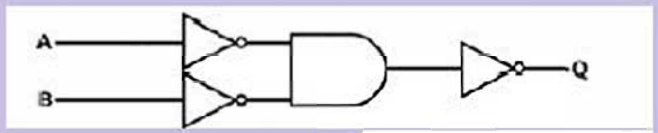
DISCRETE & INTERACTIVE

MATHEMATICS

ϕ	$\neg\phi$
T	F
F	T

$$1+0=1$$
$$1+1=1$$
$$1.1=1$$



$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ . & . & . & . \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}^T = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ . & . & . & . \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}$$

PRODUCED BY

ASS. PROF. TAREK EZZAT NASSAR

DR. Mohamed Abozeid

Contents

Introduction

Discrete mathematics is a branch of mathematics that deals with mathematical structures and objects that are fundamentally discrete or distinct in nature. Unlike continuous mathematics, which focuses on concepts such as real numbers and continuous functions, discrete mathematics focuses on countable and finite sets, integers, graphs, and logical statements.

One of the fundamental concepts in discrete mathematics is set theory, which provides the foundation for many other areas. Sets are collections of distinct elements and are used to represent various mathematical objects. Operations such as union, intersection, and complementation are defined on sets.

Logic is also a fundamental component of discrete mathematics. It deals with the rules of reasoning and inference. Propositional logic focuses on the study of logical statements and their truth values, while predicate logic extends this to include quantifiers and predicates. Logic plays a crucial role in computer science, artificial intelligence, and mathematics itself.

Another important area of discrete mathematics is combinatorics, which studies counting, arrangement, and combination of objects. Combinatorics deals with topics such as permutations, combinations, and the binomial coefficient. It has applications in various fields, including computer science, cryptography, and probability theory.

Graph theory is another key topic in discrete mathematics. It studies the properties and relationships of graphs, which consist of vertices (nodes) and edges (connections between vertices). Graph theory is widely used in computer science, network analysis, and optimization problems.

Discrete mathematics finds applications in various fields, including computer science, cryptography, operations research, and information theory. It provides the theoretical foundation for many computational algorithms, data structures, and optimization techniques. Overall, discrete mathematics is concerned with the study of discrete structures and provides a powerful toolkit for solving problems in various domains by employing rigorous mathematical reasoning and logical thinking.

Chapter One

Sets, Functions, Relations, and Logic

1.1. Set

Set is one of the basic building blocks for the types of objects considered in discrete mathematics. It's a basis for Mathematics pretty much all Mathematics can be formalized in Set Theory. Why is Set Theory important for Computer Science? It's a useful tool for formalizing and reasoning about computation and the objects of computation. The concept of a set is so fundamental that we will not attempt to give it a precise definition. A set is a completely characterized by the elements it contains.

There are two main ways of defining a set:

(1) By explicitly listing all its elements as:

$A = \{a, i, e, o, u\}$ Set of all vowels in the English alphabet.

(2) By giving a property that all elements must satisfy as:

$E = \{n \in N \mid n \text{ divides } 2\}$ set of natural numbers given by specifying a property.

In some cases both methods can be used to define the same set, as in this example

$$\{ n \in N \mid n \text{ is odd } \wedge \ n^2 + n \leq 100\} = \{1, 3, 5, 7, 9\}$$

Some Important Sets

N=natural numbers = {0, 1, 2, 3, …}.

Z=integers numbers = {…, 3, 2, 1, 0, 1, 2, 3, …}.

Z^+= positive integers numbers = {1, 2, 3, …}.

R=set of real numbers.

To say that a certain object x is an element of a set S, we write $x \in S$. To say that it isn't an element of S we write $x \notin S$. If every element of a set X is also an element of another set Y, then we say that X is a subset of Y and we write this symbolically as: $X \subseteq Y$.

Formally, the subset relation is defined as follows:

$$X \subseteq Y \quad \Leftrightarrow \quad \text{for every } x \in X \Rightarrow x \in Y.$$

As example, here's a couple of subsets of the sets A and E from above:

$$\{a, i\} \subseteq A$$

$$\{x \in N \mid n \text{ is a multiple of } 4\} \subseteq E$$

There is a set that is contained in any other set: the empty set, that is, the set with no elements. We use the symbol ∅ for it:

$$\emptyset = \{\ \}.$$

It is always trivially true that $\emptyset \subset X$ and also that $X \subseteq X$.

Example 1

The set of all real roots of the equation $x^2 - 2x - 3 = 0$ is denoted by

$\{x: x \text{ is a real number } \& \ x^2 - 2x - 3 = 0\}$ or $\{-1, 3\}$

Sometimes we shall define a set merely by listing its elements within braces:

$\{a, b, c, ..., h\}$. In particular, $\{b\}$ is the set having b as its only member.

Such a set $\{b\}$ is called a singleton.

The set $\{b, c\}$ contains b and c as its only members, and,

if $b \neq c$, then $\{b, c\}$ is called an unordered pair. Notice that $\{b, c\} = \{c, b\}$.

Example 2

The set of all real roots of the equation $x^2 - 3 = 0$ is equal to the set $\{\sqrt{3}, -\sqrt{3}\}$.

We shall extend this method of denoting sets by listing a few elements of the set, followed by dots, in such a way as to indicate the characteristic property of the elements of the set.

Example 3

Let $\{1, 2, 3, 4, ...\}$ is intended to represent the set of positive integers Z. $\{1, 4, 9, 16, 25, ..., n^2, ...\}$ is the set of squares of positive integers. When, we define a set by a property, we

should also clarify in advance what kind of objects we are talking about: in the examples above, we wrote n ∈ N to specify that we are talking about natural numbers. This larger set, containing all the objects that we are interested in, is called the universal set or just the universe. We will be using the letter U to denote the universal set. Sets can be combined and manipulated by using the operations of intersection, union, difference, complement.

1.1.1. Set Equality

Definition: 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

$$\forall\, x(x \in A \leftrightarrow x \in B)$$

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

$$\{1, 3, 5\} = \{3, 5, 1\}.$$

Here are their intuitive meaning and their rigorous mathematical definitions, assuming that S and T are any two sets:

- **Intersection** S ∩ T: the elements that belong both to S and to T.

$$S \cap T = \{x \in U \mid x \in S \wedge x \in T\}$$

- **Union** S ∪ T: the elements that belong either to S or to T (or both).

$$S \cup T = \{x \in U \mid x \in S \vee x \in T\}$$

- **Difference** S-T: the elements that belong to S but not to T.

$$S - T = \{x \in U \mid x \in S \wedge x \notin T\}$$

- **Complement** $\bar{S}$: elements (of the universe) that don't belong to S.

$$\bar{S} = \{x \in U \mid x \notin S\}$$

- **Equality** S=T: The sets S and T are equal when and only when S and T have the same members. {Equality of S and T is designated in the usual way by S = T, and denial of this equality by $S \subseteq T$}

Example 4

Let **a)** {1, 2, 3} ∪ {1, 3, 4, 6} = {1, 2, 3, 4, 6}

b) {a) ∪ {b} = {a, b}

c) {0, 2, 4, 6, 8, ... } ∪ {1, 3, 5, 7, 9, ...} = {0,1, 2, 3, 4, 5, ...}

d) {1, 2, 3} ∩ {1, 3, 4, 6} = {1, 3}

e) {0, 1, 4, 7, 8} - {1, 3, 5, 7, 9} = {0, 4, 8}

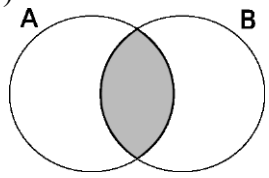
f) {1, 3, 5} ∩ {2, 4, 6} = Φ

h) $\overline{\{0,\ 2,\ 4,\ 6,\ 8,\ ...\}} = \{1, 3, 5, 7, 9, ...\}$

1.1.1. Venn Diagrams

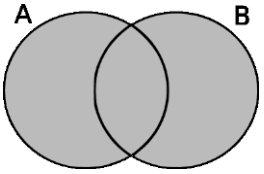
We can represent arbitrary sets pictorially by some drawings called Venn diagrams. Sets are blobs that overlap each other. Any region of the drawing can be characterized by some expression obtained by combining the sets by set operations

1)



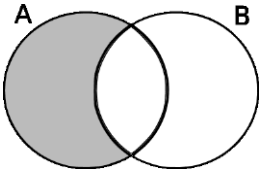
The shaded area represents $A \cap B$

2)



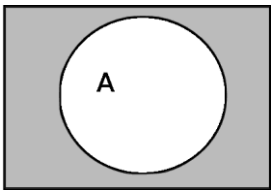
The shaded area represents $A \cup B$

3)



The shaded area represents $A - B$

4)



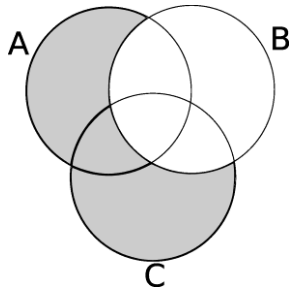
The shaded area represents $\bar{A}$

Venn diagram associated to an expression. Given any expression combining variable names for sets using the

operators of intersection, union, difference and complement, we can draw a Venn diagram and identify on it the area associated with the given expression. For example, here is a Venn diagram with a shaded area associated to the expression

5)

(A∪C)-B



1.1.2. Subsets

Definition: The set A is a subset of B, if and only if every element of A is also an element of B.

The notation $A \subset B$ is used to indicate that A is a subset of the set B.

$A \subset B$ holds if $\forall x(x \in A \rightarrow x \in B)$ is true.

The subset relation, $\subset$, is a partial order relation on sets, that is, it satisfies the properties of reflexivity, antisymmetry and transitivity:

- Reflexivity: $X \subset X$
- Antisymmetry: $(X \subset Y) \wedge (Y \subset X) \Rightarrow X = Y$
- Transitivity: $(X \subset Y) \wedge (Y \subset Z) \Rightarrow X \subset Z$

It is clearly not total: given two sets, it is not necessary that one of the two is contained in the other one. A set can contain other sets, like a box containing smaller boxes.

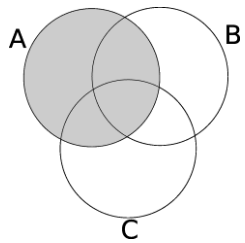
1.1.3. The algebra of sets

The expressions obtained by combining sets by set operations form a kind of algebra. To check what equalities hold in this algebra, we can use **V**enn diagrams. Remember, however, that the diagrams are only intuitive drawings and they are not considered a proper proof.

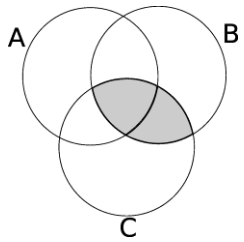
For example, we want to check if the following equality is true for all possible sets A, B and C:

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

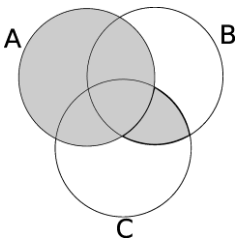
In other words: does union distribute over intersection?
Let's construct two Venn diagrams depicting the left-hand and right-hand side of this equality, respectively:



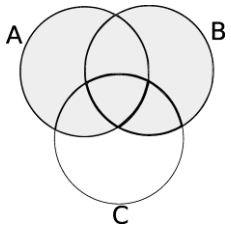
shaded area: A



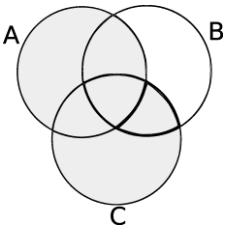
shaded area: B ∩ C



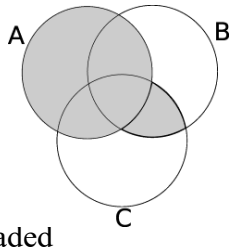
shaded area: A ∪ (B ∩ C)



shaded area: A ∪ B



shaded area: A ∪ C



shaded area: (A∪ B) ∩ (A∪ C)

We obtained the same area in the two diagrams for the two sides of the equality. This tells us that the equality is probably true.

This was not a proper proof: Venn diagrams are only an intuitive way to picture sets, they do not actually correspond to the real sets. If we want to be mathematically sure of the equality, we must prove it rigorously from the definitions.

Proof.

Let's unfold the definitions to check what it means to be an element of those two sets. For every element $x \in U$ we have that:

$$x \in A \cup (B \cap C) \Leftrightarrow (x \in A) \vee (x \in B \cap C)$$

$$\Leftrightarrow (x \in A) \vee ((x \in B) \wedge (x \in C));$$

$$x \in (A \cup B) \cap (A \cup C) \Leftrightarrow (x \in A \cup B) \wedge (x \in A \cup C)$$

$$\Leftrightarrow ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C)).$$

But now, by distributive of disjunction over conjunction, we have that:

$(x \in A) \vee ((x \in B) \wedge (x \in C)) \Leftrightarrow ((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C))$.

If you're not convinced of this step, go back to the rules of Boolean algebra. Check the rule of distributive of disjunction over conjunction and make the following substitutions: replace A by $(x \in A)$, replace B by $(x \in B)$ and replace C by $(x \in C)$. You will obtain exactly the equivalence above.

If we put all the equivalences together, we obtain:

$$x \in A \cup (B \cap C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C).$$

This states that being an element of $A \cup (B \cap C)$ is equivalent to being an element of $(A \cup B) \cap (A \cup C)$.

In conclusion: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Example 5

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

Let $A \subset (A \cup B)$ then $A \cap A = A$

: hence $A \cap (A \cup B) = A$.

Example 6

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

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

Notice that we exploited the Boolean law of distributive of disjunction over conjunction to prove distributive of union over intersection. This works because intersection was defined using conjunction and union was defined using disjunction. It is a general pattern: all the rules of Boolean algebra give corresponding rules of set algebra. Complement corresponds to negation. So if you take a Boolean equality, replace

Sign $\wedge$ **by** $\cap$, and sign $\vee$ **by** $\cup$ and sing $\neg$ by $\bar{\cdot}$, you obtain a set equality.

For example, the first **De Morgan law** becomes:

$$\overline{A \cap B} = \overline{A} \cup \overline{B}.$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}.$$

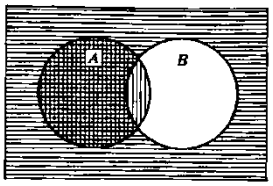
Try to prove this equality formally, like we did above for distributive.

Example 7

Show that $A \subseteq B$ if and only if $A \cap \overline{B} = \Phi$.

The cross hatched area is $A \cap \overline{B}$.

To say that this is Φ is equivalent to saying that A is entirely within B.



$A = A \cap U = A \cap (B \cup \overline{B}) = (A \cap B) \cup (A \cap \overline{B})$

Hence if $(A \cap \overline{B}) = \Phi$ then $A = A \cap B$; therefore,

By using: $A \cap B = A$ if and only if $A \subseteq B$, and therefore

$A \cap \overline{B} = (A \cap B) \cap \overline{B} = A \cap (B \cap \overline{B}) = A \cap (\Phi) = \Phi$

Example 8

Simplify $\overline{A \cap \overline{B}} \cup (B \cap C)$

$$\overline{A \cap \overline{B}} \cup (B \cap C) = (\overline{A} \cup B) \cup (B \cap C)$$

$$= \overline{A} \cup (B \cup (B \cap C)) = \overline{A} \cup B$$

1.1.4. Cartesian Product

Another important binary operation on sets is the Cartesian Product: given two sets A and B, their Cartesian product, indicated by $A \times B$ is the set of pair of elements from them. If $a \in A$ and $b \in B$, then we indicate by $\langle a,b \rangle$ the pair that they form. So we have:

$$A \times B = \{\langle a,b \rangle$$

$| a \in A \wedge b \in B\}$.

The order of the pair is important: the same two elements may form two different pairs in inverse orders.

For example, take the two sets to be:

$$A = \{\text{apple, banana, cherry}\},$$

$$B = \{\text{peach, banana, apple, strawberry}\}.$$

Then, both $\langle apple, banana \rangle$ and $\langle banana, apple \rangle$ are elements of $A \times B$ and they are considered different

$$\langle apple, banana \rangle \neq \langle banana, apple \rangle$$

Notice, in passing, that a pair like $\langle peach, cherry \rangle$ is not an element of the Cartesian product, because peach is not an element of A and also because cherry is not an element of B

$$\langle peach, cherry \rangle \notin A \times B.$$

On the other hand, the order of the elements is not important when we give a set by enumerating its elements. In that case

we are only interested in what elements are in the set, not the way they are listed:

{apple, banana} = {banana, apple},

{peach, banana, apple, strawberry} = {strawberry, peach, apple, banana}.

Example 9

If A = {1, 2} and B = {2, 3, 4}, then

A × B = {(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)}

Notice that Cartesian product is in general not commutative. In the case of the

above example, we have:

B × A = {(2, 1), (2, 2), (3, 1), (3, 2), (4, 1), (4, 2)}

So, for instance, we have (1, 2) ∈ A × B and (1, 2) ∉ B × A.

Example 10

What is A × B × C where A = {0, 1}, B= {1,2} and C= {0, 1, 2}

Solution: A× B × C={(0,1,0), (0,1,1), (0,1,2), (0,2,0),(0,2,1), (0,2,2), (1,1,0), (1,1,1), (1,1,2), (1,2,0), (1,2,1), (1,2,2)}.

1.1.5. Power Sets

Definition: The set of all subsets of a set A, denoted P(A) is called the power set of A.

Example 11

1) A= {a, b} then P(A)={ø,{a},{b},{a, b}}
2) *B*={apple, banana, cherry} then
   P (*B*) =∅, {apple}, {banana}, {cherry}, {apple, banana},
   {apple, cherry}, {banana, cherry},{apple, banana, cherry}

1.1.6. Set Cardinality

Definition: If there are exactly n distinct elements in S where n is a nonnegative integer, we say that S is finite. Otherwise it is infinite.

Definition: The cardinality of a finite set A, denoted by |A|, is the number of distinct elements of A.

Example 12

1) A = {a, i, e, o, u}, then |A|= 5

2) B={

1, 2,

3}

then

|B|= 3

3) Φ ,

then |

Φ|= 0

Exercises
1.1

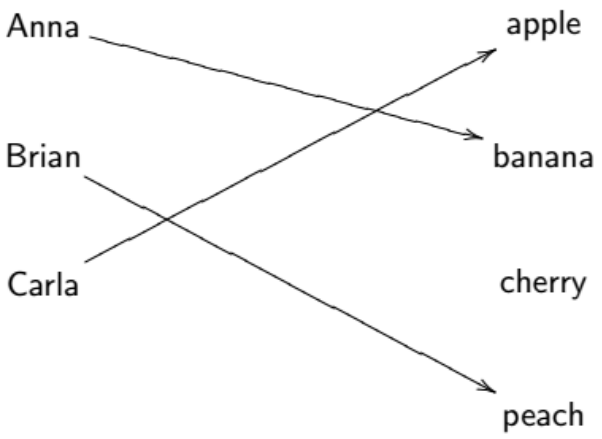
1) List all subsets of the set {1, 2,

3, 4}.

2) Prove that if $A \subseteq B$ and $B \subseteq C$,
   then $A \subseteq C$.
3) Let $A = \{x \in R \mid (x > 0) \wedge (x^2 = 3)\}$ Give a simpler definition of the set A.
4) Draw a Venn diagram to illustrate the fact $A \cup B \subseteq C$.
5) Prove the following statements:
   i) $A \cap \emptyset = \emptyset$ ii) $A \cup \emptyset = A$ *iii)* $A \cap A = A \cup A = A$
6) Prove the following:
   i) $A \subseteq B$ iff $A \cup B = B$. ii) $A \subseteq B$ iff $A \cap B = A$.
7) Prove the following:
   i) $A - \emptyset = A$. ii) $\emptyset - A = \emptyset$. iii) $A - B = A \cap \overline{B}$.
8) Let $A = \{1, 3, 5\}$, $B = \{2, 4\}$. Find $A \times A$, $B \times B$, $A \times B$, $B \times A$.
9) Use the set $A=\{1, 2, 3, 4\}$to find
   a) Power of A b) |A|

1.2. Functions

A function between two sets is a rule or a correspondence that associates to every element of the first set a unique element of the second set. For example, consider a correspondence between a set of three people and a set of fruit; it's a function that associates to every person her/his favorite fruit:



This defines a function; let's call it favorite, between two sets. We use the following notation to denote this fact:

favourite: {Anna, Brian, Carla} → {apple, banana, cherry, peach}

favourite (Anna) = banana

favourite (Brian) = peach

favourite(Carla) = apple

The set from which the function starts is called its *domain*; the one where it arrives is called its *codomain*.

When the domain is finite, as in the example above, we can define the function by just giving its values on every element, as we did. This is clearly impossible when the domain is an infinite set, for example the natural numbers. In that case the function needs to be defined by a formula or by some rule. Recursive definitions, which we studied a few lectures ago, are also a method to define a function.

1.2.1. Injective Functions (one-one)

We say that a function is *injective* if every element of the domain is associated to a different result, that is, if no two elements share the same result. Formally we can define it as follows. Suppose

$$f : A \rightarrow B$$

f is *injective* $\Leftrightarrow$ $x = y \Rightarrow f(x) = f(y)$ for all elements $x, y \in A$.

The function favourite is injective because every person has a different favourite fruit. It is very useful to apply the definition in the contrapositive way: if two elements give the same result, then they must be equal.

1.2.2. Surjective Functions (Onto)

We say that a function is *surjective* if every element of the codomain is the result of applying the function to some element of the domain, that is, if every element is the "target" of the function for some argument. Formally we can define it as follows.

f is surjective $\Leftrightarrow$ for every $b \in B$ there is some $a \in A$ such that $f(a) = b$.

The function favourite is NOT surjective because cherry is nobody's favourite fruit.

Consider instead the following function, going in the opposite direction which associates to every fruit the person that owns it:

Owner: {apple, banana, cherry, peach} $\rightarrow$ {Anna, Brian, Carla}

Owner (apple) = Anna , Owner (banana) = Carla

Owner (cherry) = Anna, Owner (peach) = Brian

This function is in fact surjective: every person owns at least one fruit. On the other hand it is not injective: when applied to apple and cherry it gives the same result, Anna.

f is injective $\Leftrightarrow$ $f(x) = f(y) \Rightarrow x = y$ for all elements $x, y \in A$.

1.2.3. Bijective Functions (one-one and onto)

A *bijective* function is one that is both injective and surjective. Neither of the two functions defined above is bijective:

favourite isn't because it's not surjective and owner isn't because it's not injective. Let's consider the following function f that associates a number smaller than 4 to fruit:

fn: { apple, banana, cherry, peach}$\rightarrow${0,1,2,3}

fn (apple) = 2 fn (banana) = 0

fn (cherry) = 3 fn (peach) = 1

This function is injective (no two elements give the same result) and surjective (every number in the codomain is the result for some argument), therefore it is bijective.

Example 13

Let f be the function from {a, b, c, d} to {1, 2, 3} defined by

$f(a) = 3, \quad f(b) = 2, f(c) = 1$, and $f(d) = 3$.

Is f onto function?

Solution:

Yes, f is onto since all three elements of the codomain are images of elements in the domain. If the codomain were changed to {1, 2 , 3, 4}, f would not be onto.

Example 13

Is the function $f(x) = x^2$ from the set of integers to the set of integers onto? Solution:

No, f is not onto because there is no integer x with $x^2 = -1$, for example.

Example 14

Let's look at three numerical functions now and determine which of the properties of injectivity, surjectivity and bijectivity they satisfy:

$$f : N \rightarrow N$$

$$f(n) = 2 \times n + 1$$

This function is injective:

Suppose f(n) = f(m), that is, $2 \times n + 1 = 2 \times m + 1$; simple Arithmetic then tells us that n = m.

On the other hand it is not surjective: the values 0 and 2 (and all other even numbers) are not results of f.

$$half : N \rightarrow N \qquad at \quad half(n) = n/2$$

This function is not injective: half (0) = 0 and half (1) = 0, so two distinct arguments give the same result.

But it is surjective: every number m can be obtained as the result of this function on a certain argument, by taking $n = 2 \times m$;

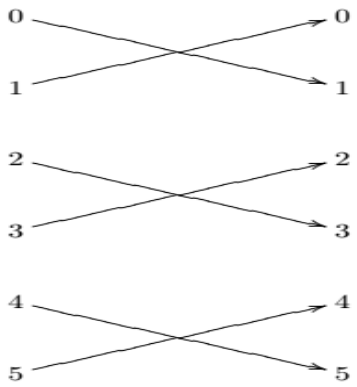
in fact, $half (2 \times m) = m$.

$$Swap : N \rightarrow N$$

$$Swap(n) = n + 1 \quad \text{if } n \text{ is even}$$

$$Swap(n) = n - 1 \quad \text{if } n \text{ is odd}$$

This function is both injective and surjective (I leave it to you to prove it). This fact can be clearly seen if we draw it using arrows



1.2.4. Composition

Suppose we have two functions such that the codomain of the first coincides with the domain of the second:

$$f : A \to B \text{ and } g : B \to C.$$

We can compose them by applying one after the other: starting with an element of A we first compute f on it and then we compute g on the result that we obtained from the first step:

$$A \xrightarrow{f} B \xrightarrow{g} C$$

$$x \longrightarrow f(x) \longrightarrow g(f(x))$$

The result is a function from A to C that we denote by $g \circ f$. Attention: the first function to be applied, f, is written to the right of the second to be applied, g.

$$g \circ f : A \longrightarrow C$$

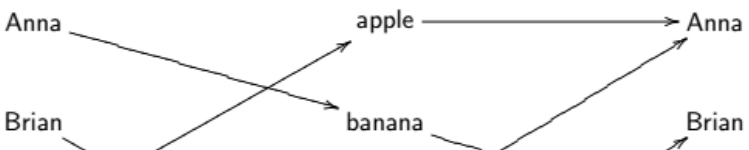
$$(g \circ f)(x) \longrightarrow g(f(x))$$

Example 15

Let's compute the composition of the favorite fruit and owner functions from above. The clearest way to do it is to represent them using arrows to show the associations and then "follow the arrows" to find the result of the composition. In our case we have:

A = {Anna, Brian, Carla}, B = {apple, banana, cherry, peach} and C = {Anna. Brian. Carla}.

$A \xrightarrow{\text{favourite}} B$ $\qquad$ $B \xrightarrow{\text{owner}} C$



Owner ∘ Favourite: {Anna, Brian, Carla} → {Anna, Brian, Carla}

$$(\text{owner} \circ \text{favourite})(\text{Anna}) = \text{Carla}$$

$$(\text{owner} \circ \text{favourite})(\text{Brian}) = \text{Brian}$$

$$(\text{owner} \circ \text{favourite})(\text{Carla}) = \text{Anna}$$

For a numeric example, let's compose the two functions f and half on the natural numbers:

$$\text{half} \circ f : \mathbb{N} \to \mathbb{N}$$

$$(\text{half} \circ f)(n) = (2 \times n + 1)/2$$

In this case the expression for the composition can be simplified:

$$(\text{half} \circ f)(n) = n.$$

The simplest of all functions is the one that doesn't do anything: it gives as result the argument itself. It is called the *identity function*:

$$\text{Id} : A \to A$$

$$\mathrm{Id}(a) = a$$

Suppose we have two functions going in opposite directions:

$$f : A \to B \text{ and } g : B \to A.$$

We say that they are *inverse* of each other if both

$$g \circ f = \mathrm{Id} \text{ and } f \circ g = \mathrm{Id}.$$

Be careful: both compositions must be checked; in general they give different functions. In fact $g \circ f$ is a function from A to A, while $f \circ g$ is a function from B to B.

For example

we notice that,

as above, $\text{half} \circ f = \mathrm{id}.$

But if we compose the functions the other way around we don't get the identity anymore.

Example 16

In the case of the function $f : R \to R$ defined by $f(x) = 2x + 3$, there is an inverse function, namely

$g : R \to R$ defined by $g(x) = (x - 3)/2$.

In the case of a function given in the form $y = f(x)$, finding

an inverse amounts to “solving” for x. Thus, in the example above, if we express the original function f in the equational form $y = 2x + 3$ then solving for x gives

$$x = (y - 3)/2 .$$

In other words, the inverse function is the function

$$g : R \rightarrow R \text{ defined by } g(y) = (y - 3)/2.$$

The only difference between this formulation of the definition of g and the first one is the use of x as the variable the first time, y the second time. In specifying a function, one is of course free to use any variable whatsoever, since the variable is just a kind of place marker, where particular arguments can be substituted in order to calculate the value. Since it is common to write real functions using x as variable, we first of all wrote the definition of g in terms of x. Another way of defining the notion of an inverse is that g is an inverse of a function

$$f : A \rightarrow B \quad \text{iff} \quad g : B \rightarrow A$$

And $g \circ f = \boldsymbol{IdA}$ and $f \circ g = \boldsymbol{IdB}$

where ***IdA***, ***IdB*** are the identity functions on A, B, respectively.

Example 17

If (f ∘ half) (2) = 3. So half and f are not inverse of each other. (We may still say that half is a left inverse of f and that f is a right inverse of half).

If $f : A \to B$ has an inverse, this is denoted by f^{-1}.

The most important fact about bijections is that they are exactly those functions that can be ***inverted***.

Theorem

The following equivalence is true for every function $f : A \to B$:

f *is bijective* $\Leftrightarrow$ f *has an inverse*.

(We will not look at the proof of this theorem, but you may want to try to give it yourself.)

For example, we remarked earlier that the function fn is bijective. It is easy to compute its inverse by associating to each number the fruit that's mapped to it by fn:

$fn^{-1} : \{0, 1, 2, 3\} \to \{$apple, banana, cherry, peach$\}$

$fn^{-1}(0) =$ banana $fn^{-1}(1) =$ peach

$fn^{-1}(2)$ = apple $fn^{-1}(3)$ = cherry.

Example 18

Let f and g be functions from the set of integers to the set of integers defined by

$$f(x) = 2x+3 \text{ and } g(x) = 3x+2.$$

What is the composition of ***f*** and ***g,*** and also the composition of ***g*** and ***f***?

Solution:

$f \circ g\,(x) = f\,(g(x)) = f(3x+2) = 2(3x+2)+3 = 6x+7$

$g \circ f\,(x) = g\,(f(x)) = g(2x+3) = 3(2x+3)+2 = 6x+11$

Example 19

Let $f : Z \rightarrow Z$ be such that $f(x) = x + 1$. Is f invertible, and if so, what is its inverse?

Solution:

The function f is invertible because it is a one to one correspondence. The inverse function f^{-1} reverses the correspondence so $f^{-1} = y-1$.

Exercises 1.2

1) Let $A = \{1, 2\}$, $B = \{1, 2, 3\}$. List all the functions from A to B.

2) Identify those functions in question (1) which are

(a) one-one (b) onto

(c) bijective

In each case, identify the range of the function.

3) Define $f : R \to R$ by

$$f(x) = \begin{cases} x^2 & \text{if } x \geq 0 \\ x - 1 & \text{if } x < 0 \end{cases}$$

Define $g : R \to R$ by

$$g(x) = \begin{cases} x + 1 & \text{if } x \geq 1 \\ 2x & \text{if } x < 1 \end{cases}$$

Find formulas for the functions $g \circ f$ and $f \circ g$.

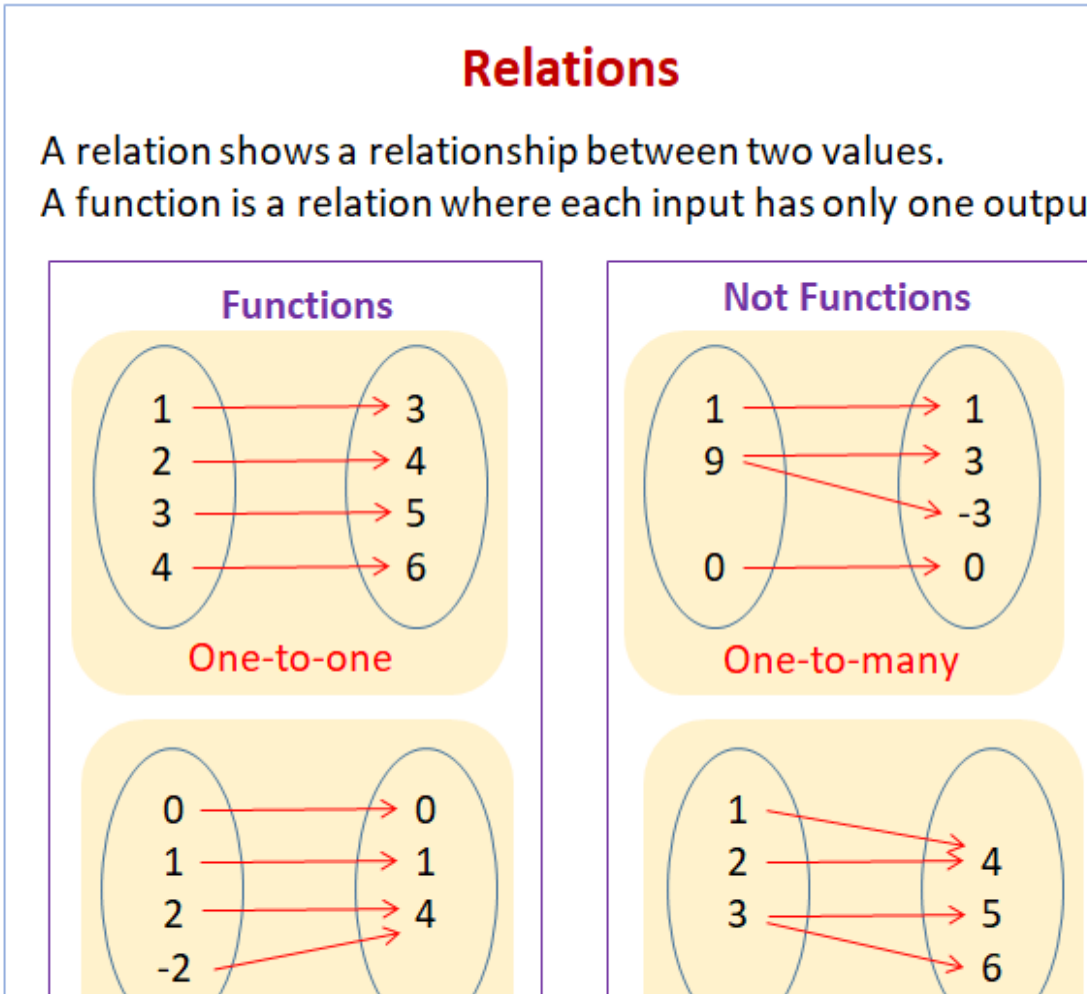
Use this example to show that $g \circ f = f \circ g$ is not in general true.

4) Define $f : \mathrm{R}^2 \to \mathrm{R}^2$ by $f(x, y) = (x + 2y, x - y)$.

Show that f is a bijection and find f^{-1}

1.3.
Relations

A relation is a set of inputs and outputs, often written as ordered pairs (input, output). We can also represent a relation as a mapping diagram or a graph. For example, the relation can be represented as:



The following diagram shows some examples of relations and functions. Scroll down the page for more examples and solutions on how to determine if a relation is a function.

1.3.1. Determining whether a relation is a function

Understanding relations (defined as a set of inputs and corresponding outputs) is an important step to learning what makes a function. A function is a specific relation, and determining whether a relation is a function is a skill necessary for knowing what we can graph. Determining whether a relation is a function involves making sure that for every input there is only one output.

How to determine if a relation is a function?

A function is a correspondence between a first set, called the domain, and a second set, called the range, such that each member of the domain corresponds to exactly one member of the range. The graph of a function f is a drawing hat

represents all the input-output pairs, (x, f(x)). In cases where the function is given by an equation, the graph of a function is the graph of the equation

$$y = f(x).$$

The vertical line test - a graph represents a function if it is impossible to draw a vertical line that intersects the graph more than once.

In the above section dealing with functions and their properties, we noted the important property that all functions must have, namely that if a function does map a value from its domain to its co-domain, it must map this value to only one value in the co-domain. Writing in set notation, if **a** is some fixed value:

$$|\{f(x)|x=a\}| \in \{0, 1\}$$

The literal reading of this statement is: the cardinality (number of elements) of the set of all values f(x), such that x= **a** for some fixed value a, is an element of the set {0, 1}.

In other words, the number of outputs that a function f may have at any fixed input **a** is either zero (in which case it is undefined at that input) or one (in which case the output is unique). However, when we consider the relation, we relax this constriction, and so a relation may map one value to more than one other value. In general, a relation is any subset of the

Cartesian product of its domain and co-domain. All functions, then, can be considered as relations also.

Notations

When we have the property that one value is related to another, we call this relation a binary relation and we write it as

$_x R_y$, where R is the relation.

Example 20

Let us examine some simple relations. Say f is defined by

{(0,0),(1,1),(2,2),(3,3),(1,2),(2,3),(3,1),(2,1),(3,2),(1,3)}

This is a relation (not a function) since we can observe that 1 maps to 2 and 3, for instance.
Less-than, "<", is a relation also. Many numbers can be less than some other fixed number, so it cannot be a function.

Definition

A relation from a set A to a set B is a subset of A×B. Hence, a relation R consists of ordered pairs (a, b), where a∈A and b∈B. If (a,b) ∈R, we say that is related to , and we also write $_aR_b$.

Example 21

Let A={1,2,3,4,5,6} and B={1,2,3,4}.

Define (a, b) ∈R if and only if (a−b) mod2 = 0.

Then

R={(1,1),(1,3),(2,2),(2,4),(3,1),(3,3),(4,2),(4,4),(5,1),(5,3),(6,2),(6,4)}.

We note that R consists of ordered pairs (a, b) where a and b have the same parity. Be cautious, that 1≤ a ≤ 6 and 1 ≤ b ≤ 4.

Hence, it is meaningless to talk about whether (1, 5) ∈R or (1, 5) ∉*R*.

1.3.2. Properties of Relations

When we are looking at relations, we can observe some special properties different relations can have.

1. Reflexive

A relation is reflexive if, we observe that for all values a:

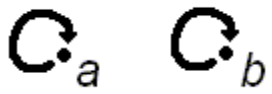
$$_a R_a$$

In other words, all values are related to themselves. The relation of equality, "=" is reflexive. Observe that for, say, all numbers a (the domain is R):

$$a = a$$

so "=" is reflexive.

In a reflexive relation, we have arrows for all values in the domain pointing back to



Note that ≤ is also reflexive (a ≤ a for any a in R). On the other hand, the relation < is not (a < a is false for any a in R).

2. Symmetric

A relation is symmetric if, we observe that for all values of a and b:

$$a R_b \quad \text{implies} \quad b R_a$$

The relation of equality again is symmetric. If x=y, we can also write that y=x also.

In a symmetric relation, for each arrow we have also an opposite arrow, i.e. there is either no arrow between x and y, or an arrow points from ›m y to x:

Neither ≤ nor < is symmetric (2 ≤ 3 and 2 < 3 but neither 3 ≤ 2 nor 3 < 2 is true).

3. Transitive

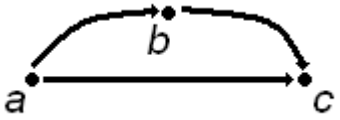
A relation is transitive if for all values a, b, c:

$$a R_b \quad \text{and} \; b R_c \quad \text{implies} \; a R_c$$

The relation greater-than ">" is transitive. If x > y, and y > z, then it is true that x > z. This becomes clearer when we write down what is happening into words. x is greater than y and y is greater than z. So x is greater than both y and z.

The relation is-not-equal "≠" is not transitive. If x ≠ y and y ≠ z then we might have x = z or x ≠ z (for example 1 ≠ 2 and 2 ≠ 3 and 1 ≠ 3 but 0 ≠ 1 and 1 ≠ 0 and 0 = 0).

In the arrow diagram, every arrow between two values a and b, and b and c, has an arrow going straight from a to c.



4. Antisymmetric

A relation is antisymmetric if we observe that for all values a and b:

$$_{a}R_{b} \quad \text{and} \quad _{b}R_{a} \text{ implies that } a=b$$

Notice that antisymmetric is not the same as "not symmetric."

Take the relation greater than or equal to, "≥" If x ≥ y, and y ≥ x, then y must be equal to x. a relation is anti-symmetric if and only if a∈A, (a,a) ∈R .

5. Trichotomy

A relation satisfies trichotomy if we observe that for all values a and b it holds true that:

$$_aR_b \quad \text{or} \quad _bR_a$$

The relation is-greater-or-equal satisfies since, given 2 real numbers a and b, it is true that whether $a \geq b$ or $b \geq a$ (both if $a = b$).

1.3.3. Operations on Relations

There are some useful operations one can perform on relations, which allow to express some of the above mentioned properties more briefly.

1. Inversion

Let R be a relation, then its inversion, R^{-1} is defined by

$$R^{-1} := \{(a,b) \mid (b,a) \text{ in } R\}.$$

2. Concatenation

Let R be a relation between the sets A and B, S be a relation between B and C. We can concatenate these relations by defining

$$R \bullet S := \{(a,c) \mid (a,b) \text{ in } R \text{ and } (b,c) \text{ in } S \text{ for some } b \text{ out of } B\}$$

3. Diagonal of a Set

Let A be a set, then we define the diagonal (D) of A by

$$D(A) := \{(a,a) \mid a \text{ in } A\}$$

Shorter Notations

Using above definitions, one can say (lets assume R is a relation between A and B):

R is *transitive* if and only if R • R is a subset of R.

R is *reflexive* if and only if D(A) is a subset of R.

R is *symmetric* if R^{-1} is a subset of R.

R is *antisymmetric* if and only if the intersection of R and R^{-1} is D(A).

R is *asymmetric* if and only if the intersection of D(A) and R is empty.

R is a function if and only if R^{-1} • R is a subset of D(B).

In this case it is a function A → B. Let's assume R meets the condition of being a function, then

R is *injective* if R • R^{-1} is a subset of D(A).

R is *surjective* if {b | (a,b) in R} = B.

1.4. Logic

1.4.1. Truth Tables

Since we have defined the logical connectives ∧, ∨, ¬, ⇒, ⇔ in terms of truth and falsity alone, and not to meaning, it is possible to represent (or illustrate) them by means of a table: a truth table. We introduce two symbols: T to denote "true" and F

ϕ	ψ	$\phi \wedge \psi$
T	T	T
T	F	F
F	T	F

to denote "false". The behavior/definition of $\varphi \wedge \psi$ can then be illustrated by the table:

In the first two columns appear all the possible combinations of values of T and F that the two statements φ and ψ can have. In the third column we give the value $\varphi \wedge \psi$ achieves according to each assignment of T or F to φ and ψ. Thus, we see that $\varphi \wedge \psi$ is T only when both φ and ψ are T. For $\varphi \vee \psi$ we have the table

ϕ	ψ	$\phi \vee \psi$
T	T	T
T	F	T
F	T	T
F	F	F

Again, the definition of ¬φ can be represented thus:

ϕ	$\neg\phi$
T	F
F	T

For φ ⇒ ψ we have:

ϕ	ψ	$\phi \Rightarrow \psi$
T	T	T
T	F	F
F	T	T
F	F	T

One can go on to construct truth tables for more complicated expressions. Consider, for example, the expression (φ ∧ ψ) ∨ (¬φ). We can build its table column by column as follows:

ϕ	ψ	$\phi \wedge \psi$	$\neg\phi$	$(\phi \wedge \psi) \vee (\neg\phi)$
T	T	T	F	T
T	F	F	F	F
F	T	F	T	T
F	F	F	T	T

We can also draw up tables for expressions such as (φ ∧ ψ) ∨ θ, but if there are n constituent statements involved there will be 2n rows in the table, so already (φ ∧ ψ) ∨ θ needs 8 rows.

Truth tables can be useful in checking that two rather complex statements are equivalent. For, by our definition of equivalence, two statements will be equivalent if they have the same truth table. For example, we can demonstrate the equivalence of ¬(φ ∧ ψ) and (¬φ) ∨ (¬ψ) as follows:

			*			*
φ	**ψ**	**φ ∧ ψ**	**¬(φ ∧ ψ)**	**¬φ**	**¬ψ**	**(¬φ) ∨ (¬**
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

*Since the two columns marked * are identical, we know that the two expressions are equivalent.*

1.4.2. Contrapositives

The contrapositive of a conditional φ ⇒ ψ is the conditional

$$\neg\, \psi \Rightarrow \neg\, \varphi$$

(Note that the introduction of the negation sign is accompanied by a change in the direction of the arrow.)

For example, for the implication If 2n - 1 is prime, then n is prime the contrapositive implication is If n is composite (i.e., not prime), then 2n - 1 is composite. The following result is the logical basis for the mathematical concept of proof by contrapositive, where an implication is proved by establishing its contrapositive.

1.4.3. Boolean Algebra

The purpose of these notes is to introduce Boolean notation for elementary logic. In this version of things we use 0 for F (False) and 1 for T (True). Negation is represented by placing a bar (or over line) across an expression.

Thus we write

$$\sim A = \overline{A}.$$

The over line can go across a complex expression. Thus we have

$$\sim (A \vee B) = \overline{A \vee B}.$$

In Boolean notation, we use multiplication for “and” and addition for ‘’ or’’

Thus, we write

$$A \vee B = A + B$$

and we write

$$A \wedge B = AB$$

Note, for example, how DeMorgan’s Law transcribes in the Boolean notation

$$\sim (A \vee B) = \overline{A+B},$$

$$\sim A \wedge \sim B = \quad A\,B$$

Remark on Boolean Arithmetic.

The Boolean values of 0 and 1 form a very simple arithmetic with the following rules.

1. $\bar{0} = 1$
2. $\bar{1} = 0$
3. $0 + 0 = 0$
4. $0 + 1 = 1 + 0 = 1$
5. $1 + 1 = 1$ (watch out for that one!)
6. $1 \times 1 = 1$
7. $0 \times 0 = 0 \times 1 = 1 \times 0 = 0$

It is a remarkable fact that all the identities in basic logic and Boolean algebra are simply the identities that are true about this arithmetic. For example, the identity $\bar{\bar{A}} = A$

can be interpreted as saying that for any element A of the Boolean Arithmetic $\bar{\bar{A}} = A$. And you only have to check that this is true for A = 0 and for A = 1 to prove it.

Note that in Boolean notation we have

$$(A \Rightarrow B) = \bar{A}B.$$

This makes a compact notation for implication.

Here is a list of identities that you are familiar with, written in Boolean notation. You can make these into exercises by either translating them into logic or set notation or seeing that they are true via truth tables or Venn diagrams *or* you can verify that they are true in Boolean arithmetic.

1. $\bar{\bar{A}} = A$.
2. A + B = B + A
3. (A + B) + C = A + (B + C)
4. AB = BA
5. (AB) C = A (BC)
6. A + A = A
7. 1 + A = 1
8. 0 + A = A
9. $A + \bar{A} = 1$
10. $A\ \bar{A} = 0$
11. A (B + C) = AB + AC
12. A + BC = (A + B) (A + C)

13. A+B=$\overline{\overline{A}\,\overline{B}}$

1.4.4. Fundamental Concepts of Boolean Algebra

Boolean algebra is a logical algebra in which symbols are used to represent logic levels. Any symbol can be used; however, letters of the alphabet are generally used. Since the logic levels are generally associated with the symbols 1 and 0, whatever letters are used as variables that can take the values of 1 or 0. Boolean algebra has only two mathematical operations, addition and multiplication. These operations are associated with the OR gate and the AND gate, respectively.

Logical Addition

When the + (the logical addition) symbol is placed between two variables, say X and Y, since both X and Y can take only the role 0 and 1, we can define the + Symbol by listing, all possible combinations for X and Y and the resulting value of X + Y. The possible input and output combinations may arranged as follows:

0 + 0 = 0
0 + 1 =1
1+ 0 = 1
1 + 1 = 1

This table represents a standard binary addition, except for the last entry. When both' X and Y represents 1‟s, the value of X + Y is 1. The symbol + therefore does not has the “Normal” meaning, but is a Logical addition symbol. The plus symbol (+) read as "OR", therefore X +Y is read as X or Y.

This concept may be extended to any number of variables for example A + B + C +D = E Even if A, B, C and D all had the values 1, the sum of the values i.e. is 1.

Logical Multiplication

We can define the "." (logical multiplication) symbol or AND operator by listing all possible combinations for (input) variables X and Y and the resulting (output) value of X. Y as,

0 .0= 0
0 .1 = 0
1 .0 = 0
1 .1 = 1

Note: Three of the basic laws of Boolean algebra are the same as in ordinary algebra; the commutative law, the associative law and the distributive law.

The commutative law:

for addition and multiplication of two variables is written as,

$$A + B = B + A$$

and

$$A \cdot B = B \cdot A$$

The associative law:

for addition and multiplication of three variables is written as,

$$(A + B) + C = A + (B + C)$$

and

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

The distributive law:

for three variables involves' both addition and multiplication and is written as,

$$A (B+ C) = A B + AC$$

Note that while either '+' and „‟ s can be used freely. The two cannot be mixed without ambiguity in the absence of further rules.

Example 22

Does

A . B + C means (A . B) + C or A . (B+ C)?

These two form different values for A = O, B = 1 and C = 1, because we have

(A . B) + C = (0.1) +

1 = 1

and A . (B + C) = 0 . (1 + 1) = 0

which are different. The rule which is used is that „." is always performed before '+'.

Thus X.Y + Z is (X.Y) + Z.

1.4.5 Logic Gates

A logic gate is defined as an electronics circuit with two or more input signals and one output signal. The most basic logic Circuits are OR gates, AND gates, and invertors or NOT gates. Strictly speaking, invertors are not logic gates since they have only one input signal; however. They are best introduced at the same time as basic gates and will therefore be dealt in this section.

OR Gate:

An OR gate is a logic circuit with two or more input signals and one output signal. The output signal will be high

(logic 1) if any one input signal is high (logic 1). OR gate performs logical addition.

The symbol for the logic OR gate is

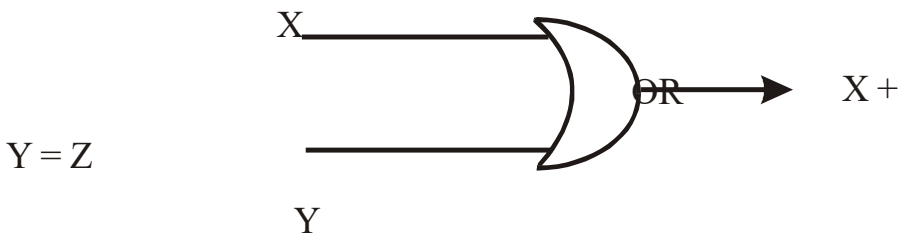
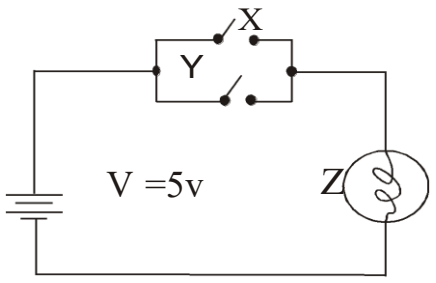


Fig. 1

A circuit that will functions as an OR gate can be implemented in several ways. A mechanical OR gate can be fabricated by connecting two switches in parallel as shown in figure 2

Fig. 2



Truth Table for a switch circuit operation as an OR gate.

Note that for the switch circuit were use diodes and resistors, Transistors and resistors and other techniques to control the voltage and resistance.

Table.1

Switch X	Switch Y	Output Z
Open	Open	0
Open	Closed	5V
Closed	Open	5V
Closed	Closed	5V

Note: If the switch is "on", it is represented by 1, and if, it is "off", it is represented by 0. Truth Table for a Two-input **OR** gate.

Table.2

In Put		**Out Put**
X	Y	Z
0	0	0
0	1	1
1	0	1
1	1	1

Truth table for a three in put **OR** gate.

Table .3

A	**B**	**C**	**X**
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1

1	1	1	1

No. of combinations = 2^n, where n is number of variables.

AND Gate:

An **AND** gate is a logic circuit with two or more input signals and one output signal. The output signal of an **AND** gate is high (logic 1) only if all inputs signals are high (Logic 1).

An **AND** gate performs logical multiplication on inputs. The symbol for **AND** gate is

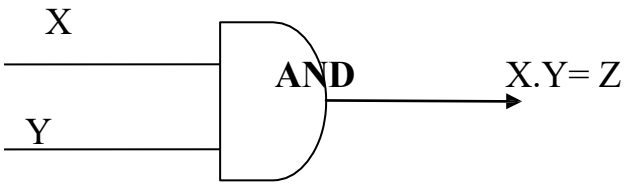


Fig.3

A circuit that will functions as an **AND** gate can be implemented in several ways. A mechanical **AND** gate can be fabricated by connecting two switches in series as show in fig. 4

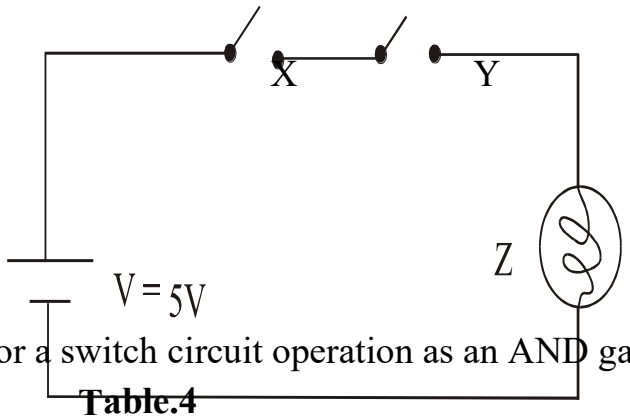


Fig.4

Truth Table for a switch circuit operation as an AND gate.

Table.4

Switch X	Switch Y	Output Z
Open	Open	0
Open	Closed	0
Closed	Open	0
Closed	Closed	5V

Truth table for a Two-input **AND** gate

Table. 5

In Put		Out Put
X	**Y**	**Z**
0	0	0
0	1	0
1	0	0
1	1	1

Truth Table for a three input **AND** gate

Table.6

Inputs			Output
A	**B**	**C**	**X**
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0

1	0	1	0
1	1	0	0
1	1	1	1

1.4.5. Complementation

The logical operation of complementary or inverting a variable is performed in the Boolean Algebra. The purpose of complementation is to invert the, input signal, since there are only two values that variables can assume in two-value logic system, therefore if the input is 1, the output is 0 and if the input is 0 the output is 1. The symbol used to represent complementation of a variable is a bar (-) above the variable, for example the complementation of A is written as $\overline{A}$ and is read as "complement of A" or "A not".

Since variables can only be equal to 0 or 1, we can say that

$$\overline{0} = 1 \qquad \text{or} \qquad \overline{1} = 0$$

$$\overline{\overline{0}} = 0 \qquad \text{or} \qquad \overline{\overline{1}} = 1$$

Invertors Or NOT gate:

An inventor is a gate with only one input signal and one output signal; the output signal is always the opposite or complement of the input signal. An invertor is also called a **NOT** gate because the output not the same as the input.

Symbol of inverter or **NOT** gate is

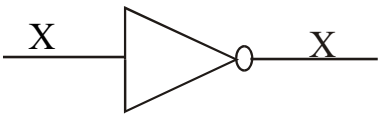


Fig.5 (i)

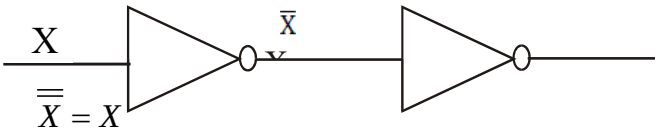


Fig.5 (ii)

Fig.5(ii) (Two invertors in series)

The circle at the output or input indicates inversion. It also distinguish between the symbol for the **NOT** gate or the symbol for a operational amplifier or certain types of buffers, because the symbol -►- can also be used for diode.

Truth Table for a **NOT** circuit

Table.7

In put	Out put
0	1
1	0

NOTE: A word is a group (or string) of binary bits that represents a closed instruction or data.

Example 23

How many input words in the Truth Table of an 6 - input OR gate? Which, input word produce a high output?

Solution

The total number of input words = $2^n = 2^6 = 32$, where n is number of inputs. In an OR gate 1 or more-high inputs produce a high output. Therefore the word of 000000 results in low outputs all other input words produce a high output.

1.4.6. Basic Duality in Boolean Algebra

We state the duality theorem without proof. Starting with a Boolean relation, we can derive another Boolean relation by

1. Changing each **OR (+)** sign to an **AND (.)** sign
2. Changing each **AND (.)** sign to an **OR (+)** sign.
3. Complementary each 0 and 1.

For instance

$$A + 0 = A$$

The dual relation is $A \cdot 1 = A$

Also since A (B + C) = AB + AC by distributive law. Its dual relation is

$$A + B\,C = (A + B)\,(A + C)$$

Fundamental Laws and Theorems of Boolean Algebra

1) OR operations

$$X + 0 = X$$

$X + 1 = 1$

$X + X = X$

$X + \overline{X} = 1$

2) AND operations

$X \cdot 0 = 0$

$X \cdot 1 = X$

$X \cdot X = X$

$X \cdot \overline{X} = 0$

3) Double complement

$\overline{\overline{X}} = X$

4) Commutative laws

$X + Y = Y + X$

$XY = YX$

5) Associative laws

$(X + Y) + Z = X + (Y + Z)$

$(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$

6) Distribution Law

$X (Y + Z) = XY + XZ$

7) Dual of Distributive Law

$X + Y \cdot Z = (X + Y) \cdot (X + Z)$

8) Laws of absorption

$X + XZ = X$

$X (1 + Z) = X.1 = X$

9) De Morgan's Theorems

$$\overline{X + Y} = \overline{Y} \cdot \overline{X}$$

$$\overline{X \cdot Y} = \overline{Y} + \overline{X}$$

Example 24

Find the complement of the expression: X + YZ and verified the result by perfect induction.

$$\overline{X + YZ} = \overline{X} \cdot \overline{YZ}$$
$$= \overline{X} \cdot (\overline{Y} + \overline{Z})$$

by DeMorgan‟s Law this relation can be verified by perfect induction.

Example 25

Express the Boolean function

$$XY+YZ+ \overline{Y}Z = XY + Z$$

Solution

$$\text{L.H.S} = XY+YZ+ \overline{Y}Z$$
$$= XY+(Y+ \overline{Y})Z$$
$$= XY+1.Z$$
$$= R.H.S$$

Exercises 1.4

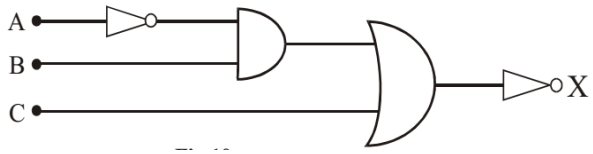
1) Simplify the Boolean expressions:

a) $(X+Y)(X+\overline{Y})(\overline{X}+Z)$

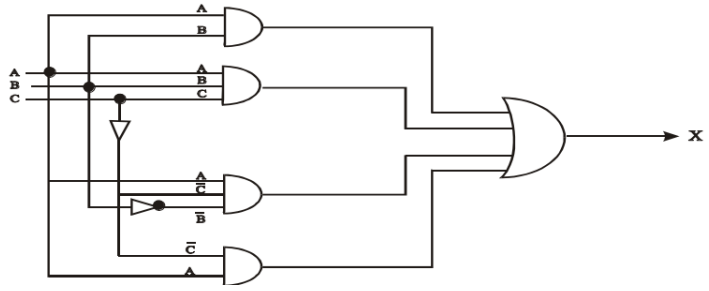
b) $XYZ+X\overline{Y}Z+XY\overline{Z}$

2) Write the Boolean expression that describes mathematically the behavior of logic circuit shown in figs

a)



b)



3) Prepare a truth table for the following Boolean expression:

a) $XYZ+\overline{X}\overline{Y}\overline{Z}$

b) $XY+\overline{X}\overline{Y}$

c) $XYZ+X\overline{Y}\overline{Z}+\overline{X}\overline{Y}\overline{Z}$

4) Draw a logic circuit using only NOR gates for which the output expression is $X=A\overline{C}+\overline{B}C$

5) Prove the following by use of a truth table:

$$\overline{A}B\overline{A}+\overline{A}BC+\overline{A}\overline{B}C=\overline{A}B+\overline{A}C$$

6) Prove that

1) $A.B+A.\overline{B}=A$ **2)** $\overline{(A+B)}.(\overline{A}+B)=\overline{A}$

Chapter 2

Induction and Recursion

2.1 Mathematical induction

Introduction

Suppose that we have an infinite ladder, as shown in Figure 1, and we want to know whether we can reach every step on this ladder. We know two things:

1. We can reach the first rung of the ladder.
2. If we can reach a particular rung of the ladder, then we can reach the next rung.

   Can we conclude that we can reach every rung? By (1), we know that we can reach the first rung of the ladder. Moreover, because we can reach the first rung, by (2), we can also reach the second rung; it is the next rung after the first rung. Applying (2) again, because we can reach the second rung, we can also reach the third rung. Continuing in this way, we can show that we can reach the fourth rung, the fifth rung, and so on. For example, after 100 uses of (2), we know that we can reach the 101st rung. But can we conclude that we are able to reach every rung of this infinite ladder? The answer is yes, something we can verify using an important proof technique called mathematical induction. That is, we can show that P (n) is true for every positive integer n, where P (n) is the statement that we can reach the nth rung of the ladder.

   Mathematical induction is an extremely important proof technique that can be used to prove assertions of this type. As we will see in this section and in subsequent sections of this chapter and later chapters, mathematical induction is used extensively to prove results about a large variety of discrete objects. For example, it is used to prove results about the complexity of algorithms, the correctness of certain types of

computer programs, theorems about graphs and trees, as well as a wide range of identities and inequalities.

In this section, we will describe how mathematical induction can be used and why it is a valid proof technique. It is extremely important to note that mathematical induction can be used only to prove results obtained in some other way. It is not a tool for discovering formulae or theorems.

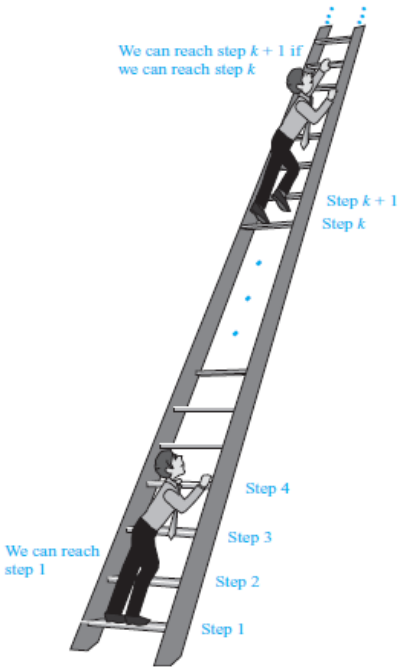


FIGURE 1 Climbing an Infinite Ladder.

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:

BASIS STEP: We verify that P (1) is true.

INDUCTIVE STEP: We show that the conditional statement P(k) → P (k + 1) is true for all positive integers k.

To prove any relation by using mathematical induction

- Basis step
  Prove the relation at n=1
- Inductive step

Assume the relation is true at n=k then Prove the relation at n=k+1

Ex 1 By using mathematical induction prove that.

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

Proof

- At n=1

$L.H.S = 1$

$R.H.S = \frac{1(2)}{2} = 1$

$R.H.S = L.H.S$

- Assume the relation is true at $n = k$

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2} \qquad (1)$$

- At $n = k + 1$

$R.H.S = \frac{(k+1)(k+2)}{2}$

$L.H.S 1 + 2 + \cdots + K + K + 1 \qquad from(1)$

$$L.H.S \frac{K(K+1)}{2} + K + 1 = \frac{K(K+1)(K+2)}{2} = R.H.S$$

Thus, the relation is true.

Ex 2 **By using mathematical induction prove that.**

$$\frac{\mathbf{1}}{\mathbf{2}!}+\frac{\mathbf{2}}{\mathbf{3}!}+\frac{\mathbf{3}}{\mathbf{4}!}+\cdots+\frac{\boldsymbol{n}}{(\boldsymbol{n}+\mathbf{1})!}=\mathbf{1}-\frac{\mathbf{1}}{(\boldsymbol{n}+\mathbf{1})!}$$

Proof

- At $n=1$

  $L.H.S=\frac{1}{2!}=\frac{1}{2}$

  $R.H.S=1-\frac{1}{2}=\frac{1}{2}$

- Assume the relation is true at $n=k$

  $$\frac{1}{2!}+\frac{2}{3!}+\frac{3}{4!}+\cdots+\frac{k}{(k+1)!}=1-\frac{1}{(k+1)!} \qquad (1)$$

- At $n=k+1$

  $R.H.S=1-\frac{1}{(k+2)!}$

$$L.H.S=\frac{1}{2!}+\frac{2}{3!}+\frac{3}{4!}+\cdots+\frac{k}{(k+1)!}+\frac{k}{(k+2)!} \qquad from\ (1)$$

$$L.H.S=1-\frac{1}{(k+1)!}+\frac{k+1}{(k+2)!}=1+\frac{-(k+2)+k+1}{(k+2)!}$$

$$L.H.S=1+\frac{\cancel{-k}-2\cancel{+k}+1}{(k+2)!}=1-\frac{1}{(k+2)!}=R.H.S$$

Thus, the relation is true.

Ex 3 **By using mathematical induction prove that.**

$$\mathbf{1}*\mathbf{2}+\mathbf{2}*\mathbf{3}+\mathbf{3}*\mathbf{4}+\cdots+\boldsymbol{n}(\boldsymbol{n}+\mathbf{1})=\frac{\boldsymbol{n}(\boldsymbol{n}+\mathbf{1})(\boldsymbol{n}+\mathbf{2})}{\mathbf{3}}$$

Proof

- At $n=1$

  $L.H.S=1(2)=2$

  $R.H.S=\frac{1(2)(3)}{3}=2=L.H.S$

- Assume the relation is true at $n=k$

$$1*2+2*3+3*4+\cdots+k(k+1)=\frac{k(k+1)(k+2)}{3}$$

❖ At $n = k + 1$

$$R.H.S = \frac{(k+1)(k+2)(k+3)}{3} \qquad (1)$$

$$L.H.S = 1*2 + 2*3 + 3*4 + \cdots + k(k+1) + (k+1)(k+2) \quad from\ (1)$$

$$L.H.S = \frac{k(k+1)(k+2)}{3} + (k+1)(k+2)$$

$$= \frac{(k+1)(k+2)(k+3)}{3} = R.H.S$$

Thus, the relation is true.

<u>Ex 4</u> Prove that the sum of the cubes of three consecutive natural numbers divided by 9.

Proof

Let the numbers are $n\ , n+1\ , n+2$

$n^3 + (n+1)^3 + (n+2)^3$

❖ At $n = 1$

$1^3 + 2^3 + 3^3 = 36 \qquad divided\ by\ 9$

$thus\ {}^{36}/_{9} = 4$

❖ Assume the relation is true at $n = k$

$$\frac{k^3 + (k+1)^3 + (k+2)^3}{9} \qquad (1)$$

❖ At $n = k + 1$

$(k+1)^3 + (k+2)^3 + (k+3)^3$

$(k+1)^3 + (k+2)^3 + [k^3 + 9k^2 + 27k + 27]$

$(k+1)^3 + (k+2)^3 + k^3 + [9k^2 + 27k + 27]$

$from\ (1)\ k^3 + (k+1)^3 + (k+2)^3\ is$ divided by 9 and $[9k^2 + 27k + 27]$ is divided by 9

The relation is true at $n = k + 1$ thus the relation is true.

<u>Ex 5</u> By using mathematical induction prove that.

$$\begin{bmatrix} \mathbf{1} & \boldsymbol{x} \\ \mathbf{0} & \mathbf{1} \end{bmatrix}^{\boldsymbol{n}} = \begin{bmatrix} \mathbf{1} & \boldsymbol{nx} \\ \mathbf{0} & \mathbf{1} \end{bmatrix}$$

Prof

- ❖ At $n = 1$

  $L.H.S = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$

  $R.H.S = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$

  $R.H.S = L.H.S$
- ❖ Assume the relation is true at $n = k$

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{k} = \begin{bmatrix} 1 & kx \\ 0 & 1 \end{bmatrix} \qquad (1)$$

- ❖ At $n = k + 1$)

  $R.H.S = \begin{bmatrix} 1 & (k+1)x \\ 0 & 1 \end{bmatrix}$

$$L.H.S = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{k+1} = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}^{k} * \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \qquad from\ (1)$$

$$L.H.S = \begin{bmatrix} 1 & Kx \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & kx + x \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & (k+1)x \\ 0 & 1 \end{bmatrix} = R.H.S$$

Thus, the relation is true.

<u>Ex 6</u> By using mathematical induction prove that.

$$\boldsymbol{x^n - y^n\ divisable\ by\ x - y}$$

Proof

- ❖ At $n = 1$

  $x^1 - y^1 = x - y\ is\ divisable\ by\ x - y$
- ❖ Assume that the relation is true at $n = k$

$$x^k - y^k / x - y \qquad (1)$$

- ❖ At $n = k + 1$

$$x^{(k+1)} - y^{(k+1)}$$
$$= x^k x - y^k y + x^k y - x^k y$$

$= x^k(x-y) - y(x^k - y^k)$ $from\ (1)$

The first term is divisible by $x - y$

The second term is divisible by $x - y$

Thus, the relation is true.

<u>Ex 7</u> By using mathematical induction prove that.

$$S_n = 4^n + 15n - 1\ is\ divisable\ by\ 9$$

Proof

- At $n = 1$

$$S_1 = 4^1 + 15(1) - 1 = 4 + 15 - 1 = {}^{18}/_{9}$$

- Assume that the relation is true at $n = k$

$$s_k = {}^{4^k + 15k - 1}/_{9} \qquad (1)$$

- At $n = k + 1$

$$s_{(k+1)} = 4^{(k+1)} + 15(k+1) - 1$$

$$= 4 * 4^k + 15k + 14 = 4 * 4^k + (60k - 45k) + (18 - 4)$$

$$= 4 * 4^k + 60k - 4) + (-45k + 18)$$

$$= 4(4^k + 15k - 1) - 9(5k - 2)$$

The 1st term $4(4^k + 15k - 1)$ is divisible by 9 from (1) and the 2nd is divisible by 9. Thus, the relation is true.

<u>Ex 8</u> Use the mathematical induction prove that.

$$n^3 - n\ is\ divisible\ by\ 3\ \ for\ n \geq 1$$

Proof

- At $n = 1$

$$1^3 - 1 = \frac{0}{3} \qquad p(1) true$$

- Assume that the relation is true at $n = k$

$$k^3 - k\ is\ divisible\ by\ 3 \quad p(k) true$$

❖ At $n = k + 1$

$$k^3 - k = k^3 + 3k^2 + 3k + 1 - k - 1$$
$$= \left(k^3 - k\right) + 3\left(k^2 + k\right)$$

The 1st term $\left(k^3 - k\right)$is divisible by 3 from (1) and the 2nd is divisible by 3. Thus, the relation is true.

2.2 Recursive Definitions

Introduction

Sometimes it is difficult to define an object explicitly. However, it may be easy to define this object in terms of itself. This process is called recursion. For instance, the picture shown in Figure 2 is produced recursively. First, an original picture is given. Then a process of successively superimposing centered smaller pictures on top of the previous pictures is carried out We can use recursion to define sequences, functions, and sets. and in most beginning mathematics courses, the terms of a sequence are specified using an explicit formula. For instance, the sequence of powers of 2 is given by $a_n = 2^n$ for n = 0, 1, 2,.... Recall that we can also define a sequence recursively by specifying how terms of the sequence are found from previous terms. The sequence of powers of 2 can also be defined by giving the first term of the sequence, namely, $a_0 = 1$, and a rule for finding a term of the sequence from the previous one, namely, $a_{n+1} = 2a_n$ for n = 0, 1, 2,… When we define a sequence recursively by specifying how terms of the sequence are found from previous terms, we can use induction to prove results about the sequence.

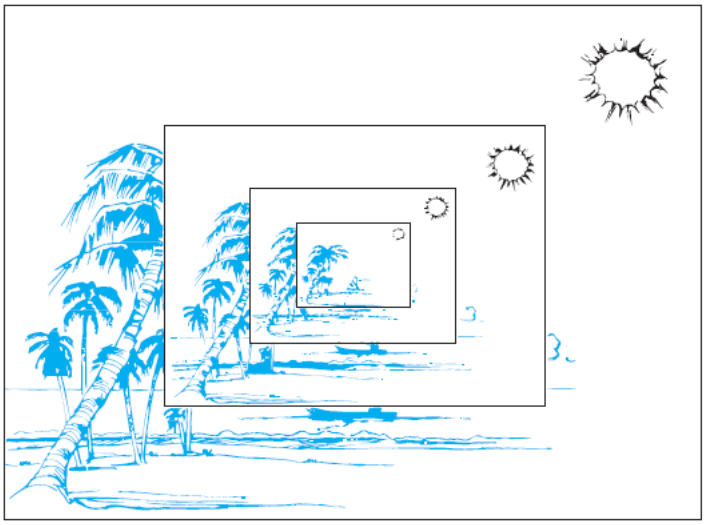


FIGURE 2 A Recursively Defined Picture.

When we define a set recursively, we specify some initial elements in a basis step and provide a rule for constructing new elements from those we already have in the recursive step. To prove results about recursively defined sets we use a method called structural induction.

Easy to define the object in terms of itself. The process of defining an object in terms of itself.

Recursively defined function

- Basis step: the Value of the function at the first Point.
- Recursive step: specifying how terms in the function are found from previous terms.

<u>Ex 9</u> Use two steps to define a function with the set of non-negative integers as it's domain (0,1,2,3,4)

- Basis step $f(0) = 0$
- Recursive step $f(n+1) = f(n) + 1 \;\; n \geq 0$

$$or\ we\ can\ write\ it\ as\ \; f(n) = f(n-1) + 1$$

Ex 10 **The sequence of powers of 2 is given by $a\_n = 2\hat{}n$ for n= 0,1,2, 3……**

- $a_0 = 2^0 = 1$
- $a_1 = 2^1 = 2$
- $a_2 = 2^2 = 4$
- $a_{n+1} = 2 * a_n$ $\quad\quad$ ***Recursive formula***

Ex 11 **Suppose that f is defined recursively by**

$f(0) = 3$

$f(n+1) = 2f(n) + 3$ $\quad\quad$ $find\ f(1), f(2), f(3)$

$f(1) = f(0+1) = 2f(0) + 3 = 2 * 3 + 3 = 9$

$f(2) = f(1+1) = 2f(1) + 3 = 2 * 9 + 3 = 21$

$Or\ f(2) = f(1+1) = 2f(1) + 3 = 2 * (2f(0) + 3) + 3$
$= 4f(0) + 6 + 3$

$= 4f(0) + 9 = 4 * 3 + 9 = 21$

$f(3) = f(2+1) = 2f(2) + 3 = 2 * 21 + 3 = 42 + 3 - 45$

Ex 12 **Give a recursive definition of the factorial function n!**

- $0! = 1$
- $1! = 1$ $\quad 2! = 2 * 1!$ $\quad 3! = 3 * 2!$ $\quad 4! = 4 * 3!$ $\quad 5! = 5 * 4!$
- $(n+1)! = (n+1) * n!$ $\quad\quad$ $n! = n * (n-1)!$

Ex 13 **The Fibonacci numbers $f_0 = 0$, $f_1 = 1$ $\quad$ $and\ f_n = f_{n-1} + f_{n-2}$ find f_5 , f_4 , f_3 , f_2**

For $n \geq 2$

- $f_2 = f_1 + f_0 = 1 + 0 = 1$
- $f_3 = f_2 + f_1 = 1 + 1 = 2$
- $f_4 = f_3 + f_2 = 2 + 1 = 3$
- $f_5 = f_4 + f_3 = 3 + 2 = 5$

Ex 14 **Give a recursive definition of** $\sum_{k=0}^{n} a_k$

- $\sum_{k=0}^{0} a_k = a_0$
- $\sum_{k=0}^{1} a_k = a_0 + a_1$
- $\sum_{k=0}^{2} a_k = a_0 + a_1 + a_2$
- $\sum_{k=0}^{3} a_k = a_0 + a_1 + a_2 + a_3$
- $\sum_{k=0}^{(n+1)} a_k = \sum_{k=0}^{n} a_k + a_{n+1}$

Recursive Definitions: "another definition" play important role in the study of strings (theory of formal language)

$$\sum set\ of\ strings\ over\ the\ alphabet\ \sum \quad is defined\ recursivery\ by$$

$$\sum = \{a, b, c, d, \dots \dots\}$$

$$\sum = \{1,2,3,4, \dots \dots\}$$

$$\sum = \{أ, ب, ت, \dots \dots\}$$

- Basis step:

$$\lambda \epsilon \sum^{*} * \quad (where\ \lambda\ is\ the\ empty\ string\ containing\ no\ symbols)$$

- Recursive step

$$if\ \omega\ \epsilon \sum^{*} *\ , x\ \epsilon \sum * \Rightarrow \omega x\ \epsilon \sum^{*} *$$

Ex 15 **let** $\sum * = \{0, 1\}$

$$\sum^{*} * = \{\lambda, 0,1,00,01,10,001,110, \dots \dots\}$$

$$\lambda \epsilon \sum^{*} * \qquad basis\ step$$

Let $00\epsilon \sum^{*}*$, $1\epsilon \sum^{*}*$ $\Rightarrow$
$001\epsilon \sum^{*}*$ *recursive step*

Ex 16 let $\sum = \{a\dashv, \vdash b\}$ show that $aab\epsilon\sum$^ *

Since $\lambda\epsilon \sum^{*}* and\ a\ \epsilon \sum* \Rightarrow\ \lambda a\epsilon \sum^{*}* \Rightarrow\ a\epsilon \sum^{*}*$

$$a\epsilon \sum^{*} * and\ a\ \epsilon \sum * \Rightarrow\ aa\ \epsilon \sum^{*} *$$

$$aa\ \epsilon \sum^{*} * and\ b\ \epsilon \sum * \Rightarrow\ aab\ \epsilon \sum^{*} *$$

Ex 17 let $\sum$ be set of symbols, $\sum^{*}*$ set of strings formed from symbols in $\sum$

The concentration of two strings recursively as follow.

1. If $\omega_1\epsilon \sum^{*}*$ and $\omega_2\epsilon \sum^{*}* and\ x\ \epsilon \sum*$ then
   $$\omega_1(\omega_2 x) = (\omega_1\omega_2)x$$
2. If ω_1 =discrete, ω_2 = mathematics $\omega_1\omega_2 = discretemathematics$
3. $\omega_1\omega_2 \neq \omega_2\omega_1$

Ex 18 Give a recursive definition of (ω) [the length of the string ω]

$l(\lambda) = 0$

$$l(\omega x) = l(\omega) + l(x) = l(\omega) + 1$$

$if\ \omega\ \epsilon \sum^{*}*\ , x\ \epsilon \sum$

Recursive Algorithm: Algorithm is called recursive if it solves a problem by reducing it to an instance of the same problem with smaller input.

Ex 19 Give a recursive algorithm for computing n! where n is non-negative integer

0! =1 basis step

n! = n * (n+1)! Recursive step

recursive algorithm for computing n!

procedure factorial (n: non-negative integer)

if n=0 then return 1

else return n*factorial (n-1)

{output is n!}

Ex 4!

n	return
4	4*f (3)
3	4*3*f (2)
2	4*3*2*f (1)
1	4*3*2*1*f (0)
0	4*3*2*1*1

Ex 20 Give a recursive algorithm for computing a^n where n is non-zero real number and n is non-negative integer.

$a^0=1$

$a^1=1$ $a^1=a*a^0$

$a^2=a*a$ $a^2=a*a^1$

$a^3=a*a*a$ $a^3=a*a^2$

algorithm

procedure power (a: non-zero real number, n: non-negative integer)

if n=0 then return 1

else return a*power (a, n-1)

{output is a^n}

Chapter 3

Number theory.

The part of mathematics devoted to the study of the set of integers and their properties is known as number theory. In this chapter we will develop some of the important concepts of number theory including many of those used in computer science. As we develop number theory, we will use the proof methods developed in Chapter 1 to prove many theorems.

We will first introduce the notion of divisibility of integers, which we use to introduce modular, or clock, arithmetic. Modular arithmetic operates with the remainders of integers when they are divided by a fixed positive integer, called the modulus. We will prove many important results about modular arithmetic which we will use extensively in this chapter.

Integers can be represented with any positive integer b greater than 1 as a base. In this chapter we discuss base b representations of integers and give an algorithm for finding them. In particular, we will discuss binary, octal, and hexadecimal (base 2, 8, and 16) representations. We will describe algorithms for carrying out arithmetic using these representations and study their complexity. These algorithms were the first procedures called algorithms.

We will discuss prime numbers, the positive integers that have only 1 and themselves as positive divisors. We will prove that there are infinitely many primes; the proof we give is considered to be one of the most beautiful proofs in mathematics. We will discuss the distribution of primes and many famous open questions concerning primes. We will introduce the concept of greatest common divisors and study the Euclidean algorithm for computing them. This

algorithm was first described thousands of years ago. We will introduce the fundamental theorem of arithmetic, a key result which tells us that every positive integer has a unique factorization into primes.

We will explain how to solve linear congruences, as well as systems of linear congruences, which we solve using the famous Chinese remainder theorem. We will introduce the notion of pseudoprimes, which are composite integers masquerading as primes, and show how this notion can help us rapidly generate prime numbers.

This chapter introduces several important applications of number theory. In particular, we will use number theory to generate pseudorandom numbers, to assign memory locations to computer files, and to find check digits used to detect errors in various kinds of identification numbers. We also introduce the subject of cryptography. Number theory plays an essentially role both in classical cryptography, first used thousands of years ago, and modern cryptography, which plays an essential role in electronic communication. We will show how the ideas we develop can be used in cryptographical protocols, introducing protocols for sharing keys and for sending signed messages. Number theory, once considered the purest of subjects, has become an essential tool in providing computer and Internet security.

3.1 Division

if a, b are integers; a ≠ 0 then a divides b if there an integer c such that $b = a * c$ $\frac{b}{a} = c$

Note a is factor of b. b is multiple of a

a/b a divides b a ∤ b a not divide b

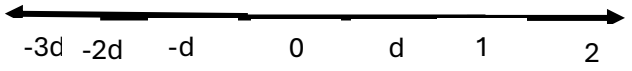
a/b a divided by b

Ex 1 **Determine whether 3\7 and 3\12 are divisible or not.**

$3 \not\backslash 7 \Rightarrow \frac{7}{3}$ $\neq not\ integer$ X

$3 \backslash 12 \Rightarrow \frac{12}{3} = 4$ √

Ex 2 **A number line indicates which integer are divisible by the +ve integer d.**



$\frac{0}{d} = 0$ $d \backslash 0$

$\frac{\pm kd}{d} = \pm k$ $d \backslash \pm kd$

Ex 3 **let n and d be +ve integers how many +ve integers not exceed n are divisible by d?**

$\frac{??}{d}\ in\ condition\ ??\leq n \Rightarrow\gg= kd$

$0 < kd \leq n \quad ; k\epsilon z^{+}$ $0 < k \leq \frac{n}{d}$

$if\ \frac{n}{d}\ integer$ √

$if\ \frac{n}{d}\ notinteger$ $X \Longrightarrow approximate\ to\ minimum$

Number of +ve integers not exceeding n are divisible by d [n\d]

Note

Floor function $\lfloor x \rfloor$ approximate to minimum

ceiling function $\lceil x \rceil$ approximate to maximum

greatest integer function ($[x]$)

x	$\lfloor x \rfloor$	$\lceil x \rceil$	$(\lfloor x \rfloor)$
2	2	2	2
2.001	2	3	$2 \Rightarrow 2 \leq 2.001 \leq 3$
2.4	2	3	$2 \Rightarrow 2 \leq 2.001 \leq 3$
-2.7	-3	-2	$-3 \Rightarrow -3 \leq -3 \leq -3$
-5	-5	-5	$-5 \Rightarrow -5 \leq -5 \leq -5$

<u>Ex 4</u> how many +ve integers not exceeding 80 are divisible by 3?

$$0 < kd \leq n$$

$$0 < 3k \leq 80 \qquad \Rightarrow \qquad \left\lfloor \frac{80}{3} \right\rfloor = 26$$

$$0 < k \leq \frac{80}{3} \qquad \Rightarrow \qquad \frac{80}{3} = 26.66667$$

Theorem: let a, b and c be integers where a ≠ 0, then

(i) $if\ a \backslash b\ and\ a \backslash c\ \Rightarrow a \backslash (b + c)$
(ii) $if\ a \backslash b\ \Rightarrow a \backslash bc\ \ , c\ integer$
(iii)$if\ a \backslash b\ and\ b \backslash c\ \Rightarrow \backslash c$

Result

$if\ a \backslash b\ and\ a \backslash c\ \Rightarrow a \backslash (mb + nc)\ , where\ m\ and\ n\ are\ integers$

<u>Ex 5</u> Does the following is true or not.

- $2\ is\ divided\ by\ 4?\ \frac{4}{2} = 2\ true$
- $2\ is\ divided\ by\ 8\ ?\ \frac{8}{2} = 4\ true$
- $2\ is\ divided\ by\ (4 + 8)?\ \frac{(4+8)}{2} = 6\ true$

- $2\ is\ divided\ by\ 4?\ \frac{4}{2} = 2\ true$
- $2\ is\ divided\ by\ 4 * 5?\ \frac{4*5}{2} = 10\ true$

- $2\ is\ divided\ by\ 4?\ \frac{4}{2} = 2\ true$
- $4\ is\ divided\ by\ 16?\ \frac{16}{4} = 4\ true$

- $2\ is\ divided\ by\ 16?\ \frac{16}{2} = 8\ true$

The division algorithm: let a be integer, d be +ve integer, then $\frac{a}{d} = q$ a is dividend m d is divisor and q is quotient and r is reminder where $0 \leq r < d\ \ r\ is\ not\ negative$

$$a = dq + r$$

$$r = a\ mod\ d$$

$$r = a - dq$$

<u>Ex 6</u> what are the quotient and reminder when 101 is divided by 11.

$$q = \left\lfloor \frac{101}{11} \right\rfloor = 9 \quad \Longrightarrow\ 101\ div\ 11 = 9$$

$$r = 101 - 11 * 9 = 2 \quad \Longrightarrow \quad 101\ mod\ 11 = 2$$

<u>Ex 6</u> what are the quotient and reminder when -11 is divided by 3.

$$q = \left\lfloor \frac{-11}{3} \right\rfloor = -4 \quad \Longrightarrow\ -11\ div\ 3 = -4$$

$$r = -11 - 3 * -4 = 1 \quad \Longrightarrow \quad -11\ mod\ 3 = 1$$

<u>Ex 7</u> evaluates.

- $11\ mod\ 2 = 1\ \Rightarrow \frac{11}{2} = 5 \Longrightarrow r = 11 - 2 * 5 = 11 - 10 = 1$
- $-11\ mod\ 2 = 1\ \Rightarrow \frac{-11}{2} = -5 \Longrightarrow r = -11 - 2 * -5 = -11 + 10 = 1$

<u>Note</u>

- $a \backslash b\ \Leftrightarrow -a \backslash b$

Ex 8 Show that if a is an integer, then $1\backslash a$

$$q = \left\lfloor \frac{a}{1} \right\rfloor = a$$

$$r = a - 1 * a = 0 \Longrightarrow 1\backslash a$$

Ex 9 Show that if a is an integer greater then 0, then $a\backslash 0$

$$q = \left\lfloor \frac{0}{a} \right\rfloor = 0$$

$$r = 0 - a * 0 = 0 \Longrightarrow a\backslash 0$$

Modular arithmetic

Ex 10 What time does a 24-hour clock read 100 hours after it read 2:00

$r = 102\ mod\ 24 = 6$

$r = 102 - 24 * 4 = 6$

Relation between two integers have the same reminder.

Let $a\ mod\ m = c$ and

$b\ mod\ m = c$

Found relation between a and b.

Definition: a, b are integers and m are +ve integers $\Longrightarrow$ a is congruent to b model

1. $a\ mod\ m = b\ mod\ m \Leftrightarrow a \equiv b(mod\ m)$
2. $a \equiv b(mod\ m) \Leftrightarrow m(a - b)$
3. $a \equiv b(mod\ m) \Leftrightarrow integer\ k\ a = b + km$

Ex 11 **Decide whether each of these integers is congruent to 5 module 6**

1. **17**
2. **24**

$$17 \equiv 5\ (mod\ 6)$$

$$6\backslash(17-5) = \frac{17-5}{6} = 2 \qquad r = 0$$

Or

$$17\ mod\ 6 = 5 \qquad r = 17 - 6 * 2 = 5$$

$$6\ mod\ 5 = 5 \qquad r = 5 - 6 * 0 = 5$$

$$24 \not\equiv 5\ (mod\ 6)$$

Ex 12 **list five integers that are congruent to 2 module to 4**

$$a \equiv b(mod\ m) \Leftrightarrow a = b + mk$$

$$\frac{a-b}{m} = \frac{a-2}{4} = k \qquad integer$$

$$a - 2 = 4k \Rightarrow a = 4k + 2$$

k	a
0	2
1	6
2	10
3	14
4	18

Ex 13 **list all integers between -100 and 100 that are congruent to -1 module 25**

$$a \equiv -1(mod\ 25) \Leftrightarrow a = -1 + 25k$$

$$-100 < a < 100$$

$$-100 < -1 + 25k < 100$$

$$-99 < 25k < 101$$

$$-3.96 < k < 4.04$$

$$k = -3, -2, -1, 0, 1, 2, 3, 4$$

$$at\ k = -3 \Rightarrow a = -1 + (25 * -3) = -76$$

$$at\ k = 4 \Rightarrow a = -1 + (25 * 4) = 99$$

Ex 14 Suppose that a is integer $\boldsymbol{a \equiv 4(mod\ 13)}$

Find the integer C with $0 \leq C \leq 12\ such\ that\ c \equiv 9a(mod\ 13)$

Let

$$a \equiv 4(mod\ 13) \Leftrightarrow a = 4 + 13k$$

$$k = 0 \Rightarrow a = 4$$

$$k = 1 \Rightarrow a = 17$$

$$C = 9a(mod\ 13)$$

$$C = 36(mod\ 13) = 10$$

$$C = 9 * 17(mod\ 13) = 10$$

And so, on

Theorem: let m be +ve integer and let a, b, c, d are integers

$$if\ a \equiv b(mod\ m),\quad c \equiv d(mod\ n)$$

$$a + c \equiv b + d(mod\ m)$$

$$a * c \equiv b * d(mod\ m)$$

Ex 15 $\boldsymbol{7 \equiv 2(mod\ 5)}$

$$\boldsymbol{11 \equiv 1(mod\ 5)}$$

$$\boldsymbol{7 + 11 \equiv (2 + 1)(mod\ 5)}$$

$$\boldsymbol{7 * 11 \equiv (2 * 1)(mod\ 5)}$$

Corollary (1): let m be +ve integer and let a, b are integers then.

$$(a+b)modm = \big((a\ md\ m) + (mod\ m)\big)$$

Ex 16 **Evaluate**

$$(-133\ mod\ 23 + 261\ mod\ 23)mod\ 23$$

$$= (-133 + 261)mod\ 23 = 128\ mod\ 23 = 13$$

Corollary (2): let m be +ve integer and let a, b are integers then.

$$(ab)mod\ m = \big((a\ mod\ m\ )(\ b\ mod\ m)\big)mod\ m$$

$$a^2 mod\ m = \big((a\ mod\ m\ )(\ a\ mod\ m)\big)mod\ m$$

$$a^4 mod\ m = \big((a^2\ mod\ m\ )(\ a^2\ mod\ m)\big)mod\ m$$

Ex 17 **Evaluate**

$$(3^4 mod 17)^2 mod 11$$

$$3^1 mod 17 = 3$$

$$3^2 mod 17 = 9$$

$$3^4 mod 17 = \big((3^2 mod\ 17) * (3^2 mod\ 17)\big)mod 17 = 81 mod\ 17$$
$$= 13$$

$$13^2 mod\ 11 = \big((13\ mod\ 11) * (13\ mod\ 11)\big)mod\ 11$$
$$= 2 * 2\ mod\ 11 = 4\ mod\ 11 = 4$$

Ex 18 **Evaluate**

$$5^{11}\ mod 12$$

$$5^1 * 5^2 * 5^8\ mod 12$$

$$5^1\ mod 12 = 5$$

$$5^2\ mod 12 = 25\ mod\ 12 = 1$$

$$5^4\ mod 12 = 1\ mod\ 12 = 1$$

$$5^8 \, mod 12 = 1 \, mod \, 12 = 1$$

$$5^{11} \, mod 12 = 5^1 * 5^2 * 5^8 \, mod 12 = 5 * 1 * 1 = 5$$

$$5^{11} \, mod 12 = 5$$

3.2 Integer representation: integer can be expressed using any integer greater than one as

1. Decimal (base 10)
2. Binary (base 2)
3. Octal (base8)
4. Hexadecimal (base 16)

Theorem: base b expression of n

let b an integer >1 then n is a +ve integer, it can be expressed uniquely in the form.

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0 b^0$$

$$(a_k, a_{k-1}, a_{k-2}, \ldots., a_1, \ a_0)_b$$

Where k is a non-negative integers $a_k, a_{k-1}, a_{k-2}, \ldots., a_1, a_0$ less then b and $a_k \neq 0$

Example

$$(983)_{10} = 9 * 10^2 + 8 * 10^1 + 3 * 10^3$$

Decimal expression: the decimal numbering system has 10 digits (0, 1, 2, …, 9)

Example 12234_{10} , 1100_{10} , 30_{10}

Binary expression: the binary notaton each digit is either 0 or 1

Example 11100010101010_2

<u>Ex 19</u> what is the decimal expression of the integer has $(10101)_2$ as its binary expression.

$(10101)_2 = 1*2^4 + \cancel{0*2^3} + 1*2^2 + \cancel{0*2^1} + 1*2^0 = 21$

$(10101)_2 = (21)_{10}$

Octal (base 8) and Hexadecimal (base 16): expressing they using characters, such as letters and digits

Octal expression base b=8

Octal digits used (0, 1, 2, 3, 4, 5, 6, 7) example 765_8 , 427_8

<u>Ex 20</u> what is the decimal expression of $(7016)_8$ as its octal expression

$(7016)_8 = 7*8^3 + 0*8^2 + 1*8^{1+}6*8^0 = (3598)_{10}$

$(7016)_8 = (3598)_{10}$

hexadecimal expression base b=16

Hexadecimal digits used (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F) example $7AC_{16}$, $4FD_{16}$

<u>Ex 21</u> what is the decimal expression of $(2AE0B)_{16}$ as its hexadecimal expression

$(2AE0B)_{16} = 2*16^4 + 10*16^3 + 14*16^2 + 0*161 + 11*16^0 = (175627)_{10}$

<u>Ex 22</u> Convert the following binary numbers to decimal

1. **011010_2**

$\cancel{0}$	**1**	**1**	**$\cancel{0}$**	**1**	**0**
$\cancel{2^5}$	**2^4**	**2^3**	**$\cancel{2^2}$**	**2^1**	**2^0**

$011010_2 = 1*2^4 + 1*2^3 + 1*2^1 = (26)_{10}$

2. **10011_2**

1	**$\cancel{0}$**	**$\cancel{0}$**	**1**	**1**
2^4	**$\cancel{2^3}$**	**$\cancel{2^2}$**	**2^1**	**2^0**

$110011 == 1*2^4 + 1*2^3 + 1*2^0 = 25$

3. **10001.101_2**

1	**~~0~~**	**~~0~~**	**~~0~~**	**1**	**1**	**~~0~~**	**1**
2^4	**~~2^3~~**	**~~2^2~~**	**~~2^1~~**	**2^0**	**2^{-1}**	**~~2^{-2}~~**	**2^{-3}**

10001.101_2 = $1*2^4+1*2^0+1*2^{-1}+1*2^{-3}=17.625$

Convert decimal to binary: it's made by dividing on 2 and tack the reminder

Ex Convert 75_{10} to binary.

75	2	1
37	2	1
18	2	0
9	2	1
4	2	0
2	2	0
1	2	1
0		

$(11)_{10}$ =??$_2$

11	2	1
5	2	1
2	2	0
1	2	1
0		

$(11)_{10}$ =1011_2

Converting decimal and binary to hexadecimal table

Hexadecimal	Decimal	binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110

7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Ex 23Convert $5CA_{16}$ to binary

$5CA_{16} = 010111001010_2$

Ex 23Convert $C40E_{16}$ to binary

C	**4**	**0**	**E**
12	**4**	**0**	**14**
1100	**0100**	**0000**	**1110**

$C40E_{16} = 1100010000001110_2$

Convert to binary.

- $10A7_{16}$
- $D85C_{16}$

Ex 20 Convert from binary to hexadecimal

1101100001011100_2

1. Divide each 4 digit as number 1101 1000 0101 1100
2. Convert each number separately.

1101	1000	0101	1100
13	8	5	12
D	8	5	C

$1101100001011100_2 = D85C_{16}$

Addition in binary

0+0=0

1+0=1

0+1=1

1+1=0 and reminder 1

<u>Ex 21</u> Add 101100+11010.

1	1	1				
	1	0	1	1	0	0
↓	↓	1	1	0	1	0
1	0	0	0	1	1	0

Multiplication in binary

ab= $a(b_0 2^0 + b_1 2^1 + \cdots + b_k 2^k = ab_0 2^0 + ab_1 2^1 + \cdots + ab_k 2^k$

<u>Ex 22</u> Multiply 110 and 101

			1	1	0
			1	0	1
0	0	0	1	1	0
0	0	0	0		
	1	1	0		
0	1	1	1	1	0

3.3 Primes: +ve integer p >1 is called prime if the only +ve factor of P is 1 and P "if P is not prime called composite"

Example

- 7 is prime $\frac{7}{1}, \frac{7}{7}$
- 9 is composite $\frac{9}{3}, \frac{9}{1}, \frac{9}{9}$
- 1 is not prime because it has only one +ve factor.

- N is composite integer ⇔ an integer a ≡ a\n 1< a< n

Theorem “fundamental theorem of arithmetic”:

Every integer >1 can be written uniquely as a prime or as the product of two or more primes. If n is composite integer, them n equal to $\sqrt{n}$

Example the integer 100 is prime or not.

$$the\ prime\ number\ \leq \sqrt{100} \Rightarrow 2,3,5,7$$

$$\frac{100}{2}\ is\ integar\ numeber\ \Rightarrow 100\ is\ not\ prime$$ "compsit

<u>Ex 23</u> the integer 101 is prime or not

$$the\ prime\ number\ \leq \sqrt{101} \Rightarrow 2,3,5,7$$

$$\frac{101}{2}\ is\ \ not\ integar\ numeber$$

$$\frac{101}{3}\ is\ \ not\ integar\ numeber$$

$$\frac{101}{5}\ is\ \ not\ integar\ numeber$$

$$\frac{101}{7}\ is\ \ not\ integar\ numeber$$

101 is a prime number.

Ex 24 **Find the prime factorization of 100.**

2	100
2	50
2	25
5	5
5	1

$$100 = 2 * 2 * 5 * 5$$

Ex 25 **Find the prime factorization of 1001.**

$$the\ prime \leq \sqrt{1001} \quad are \quad 2, 3, 5, 7, 11, 13, 17, \ldots.$$

$$the\ prime \leq \sqrt{143} \quad are \quad 2, 3, 5, 7, 11$$

$$the\ prime \leq \sqrt{13} \quad are \quad 2, 3$$

1001=7*11*13

7	1001
11	143
13	13
	1

3.4 Greatest common divisor "GCD": let a and b be integers, not booth zero the largest integer.

$$d \ni d\backslash a, d\backslash b\ is\ called \gcd of\ a\ and\ b \gcd(a, b)$$

$$a = P_1^{a_1}\ P_2^{a_2}\ \ldots\ldots P_n^{a_n}$$

$$b = P_1^{b}\ P_2^{b_2}\ \ldots\ldots P_n^{b_n}$$

$$\gcd(a, b) = P_1^{\min(a_1, b_1)}, P_2^{min(a_2, b_2)}, \ldots\ldots P_n^{min(a_n, b_n)}$$

Ex 26 **What is the greatest common divisor of 24, 36.**

2	24
2	12
3	6
2	2
	1

2	36
2	18
3	9
3	3
	1

$\sqrt{24}$ *are* 2,3 $\sqrt{36}$ *are* 2,3

$24 = 2^3 * 3^1$ $36 = 2^2 * 3^2$

$$\gcd(24,36) = 2^{\min(3,2)} * 3^{\min(1,2)} = 2^2 * 3^1 = 4 * 3 = 12$$

Ex 27 What is the greatest common divisor of , 500.

2	120	2	500
2	60	2	250
2	30	5	125
5	15	5	25
3	3	5	5
	1		1

$\sqrt{120}$ *are* 2,3,5 $\sqrt{500}$ *are* 2,5

$120 = 2^3 * 3^1 * 5^1$ $500 = 2^2 * 5^3$

$$\gcd(120,500) = 2^{\min(3,2)} * 5^{\min(1,3)} = 2^2 * 5^1 = 4 * 5 = 20$$

Note: the integers a and b are relativity prime if their gcd is 1

Example 17 and 22 are relativity prime because the gcd (17,20) =1

The integers $a_1, a_2, \ldots a_{n-1}, a_n$ one pairwise relativity prime if gcd $(a_i, a_j)=1$

When ever $1 \leq i < j \leq n$

Ex 28

1. **Found if the integers 10, 17, 21 pairwise relatively prime or not.**
2. **Found if the integers 10, 19, 24 pairwise relatively prime or not.**
    1. gcd (10, 17) =1

       gcd (10, 21) =1

       gcd (17, 21) =1

10, 17, 21 are pairwise relatively prime

2. gcd (10, 24) =2 ≠1

   10, 19, 24 are not pairwise relatively prime

3.5 Least common multiple "LCM": the least common multiple of +ve integers a, b is the smallest +ve integer that is divisible by both a and b

$$\gcd(a,b) = P_1^{\max(a_1,b_1)}, P_2^{\max(a_2,b_2)}, \dots \dots P_n^{\max(a_n,b_n)}$$

Example: found lcm of 24, 36 and 120, 500

$$lcm(24{,}36) = 2^3 * 3^2 = 8 * 9 = 72$$

$$lcm(120{,}500) = 2^3 * 5^3 * 3^1 = 8 * 125 * 3 = 3000$$

Theorem: let a, b +ve integers then ab=gcd (a, b) * lcm (a, b)

Methods of finding gcd

1. **The Euclidean algorithm:** let a=bq+r where a, b, q, r are integers then

   gcd (a, b) = gcd (b, r) if r=0, then gcd (a, b) = b

Ex 29

Evaluate gcd (414, 662)
Assum that 414 is a and 662 is b

$$\frac{662}{414} \Longrightarrow q = 1, r = 248$$
$$\frac{414}{248} \Longrightarrow q = 1, r = 166$$
$$\frac{248}{166} \Longrightarrow q = 1, r = 82$$
$$\frac{166}{82} \Longrightarrow q = 2, r = 2$$
$$\frac{82}{2} \Longrightarrow q = 41, r = 0$$

gcd (a, b) =gcd (662, 414) = gcd (b, r) =gcd (82, 2)=2

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	662	414	1	248
1	414	248	1	166
2	248	166	1	82
3	166	82	2	2
4	82	②	41	⓪

If r=0 gcd (a, b) =b=2

2. **Bézout's theorem**: gcd (a, b) can be expressed as a linear combination.
   gcd (a, b) = Sa +tb
   we set S_0 =1 and S_1=0 and t_0 =0 and t_1=1
   $S_j = S_{j-2} - q_{j-1} S_{j-1}$
   $t_j = t_{j-2} - q_{j-1} t_{j-1}$
   where j=2,3,….n

Ex 30

Evaluate gcd (252, 198) using Bézout's theorem.

	A	b				
j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	S_j	t_j
0	252	188	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
4					④	⊖⑤

4a-5b=18

gcd (252, 198) = 18

3.6 Applications

1. **Hashing function** "Find the memory location ": h(k) = k mod m

Example: Find the memory location by the hashing fun h(k) = k mod 111 to the records of customer with social security number 064212848 and 037149212

h (064212848) = 064212848 mod 11= 14

h (037149212) = 037149212 mod 11= 65

2. **Pseudorandom number** its use in simulation and cryptography
   Linear congruential method

$$x_{n+1} = (ax_n + c) mod\ m$$

$$x_0 \Rightarrow seed,\quad a \Rightarrow multiplier\quad c \Rightarrow increment\quad m \Rightarrow moduls$$

Example m=9, a=7, c=4, x_0=3

$$x_1 = (7x_0 + 4) mod\ 9 = 25\ mod\ 9 = 7$$

$$x_2 = (7x_1 + 4) mod\ 9 = 53\ mod\ 9 = 8$$

$$x_3 = (7x_2 + 4) mod\ 9 = 60\ mod\ 9 = 6$$

$$x_9 = (7x_8 + 4) mod\ 9 = 39\ mod\ 9 = 3$$

Then the numbers will repeat again so m must be great number to prevent any when tp knew how large the cycle is

3. **Cryptography**

$f(p) = (p + k) mod\ m$ $\qquad$ $encryption$

$f(p) = (p - k) mod\ m$ $\qquad$ $dycryption$

Where m: number of elements in the language used

Example To encrypt the message “stop global warming”.

m= 26 the number of English alphabet

use k =11

S	T	O	P	G	L	O	B	A	L	W	A	R	M	I	N	G
18	19	14	15	6	11	14	1	0	11	22	0	17	12	8	13	6

$$f(p) = (p + k) mod\ m$$

$$f(18) = (18 + 11) mod\ 26$$

Repeat the iteration for every character the final is

3	4	25	0	17	22	25	12	11	22	7	11	2	23	19	24	17
D	E	Z	A	R	W	Z	M	L	W	H	L	C	X	T	Y	R

Chapter 4

Graph theory.

Introduction

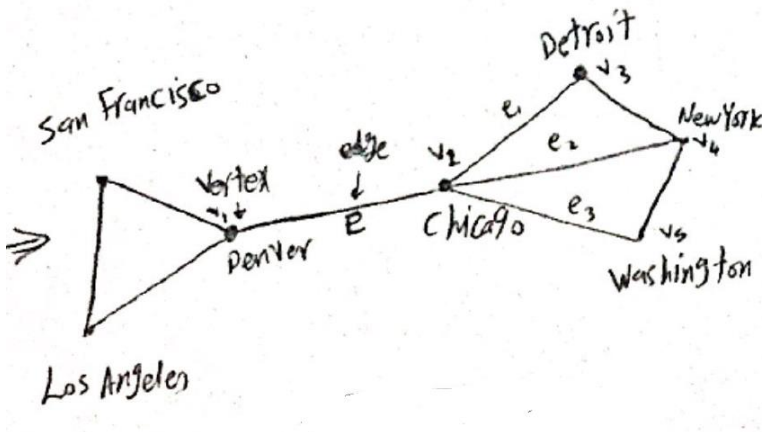
Graphs are discrete structures consisting of vertices and edges that connect these vertices. There are different kinds of graphs, depending on whether edges have directions, whether. multiple edges can connect the same pair of vertices, and whether loops are allowed. Problems in almost every conceivable discipline can be solved using graph models. We will give examples to illustrate how graphs are used as models in a variety of areas. For instance, we will show how graphs are used to represent the competition of different species in an ecological niche, how graphs are used to represent who influences whom in an organization, and how graphs are used to represent the outcomes of round-robin tournaments. We will describe how graphs can be used to model acquaintanceships between people, collaboration between researchers, telephone calls between telephone numbers, and links between websites. We will show how graphs can be used to model roadmaps and the assignment of jobs to employees of an organization.

Using graph models, we can determine whether it is possible to walk down all the streets in a city without going down a street twice, and we can find the number of colors needed to color the regions of a map. Graphs can be used to determine whether a circuit can be implemented on a planar circuit board. We can distinguish between two chemical compounds with the same molecular formula but

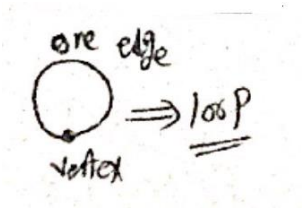
different structures using graphs. We can determine whether two computers are connected by a communications link using graph models of computer networks. Graphs with weights assigned to their edges can be used to solve problems such as finding the shortest path between two cities in a transportation network. We can also use graphs to schedule exams and assign channels to television stations. This chapter will introduce the basic concepts of graph theory and present many different graph models. To solve the wide variety of problems that can be studied using graphs, we will introduce many different graph algorithms. We will also study the complexity of these algorithms.

4.1 Graphs

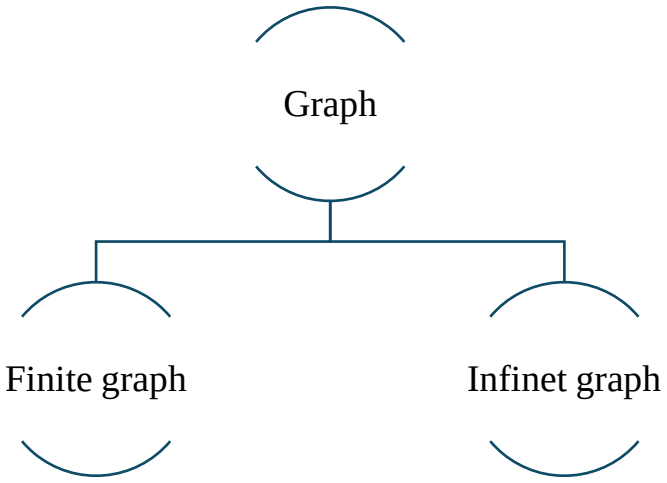
Definition: a graph G = (V, E) consists of V (a non-empty set of vertices) or nodes and E (a set of edges). Each edge has either one or two vertices associated with it, called its endpoint an edge is said to connect it's endpoints.



Computer network



Remark



Finite graph

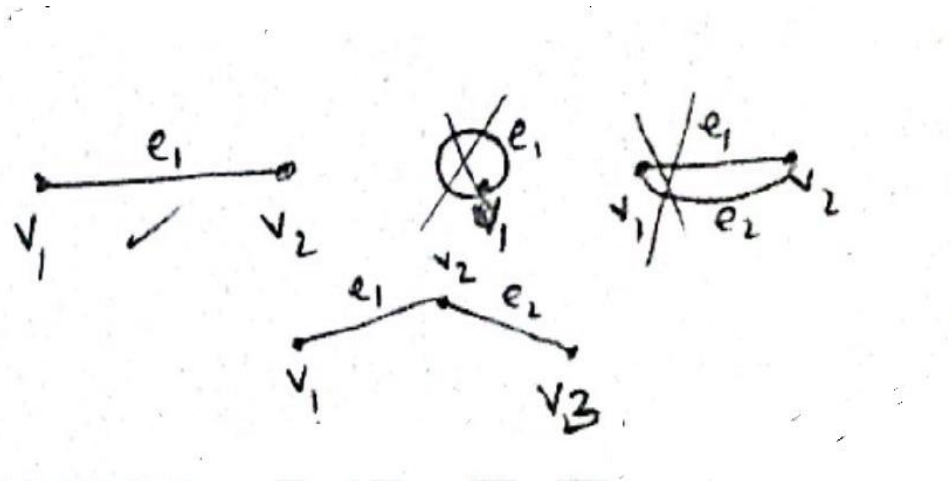
- Finite vertex set.
- Finite edge set

Infinite graph

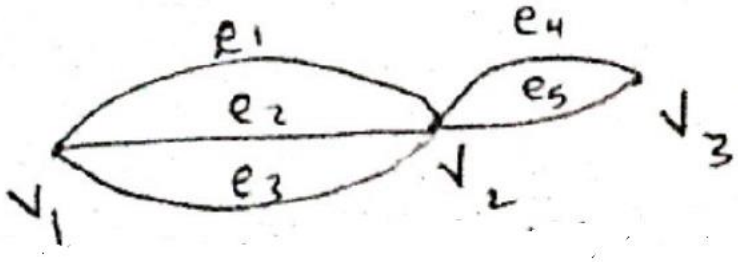
- Infinite vertex set.
- Infinite edge set

Types of undirected graph

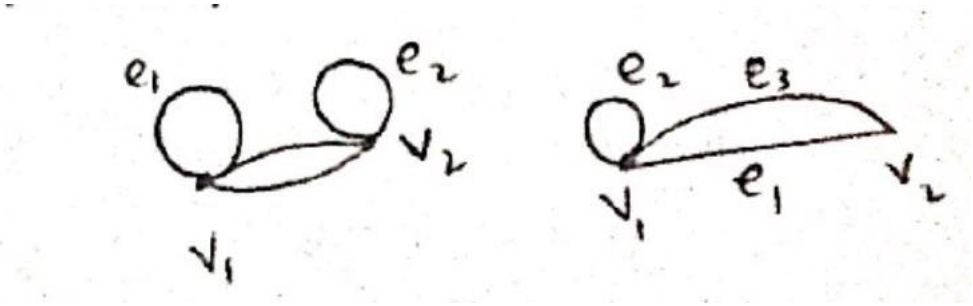
Simple graph: "each edge of the graph connects two different vertices and where no two edge connect the same pair of vertices."



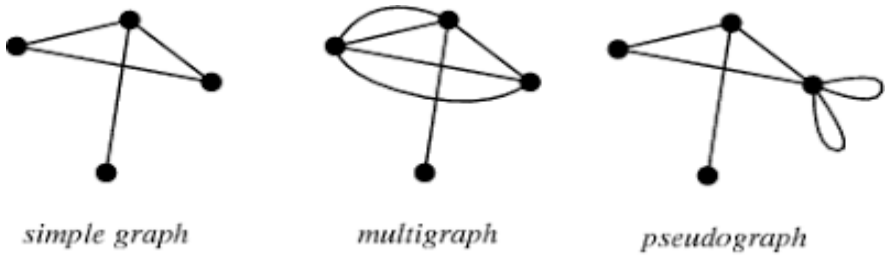
Multigraph: graphs that may multiple edges connecting the same vertices"



Loop: "edge that connect a vertex to itself" self-edge.

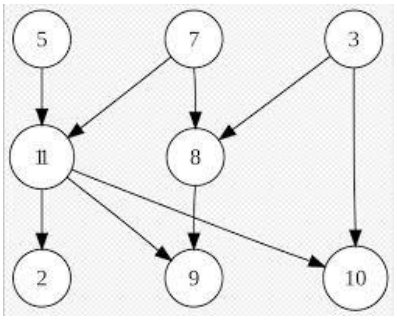


Pseudo graph: graph that may include loop, and possibly multiple edges connecting the same pair of vertices or a vertex to itself.

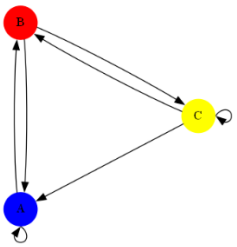


Undirected graph

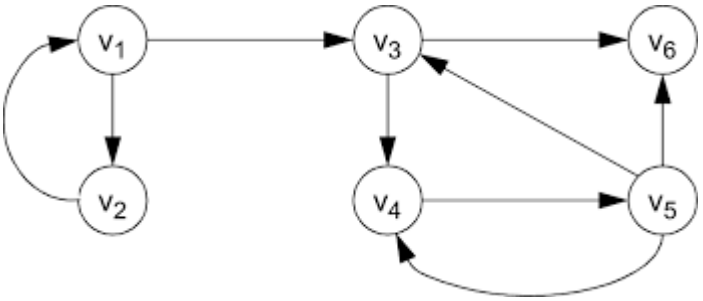
Directed graph: “digraph” (V, E) Consists of a nonempty set of vertices V and a set of directed edges (arcs) E. Each edge is associated with an ordered Pairs of vertices.



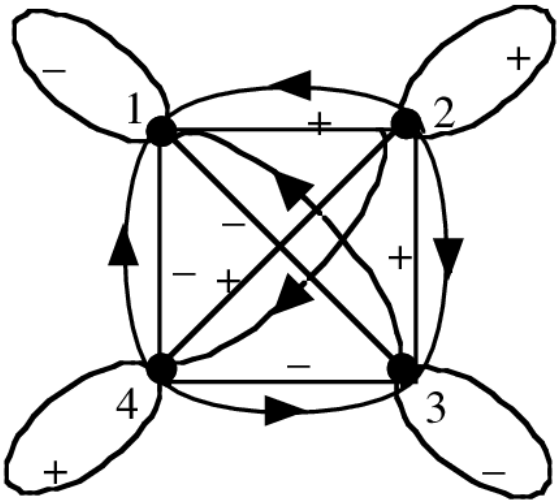
Simple directed graph: "when a directed graph has no loops and has no multiple directed edges."



Directed multigraphs: have multiple directed edges from vertex to a second Vertex (Possibly the same vertex)



Mixed graph: "For some models may need a graph where some edges one undirected, while other one directed



Comparison between different type of graph

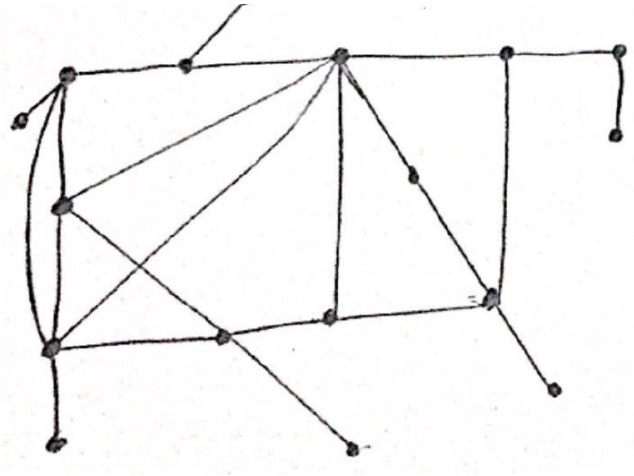
Type	Edges	Multi edges allow	Loops allow
Simple graph	Undirect	X	X
Multi graph	Undirect	√	X
Pseudo graph	Undirect	√	√
Simple direct	Direct	X	X
Multi direct	Direct	√	√
Mixed graph	Direct	√	√

4.2 Graph models: graphs one used in a wide variety of models.

- ❖ Social Networks.
- ❖ Communication
- ❖ Information
- ❖ Transportation
- ❖ Biological
- ❖ Software design Applications
- ❖ Tournaments.
- ❖ Other.

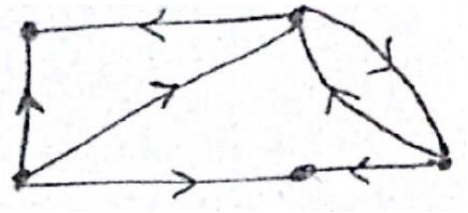
Social Networks

Social structures based on different kinds of relationships between People or groups of People. acquaintanceship and friendship Graphs (Simple graph) as Facebook "virtual word"



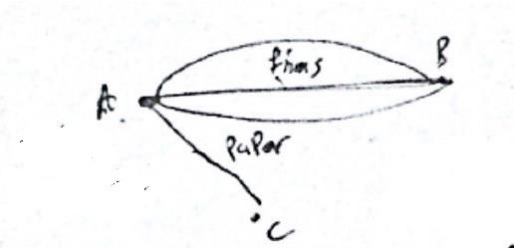
Undirect simple graph

Inference graphs: In studies of group behavior, it is observed that Certain People Con influence the thinking of others.



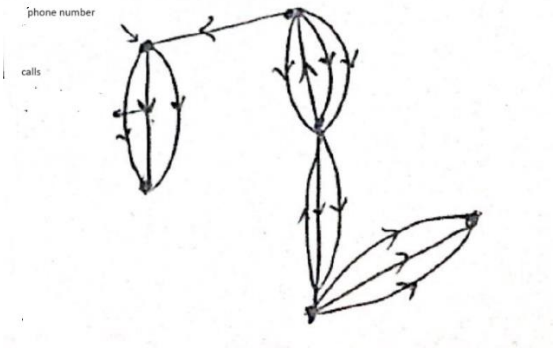
Simple direct graph

Collaboration Graphs: (Hollywood links graph)



Multiple graph with more than 2.9 million vertex till 2018

Communication Networks: "Call graphs" graphs can be used to model telephone Calls made in a network.

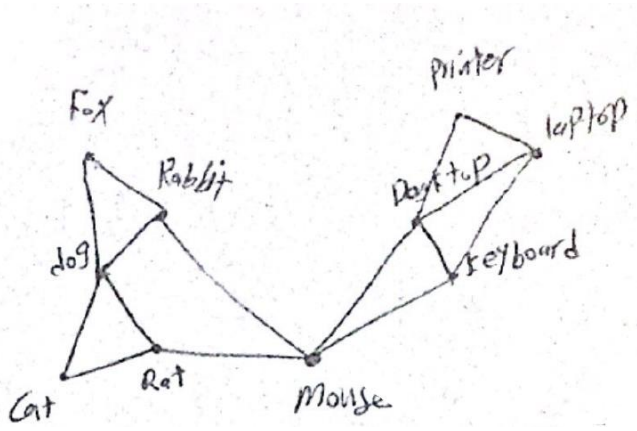


Multi graphs

Transportation Networks: we can use graphs to model many different types of transportation networks (road, air, shipping, _) like underground metro network in Egypt.

Biological Networks: Many aspects of the biological sciences Can be modeled using graphs. (Protein interaction graphic): A Protein interaction in a living Cell occurs when two or more proteins in that Cell bind to perform a biological function.

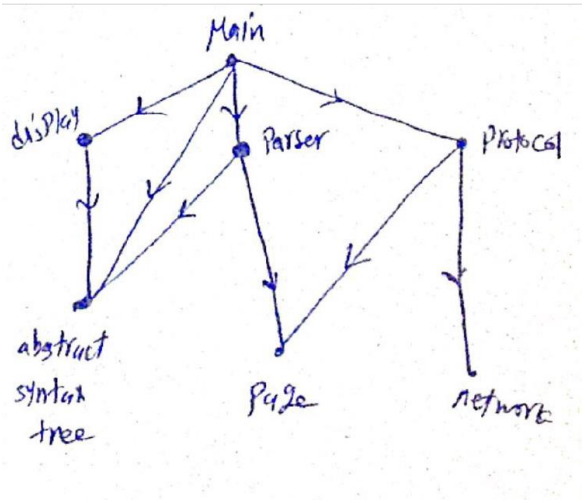
Semantic Networks: graphs models one used extensively in natural language understanding (NLU). the subject of enabling machine, to is assemble and Parse human speech Its, goal is to allow machines to understand and communicate as human do.)



Software design Applications: graphs models one useful tools in the design of software

(Modelle dependency graphs):

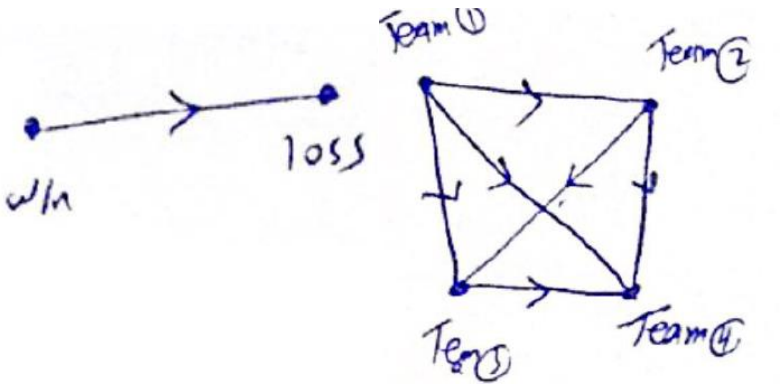
- how to structure a program into different Parts
- Understanding how the different modules of a program interact



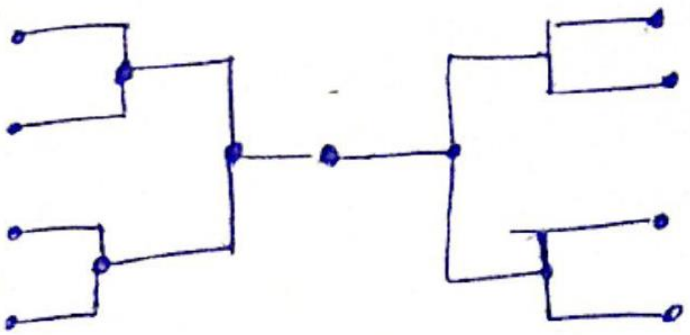
Web browser graph

Tournaments:

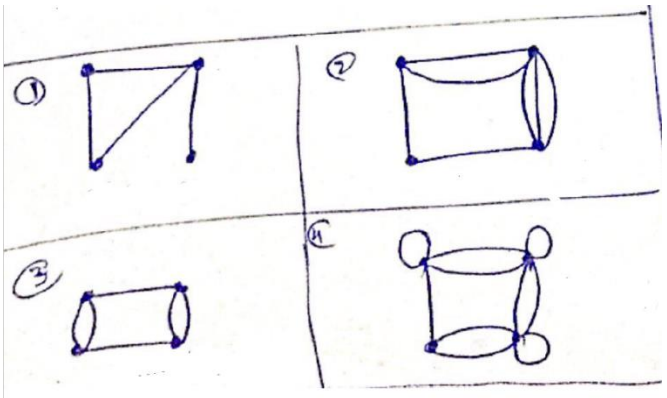
1. **Round-robin tournament:** each team plays every other team exactly once and no draws one allowed.

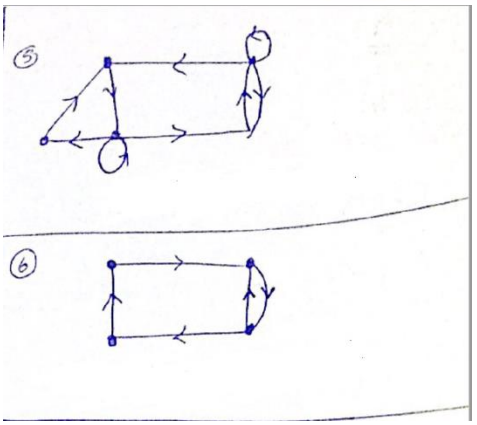


Single-elimination tournament: each contestant is eliminated after one lose.



Example (1): determine the type of the graphs.





Example (2): construct the intersection graph of these collection of sets.

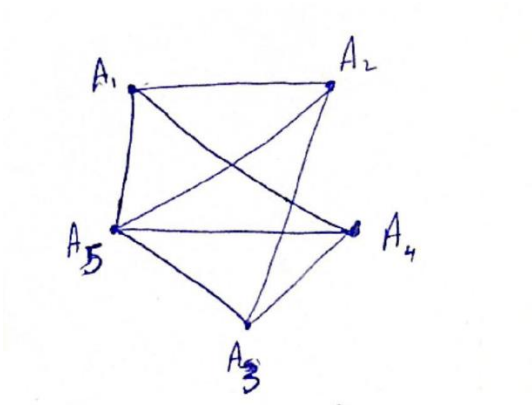
A_1= {0, 2, 4, 6, 8}

A_2= {0, 1, 2, 3, 4}

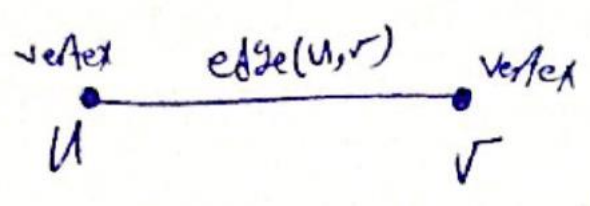
A_3= {1, 3, 5, 7, 9}

A_4= {5, 6, 7, 8, 9}

A_1= {0, 1, 8, 9}

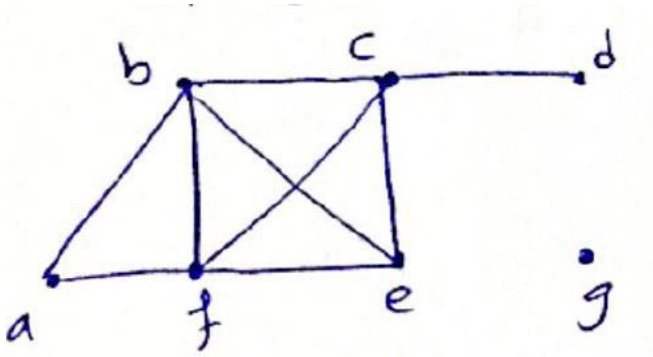


4.3 Basic graph terminology: two vertices U and V in an undirected graph G are called adjacent (neighbors) in G if U and V are endpoints of an edge e of G.



edge(e) is called incident with the vertices U and V

Neighborhood of Vertex (V) N(V): Set of all neighbors of a vertex. V of G= (V, E)



- **N(a)= {b, f)**
- **N (b)= {a, c, f, e)**
- **N(e)= {b, f, c}**
- **N(c)= {b, f, e, d}**
- **N(d)= {c}**
- **N(g)=ϕ**

Remek: If A is subset of V, then the set of all Vertices in G that are adjacent to at least one.

Vertex in A N(A)=U N(V) V€A

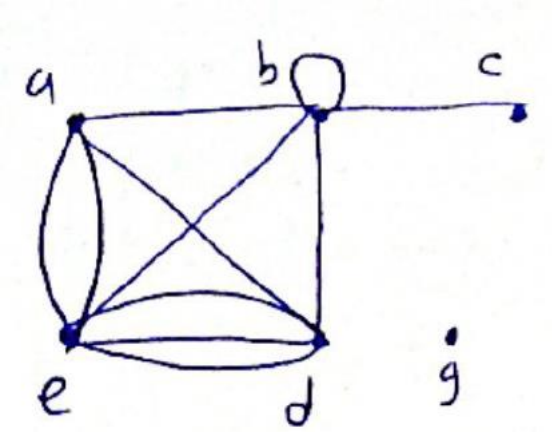
The degree of a vertex (undirected graph): it's the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex.

- deg (a)=2
- deg (b)=4
- deg (e)=3
- deg (c)=4
- deg (d)=1
- deg (g)=0

Isolated: is a vertex of degree zero (is not adjacent to any vertex) vertex g is isolated.

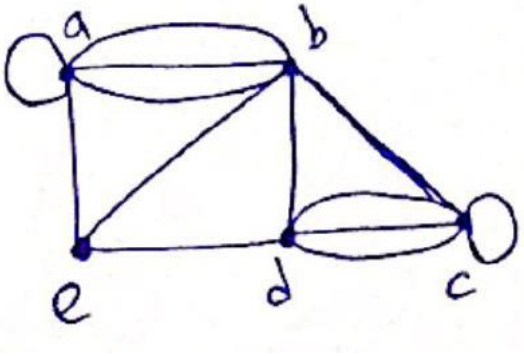
Pendant: A vertex is Pendant it and only if it has degree one. Vertex d is Pendant.

Example what are the degrees and what are the neighborhoods of the vertices in the following graph?



deg (a)= 4 deg (b)= 6 deg (c)= 1 Pendant deg(e)= 6

deg (g)= 0 Isolated deg (d)= 5



deg (a)= 6 deg (b)= 6 deg (c)= 6 deg(e)= 3 deg (d)= 5

The handshaking Theorem: Let G= (V, E) be undirected graph with m edges. Then $2m = \sum_{v \in V} \deg(v)$

Edge having two end Points and a handshake involving two hands.

In exercise 1 $\sum_{v\in V} \deg(v) = 4 + 6 + 1 + 6 + 5 + 0 = 22$

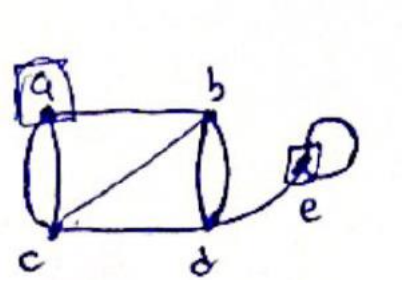
m=22/2 =11

Exercise How many edges one there in an undirected graph with lo vertices Cach of degree six.

$$\sum_{v\in V} \deg(v) = 10 * 6 = 60$$

$$m(edges) = \frac{60}{2} = 30$$

Theorem An undirected graph has an even number of vertices of odd degree.



Let V_1 set of vertices of even degree = {b, c, d}

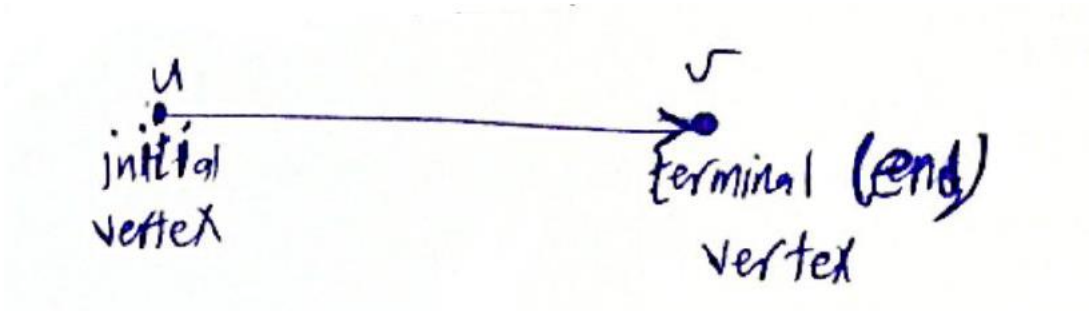
Let V_2 set of vertices of odd degree = {a, e} $2m = \sum_{v\in V} \deg(v)$

$$2m = \sum_{v\in V_1} \deg(v) + \sum_{v\in V_2} \deg(v)$$

Directed graphs: when (u, v) is an edge of the graph G with directed edges.

Ⓤ adjacent to v

Ⓥ adjacent from u



Note initial and end of a loop are the same.

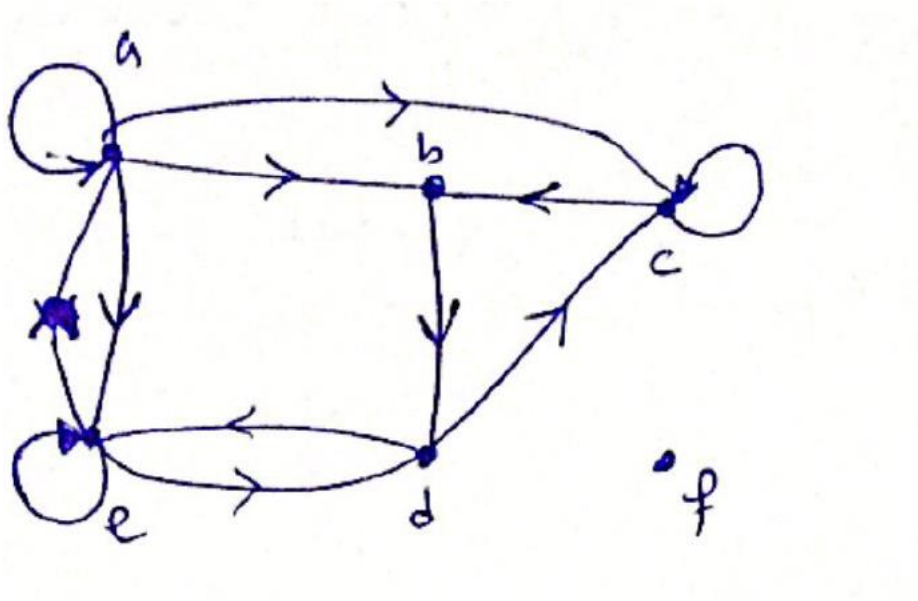
In-degree of a vertex $\deg^-(v)$: is the number of edges with V as their terminal vertex.

In-degree of a vertex $\deg^+(v)$: is the number of edges with V as their initial vertex.

Note loop at a vertex contributes 1 to both $\deg^-(v)$ and $\deg^+(v)$

Exercise Calculate the number of vertices, number of edges, In-degree of every vertex, and out-degree of every vertex.

Example



Number of vertex =6 number of edges =12

$\deg^-(a) = 2$ $\deg^+(a) = 4$

$\deg^-(b) = 2$ $\deg^+(b) = 1$

$\deg^-(c) = 3$ $\deg^+(c) = 2$

$\deg^-(d) = 2$ $\deg^+(d) = 2$

$\deg^-(0) = 3$ $\deg^+(e) = 3$

$\deg^-(f) = 0$ $\deg^+(f) = 0$

$$\sum_{v \in V} deg^-(v) = 12 \qquad \sum_{v \in V} deg^+(v) = 12$$

Theorem Let G= (V, E) be graph with directed edges. Then,

$$\sum_{v \in V} deg^-(v) = \sum_{v \in V} deg^+(v) = |E|$$

Note

- ❖ null graph: a graph without any edge
- ❖ regular graph: a graph in which all vertices are of equal degree.

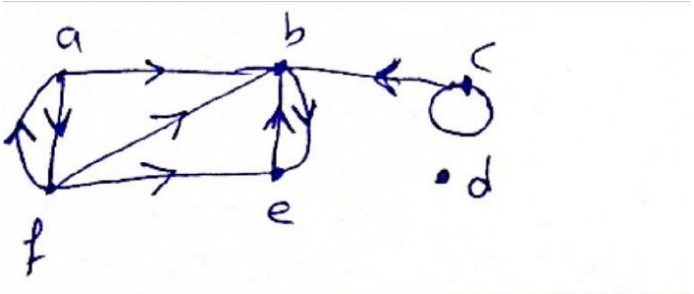
Exercise Can a simple graph exist with 15 vertices each of degree five?

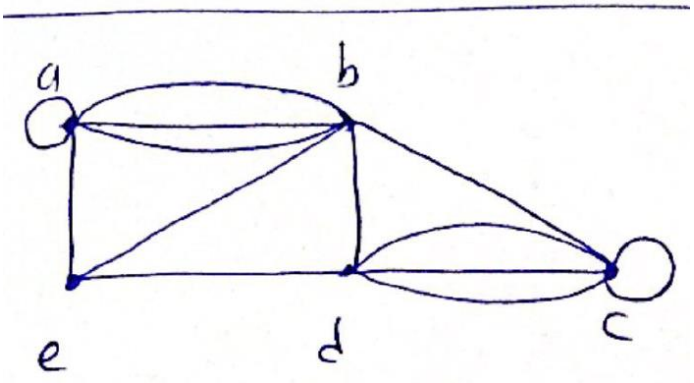
$$2m = \sum_{v \in V} deg(v) = 15 * 5 = 75$$

$m = |E| = 37.5$ $not\ simple\ graph$

Simple graph m must be integer 0.5 means that there is loop in the graph.

Exercise Find the number of vertices, edges, degree of each vertex in the fllowing graphs:

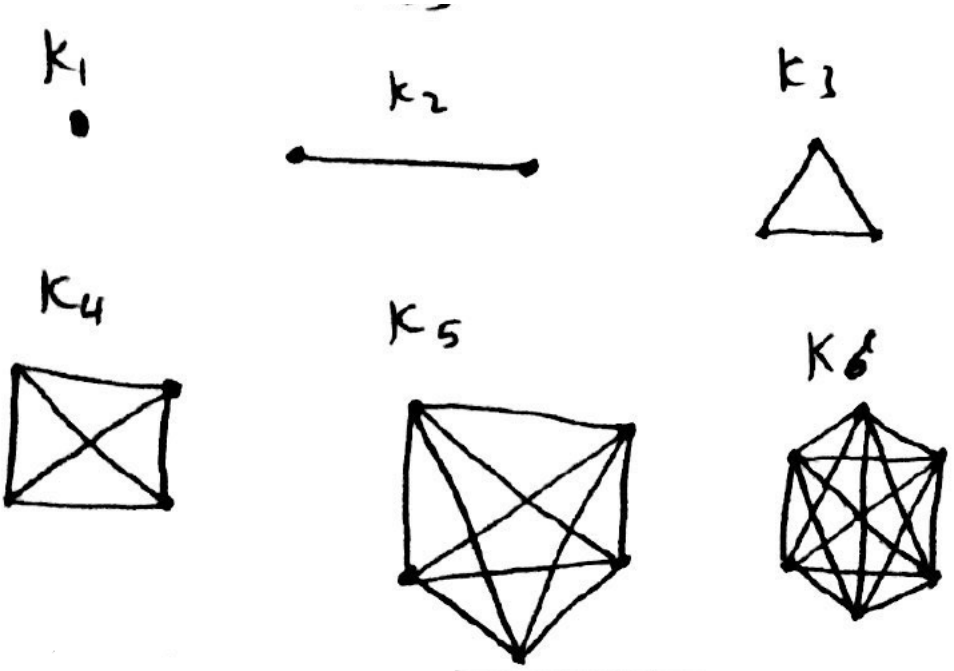




4.4 Some special simple graphs:

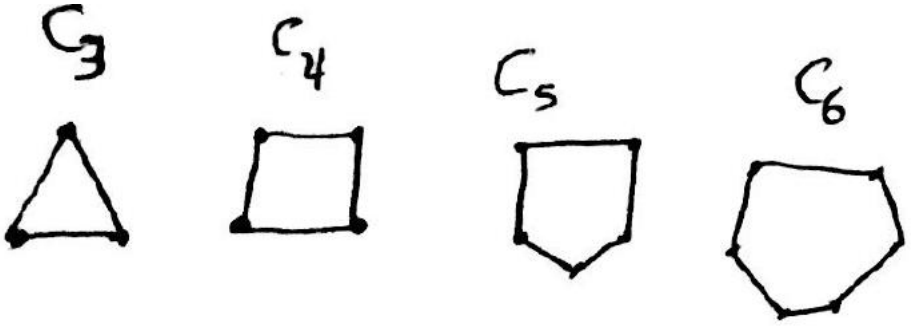
1. **Complete graph (K_n) $n \geq 1$**

Is the simple graph that contains one edge between each Pair of distinct vertices.

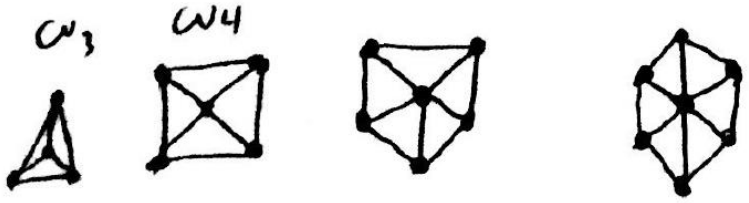


2. **Cycles: (C_n), $n \geq 3$:** The cycle C_n; $n \geq 3$ Consists of n Vertices v_1, v_2, …,v_n and edges

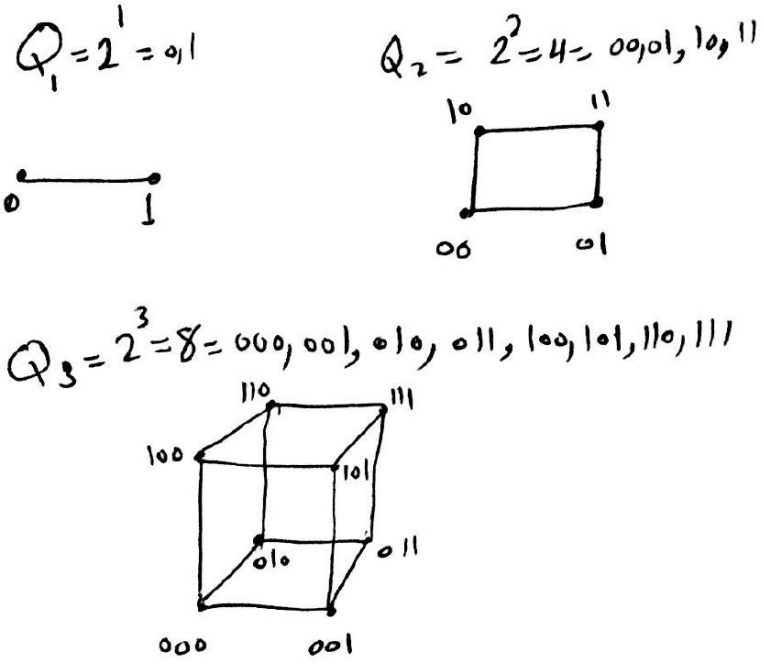
$\{v_1, v_2\}, \{v_2, v_3\}, \ldots\ldots \{v_{n-2}, v_{n-1}\}, \{v_{n-1}, v_n\}$



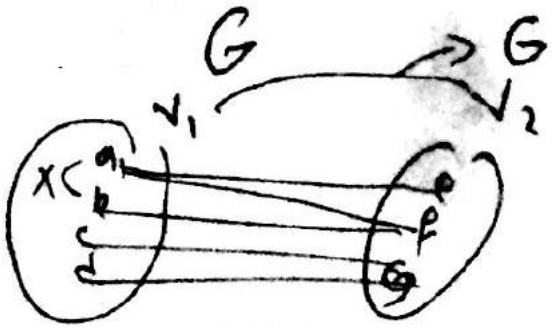
3. **wheels: (Wn), n≥3:** We obtain the wheel W_n when we add an additional Vertex to the cycle C_n and connect this new vertex to each of the n vertices in C_n by new edge.



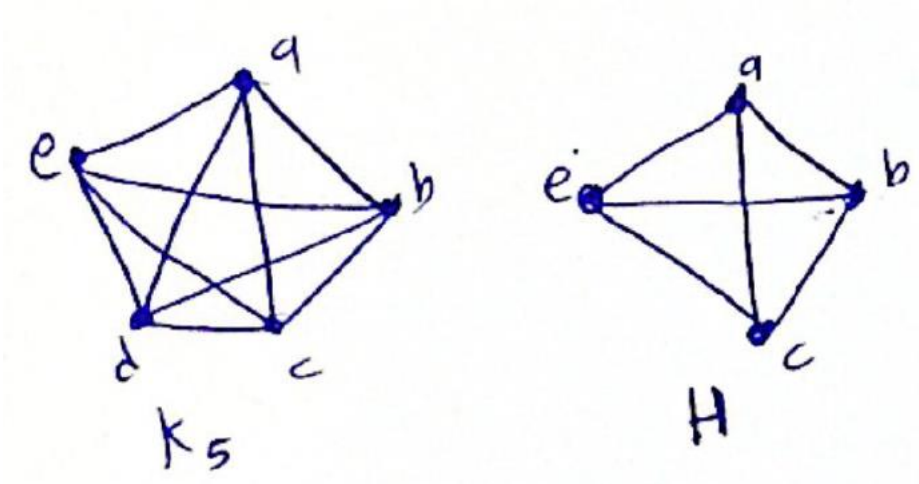
4. **n-Cubes (Q_n):** The n-dimensional hypercube (n-cube) Q_n is the graph that has vertices representing the 2^n bit strings of length n. Two vortices are adjacent if and only if the bit strings that they represent differ in one exactly one-bit Position.



Bipartite graphs: if vertex ser V Can be Partitioned into two disjoint sets V, and V_2 such that every edge in the graph Connects a vertex in V_1 and a Vertex in V_2 (so that no edge in G connects two vertices in V_1, or two vertices in V_2)⇒ (V_1,V_2) a bipartition of the vertex set V of G

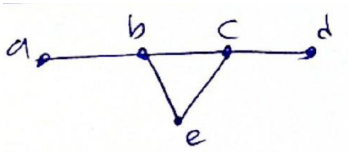


Subgraph induced: Let G = (V, E) be a simple graph. The subgraph induced by a Subset W of the vertex set V is the graph (W, F), where edge Set F Contains an edge in E if and only if both endpoints of this edge one in W.

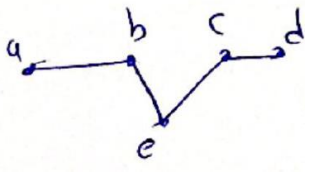


H subgraph induced by W= {a, b, c, d}

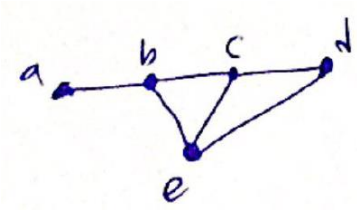
Removing or adding edge of a graph



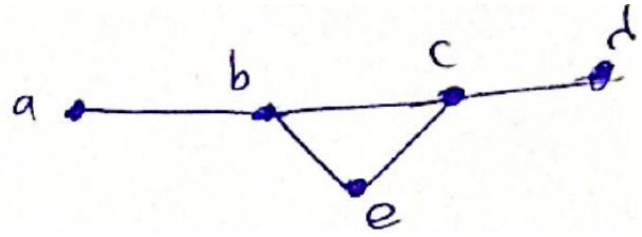
Removing G - {b, c}



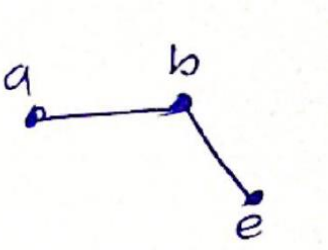
Adding G + {e, d}



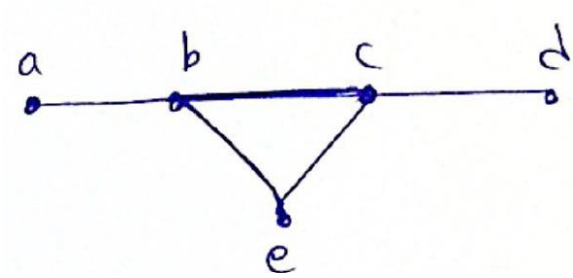
Removing vertices from graph



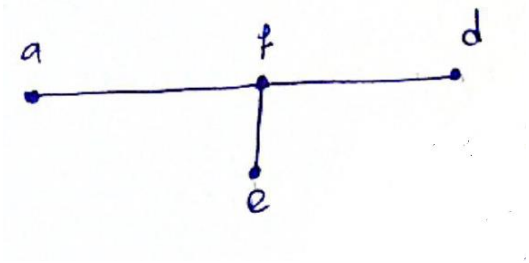
Removing vertex C



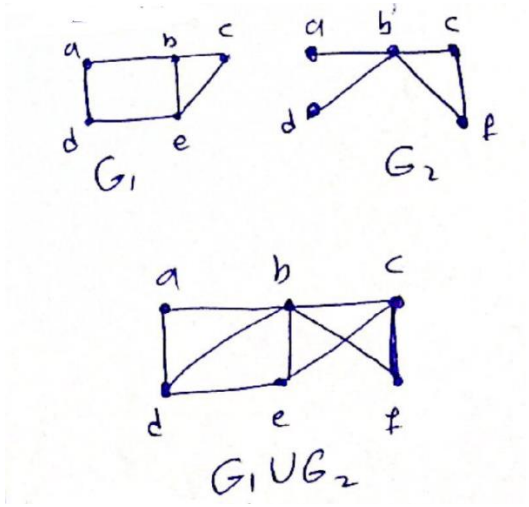
Edge contraction:



G contract by replacing {b, c} by F



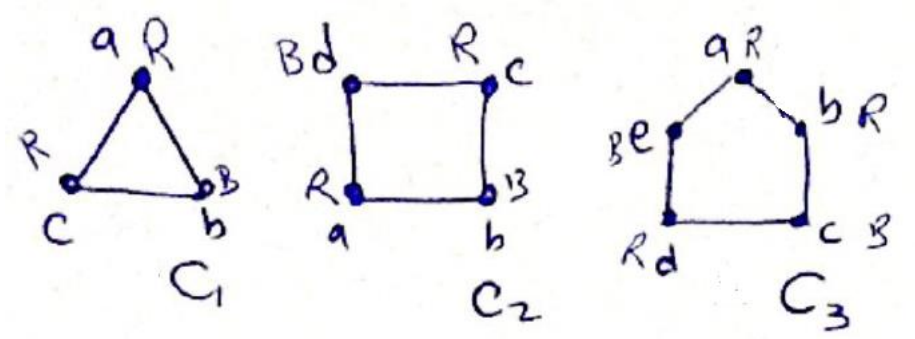
Graph union.



$V=V_1 \cup V_2$

$E= E_1 \cup E_2$

Example: Determine whether the following graphs is bipartite or not

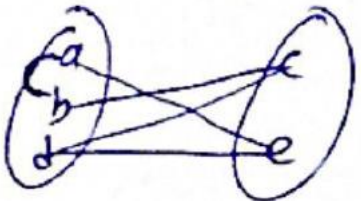


C1 is not bipartite. C2 is bipartite. C3 is not bipartite.

Determining whether it is possible to assign either red or blue to each Vertex So that no two adjacent Vertices are assigned the same color.

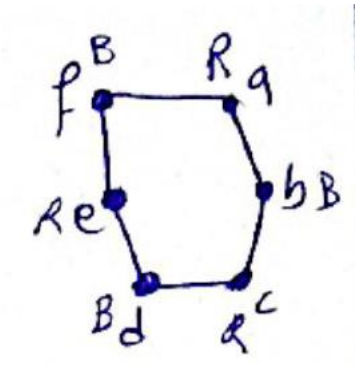
In C3: $V_1 = \{a, b, d\}$ red color

$V_2 = \{c, e\}$ blue color



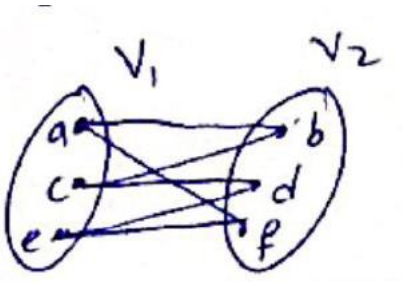
So C3 is not bipartite.

Example: Determine whether the following graph is bipartite or not



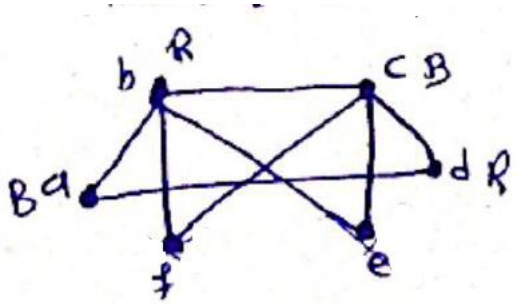
$V_1 = \{a, c, e\}$

$V_2 = \{b, d, f\}$



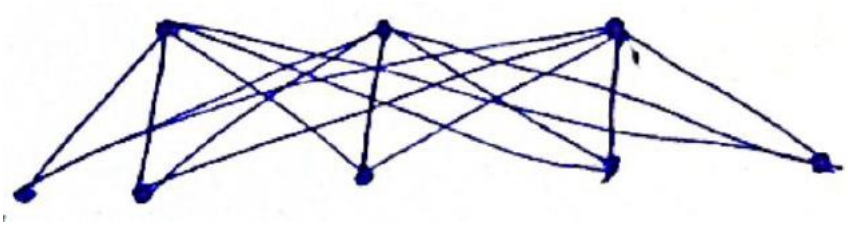
So, the graph is bipartite.

Example: Determine whether the following graph is bipartite or not

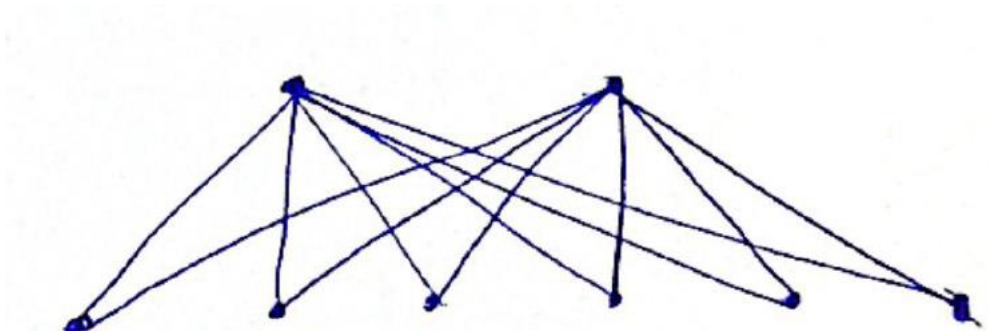


The graph is not bipartite.

Complete bipartite graphs ($K_{m,n}$): Is a graph that has it Vertex Set Partitioned into two subsets of m and n vertices, respectively with an edge between two vertices it and only if one vertex, is in the first subset and the other is in the second subset.



$K_{3,5}$ complete bipartite

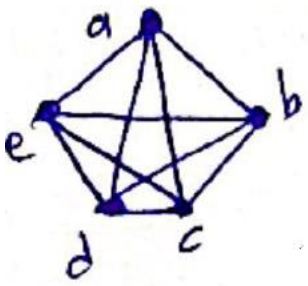


$K_{2,6}$ complete bipartite

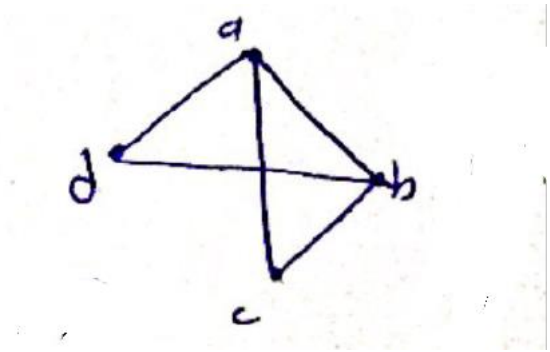
A subgraph of graph G= (V, E): is a graph H= (W, F) where$w \leq V$

$$and\ F \leq E.$$

A subgraph H of G is a proper subgraph of G if H # G



Original graph



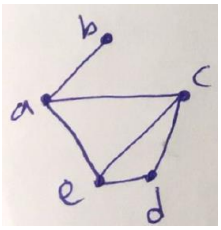
Proper subgraph of K_5

4.5 Representing graphs: There are many useful ways to represent graphs. In working with a graph, it is helpful to be able to choose its most appropriate representation. In this section, we will show how to represent graphs in several different ways.

- ❖ using Representing graphs adjacency list.
- ❖ using Representing graphs adjacency matrix
- ❖ using Representing graphs incidence matrix

Adjacency list: Is a way to represent a graph with no multiple edges, which specify the Vertices that are adjacent to each Vertex of the graph.

Example Use adjacency list to describe the following simple graph.



Vertex	Adjacent vertices
A	b, c, e
B	A
C	a, e, d
D	c, e
E	a, c, d

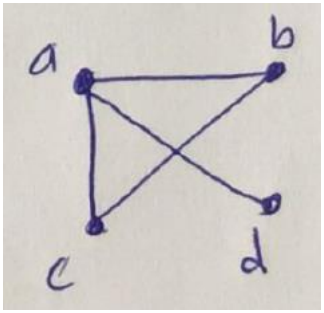
Adjacency matrix: let G= (V, E) is a simple graph, where $|v| = n$. suppose that the Vertices of G ane listed arbitrarily as V_1, V_2, ….., V_n .

The adjacency matrix A (A_G) of G with respect to this listing of vertices is nxn zers-ore matrix with 1 as its (i, j) entry when V_i. and V_J one adjacent, and o as its (i, j) entry when they are not adjacent

A $[a_{ij}]$, where

$$a_{ij} = \begin{cases} 1 & if \ \{V_i, V_j\} is \ an \ edge \ of \ G \\ 0 & otherwise \end{cases}$$

Example use an adjacency matrix to represent the following graph.

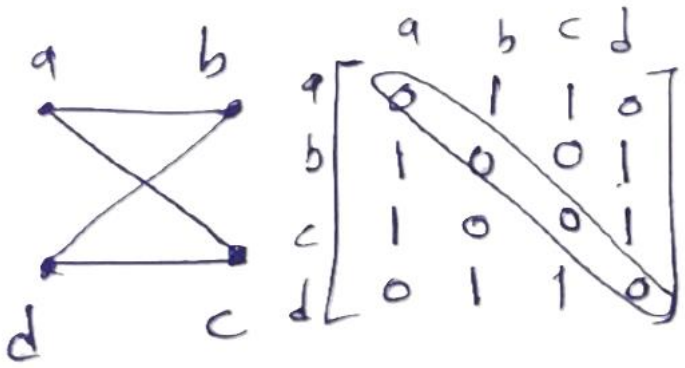


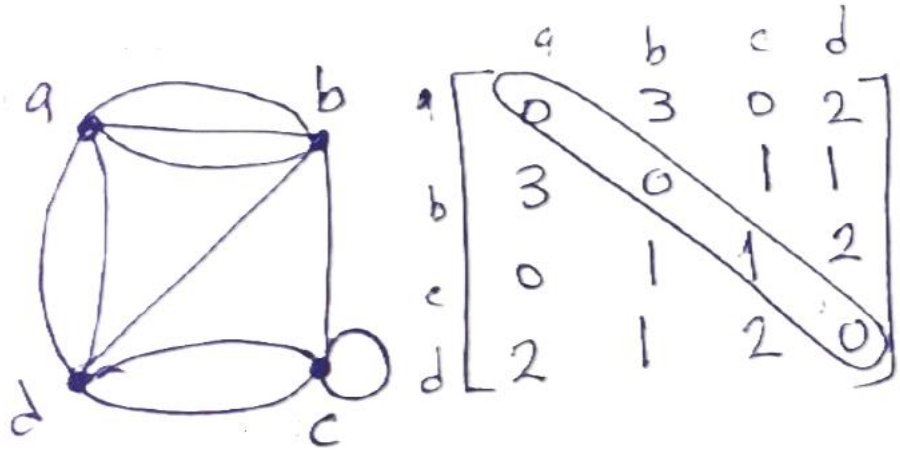
$$\begin{array}{c} \\ a \\ b \\ c \\ d \end{array} \begin{array}{c} \begin{array}{cccc} a & b & c & d \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

All undirected greatly have symmetric adjacency matrices.

Note Adjacency matrix of a graph is based on the ordering chosen for the Vertices. Hence, there may be as many as n! different adjacency matrices for a graph with Vertices.

Example adjacency matrices



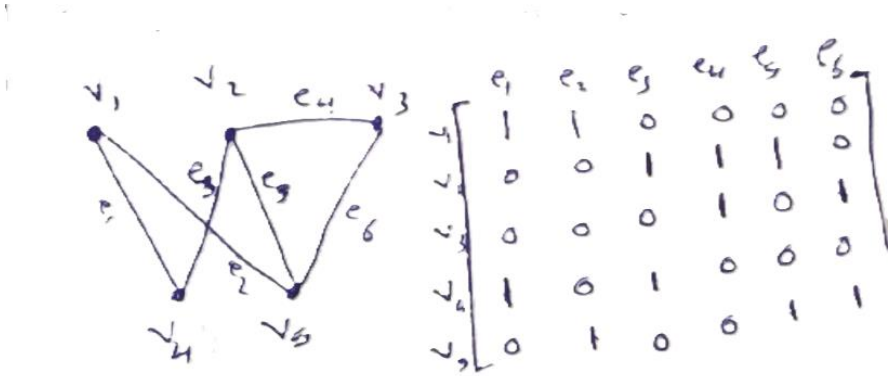


Incidence Matrix: Let G = (V, E) be undirected graph. Suppose that $V_1, V_2, \ldots, V_n$ are the vertices and $e_1, e_2, \ldots, e_n$ are the edges of Go Then the incidence matrix w, r, t. this ordering of V and E is the (n x m) matrix

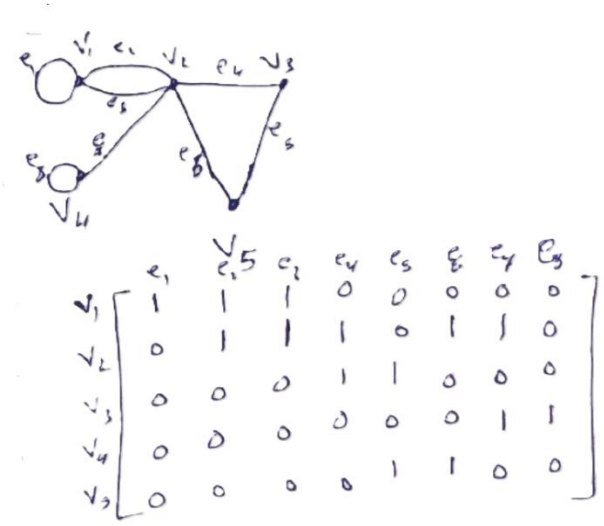
M=[a_{ij}], where

$$a_{ij} = \begin{cases} 1 & when\ edge\ e_j is\ incident with\ s_i \\ 0 & otherwise \end{cases}$$

Example of incidence matrix of graph



Example (1)



Example (2)

References

1- Rowan Garnier and John Taylor, Discrete Mathematics for New Technology, 2nd Edition, Institute of Physics Publishing, 2001.

2- S. Lipschutz−M. L. Lipson, Schaum's Outline of Theory and Problems of Discrete Math, 2004.

3-Kenneth H. Rosen, Discrete Mathematics and Its Applications, 7th Edition, 2007.