Propositions

Def^{n}: A sentence that is either true or false but not both is called proposition

Precedence Order:- $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

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

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

De Morgan's Laws

1. $\neg(p \vee q) \equiv \neg p \wedge \neg q$
2. $\neg(p \wedge q) \equiv \neg p \vee \neg q$

Defn Contrapositive

If $p \rightarrow q$

then $\neg q \rightarrow \neg p$

Q. Show that negation of $p \rightarrow q$ is logically equivalent to $p \wedge \neg q$

Quantifier

- Universal Quantifier ($\forall x$; for all x)
- Existential Quantifier ($\exists x$; there exists x)

25/07/16

GENERALIZED DE MORGAN LAWS FOR LOGIC

Propositional function (P)

Quantifier: Universal, Existential

If P is a propositional fn then each pair of propositions in (a) & (b) has the same value, true or false.

(a) $\neg(\forall x\, P(x))$; $\exists x\, (\neg P(x))$

(b) $\neg(\exists x\, P(x))$; $\forall x\, (\neg P(x))$

Proof & Logic

Mathematical system:
- Axioms, already proved.
- Definitions, new concepts in terms of existing concepts.
- Term, already existing concepts.

Theorem → It is a proposition that has been proved.

Lemma → It is a theorem which is useful to prove other theorem.

Corollary → It is a theorem that follows easily from other theorems.

* Direct Proof
* Proof by contradiction
* Proof by Contraporitive
* Proof by Cases
* Proof by equivalence

If $p(x_1, x_2, \ldots, x_n)$ (true) then $q(x_1, x_2, \ldots, x_n)$ (true).

p	q	p→q	
T	T	T	✓
T	F	F	x
F	T	T	
F	F	T	

In case of theorem, we take hypothesis true & prove consequent true.

Proof by contradiction:

Defn → A proof by contradiction establishes $p \to q$ by assuming p is true & then conclusion q is false & then using $p \wedge \neg q$ as well as other axioms, previously derived theorems, rules of inference decides (try to find) a contradiction $p \to \neg q$

Proof by contrapositive

Suppose we prove by contradiction $p \to q$ ⟩
$\neg q \to \neg p$

Ex: for all $x \in R$

if x^2 is irrational then x is irrational.
$p \to q$

if x is rational then x^2 is rational. → True
$\neg q \to \neg p$ ⇒ $p \to q$ True.

Defn An argument is a sequence of propositions.

p_1
p_2
⋮
p_n
$\therefore q$

or $p_1, p_2, p_3, \cdots p_n \mid \therefore q$

If $(p_1, p_2, \cdots p_n)$ are all true, then q is true.

We assume it to be true despite of its actual truth value.

---

* Tautology — Set of propositions that are Always true
* Contradiction — Always false
* Contigency — Neither true nor false (Neither tautology nor contradiction)

STRONG FORM OF MATHEMATICAL INDUCTION

Principal of Mathematical Induction:-

BS: $S(1)$ is true — If $S(n)$ is a propositional fn.

IS: for all $n \geq 1$, if $S(n)$ is true then $S(n+1)$ is true.

Then $S(n)$ is true for every the integer n.

Suppose we have a propositional function $S(n)$ whose domain of discourse is set of integers greater than or equal to n_0

BS. $S(n_0)$ is true

IS. for all $n > n_0$, if $S(k)$ is true then $S(n)$ is true. $(n_0 \leq k < n)$

Then $S(n)$ is true for every integer $n > n_0$.

Power Set: The set of all subsets of a given set is called the power set. → $P(x)$

$|X| = 3 \quad |P(x)| = 2^3$

Properties of set.

A, B, C $\cup, \cap, -$

Associative: $(A \cup B) \cup C = A \cup (B \cup C)$

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

Commutative: $A \cup B = B \cup A$, $A \cap B = B \cap A$.

Distributive: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

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

Identity: $A \cup \phi = A$, $A \cap U = A$

(U - universal)

Complement: $A \cup \bar{A} = U$, $A \cap \bar{A} = \phi$

Bound: $A \cup U = U$, $A \cap \phi = \phi$

Absorption: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$.

11/08/16

Partition of sets.

A partition of a set X divides X into non-overlapping subsets.

Prove the absorption law :-

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

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

Def^n : Let X and Y be two sets. The function is defined as a subset of cartesian product $X \times Y$ where for each $x \in X$, there is exactly one element $y \in Y$ with the ordered pair $(x, y) \in f$.

X - domain of f
y - Range of f.

22/08

Relations

Relations generalize the notion of functions.

Students X = {A, B, C, D}
Course Y = {Comp Sc., Math, Hum., Hist.} → R

Subset of Cartesian product of X & Y. → Relation

R = {(A, Comp Sc), (A, Hum), (B, Hist), (B, Hum) - -}

PAGE:
DATE: / /

x can relate to only one y.

Function v/s Relation → one x can relate to more than one y.

* Both are cartesian product
but function is a special class of Relation with 2 properties.

1. X is the domain
2. for each $y \in Y$, $(x, y) \in f$, y is the range.

1. Reflexive : A relation R on set X is reflexive if $(x, x) \in R$, for all $x \in X$.

2. **Symmetric** A relation R from a set X to a set Y is symmetric if $\forall (x,y) \in R$ and $x \in X, y \in Y$ then $(y,x) \in R$.

Anti-Symmetric A relation R on a set X is called anti-symmetric if $\forall (x,y) \in R$, $x, y \in X$ then $(y,x) \notin R$

If no member $(x,y) \in R$ where $x \neq y$.
$x, y \in X$ then $(y,x) \notin R$.

3. **Transitive** A relation R on set X is transitive if $(x,y) \in R$, $(y,z) \in R$, $x, y, z \in X$ $(x=y=z)$

Ex.

3. **Transitive** A relation R on set X is transitive if $(x,y) \in R$, $(y,z) \in R$, $x, y, z \in X$ $(x=y=z)$

Ex.

PARTIAL ORDER A relation R on a set X is called a partial order if the relation is Reflexive, anti-symmetric, and transitive

not $(x \neq y$ and $x \leq y)$ Not satisfying P.O.

If for a set X, each pair of elements (for all x, y) are comparable then we define the relation as a total order or linear order, chain.

A set X together with the relation R is called partially ordered set or poset.

Well Ordered Set:

$(X, \leq)$ is a well ordered set if it a poset and the relation R $(\leq)$ is a total order and every non-empty subset has a least element.

Equivalence Relation:-

A relation on a set X is equivalence relation if the relation is reflexive, symmetric & transitive.

25/08/16

Equivalence Class

Equivalence Relation → Reflexive, Symmetric, Transitive.

Theorem:- Let R be a equivalence relation on a set X, and

$[a] = \{x \in X \mid xRa\}$

Then $S = \{[a] \mid a \in X\}$ is a partition on X

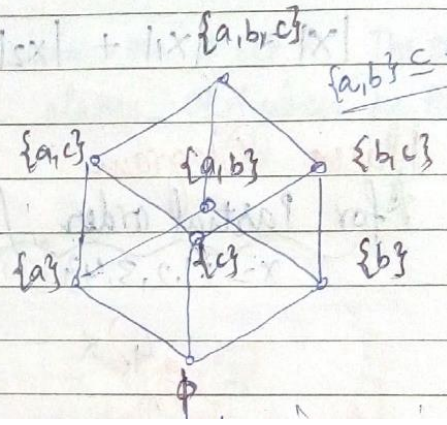
Here $[a]$ is set of elements of X that are related to a, $a \in X$.

Hasse Diagram

Power Set $P(S)$

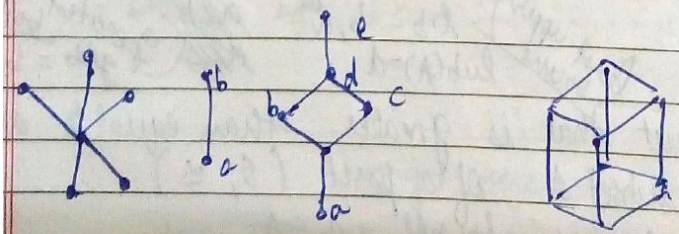
where $S = \{a, b, c\}$

$P(S) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{c,a\}, \{a,b,c\}\}$



Application of poset - Lattice

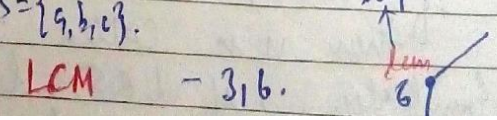
In a poset if every pair has both greatest lower bound (glb) and least upper bound (lub) then it is called a lattice.



$S = \{a, b, c\}$.

lub.

poset $(Z^+, /)$ - LCM - 3, 6.



Closures of Relations

* Computer Network
* Connectivity.

Let R be a relation on a set A with some property P, reflexivity, symmetry, transitivity. If S be a relation containing R with property P such that S contains all the relations (R) with property P then S is the closure of R.

Recurrence relation is an equation that generate the nth value from certain of its predecessors (previous terms) initial conditions must be explicitely defined.

★ Problem: Transfer all disks from peg 1 to peg 2 1) One disc at a time
2) Whenever we assume a disk in a peg, then disc with small diameter only can be placed on the disc with larger diameter

3 pegs – n disk with different size, stacked in a peg

Soln • Sequences – no. of moves.

(largest) n^{th} → 1 to 2
all $(n-1)$ to 3.

$c_1 = 1$
$c_2 = 3$

→ $n-1$ from 1 to 3 & then from 3 to 2.

$c_n = 1 + 2 c_{n-1}$.

Methods:-

1. Iteration
2. Linear homogeneous recurrence relation.

Let a_n be a linear homogeneous recurrence relation of order k with constant coefficients.

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}, \quad c_k \neq 0.$$

$c_1, c_2 \dots c_k$ → Constant coefficients

• $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ – 2nd order l.h.r.r.

$a_n = 2n\, a_{n-1}$

Not a l.h.r.r

$a_n = a_{n-1} + 2n$

$a_n = c_1 a_{n-1} a_{n-2}$ → Not l.h.r.r but homogeneous

It is a non-linear recurrence relation.

Ex. 2

$a_n = 5a_{n-1} - 6a_{n-2}$

$a_0 = 7, \quad a_1 = 16.$

Let the sol^n be $V_n = t^n$

(We are trying to get the sol^n of a simplified recurrence relation & then to develop the final one.)

$V_n = 5V_{n-1} - 6V_{n-2}$

$t^n = 5t^{n-1} - 6t^{n-2}$ — divide it by t^{n-2}

$t^2 = 5t - 6$

$t^2 - 5t + 6 = 0$

$(t-2)(t-3) = 0$

$t = 2, 3.$

$n=2 \cdot S_{n-1}$

$S_n = 2^n$

* If S & T are the solution then $bS + dT$ will be the sol^n also. $S_n = 2^n$, $T = 3^n$

Theorem: Let $a_n = c_1 a_{n-1} + c_2 a_{n-2}$ be a 2nd order linear homogeneous recurrence relation with constant coefficients.

If both roots of $(t^2 - c_1 t - c_2 = 0)$ are equal to 'r' then there exists b & d such that

$a_n = br^n + dnr^n$ exist and gives the sol^n of above relation.

Theorem:- Let $c_1, c_2, \ldots c_k$ be real numbers

$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0$

has t distinct roots $r_1, r_2, \ldots, r_t$ with multiplicities $m_1, m_2, \ldots, m_t$

$m_1 + m_2 + \cdots + m_k = k$

$\{a_n\}$ is a sol^n

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

iff

$a_n = (a_{1,0} + a_{1,1} n + \cdots + a_{1,m_1-1} n^{m_1-1}) r_1^n +$

$(a_{2,0} + a_{2,1} n + \cdots + a_{2,m_2-1} n^{m_2-1}) r_2^n +$

$\vdots$

$(a_{t,0} + a_{t,1} n + \cdots + a_{t,m_t-1} n^{m_t-1}) r_t^n$

Examples:- $a_n = a_{n-1} + a_{n-2} + n!$

$a_n = a_{n-2} + n^2 + 5$

$a_n = a_{n-1} + 5^n$

Theorem: If $\{a_n^{(p)}\}$ is a particular solution of the nonhomogeneous linear recurrence relation with constant coefficient $a_n = c_1 a_{n-1} + \dots + c_k a_{n-k} + F(n)$, then every solution is of the form $\{a_n^{(p)} + a_n^{(h)}\}$ where $\{a_n^{(h)}\}$ is a solution of the associated homogeneous recurrence relation $a_n = c_1 a_{n-1} + \dots + c_k a_{n-k}$.

$\rightarrow a_n^{(p)} = c_1 a_{n-1}^{(p)} + c_2 a_{n-2}^{(p)} + \dots + c_k a_{n-k}^{(p)} + F(n)$ $\leftrightarrow$

P.P. Simple Form

Theorem

If $(n+1)$ objects are put in n boxes then at least one box contains two or more objects.

Proof

$f: X \to Y$

- If X has more no. of elements than Y, then f is not one-to-one.
- If X & Y both have same no. of elements & f is one-to-one then f is onto.
- If ——— onto
  then f is one-to-one.

Application 3

Given m integers $a_1, a_2, \dots, a_m$ there exist integer k and l with $0 \le k < l \le m$ such that $a_{k+1} + a_{k+2} + \dots + a_l$ is divisible by m.

Consider the following m sums.

a_1, a_1+a_2, $a_1+a_2+a_3$, ..., $a_1+a_2+\cdots+a_m$

If we divide each sum by m, then the remainder will be 1 to $m-1$ (we will not consider 0)

m sums → m no. of pigeons

$m-1$ remainders → $(m-1)$ pigeonholes

⇒ Two sums must have same remainders when divided by m.

Let the following two sum have the same remainder r :-

$$a_1+a_2+\cdots+a_k = bm+r \quad \text{---(1)}$$

Theorem: Let $A_1, A_2, \ldots A_n$ be finite sets

then

$$|A_1 \cup A_2 \cup A_3 \cdots \cup A_n| = \sum_{1\le i\le n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |(A_1 \cap A_2 \cap A_3 \cdots \cap A_n)|$$

Semigroup

G is an algebraic str. defined as $\{G, \cdot\}$ that associates to each ordered pair $a, b \in G$ an element $a \cdot b \in G$ such that the following properties hold

A1 : closure , $a, b \in G \Rightarrow a \cdot b \in G$

A2 : associative , $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

then G is called Semigroup.

Monoid

G is a Monoid defined as $\{G, \cdot\}$ that associates to each ordered pair $a, b \in G$ an element $a \cdot b \in G$ such that the following properties hold

A1 : closure , $a, b \in G \Rightarrow a \cdot b \in G$

A2 : associative , $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

A3 : (Identity) and there exist an element $e \in G$ such that $a \cdot e = e \cdot a = a$, $a \in G$

Group.

G is a Group defined as $\{G, \cdot\}$ that associates to each ordered pair $a, b \in G$ an element $a \cdot b \in G$, such that the following properties hold

A1 : closure

A2 : Associative

A3 : Identity

A4 : Inverse :-

Inverse element → there exists an element a^{-1}

$a \cdot a^{-1} = e$, $a, a^{-1} \in G$

$a \cdot I_R = e$, $a \cdot b \in G$

$I_L \cdot a = e$

$a^{-1} \cdot a = e$

* If group holds A5 also (commutativity) → ABELIAN GROUP.

Cyclic Group

A group is cyclic if every element of G can be generated from one particular element $a \in G$ as a power of a^k, k is an integer.

a – generator

Cyclic group is abelian

Subgroup

We consider a nonempty subset H of group G. H is defined as the subgroup of G if it is closed under the group operation of G and satisfies the other group properties.

Ex. H – Set of integers
G – Set of rational no.s.
op^n – addition

Coset

Let a be an element of group G with binary operation $*$. H is the subgroup of G

The set $a*H = \{a*h ; h \in H\}$ is the left coset of H

and $H*a = \{h*a ; h \in H\}$ is the right coset of H.

If G is commutative $a*h = h*a$ ∴ coset of H

LAGRANGE'S THEOREM

Let G be a group of order n (→ cardinality) and H (→ subgroup) be of order m. Then m divides n and the partition G/H consists of n/m cosets of H

Ring: A Set R (R, +, x) with two binary operations addition and multiplication that satisfies the following axioms

A1-A5 – wrt addition & additive identity 0, inverse is (-a), $a \in R$.

M1 – closure under multiplication

M2 – associative with multiplication $a \times (b \times c) = (a \times b) \times c$

M3 – Distributive (multiplication is distributive over addition).

$a \times (b+c) = a \times b + a \times c$

$(b+c) \times a = b \times a + c \times a$.

M4 – Commutative over multiplication

$a \times b = b \times a$.

Commutative Ring: A1-A5, M1-M4

Field (F, +, x): is a set of elements with two binary operators, +, x that satisfies axioms A1-A5, M1-M6 and

M7 – Multiplicative inverse

- addition, subtraction

$a - b = a + (-b)$

- Multiplication

a^{-1} $\quad a/b = a \times b^{-1}$

Finite Field: If the no. of elements are finite.

$q = p^m$

5	2	3
6	1	6
	↑ Additive Inverse	↑ Multiplicative Inverse

Galois Field

↳ GF(p)

↳ GF(p^m) — Extended field

for any +ve integer we get the field GF(p^m).

Arithmetic Field

$q = p^m$

* Conversion between integer arithmetic to polynomial arithmetic and both follow modular arithmetic $a \bmod n (a = k_1 n + r_a)$
* To construct the field we need one irreducible polynomial.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} = \sum_{i=0}^{n-1} a_i x^i$$

$p(x)$ → irreducible polynomial of degree $(n-1)$.