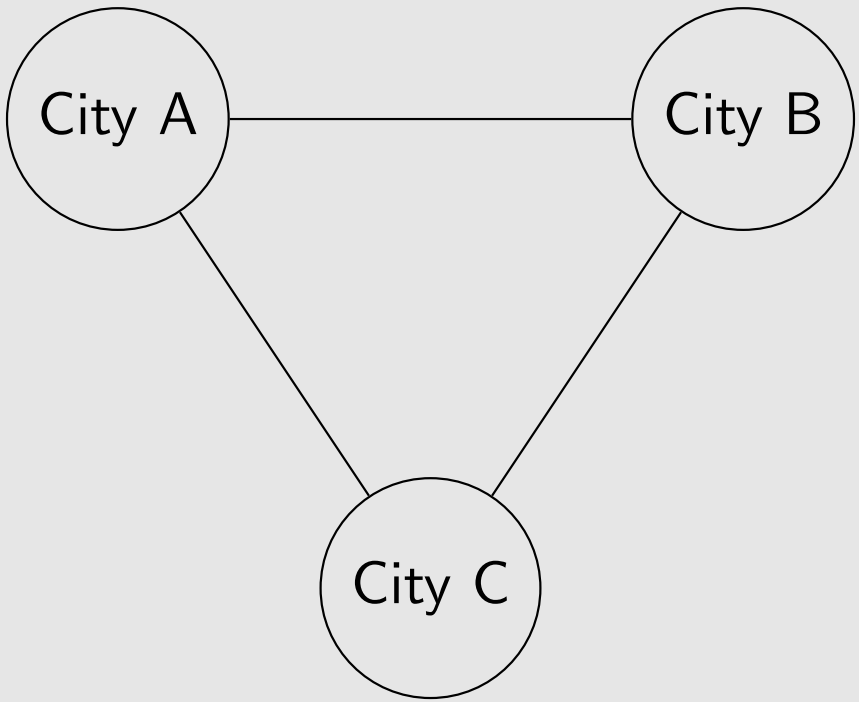
- **Graph Representation**: Users as vertices, friendships as edges.
- **Example**: Facebook, where users (vertices) are connected by friend relationships (edges).



Applications of Graphs

Road Networks

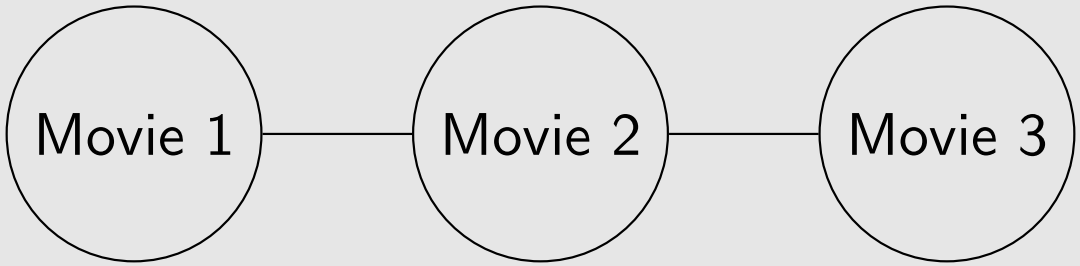
- **Graph Representation**: Cities as vertices, roads as edges.
- **Example**: Google Maps, where cities (vertices) are connected by roads (edges).



Applications of Graphs

Recommendation Systems

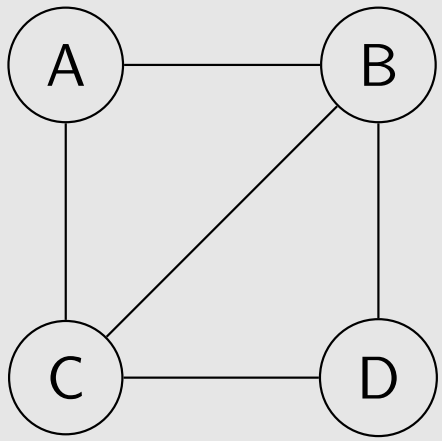
- **Graph Representation**: Items as vertices, connections as similarity or interactions.
- **Example**: Netflix, where movies (vertices) are connected based on user ratings or genre similarities.



Types of Graphs

Undirected Graph

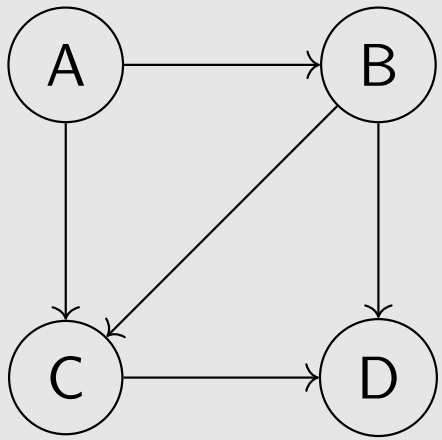
- **Definition**: A graph where edges have no direction.
- **Example**:



Types of Graphs

Directed Graph (Digraph)

- **Definition**: A graph where edges have a direction. Each directed edge is associated with an ordered pair of vertices.
- A directed edge/an arc associated with the ordered pair (u, v) is said to start at u and end at v.
- **Example**:



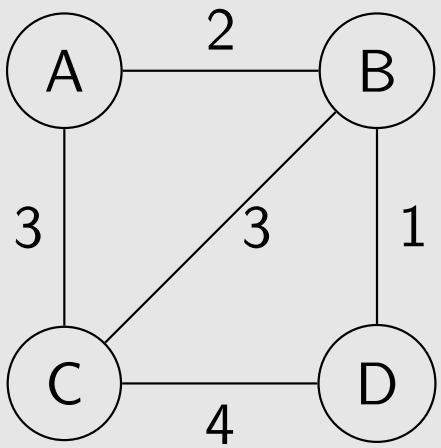
Types of Graphs

- A directed graph with no multiple directed edges and loops is called simple directed graph.
- A directed graph with multiple directed edges and loops is called directed multi-graph or multi-directed graph or multidigraph.
- A graph with both directed and undirected edges is called a mixed graph.

Types of Graphs

Weighted Graph

- **Definition**: A graph where edges have weights or costs.
- **Example**:

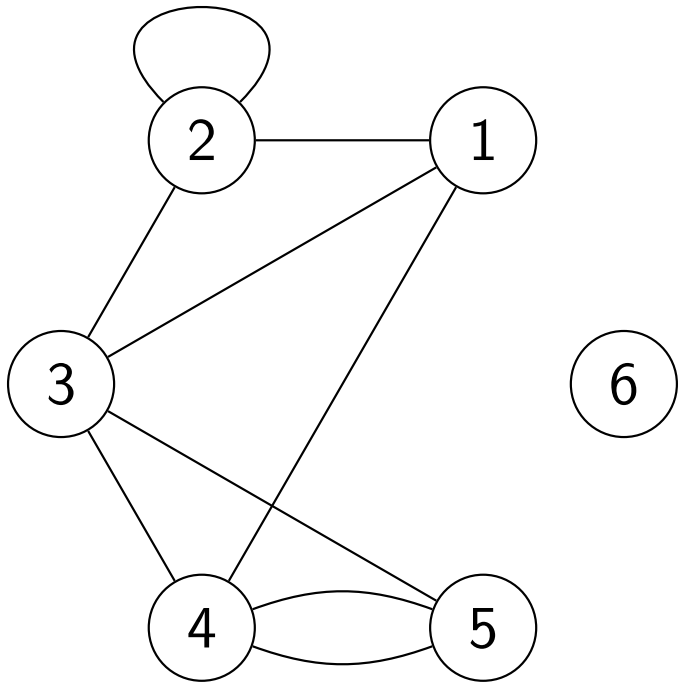


Terminology for Undirected Graphs

- Two vertices u and v in an undirected graph G are called adjacent (or **neighbours**) in G if u and v are endpoints of an edge e of G.
- Such an edge e is called incident with the vertices u and v.
- The set of all neighbours of a vertex v of $G = (V, E)$, denoted by $N(v)$, is called the neighbourhood of v.
- The degree of a vertex in an undirected graph is the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex. The degree of the vertex v is denoted by $\deg(v)$.

Example

- $\deg(1) = 3, \deg(2) = 4, \deg(3) = 4, \deg(4) = 4, \deg(5) = 3, \deg(6) = 0.$
- The neighbourhood of the vertex 1 is : $N(1) = \{2, 3, 4\}$. Similarly, $N(2) = \{1, 2, 3\}, N(3) = \{1, 2, 4, 5\}, N(4) = \{1, 3, 5\}, N(5) = \{3, 4\}, N(6) = \phi.$
- The vertex 6 is called an **isolated vertex**.



Handshaking Theorem

- The Handshaking Theorem is a fundamental result in graph theory that relates the degrees of vertices in a graph to the number of edges.
- Let $G = (V, E)$ be an undirected graph with n vertices and m edges. The total degree of all vertices in G is equal to twice the number of edges:

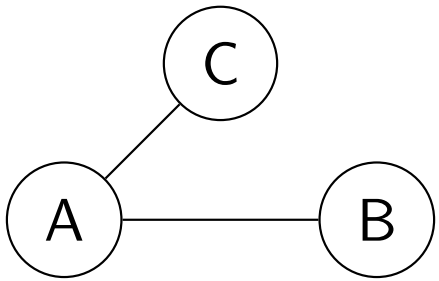
$$\sum_{v \in V} \deg(v) = 2m.$$

- This can also be written as:

$$2m = \text{sum of degrees of all vertices}$$

Example

Let's consider a simple graph:



This graph has 3 vertices and 3 edges.

The degrees of the vertices are:

- deg(A) = 2
- deg(B) = 1
- deg(C) = 1

The sum of the degrees of all vertices is $2+1+1=4$, which is equal to 2×2, the number of edges.

Corollaries of Handshaking Theorem

The Handshaking Theorem leads to some interesting corollaries:

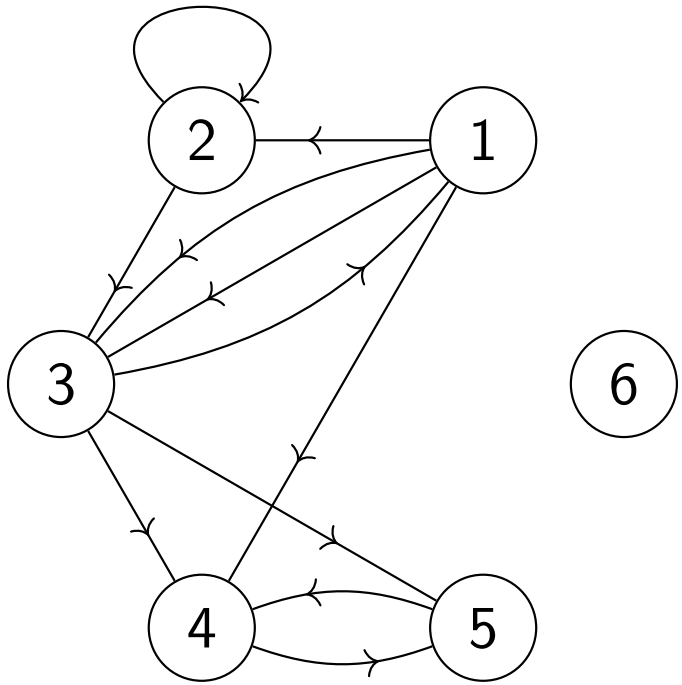
- The sum of the degrees of all vertices in any graph is always even.
- In any graph, the number of vertices with odd degree is always even.
- In any graph, there must be an even number of vertices of odd degree.

Terminologies for Directed Graphs

- When (u, v) is a directed edge or an arc of a digraph G, then u is said to be adjacent to v and v is said to be adjacent from u.
- The vertex u is called the initial vertex of (u, v), and v is called the terminal or end vertex of (u, v).
- The initial vertex and terminal vertex of a directed loop are the same.
- In a digraph the in-degree of a vertex v, denoted by $\deg^-(v)$, is the number of edges with v as their terminal vertex. The out-degree of v, denoted by $\deg^+(v)$, is the number of edges with v as their initial vertex.
- Note that a directed loop at a vertex contributes 1 to both the in-degree and the out-degree of this vertex.

Example

- $\deg^-(1) = 1, \deg^-(2) = 2, \deg^-(3) = 3, \deg^-(4) = 3, \deg^-(5) = 2, \deg^-(6) = 0.$
- $\deg^+(1) = 4, \deg^+(2) = 2, \deg^+(3) = 3, \deg^+(4) = 1, \deg^+(5) = 1, \deg^+(6) = 0.$



Handshaking Theorem for Directed Graphs

- The Handshaking Theorem for directed graphs states that the sum of the in-degrees of all vertices is equal to the sum of the out-degrees of all vertices, which is also equal to the total number of edges in the digraph.
- Mathematically:

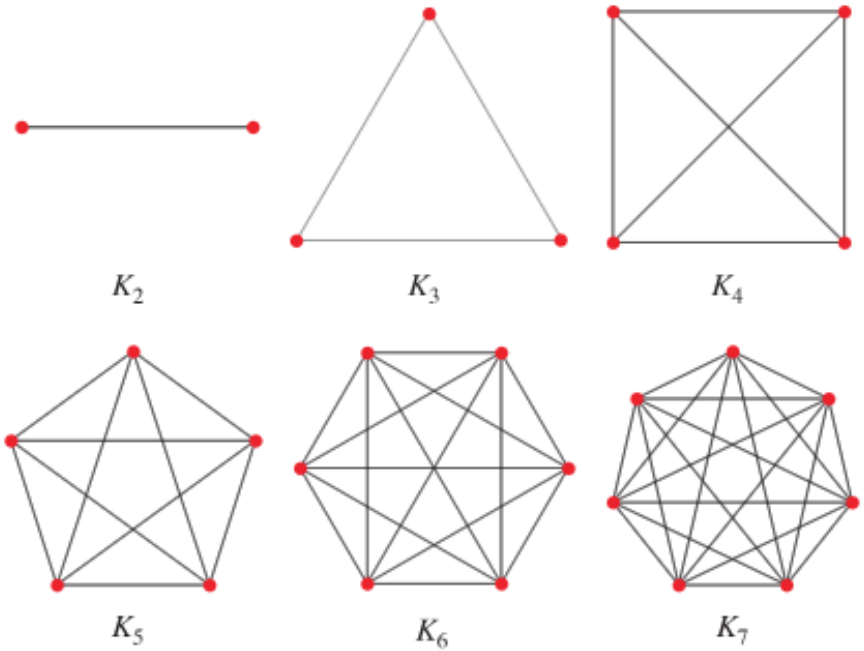
$$\sum_{v \in V} \text{in-degree}(v) = \sum_{v \in V} \text{out-degree}(v) = |E|$$

where $|E|$ is the number of directed edges in the digraph.

Special Classes of Graphs

Complete Graph

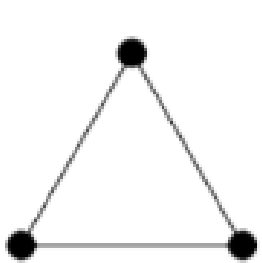
- A complete graph is a graph in which every pair of distinct vertices is connected by a unique edge.
- In other words, it is a graph where each vertex is connected to every other vertex in the graph.



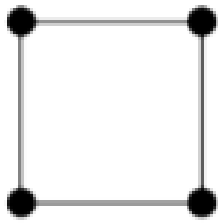
- The complete graph on n vertices is denoted by K_n.
- K_n has ${}^nC_2 = n(n-1)/2$ edges.

Cycle Graph

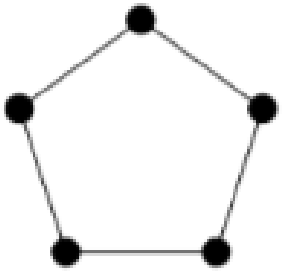
- A cycle graph, denoted by C_n, $n \geq 3$, consists of n vertices $v_1, v_2, \cdots, v_n$ and edges $\{v_1, v_2\}, \{v_2, v_3\}, \cdots, \{v_{n-1}, v_n\}$, and $\{v_n, v_1\}$.



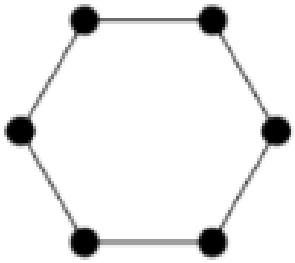
C_3



C_4



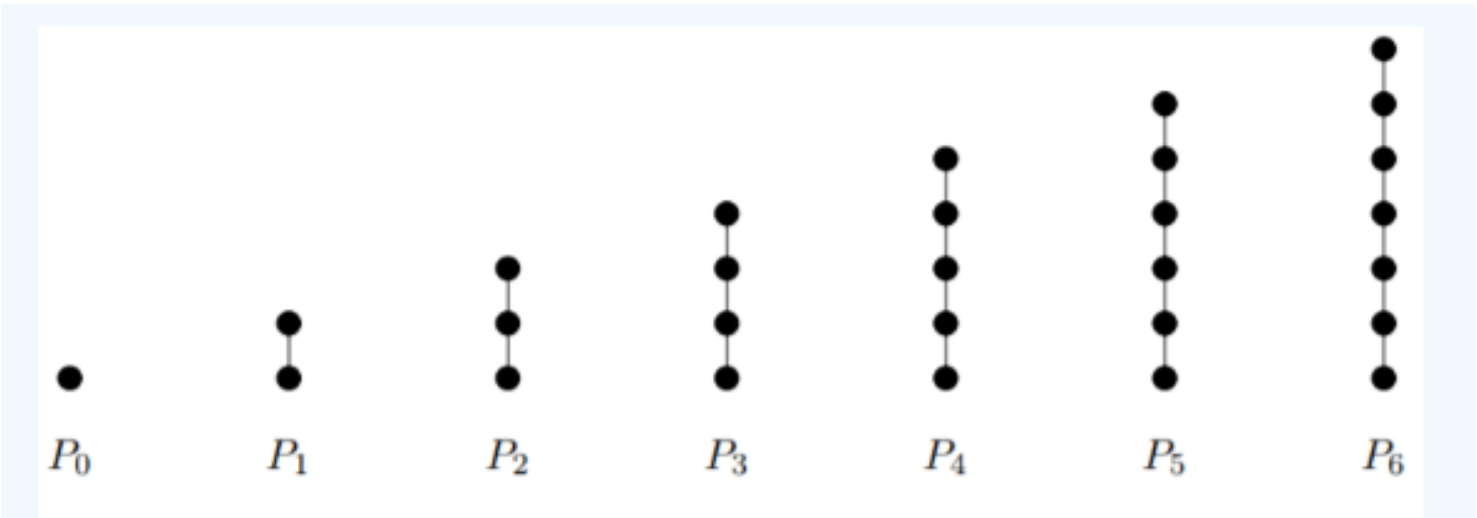
C_5



C_6

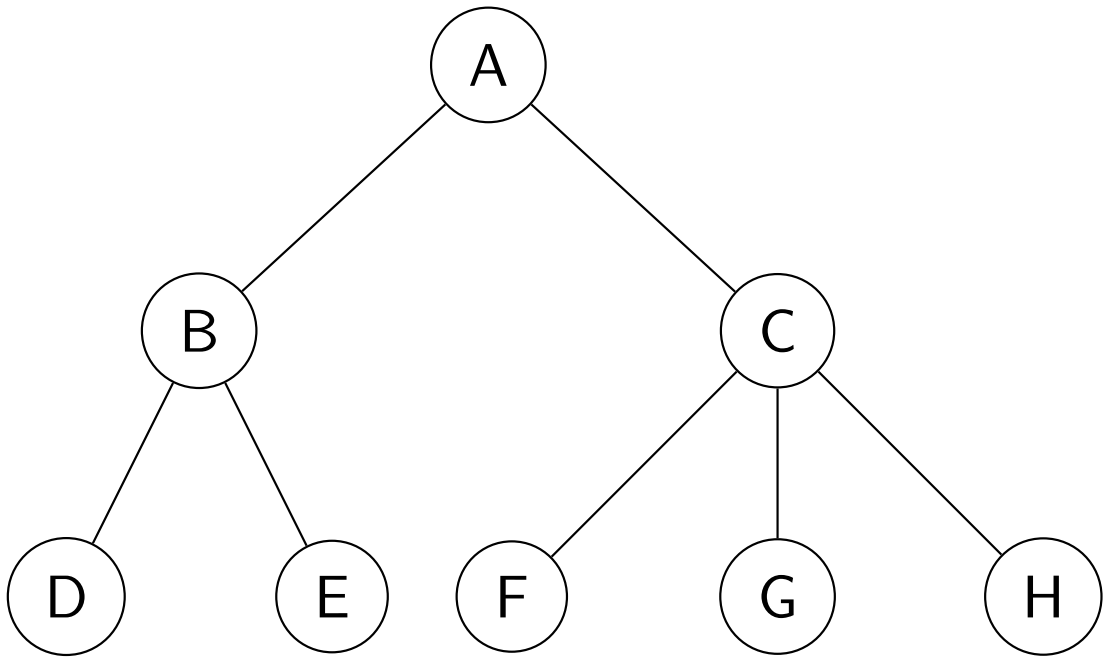
Path Graph

- A path graph on n vertices, denoted by P_n, is a graph whose vertices can be listed in the order $v_1, v_2, \cdots, v_n$ such that the edges are $\{v_i, v_{i+1}\}$ where $i = 1, 2, \cdots, n-1$.
- Equivalently, a path with at least two vertices is connected and has two terminal vertices (vertices that have degree 1), while all others (if any) have degree 2.



Tree and Forest

- A tree is an undirected graph in which any two vertices are connected by exactly one path, or equivalently a connected acyclic undirected graph.
- The number of edges of a tree on n vertices is always $n - 1$.
- **Example**:

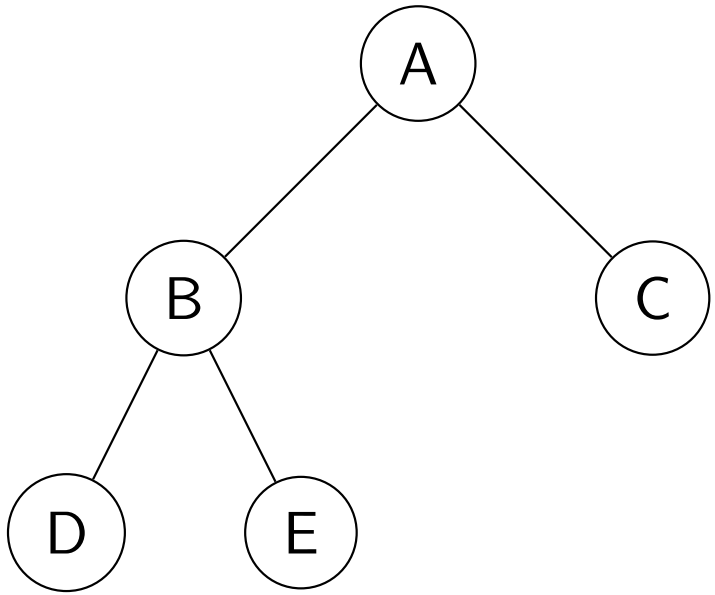


Tree and Forest

- A forest is an undirected graph in which any two vertices are connected by at most one path, or equivalently an acyclic undirected graph, or equivalently a disjoint union of trees.

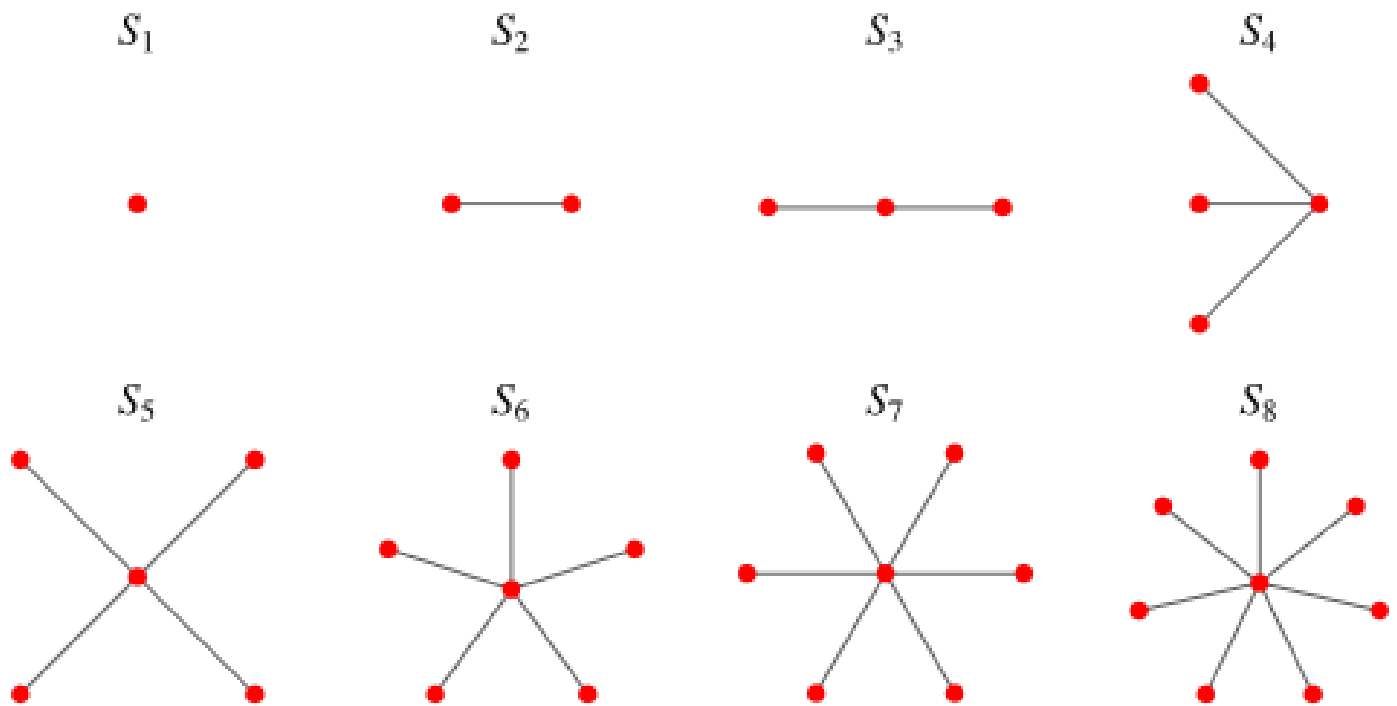
Binary Tree

- **Definition**: A tree in which each node has at most two children.
- **Example**:



Star Graph

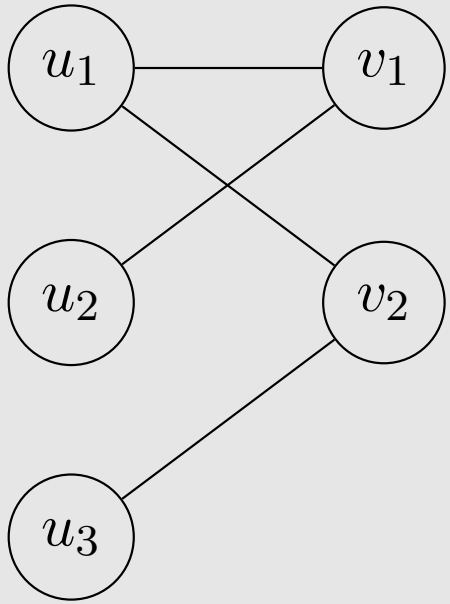
- The star graph S_n of order n is a tree on n nodes with one node having vertex degree $n-1$ and the other $n-1$ having vertex degree 1.



Special Types of Graphs (Cont'd)

Bipartite Graph

- **Definition**: A graph whose vertices can be divided into two disjoint sets U and V, such that each edge connects a vertex in U to a vertex in V.
- **Example**:



- A graph is bipartite if and only if it does not contain any cycle subgraphs of odd order.

Complete Bipartite Graph

- A complete bipartite graph is a bipartite graph (i.e., a set of graph vertices decomposed into two disjoint sets such that no two vertices within the same set are adjacent) such that every pair of vertices in the two sets are adjacent.
- If there are p and q graph vertices in the two sets, the complete bipartite graph is denoted $K_{p,q}$.
- Note that $S_n = K_{1,n-1}$ and $C_4 = K_{2,2}$.

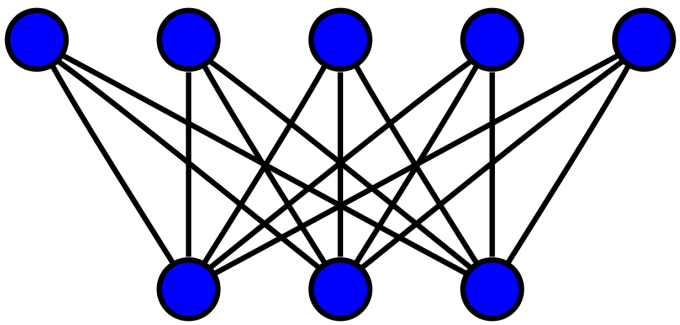


Figure: $K_{5,3}$

Regular Graph

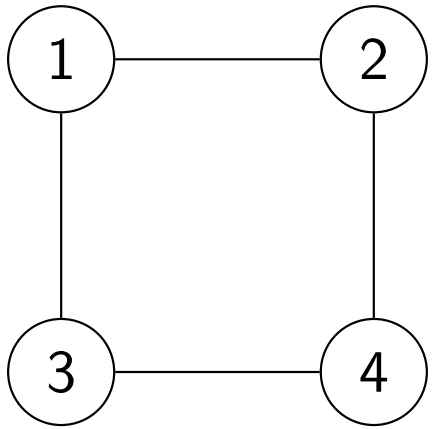
- A simple graph is called regular if every vertex of this graph has the same degree.
- A regular graph is called n-regular if every vertex in this graph has degree n.
- The complete graph K_n on n vertices is $n-1$ regular.
- The cycle graph C_n on $n \geq 3$ vertices is 2-regular.
- A regular graph of degree k with n vertices has $\frac{kn}{2}$ edges.

Representation of Graphs

Adjacency Matrix of a Graph

Definition

The adjacency matrix of a graph is a square matrix where the rows and columns are indexed by the vertices of the graph. If there is an edge between vertices i and j, the entry in the matrix at row i and column j (as well as row j and column i for undirected graphs) is 1. If there is no edge, the entry is typically 0. For a directed graph, the matrix can have 1s representing edges going from i to j and 0s otherwise.



$$A = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

- In simple terms, if G is an undirected simple graph on n vertices, then its adjacency matrix $A(G) = (a_{ij})$ is an $n \times n$ matrix whose row and columns are indexed by the vertices of the graph and its ij-th entry is given by

$$a_{ij} = \begin{cases} 1 & \text{if } \{i, j\} \text{ is an edge of } G, \\ 0 & \text{otherwise.} \end{cases}$$

- The adjacency matrix of a simple undirected graph is always symmetric and is a binary matrix.

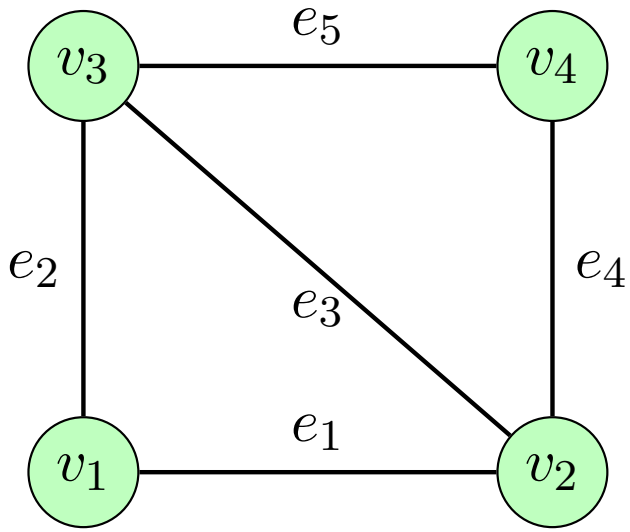
0-1 Incidence Matrix of a Graph

- The 0-1 incidence matrix of a graph is a matrix representation that describes the relationships between vertices and edges using binary values.
- Let $G = (V, E)$ be a graph with n vertices and m edges. The 0-1 incidence matrix M of G is an $n \times m$ matrix defined as follows:

$$m_{ij} = \begin{cases} 1 & \text{if vertex } v_i \text{ is incident to edge } e_j \\ 0 & \text{otherwise} \end{cases}$$

Example

Consider the following graph:



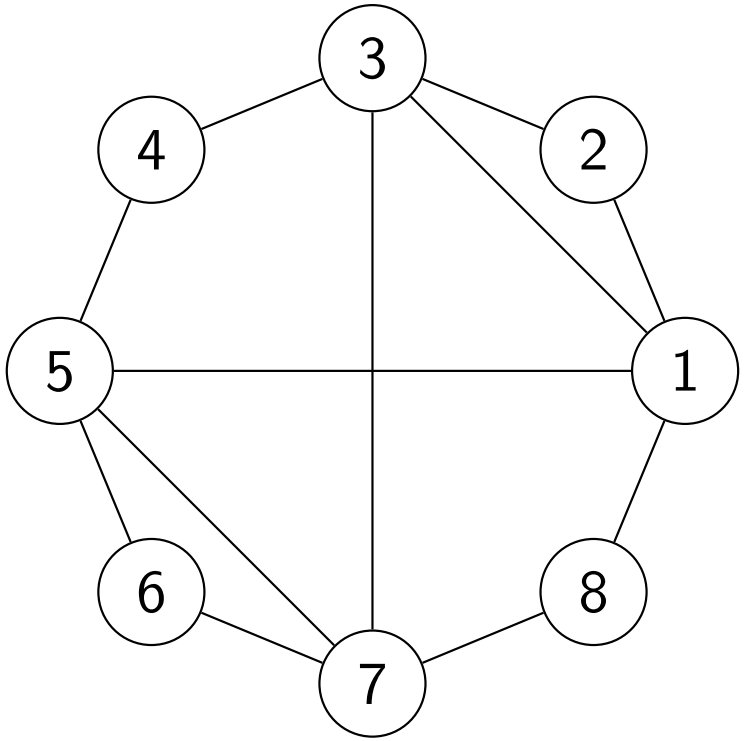
The 0-1 incidence matrix M of this graph is:

$$M = \left(\begin{array}{c|ccccc} & e_1 & e_2 & e_3 & e_4 & e_5 \\ \hline v_1 & 1 & 1 & 0 & 0 & 0 \\ v_2 & 1 & 0 & 1 & 1 & 0 \\ v_3 & 0 & 1 & 1 & 0 & 1 \\ v_4 & 0 & 0 & 0 & 1 & 1 \end{array}\right)$$

A Walk and a Circuit in a Graph

- A walk in a graph is a sequence of vertices connected by edges. Each consecutive pair of vertices in the sequence must be adjacent in the graph.
- A trail is a walk in which all edges are distinct.
- A path is a trail in which all vertices (and therefore also all edges) are distinct.
- A circuit in a graph is a closed walk where the starting and ending vertices are the same.

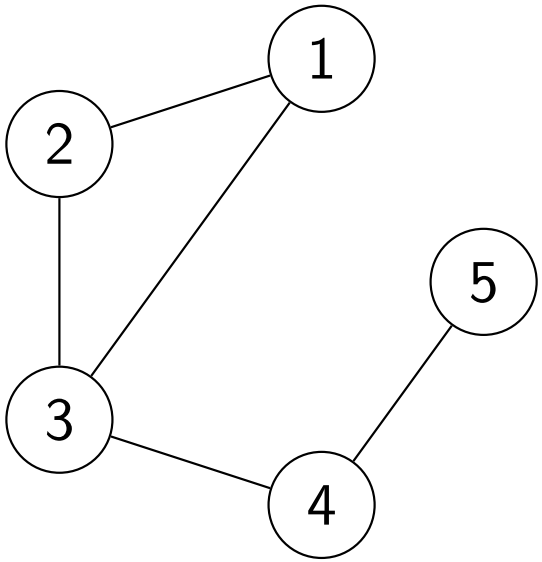
Example



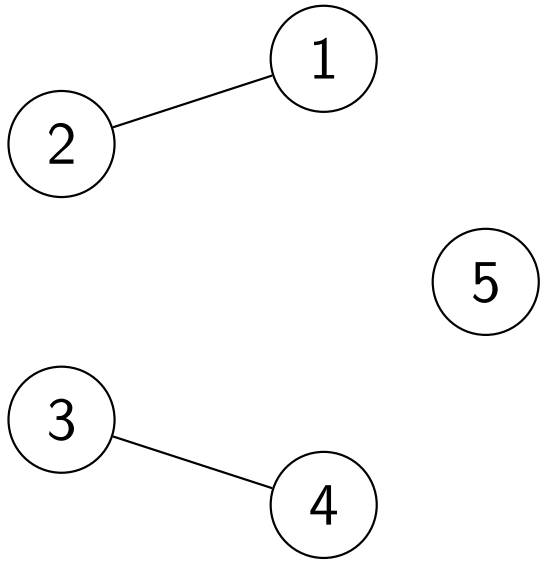
- 1-3-7-6-5-7 is a walk, but 1-3-7-8-6 is not a walk.
- 1-3-7-6-5-7 is a trail, but 1-3-7-5-1-3-4 is not a trail.
- 1-3-7-6-5 is a path, but 1-3-7-5-6-7 is not a path.
- 1-3-7-5-1 is a circuit, but 1-3-7-5-4-3 is not a circuit.

Connected Graph

- An undirected graph is called connected if there is a path between every pair of distinct vertices of the graph.
- An undirected graph that is not connected is called disconnected.
- Example:



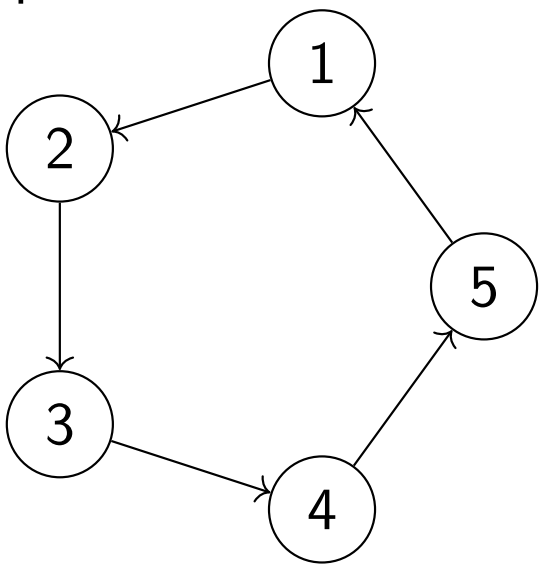
Connected Graph



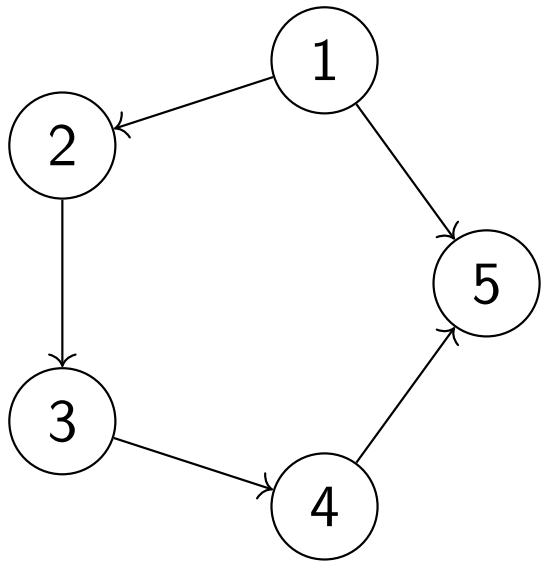
Disconnected Graph

Connectedness in Directed Graphs

- A directed graph is strongly connected if there is a path from u to v and from v to u whenever u and v are vertices in the digraph.
- A directed graph is weakly connected if there is a path between every two vertices in the underlying undirected graph.
- Example:



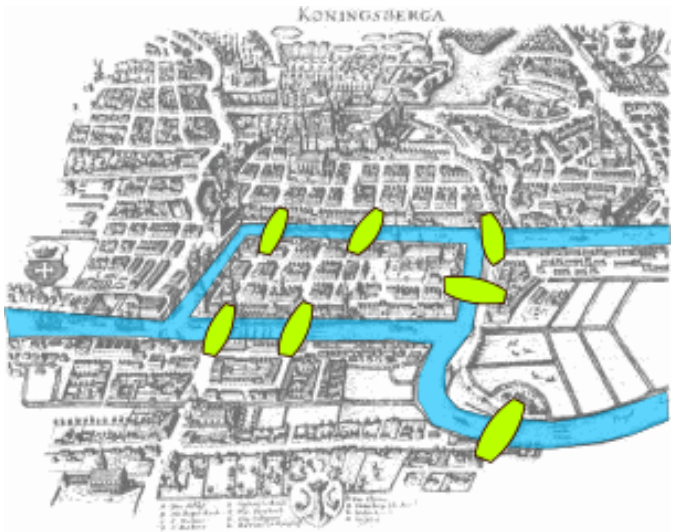
Strongly Connected Digraph



Weekly Connected Digraph

Euler Graph

- Given a graph G, is it possible to find a walk that traverses each edge exactly once, goes through all points, and ends at the starting point?

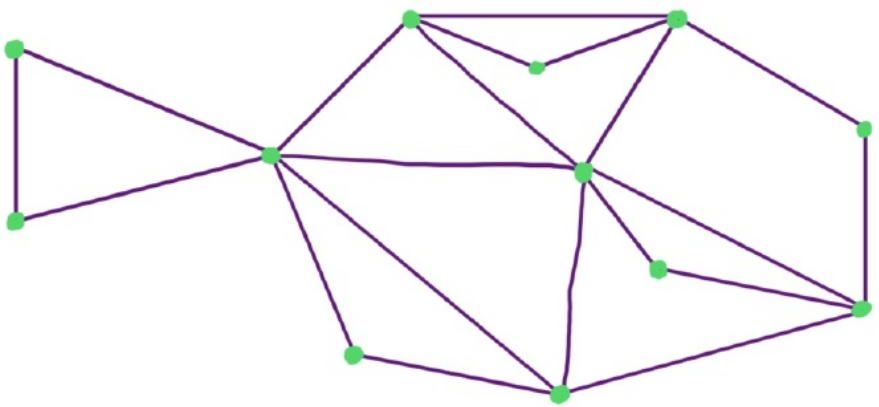


- A graph for which this is possible is called Eulerian.
- **Euler Graph**: An Euler graph is a graph that contains an Euler circuit, which is a closed walk that covers every edge exactly once. In other words, an Euler graph is a connected graph where every vertex has an even degree.

Equivalent Conditions for an Eulerian Graph

The following statements are equivalent for a connected graph G:

1. G is Eulerian.
2. Every point of G has even degree.
3. The set of edges of G can be partitioned into cycles.

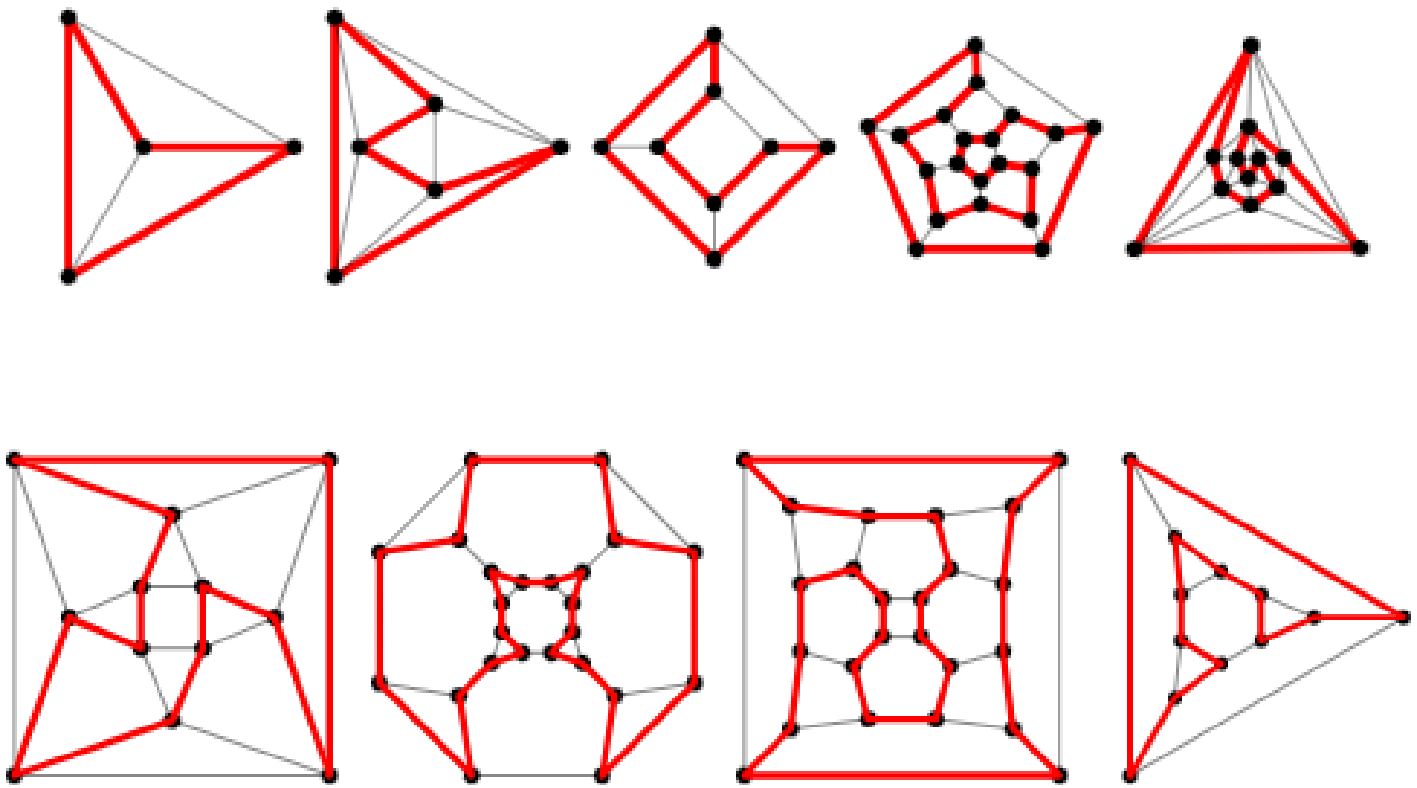


- **Euler Circuit**: An Euler circuit is a circuit (closed walk) in a graph that visits every edge exactly once and returns to the starting vertex. It is a closed trail in which all vertices are visited exactly once, except possibly the starting and ending vertices.
- **Euler Path**: An Euler path is a path (open walk) in a graph that visits every edge exactly once. Unlike an Euler circuit, an Euler path may start and end at different vertices. If the Euler path starts and ends at the same vertex, it's called an Euler circuit.

Hamiltonian Graph

- A simple path in a graph G that passes through every vertex exactly once is called a Hamilton path.
- A simple circuit in a graph G that passes through every vertex exactly once is called a Hamilton circuit.
- A graph that contains a Hamiltonian cycle is called a Hamiltonian graph.

Examples



Thank You.

