DISCRETE MATHEMATICS

www.ankurgupta.net

These notes have been prepared from the following books :-

(1) Discrete Mathematics and Its Applications by Kenneth H. Rosen
(2) Discrete Mathematics by Seymour Lipschutz, Marc Lars Lipson

Kindly refer the above books for more details.

Logic and Proofs

The rules of logic specify the meaning of mathematical statements

Once we prove a mathematical statement is true, we call it a theorem.

A correct mathematical argument about a theorem is a proof.

Propositional Logic :-

The rules of logic give precise meaning to mathematical statements. These rules are used to distinguish between valid and invalid mathematical arguments.

Propositions :-

A proposition is a declarative sentence, that is either true or false, but not both.

Eg :-

(i) $1 + 1 = 2$ is a proposition

(ii) What time is it? is not a proposition.

The area of logic that deals with propositions is called the propositional calculus or propositional logic.

New propositions, called compound propositions, are formed from existing propositions using logical operators.

Logical Operators :-

(1) **Negation** :-

$\neg p$, $\bar{p}$, not p

p	$\neg p$
T	F
F	T

(2) **Conjunction** :-

$p \wedge q$, p and q

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

Sometimes the word "but" is used instead of "and" in a conjunction.

E.g.:- The sun is shining, but it is raining.

(3) **Disjunction** :- (Inclusive OR)

$p \vee q$, p or q

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

It is one of the two ways the word or is used in English, namely, in an inclusive way.

E.g.:- Students who have taken calculus or computer science can take this class.

(4) **Exclusive OR** :-

$p \oplus q$ $\quad \boxed{p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)}$

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

The logical operators, Conjunction, Disjunction and Exclusive OR are called as connectives, since they form ~~pro~~ new propositions using two or more existing propositions.

Dual of a Compound Proposition :-

The dual of a compound proposition that contains only the logical operators $\vee$, $\wedge$, and $\neg$ is the compound proposition obtained by replacing each $\vee$ by $\wedge$, each $\wedge$ by $\vee$, each T by F, and each F by T. The dual of S is denoted by S^*.

Duals of two equivalent compound propositions ~~are~~ are also equivalent, where these compound proposition contain only the operators $\wedge, \vee$, and $\neg$

$(S^*)^* = S$

$S \Rightarrow p \wedge T \equiv p$
$S^* \Rightarrow p \vee F \equiv p$

$S \Rightarrow \neg(p \wedge q) \equiv \neg p \vee \neg q$
$S^* \Rightarrow \neg(p \vee q) \equiv \neg p \wedge \neg q$

Conditional Statements:-

$p \rightarrow q$ / if p, then q.

A conditional statement is also called an implication.

Here p is called the hypothesis or antecedent or premise and q is called the conclusion or consequence.

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

Ways to express the conditional statement ($p \rightarrow q$):-

(i) if p, then q
(ii) p implies q
(iii) if p, q
(iv) p only if q
(v) p is sufficient for q
(vi) a sufficient condition for q is p.
(vii) q if p
(viii) q whenever p
(ix) q when p
(x) q is necessary for p
(xi) A necessary condition for p is q.
(xii) q follows from p.
(xiii) q unless $\neg p$.

I will be there ~~at~~ at nine unless the train is late.

"p only if q" says that p can not be true when q is not true. That is, the statement is false if p is true, but q is false.

"q unless $\neg p$" means that if $\neg p$ is false, then q must be true.

Converse:-
The proposition $q \rightarrow p$ is called the converse of $p \rightarrow q$.

Contrapositive:-
The proposition $\neg q \rightarrow \neg p$ is called the contrapositive of $p \rightarrow q$

Inverse:-
The proposition $\neg p \rightarrow \neg q$ is called the inverse of $p \rightarrow q$

A conditional statement and its contrapositive are equivalent.

The converse and the inverse of a conditional statement are also equivalent.

Functionally Complete Collection of Logical Operators:-
A collection of logical operators is called functionally complete if every compound proposition is logically equivalent to a compound proposition involving only these logical operators.

Eg:- $\neg, \wedge$ / $\neg, \vee$ / NAND / NOR / $\rightarrow$ / $\leftrightarrow$

BiConditionals :-

$p \leftrightarrow q$ / p if and only if q

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

Other ways to express $p \leftrightarrow q$:-

(i) p is necessary and sufficient for q
(ii) if p then q, and conversely
(iii) p iff q

$p \leftrightarrow q$ has exactly the same truth value as $(p \to q) \wedge (q \to p)$.

Implicit use of Biconditionals :-

Biconditionals are often expressed using an "if, then" or an "only if" in natural language. The other part of the "if and only if" is implicit.

www.ankurgupta.net

Precedence of Logical Operators :-

'$\neg$' > '$\wedge$' > '$\vee$' > '$\to$' > '$\leftrightarrow$'

Tautology :-
A compound proposition that is always true, no matter what the truth values of the propositions that occur in it, is called a tautology.

Contradiction :-
A compound proposition that is always false is called a contradiction.

Contingency :-
A compound proposition that is neither a tautology nor a contradiction is called a contingency.

Tautology $\Rightarrow$ Valid
Contingency $\Rightarrow$ Satisfiable
Contradiction $\Rightarrow$ Unsatisfiable

www.ankurgupta.net

Logical Equivalences :-

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

OR

Compound propositions that have the same truth values in all possible cases are called logically equivalent.

The notation $p \equiv q$ denotes that p and q are logically equivalent. Sometimes, the symbol $\Leftrightarrow$ is also used.

Logical Equivalences Involving Logical Operators :-

Equivalence	Name
$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity Laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination Laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent Laws
$\neg(\neg p) \equiv p$	Double Negation Law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative Laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative Laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive Laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's Laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption Laws
$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation Laws

Logical Equivalences Involving Conditional Statements :-

$p \rightarrow q \equiv \neg p \vee q$

$p \rightarrow q \equiv \neg q \rightarrow \neg p$

$p \vee q \equiv \neg p \rightarrow q$

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

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

$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$

$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$

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

$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Logical Equivalences Involving Biconditionals :-

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

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

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q \equiv \neg p \leftrightarrow q$

$p \leftrightarrow q \equiv \neg(p \oplus q)$

If --- Then ---- Unless --- Rule :-

If x is A then y is B unless z is C.

$\Rightarrow$ If x is A and z is not C then y is B.

$\Rightarrow$ If x is A and z is C then y is not B.

If X, then Y unless Z

$\Rightarrow (X \wedge \neg Z) \rightarrow Y$

$\Rightarrow X \rightarrow (\neg Z \rightarrow Y)$

Predicates and Quantifiers :-

Predicates :-

We can denote the statement "x is greater than 3" by $P(x)$, where P denotes the predicate "is greater than 3" and x is a variable.

The statement $P(x)$ is also said to be the value of the propositional function P at x.

A statement of the form $P(x_1, x_2, \ldots, x_n)$ is the value of the propositional function P at the n-tuple $(x_1, x_2, \ldots x_n)$, and P is also called an n-place predicate or a n-ary predicate.

The area of logic that deals with predicates and quantifiers is called the predicate calculus.

Quantifiers :-

Quantification expresses the extent to which a predicate is true over a range of elements.

In English, the words all, some, many, none, and few are used in quantifications.

www.ankurgupta.net

Universal Quantifiers :-

The universal quantification of $P(x)$ is :-

$\forall x\, P(x)$ / for all x $P(x)$ / for every x $P(x)$

→ An element for which $P(x)$ is false is called a counterexample of $\forall x P(x)$.

If the domain x is empty, the $\forall x\, P(x)$ is true for any propositional function $P(x)$ because there are no elements x in the domain for which $P(x)$ is false.

Other ways to express "Universal Quantification" :-

all of / for each / given any / for arbitrary / for any.

When all the elements in the domain can be listed - say, $x_1, x_2, \ldots, x_n$ - it follows that the universal quantification $\forall x\, P(x)$ is the same as the conjunction :-

$P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$

because this conjunction is true if and only if $P(x_1), P(x_2), \ldots P(x_n)$ are all true.

Existential Quantifier :-

The existential quantification of $P(x)$ is :-
"There exists an element x such that $P(x)$"
or $\exists x\, P(x)$.

Other ways to express "Existential Quantifier" :-

for some / for at least one / there is

If the domain x is empty, then $\exists x\, Q(x)$ is false whenever $Q(x)$ is propositional function because when the domain is empty, there can be no element x in the domain for which $Q(x)$ is true.

When all elements in the domain can be listed say $x_1, x_2, \ldots x_n$ – the existential quantificato $\exists x\, P(x)$ is the same as the disjunction :-
$P(x_1) \vee P(x_2) \vee \_\_\_ \vee P(x_n)$,
because this disjunction is true if and only if at least one of the $P(x_1), P(x_2), \_\_, P(x_n)$ is true.

Important Points :-

$\forall x\, P(x) = P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \ldots$
$\exists x\, P(x) = P(x_1) \vee P(x_2) \vee P(x_3) \vee \ldots$

$\neg \forall x\, P(x) = \exists x\, \neg P(x) = \neg P(x_1) \vee \neg P(x_2) \vee \neg P(x_3) \vee \ldots$

$\neg \exists x\, P(x) = \forall x\, \neg P(x) = \neg P(x_1) \wedge \neg P(x_2) \wedge \neg P(x_3) \wedge \ldots$

Quantifiers with Restricted Domains :-

E.g.:- $\forall x < 0\ (x^2 > 0)$
$\exists z > 0\ (z^2 = 2)$.

The restriction of a universal quantification is the same as the universal quantification of a conditional statement.

$\forall x < 0\ (x^2 > 0) \equiv \forall x\, (x < 0 \rightarrow x^2 > 0)$

The restriction of an existential quantification is the same as the existential quantification of a conjunction.

$\exists z > 0\ (z^2 = 2) \equiv \exists z\, (z > 0 \wedge z^2 = 2)$

Precedence of Quantifiers :-

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical operators from propositional calculus

Eg.:- $\forall x\, P(x) \vee Q(x)$ is equivalent to $(\forall x\, P(x)) \vee Q(x)$

Binding Variables:-

When a quantifier is used on the variable x, we say that this occurance of the variable is bound.

An occurance of a variable that is not bound by a quantifier or set equal to a particular value is said to be free.

The part of a logical expression to which a quantifier is applied is called the **scope** of this quantifier. Consequently, a variable is free if it is outside the scope of all quantifiers in the formula that specifies this variable.

E.g.:-

(i) $\exists x (x+y=1)$

→ x is bound

→ y is free

(ii) $\exists x (P(x) \wedge Q(x)) \vee \forall x R(x)$

→ Scope of first quantifier, $\exists x$, is the expression $P(x) \wedge Q(x)$.

→ Scope of second quantifier $\forall x$, is the expression $R(x)$.

Note:-

In common usage, the same letter is often used to represent variables bound by different quantifiers with scopes that do not overlap.

Logical Equivalences Involving Quantifiers:-

$$\forall x (P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$$

$$\exists x (P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$$

$$\forall x (P(x) \vee Q(x)) \not\equiv \forall x P(x) \vee \forall x Q(x)$$

$$\exists x (P(x) \wedge Q(x)) \not\equiv \exists x P(x) \wedge \exists x Q(x)$$

Some Important Results:-

$$\forall x P(x) \vee \forall x Q(x) \longrightarrow \forall x (P(x) \vee Q(x))$$

$$\exists x (P(x) \wedge Q(x)) \longrightarrow \exists x P(x) \wedge \exists x Q(x)$$

$$\forall x (P(x) \rightarrow Q(x)) \longrightarrow \forall x P(x) \longrightarrow \forall x Q(x)$$

Negating Quantified Expressions:-

$$\left.\begin{aligned} \neg \forall x P(x) &\equiv \exists x \neg P(x) \\ \neg \exists x P(x) &\equiv \forall x \neg P(x) \end{aligned}\right\} \text{De Morgan's laws for quantifiers}$$

Nested Quantifiers :-

Two quantifiers are nested if one is within the scope of the other, such as:-

$\forall x\, \exists y\, (x + y = 0)$.

The above statement is same as $\forall x\, Q(x)$, where $Q(x)$ is $\exists y\, P(x,y)$, where $P(x,y)$ is $x + y = 0$.

The order of Quantifiers :-

The order of the quantifiers is important, unless all the quantifiers are universal quantifiers or all are existential quantifiers.

$\forall x\, \forall y\, P(x,y) \equiv \forall y\, \forall x\, P(x,y)$

$\exists x\, \exists y\, P(x,y) \equiv \exists y\, \exists x\, P(x,y)$

$\forall x\, \exists y\, P(x,y) \not\equiv \exists y\, \forall x\, P(x,y)$

$\exists y\, \forall x\, P(x,y) \longrightarrow \forall x\, \exists y\, P(x,y)$

Negating Nested Quantifiers :-

Successively applying the rules for negating statements involving a single quantifier.

Eg :- $\neg \forall x\, \exists y\, \forall z\, P(x,y,z)$

$\equiv \exists x\, \neg \exists y\, \forall z\, P(x,y,z)$

$\equiv \exists x\, \forall y\, \neg \forall z\, P(x,y,z)$

$\equiv \exists x\, \forall y\, \exists z\, \neg P(x,y,z)$

Important Points to Remember

~~(1) How many different truth tables of compound propositions such that p and q are~~

(1) How many different truth tables of compound propositions are there that involve the propositional variables p and q?

Answer :- $2^4 = 16$ ← No of Rows in truth table

(2^{2^n}) where n is no of propositional variables

(2) Disjunctive Normal forms or Sum of Products :-

$(p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r)$ ...

(3) Conjunctive Normal Form or Product of Sums :-

$(p \vee q \vee r) \wedge (p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r)$ ...

(4) Satisfiable :-

A compound proposition is satisfiable if there is an assignment of truth values to the variables in the compound proposition that makes the compound proposition true.

(5) Some important translations from english language statements into logical expressions :-

(i) No one is perfect.
$\forall x \neg P(x)$

(ii) Not everyone is perfect.
$\neg \forall x P(x) \;/\; \exists x \neg P(x)$

(iii) All your friends are perfect.
$\forall x (F(x) \to P(x))$

(iv) At least one of your friends is perfect.
$\exists x (F(x) \wedge P(x))$

(v) Everyone is your friend and is perfect.
$\forall x (F(x) \wedge P(x))$

(vi) The negation of a contradiction is a tautology.
$\forall x (C(x) \to \neg T(x))$

(vii) The disjunction of two contingencies can be a tautology.
$\exists x \exists y (\neg T(x) \wedge \neg C(x) \wedge \neg T(y) \wedge \neg C(y) \wedge T(x \vee y))$

(viii) The conjunction of two tautologies is a tautology.
$\forall x \forall y ((T(x) \wedge T(y)) \to T(x \wedge y))$

☆ (6) $\exists ! x\, P(x)$ (Used for unique)
→ There exists a unique x, such that P(x) is true.

(7) Valid :-

A well formed formula (wff) is called valid, if it is true for all assignment of truth values to the variables in wff.

(8) Closed Formula :-

A formula with no free variables.

(9) Only Free Variables Matter :– The truth value of a formula depends only on the truth values of free variables of the formula.

The truth value of a propositional formula(F) in an interpretation I depends on the truth values of all variables p occurring in F.

The truth value of a quantified boolean formula in an interpretation I does not depend on the values in I of variables occurring in quantifiers, called bound variables.

$I \models A$ represents interpretation I satisfies formula A.

(10) Satisfiablity of quantified formulas :–

For every interpretation I and closed formula F, the following propositions are equivalent :–

(i) $I \models F$
(ii) F is satisfiable
(iii) F is valid.

The value of quantified boolean formulas does not depend on the values of its quantified (bound) variables.

Example :– Evaluation of the formula $\forall p \exists q\, (p \leftrightarrow q)$ in the interpretation $I = \{p \mapsto 1, q \mapsto 0\}$ or I_{10}.

$$I_{pq} \models \forall p\, \exists q\, (p \leftrightarrow q)$$

$\wedge$

$$I_{0q} \models \exists q (p \leftrightarrow q) \qquad I_{1q} \models \exists q (p \leftrightarrow q)$$

$\vee \qquad \vee$

$$I_{00} \models (p \leftrightarrow q) \quad I_{01} \models (p \leftrightarrow q) \quad I_{10} \models (p \leftrightarrow q) \quad I_{11} \models (p \leftrightarrow q)$$

$$\Rightarrow \quad I_{pq} = [(I_{00} \vee I_{01}) \wedge (I_{10} \vee I_{11})]$$

(for all p, q.)

www.ankurgupta.net

Sets, Functions & Relations

Set:-

A set is an unordered collection of objects.

\# The objects in a set are called the elements, or members of the set.

$a \in A \Rightarrow$ a is an element of the set A.

$a \notin A \Rightarrow$ a is not an element of the set A.

Some Important Sets:-

$N = \{0, 1, 2, \ldots\}$, the set of Natural Numbers

$Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, the set of Integers

$Z^+ = \{1, 2, 3, \ldots\}$, the set of positive integers.

$Q = \{p/q \mid p \in Z; q \in Z$ and $q \neq 0\}$, the set of rational numbers.

R; the set of Real Numbers.

Note:- Some people do not consider 0 a natural number.

\# Sets can have other sets as members.

$\rightarrow A = B$, if and only if $\forall x\,(x \in A \leftrightarrow x \in B)$

Equal Sets :-

Two sets are equal if and only if they have the same elements. We write $A = B$ if A and B are equal sets.

Empty Set or Null Set :-

A set that has no elements.

ϕ / { }.

Singleton Set :-

A set with only one element.

Subset :-

A set A is said to be a subset of B if and only if every element of A is also an element of B.

$$A \subseteq B$$

$A \subseteq B$ if and only if $\forall x\,(x \in A \rightarrow x \in B)$

For every set S :-

(i) $\phi \subseteq S$

(ii) $S \subseteq S$

Important :-

$\phi \notin \{0, 1, \ldots\}$

$\phi \in \{\phi, 0, 1, \ldots\}$

$\phi \subset \{0, 1, \ldots\}$

Proper Subset :-

If a set A is a subset of the set B, but that $A \neq B$, we write $A \subset B$ and say that A is a proper subset of B.

$A \subset B$, if

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

is true.

Finite and Infinite Sets :-

A set S with exactly n distinct elements, where n is a non-negative integer, is called a finite set. Here n is the cardinality of S. The cardinality of S is denoted by $|S|$.

A set is said to be infinite if it is not finite.

Power Set :-

Given a set S, the power set of S is the set of all subsets of the set S. The power set of S is denoted by $P(S)$.

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

Ordered n-tuples :-

The ordered n-tuple $(a_1, a_2, \ldots a_n)$ is the ordered collection that has a_1 as its first element, a_2 as its second element, ..., and a_n as its n^{th} element.

Two ordered n-tuples are equal if and only if each corresponding pair of their elements is equal.

2-tuples are called ordered pairs. E.g. (a,b)

Cartesian Product :-

The cartesian product of the sets $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \ldots \times A_n$, is the set of ordered n-tuples $(a_1, a_2, \ldots a_n)$, where a_i belongs to A_i for $i = 1, 2, \ldots n$.

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots n\}$$

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

Using Set Notation with Quantifiers :-

(a) $\forall x \in S\, (P(x))$

→ It is shorthand for $\forall x (x \in S \rightarrow P(x))$

(b) $\exists x \in S\, (P(x))$

→ It is shorthand for $\exists x (x \in S \wedge P(x))$

$A \times \phi = \phi \times A = \phi$

Truth set of Quantifiers :-

Given a predicate P, and a domain D, the truth set of P is the set of elements x in D for which P(x) is true. The truth set of P(x) is denoted by :-

$$\{x \in D \mid P(x)\}$$

$\forall x\, P(x)$ is true over the domain U if and only if the truth set of P is U.

$\exists x\, P(x)$ is true over the domain U, if and only if the truth set of P is nonempty.

Set Operations :-

(i) Union :-

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

(ii) Intersection :-

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

(iii) Difference :-

The difference of sets A and B, denoted by A − B, is the set containing those elements that are in A but not in B.

The difference of A and B is also called the complement of B with respect to A.

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

(iv) Complement :-

Let U be the universal set. The complement of the set, denoted by $\bar{A}$, is the complement of A with respect to U.

$$\bar{A} = U - A$$

or

$$\bar{A} = \{x \mid x \notin A\}$$

Two sets are called disjoint if their intersection is empty set.

Set Identities :-

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

Symmetric Difference :- The symmetric difference of A and B, denoted by $A \oplus B$ is the set containing those elements in either A or B, but not in both A and B.

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

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

Principle of Inclusion-Exclusion :-

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

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

Multisets :-
Multisets are unordered collections of elements where an element can occur as a member more than once.

→ The union of the multisets P and Q is the multiset where the multiplicity of an element is the maximum of its multiplicities in P and Q. $(P \cup Q)$

→ The intersection of P and Q is the multiset where the multiplicity of an element is the minimum of its multiplicities in P and Q. $(P \cap Q)$

The difference of P and Q is the multiset where the multiplicity of an element is the multiplicity of the element in P less its multiplicity in Q unless its difference is negative, in which case the multiplicity is 0. $(P - Q)$

The sum of P and Q is the multiset where the multiplicity of an element is the sum of multiplicities in P and Q. $(P + Q)$

Functions

Function:-

Let A and B be nonempty sets. A function f from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A.

If f is a function from A to B, we write $f : A \to B$, and say:- f maps A to B.

→ Functions are sometimes also called mappings or transformations.

Domain and Co-domain:-

If f is a function from A to B, we say that A is the domain of f and B is the codomain of f.

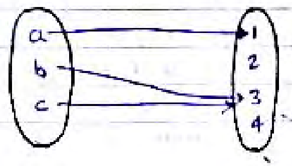
Image and Pre-image:-

If $f(a) = b$, we say that b is the image of a and a is the preimage of b.

Range:-

The range of f is the set of all images of elements of A.

Range $\subseteq$ Codomain



Domain = {a, b, c}
Codomain = {1, 2, 3, 4}
Range = {1, 3}

Equality of functions :-

Two functions are equal when they have the same domain, have the same codomain and map elements of their common domain to the same elements in their common codomain.

Addition and Multiplication of functions :-

Let f_1 and f_2 be functions from A to R. Then $f_1 + f_2$ and $f_1 f_2$ are also functions from A to R defined by :-

$$(f_1 + f_2)x = f_1(x) + f_2(x).$$
$$(f_1 f_2)x = f_1(x) f_2(x)$$

Increasing and Strictly Increasing Functions :-

A function f is called increasing if $f(x) \le f(y)$, and strictly increasing if $f(x) < f(y)$, whenever $x < y$ and x and y are in the domain of f.

Increasing :- $\forall x \forall y (x < y \rightarrow f(x) \le f(y))$

Strictly Increasing :- $\forall x \forall y (x < y \rightarrow f(x) < f(y))$

Decreasing and Strictly Decreasing Functions :-

A function f is called decreasing if $f(x) \ge f(y)$, and strictly decreasing if $f(x) > f(y)$, whenever $x < y$ and x and y are in domain of f.

Decreasing :- $\forall x \forall y (x < y \rightarrow f(x) \ge f(y))$

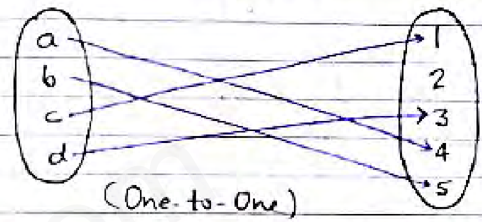
Strictly Decreasing :- $\forall x \forall y (x < y \rightarrow f(x) > f(y))$

Here domain and Codomain are subsets of the set of real num

One to One Functions :-

A function f is said to be one-to-one, or injective, if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f.

$$\forall a \forall b (f(a) = f(b) \rightarrow a = b)$$



(One-to-One)

A function that is either strictly increasing or strictly decreasing must be one-to-one.

A function that is increasing, but not strictly increasing, or decreasing but not strictly decreasing, is not necessarily one-to-one.

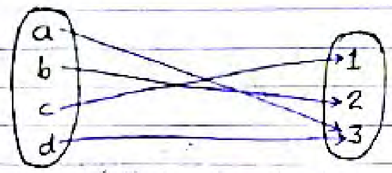
→ One-to-One functions never assign the same value to two different domain elements.

Onto Functions :-

A function f from A to B is called onto, or surjective, if and only if for every element $b \in B$, there is an element $a \in A$ with $f(a) = b$.

$$\forall y \, \exists x \, (f(x) = y)$$

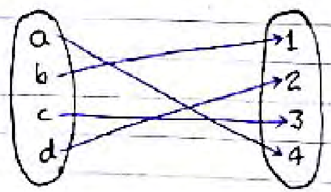
For onto functions, the range and the codomain are equal, i.e. every member of the codomain is the image of some element of the domain.



(Onto function)

One-to-One Correspondence :-

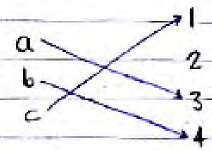
A function f is a one-to-one correspondence, or a bijection, if it is both one-to-one and onto.



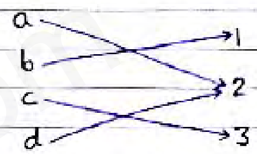
$f(x) = x^3$ (from R to R) is a bijection.

Some Examples :-

(a) One-to-One, not Onto :-

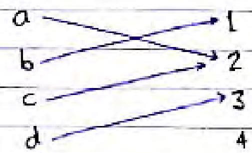


(b) Onto, not one-to-one :-



(c) One-to-One and Onto :-

(d) Neither one-to-one nor onto :-



(e) Not a function :-

Inverse Functions :-

Let f be a one-to-one correspondence from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B, the unique element a in A, such that $f(a) = b$. The inverse function of f is denoted by f^{-1}.

Hence, $f^{-1}(b) = a$, when $f(a) = b$.

$f^{-1} \neq 1/f$

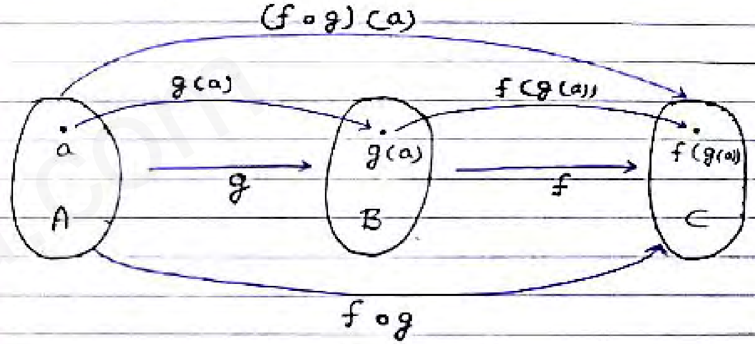
If a function f is not a one-to-one correspondence, we can not define an inverse function of f.

A one-to-one correspondence is called invertible because we can define an inverse of this function.

Compositions of Functions :-

Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The composition of the functions f and g, denoted by $f \circ g$, is defined by :-

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



$f \circ g \neq g \circ f$

$f^{-1} \circ f = f^{-1}(f(a)) = f^{-1}(b) = a$

$f \circ f^{-1} = f(f^{-1}(b)) = f(a) = b$

$(f^{-1})^{-1} = f$

Note :- (i) If both f and g are one-to-one functions, then $f \circ g$ is also one-to-one.
(ii) If both f and g are onto functions, then $f \circ g$ is also onto.
(iii) If f and $f \circ g$ are one-to-one, then g is also one-to-one.
(iv) If f and $f \circ g$ are onto, then it does not mean that g is also onto.

If f is an invertible function from Y to Z and g is an invertible function from X to Y, then:-

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$

www.ankurgupta.net

Some Important Points

(1) Let f be a function from the set A to set B. Let S and T be subsets of A, then:-

$$f(S \cup T) = f(S) \cup f(T)$$
$$f(S \cap T) \subseteq f(S) \cap f(T)$$

(2) No. of functions N_f on a set with n elements :-

$$N_f = n^n$$

(3) No. of functions N_f from a set A with n elements to another set B with m elements :-

$$N_f = m^n$$

www.ankurgupta.net

Relations

Binary Relation:-

Let A and B be sets. A binary relation from A to B is a subset of $A \times B$.

$$aRb \iff (a,b) \in R$$
$$a \not R b \iff (a,b) \notin R$$

Functions as Relations:-

A function is always a relation but a relation can be a function or not.

A relation can be used to express a one-to-many relationship between the elements of the set A and set B, while a function ~~represent~~ represents a relation where exactly one element of B is related to each element of A.

Relations on a Set:-

A relation on the set A is a relation from A to A.

M. Important

How many relations are there on a set with n elements?

Answer:- A relation on a set A is a subset of $A \times A$. Because $A \times A$ has n^2 elements and a set with m elements has 2^m subsets, there are 2^{n^2} subsets of $A \times A$.

Thus there are 2^{n^2} relations on a set with n elements

$\boxed{2^{n^2} > n^n}$ (No. of relation > No. of functions)

Properties of Relations :-

(i) Reflexive Relation :-

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

(ii) Symmetric Relation :-

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

$$\forall a \forall b\,((a,b) \in R \rightarrow (b,a) \in R)$$

(iii) Antisymmetric Relation :-

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

$$\forall a \forall b\,(((a,b) \in R \wedge (b,a) \in R) \rightarrow (a = b))$$

The terms symmetric and antisymmetric are not opposites, because a relation can have both of these properties or may lack both of them.

(iv) Asymmetric Relation :-

An asymmetric relation is a binary relation which is not a symmetric relation.

or

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

$$\forall a \forall b\,((a,b) \in R \rightarrow \neg (b,a) \in R)$$

~~# A relation is antisymmetric~~

A relation is asymmetric if and only if it is both antisymmetric and irreflexive.

(v) Irreflexive Relation :-

A relation R on a set A is irreflexive if for every $a \in A$, $(a,a) \notin R$. That is, R is irreflexive if no element in A is related to itself.

$$\forall a\,((a,a) \notin R)$$

A relation on a set can be neither reflexive nor irreflexive.

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

$\forall a \forall b \forall c \, (((a,b) \in R \wedge (b,c) \in R) \rightarrow (a,c) \in R)$.

How many relations are there on a set with n elements, that are :-

(i) Reflexive $\longrightarrow 2^{n(n-1)}$

(ii) Symmetric $\longrightarrow 2^{n(n+1)/2}$

(iii) Antisymmetric $\longrightarrow$

(iv) Asymmetric $\longrightarrow$

(v) Irreflexive $\longrightarrow 2^{n(n-1)}$

(vi) Reflexive & Symmetric $\longrightarrow 2^{n(n-1)/2}$

(vii) Neither reflexive nor irreflexive $\longrightarrow$

No. of different relations from a set with m elements to a set with n elements $\longrightarrow 2^{mn}$

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

Let R be a relation on a set A. The powers R^n, $n = 1, 2, 3 \ldots$, are defined recursively by :-

$R^1 = R$ and $R^{n+1} = R^n \circ R$.

The relation R on a set A is transitive if and only if $R^n \subseteq R$ for $n = 1, 2, 3 \ldots$

Inverse Relation :- Let R be a relation from a set A to a set B. The inverse relation from B to A, denoted by R^{-1}, is the set of ordered pairs :- $\{(b,a) \mid (a,b) \in R\}$

Complementary Relation :- The complementary relation $\bar{R}$ is the set of ordered pairs :- $\{(a,b) \mid (a,b) \notin R\}$

www.ankurgupta.net

Representing Relations Using Matrices:-

Let R is a relation from A to B. The relation R can be represented by the matrix $M_R = [m_{ij}]$, where:-

$$m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases}$$

The matrix of a relation on a set, which is a square matrix, can be used to determine whether the relation has certain properties.

A relation R is reflexive if all the elements on the main diagonal of M_R are equal to 1.

A relation R is irreflexive if all the elements on the main diagonal of M_R are equal to 0.

A relation R is symmetric if and only if:

$$M_R = (M_R)^T$$

A relation R is antisymmetric if and only if, either $m_{ij} = 0$ or $m_{ji} = 0$, when $i \neq j$.

Some Important Properties:-

(i) $M_{R_1 \cup R_2} = M_{R_1} \vee M_{R_2}$

(ii) $M_{R_1 \cap R_2} = M_{R_1} \wedge M_{R_2}$

(iii) $M_{S \circ R} = M_R \odot M_S$

Representing Relations Using Digraphs :-

A relation is reflexive if and only if there is a loop at every vertex of the directed graph.

A relation is irreflexive, if and only if, there is no loop at any vertex of the directed graph.

A relation is symmetric if and only if for every edge between distinct vertices in its digraph, there is an edge in the opposite direction.

A relation is antisymmetric if and only if there are never two edges in opposite directions between distinct vertices.

A relation is transitive if and only if whenever there is an edge from x to y and an edge from y to z, there is an edge from x to z.

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

$A \times (B \cup C) = (A \times B) \cup (A \times C)$

Closures of Relations :-

(i) Reflexive Closure :- The reflexive closure of R equals $R \cup \Delta$, where $\Delta = \{(a,a) \mid a \in A\}$ is the diagonal relation on A.

(ii) Symmetric Closure :- The symmetric closure of R equals $R \cup R^{-1}$, where :- $R^{-1} = \{(b,a) \mid (a,b) \in R\}$

(iii) Transitive Closure :- The transitive closure of a relation R equals the connectivity relation R^*, where :-

$$R^* = \bigcup_{n=1}^{\infty} R^n$$

Here R^* consists of the pairs (a,b) such that there is a path of length n from a to b in R.

or

$$M_{R^*} = M_R \vee M_R^{[2]} \vee M_R^{[3]} \vee \dots \vee M_R^{[n]}$$

where, n = no. of elements in matrix

Equivalence Relations :-

A relation on a set A is called an equivalence relation if it is reflexive, symmetric and transitive.

Two elements a and b that are related by an equivalence relation are called equivalent. Its represented by $a \sim b$.

Equivalence Classes :-

Let R be an equivalence relation on a set A. The set of all elements that are related to an element a of A is called the equivalence class of a.

The equivalence class of 'a' with respect to R is denoted by $[a]_R$

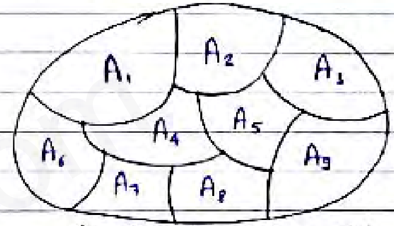
Or

If R is an equivalence relation on a set A, the equivalence class of the element a is :-

$$[a]_R = \{ s \mid (a, s) \in R \}$$

Partitions :-

The equivalence classes of an equivalence relation on a set form a partition of the set. The subsets in this partition are the equivalent classes. Two elements are equivalent with respect to this relation if and only if they are in the same subset of the partition.



A Partition of a Set

Intersection of two equivalence relations on a set is also an equivalence relation.

i.e. $R \rightarrow$ Equivalence relation on A

$S \rightarrow$ Equivalence relation on A

$R \cap S \rightarrow$ Equivalence relation on A.

Refinements :-

A partition P_1 is called a refinement of the partition P_2 if every set in P_1 is a subset of one of the sets in P_2.

www.ankurgupta.net

Partial Orderings:-

A relation R on a set S is called a partial ordering or partial order if it is reflexive, antisymmetric, and transitive. A set S together with a partial ordering R is called a partially ordered set, or poset, and is denoted by (S, R).

Members of S are called elements of the poset.

The notation $a \leq b$ is used to denote that $(a, b) \in R$ in an arbitrary poset (S, R).

Comparable and Incomparable Elements:-

The elements a and b of a poset $(S, \leq)$ are called comparable if either $a \leq b$ or $b \leq a$.

When a and b are elements of S, such that neither $a \leq b$, nor $b \leq a$, then a and b are called incomparable.

In "Partial Order", the adjective 'partial' is used to describe partial orderings because pairs of elements may be incomparable.

Total Order :-

If $(S, \preccurlyeq)$ is a poset and every two elements of S are comparable, S is called a totally ordered or linearly ordered set, and $\preccurlyeq$ is called a total order or a linear order. A totally ordered set is also called a chain.

If there exists some elements that are not comparable, then S is called a partially ordered set, and $\preccurlyeq$ is called a partial order.

Well-Ordered Set :-

$(S, \preccurlyeq)$ is a well-ordered set if it is a poset such that $\preccurlyeq$ is a total ordering and every nonempty subset of S has a least element.

E.g.:- The set Z, with the usual $\leq$ ordering, is not well-ordered because the set of negative integers, which is a subset of Z, has no least element.

Lexicographic Order :-

The words in a dictionary are listed in lexicographic order.

E.g.:- (a_1, a_2) is less than (b_1, b_2), that is:-

$$(a_1, a_2) \prec (b_1, b_2)$$

either if $a_1 \prec_1 b_1$ or if both $a_1 = b_1$ & $a_2 \prec_2 b_2$

(i) $(3, 5) \prec (4, 8)$

(ii) $(3, 8) \prec (4, 5)$

(iii) $(4, 11) \nprec (4, 9)$

Hasse Diagram :-

Steps to create Hasse Diagram :-

~~(i) Remove all self loops.~~

(i) Start with the directed graph of the relation.

(ii) Remove all self loops.

(iii) Remove all edges that must be in the partial ordering because of the presence of other edges and transitivity.

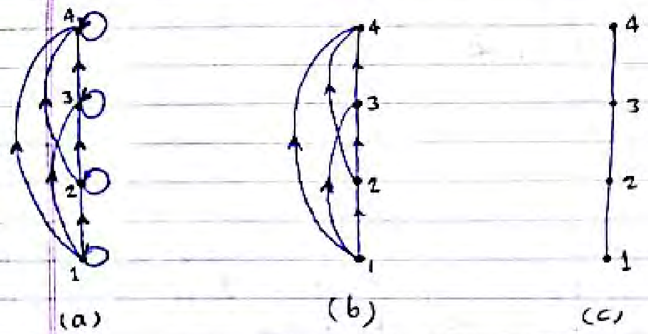
(iv) Arrange each edge so that its initial vertex is below its terminal vertex.

(v) Remove all the arrows on the directed edges, because all edges point "upword" towards their terminal vertex.

Hasse Diagrams are used to represent partial ordering relations.

The Hasse Diagram contains sufficient information to find the partial ordering.

Constructing the Hasse Diagram for $(\{1,2,3,4\}, \leq)$:-



www.ankurgupta.net

Maximal Element :-

An element of a poset is called maximal if it is not less than any element of the poset. That is, a is maximal in the poset $(S, \leq)$, if there is no $b \in S$ such that $a < b$.

Minimal Element :-

An element of a poset is called minimal if it is not greater than any element of the poset. That is, a is minimal in the poset $(S, \leq)$, if there is no $b \in S$ such that $b < a$.

Maximal and Minimal elements are the top and bottom elements in the hasse diagram.

Greatest Element :-

An element in a poset, that is greater than every other element, is called the greatest element. That is, a is the greatest element of the poset $(S, \leq)$ if $b \leq a$ for all $b \in S$.

The greatest element is unique when it exists.

Least Element :-

An element in a poset, that is less than every other element, is called the least element. That is, a is the least element of the poset $(S, \leq)$ if $a \leq b$ for all $b \in S$.

The least element is unique, when it exists.

Upper bound and lower bound :-

An element, that is greater than or equal to all the elements in a subset A of a poset $(S, \preccurlyeq)$, is called the upper bound of A.

An element, that is less than or equal to all the elements in a subset A of a poset $(S, \preccurlyeq)$, is called the lower bound of A.

Least Upper Bound :-

The element x is called the least upper bound of the subset A if x is an upper bound that is less than every other upper bound of A. It is denoted by lub(A).

The least upper bound of the subset A is unique if it exists.

Greatest Lower Bound :-

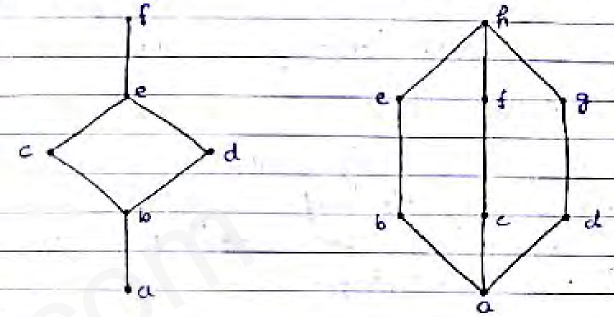
The element y is called the greatest lower bound of the subset A if y is a lower bound that is greater than every other lower bound of A. It is denoted by glb(A).

The greatest lower bound of the subset A is unique if it exists.

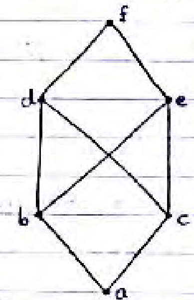
Lattices :-

A poset in which every pair of elements has both, a least upper bound and a greatest lower bound is called a lattice.

Eg :-



The below Hasse Diagram is not a lattice :-



In this diagram, the elements b & c don't have any least upper bound and the elements d & e don't have any greatest lower bound.

Topological Sorting :-

A total ordering $\preccurlyeq$ is said to be compatible with the partial ordering R if $a \preccurlyeq b$ whenever aRb.

Constructing a compatible total ordering from a partial ordering is called topological sorting.

It is generally used to order the tasks in such a way that if a and b are tasks where b can not be started until a has been completed, then a comes before b.

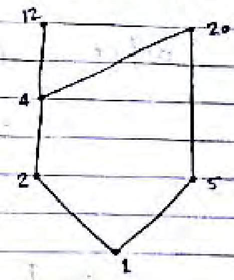
Algorithm for Topological Sorting :-

TOPOLOGICAL-SORT ((S, $\preccurlyeq$): finite poset)

```
    k := 1
    while S ≠ ∅
    begin
        a_k := a minimal element of S.
        S := S − {a_k}
        k := k + 1
    end
    {a_1, a_2 -- a_n} is a compatible total ordering
  of S. }
```

A poset can have multiple different - 2 topological sortings.

E.g:→ Total ordering for the poset ({1, 2, 4, 5, 12, 20}, |) are :-



(i) 1, 2, 5, 4, 12, 20

(ii) 1, 2, 4, 12, 5, 20

(iii) 1, 5, 2, 4, 20, 12 and so on.

Lattices (from Lipschutz) :-

Let L be a nonempty set closed under two binary operations called meet and join, denoted respectively by $\wedge$ and $\vee$. Then L is called a lattice if the following axioms hold where a, b, c are elements in L.

(1) Commutative law :-

(1a) $a \wedge b = b \wedge a$ (1b) $a \vee b = b \vee a$

(2) Associative law :-

(2a) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

(2b) $(a \vee b) \vee c = a \vee (b \vee c)$

(3) Absorption law :-

(3a) $a \wedge (a \vee b) = a$ (3b) $a \vee (a \wedge b) = a$

Lattice is sometimes denoted by $(L, \wedge, \vee)$.

Lattices and Order :-

Given a lattice L, we can define a partial order on L as follows:-

$$a \leq b \quad \text{if} \quad a \wedge b = a$$

OR

$$a \leq b \quad \text{if} \quad a \vee b = b$$

Let P be a poset such that least upper bound and greatest lower bound exist for any a, b in P.

$a \wedge b = lub(a, b)$ and $a \vee b = glb(a, b)$,

then $(P, \wedge, \vee)$ is a lattice.

Sublattices :-

Suppose M is a nonempty subset of a lattice L. We say M is sublattice of L, if M itself is a lattice (with respect to the operations of L).

Bounded Lattices :-

A lattice L is said to have a lower bound 0 if for any element x in L, we have $0 \leq x$.

Analogously, L is said to have an upper bound I if for any x in L, we have $x \leq I$.

We say L is bounded if L has both a lower bound 0 and an upper bound I.

In such a lattice, we have the identities:-

$a \vee I = I$, $a \wedge I = a$, $a \vee 0 = a$, $a \wedge 0 = 0$

for any element a in L.

Distributive Lattices :-

A lattice L is said to be distributive if for any elements a, b, c in L, we have the following (distributive law):-

(i) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$

(ii) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Otherwise, L is said to be nondistributive.

Complement :-

Let L be a bounded lattice with lower bound 0 and upper bound I. Let a be an element of L. An element x in L is called a complement of a if

$$a \vee x = I \quad \text{and} \quad a \wedge x = 0$$

In a bounded distributive lattice, complements are unique if they exist.

Complemented Lattice :-

A lattice L is said to be complemented if L is bounded and every element in L has a complement.

Groups

Semi-Groups and Monoids :-

Let S be a nonempty set with an operation, then :-

(i) S is called a semigroup if the operation is associative. ($a(bc) = (ab)c$).

(ii) If the operation also has an identity element, then S is called a monoid.

Groups :-

Let G be a nonempty set with a binary operation, then G is called a group if the following axioms hold :-

(i) Associative Law :- For any a, b, c in G, we have:

$$(ab)c = a(bc)$$

(ii) Identity Element :-

There exists an element e in G, such that $ae = ea = a$ for $\forall a \in G$.

(iii) Inverses :-

For each a in G, there exists an element a^{-1} in G, such that :-

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

Abelian Group :-

A group G is said to be abelian (or commutative) if the commutative law holds, i.e. if $ab = ba$ for every $a, b \in G$.

The number of elements in a group G, denoted by $|G|$, is called the order of G, and G is called a finite group if its order is finite.

Examples:-

(a) Consider the positive integers N, then:-

(i) $(N, +)$ is a semigroup.

(ii) $(N, \times)$ is a monoid.

(b) The set Z of integers is an abelian group under addition. The identity element is 0 and $-a$ is the additive inverse of a in Z.

Cyclic Subgroups:-

Let G be any group and let a be any element of G. As usual, we define $a^0 = e$ and $a^{n+1} = a^n \cdot a$.

All the powers of a:-

$$\ldots a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \ldots$$

form a subgroup of G called the cyclic group generated by a, and will be denoted by $gp(a)$.

The smallest positive integer m such that $a^m = e$ is called the order of a and is denoted by $|a|$. If $|a| = m$, then its cyclic subgroup $gp(a)$ has m elements given by:-

$$gp(a) = \{e, a, a^2, \ldots a^{m-1}\}$$

Cyclic Group:-

A group G is said to be cyclic if it has an element a, such that:-

$$G = gp(a).$$

Homomorphism:-

A mapping f from a group G into a group G' is called a homomorphism, if

$$f(ab) = f(a)f(b)$$

for every $a, b \in G$.

Example:- Let G be the group of real numbers under addition, and let G' be the group of positive real numbers under multiplication. The mapping $f: G \to G'$ defined by $f(a) = 2^a$ is a homomorphism because:-

$$f(a+b) = 2^{a+b} = 2^a 2^b = f(a) f(b)$$

www.ankurgupta.net

Combinatorics

Permutation and Combination

(1) $0! = 1$

(2) $P(n, r) = {}^nP_r = \frac{n!}{(n-r)!}$

(3) $C(n, r) = {}^nC_r = \frac{n!}{r!\,(n-r)!}$

(4) Any number means zero or more times.

(5) Some or all means one or more times.

(6) Sum Rule :-
If one event can occur in m-ways and another event in n-ways, then there are (m+n) ways in which one of these events can occur.

(7) Product Rule :-
If one event can occur in m-ways, and for each of m-ways, there are associated n-ways in which another event can occur, then there are mn-ways in which these two events can occur.

(8) Number of ways of arranging r-objects, when they are selected from n-objects, allowing repeatition $= n^r$

(9) Suppose there are n_1-objects of the first kind, n_2-objects of the second kind ---- n_k-objects of the k^{th} kind, then the no. of ways to select one or more objects from the collection is:-
$(n_1+1)(n_2+1) \ldots (n_k+1) - 1$

(10) Consider n-cells and r-distinct objects to be distributed, then:-

(a) If $n \geq r$ and if each cell can hold only one object, then there are $({}^{n}P_r = {}^{n}C_r \cdot r!)$ - ways to distribute these r-objects.

(b) If $r \geq n$ and if each cell can hold only one object, then there are $({}^{r}P_n = {}^{r}C_n \cdot n!)$ - ways to distribute these r-objects.

(c) If each cell can hold any number of objects then there are n^r ways of distributing the objects.

(d) If there are n_1-objects of the first kind, n_2-objects of the second kind ... n_k-objects of the k^{th} kind, then there are $n!/(n_1!\, n_2! \ldots n_k!)$ ways of distributing the objects, where $n_1+n_2+\ldots+n_k = n$

(e) If there are n_1-objects of the first kind, n_2-objects of the second kind ... n_k-objects of the k^{th} kind, and if $n_1+n_2+\ldots+n_k = r \leq n$, then there are ${}^{n}P_r/(n_1!\, n_2! \ldots n_k!)$ - ways of distributing the r-objects among the n-cells where each cell can hold only one object.

☆☆ (f) If each cell can hold any no. of objects and if the objects are ordered inside the cells, then there are ${}^{n+r-1}P_r$ - ways of distributing the r-objects among n-cells.

(11) Consider n-cells and r-similiar objects to be distributed, then :-

(a) If $r \leq n$, and each cell can hold only one object, then there are ${}^{n}C_r$ - ways of distributing the r-objects.

☆☆ (b) If a cell can hold any no. of objects, then there are ${}^{n+r-1}C_r$ ways of distributing the r-objects.

(c) If $r \geq n$ and if no cells remain empty, then there are ${}^{r-1}C_{n-1}$ ways of distributing the r-objects.

$$\boxed{{}^{r-1}C_{n-1} = {}^{n+(r-n)-1}C_{r-n} = {}^{r-1}C_{r-n} = {}^{r-1}C_{n-1}}$$

Every cell contains at least one object, and we have to distribute $(r-n)$ - objects

(d) If each cell should contain atleast q-objects and if $r \geq nq$, then there are ${}^{n+r-nq-1}C_{r-nq}$ - ways of distributing the r-objects

(12) Circular Permutation :-

The number of ways in which n-different things can be arranged in a circle is $(n-1)!$

If the clockwise and anti-clockwise arrangements are not distinguished, then the no. of arrangements is $\frac{1}{2}(n-1)!$

(13) Permutation and Combination under certain conditions :-

(a) No. of combinations of n-dissimiliar things taken r at a time, when p-particular things always occur = ${}^{n-p}C_{r-p}$

(b) No. of combinations of n-dissimiliar things taken r at a time, when p-particular things never occur = ${}^{n-p}C_{r}$

(c) No. of permutations of n-dissimiliar things taken r at a time, when p-particular things always occur = ${}^{n-p}C_{r-p} \cdot r!$

(d) No. of permutations of n-dissimiliar things taken r at a time, when p-particular things never occur = ${}^{n-p}C_{r} \cdot r! = {}^{n-p}P_{r}$.

(14) Division into groups :-

(a) The no. of ways in which (m+n) things can be divided into two groups containing m and n things respectively :-

$$ {}^{m+n}C_m \cdot {}^{n}C_n = \frac{(m+n)!}{m!\,n!} $$

(b) If n = m, the groups are equal and in this case, the no. of different ways of subdivision :-

$$ \frac{(2m)!}{m!\,m!\,2!} $$

(c) If 2m things are to be divided equally between two persons, then the no. of ways of subdivision :- $\frac{(2m)!}{m!\,m!}$

(15) Selection out of identical things :-

(a) If there are n- identical things, out of which we have to draw r- things, then the number of combinations will be 1.

(b) If there are n- identical things and we have to make a selection of any no. of things including none, then the no. of selections will be n+1.

(c) Total no. of ways in which it is possible to make selection by taking some or all out of p+q+r.. things, where p are alike of one kind, q are alike of one kind, and so on :-

$$ (p+1)(q+1)\_\_\_-1 $$

(d) If there are p- things alike of one kind, q alike of one kind, while r of all different kind, then total no. of non-empty selection is :-

$$ (p+1)(q+1) \cdot 2^r - 1 $$

(16) If some or all of n-things be taken at a time, where all n-things are of different kind, then the number of combinations will be :-

$$ \boxed{{}^{n}C_1 + {}^{n}C_2 + \_\_\_ + {}^{n}C_n = 2^n - 1} $$

(17) Gap Method :-

Suppose 5-males A, B, C, D, E are arranged in a row as :-

$\times A \times B \times C \times D \times E \times$

Now if 3-females P, Q, R are to be arranged so that they are never together, we will arrange them in b/w 6-gaps.

So, total no. of arrangements $= {}^5P_5 \cdot {}^6P_3$

$= 5! \cdot {}^6P_3$

www.ankurgupta.net

Counting and Summation

Exponent of prime p in n! :-

$$E_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^s}\right]$$

Example :- Find the exponent of 15 in 100!

Solution :- We have, $15 = 3 \times 5$

Now,

$$E_3(100!) = \left[\frac{100}{3}\right] + \left[\frac{100}{3^2}\right] + \left[\frac{100}{3^3}\right] + \left[\frac{100}{3^4}\right]$$

$$= 33 + 11 + 3 + 1 = 48$$

$$E_5(100!) = \left[\frac{100}{5}\right] + \left[\frac{100}{5^2}\right]$$

$$= 20 + 4 = 24$$

$$E_{15}(100!) = \min(48, 24)$$

$$= 24 \text{ Ans}$$

Summation :-

(1) $\sum n = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$

(2) $\sum n^2 = 1^2 + 2^2 + \ldots + n^2 = \frac{1}{6} n(n+1)(2n+1)$

(3) $\sum n^3 = 1^3 + 2^3 + \ldots + n^3 = \left[\frac{1}{2} n(n+1)\right]^2$

The Pigeonholes Principle :-

If n-pigeon holes are occupied by $kn+1$ or more pigeons, where k is a positive integer, then at least one pigeonhole is occupied by $(k+1)$ or more pigeons.

Example :- Find the minimum no. students in a class, so that ~~three are~~ of them are born in the same month.

Solution :-

$$2 \times 12 + 1 = 25 \text{ Ans}$$

Recurrence Relations

Recurrence Relation :-

A recurrence relation for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely, $a_0, a_1, \ldots, a_{n-1}$, for all integers n with $n \geq n_0$, where n_0 is a nonnegative integer.

A sequence is called a solution of a recurrence if its terms satisfy the recurrence relation.

Solving Recurrence Relations :-

(1) Substitution Method :-

This is done in two steps :-

(a) Apply the recurrence formula iteratively and look for a pattern to predict an explicit formula using internal conditions

(b) Use induction to prove the predicted formula

Example :- $a_n = a_{n-1} + 3, \quad n \geq 2$ and $a_1 = 2$

Now,

$$a_n = (a_{n-2} + 3) + 3 = a_{n-2} + 2 \cdot 3$$

$$a_n = (a_{n-3} + 3) + 2 \cdot 3 = a_{n-3} + 3 \cdot 3$$

$$\vdots$$

$$a_n = (a_{n-i} + 3) + (i-1)\,3 = a_{n-i} + i \cdot 3$$

Put $i = n-1$

$$a_n = a_1 + (n-1) \cdot 3$$

$$\Rightarrow a_n = 2 + 3n - 3$$

$$\Rightarrow \boxed{a_n = 3n - 1}$$

classmate
Date
Page

(2) Solving Linear Homogeneous Recurrence Relations with Constant Coefficients :-

Definition :-
A linear homogeneous recurrence relation of degree k with constant cofficients is a recurrence relation of the form :-

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$$

where $c_1, c_2 \ldots c_k$ are real numbers and $c_k \neq 0$

Examples :-
(a) The recurrence relation $f_n = f_{n-1} + f_{n-2}$ is a linear homogeneous recurrence relation of degree two
(b) The recurrence relation $a_n = a_{n-5}$ is a linear homogeneous recurrence relation of degree five.

Solution :-
Basically, when solving such recurrence relations, we try to find out solutions of the form $a_n = r^n$ where r is a constant.

Now $a_n = r^n$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$ if and only if :-

$$r^n = c_1 r^{n-1} + c_2 r^{n-2} + \ldots + c_k r^{n-k}$$
$$\Rightarrow r^n - c_1 r^{n-1} - c_2 r^{n-2} \ldots - c_k r^{n-k} = 0$$
$$\Rightarrow r^k - c_1 r^{k-1} - c_2 r^{k-2} \ldots - c_k = 0$$

This is called the characteristic equation of the recurrence relation.

classmate
Date
Page

Example :- What is the solution of the recurrence relation $a_n = a_{n-1} + 2a_{n-2}$ with $a_0 = 2$ and $a_1 = 7$?

Solution :-
The characteristic equation of the recurrence relation is $r^2 - r - 2 = 0$
Its roots are :- $r = 2$ and $r = -1$

Hence, the solution of this recurrence relation is :-

$$a_n = \alpha_1 (2)^n + \alpha_2 (-1)^n$$

for some constants α_1 & α_2

Since, we know that $a_0 = 2$ and $a_1 = 7$, it follows that :-

$$a_0 = 2 = \alpha_1 + \alpha_2$$
$$a_1 = 7 = \alpha_1 \cdot 2 + \alpha_2 \cdot (-1)$$

Solving these two equations gives us :-
$\alpha_1 = 3$ and $\alpha_2 = -1$

Therefore, the solution to the recurrence relation is :-

$$a_n = 3 \cdot 2^n - (-1)^n$$

If both the roots of the characteristic equation are same :-
The solution of the recurrence will be :-

$$a_n = \alpha_1 (r_0)^n + \alpha_2 \cdot n \cdot (r_0)^n$$