DATE: PAGE:

for $\langle Z_6, +\rangle$

Let $H = \{0, 2, 4\}$

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

H is a ~~group~~. subgroup of $\langle Z_6, +\rangle$.

∴

Sub group

$\langle G, * \rangle$

Let G be a group, H be subset of G. and If we say that H is group under binary operation * then we say. H is sub group of $\langle G, * \rangle$

Let $\langle G, * \rangle$ be a group under binary operation *, with e as it's identity element

If $\exists a \in G$, the group $\langle G, * \rangle$ can be generated using the integral power of an element 'a' then that group is called as cyclic group. And 'a' is called as generator of group

$a^n = a \cdot a \cdot a \cdots \cdot a$ (n times)

Ex: $\langle Z_6, + \rangle = \{0, 1, 2, 3, 4, 5\}$

$1^0 = 0 \bmod 6 = 0$
$1^1 = 1 \bmod 6 = 1$
$1^2 = 2 \bmod 6 = 2$
$1^3 = (1+1+1) \bmod 6 = 3$
$1^4 = 4 \bmod 6 = 4$
$1^5 = 5 \bmod 6 = 5$

∴ 1 is the generator &
G is cyclic group

DATE: PAGE:

Multiplicative group mod n

Represented as. $\langle Z_n^*, \bullet \rangle$ or $\langle Z_n^*, \times \rangle$

Z_n^* is a group only if n is a prime number.

If n is a composite number then only co-prime's of n are present in Z_n^*

Z_5^*

*	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$ax = 1 \bmod n$

x is multiplicative inverse of a.

$\langle Z_{12}^*, \cdot \rangle = \{1, 5, 7, 11\}$

$\langle Z_6^*, \cdot \rangle = \{1, 5\}$

DATE: PAGE:

Additive group mod n

[Addition modulo n operation]

$a \equiv a' \bmod n$
$b \equiv b' \bmod n$
$a+b = (a'+b') \bmod n.$

This operation is denoted by $\langle Z_n, +_n \rangle$ or $\langle Z_n, + \rangle$

Ex: $\langle Z_6, + \rangle$

There are 6 Equivalence classes

$[0]_6 = \{-12, -6, 0, 6, 12\}$
$[1]_6 = \{-11, -5, 1, 7, 13\}$
$[2]_6 = \{-10, -4, 2, 8, 14\}$
⋮
$[5]_6 = \{-7, -1, 5, 11, 17\}$

$\therefore [13]_6 + [-4]_6 = [13 + -4]_6$
$1 + 2 = [9]_6$
$3 = 3.$

Cayley table

Z_6	0	1	2	3	4	5.
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4.

$e=0$	
a	a'
0	0
1	5
2	4
3	3.

Multiplicative

Represented

Z_n^* is a g
a prime

If n is
only co-prim
in Z_n^*

Z_5^*

*	1	2
1	1	2
2	2	4
3	3	1
4	4	3

$ax \equiv 1$
x is m

$\langle Z_{12}^* $
$\langle Z_6^*$

PAGE:

DATE: PAGE:

Group

Monoid and existence of Inverse.

$\forall a \in S, \exists a' \in S \mid a*a' = a'*a = e$.

~~Commutative~~

Abelian group

Group and commutative property

$\forall a, b \in S, a*b = b*a$.

Q) Let G be a set all non zero real numbers.
Let $a*b = \frac{1}{2}ab$.
S.T $\langle G, * \rangle$ is an abelian group.

-> i) $\langle G, * \rangle$ is closure property
$\forall x, y \in G, \frac{1}{2}xy \in G$.

ii) $\forall x, y, z \in G$.
$(x*y)*z = x*(y*z)$
$(\frac{1}{2}xy)*z = x*(\frac{1}{2}yz)$
$\frac{xyz}{4} = \frac{xyz}{4}$

$\therefore \langle G, * \rangle$ is associative

iii) $\exists 2 \in G$
$\forall x \in G, x*2 = 2*x = x$

iv) $\forall x \in G, \forall \frac{4}{x} \in G$
$x*\frac{4}{x} = \frac{4}{x}*x = 2$

v) $\forall x, y \in G, x*y = y*x \Rightarrow \frac{1}{2}xy = \frac{1}{2}yx$

Group theory.

DATE: PAGE:

Basics of Cryptography is group theory

1) Carrier of Algebra
   set on which operations on done
2) Operation
   operation done on COA
3) Distinguished element.
   Identity element, Inverse element

Semigroup

① S should be closed under the operation *
   $\langle S, * \rangle$
   i.e. $\forall x, y \in S$ then $x * y \in S$ and $y * x \in S$

2) Associative property

$\forall a, b, c \in S \quad (a*b)*c = a*(b*c)$

Monoid

Semigroup and existence of identity element.
$\exists e \in S$,
$\forall a \in S$, $a*e = a$ and $e*a = a$

Group
Monoid
Inverse
$\forall a \in S$,
Commute
Abelia
Group
$\forall a, b \in S$
Let
real
Let
S.T <
-> i) <
ii)
iii)
iv)

DATE: PAGE:

Consider a function.
$F: R \to R$. $g: R \to R$.
$f(x) = 3x+7$. $g(x) = x(x^3-1)$.
(a) verify one-one.

$f(x)$ is one to one
$g(x)$ is not one to one

$f: Z \to Z$ $f(a) = a+1$ $\forall a \in Z$.
verify f is bijective
as $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
$\therefore$ $f(a)$ is injective
as $\forall a \in Z \Rightarrow a+1 \in Z$ $\therefore$ $f(a)$ is surjective
$\therefore$ $f(a)$ is bijective

S.T. $f: R \to R^+$ $F(x) = x^2$.
is surjective function
Consider $y = f(x) = x^2$.
as $y > 0$.
and $\forall y \in R^+$, $\exists x \in R$ ll $y = x^2$
$\therefore$ $f(x)$ is surjective function

S.T. $f: R^+ \to R^+$ $f(x) = x^2$
is bijective

DATE: PAGE:

Invertible functions

$f: A \to B$
$g: B \to A$
$y = f(x)$ $\quad g(y) = x$.

$f^{-1}(f(x)) = x$ & $f(f^{-1}(y)) = y$
$f^{-1} \circ f = I_A$
$f \circ f^{-1} = I_B$

Q) Let $A = \{1, 2, 3, 4\}$ $B = \{a, b, c\}$ $C = \{w, x, y, z\}$

$F = \{(1,a) (2,a) (3,b) (4,c)\}$
$g = \{(a,x) (b,y) (c,z)\}$
Find $g \circ f$.

$g \circ f = \{(1,x) (2,x) (3,y) (4,z)\}$

Q) $F(x) = x^3$, $g(x) = x^2 + 1$

→ $g \circ f = g(f(x)) = g(x^3) = x^6 + 1$
$f \circ g = f(g(x)) = f(x^2+1) = (x^2+1)^3$.
$g \circ g = g(x^2+1) = (x^2+1)^2 + 1$
$f \circ f = f(f(x)) = f(x^3) = x^9$.

Q) Consider a
$F: R \to R$.
$f(x) = 3x + 7$.
verify

$f(x)$ is
$g(x)$ is

2) $f: Z \to Z$
verify
→ as $f(x$
$f(a$
as $\forall a$
$\Rightarrow f(a$

3) S.T.
is
→ Consi
as
and
$\therefore f$

4) S.T.

DATE: PAGE:

are functions.

(4,4)}
nly relation

ge
+4)}
}

x,y,z}

5,y)}

2,3,4}
y,x}

ing.

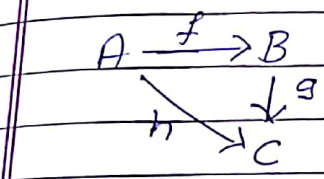
ty.
nt

ve, injective
njective.

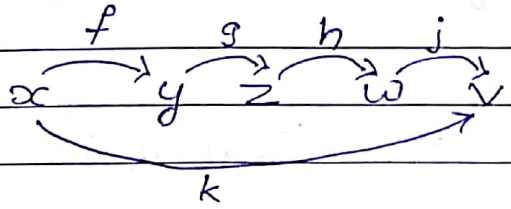
DATE: PAGE:

Q) If 2187 function from A → B.
|B| = 3 |A| = ?
$2187 = 3^{|A|}$
$\therefore |A| = \log_3 2187$

Composition of functions



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



$k = j \circ h \circ g \circ f$
$k(x) = j(h(g(f(x))))$
$k(x) = j(h(g(y)))$
$k(x) = j(h(z))$
$k(x) = j(w)$
$v = v$

Q) Determine if relations are functions or not.

i) $A = \{1, 2, 3, 4\}$.

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

$\because 2 \to 3$ & $2 \to 1$ so only relation

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

2 does not have a image

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

Function & Range $= \{1, 4\}$.

Q) Let $A = \{1,2,3,4,5\}$ $B = \{w, x, y, z\}$

$f: A \to B$.

$f = \{(1,w)\ (2,x)\ (3,x)\ (4,y)\ (5,y)\}$

Find images for.

$A_1 = \{1\}$. $A_2 = \{2,3\}$. $A_3 = \{2,3,4\}$.

$= \{w\}$ $= \{x\}$ $= \{y, x\}$.

Q) Find the nature of following function $A = \{1, 2, 3\}$

a) $f = \{(1,1)\ (2,2)\ (3,3)\}$ Identity.

b) $g = \{(1,2)\ (3,2)\ (2,2)\}$ Constant

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

d) $j = \{(1,2)\ (2,3)\ (3,1)\}$ bijective, injective, surjective.

Q) $|A| = m$ $|B| = n$. $f: A \to B$.

How many functions are possible from A to B

→ n^m

Q) If $|B| = 3$

$2 \mid 8$

$\therefore |A$

Compo

A =

h

h

x

DATE: PAGE:

3) One to one / Injective function

A function f from set A to set B is called injective function, if every element A has unique image in set B.

$f: A \to B$.

$\forall x_1, x_2 \in A$.

if $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

if $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

4) Onto / Surjective function

A function f from A to B such that every element of b has preimage in A.

$f: A \to B$.

Range = Co-domain

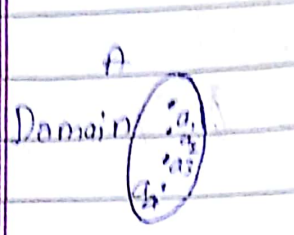
$\forall b \in B, \exists a \in A \quad f(a) = b$.

5) Bijective.

A function f from A to B such that f is both one to one and onto then. f is bijective function.

Functions

DATE: PAGE:



$f : A \to B$.

$b_1 = f(a_1)$

$b_2 = f(a_2)$

$b_4 = f(a_3) = f(a_4)$

$\therefore$ Range $= \{b_1, b_4\}$.

Types of functions.

1) Identity function.

A function f on set A is called identity function if image of every element in set A is itself

$f : A \to A$ such that $f(a) = a, \forall a \in A$

2) Constant function

A function f from $A \to B$ is a constant if all the elements of A have same image in B.

$f : A \to B \mid \forall a \in A \; f(a) = c, \; c \in B$.

DATE: PAGE:

$[(1,3)] = \{(2,2)\ (3,1)\ (1,3)\}$

$[(2,4)] = \{(1,5)\ (5,1)\ (3,3)\ (4,2)\ (2,4)\}$

Q). For a equivalence relation R. on A

$A = \{1, 2, 3, 4\}$

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

Determine the partitions induced on set A.

→

$[1] = \{1, 2\}$

$[2] = \{2, 3\}$

$[3] = \{3, 4\}$

$P = \{$

Q) $A = \{1, 2, 3, 4, 5, 6, 7\}$ R be on A.

$A = \{1, 2\} \cup \{3\} \cup \{5, 7, 4\} \cup \{6\}$

$R = \{(1,1) \ldots (1,2)\ (2,1)$
$(3,3)\ (4,4)\ (5,7)\ (7,7)$
$(4,5)\ (5,4)\ (4,7)\ (7,4)$
$(5,7)\ (7,5)\ (6,6)\ ;\}$

A)

R on $A \times A$. iff $x_1 + y_1 = x_2 + y_2$.

$A = \{1, 2, 3, 4, 5\}$.

$R = \{(x, y_1), (x_2, y_2)\}$.

$\forall x, y\ \ x + y = y + x$

Reflexive. symmetric.

DATE: PAGE:

"Congruence modulo n" Relation

$a \equiv b \bmod n$

When you divide a by n it will give same remainder b.

for $n = 5$
We have 5 classes $[0], [1], [2], [3], [4]$

$[0] = \{0, 5, 10, 15, -5, -10 \ldots\}$
$[1] = \{1, 6, 11, 16, -4, -9 \ldots\}$
$[2] = \{2, 7, 12, 17, -3, -8 \ldots\}$
$[3] = \{3, 8, 13, 18, -2, -7, \ldots\}$
$[4] = \{4, 9, 14, 19, -1, -6, \ldots\}$

$a \equiv b \bmod n$ is equal to.
$a - b$ is multiple of n.

Partition of a set

Let A be a non-empty set. Let $A_1, A_2 \ldots A_k$ are non-empty subsets of A, such that following conditions should hold

i) $A = A_1 \cup A_2 \cup \ldots A_k$
ii) $A_i \cap A_j = \emptyset \quad \forall i \neq j$

$P = \{A_1, A_2 \ldots A_k\}$ is called partition of set A. $A_1, A_2 \ldots A_k$ are called ~~partition~~ blocks of partition

DATE:

PAGE:

Equivalence Class

R is equivalence rel^n on set S
set S can be partitioned into equivalence classes.

$$Y = Y_1 \cup Y_2 \cup \cdots Y_n$$
$$Y_i \cap Y_j = \phi, \forall i \neq j$$

Q) Consider a relation R on Z defined by xRy if $x-y$ is multiple of 2
Z R is an equivalence relation.

-> Two classes are present
i) Even Integers
ii) Odd Integers

$$[E] = \{ \cdots -6, -4, -2, 0, 2, 4, 6, 8 \cdots \}$$
$$[O] = \{ \cdots -3, -1, 1, 3, 5, \cdots \}$$

$$P = \{[E], [O]\}$$

P = partition of a given set.

Q) Let R be an equivalence relation on A, for each element $x \in A$. The equivalence class for x is denoted by $[x]$ and is defined as $[x] = \{ y \in A \mid yRx \}$.

DATE: PAGE:

If a relation is reflexive, transitive, and symmetric then it is an equivalence relation.

1) Let R and S be relations on set A
If R and S are reflexive.
PT. R∩S and R∪S are reflexive

2) Let R be a relation on set A.
If i) R is Reflexive if and only if $\bar{R}^c$ is reflexive
ii) If R is Reflexive so is R^c
iii) If R is symmetric R^c & $\bar{R}$ is also symmetric.

3) Let R be a Relation on A.
$A = \{a, b, c\}$

$$\begin{matrix} & a & b & c \\ a & 1 & 0 & 1 \\ b & 0 & 1 & 0 \\ c & 0 & 0 & 1 \end{matrix}$$

Determine If R is equivalence.

4) Let $A = A_1 \cup A_2 \cup A_3$.
$A_1 = \{1, 2\}$, $A_2 = \{2, 3, 4\}$, $A_3 = \{5\}$
Define a Relation R on A
xRy iff xy are in the same set A;

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

DATE: PAGE:

4) Anti Symmetric Relation

$\forall\ x, y \in A$, if $(x,y) \in R$ & $(y,x) \in R$ then $x = y$.

$\forall\ x, y \in A \quad xRy \wedge yRx \rightarrow x = y$

5) Transitive Relation

$\forall\ x, y, z \in A$ if $(x,y) \in R$ and $(y,z) \in R$ then $(x,z) \in R$.

if $xRy \wedge yRz \rightarrow xRz$

Q) $A = \{1, 2, 3\}$

$R_1 = \{(1,2), (2,1), (1,3), (3,1)\}$ Symmetric, Irrefl... No R

$R_2 = \{(1,1), (2,3), (3,3)\}$ Transitive. Symmetric, Non-sy...

$R_3 = \{(2,3), (3,4), (2,4)\}$ Transitive, Irreflexive.

Non symmetric

$R_4 = \{(1,1) (2,2) (3,3) (2,3)\}$ Reflexive transitive, Antisymmetric

Q) $\equiv$

Reflexive, Transitive, symmetric

Q) $\leq$, $\geq$

Reflexive, Transitive, Antisymmetric

Q) $<$, $>$

Irreflexive, Transitive.

If a... and equiva...

Let ... If ... P.T.

Let ... If i... R

is T...

ii) If ... als...

3) Let ...

4) ...

D...

Properties of Relation

1) Reflexive
2) Irreflexive
3) Symmetric.
4) Anti-Symmetric.

Reflexive relation

A Relation R on set A is said to reflexive
if $\forall a, (a,a) \in R$.
~~and for some element~~
if $\exists a, (a,a) \notin R$ then R is non-reflexive relation or not reflexive relation.

Irreflexive relation

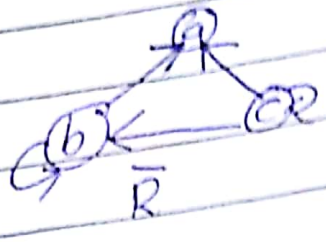
A relation R on set A is called irreflexive
if $\forall a, (a,a) \notin R$.

Symmetric relation

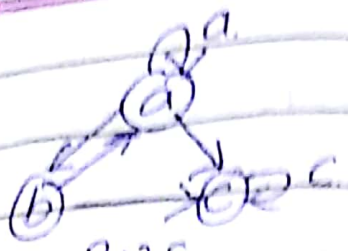
A relation R on set A is called symmetric relation.

$\forall a, b$, if $(a,b) \in R$ then $(b,a) \in R$.

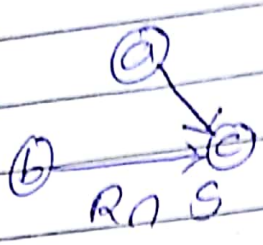
If
$\exists a, b$, if $(a,b) \in R$ and $(b,a) \notin R$
the R is not-symmetric relation.



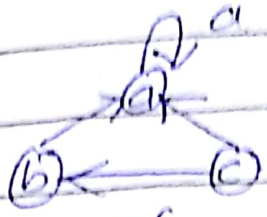
$\bar{R}$



R ∪ S



R ∩ S



R^c

Composition of Relation

If R is a relation from A to B
S ——— II ——— from B to C.

Then composition of relation is
$R.S = \{\langle a,c\rangle \mid a \in A, c \in C$ & there exists $b \in B$, $\ni \langle a,b\rangle \in R$ & $\langle b,c\rangle \in S\}$

Q) $A = \{1,2,3,4\}$ $B = \{w,x,y,z\}$ $C = \{5,6,7\}$
$R_1 = \{(1,x)\ (2,x)\ (3,y)\ (3,z)\}$
$R_2 = \{\langle w,5\rangle\ \langle x,6\rangle\}$
$R_3 = \{(w,5).(w,6)\}$

$R_1 \cdot R_2 = \{(1,6)\ (2,6)\}$
$R_1 \cdot R_3 = \{\}$

DATE: PAGE:

1) Union operation

$R_1 \cup R_2$

$\langle a,b \rangle \in R_1 \cup R_2$

If $\langle a,b \rangle \in R_1$ or $\langle a,b \rangle \in R_2$.

2) Intersection operation

$R_1 \cap R_2$

$\langle a,b \rangle \in R_1 \cap R_2$

If $\langle a,b \rangle \in R_1$ and $\langle a,b \rangle \in R_2$.

3) Complement operation

$\overline{R}$.

$\langle a,b \rangle \in \overline{R}$

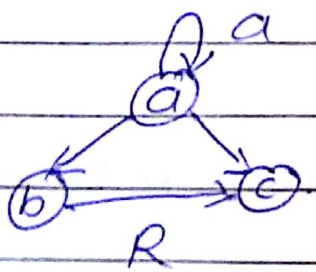
If $\langle a,b \rangle \notin R$ and $\langle a,b \rangle \in A \times B$.

4) Converse of Reln. (R^c)

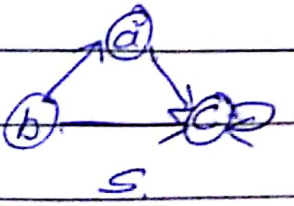
If $\langle a,b \rangle \in R$

then $\langle b,a \rangle \in R^c$.

Q) Di-graphs of two relations R & S on set $A = \{a,b,c\}$ are given. Draw diagraphs for $R, R^c, \overline{R^c}, R \cup S, R \cap S$.



R



S

DATE: PAGE:

In-degree = No of edges terminating at a node

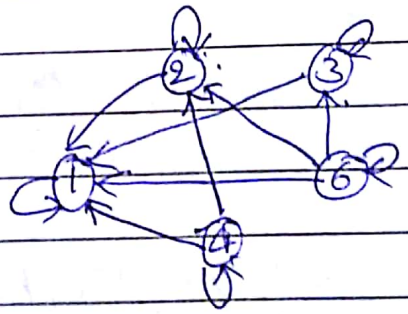
Out-degree = No of edges originating at a node

Q) Relation R be on A

$A = \{1, 2, 3, 4, 6\}$ Draw zero one & graph

$\langle a, b \rangle \in R$ if $a = mb$ $m \in I$

R	1	2	3	4	6
1	1	0	0	0	0
2	1	1	0	0	0
3	1	0	1	0	0
4	1	1	0	1	0
6	1	1	1	0	1



Operations on Relations

Let R_1 & R_2 be two relations from set A to set B

1) Union

$R_1 \cup R_2 = \{\langle a, b \rangle \mid \langle a, b \rangle \in R_1 \text{ or } \langle a, b \rangle \in R_2\}$

If

2) Int

3) Co

4) C

Q)

Representation of Relation

1) Zero-One matrices
2) Di-graph

$A = \{a_1, a_2 \cdots a_m\}$
$B = \{b_1, b_2 \cdots b_n\}$

$\langle a_i, b_j \rangle$, $1 \le i \le m$, $1 \le j \le n$

Representation as Zero matrices

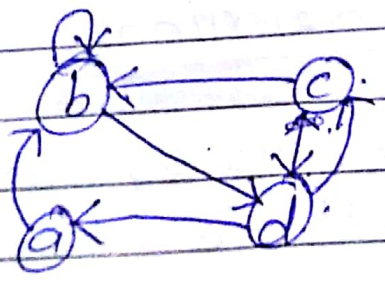
$$m_{ij} = \begin{cases} 1, & \langle a_i, b_j \rangle \in R \\ 0, & \langle a_i, b_j \rangle \notin R \end{cases}$$

m_{ij} is the element of matrix

Di-graph Representation (Directed graph)

Let R be a relation on finite set A. R can be represented pictorially as.

$R = \{\langle a,b \rangle, \langle b,b \rangle, \langle b,d \rangle, \langle c,b \rangle, \langle c,d \rangle, \langle d,a \rangle, \langle d,c \rangle\}$



Matrix representation

	a	b	c	d
a	0	1	0	0
b	0	1	0	1
c	0	1	0	1
d	1	0	1	0

Relations

DATE: PAGE:

Let $A = \{0, 1, 2\}$.
$B = \{2, 4\}$.

Relation between $A \times B$ is a subset of $(A \times B)$

$A \times B = \{\langle 0,2\rangle, \langle 0,4\rangle, \langle 1,2\rangle, \langle 1,4\rangle, \langle 2,2\rangle, \langle 2,4\rangle\}$

Let $A \times B$ be two non-zero sets then a subset of $(A \times B)$ is called a relation from A to B.

If R is a relation from A to B.
R is set of ordered pairs. $\langle a, b\rangle$
such that $a \in A$, $b \in B$.

If R is a relation from A to A then R is subset of $A \times A$.

$|A \times B| = |A| \times |B| = m \times n$.

Q) Let $A \times B$ be finite $|B| = 3$.
if $|A \times B| = \log_2 4096$ & $|A| = ?$

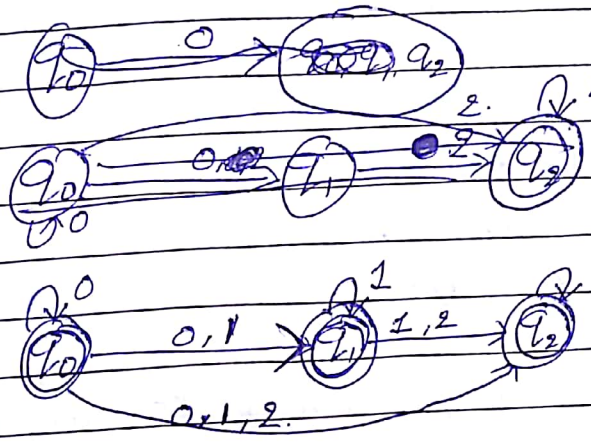
$\Rightarrow \log_2 4 \times 1024 = \log_2 2^{12} = 12$.

$\therefore |A| = 4$.

Q) $A = \{1, 2, 3, 4, 6\}$. R be a relation on A defined by $(a, b) \in R$ // a is multiple of B.

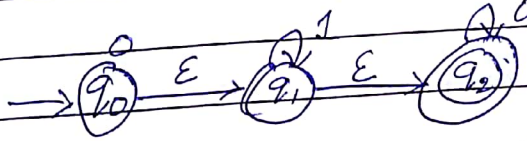
$= R = \{(2,1), (3,1), (4,1), (6,1), (1,1), (4,2), (6,2), (2,2), (6,3), (3,3), (4,4), (6,6)\}$

	0	1	2
q_0	$\{q_0, q_1\}$	$\{q_1, q_2\}$	$\{q_2\}$
q_1	ϕ	$\{q_1, q_2\}$	$\{q_2\}$
q_2	ϕ	ϕ	$\{q_2\}$



Accepting states are EClose(q_0)

8) Convert the following to NFA



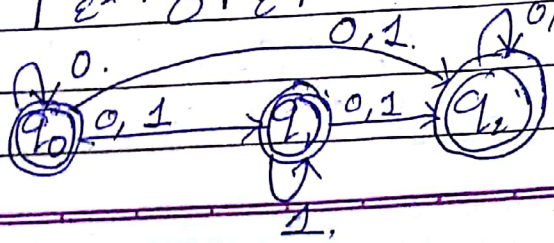
->

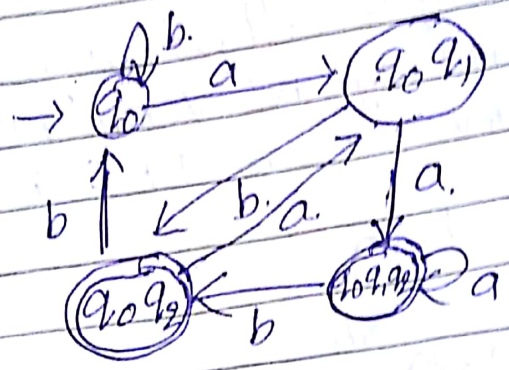
	0	1	ε^*
q_0	0	ϕ	q_0, q_1, q_2
q_1	ϕ	1	q_1, q_2
q_2	q_2	q_2	q_2

q_0	q_0, q_1, q_2	q_2, q_2	q_2, q_2
q_1	q_1, q_2	q_2	q_2
q_2	q_2	q_2	q_2
	ε^*	0	ε^*

	ε^*	1	ε^*
q_0	q_0, q_1, q_2	q_1, q_2	q_1, q_2
q_1	q_1, q_2	q_1, q_2	q_1, q_2
q_2	q_2	q_2	q_2

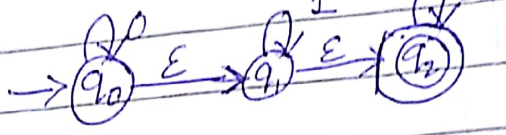
	0	1
q_0	q_0, q_1, q_2	q_1, q_2
q_1	q_2	q_1, q_2
q_2	q_2	q_2





bbb
aba

Conversion of ε-NFA to NFA



	0	1	2	ε^*
q_0	q_0	ϕ	ϕ	q_0, q_1, q_2
q_1	ϕ	q_1	ϕ	q_1, q_2
q_2	ϕ	ϕ	q_2	q_2

No. of states remain same

	ε^*	0	ε^*
q_0	q_0, q_1, q_2	q_0	q_0, q_1, q_2
q_1	q_1, q_2	ϕ	ϕ
q_2	q_2	ϕ	ϕ

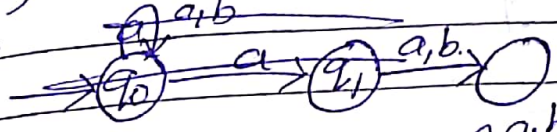
	ε^*	1	ε^*
q_0	q_0, q_1, q_2	q_1	q_1, q_2
q_1	q_1, q_2	q_1	q_1, q_2
q_2	q_2	ϕ	ϕ

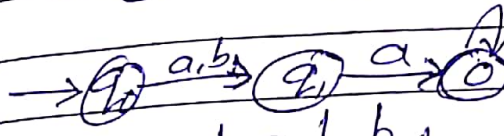
	ε^*	2	ε^*
q_0	q_0, q_1, q_2	q_2	q_2
q_1	q_1, q_2	q_2	q_2
q_2	q_2	q_2	q_2

DATE: PAGE:

Q) Draw an that accepts all strings
i) in which i) second symbol from LHS is a
ii) Second symbol from RHS is a

→ i)

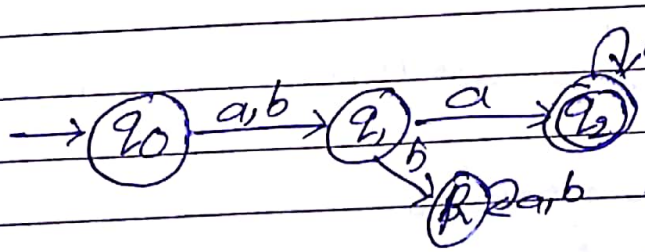




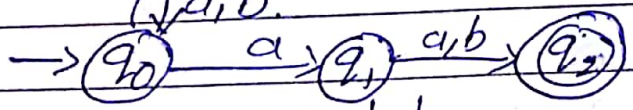
	a	b
q_0	q_0	q_0
q_1	q_2	ϕ.
q_2	q_2	q_2

	a	b
q_0	q_0	q_0
q_1	q_2	R
q_2	q_2	q_2
R	R	R

~~abcab~~.



ii)

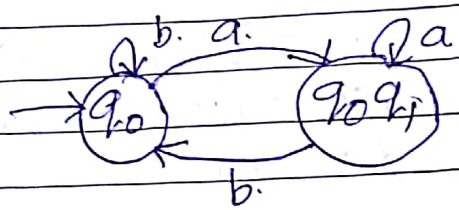


	a	b
q_0	$\{q_0, q_1\}$	q_0
q_1	q_2	q_2
q_2	ϕ	ϕ

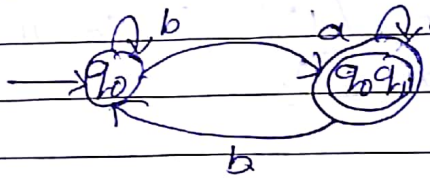
	a	b.
q_0	$\{q_0, q_1\}$	q_0.
$\{q_0, q_1\}$	$\{q_0, q_1, q_2\}$	$\{q_0, q_2\}$.
$\{q_0, q_1, q_2\}$	$\{q_0, q_1, q_2\}$	$\{q_0, q_2\}$
$\{q_0, q_2\}$	$\{q_0, q_1\}$	q_0.

DATE: PAGE:

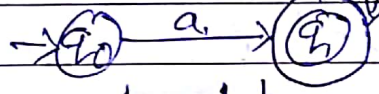
	a	b
q_0	$\{q_0, q_1\}$	$\{q_0\}$
$\{q_0, q_1\}$	$\{q_0, q_1\}$	$\{q_0\}$



State where q_1 is present is our final state

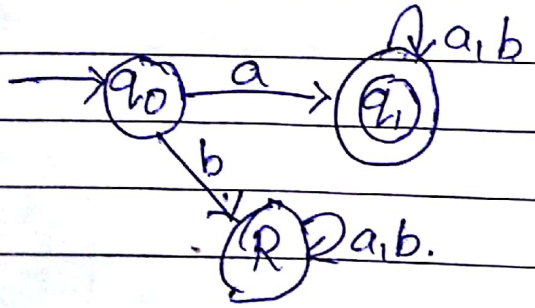


Q) Strings starting with 'a'.



	a	b
q_0	q_1	ϕ
q_1	q_1	q_1

	a	b
q_0	q_1	R
q_1	q_1	q_1
R	R	R



Q) Draw
din w
ii) S
is

→
→
→

DATE: PAGE:

$\delta^*(q_0, 001) = E\text{Close}[\delta(\delta^*(q_0, 00), 1)]$
$= E\text{Close}[\delta(q_0, 1) \cup \delta(q_2, 1)]$
$= E\text{Close}[q_1 \cup \phi]$
$= \{q_1, q_2\}$

$\delta^*(q_0, 0112) = E\text{Close}[\cup \delta((\delta^* q_0, 011), 2)]$
$= E\text{Close}[\delta(q_0, 2) \cup \delta(q_2, 2)]$
$= E\text{Close}[\phi \cup q_2]$
$= q_2$

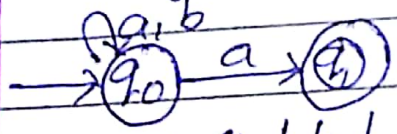
$\delta^*(q_0, 01122) = E\text{Close}[\cup \delta(\delta^*(q_0, 0112), 2)]$
$= E\text{Close}[\delta(q_2, 2)]$
$= q_2$

$\therefore$ as $\delta^*(q_0, 01122) = q_2 \cap A \neq \phi$

$\therefore$ String is accepted

Converting NFA to DFA

using Subset construction method



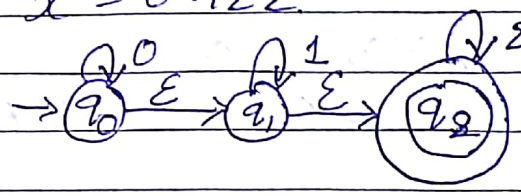
	a	b
q_0	q_0, q_1	q_0
q_1	ϕ	ϕ

DATE: PAGE:

E closure for any state q is defined as

1) The state q is in eclose(q).
2) If any state p ∈ eclose(q), if there is a transition from p to r labelled with ∈, then state r is in eclose(q).

Q) x = 0122

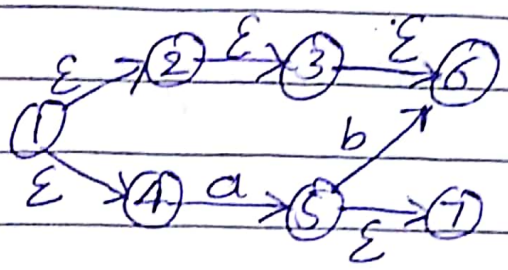


$\delta^*(q_0, \varepsilon) = E\,Close[\delta^*(q_0, \epsilon)]$
$= Eclose(q_0)$
$= \{q_0, q_1, q_2\}$

$\delta^*(q_0, 0) = EClose[(\delta^*(q_0, \epsilon), 0)]$.
$= EClose[\delta(q_0, 0) \cup \delta(q_1, 0) \cup \delta(q_2, 0)]$
$= EClose[\{q_0\} \cup \phi \cup \phi]$
$= EClose[q_0]$
$= \{q_0, q_1, q_2\}$.

$\delta^*(q_0, 01) = EClose[(\delta^*(q_0, 0), 1)]$
$= EClose[\delta(q_0, 1) \cup \delta(q_1, 1) \cup \delta(q_2, 1)]$
$= EClose[\phi \cup q_1 \cup \phi]$.
$= EClose[q_1]$
$= \{q_1, q_2\}$

Ex:



$\varepsilon(1) = \Lambda(1) = E\text{close}(1) = \{2, 3, 4, 6, 1\}$

$\varepsilon(2) = \{2, 3, 6\}$

$\varepsilon(4) = \{4\}$

$\varepsilon(5) = \{5, 7\}$

Extended definition of transition Fun^c δ^* for ε-NFA

Let $M = \{Q, \Sigma, q_0, A, \delta\}$ be an ε-NFA the

$\delta^* : Q \times \Sigma^* \longrightarrow 2^Q$ is defined

i) For any $q \in Q$

$\delta^*(q, \varepsilon) = E\text{close}(q)$

ii) For any $q \in Q$, $x \in \Sigma^*$, $a \in \Sigma$.

$$\delta^*(q, xa) = E\text{Close}\left(\bigcup_{q_i \in \delta^*(q,x)} \delta(q_i, a)\right).$$

$L(M) = \{x \mid x \in \Sigma^*, \delta^*(q_0, x) \cap A \neq \emptyset\}$

DATE: PAGE:

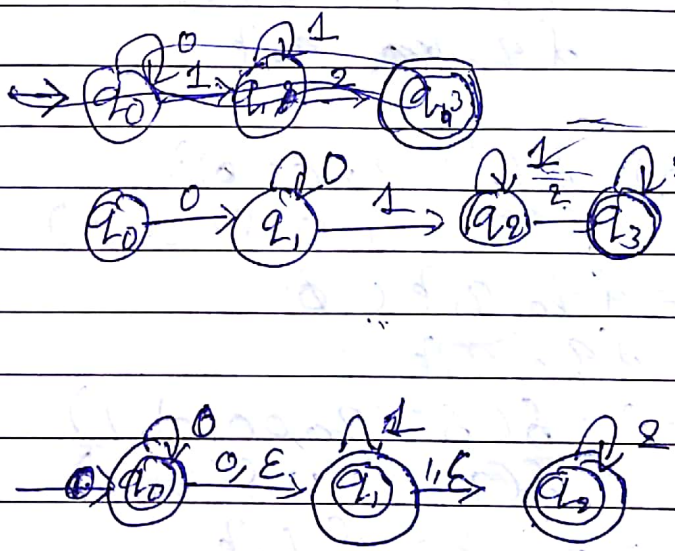
ε-NFA

NFA in which ε transitions are allowed.

$\varepsilon - NFA = (Q, \Sigma, q_0, A, \delta)$

$q_0 \in Q$.
$A \subseteq Q$.
$\delta : Q \times (\Sigma \cup \{\varepsilon\}) \to 2^Q$.

Q) Draw an NFA that accepts ~~does~~ strings that has atleast one occurence of $0^n 1^m 2^p$ $n, m, p \geq 1$.



ε - Closure

All the states which can be reached from q_0 using ε transitions

Ex:

$\varepsilon(1) =$
$\varepsilon(2)$
$\varepsilon(4)$
$\varepsilon(5$

Ex

Le
th

δ
i)

i

PAGE:

DATE: PAGE:

Condition for NFA to accept a string.

$L(M) = \{ x \mid x \in \Sigma^*, \delta^*(q_0, x) \cap A \neq \phi \}$

$x = 00101$

$\delta^*(q_0, \epsilon) = \{q_0\}$

$\delta^*(q_0, 0) = \delta(\delta^*(q_0, \epsilon), 0)$

$= \{q_0, q_1\}$

$\delta^*(q_0, 00) = \delta(\delta^*(q_0, 0), 0)$

$= \delta(q_0, 0) \cup \delta(q_1, 0)$

$= \{q_0, q_1\} \cup \phi$

$= \{q_0, q_1\}$

$\delta^*(q_0, 001) = \delta(\delta^*(q_0, 00), 1)$

$= \delta(q_0, 1) \cup \delta(q_1, 1)$

$= \{q_0\} \cup \{q_2\}$

$= \{q_0, q_2\}$

$\delta^*(q_0, 0010) = \delta(\delta^*(q_0, 001), 0)$

$= \delta(q_0, 0) \cup \delta(q_2, 0)$

$= \{q_0, q_1\} \cup \phi$

$= \{q_0, q_1\}$

$\delta^*(q_0, 00101) = \delta(\delta^*(q_0, 0010), 1)$

$= \delta(q_0, 1) \cup \delta(q_1, 1)$

$= \{q_0\} \cup \{q_2\}$

$= \{q_0, q_2\}$

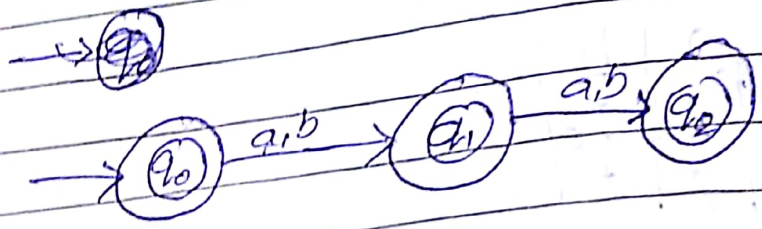
$A = \{q_2\}$

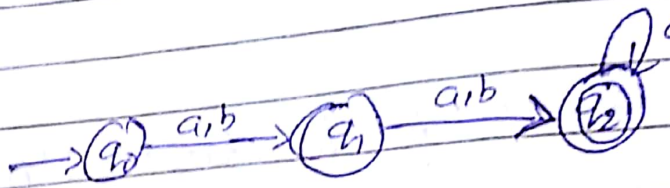
$\therefore$ as $\delta^*(q_0, 00101) \cap A \neq \phi$

$\therefore$ x is accepted by FSM.

DATE: PAGE:

Q) Draw an NFA that accepts string of length atmost 2 and atleast 2.





Extended definition of δ^* for NFA.

Let $M = (Q, \Sigma, q_0, A, \delta)$ be a NFA.

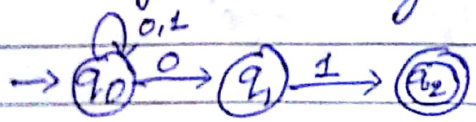
The fun^c $\delta^* : Q \times \Sigma \to 2^Q$.

1) For any $q \in Q$, $\delta^*(q, \epsilon) = \{q\}$.

2) For any $q \in Q$, $x \in \Sigma^*$, $a \in \Sigma$

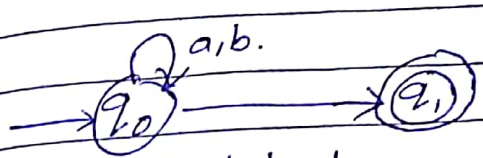
$$\delta^*(q, xa) = \bigcup_{q_i \in \delta^*(q,x)} \delta(q_i, a)$$

Q) Strings ending with 01.



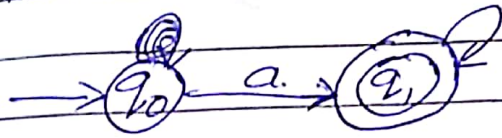
DATE: PAGE:

Q) NFA to accept strings ending with a

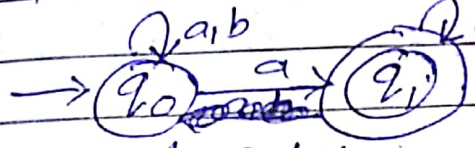


	a	b
q_0	$\{q_0, q_1\}$	q_0
q_1	ϕ	ϕ

Q) Draw an NFA to start with A.



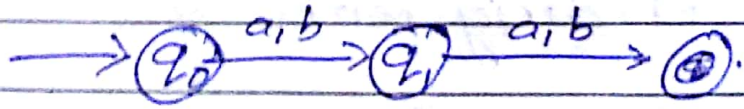
Q) Draw an NFA for string containing A



	a	b
q_0	q_1	ϕ
q_1	ϕ	ϕ

	a	b
q_0	$\{q_0, q_1\}$	$\{q_0\}$
q_1	q_1	q_1

Q) Draw an NFA for language that accepts strings of length which are exactly 2.



DATE: PAGE:

(Non- Deterministic finite Automata NFA

only δ function varies for NFA other all are same for DFA.

$\delta : Q \times \Sigma \rightarrow 2^Q$

$\therefore Q \times \Sigma$ maps to power set.

$Q = \{q_0, q_1\}$

$\Sigma = \{a, b\}$

$Q \times \Sigma = \{\langle q_0, a\rangle \langle q_0, b\rangle \langle q_1, a\rangle \langle q_1, b\rangle\}$

$2^Q = \{\phi, q_0, q_1, q_0 q_1\}$

* In DFA.
with a current state and single i/p symbol there will be a unique state.

But In NFA
need not be a unique state. it can be null state or 2 or more transitions.

Q)

Q)

Q)

Q)

NFA
with

q_0

q_0
q_1

Dfa

Df

->

Extended definition of transition function

δ^* or $\hat{\delta}$

For a language L & Σ.

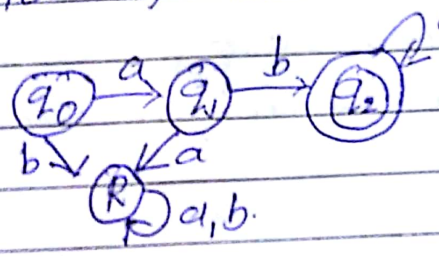
$x \in \Sigma^*, a \in \Sigma$

$\delta^*(q, xa) = \delta(\delta^*(q, x), a)$

$\delta^*(q, x) = q \in Q$.

$$\boxed{\delta^*(q, a) = \delta(q, a)}$$

Q) Find if abaab is accepted by.



→ $\delta^*(q_0, abaab) \Rightarrow q_2$

$\delta^*(q_0, \epsilon) = q_0$.

$\delta^*(q_0, a) = \delta(q_0, a) = q_1$

$\delta^*(q_0, ab) = \delta(\delta^*(q_0, a), b) = \delta(q_1, b) = q_2$

$\delta^*(q_0, aba) = \delta(\delta^*(q_0, ab), a) = \delta(q_2, a) = q_2$

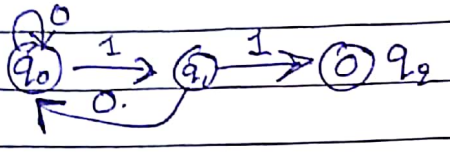
$\delta^*(q_0, abaa) = \delta(\delta^*(q_0, aba), a) = \delta(q_2, a) = q_2$

$\delta^*(q_0, abaab) = \delta(\delta^*(q_0, abaa), a) = \delta(q_2, a) = q_2$.

$\therefore q_2 \in A$

DATE: PAGE:

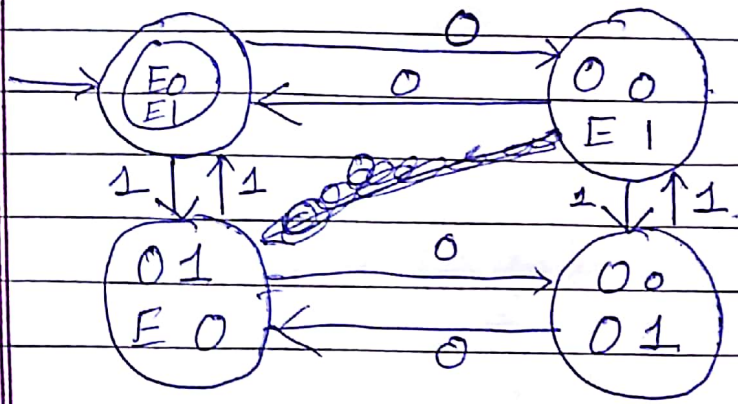
Q) DFA to accept 11 as substring



Q) DFA for

$L_1 = \{x \in \{0,1\}^* : x$ has even no of 0's and x has even no of 1's$\}$

→



Ex

δ

Fo

x

δ

δ

Q)

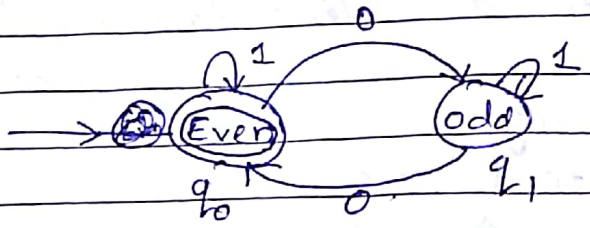
→

DATE: PAGE:

Q) $L = \{x \in \{0,1\}^* : x \text{ has even number of } 0\}$

: $L = \{1, 00, 11, 001, 010, 100, 111 - \ldots\}$.

Finite state machine to this language is



Final states are represented by two circles

FSM consists of

1) States. $Q = \{q_0, q_1\}$.
2) Alphabet Set, $\Sigma = \{0, 1\}$
3) Initial state → ○
4) Final state ◎
5) Transition Function.

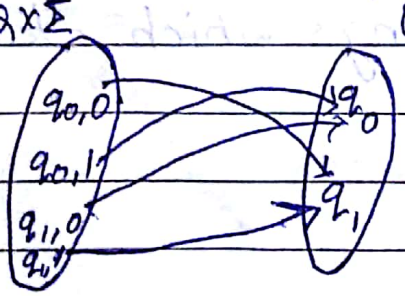
$\delta : Q \times \Sigma \rightarrow Q$.

$Q = \{q_0, q_1\}$.

$\Sigma = \{0, 1\}$

$Q \times \Sigma = \{q_0, q_1\} \times \{0, 1\}$

$= \{(q_0,0), (q_0,1), (q_1,0), (q_1,1)\}$.



f compiler
belongs

$\Sigma^* =$ ~~[illegible]~~
= set of finite strings over symbols of Σ.

$\Sigma^* = \{\lambda, a, b, aa, ab, ba, bb, aaa, aab \ldots \ldots\}$

* is called as Kleene star or closure [star] operation.

<u>Null string</u>
Represented as
Σ^0 or λ or Λ or ε
$|\lambda| = |\Sigma^0| = |\varepsilon| = |\Lambda| = 0$

* $\Sigma^+ = \Sigma^* - \{\lambda\}$.
Positive closure operation.

<u>Language</u>

Language L over Σ is a subset of Σ^*.

Ex:- i) $\Sigma = \{a, b\}$
$L = \{aa, ab, ba, bb\}$ set of all strings of len-2.

ii) $\Sigma = \{0, 1\}$
$L = \{0, 01, 011, 001, 010, 000 \ldots\}$
Set of all strings which starts with 0.

Finite state Automata

It is used lexicle analysis of compiler. To recognize strings which belongs to a certain language.

Symbol

It is a basic building block of FSA.

Ex: 0, 1, a, b, ..., x, $ ...

Alphabet

It is a finite non-empty set of symbols.

It is denoted by symbol Σ.

Ex: $\Sigma = \{0, 1\}$ $\Sigma = \{a, b\}$

$\Sigma = \{a, b, c, \ldots x, y, z\}$.

String

It is a sequence of symbol over the alphabet set Σ.

Ex: ab, a, aa, abb.

Power of Σ

Ex: $\Sigma = \{a, b\}$

Σ^1 = Set of strings of len 1 = a, b.

Σ^2 = Set of strings of len 2 =

$= \{\Sigma\Sigma\} = \{a, b\}\{a, b\} = aa, ab, ba, bb.$

PAGE:

DATE: PAGE:

Q) Translate each of the following sentences into symbol
i) Using ∃ ii) Using ∀

1) Not all cars have carburators
2) Some numbers are not real

1) p(x): car x has carburator.
∃x, ¬p(x).

p(x): x is a car.
q(x): x has carburator
~~∀x p(x) ∧ ∃x, q(x)~~
¬∀x [p(x) → q(x)]
∃x [p(x) ∧ ¬q(x)].

2) p(x): x is a number
q(x): x is a real number

~~2: ∀x (p(x) → ¬q(x))~~
2: ¬[∀x [p(x) ∧ q(x)]

2: ∃x (p(x) ∧ ¬q(x))
∀x (¬p(x) ∨ q(x))
¬[∀x (p(x) → q(x))]

Q) Prove that

$\forall x [p(x) \to q(x)] \wedge \exists x, p(x) \Rightarrow \exists x, q(x)$

W.K.T.

$\exists x, p(x) \Rightarrow p(a)$ for some $a \in U$

for some $a \in U$, $p(a) \to q(a)$

Using

Modesponens rule

$(p(a) \to q(a)) \wedge p(a) \Rightarrow q(a)$

$q(a) \Rightarrow \exists x, q(x)$

Q) Analyze the following argument is valid or not valid

1: All squares have four sides.

2: Quadrilateral ABCD has four sides.

$\therefore$ ABCD is a square

U = Set of all quadrilaterals.

$p(x)$: x is a square

$q(x)$: x has 4 sides.

a : The quadrilateral ABCD has 4 sides

$\forall x, (p(x) \to q(x))$

$q(a)$

$\therefore p(a)$

To prove

$\therefore \forall x (p(x) \to q(x)) \wedge q(a) \Rightarrow p(a)$

$[p(a) \to q(a)] \wedge q(a) \Rightarrow p(a)$

$[\neg p(a) \vee q(a)] \wedge q(a) \Rightarrow p(a)$.

$\therefore$ Statement is not valid.

in symbolic

hen $x^2 - 1$ is even.

)

Statements

specification

a is true

s true

DATE

PAGE

q) $P(a)$, for some a
$\therefore \exists x, P(x)$

Existential generalization

Logically Equivalent statement and Logically Implied statement.

* $\forall x [p(x) \wedge q(x)] \Leftrightarrow \forall x p(x) \wedge \forall x q(x)$
* $\forall x [p(x) \vee q(x)] \not\Leftrightarrow \forall x p(x) \vee \forall x q(x)$
* $\forall x\, p(x) \vee \forall x\, q(x) \Rightarrow \forall x [p(x) \vee q(x)]$
* $\exists x [p(x) \vee q(x)] \Leftrightarrow \exists x\, p(x) \vee \exists x\, q(x)$
* $\exists x\, p(x) \wedge \exists x q(x) \not\Leftrightarrow \exists x [p(x) \wedge q(x)]$
* $\exists x [p(x) \wedge q(x)] \Rightarrow \exists x\, p(x) \wedge \exists x\, q(x)$

DATE: PAGE:

Q) $p(x)$: x is odd
$q(x)$: $x^2 - 1$ is even.
Express the statement in symbolic.

→ .
for any x if x is odd then x^2-1 is even

$\Rightarrow \forall x \in Z, p(x) \rightarrow q(x)$

Negation
$\exists x \in Z, p(x) \wedge \neg q(x)$

Rules of Quantified Statements

premise
$\forall x\ p(x)$ → Universal specification
$\therefore p(c)$. ⇒ Conclusion

1) $\forall x, p(x) \Rightarrow p(x)$

2) ~~$p(a)$ for any arbitary a is true~~
~~universal generalization~~

~~$\therefore \forall x\ p(x)$~~

2) $p(a)$ For any arbitrary a is true
$\therefore \forall x\ p(x)$

Universal generalization

3) $\exists x, p(x)$ is true
$\therefore p(a)$ for some a is true

Existential specification.

a) $p(a)$ ...
Exis...
Log...
log...

DATE: PAGE:

Q) $\exists x [\{p(x) \vee q(x)\} \rightarrow r(x)]$

-> $\forall x [\{p(x) \vee q(x)\} \wedge \neg r(x)]$

Q) Write the following proposition in symbolic form and find its negation.

-> i) All integers are rational numbers but some rational numbers are not integers

-> $p(x)$: x is a rational number
$q(x)$: x is an integers

$\forall x \; p(x) \rightarrow q$

* $\forall x [(p(x) \rightarrow q(x)) \wedge \neg (p(x) \rightarrow q(x))]$

* $[\forall x \in Z, p(x)] \wedge [\exists x \in Q, \neg q(x)]$

Negation

$\neg [\forall x \in Z, p(x) \wedge \exists x \in Q, \neg q(x)]$
$\exists x \in Z, \neg p(x) \vee \forall x \in Q, q(x)$

Some integers are not rational numbers or all rational numbers are integers.

DATE: PAGE:

1) $\forall x, [r(x) \to p(x)]$
-> If x is a perfect square then x is a positive integer
(True)

2) $\exists x\ [s(x) \wedge \neg q(x)]$
-> there exists an interger x such x is divisble by 3 and x is not even
(True)

3) $\forall x\ (\neg r(x))$
-> x is not a perfect square
(False)

4) $\forall x\ [r(x) \vee s(x)]$
-> x is perfect square or x is divisible by 3

Negation of Quantified Statement

1) $\neg(\forall x, p(x)) \iff \exists x\ \neg p(x)$.

$\forall x\ p(x) \iff p(1) \wedge p(2) \wedge p(3) \ldots$
$\exists x\ p(x) \iff p(1) \vee p(2) \vee p(3) \ldots\ldots$

2) $\neg(\exists x, p(x)) \iff \forall x, \neg p(x)$

a) $\exists x\ [p(x) \wedge q(x)]$
-> $\forall x\ [\neg p(x) \vee \neg q(x)]$

a) $\forall x\ [p(x) \to q(x)]$
-> $\exists x\ p(x) \wedge \neg q(x)$

a) $\exists x\ [q$
-> $\forall x\ [q$

a) While th
in sym
-> 1) All i
but
in t
-> p(x):
q(x):

$\forall x$
$\forall x$

Neg

Sc

DATE: PAGE:

th his.

this course

then I

nbers

of

DATE: PAGE:

Quantifiers

$\forall$ ⇒ for all, for any, for each
$\exists$ = There exist, atleast one, For some

$\forall$ is universal quantifiers.
$\exists$ is existensial quantifiers.

They are used with open statements

Ex:

1) → Each number multiplied by 2 is even.
$\forall x \in Z$, $2x$ is even

2) For every real number x, there is a real number y for which $y^2 = x$
$\forall x \in R, \exists y \in R : y^2 = x$

Q) $p(x) : x > 0$
$q(x) : x$ is even
$r(x) : x$ is perfect square
$s(x) : x$ is divible by 3.

1) At least one int is even
$\exists x \in Z : q(x)$

2) There exist a positive integer; i.e. even
$\exists x \in Z^+ ; p(x) \wedge q(x)$

3) Some even integers are divisible by 3.
$\exists x \in Z, q(x) \wedge s(x)$

4) If x is even & a perfect square then x is not divisible by 3
$\forall x \in Z, [q(x) \wedge r(x)] \rightarrow \neg s(x)$.

DATE: PAGE:

Q) 1st: If Ravi goes out with his he won't study.

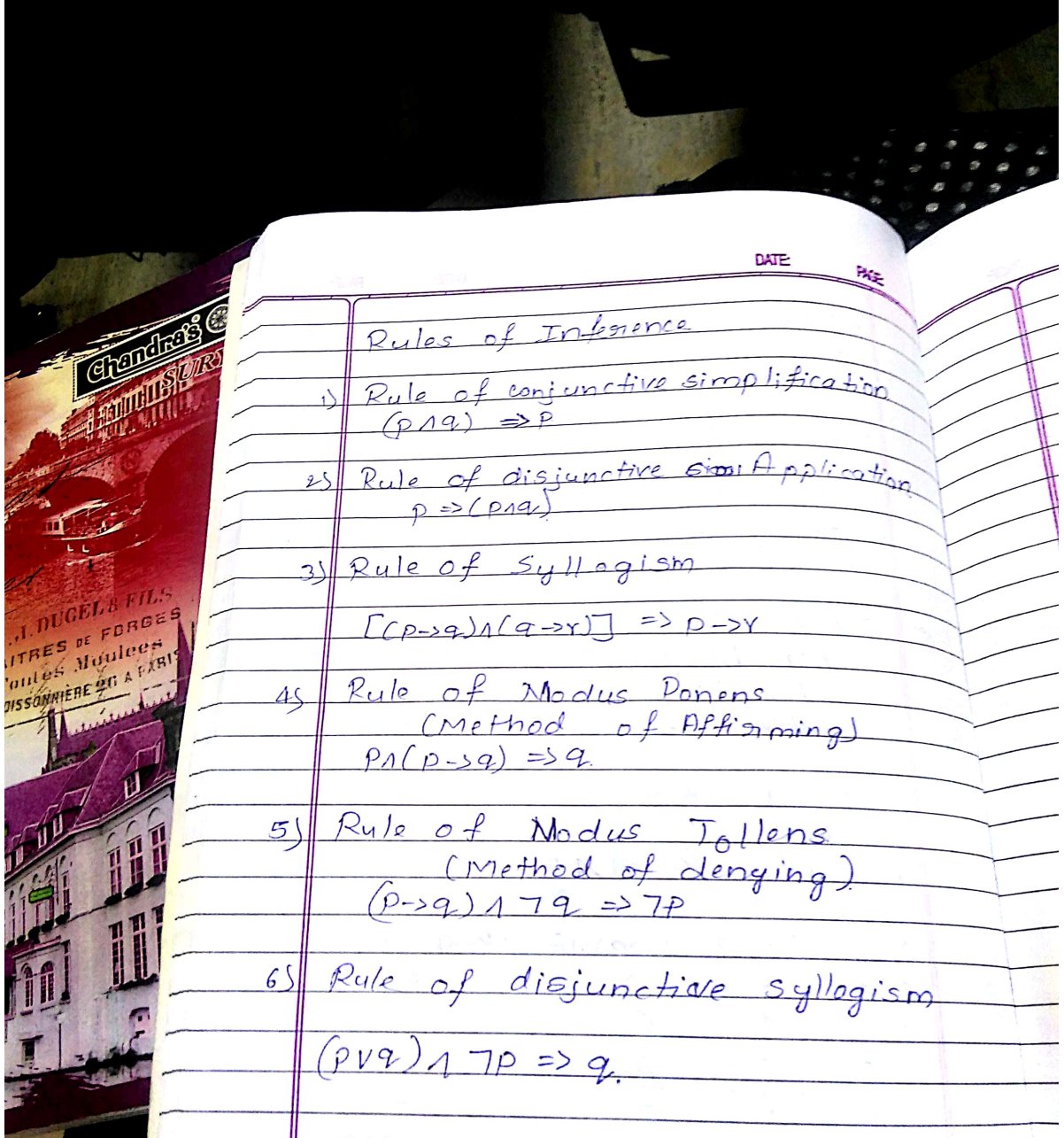
Q) 1st: I will get grade A in this course or I will not graduate
2nd: If I donot graduate then I will join army.
3rd: I got grade A
∴ I will not join army.
-> ~~Valid~~ Invalid

Open statements

Qualifiers => p(x): x is an even number
Free variables -> q(x): x is multiple of 4.
Universe -> r(x): x+3=6.

We can bound open statements using specific values or using set of values
i.e. x=4 or x∈Z

Unary => p(x), q(x)
Binary => p(x,y), q(x,z)
Ternary => p(x,y,z)



DATE PAGE

Rules of Inference

1) Rule of conjunctive simplification
$(p \wedge q) \Rightarrow p$

2) Rule of disjunctive ~~simplification~~ Application
$p \Rightarrow (p \vee q)$

3) Rule of Syllogism
$[(p \to q) \wedge (q \to r)] \Rightarrow p \to r$

4) Rule of Modus Ponens
(Method of Affirming)
$p \wedge (p \to q) \Rightarrow q$

5) Rule of Modus Tollens
(Method of denying)
$(p \to q) \wedge \neg q \Rightarrow \neg p$

6) Rule of disjunctive syllogism
$(p \vee q) \wedge \neg p \Rightarrow q$.

DATE: PAGE:

Given a set of premises, we need to see if its valid or not
(argument is valid or not

$P_1, P_2 \cdots P_n$: Premises.

$P_1 \wedge P_2 \cdots P_n \Rightarrow Q$ should be a tautology for argument to be valid.

1: If sachin hits a century.
then he gets a free car.
2: Sachin hits a century
∴ Sachin gets a free car

P1: $P \to q$
P2: P
Argument $(P \to q) \wedge P \Rightarrow q$

P	q	$P \to q$	$(P \to q) \wedge P$	$(P \to q) \wedge P \to q$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

Argument is a tautology.
∴ it is true

DATE: PAGE:

Law of Duality

Replace $\wedge$ (by $\vee$) and ($\vee$ by $\wedge$)

Replace T by F and vice versa.

* If $U \Leftrightarrow V$ then $U^d \Leftrightarrow V^d$

$(U^d)^d \Leftrightarrow U$

Logical Equivalent

- $P \to q$: Condition
- $q \to P$: Converse
- $\neg P \to \neg q$: Inverse
- $\neg q \to \neg P$: Contrapositive

] logically equivalent

Q) Contrapostive of $P \to (q \to r)$

=> $\neg(q \to r) \to \neg P$.

$\equiv \neg(\neg(q \to r)) \to \neg P$

$= q \wedge r \vee \neg P$

Rules of Inference

Consider a set of proposition.

Then the compound proposition

$P_1 \wedge P_2 \wedge P_3 \wedge \cdots P_n \Rightarrow Q$

(logically implies)

This is called argument.

Given a set of
to see if its v
Cargument is va

$P_1, P_2 \cdots P_n : P$

$P_1 \wedge P_2 \cdots P_n \Rightarrow$
tautology for

Q) 1: If sachin
then be
2: Sachin hit
∴ Sachin

P1: P → q
P2: P
Argument

P	q	P → q
0	0	1
0	1	1
1	0	0
1	1	1

Argume
∴ it

DATE: PAGE:

DATE: PAGE:

Q) Express the following propositions only using NAND and NOR connectives

1) $\neg P$.
-> $\neg(P \vee P) = P \downarrow P$.
$\neg(P \wedge P) = P \uparrow P$.

2) $P \wedge q$.
-> ~~$\neg(\neg P \vee \neg q)$~~ =
$P \wedge q = \neg(\neg P \vee \neg q)$
$= \neg(r)$
$= r \downarrow r$.
$= (P \uparrow q) \uparrow (P \uparrow q)$
$= \neg(\neg P) \wedge \neg(\neg q)$
$= \neg[\neg P \vee \neg q] = (P \downarrow P) \downarrow (q \downarrow q)$

$\overline{ab} = \bar{a} + \bar{b}$
$a + b = \overline{\bar{a}\,\bar{b}}$
$= \overline{a \downarrow b}$
$a \downarrow b = \bar{a}\,\bar{b}$

$r = \neg P \vee \neg q$
$r = \neg(P \wedge q)$
$r = P \uparrow q)$

3) $P \vee q$
-> $\neg(\neg P \wedge \neg q)$
$= (P \uparrow P) \uparrow (q \uparrow q)$.
$= (P \downarrow q) \downarrow (P \downarrow q)$

4) $P \rightarrow q$
$= \neg P \vee q$.
$= \neg(P \wedge \neg q)$
$= P \uparrow (\neg q)$
$= P \downarrow (q \uparrow q)$
$= P \uparrow (q \downarrow q)$

$= \neg(\neg P) \vee \neg(\neg q)$
$= \neg(P \wedge \neg q)$
$= \neg(P \uparrow (q \uparrow q))$
$= [P \uparrow (q \uparrow q)] \uparrow [P \uparrow (q \uparrow q)]$
$= (P \downarrow P) \vee (q)$

DATE: PAGE:

NAND NOR Connectives
↑ ↓

* $\neg(P \wedge Q) \iff (P \uparrow Q)$
* $\neg(P \vee Q) \iff (P \downarrow Q)$

P	Q	$P \uparrow Q$	$P \downarrow Q$
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

(a) $P \uparrow (Q \uparrow R)$

$= P \uparrow (\neg(Q \wedge R))$

$= \neg(P \wedge (\neg(Q \wedge R)))$

$= \neg P \vee (Q \wedge R)$

(b) $P \downarrow (Q \downarrow R)$

$P \downarrow (\neg(Q \vee R))$

$= \neg(P \vee (\neg(Q \vee R)))$

$= \neg P \wedge (Q \vee R)$

$= \neg(P \vee (\neg Q \wedge \neg R))$

$= \neg(P \vee \neg Q) \wedge (P \vee \neg R)$

$(P \downarrow Q) \downarrow R$

$= (\neg(P \vee Q)) \downarrow R$

$= \neg((\neg(P \vee Q)) \vee R)$

$= (P \vee Q) \wedge \neg R$.

7) $P \vee q \wedge \neg(\neg P \vee q)$

$\Rightarrow (P \vee q) \wedge (P \wedge \neg q)$.

$= [(P \vee q) \wedge P] \wedge \neg q$ Absorption laws.

$= P \wedge \neg q$.

8) $\neg q [\{(P \vee q) \wedge r\} \rightarrow \neg q]$

$= [(P \vee q) \wedge r] \wedge q$

$= (P \vee q) \wedge q \wedge r$

$= q \wedge r$.

9) $P \rightarrow (q \rightarrow r)$

$\Rightarrow = P \rightarrow (\neg q \vee r)$.

$= \neg P \vee (\neg q \vee r)$

$= \neg(P \vee q) \vee r$.

$= (\neg P \vee \neg q) \vee r$.

$= \neg (P \wedge q) \vee r$.

$= (P \wedge q) \rightarrow r$.

$\neg P \vee r \Rightarrow P \rightarrow r$

10) $[\neg P \wedge (\neg q \wedge r)] \vee [q \wedge r] \vee [P \wedge r]$

$= [\neg(P \vee q) \wedge r] \vee [q \wedge r] \vee [P \wedge r]$

$= [\neg(P \vee q) \wedge r] \vee [r \wedge q] \vee [r \wedge P]$

$= [\neg(P \vee q) \wedge r] \vee [r \wedge (P \vee q)]$.

$= [r \wedge \neg(P \vee q)] \vee [r \wedge (P \vee q)]$

$= r \wedge [\neg(P \vee q) \vee (P \vee q)]$

$= r \wedge T$

$= r$.

DATE: PAGE:

Q) $[P \to (q \wedge r)] \Leftrightarrow [(P \to q) \wedge (P \to r)]$

P	q	r	$q \wedge r$	$P \to (q \wedge r)$	$P \to q$	$P \to r$	$(P \to q) \wedge (P \to r)$
0	0	0	0	1	1	1	1
0	0	1	0	1	1	1	1
0	1	0	0	1	1	1	1
0	1	1	1	1	1	1	1
1	0	0	0	0	0	0	0
1	0	1	0	0	0	1	0
1	1	0	0	0	1	0	0
1	1	1	1	1	1	1	1

Q) $P \vee q \wedge \neg(\neg P \vee q) \Leftrightarrow P \wedge \neg q$

$\Rightarrow$ ~~$(P \vee q) \wedge (P \vee \neg q)$~~

$= P \vee (q \wedge \neg q)$

$= P \vee q \wedge (P \wedge \neg q)$

$= (P \vee q \wedge P) \wedge \neg q)$

$= (P \vee q) \wedge \neg q)$

A

$(P \vee q) \wedge (P \wedge \neg q)$

$((P \vee q) \wedge P) \wedge (\neg q)$

$(P \wedge P) \vee (P \wedge q) \wedge (\neg q)$

~~$P \vee (P \wedge q) \wedge q$~~

Q) $\neg[\{(P \vee q) \wedge r\} \to \neg q] \Leftrightarrow q \wedge r$

Q) $P \to (q \to r) \Leftrightarrow (P \wedge q) \to r$

Q) $[\neg P \wedge (\neg q \wedge r)] \vee [q \wedge r] \vee (P \wedge r) \Leftrightarrow r$

Q) $P \vee q \wedge \neg(\neg P$

$\Rightarrow (P \vee q) \wedge (P \wedge$

$= [(P \vee q) \wedge P]$

$= P \wedge \neg q$

Q) $\neg q [\{q (P$

$= [(P \vee q) \wedge$

$= (P \vee q)$

$= q$

Q) $P \to (q$

$\to = P \to ($

$= \neg P$

$=$

$=$

$= \neg ($

$= (P$

Q) $[\neg P$

$=$

$=$

$=$

$=$

$=$

$=$

PAGE: DATE: PAGE:

Tautology

$P \vee \neg P$ is always true.
Any compound statement is always true.

Contradiction

$P \wedge \neg P$ is always false
Any compound statement is always false.

Contingency

Compound statement can either be true or false.

logical Equivalence ($\Leftrightarrow$)

$P \Leftrightarrow q$ if both have same truth value
or $P \leftrightarrow q$ is always tautology.

~~Laws~~ of log.

8) S.T. ~~$P \rightarrow (Q \wedge R) \Leftrightarrow [\neg R \rightarrow \neg(P \vee Q)]$~~ $(P \vee q) \rightarrow r \Leftrightarrow [\neg r \rightarrow \neg(P \vee q)]$

P	q	r	P∨q	(P∨q)→r	¬P∨q	¬r	¬r→¬(P∨q)
0	0	0	0	1	1	1	1
0	0	1	0	1	1	0	1
0	1	0	1	0	0	1	0
0	1	1	1	1	0	0	1
1	0	0	1	0	0	1	0
1	0	1	1	1	0	0	1
1	1	0	1	0	0	1	0
1	1	1	1	1	0	0	1

DATE:
PAGE

8) De Morgan's law.

$\neg(P \vee q) \Leftrightarrow \neg P \wedge \neg q$
$\neg(P \wedge q) \Leftrightarrow \neg P \vee \neg q.$

9) Associative law

$P \vee (q \vee r) \Leftrightarrow (P \vee q) \vee r$
$P \wedge (q \wedge r) \Leftrightarrow (P \wedge q) \wedge r.$

10) Distributive laws
$P \vee (q \wedge r) = (P \vee q) \wedge (P \vee r)$
$P \wedge (q \vee r) = (P \wedge q) \vee (P \wedge r)$

11) Law of Negation of a conditional

$\neg(P \rightarrow q) \Leftrightarrow P \wedge \neg q.$

12) Transitive Rule
If $u \Leftrightarrow v$ and $v \Leftrightarrow w$
then $u \Leftrightarrow w$

PAGE:

$P \rightarrow \neg q$

1
1
1
0

nts.
lse.

ing.

Laws of Logic

DATE: PAGE:

1) Law of Double Negation.

$\neg\neg P \Leftrightarrow P$.

2) Idempotent law

$P \vee P \Leftrightarrow P$; $P \wedge P \Leftrightarrow P$.

3) Identity law.

$(P \vee F) \Leftrightarrow P$; $(P \wedge T) \Leftrightarrow P$

4) Inverse laws

$(P \vee \neg P) \Leftrightarrow T$; $(P \wedge \neg P) \Leftrightarrow F$

5) Commutative law.

$P \vee q \Leftrightarrow (q \vee P)$

$P \wedge q \Leftrightarrow q \wedge P$

6) Absorption law.

$P \vee (P \wedge q) \Leftrightarrow P$; $P \wedge (P \vee q) \Leftrightarrow P$.

7) Domination law.

$P \vee T \Leftrightarrow T$; $P \wedge F \Leftrightarrow F$

DATE: PAGE:

Q)

p	q	¬p	¬q	p∧¬q	¬p∨¬q	p→¬q
0	0	1	1	0	1	1
0	1	1	0	0	1	1
1	0	0	1	1	1	1
1	1	0	0	0	0	0

Q) Let p & q be primitive statements. for which condition p→q is false. Determine the truth values of following compound proposition.

-> i) p∧q = false
ii) ¬p∨q = false
iii) q→p = true
iv) ¬q→¬p = false

Q) Let p, q & r be propositions having 0, 0, & 1. Find truth value of following compound proposition.

i) (p∨q)∨R. = true
(p∧q)∧r = false
(p∧q)→r = true
p→(q∧r) = true
p→(q→(¬r)) = true
p∧(r→q) = false

PAGE: DATE: PAGE:

Q) For given propositions.
p: Circle is a conic
q: 2 is a composite number
r: $\sqrt{2}$ is irrational number

Express the following cp in words

1) $p \wedge \neg q$.
→ Circle is a conic and 2 is not a composite number

2) $q \rightarrow \neg p$
⇒ If 2 is a composite number then circle is not conic

3) $p \rightarrow (q \bar{\vee} r)$
If circle is conic then either 2 is a composite number or $\sqrt{2}$ is irrational number but not both.

4) $\neg p \leftrightarrow q$.
→ If circle is not a conic then 2 is a composite number and If 2 is a composite number then circle is not conic

5) $\neg p \vee q$.
→ Circle is not a conic or 2 is a composite number.

5) Conditional operator ($\rightarrow$)

$p \rightarrow q$ If p then q.

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

If p is true $\Leftrightarrow$ q is true
If p is false q can either be true or false

6) Biconditional operator ($\leftrightarrow$)

$P \leftrightarrow q$.

-> If p then q and If q then p

p	q	$P \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

DATE: PAGE:

Open statement
They can either be true or false
Ex:
p(x): x is even number

Logical Connectives

1) Negation (~ or ¬)

p: 2 is even number.
¬p: 2 is not even number.

2) Conjunction operator (∧)

And operation.

3) Disjunction operator (∨)

OR operation.

4) Exclusive OR (⊻)

p	q	p ⊻ q
0	0	0
0	1	1
1	0	1
1	1	0

DATE: PAGE:

$$a_n = \alpha(7)^n + \beta(3)^n + \frac{n^2}{4} + \frac{n}{3} + \frac{13}{72}$$

Propositional Logic

It ~~can~~ is a simple statement which has truth values.

It can either be true or false.

Simple propositions cannot be divided.

~~(They are co~~

Compound propositions are formed using logical connectives.

Simple propositions part of compound propositions are called as primitives.

Propositions are indicated by small or capital letters.

$\wedge$ → And

$\vee$ → OR

$\overline{\vee}$ → X-OR.

$$a_n^{(P)} = \frac{7n}{2} + \frac{21}{4}$$

$$a_0 = \alpha + \beta + \frac{21}{4} = 1$$

$$a_1 = 2\alpha + 3\beta + \frac{7}{2} + \frac{21}{4} = 1.$$

$$\alpha = -5 \qquad \beta = \frac{3}{4}$$

$$a_n = -5(2)^n + \frac{3^{n+1}}{4} + \frac{7n}{2} + \frac{21}{4}$$

4) $a_{n+2} - 10a_{n+1} + 21a_n = 3n^2 - 2, \quad n \geq 0.$

->

$$r^2 - 10r + 21 = 0.$$

$$r = 7, 3.$$

$$a_n^{(P)} = A_2 n^2 + A_1 n + A_0$$

$$A_2(n+2)^2 + A_1(n+2) + A_0 - 10[A_2(n+1)^2 + A_1(n+1) + A_0] + 21[A_2 n^2 + A_1 n + A_0] = 3n^2 - 2$$

$$A_2[(n+2)^2 - 10(n+1)^2 + 21n^2] + A_1[n+2 - 10(n+1) + 21n] + A_0 - 10A_0 + 21A_0 = 3n^2 - 2$$

$$A_2[n^2 + 4 - 10n^2 - 10 - 20n + 21n^2] + A_1[12n - 8] + 12A_0 = 3n^2 - 2$$

$$A_2[12n^2 - 16n - 6] + A_1[12n - 8] + 12A_0 = 3n^2 - 2.$$

$$n^2[12A_2] + n[-16A_2 + 12A_1] + 12A_0 - 8A_1 - 6A_2 = -2$$

$$12A_2 = 3$$

$$A_2 = 1/4.$$

$$12A_1 = 16A_2$$

$$3A_1 = 4A_2$$

$$A_1 = 1/3$$

$$12A_0 - 8A_1 - 6A_2 = -2$$

$$12A_0 - \frac{8}{3} - \frac{6}{4} = -2$$

$$12A_0 = \frac{13}{6}$$

$$A_0 = \frac{13}{96}.$$

DATE: PAGE:

3) $a_{n+2}^2 - 5a_{n+1}^2 + 6a_n^2 = 7n$

$b_n = a_n^2$

$b_{n+2} - 5b_{n+1} + 6b_n = 7n$

$\Rightarrow r^2 - 5r + 6 = 0$

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

$b_n^{(h)} = \alpha(2)^n + \beta(3)^n$

$b_n^{(p)} = A_1 n + A_0$.

$(A_1(n+1) + A_0)^2 - 5(A_1(n+1) + A_0) + 6(A_1 n + A_0) = 7n$

$(A_1 n + 2A_1 + A_0)^2 - 5(A_1 n + A_1 + A_0) + 6A_1 n + 6A_0 = 7n$

$A_1^2 n^2 + 4A_1^2 + A_0^2 - 2A_1 n A_0 - 4A_1^2 n - 4A_1 A_0$
$- 5A_1 n - 5A_1 - 5A_0 + 6A_1 n + 6A_0 = 7n$

$A_1^2 n^2 + 4A_1^2 + A_0^2 - 2A_1 n A_0 - 4A_1^2 n - 4A_1 A_0$
$+ A_1 n + A_1 - 5A_0$

$A_1(n+2) + A_0 - 5[A_1(n+1) + A_0] + 6[A_1 n + A_0] = 7n$

$A_1 n + 2A_1 + A_0 - 5A_1 n - 5A_1 - 5A_0 + 6A_1 n + 6A_0 = 7n$

$2A_1 n - 3A_1 + 2A_0 = 7n$

$A_1 = \frac{7}{2}$.

$2A_0 = 3A_1$

$A_0 = \frac{3 \times 7}{4} = \frac{21}{4}$.

$a_n(p) =$

$a_0 =$

$a_1 =$

$\alpha =$

a_n

4) a_n

->

a_1

F

$\therefore a_n = \frac{1}{9}(-2)^n + \left(\frac{-2}{3}\right) n(-2)^n + \frac{8}{9}$

2) $a_{n+2} - 4a_{n+1} + 3a_n = -200, \; a_0 = 3000, a_1 = 3300$

→ $r^2 - 4r + 3 = 0$

$r = 3, 1.$

$\therefore a_n^{(h)} = \alpha(3)^n + \beta(1)^n.$

$= \alpha(3^n) + \beta$

$a_n^{(p)} = An \; A_0.$

$(n+2)A_0 - 4(n+1)A_0 + 3nA_0 = -200.$

$nA_0 + 2A_0 - 4nA_0 - 4A_0 + 3nA_0 = -200$

$A_0 = \frac{-200}{(3n+1)}$

$nA_0 + 2A_0 - 4nA_0 - 4A_0 + 3nA_0 = -200$

$-2A_0 = -200$

$A_0 = 100.$

$a_n = \alpha 3^n + \beta + 100n.$

$3000 = \alpha + \beta$ ①

$3300 = 3\alpha + \beta + 100$

$\therefore 3\alpha + \beta = 3200$ ②

$\alpha = 100, \; \beta = 2,900.$

$a_n = 100(3^n) + 100n + 2,900.$

DATE: PAGE:

1) $a_n + 4a_{n-1} + 4a_{n-2} = 8, \quad n \geq 2, a_0 = 1, a_1 = 2$

2) $a_{n+2} - 4a_{n+1} + 3a_n = -200, \quad n \geq 0, a_0 = 3000, a_1 = 3$

3) $a^2_{n+2} - 5a^2_{n+1} + 6a^2_n = 7n, \quad n \geq 0, a_0 = a_1 = 1$

4) $a_{n+2} - 10a_{n+1} + 21a_n = 3n^2 - 2, \quad n \geq 0,$

5) $a_n - 3a_{n-1} - 4a_{n-2} = 4^n, \quad n \geq 2$

1) $a_n + 4a_{n-1} + 4a_{n-2} = 8$

$\rightarrow \quad r^2 + 4r + 4 = 0$

$r = -2, -2.$

$a_n^{(p)} = A_0.$

~~$A_0^2 + 4A_0 + 4 = 8$~~

~~$A_0^2 + 4A_0 = 4$~~

~~$A_0 =$~~

$A_0 + 4A_0 + 4A_0 = 8$

$A_0 = 8/9$

$a_n = \alpha(-2)^n + \beta n(-2)^n + 8/9$

$a_0 = 1$

$\alpha + 8/9 = 1$

$\alpha = 1/9$

$a_1 = 2$

$-\frac{2}{9} + \beta(-2) + 8/9 = 2$

$(-2)\beta = 2 - \frac{2}{3} = -2$

Mathematical Induction

DATE: PAGE:

i) Basis step : $n = 1$.
ii) Induction hypothesis: Assume expression is true for $n = k$.
iii) Induction hypothesis: Now prove that expression is true for $n = k+1$

Q) $3^{n+1} - 1 = 2z \quad (z \in N)$

-> $\therefore n = 1$

$\Rightarrow LHS = 3 - 1 = 2$

$\Rightarrow z = a \quad (a \in N)$

For $n = k$

$\therefore 3^k - 1 = 2y. \quad (y \in N)$

For $n = k+1$

$\Rightarrow 3^{k+1} - 1 = 3^k \cdot 3 - 1$

$= (2y+1)3 - 1$

$= 6y + 2.$

$= 2(3y+1)$

$= 2x \qquad x = 3y+1 \therefore x \in N$

$\therefore$ Proved.

Q) $1 + 3 + 5 + \cdots + (2n-1) = n^2$

-> i) $n = 1$

$\Rightarrow 1 = 1^2 = 1$

ii) Let $n = k$

$\Rightarrow 1 + 3 + 5 + \cdots + (2k-1) = k^2.$

iii) To prove for $n = k+1$

$\Rightarrow 1 + 3 + 5 + \cdots + (2k-1) + (2(k+1)-1)$

$= k^2 + 2k + 1$

$= (k+1)^2$

$\therefore$ Proved

Q) -> i)

ii)

iii)

Q) ->

$\therefore$

DATE: PAGE:

Q) $n^3+2n = 3z \quad (z \in N)$

→ i) $n = 1$

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

$\therefore z = 1$

ii) $n = k.$

$k^3+2k = 3y \quad (y \in N)$

iii) $n = k+1.$

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

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

$= k^3+1+3k^2+3k+2k+2.$

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

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

as $y \in N$ & $k^2+k+1 \in N$

$= 3x \quad \therefore x \in N$

$LHS = RHS$ proved

Q) $2^n < n! \quad \forall n > 3$

→ ~~$\forall \Rightarrow \exists$~~

i) $n = 4.$

$2^4 = 16$

$\therefore 16 < 4! = 24$

$16 < 24$

ii) Let $n = k$

$\Rightarrow 2^k < k!$

iii) To prove $2^{(k+1)} < (k+1)!$

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

$< k! \cdot 2.$

LKT as $k > 3 \Rightarrow (k+1) > 2$

$\therefore k! \cdot 2 < k!(k+1)$

$\therefore < (k)!(k+1)$

$\therefore 2^{k+1} < (k+1)!$

$\therefore$ Proved