1. Introduction to Formal Language, Logic and Proof (7 hours- 9 Marks)

1.1. Brief review of set theory, function and relation
1.2. Propositional logic, expressing statements in propositional logic, rules of inference and proofs in propositional logic, introduction to predicate logic
1.3. Proofs, principle of mathematical induction, diagonalization principle, pigeonhole principle
1.4. Alphabet and language
1.5. Operations on languages: Union, concatenation, Kleene star

TOC Introduction:

The theory of computation is the branch that deals with whether and how efficiently problems can be solved on a model of computation, using an algorithm.
The field is divided into three major branches:

- automata theory,
- computability theory

Set Theory, Functions, and Relations: A Detailed Review

1. Set Theory

1.1. Key Concepts and Notation

A set is a well-defined collection of distinct objects (elements). These elements can be anything: numbers, symbols, or even other sets.
For example, the collection of the four letters a, b, c, and d is a
set, name L
The objects comprising / consists of a set are called its elements or members.

Notation:

- Roster (Listing) Method: Elements are explicitly listed: A = {1, 2, 3}.
- Set Builder Notation: Describes elements with a condition: A = {x | x is a positive integer and x < 4}.

  e.g. L = {a, b, c, d}, S= {5,10,15,20}, V= {a, e, i, o , u}.
  - L={x|x is a lowercase letter between a and d}.
  - S={x|x=5n,n∈Z+,1≤n≤4}

  This describes S as the set of all X such that X is a multiple of 5 and lies between 5 and 20.

- **For an element that belongs to a set:**
  Example: b is an element of the set L, which we write as: b∈L
  This means L contains b.
- **For an element that does not belong to a set:**
  Example: z is **not** an element of the set L, which we write as: z∉L
  This means L does not contain z.

Important Properties:
- Elements are unique. A = {1, 2, 2} simplifies to A = {1, 2}.
- Order does not matter. {1, 2} = {2, 1}.

1.2. Types of Sets

1. Singleton Set: A set with exactly one element.

Characteristics:

- Also called a unit set.
- The cardinality of a singleton set is 1.

Example: S = {a}.

A = {f :x is a divisor of a prime number other than the prime itself}

= {1} .

2. Infinite Sets: A set that has an uncountable or infinite number of elements.

Characteristics:

The number of elements in the set is not finite, and it goes on indefinitely.

Includes uncountable sets like real numbers ($\mathbb{R}$) or countable sets like integers ($\mathbb{Z}$).

Example: A = {x : is a natural number} = {1, 2, 3, 4, 5, 6, …….} .

3. Finite Set

A set that has a definite or countable number of elements.

Characteristics:

The number of elements in the set is finite and can be determined.

Example: A = {x:x is a vowel in the English language} = {a, e, i, o, u} .

4.. Empty set: A set that contains no elements. It is also called a null set.

Denoted by the symbol { } or **Ø.**

Any set other than the empty set is said to be nonempty

Example: A = {x: x is a male student in a girl's campus}

1.2.1. Relation between sets

Two sets A and B (say) may have common elements between them and there may exist relations between them defined as:

(a) Subset: A set A is said to be the subset of B if all elements of A belong to B. It is written as A ⊆ B.

For example,

A = { x : x is a letter in the English alphabet }

B = { x : x is a vowel }

Thus, B is a subset of A. B ⊆ A.

(b) Equal sets: Two sets A and B are said to be equal sets if they have the same elements in any order.

For example,

A = { a, e, i, o, u }

B = { a, i, e, o, u }

Then A = B.

(c) Intersecting sets: Two sets A and B are intersecting sets if they have at least one element in common.

A = { a, e, i, o, u }

B = { a, b, c, d, e }

(d) Disjoint sets: Two sets A and B are disjoint if they have no element in common.

A = { a, b, c } B = { y, z }

(e) Equivalent sets: Two sets A and B are said to be equivalent if they have the same number of elements.

A = { 0, 1, 2 }

B = { a, b, c, d } Here, n(A) = n(B).

(f) **Power set:** The power set is the set of any possible subset of any set. The power set of A, denoted P(A) i.e. a set containing '*n*' elements has a power set containing 2^n elements.

For example,

1. Let A = { 0, 1 } Then, power set of A: P(A) = 2^2= { {}, { 0 }, { 1 }, { 0, 1 } }.

2. Let S = {1, 2, 3}. So P(S) = {∅, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3}}.

Other examples of types of sets

(a) Universal set: A fixed state is a universal set if it contains all the subjects under discussion. For example, For the sets of people of different countries, the set of people in the world is universal set.

(b) Uncountable set: A set is uncountable if it contains so many elements that they can't be put one to one correspondence with the set of natural numbers. In other words, it is opposite to that of countably infinite set.
For example, The set of real numbers in [0, 1]

(c) Countably infinite set: A set is said to be countably infinite set if its elements can be put one- one correspondence with the set of natural numbers.
For example,
Z = { x : x is a element of integers }
= { -3, -2, -1, 0, 1, 2, 3, ... }
Here, we can't never count the cardinality of sets but if we arrange elements in such a way that
Z = { 0, -1, 2, -2, 2, -3, 3, ... }
And then if we are asked to count number of elements up to -3, we can do that. So, the set of integers is the countably infinite set.

1.3. Operation on sets

1. *Union:* Union of two sets A and B is the set of all elements belonging to at least one of the two sets or both. It is denoted by A ∪ B.
   A ∪ B = { x : x ∈ A or x ∈ B }

2. *Intersection:* Intersection of two sets A and B is the set of all elements belonging to both of the sets. It is denoted by A ∩ B.
   A ∩ B = { x : x ∈ A and x ∈ B }

3. *Difference:* The difference of two sets A and B denoted by A - B is the set of all elements of A that aren't elements of B.
   A - B = { x : x ∈ A and x ∉ B }

4. *Symmetric difference:*
   Symmetric difference of two sets A and B is the set of all elements which are in either of the sets and not in their intersection. The symmetric difference is denoted by A Δ B
   Let A, B be sets. Then A Δ B is
   A Δ B = (A - B) ∪ (B - A)
   AΔB: = {x: x ∈ A or x ∈ B, but x ∉ A ∩ B}
   Example: Let A = {1, 2, 3} and B = {1, 3, 5}. Then A Δ B = {2, 5}.

5. Complement: The "complement" of set A, written as A is the set containing everything that is not in A.

1.4 Properties of set operation

Set Identities

An **identity** is an equation that is universally true for all elements in some set. For example, the equation $a + b = b + a$ is an identity for real numbers because it is true for all real numbers a and b. The collection of set properties in the next theorem consists entirely of set identities. That is, they are equations that are true for all sets in some universal set.

Theorem 6.2.2 Set Identities

Let all sets referred to below be subsets of a universal set U.

1. *Commutative Laws:* For all sets A and B,
   $$\text{(a) } A \cup B = B \cup A \quad \text{and} \quad \text{(b) } A \cap B = B \cap A.$$
2. *Associative Laws:* For all sets A, B, and C,
   $$\text{(a) } (A \cup B) \cup C = A \cup (B \cup C) \quad \text{and}$$
   $$\text{(b) } (A \cap B) \cap C = A \cap (B \cap C).$$
3. *Distributive Laws:* For all sets, A, B, and C,
   $$\text{(a) } A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{and}$$
   $$\text{(b) } A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$
4. *Identity Laws:* For all sets A,
   $$\text{(a) } A \cup \emptyset = A \quad \text{and} \quad \text{(b) } A \cap U = A.$$
5. *Complement Laws:*
   $$\text{(a) } A \cup A^c = U \quad \text{and} \quad \text{(b) } A \cap A^c = \emptyset.$$
6. *Double Complement Law:* For all sets A,
   $$(A^c)^c = A.$$
7. *Idempotent Laws:* For all sets A,
   $$\text{(a) } A \cup A = A \quad \text{and} \quad \text{(b) } A \cap A = A.$$
8. *Universal Bound Laws:* For all sets A,
   $$\text{(a) } A \cup U = U \quad \text{and} \quad \text{(b) } A \cap \emptyset = \emptyset.$$
9. *De Morgan's Laws:* For all sets A and B,
   $$\text{(a) } (A \cup B)^c = A^c \cap B^c \quad \text{and} \quad \text{(b) } (A \cap B)^c = A^c \cup B^c.$$
10. *Absorption Laws:* For all sets A and B,
    $$\text{(a) } A \cup (A \cap B) = A \quad \text{and} \quad \text{(b) } A \cap (A \cup B) = A.$$
11. *Complements of U and $\emptyset$:*
    $$\text{(a) } U^c = \emptyset \quad \text{and} \quad \text{(b) } \emptyset^c = U.$$
12. *Set Difference Law:* For all sets A and B,
    $$A - B = A \cap B^c.$$

Show that $A-(B\cup C)=(A-B)\cap(A-C)$.

$$\begin{aligned} x\in A-(B\cup C) &\Rightarrow x\in A \text{ and } x\notin B\cup C \\ &\Rightarrow x\in A \text{ and } x\notin B \text{ and } x\notin C \\ &\Rightarrow (x\in A \text{ and } x\notin B) \text{ and } (x\in A \text{ and } x\notin C) \\ &\Rightarrow x\in A-B \text{ and } x\in A-C \\ &\Rightarrow x\in (A-B)\cap(A-C) \end{aligned}$$

Therefore $A-(B\cup C)\subseteq(A-B)\cap(A-C)$ (1)

Conversely,

$$\begin{aligned} x\in (A-B)\cap(A-C) &\Rightarrow x\in A-B \text{ and } x\in A-C \\ &\Rightarrow (x\in A \text{ and } x\notin B) \text{ and } (x\in A \text{ and } x\notin C) \\ &\Rightarrow x\in A \text{ and } (x\notin B \text{ and } x\notin C) \\ &\Rightarrow x\in A \text{ and } x\notin B\cup C \\ &\Rightarrow x\in A-(B\cup C) \end{aligned}$$

Therefore, $(A-B)\cap(A-C)\subseteq A-(B\cup C)$.

Hence $A-(B\cup C)=(A-B)\cap(A-C)$.

Countably infinite set: A set is said to be countably infinite set if its elements can be put one- one (objective) correspondence with the set of natural numbers.

Or A set is countably infinite if there is a one-to-one (objective) correspondence between 'elements of the set' and 'natural numbers'.

Uncountably infinite set: A set is Uncountably infinite if there is no one-to-one correspondence between 'elements of the set' and 'natural numbers'.

Examples of countably infinite sets:

(i) Set of "Natural numbers" is a trivial example.

N = {1, 2, 3, 4, 5, ...}

(ii) "Set of integers (Z)"

Explanation:

Let a function f : Z → N be defined as

f(0) = 1

f(x) = 2x if x > 0

f(x) = – 2x + 1 if x < 0

0	→	1
1	→	2
– 1	→	3
2	→	4
– 2	→	5
……	……	…….
……	…….	……..

Hence all integers are mapped to natural numbers.

(iii) Set of "Rational numbers (Q)"
Explanation:
Before proving 'Q' to be a countably infinite set,
let us prove an important theorem about union of countable sets.
'A', 'B' be two countable sets.

Let $A = \{a_1, a_2, a_3, a_4 .....\}$
$B = \{b_1, b_2, b_3, b_4 .....\}$

Let $A \cup B = C = \{a_1, b_1, a_2, b_2, a_3, b_3, ...\}$

$= \{c_1, c_2, c_3, c_4 ..... c_n ...\}$

$a_1 \rightarrow 1$
$b_1 \rightarrow 2$
$a_2 \rightarrow 3$
$b_2 \rightarrow 4$
.....
.....
$a_n \rightarrow 2n - 1$
$b_n \rightarrow 2n$

There is one-one correspondence between elements of 'C' and 'N'.
Hence union of two countable sets is countable.

(iv) **A positive rational number 'q' is of the form a/b where a, b ∈ N**

Arrange rational numbers in the orders of a + b.
If a + b for two rational numbers is same, arrange them in the order of 'a'

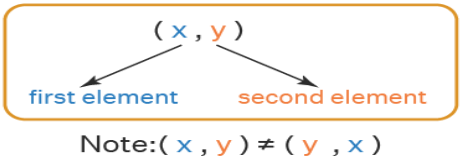
$$\left\{ \underbrace{\frac{1}{1}}_{a+b=2}, \underbrace{\frac{1}{2}, \frac{2}{1}}_{a+b=3}, \underbrace{\frac{1}{3}, \frac{2}{2}, \frac{3}{1}}_{a+b=4}, \underbrace{\frac{1}{4}, \frac{2}{3}, \frac{3}{2}, \frac{4}{1}}_{a+b=5}, \ldots\ldots \right\}$$

First element corresponds to 1, second to 2 and so on.
Hence rational numbers set is countably infinite set.

Note: The ordering of elements need not be same as given above.
It is merely one of many possible orderings.
For example,
→f(n)=2n, n ∈ N is countable infinite
→Z = {x: x is an element of integers}
= { -3, -2, -1, 0, 1, 2, 3, ...}
Here, we can't never count the cardinality of sets but if we arrange elements in such a way that
Z = {0, -1, 2, -2, 2, -3, 3, ...}
And then if we are asked to count number of elements up to -3, we can do that. So, the set of integers is the countably infinite set.

Uncountable set: A set is uncountable if it contains so many elements that they can't be put one to one correspondence with the set of natural numbers. In other words, it is opposite to that of countably infinite set.
Example:
Real Numbers, Rational Numbers, Irrational Numbers, Complex Numbers:

Order pair: An **ordered pair** is a pair formed by two elements that are separated by a comma and written inside the parentheses.



For example, (x, y) represents an ordered pair, where 'x' is called the first element and 'y' is called the second element of the ordered pair.

Cartesian Product of sets *A* and *B* is defined as the set of all ordered pairs (*x, y*) such that *x* belongs to *A* and *y* belongs to *B.* It is denoted by as $A \times B$ (read "*A* **cross** *B").*

i.e $A \times B = \{ (x, y) : x \in A \text{ and } y \in B \}$

For example, if $A = \{1, 2\}$ and $B = \{3, 4, 5\}$,
then the Cartesian Product of *A* and *B* is $\{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$.

Remark: Let S be a set. The subset relation forms a partial order on 2^S. To show two sets A and B are equal, we must show $A \subset B$ and $B \subset A$.
We demonstrate how to prove two sets are equal below.

Proposition 1.1. Let $A = \{6n: n \in Z\}$,
$B = \{2n: n \in Z\}$,
$C = \{3n: n \in Z\}$.
So $A = B \cap C$.

Proof. We first show that $A \subset B \cap C$.
Let $n \in Z$.
So $6n \in A$ i.e. we need to show $6n \in B \cap C$.
As 2 is a factor of 6, $6n = 2 \cdot (3n) \in B$.
Similarly, as 3 is a factor of 6, $6n = 3 \cdot (2n) \in C$. So $6n \in B \cap C$.

now show that
$B \cap C \subset A$.
Let $x \in B \cap C$.
Let $n1, n2 \in Z$ such that $x = 2n1 = 3n2$.
As 2 is a factor of x and 3 is a factor of x, it follows that $2 \cdot 3 = 6$ is also a factor of x. Thus, $x = 6n3$ for some $n3 \in Z$.
So $x \in A$. Thus, $B \cap C \subset A$. Thus, $A = B \cap C$, as desired.

Proposition 1.2. Let A, B, C be sets. Then $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Proof: Let $(x, y) \in A \times (B \cup C)$.
If $y \in B$, then $(x, y) \in (A \times B)$.
Otherwise, $y \in C$ and so $(x, y) \in (A \times C)$.
Thus, $A \times (B \cup C) \subset (A \times B) \cup (A \times C)$.
Now
let $(d, f) \in (A \times B) \cup (A \times C)$.
Clearly, $d \in A$.
So f must be in either B or C.
Thus, $(d, f) \in A \times (B \cup C)$,
which implies $(A \times B) \cup (A \times C) \subset A \times (B \cup C)$.
We conclude that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

2. Relations:

A relation is a connection or association between elements of two sets.
A relation is a correspondence between two sets (called the domain and the range) such that to each element of the domain, there is assigned one or more elements of the range.

State the domain and range of the following relation. Is the relation a function?

{(2, –3), (4, 6), (3, –1), (6, 6), (2, 3)}

The above list of points, being a relationship between certain x's and certain y's, is a relation. The domain is all the x-values, and the range is all the y-values. To give the domain and the range, just list the values without duplication:

domain: {2, 3, 4, 6}

range: {–3, –1, 3, 6}

Mathematical Definition of Relation:

A relation on sets S and T is a set of ordered pairs (s, t), where

(a) s ϵ S (s is a member of S)

(b) t ϵ T

(c) S and T need not be different

(d) The set of all first elements in the "domain" of the relation, and

(e) The set of all second elements is the "range" of the relation.

Example:

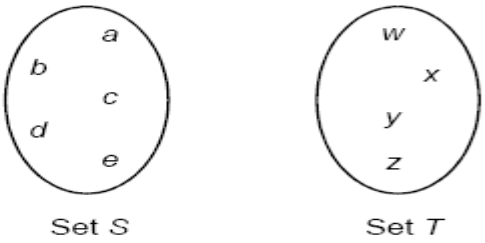


Fig. 1 Sets S and T are disjoint

Suppose S is the set $\{a, b, c, d, e\}$ and set T is $\{w, x, y, z\}$.

Then a relation on S and T is

$$R = \{(a, y),\ (c, w),\ (c, z),\ (d, y)\}$$

The four ordered pairs in the relation is represented as shown in Fig. 2.

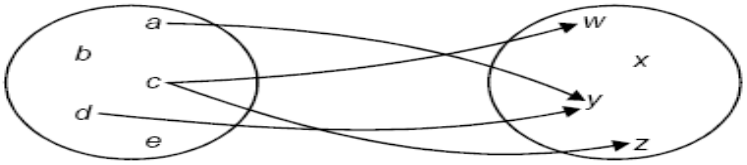


Fig. 2 Relation $R = \{(a, y), (c, w), (c, w), (c, z), (d, y)\}$

Types of Relations

1. Reflexive Relation
2. Symmetric/Anti- symmetric relation
3. Transitive relation
4. Equivalence Relation
5. Partial order
6. Total Order Relation

Types of relation

Identity relation:

In an identity relation "R", every element of the set "A" is related to itself only. Note the conditions conveyed through words "every" and "only". The word "every" conveys that identity relation consists of ordered pairs of element with itself - all of them. The word "only" conveys that this relation does not consist of any other combination.

E.g. Consider a set A={1,2,3} Then, its identity relation is: R={(1,1), (2,2),(3,3)}

Reflexive relation: In reflexive relation, "R", every element of the set "A" is related to itself. The definition of reflexive relation is exactly same as that of identity relation except that it misses the word "only" in the end of the sentence

i.e. A relation R ⊆ A x A is reflexive if (a, a) ∈ R for each a ∈ A. The directed graph representing a reflexive relation has a loop from each node to itself.

Consider a set

Let, A= {1,2,3} Then, one of the possible reflexive relations can be:
R= {(1,1), (2,2), (3,3), (1,2), (1,3)}
However, following is not a reflexive relation: R1= {(1,1), (2,2), (1,2), (1,3)}
But we can say R= {(1, 1), (2, 2), (3, 3)} is a reflexive relation defined on set A

Symmetric Relations:

A relation R ⊆ A x A is symmetric if (b, a) ∈ R whenever (a, b) ∈ R.

Let A= {1, 2, 3}
then R= {(1, 2), (2, 1), (2, 3), (3, 2)} is a Symmetric relation defined on set A

In symmetric relation, the instance of relation has a mirror image.

condition of symmetric relation as:

Iff (x,y)∈R⇒(y,x)∈R for all x,y∈A

The symbol "Iff" means "If and only if". Here one directional arrow means "implies".

Alternatively, the condition of symmetric relation can be stated as: xRy⇒yRx for all x, y ∈ A

It means that if (1,3) is an instance, then (3,1) is also an instance in the relation. Clearly, an ordered pair of element with itself like (1,1) or (2,2) is themselves their mirror images.

Consider some of the examples of the symmetric relation,

R1={(1,2),(2,1),(1,3),(3,1)}
R2={(1,2),(1,3),(2,1),(3,1),(3,3)}

Anti –symmetric Relations: if the relation is not symmetric then it is anti –symmetric. i.e.

A relation R ⊆ A x A is anti-symmetric if (b, a) ∈**R** where a and b are distinct and (a, b) ∉ **R**.

Example: if A={3,4,5}
Then R={(3,4),(3,5),(4,5)}

Transitive relation:

A binary relation R is transitive if whenever (a, b) ∈ R and (b, c) ∈ R, then (a, c) ∈ R.
The relation {(a, b): a, b ∈ P and a is an ancestor of b} is transitive, since if a is an ancestor of b and b is an ancestor of c, then a is an ancestor of c. So is the less-than-or-equal relation
Let A= { 1, 2, 3}
then R= { (1, 2), (2, 3) , (1, 3) } is a transitive relation defined on set A
If "R" be the relation on set A, then we state the condition of transitive relation as:

Iff(x,y)∈R and (y,z)∈R⇒(x,z)∈R for all a,b,c∈A

Alternatively, xRy and yRz⇒xRz for all x,y,z∈A

Equivalence relation:

A relation is equivalence relation if it is reflexive, symmetric and transitive at the same time. In order to check whether a relation is equivalent or not, we need to check all three characterizations.

A subset *R* of *A* x *A* is called an equivalence relation on *A* if *R* satisfies the following conditions:

(i) $(a, a) \in R$ for all $a \in A$ (R is reflexive)
(ii) If $(a, b) \in R$, then $(b, a) \in R$, then $(a, b) \in R$ (R is symmetric)
(iii) If $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$ (R is transitive)
Let A= { 1, 2, 3}
then R= { (1, 1), (2, 2) , (3, 3) , (1, 2) , (1, 3) , (2, 3) , (2, 1) , (3, 1) , (3, 2) }

Partial Ordering Relations
A relation R on a set S is called a "Partial ordering" or a "Partial order", if R is reflexive, antisymmetric and transitive.
Let A= { 1, 2, 3}
then R= { (1, 1), (2, 2) , (3, 3) , (1, 2), (2, 3) }
A set S together with a partial ordering R is called a "Partially ordered set" or "Poset".

Partition
A Partition P of S is a collection $\{Ai\}$ of nonempty subsets of S with the properties:
(i) Each $a \in S$ belongs to some Ai,
(ii) If $Ai \neq Aj$, then $Ai \cap Aj = \emptyset$.

3. Functions: A function is a special type of relation where each element of the domain is related to exactly one element of the codomain. Example: A = {1, 2, 3}, B = {x, y, z}, f = {(1, x), (2, y), (3, z)}.

Suppose every element of S occurs exactly once as the first element of an ordered pair. In Fig shown, every element of S has exactly one arrow arising from it. This kind of relation is called a "function".

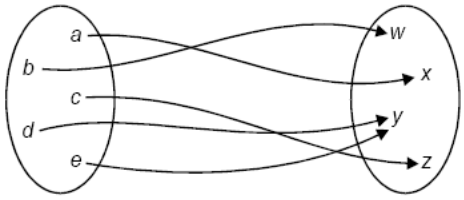


Fig. A Function

A function is otherwise known as "Mapping". A function is said to map an element in its domain to an element in its range. Every element in S in the domain, i.e., every element of S is mapped to some element in the range. No element in the domain maps to more than one element in the range.

Functions as relations
A function $f: A \rightarrow B$ is a relation from A to B i.e., a subset of A x B, such that each $a \in A$ belongs to a unique ordered pair (a, b) in f.

Kinds of Functions
(a) *One-to-One Function* (*Injection*): A function $f: A \rightarrow B$ is said to be one-to-one if different elements in the domain A have distinct images in the range.

For set A and B defined above
$R_1 \subset A \times B = \{(1, 3), (2, 4)\}$ is one-one function

A function f is one-to-one if $f(a) = f(a')$ implies $a = a'$.

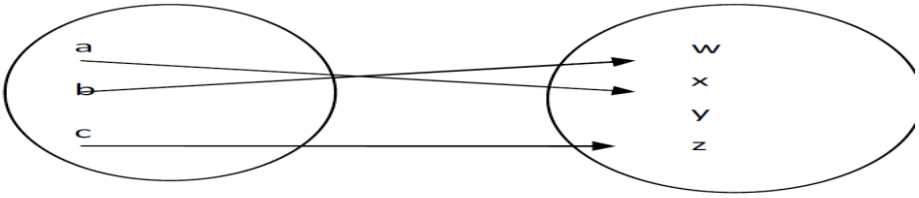
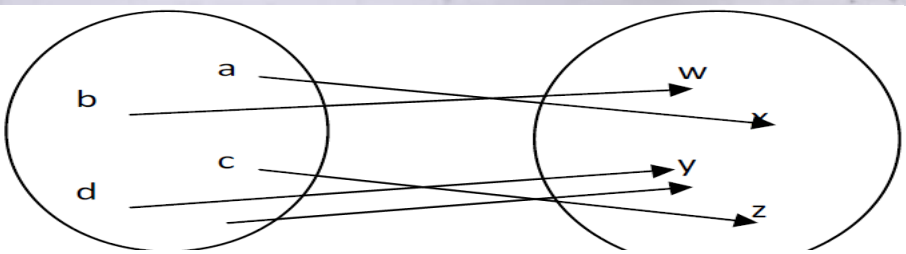


Fig: One to one function (Injection)

(b) *Onto function (Surjection): A function f : A→B is said to be an onto function if each element of B* is the image of some element of *A*. i.e., *f :A→B* is onto if the image of *f* is the entire codomain, i.e. if *f* (*A*) = *B*. i.e., *f* maps *A* onto *B*.

For set A and set B defined above
$R_2 \subset A \times B = \{(1, 3), (2, 4)\}$ is onto function.
Here, no element of B is left-over.



(c) *One-to-one onto Function (Bijection): A function that is both one-to-one and onto is called a "Bijection". Such a function maps each and every element of A* to exactly one element of *B*, with no elements left over. Fig. below shows bijection

$R \subset A \times B = \{(1, 3), (2, 4)\}$

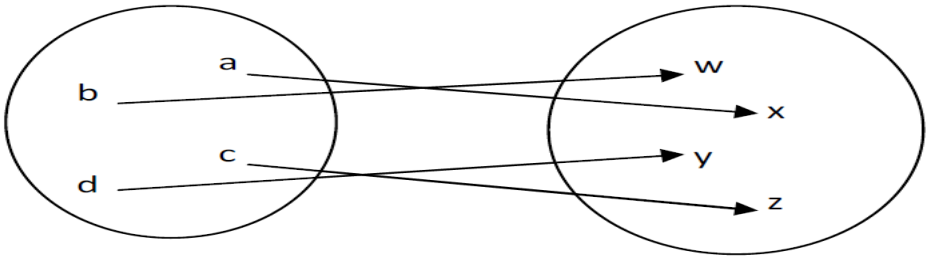


Fig: *Bijection*

1.2. Propositional Logic and Predicate Logic

Propositional Logic

Propositional logic (also called sentential logic) deals with statements that are either true or false. These statements are referred to as **propositions**, and in propositional logic, we work with **propositional variables** (such as p, q, etc.), which represent these statements.

Expressing Statements in Propositional Logic

In propositional logic, we use logical connectives to build more complex statements from simple propositions. Some common connectives are:R

1. **Negation** (¬): The negation of a proposition p is ¬p, which means "not p."
    - Example: If P represents "It is raining," then ¬p means "It is not raining."
2. **Conjunction** (∧): The conjunction of P and q is p∧q , meaning "both P and q are true."
    - `Example: "It is raining and it is cold."`
3. **Disjunction** (∨): The disjunction of P and q is p∨q, meaning "either P or q (or both) are true."
    - `Example: "It is raining or it is snowing."`
4. **Implication** (→): The implication p → q means "if P, then q" or " P implies q."
    - Example: "If it is raining, then the ground is wet."
5. **Biconditional** (↔): The biconditional p ↔ q means "P if and only if q."
    - `Example: "You are a student if and only if you attend school."`

Rules of Inference: Rules of inference allow us to derive conclusions from premises in a logically valid way. Some key rules include:

1. Modus Ponens:
   - If p → q (if P, then q) and P are both true, then we can conclude q.
   - Example: If it is raining, the ground will be wet. It is raining. Therefore, the ground is wet.
2. Modus Tollens:
   - If p → q and ¬q (not q) are both true, then we can conclude ¬p
   - Example: If it is raining, the ground will be wet. The ground is not wet. Therefore, it is not raining.
3. Disjunctive Syllogism:
   - If p∨q is true, and ¬p (not P) is true, then we can conclude q.
   - Example: Either it is raining or it is snowing. It is not raining. Therefore, it is snowing.
4. Conjunction:
   - If P and q are both true, then p∧q (both P and q) is true.
   - Example: It is raining and it is cold.
5. Simplification:
   - If p ∧ q is true, then we can conclude P or q is true.
   - Example: It is raining and it is cold. Therefore, it is raining.
6. Hypothetical Syllogism:
   - If p → q and q → r are both true, then p → r is true.
   - Example: If it is raining, the ground will be wet. If the ground is wet, we will need an umbrella. Therefore, if it is raining, we will need an umbrella.

Proofs in Propositional Logic

A proof in propositional logic is a sequence of steps that demonstrates the truth of a statement starting from axioms or previously proven statements. The goal is to show that the conclusion logically follows from the premises. In formal proofs, one applies the rules of inference to derive conclusions.

For example, to prove p → q from a set of premises, you would show, step by step, that assuming P leads to the conclusion q.

Introduction to Predicate Logic

Predicate logic extends propositional logic by dealing with predicates, which are functions that take objects from a domain and return a truth value (true or false). In predicate logic, we are not limited to entire propositions, but rather to statements involving variables.

1. **Predicates**: A predicate is a function that takes an object (or multiple objects) and returns a truth value. For example:
   - P(x): "x is a prime number."
   - Q(x,y): "x is greater than y."
2. **Quantifiers**: Predicate logic uses quantifiers to express the extent of a statement:
   - **Universal Quantifier** (∀): "For all" or "Every."
     Example: ∀xP(x) means "Every x is prime."
   - **Existential Quantifier** (∃): "There exists" or "For some."
     Example: ∃xP(x) means "There exists an x such that x is prime."
3. Predicates in Action:

- Example 1: ∀x(P(x)→Q(x)) could mean "For every x, if x is prime, then x is greater than 1."
- Example 2: ∃x(P(x)∧Q(x)) could mean "There exists an x such that x is prime and x is greater than 1."

Methods of proof Theorem:

- A **theorem** is a mathematical proposition that is true. Many theorems are conditional propositions.
- For example, if f(x) and g(x) are continuous then f(x)± g(x) are also continuous.
- If theorem is of the form "if p then q", the p is called hypothesis and q is called conclusion.

Proof :

A proof of a theorem is a logical argument that establishes the theorem to be true. There are different types of proofs of a theorem.

Some of them are given below:

- Direct proof
- Indirect proof
- Proof by contradiction
- Proof by cases
- Proof by mathematical induction
- Proof by counter examples

Direct Proofs:

To prove p→q, we start assuming hypothesis p is true and we use information already available to prove q is true, and if q is true then the argument is valid. This is called direct proof.

E.g. If a and b are odd integers, then a+b is an odd integers.

Here a and b are odd integers. Since every odd numbers can be written by 2l+1 where l is any integer.

So, a = 2m+1

b = 2n+1 for some integers m and n

Now, a+b = 2m+1+2n+1 = 2m+2n+2 = 2(m+n+1) = 2*k where k = m+n+1 is any integer. This shows a+b is even.

<u>Proof by contradiction</u>:

The following proof proceeds by contradiction. That is, we will assume that the claim we are trying to prove is wrong and reach a contradiction. If all the derivations along the way are correct, then the only thing that can be wrong is the assumption, which was that the claim we are trying to prove does not hold.

This proves that the claim does hold.

Eg: For all integers n, if n2 is odd, then n is odd.

Suppose not. [We take the negation of the given statement and suppose it to be true.]

Assume, to the contrary, that ∃ an integer n such that n2 is odd and n is even.

[We must deduce the contradiction.]

By definition of even,

we have n = 2k for some integer k.

So, by substitution we have

n. n = (2k). (2k) =2. (2.k.k)

Now (2.k.k) is an integer because products of integers are integer; and 2 and k are integers. Hence,

n. n = 2. (some integer)

or n2 = 2. (some integer)

and so by definition of n2 even, is even.

So the conclusion is since n is even, n2, which is the product of n with itself, is also even. This contradicts the supposition that n2 is odd.

[Hence, the supposition is false and the proposition is true.] Proof

4. Mathematical Principles: Detailed Explanation and Examples

1. Principle of Mathematical Induction

The Principle of Mathematical Induction is a method used to prove statements or formulas that involve positive integers. It works by showing a base case and then proving that if the statement is true for one integer, it must be true for the next.

To prove that the given statement for only one natural number implies the given statement for the next natural number.

If it is known that

- Some statement is true for n= n_0 (+ ve integer)
- Assumption that statement is true for n implies that statement is true for n+1 then that statement is true for all positive integer greater or equal to n_0

Steps in the Principle of Mathematical Induction:

1. **Denote the Statement**:
   The statement to be proven is denoted by P(n), where n is a positive integer.
2. **Base Case**:
   Prove that the statement is true for n=0 or n = 1 (or the smallest value of n). That is, verify that P(0) or P(1)is true.
3. **Inductive Hypothesis**:
   Assume P(k) is true for some arbitrary positive integer k. This is called the **inductive hypothesis**.
4. **Inductive Step**:
   Using the inductive hypothesis P(k), prove that P(k+1) is also true. This involves showing that the truth of P(k) implies the truth of P(k+1).
5. **Conclusion**:
   If both the base case and the inductive step are proven, it follows by the Principle of Mathematical Induction that P(n) is true for all n∈N (natural numbers).

If both the base case and inductive step hold, the statement is true for all n ≥ 1.

Example 1:

Prove by induction:

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Prove that the sum of the first n natural numbers is $S_n = \frac{n(n+1)}{2}$.

1. **Base Case**: For $n = 1$, $S_1 = \frac{1(1+1)}{2} = 1$, which is true.
2. **Inductive Hypothesis**: Assume $S_k = \frac{k(k+1)}{2}$.
3. **Inductive Step**: Show $S_{k+1} = S_k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$, which matches the formula.

Example 2: Sum of Squares Formula

Prove that the sum of the first n squares is:

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Step 1: Base Case (n = 1): Verify the formula holds for n = 1.

$$1^2 = \frac{1(1+1)(2\cdot 1+1)}{6} = \frac{1\cdot 2\cdot 3}{6} = 1.$$

The base case holds.

Step 2: Inductive Hypothesis: Assume the formula is true for n = k.

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Step 3: Inductive Step: Show it is true for n = k+1 using the hypothesis.

$$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2.$$

Simplify:

$$\frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)^2}{6} = \frac{(k+1)\big(k(2k+1)+6(k+1)\big)}{6}.$$

Expand and simplify to:

$$\frac{(k+1)(k+2)(2k+3)}{6}.$$

This matches the formula for $n = k+1$. Thus, the formula is true for all n.

Example 2: **Inequality Proof**

Prove $2^n > n^2$ for $n \geq 5$.

The proof involves:

1. Verifying the base case.
2. Assuming the inequality holds for n = k.
3. Showing it holds for n = k+1.

Base Case ($n = 5$):

$$2^5 = 32 > 25 = 5^2.$$

The base case holds.

Inductive Hypothesis: Assume $2^k > k^2$ for $k \geq 5$.

Inductive Step: Show $2^{k+1} > (k+1)^2$:

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot k^2.$$

By assumption, $2 \cdot k^2 > (k+1)^2$ for $k \geq 5$. Expanding $(k+1)^2$ gives:

$$2k^2 > k^2 + 2k + 1.$$

This simplifies to $k^2 > 2k + 1$, which is true for $k \geq 5$.

Thus, the inequality holds.

Example 3: Prove that **$n<2^n$** for all positive integers **n** using the **Principle of Mathematical Induction**.

Step 1: Denote the Statement: Let P(n) represent the statement:

$$n<2^n$$

We need to show that this inequality holds for all positive integers n.

Step 2: Base Case

For n=1:

$1<2^1$

1<2.

This is true, so the base case holds.

Step 3: Inductive Hypothesis

Assume P(k) is true for some k≥1. That is:

$k<2^k$.

Step 4: Inductive Step: We need to prove P(k+1), i.e.,

$k+1<2^{k+1}$

Left-Hand Side (LHS):

From the inductive hypothesis, $k < 2^k$.

Adding 1 to both sides:

$$k + 1 < 2^k + 1.$$

Right-Hand Side (RHS):

We know $2^{k+1} = 2 \cdot 2^k$.

Since $2^k + 1 \leq 2 \cdot 2^k$ for $k \geq 1$ (as $2^k > 1$), it follows that:

$$k + 1 < 2^{k+1}.$$

By the Principle of Mathematical Induction, $n<2^n$ is true for all positive integers n.

Question:

Use mathematical induction to show that

$$n^n \geq 2^n \tag{3.5.31}$$

for all integers $n \geq 2$.

Solution

Proceed by induction on n. When $n = 2$, the inequality becomes $2^2 \geq 2^2$, which is obviously true. Assume it holds when $n = k$ for some integer $k \geq 2$:

$$k^k \geq 2^k. \tag{3.5.32}$$

We want to show that it still holds when $n = k+1$:

$$(k+1)^{k+1} \geq 2^{k+1}. \tag{3.5.33}$$

Since $k \geq 2$, it follows from the inductive hypothesis that

$$(k+1)^{k+1} \geq k^{k+1} = k \cdot k^k \geq 2 \cdot 2^k = 2^{k+1}. \tag{3.5.34}$$

Therefore, the inequality still holds when $n = k+1$. This completes the induction.

Q. Prove that n(n+1)(2n+1) is a multiple of 6 for all integers n ≥ 1.

Solution

Proceed by induction on n. When $n=1$, we have $n(n+1)(2n+1)=1\cdot 2\cdot 3=6$, which is clearly a multiple of 6. Hence, the claim is true when $n=1$. Assume the claim is true when $n=k$ for some integer $k\geq 1$; that is, assume that we can write

$$k(k+1)(2k+1)=6q \tag{3.5.4}$$

for some integer q. We want to show that the claim is still true when $n=k+1$; that is, we want to show that

$$(k+1)(k+2)[2(k+1)+1]=(k+1)(k+2)(2k+3)=6Q \tag{3.5.5}$$

for some integer Q. Using the inductive hypothesis, we find

$$\begin{aligned}(k+1)(k+2)(2k+3) &= (k+1)(2k^2+7k+6)\\ &= (k+1)[(2k^2+k)+(6k+6)]\\ &= (k+1)[k(2k+1)+6(k+1)]\\ &= k(k+1)(2k+1)+6(k+1)^2\\ &= 6q+6(k+1)^2\\ &= 6\,[q+(k+1)^2],\end{aligned}$$

where $q+(k+1)^2$ is clearly an integer. This completes the induction.

Q1. Show that 2^{2n}-1 is divisible by 3 using the principles of mathematical induction.

To prove: Assume that the given statement be P(n)

2^{2n}-1 is divisible by 3

Step 1 Base Case:

For n= 1, the given statement can be written as

P (1) = $2^{2(1)}$-1 = 4-1 = 3. So 3 is divisible by 3. (i.e.3/3 = 1)

Step 2 Inductive Hypothesis:

Let us assume that P(n) is true for all the natural numbers n=k, so the statement can be written as

P(k) = 2^k-1 is divisible by 3, for every natural number

It means that 2^{2k}-1 = 3a (where **a** belongs to natural number)

Step 3 Inductive Step: Now, we need to prove the statement is true for n= k+1 by using above **Hypothesis**

Hence,

P(k+1) = $2^{2(k+1)}$-1

= 2^{2k+2}-1

= 2^{2k}. 2^2 – 1

= (2^{2k}. 4)-1

= {(3+1) 2^{2k} } - 1

=3.2^{2k} +(2^{2k}-1)

The above expression can be written as

P(k+1) =3.2^{2k} + 3a

Now, take 3 outside, we get

P(k+1) = 3(2^{2k} + a) = 3b, where “b” belongs to natural number

It is proved that p(k+1) holds true, whenever the statement P(k) is true.

Thus, 2^{2n}-1 is divisible by 3 is proved using the principles of mathematical induction

Q.Show that 11^{n+2} + 12^{2n+1} is divisible by 133 **for any integer n**.

Let P (n) = 11^{n+2} + 12^{2n+1}

Step 1: Base Case:

For n = 1,

P (1) = 11^3+12^3=3059=133 x 23

So, 133 divide P (1) . so base case holds true.

Step 2: **Inductive Hypothesis:**

Let us assume that P(n) is true for all the natural numbers n=k,
so the statement can be written as

$P(k) = 11^{k+2}+12^{2k+1}=133 \times s$ ..... (ii)

Step 3: **Inductive Steps:**

For n = k + 1,

$P(k+1) = 11^{k+2+1}+12^{2(k)+3}$

$=11[133s-12^{2k+1}] + 144.\ 12^{2k+1}$

$= 11 \times 133s + 12^{2k+1}.133$

$=133[11s+12^{2k+1}]$

$=133 \times t$..... (iii)

As (i), (ii), and (iii) all are true, hence P (n) is divisible by 133.

Q 2: Show that $1 + 3 + 5 + \ldots + (2n-1) = n^2$

Solution:

Step 1: Result is true for n = 1

That is $1 = (1)^2$ (True)

Step 2: Assume that result is true for n = k

$1 + 3 + 5 + \ldots + (2k-1) = k^2$

Step 3: Check for n = k + 1

i.e. $1 + 3 + 5 + \ldots + (2(k+1) -1) = (k+1)^2$

We can write the above equation as,

$1 + 3 + 5 + \ldots + (2k-1) + (2(k+1) -1) = (k+1)^2$

Using step 2 result, we get

$k^2 + (2(k+1) -1) = (k+1)^2$

$k^2 + 2k + 2 -1 = (k+1)^2$

$k^2 + 2k + 1 = (k+1)^2$

$(k+1)^2 = (k+1)^2$

L.H.S. and R.H.S. are same.

So the result is true for n = k+1

By mathematical induction, the statement is true.

We see that the given statement is also true for n=k+1. Hence we can say that by the principle of mathematical induction this statement is valid for all natural numbers n.

Q. Prove using mathematical induction, $n^4 - 4n^2$ is divisible by 3 for n>=0.

Solution:

Basic step:

For n=0, $n^4 - 4n^2 = 0$, which is divisible by 3.

Induction hypothesis: Let $n^4 - 4n^2$ is divisible by 3.

Induction step:

$$(n+1)^4 - 4(n+1)^2$$
$$= [(n+1)^2]^2 - 4(n+1)^2$$
$$= (n^2 + 2n + 1)^2 - (2n+2)^2$$
$$= (n^2 + 2n + 1 + 2n + 2)\ (n^2 + 2n + 1 - 2n - 2)$$
$$= (n^2 + 4n + 3)\ (n^2 - 1)$$
$$= n^4 + 4n^3 + 3n^2 - 3 - 4n - n^2$$
$$= n^4 + 4n^3 + 2n^2 - 4n - 3$$
$$= n^4 + 4n^3 - 4n^2 + 6n^2 - 4n - 3$$
$$= n - 4n^2 + 6n^2 - 3 + 4n^3 - 4n$$

$= (n^2 - 4n^2) + (6n^2) - (3) + 4(n^3 - n)$

$(n^2 - 4n^2)$ is divisible by 3 from our hypothesis. $6n^2$, 3 are divisible by 3.

We need to prove that $4(n^3 - n)$ is divisible by 3. Again use mathematical induction.

Basic step:

For n = 0,

4(0-0) = 0 is divisible by 3.

Induction hypothesis:

Let $4(n^3 - n)$ is divisible by 3.

Induction step:

$4[(n + 1)^3 - (n + 1)]$

$= 4[(n^3 + 3n^2 + 3n + 1) - (n + 1)]$

$= 4[n^3 + 3n^2 + 3n + 1 - n - 1]$

$= 4[n^3 + 3n^2 + 2n]$

$= 4[n^3 - n + 3n^2 + 3n]$

$= 4(n^3 - n) + 4.3n^2 + 4.3n$

$4(n^3 - n)$ is divisible by 3 from our hypothesis. $4.3n^2$ is divisible by 3.

$4.3n$ is divisible by 3.

Thus we can say that

$= (n^2 - 4n^2) + (6n^2) - (3) + 4(n^3 - n)$ is divisible by 3. That is,

$n^4 - 4n^2$ is divisible by 3

2. Diagonalization Principle

The Diagonalization Principle is a technique used to prove uncountability or contradictions. It is famously associated with Cantor's proof (**Cantor's Diagonal Argument**.) that the real numbers are uncountable.
Its principle are as follows:

I. Assume condition for contradiction
II. Find the reversed diagonal and check whether it is different form each row in table or not.
III. If it is different from each row in the table, it contradicts the assumed condition providing the theorem.

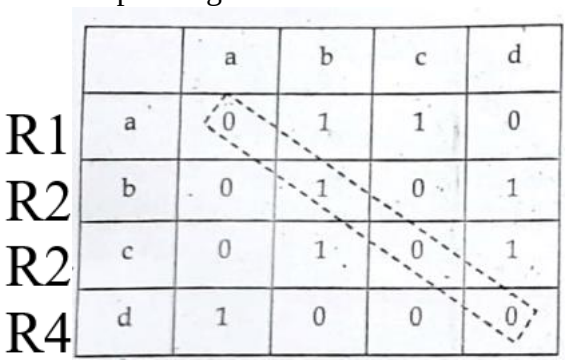
Explanation: Let R be a binary relation defined on Set A and D be a Diagonal set defined on relation R as

{a : a ∈ A and (a, a) ∉ R}

Let A be a finite Set A = {a, b, c, d} and R be a binary relation on set A such that

R= {(a, b), (a, c), (b, b),(b, d),(c, b),(c, d),(d, a)}

Now, we can represent R in a square table, rows and columns representing the elements and cell having 1s if there is a link between the corresponding elements.



The diagonal element is

D= | 0 | 1 | 0 | 0 | ={0,1,0,0}={b}

And taking the complement of diagonal (replacing 1s with 0s and vice-versa) i.e

$\overline{D}$ = | 1 | 0 | 1 | 1 | ={1,0,1,1}={a,c,d}

Also, its Row sets are

R1={b,c},
R2={b,d},
R2={b,d},
R4={a},

And you can see that it is diagonal set complement different from each row. And if the reversed diagonal element is different from each row, it contradicts assumptions with what table is made up to and in the way, the theorem can be proved.

Example 1: Uncountability of Real Numbers

Cantor's proof constructs a number not on any presumed list of real numbers, proving that the real numbers cannot be enumerated.

Prove that $[0, 1]$ is uncountable.

1. Assume the real numbers in $[0, 1]$ can be listed as $x_1, x_2, x_3, \ldots$, where each x_i has a decimal expansion (e.g., $x_1 = 0.a_{11}a_{12}a_{13}\ldots$).
2. Construct a number $y = 0.b_1b_2b_3\ldots$, where:

$$b_i = \begin{cases} 1 & \text{if } a_{ii} \neq 1, \\ 2 & \text{if } a_{ii} = 1. \end{cases}$$

3. The number y differs from every x_i in the i-th digit. Therefore, y is not in the list.
4. Contradiction: The list cannot contain all real numbers in $[0, 1]$, proving it is uncountable.

Example 2: Noncomputability of the Halting Problem

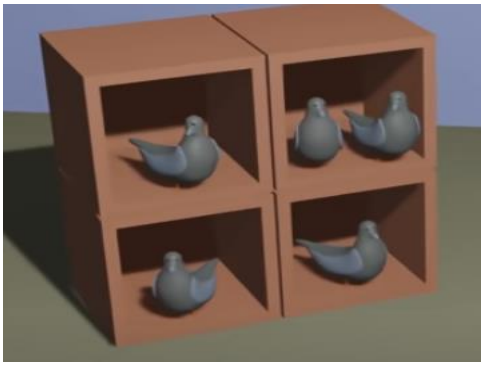
The Halting Problem uses diagonalization to show that no algorithm can decide whether an arbitrary program halts. This creates a paradox when such an algorithm is assumed.

1. Suppose such an algorithm H exists, taking input (P, I) (program P and input I) and outputting:
   - "Yes" if $P(I)$ halts.
   - "No" if $P(I)$ does not halt.
2. Construct a program $D(x)$ that calls $H(x, x)$ and:
   - Halts if $H(x, x) = \text{No}$,
   - Loops indefinitely if $H(x, x) = \text{Yes}$.
3. What happens when D is given its own code as input? This creates a paradox, showing H cannot exist.

3. Pigeonhole Principle: If A and B are non-empty finite sets and |A|>|B| then there is no one-to-one function from A to B.

It states that if *n+**1*** or more objects are placed into *n* containers, at least one container must contain more than one object.

i.e Let n →Pigeons and m→Pigeonholes with n>m then at least one Pigeonholes must contain more than one Pigeons in it.



Example:

If 10 people each have an integer between 1 and 9 as their favorite number, at least two people share the same favorite number (since there are only 9 numbers but 10 people).

Example 1: Sock Drawer

If you have 10 pairs of socks (20 socks total) in two colors, picking 11 socks ensures at least 6 are of the same color (by dividing 11 socks among 2 colors).

1. **Why?** There are 2 colors (pigeonholes) and 11 socks (pigeons).
2. Dividing 11 socks among 2 colors:

$$\lceil 11/2 \rceil = 6.$$

Example 2: Divisibility

In any set of n+1 integers, there exist two numbers whose difference is divisible by n. This is proven using remainders (modulo n) and the Pigeonhole Principle.

Prove that in any set of $n+1$ integers, there exist two numbers whose difference is divisible by n.

1. Consider $n+1$ integers $a_1, a_2, \ldots, a_{n+1}$.
2. Look at their remainders when divided by n: $r_1, r_2, \ldots, r_{n+1}$.
3. Since there are n possible remainders (0 to $n-1$), at least two integers must have the same remainder.
4. If $a_i \equiv a_j \pmod{n}$, then $a_i - a_j$ is divisible by n.

Alphabet and Language in Theory of Computation

Introduction

In the Theory of Computation, alphabet and language are fundamental concepts that form the basis for studying formal systems and automata. This document provides a detailed overview, examples, and applications of these concepts.

1. Alphabet (Σ)

An alphabet is a finite, non-empty set of symbols. These symbols are the building blocks for creating strings and languages.

Examples:

- Binary alphabet: Σ = {0, 1}
- Alphabet for English letters: Σ = {a, b, c, ..., z}
- Alphabet for DNA sequences: Σ = {A, T, G, C}

2. Language (L)

A language is a set of strings over a given alphabet. Formally, if Σ is an alphabet, then a language L is a subset of Σ*, where:

- Σ* is the set of all possible strings (of any finite length, including the empty string) over Σ.
- **Є**: The **empty string**, which has no symbols.

Examples:

- L = {0, 1, 11, 101}, a finite language over Σ = {0, 1}.
- L = {w ∈ {a, b}* : w starts with a}, an infinite language over Σ = {a, b}.
- The set of valid arithmetic expressions over an alphabet of digits and operators.

Types of Languages:

1. **Regular Languages**: Described using regular expressions or recognized by finite automata.
2. **Context-Free Languages:** Generated by context-free grammars and recognized by pushdown automata.
3. **Recursive Languages:** Recognized by Turing machines that halt on all inputs.
4. **Recursively Enumerable Languages:** Recognized by Turing machines but may not halt for all inputs.

Operations on Languages:

Languages can be manipulated using various operations:

- Union: $L_1 \cup L_2$ (all strings in L_1 or L_2).
- Concatenation: $L_1 \cdot L_2$ (strings formed by concatenating strings from L_1 with strings from L_2).
- Kleene Star: $L^* = \{\epsilon, w_1, w_2, w_1w_2, \dots\}$, where $w_i \in L$.

Relation Between Alphabet and Language:

1. The **alphabet** defines the "building blocks" or symbols.
2. A **language** defines specific patterns or sets of strings constructed using these symbols.
3. Together, they form the foundation for analyzing computational systems, automata, and grammars in theoretical computer science.

3. Examples of Alphabets and Languages

Example 1: Binary Alphabet

- Alphabet: Σ = {0, 1}
- Language
  - L_1= {w ∈ Σ*: w has an even number of 0s}.
    Example strings: ϵ,11, 1010, 0000 ,…..
  - L_2= {w ∈ Σ*: w starts with 1 and ends with 0}.
    Example strings: 10, 110, 1010, ….

Example 2: DNA Alphabet

- Alphabet: $\Sigma = \{A, T, G, C\}$
- Languages:
  - $L_1 = \{w \in \Sigma^* : w \text{ contains } ATG \text{ as a substring}\}$
    - Example strings: $ATG, ATGCC, CCATG$
  - $L_2 = \{w \in \Sigma^* : |w| \text{ is divisible by } 3\}$
    - Example strings: $ATG, ATGATG, TTTGGG$

4. Applications of Alphabets and Languages

1. Design of Compilers and Parsers:

- **Alphabet**: Programming language tokens (e.g., keywords, identifiers, symbols).
  - Example: For C++, $\Sigma = \{if, else, +, -, \{, \}, ;, a - z\}$.
- **Language**: The set of all syntactically valid programs in the language.
  - Defined using **context-free grammars (CFGs)**.

2. Regular Expressions in Text Processing:

- Regular expressions define patterns in languages.
  - Example: The regex $(a|b)^*c$ represents the language $L = \{w \in \{a, b, c\}^* : w \text{ ends with } c\}$.
  - Applications: Searching for patterns in text files, log analysis, and data validation.

3. Finite Automata in String Matching:

Example:

- Input alphabet: $\Sigma = \{a, b\}$.
- DFA/NFA: Recognizes a language like $L = \{w : w \text{ starts with } a \text{ and contains } b \text{ at least once}\}$.
- Application: Efficient pattern matching algorithms (e.g., in spam filters or search engines).

4. Cryptography

- Languages of encrypted messages use alphabets like Σ= {0,1} or alphanumeric symbols.
- Language constraints ensure security, like avoiding patterns that can simplify decryption.

5. Natural Language Processing (NLP)

- Alphabets: Characters, phonemes, or words (e.g., Σ={a,b,…,z,space}).
- Languages: Grammatically correct sentences (defined by formal grammars).

6. Formal Verification

- Verifying systems by modeling their behaviors as languages.
- Example: A system's behavior can be modeled as a language over Σ={request,grant,release}.
- Checking properties like deadlock-freedom involves examining these languages.

1.5. Operations on Languages: Union, Concatenation, and Kleene Star

In formal language theory, operations on languages are essential for constructing new languages from existing ones.

Three fundamental operations:

1. Union,
2. Concatenation,
3. and Kleene Star.

1. Union of Languages

Definition: The union of two languages L_1 and L_2, denoted by $L_1 \cup L_2$, is the set of strings that belong to either L_1 or L_2 or both.

$L_1 \cup L_2 = \{w \mid w \in L_1 \text{ or } w \in L_2\}$

Example:

- Let $L_1 = \{a, b\}$ and $L_2 = \{b, c\}$.

  $L_1 \cup L_2 = \{a, b, c\}$.

2. Concatenation of Languages

Definition: The concatenation of two languages L_1 and L_2, denoted by $L_1 \cdot L_2$ or L_1L_2, is the set of all strings formed by taking a string from L_1 followed by a string from L_2.

$$L_1 \cdot L_2 = \{w_1w_2 \mid w_1 \in L_1, w_2 \in L_2\}$$

Example:

- Let $L_1 = \{a, b\}$ and $L_2 = \{c, d\}$.
- $L_1 \cdot L_2 = \{ac, ad, bc, bd\}$.

3. Kleene Star

Definition: The Kleene star of a language L, denoted by L*, is the set of all strings that can be formed by concatenating zero or more strings from L, including the empty string ε.

$$L^* = \bigcup_{i=0}^{\infty} L^i$$

- Here, $L^0 = \{\epsilon\}$, and $L^i = L \cdot L^{i-1}$ for $i \geq 1$.

Example:

- Let $L = \{a, b\}$.
- $L^* = \{\epsilon, a, b, aa, ab, ba, bb, aaa, \ldots\}$.

Summary of Key Properties

1. Union is commutative and associative:

   $L_1 \cup L_2 = L_2 \cup L_1$,

   $(L_1 \cup L_2) \cup L_3 = L_1 \cup (L_2 \cup L_3)$

2. Concatenation is associative but not commutative:

   $(L_1 \cdot L_2) \cdot L_3 = L_1 \cdot (L_2 \cdot L_3)$

3. Kleene Star properties:

- L* always contains ε.
- L* · L* = L*.
- If L is finite, L* is generally infinite unless L = {ε}.