Foundation for Advancement of Science & Technology

Discrete Structures

		Notes	Practise
Chapter 01: Logic and Proofs			
1) Propositional Logic	(1.1)	✓	✓
2) Applications of propositional logic	(1.2)	✓	✓
3) propositional equivalences	(1.3)	✓	✓
4) predicates and quantifiers	(1.4)	✓	✓
5) nested quantifiers	(1.5)	✓	✓
6) rules of inference	(1.6)	✓	✓
7) proofs	(1.7)	✓	✓
Chapter 02: Basic Structures			
8) Sets	(2.1)	✓	✓
9) set operations	(2.2)	✓	✓
10) functions	(2.3)	✓	✓
11) sequences and summations	(2.4)	✓	✓
12) cardinality of sets	(2.5)	✓	✓
Chapter 04: Number Theory & cryptography			
13) divisibility & modular arithmetic	(4.1)	✓	✓
14) primes and gcd	(4.3)	✓	✓
15) solving congruences	(4.4)	✓	✓
16) applications of congruences	(4.5)	✓	✓
17) cryptography rsa	(4.6)	✓	✓
Chapter 05: Induction			
18) mathematical induction	(5.1)	✓	✓

Foundation for Advancement of Science & Technology

		Notes	Praise
Chapter 6: Counting			
19) basics of counting	(6.1)	✓	✓
20) pigeonhole principle	(6.2)	✓	✓
21) permutation & combination	(6.3)	✓	✓
22) binomial	(6.4)	✓	✓
~~23) generalized P and C~~	~~(6.5)~~		
Chapter 9: Relations			
24) relations and properties	(9.1)	✓	✓
~~25) n-ary relations~~	~~(9.2)~~		
26) representing relations	(9.3)	✓	✓
27) equivalence relations	(9.5)	✓	✓
28) partial orderings	(9.6)	✓	✓
Chapter 10: Graphs			
29) graph models	(10.1)	✓	✓
30) graph types	(10.2)	✓	✓
31) isomorphism	(10.3)	✓	✓
32) Euler & Hamilton Paths	(10.5)	✓	✓
33) Shortest Path	(10.6)	✓	✓
34) planar graphs	(10.7)	✓	✓
Chapter 11: Trees			
35) Intro	(11.1)	✓	✓
36) applications	(11.2)	✓	✓
37) tree traversal	(11.3)	✓	✓
38) spanning trees	(11.4)	✓	✓
39) min spanning trees	(11.5)	✓	✓

Foundation for Advancement of Science & Technology

Chapter 01: The Foundations - Logic and Proofs

1) Propositional logic

- Proposition = any declarative statement

e.g: Toronto is capital of Canada , $1+1=2$

$x+1=2$ ⟶ not proposition (will be if value assigned to it)

- Negation ($\neg p$) = negative of truth value of p

e.g: p = Michael's PC runs linux

$\neg p$ = Michael's PC does not run linux

p	¬p
T	F
F	T

- Conjunction ($\wedge$) = and (T when both T, else F)

words used = and , but

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

- disjunction ($\vee$) = or (F when both F , else T)

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

- exclusive or ($\oplus$) = only one of them

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

- implication ($\rightarrow$) "if p, then q"

e.g "If you get 100% on the final, you get an A"

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

- converse ($q \rightarrow p$)
- contrapositive ($\neg q \rightarrow \neg p$) same truth value as $p \rightarrow q$
- inverse ($\neg p \rightarrow \neg q$)

		negation	negation	implication	converse	contrapositive	inverse
p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$q \rightarrow p$	$\neg q \rightarrow \neg p$	$\neg p \rightarrow \neg q$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	F	T
F	T	T	F	T	F	T	F
F	F	T	T	T	T	T	T

- biconditional ($\leftrightarrow$) T when both same, else F

words: p necessary and sufficient for q, p iff q

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

Precedence of operators

1) $\neg$ 2) $\wedge$ 3) $\vee$ 4) $\rightarrow$ 5) $\leftrightarrow$

2) Applications of Propositional Logic

translating into english sentences

6) You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years older.

q = you can ride roller coaster $(r \wedge \neg s) \rightarrow \neg q$

r = you are under 4 feet tall

s = you are older than 16 years.

Foundation for Advancement of Science & Technology

3) Propositional Equivalences

- Tautology: a compound statement that is always true
- Contradiction: a compound statement that is always false
- Contingency: sometimes true, sometimes false

De Morgan's laws

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

Identity laws

3) $p \wedge T \equiv p$
4) $p \vee F \equiv p$

Domination laws

5) $p \vee T \equiv T$
6) $p \wedge F \equiv F$

Idempotent laws

7) $p \wedge p \equiv p$
8) $p \vee p \equiv p$

Double negation law

9) $\neg(\neg p) \equiv p$

Commutative law

10) $p \vee q \equiv q \vee p$
11) $p \wedge q \equiv q \wedge p$

Associative law

12) $(p \vee q) \vee r \equiv p \vee (q \vee r)$
13) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

Distributive law

14) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
15) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

Absorption laws

16) $p \vee (p \wedge q) \equiv p$
17) $p \wedge (p \vee q) \equiv p$

Negation laws

18) $p \vee \neg p \equiv T$
19) $p \wedge \neg p \equiv F$

Foundation for Advancement of Science & Technology

Logical Equivalences involving conditional Statements

20) $p \to q \equiv \neg p \vee q$

21) $p \to q \equiv \neg q \to \neg p$

22) $p \vee q \equiv \neg p \to q$

23) $p \wedge q \equiv \neg(p \to \neg q)$

24) $\neg(p \to q) \equiv p \wedge \neg q$

} same when multiplied by negation

25) $(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$

26) $(p \to q) \wedge (q \to r) \equiv (p \vee q) \to r$

27) $(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

28) $(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

Logical Equivalences involving Biconditional Statements

29) $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

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

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

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

4) Predicates and Quantifiers

- predicates = property of the subject of the statement.
- quantifiers = tells the range for which a predicate is true

$\forall$ universal quantification (for all) true for every x.

$\exists$ for some (there is an x for which $P(x)$ is true) / atleast one

Q) Let $P(n)$ be $x+1 > x$. what is truth value of quantification

$\forall x\, P(x)$ is true

Foundation for Advancement of Science & Technology

Equivalences

1) $\neg \forall x P(x) \equiv \exists x \neg P(x)$

2) $\neg \exists x Q(x) \equiv \forall x \neg Q(x)$

1.5 : Nested Quantifiers

$\forall x \forall y (x + y = 0)$

= for every real number x, there is a real number y such that $x+y=0$.

$\forall x \forall y ((x > 0) \wedge (y < 0) \rightarrow (xy < 0))$

where domain for both is all real numbers

= for every real number x and for every real number y, if $x > 0$ and $y < 0$ then $xy < 0$. if x is positive and y is negative, then xy is negative.

Quantification of two variables

Statement	When True	When false
$\forall x \forall y P(x,y)$ $\forall y \forall x P(x,y)$	$P(x,y)$ is true for every pair x,y	There is a pair x,y for which $P(x,y)$ is false.
$\forall x \exists y P(x,y)$	for every x there is a y for which $P(x,y)$ is true	There is an x such that $P(x,y)$ is false for every y.
$\exists x \forall y P(x,y)$	There is an x for which $P(x,y)$ is true for every y	for every x there is a y for which $P(x,y)$ is false
$\exists x \exists y P(x,y)$ $\exists y \exists x P(x,y)$	There is a pair x,y for which $P(x,y)$ is true	$P(x,y)$ is false for every pair x,y.

* in nested quantifiers, see sign of last quantification.

$\forall x$ (for all) then implication sign ($\rightarrow$)

$\exists x$ (for some) then and sign ($\wedge$)

Translate $\forall x (C(x) \vee \exists y (C(y) \wedge F(x,y)))$

$C(x)$ = x has computer

$F(x,y)$ = x and y are friends

domain for both x and y consists of all students in your school

for every student x in your school, x has a computer or there is a student y such that y has a computer and x and y are friends.

6) Rules of Inference

1) Modus ponens

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q \end{array} \qquad (p \wedge (p \to q)) \to q$$

2) Modus tollens

$$\begin{array}{l} \neg q \\ p \to q \\ \hline \therefore \neg p \end{array} \qquad (\neg q \wedge (p \to q)) \to \neg p$$

3) Hypothetical Syllogism

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array} \qquad ((p \to q) \wedge (q \to r)) \to (p \to r)$$

4) Disjunctive Syllogism

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array} \qquad ((p \vee q) \wedge \neg p) \to q$$

Foundation for Advancement of Science & Technology

5) Addition

$$\frac{p}{\therefore p \vee q} \qquad p \rightarrow (p \vee q)$$

6) Simplification

$$\frac{p \wedge q}{\therefore p} \qquad (p \wedge q) \rightarrow p$$

7) Conjunction

$$\frac{p \quad q}{\therefore p \wedge q} \qquad (p \wedge q) \rightarrow (p \wedge q)$$

8) Resolution

$$\frac{p \vee q \quad \neg p \vee r}{\therefore q \vee r} \qquad ((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$$

9) Universal Instantiation

$$\frac{\forall x \, P(x)}{\therefore P(c)}$$

10) Universal Generalization

$$\frac{P(c) \text{ for arbitrary } c}{\therefore \forall x \, P(x)}$$

11) Existential Instantiation

$\exists x\, P(x)$

$\therefore P(c)$ for some element c

12) Existential Generalization

$P(c)$ for some element c

$\therefore \exists x\, P(x)$

* product of two odd numbers is odd
* product of two even numbers is even
* sum of two odd numbers is even
* sum of two even numbers is even
* subtraction of two odd numbers is even
* subtraction of two even number is even
* sum of odd + even is odd
* subtraction of odd and even is odd.

7) Proofs

- definitions

1)	even	$n = 2K$
2)	odd	$n = 2K+1$
3)	rational	$r = p/q$ and $q \neq 0$
4)	prime	$n = r \cdot s$ and $n > 1$ and ($r = 1$ or $s = 1$)
5)	composite	$n = r \cdot s$ and $n > 1$ and $r \neq 1$ and $s \neq 1$
6)	division	$n = d \cdot K$ or $K = \frac{n}{d}$, $d \neq 0$

- direct proof $(p \rightarrow q)$

assume p is true, if p is T then q must also be T

- Indirect proof
  1) proof by contraposition $(\neg q \rightarrow \neg p)$
     1) assume concl is false
     2) show assumption is false, so original conditional statement is T

Foundation for Advancement of Science & Technology

2) proof by contradiction

1) suppose $\neg p$ is true

2) show both p and $\neg p$ are true, hence contradiction

3) mathematical induction

1) show $p(1)$ is true

2) show $p(k) \rightarrow p(k+1)$ is true

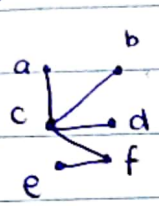
multiple edges

Foundation for Advancement of Science & Technology

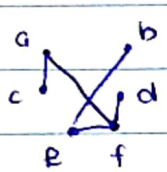
Chapter 11 : Trees

35) Introduction

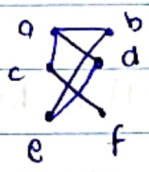
- a tree is a connected undirected graph with no simple circuits, multiple edges or loops.



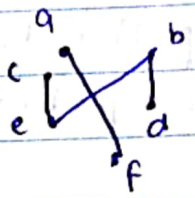
tree



tree



not tree
e, b, a, d, e.
(multiple edge)

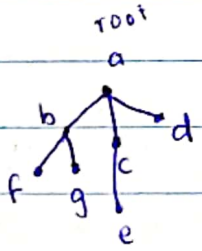


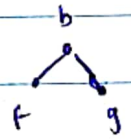
not tree
(not connected)

- an undirected graph is a tree if and only if there is a unique simple path between any two of its vertices

Rooted Tree

a vertex is designated as root and every edge is directed away from root.

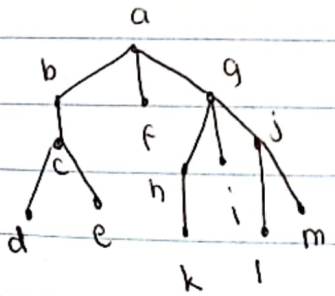




subroot
b.

vertices of rooted tree is leaf

vertices that have children are internal vertices



parent of c = b

children of g = h, i, j

siblings of h = i, j

ancestors of e a, b, c

descendants of b c, d, e

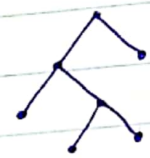
internal vertices: a, b, c, g, h, j

leaves: d, e, f, k, i, l, m

Foundation for Advancement of Science & Technology

• a rooted tree is called m-ary tree if all internal vertices (children) have not more than m children.

• a rooted tree is called full m-ary tree if every internal vertex has exactly m children. (if m = 2 → binary tree)



full binary tree

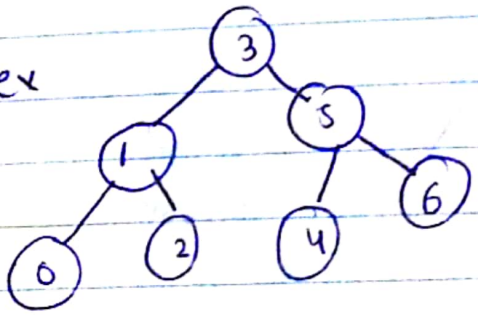
not full m-ary tree bec some have 3 children and some 2

• Ordered rooted trees
drawn so children of each internal vertex are shown in order from L to R
• first child is called left child and second right

Properties of trees
1) a tree with n vertices has n-1 edges

3.6) Application of Trees
. Binary Search Tree (has max 2 child)
a tree in which forevery node
→ left child < node
→ right child > node

ex

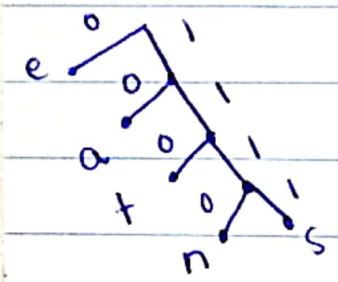


the inorder traversal will result in sorted order
* first compare w/ root then next element

- decision trees

based on comparisions

- Prefix codes



e = 0
a = 10
t = 110
n = 1110
s = 1111

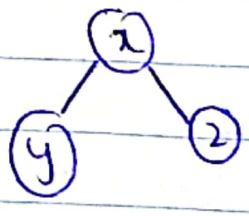
see for 0 or 4 1s.

11111011100

s a n e.

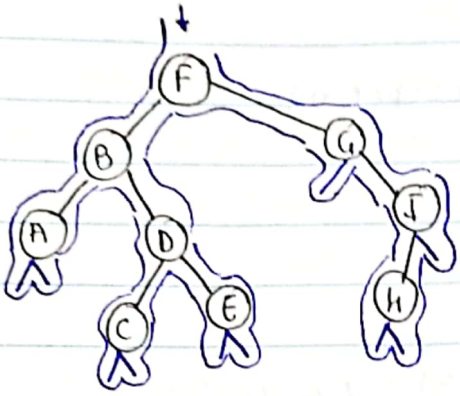
37) Tree Traversal

Pre order	root left right
In order	left root right
Post order	left right root



preorder	x y z
Inorder	y x z
postorder	y z x

of Science & Technology



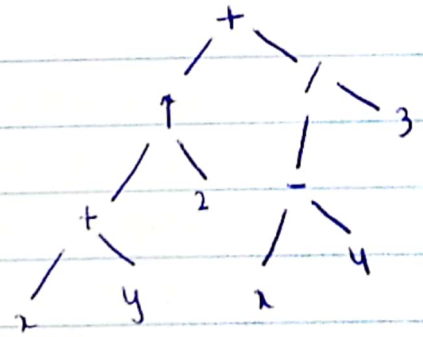
1) start from root
2) go through each node
   1 → pre order
   2 → in order
   3 → post order

pre order = FBADCEGIH
in order = ABCDEFGHI
post order = ACEDBHIGF

Infix, Prefix and Postfix Notation

Inorder traversal → infix form
Preorder traversal → prefix form
postorder traversal → postfix form

Q) ordered rooted tree for ((x+y) ↑ 2) + ((x-4)/3)



* inorder is general type (use brackets)

Q) Prefix form for ((x+4) ↑ 2) + ((x - 4)/3) preorder

+ ↑ + x y 2 / - x 4 3

Root L R.

Foundation for Advancement of Science & Technology

Q) value of prefix expression (prefix = pre order so root before)

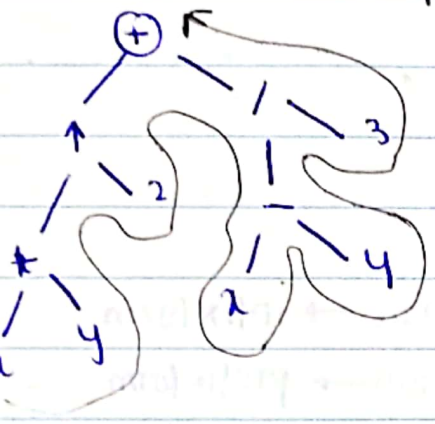
+ - * 2 3 5 / ↑ 2 3 4

(2 x 3) = 6 - 5 = 1 (2 ^ 3) = 8 / 4 = 2

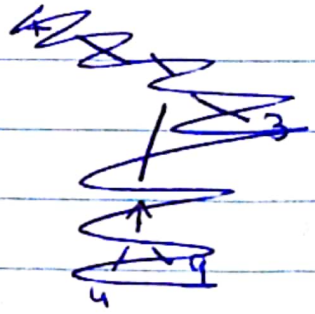
1 + 2 = 3

Q) postfix form of expression ((x+y) ↑ 2) + ((x-4) / 3)? (post order)

L R root



x y + 2 ↑ x 4 - 3 / +



Q) value of postfix 7 2 3 * - 4 ↑ 9 3 / +

2 x 3 = 6

7 - 6 = 1 ↑ 4 = 1 9 / 3 = 3

1 + 3 = 4

Foundation for Advancement of Science & Technology

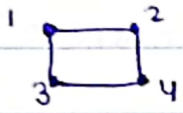
38) Spanning Trees

a connected subgraph S of graph G (V, E) iff
1) S contains all vertices of G
2) S contains (V - 1) edges

cannot have any cycle

subgraph = can be equal to or less

connected = every vertex should be reachable.



G

4 vertex

connected.

(4-1) = 3 edges.

K_4 how many possible spanning trees?

n^{n-2} → no. of spanning trees (n = no. of vertex) for complete graph

39) Minimum Spanning Trees

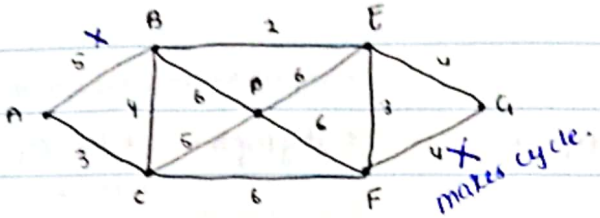
- Kruskal's Algorithm

1) construct min heap wl 'e' edges
2) take one by one edge and add in spanning tree (cycle should not be created)

Best case (n-1) edges

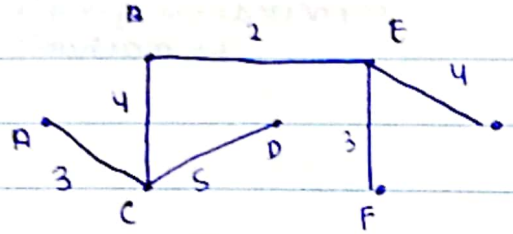
Worst case e edges

* can be disconnected while making it, but end result → will be connected.



(n-1) edges → (7-1) = 6

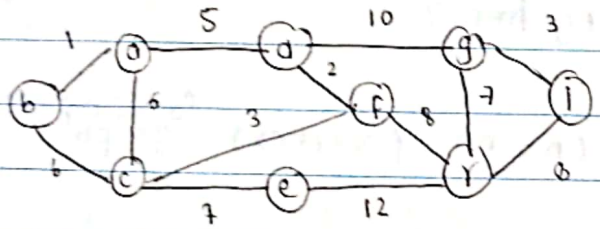
select edges so no loop and least cost.



1) choose min weight edge and draw
2) choose next min but ensure no loop

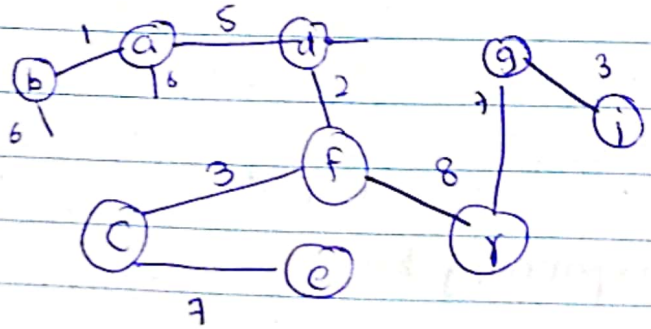
cost = 21

Prim's Algorithm



edges = n-1

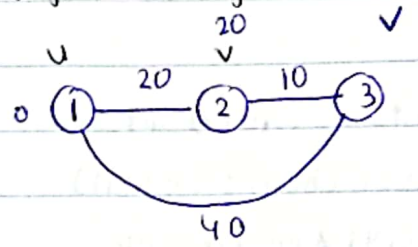
1) start from any vertex
2) keep prev. greater edge in mind too
3) no loop



Foundation for Advancement of Science & Technology

1) see from source
2) see from added source too, select shortest

Dijkstra's Algorithm



source = 1

distance of v

d(u) = 0 + 20 < ∞ } from 1

d(u) = 0 + 40 < ∞

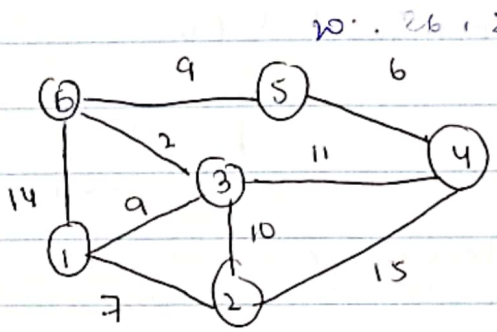
d(v)

20 + 10 < 40 so d(v) = 30

distance cost distance

if d(u) + c(u,v) < d(v)

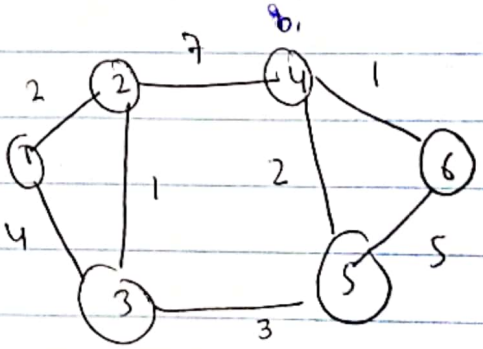
d(v) = d(u) + c(u,v)



source	Destination				
1	2	3	4	5	6
	7	9	∞	∞	14
1,2	7	9	22	∞	14
1,2,3	7	9	20	∞	11
1,2,3,6	7	9	20	20	11
1,2,3,6,4				23	

1,2,3,6,4,5

Shortest path: 1,3,6



	1	2	3	4	5	6
		2	4			
	123		3	9		
	1235			9	6	
	12354			8		9

1 2 3 5 4 6

Shortest path: 1,2,4,6

Roster method: simple curly brackets
Set Builder: all members w/ property.
ex: O = set of all the integers < 10.
O = {x | x is an odd +ve integer < 10}

6) Sets

set: a well defined unordered collection of distinct elements is called set

A = {1, 2, 3, 4} B = {2, 3, 4, 1} order doesn't matter (both are equal)

C = {1, 1, 2, 2, 3, 4} also equal bec it means {1, 2, 3, 4} * no duplicate

nullset/emptyset: a set w/ no elements. Denoted as ∅ or { }

subset: if every element of A is also element of B then A is subset of B

A = {1, 2, 3, 4} B = {1, 2, 3, 4, 5}

A ⊆ B

A = {1, 2, 3, 4} C = {2, 3}

C ⊆ A (C ≤ A) less than or equal elements

Proper subset = any subset of A which is not a trivial subset of A. (complete)

A = {1, 2, 3, 4} B = {1, 2, 3} should be less (cannot be equal)

A ⊂ B (B ⊂ A) less elements

Cardinality: total number of elements in a set

if A ⊆ B and B ⊆ A then A = B

Power set: if A is a finite set then set of all subsets of A is power set.

A = {1, 2, 3}

P(A) = { ∅, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3} }

|A| = n elements in Power set = 2^n

Cartesian Product: denoted by $A \times B$, is set of all ordered pairs (a,b)

$A = \{1,2\}$ $B = \{a,b,c\}$

$A \times B = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}$

$N = \{0,1,2,3,\dots\}$ set of natural numbers

$Z = \{\dots,-1,0,1,\dots\}$ set of integers

$Z^+ = \{1,2,3,4\dots\}$ set of integers (positive)

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

R set of real numbers (any +, - number) includes rational & irrational

R^+ set of posible real numbers

C set of complex numbers

9) Set Operations

1) Union = set of elements in A or B or both ($\cup$)

2) Intersection = set of elements in both A and B ($\cap$)

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

3) disjoint sets: sets whose intersection is empty

4) difference $(A-B)$ elements in A but not in B

5) Complement: elements not in that set

Set Identities: (same as propositional equivalences)

$\wedge \rightarrow \cap$

$\vee \rightarrow \cup$

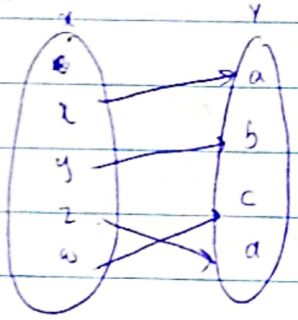
membership table (0 and 1s)

Foundation for Advancement of Science & Technology

Symmetric Difference ⊕ set containing elements in either A / B but not in both

(10) functions

if x and y are two sets and each element of x is assigned to unique element of y then it is a function



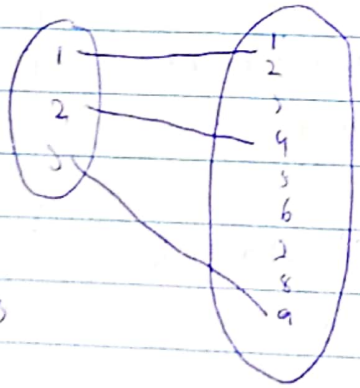
* (x has to be mapped but can't be mapped twice

A element of y can be empty

domain

if a function from A to B then A is domain and B is codomain

$f = x^2$



domain = {1, 2, 3}

range = {1, 4, 9}

codomain = {1, 2, 3, 4, 5, 6, 7, 8, 9}

codomain: all elements of B

R is subset of B ($R \subseteq B$)

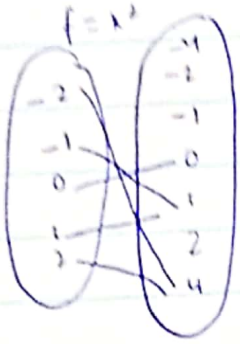
Range - connected elements

[ ] included
( ) not included

Kinds of function

1) one to one function (unique image)

image should be different for different elements



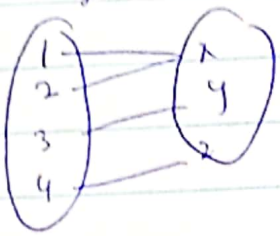
* if a function is not one to one then it is many to one

image of 2 and -2 same.

2) Onto function

preimage for all y element exists.

range = codomain



* if not onto then called into.

3) bijective one to one + onto.

*for check range, make x subject and see where 0.

4) Inverse

make x subject of the function.

5) Composite function

if $f: A \to B$ and $g: B \to C$ then $gof: A \to C$

$f(x) = x^2 + 1$ $\quad g(x) = 2x + 1$

$gof(x) = g(f(x))$

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

11) Sequences and Summations

Geometric series

$Tn = ar^{n-1}$ $\quad Sn = \frac{a(r^n - 1)}{r - 1}$

Arithmetic Series

$Tn = a + (n-1)d$ $\quad Sn = \frac{n}{2}[2a + (n-1)d]$

Summations

$\sum_{\text{starting point}}^{\text{endpoint}} f(x)$

Summation formulas

1) $\sum_{k=0}^{n} ar^k \quad (r \neq 0)$ $\quad \frac{ar^{n+1} - a}{r - 1} \quad r \neq 1$

2) $\sum_{k=1}^{n} k$ $\quad \frac{n(n+1)}{2}$

Foundation for Advancement of Science & Technology

3) $\sum_{k=1}^{n} k^2$ $\quad \frac{n(n+1)(2n+1)}{6}$

4) $\sum_{k=0}^{\infty} x^k$ $\quad |x|<1$ $\quad \frac{1}{1-x}$

5) $\sum_{k=1}^{\infty} k x^{k-1}$ $\quad |x|<1$ $\quad \frac{1}{(1-x)^2}$

Set Builder Notation

$S = \{ x \mid P(x) \}$

$A - B = A \cap \bar{B}$

$A \cap \bar{A} = \emptyset$

Set identities

1) Identity law
$A \cup \emptyset = A$
$A \cap U = A$

2) Domination Law
$A \cup U = U$
$A \cap \emptyset = \emptyset$

3) Idempotent law
$A \cup A = A$
$A \cap A = A$

4) Complement law
$(\bar{A}) = A$

5) Commutative law
$A \cup B = B \cup A$
$A \cap B = B \cap A$

6) Associative law
$A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cap C) = (A \cap B) \cap C$

7) Distributive law
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

8) Demorgan law
$\overline{A \cup B} = \bar{A} \cap \bar{B}$
$\overline{A \cap B} = \bar{A} \cup \bar{B}$

9) Absorption law
$A \cup (A \cap B) = A$
$A \cap (A \cup B) = A$

(3) Divisibility and Modular Arithmetic

Division

$a|b \rightarrow \frac{b}{a}$ $(b = ac)$

if $a|b$ and $a|c$ then $a|(b+c)$

$b = ad$ and $c = ae$

$b+c = ad+ae \rightarrow a(d+e)$

★ $a = dq + r$

$q = a \text{ div } d$ $(\frac{a}{d})$ integer that divides

$r = a \bmod d$ $(a-d)$ remainder $(d-q)$

$101 = 11 \cdot q + r$

$101 = 11 \cdot 9 + 2$ $q = 9$, $r = 2$

modular arithmetic

a is congruent to b modulo m if m divides $a - b$ $a \equiv b \bmod m$

is 17 congruent to 5 modulo 6

$17 - 5 = \frac{12}{6} = 2$ $17 \equiv 5 \bmod 6$

★ a and b are congruent modulo m iff there is integer k such as $a = b + km$

★ if $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then $a + c \equiv b + d \pmod m$ & $ac \equiv bd \pmod m$

★ $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

★ $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Foundation for Advancement of Science & Technology

14) Primes and Greatest Common Divisor

prime number = integer p is prime if its only factors are p and 1.

a | n such that $1 < a < n$ → composite

* if n is a composite integer then n has a prime divisor less than or equal to $\sqrt{n}$

Q) show 101 is prime

$\sqrt{101} = 10.05$

prime numbers less than 10 = 2, 3, 5, 7

101 not divisible by 2, 3, 5 or 7 hence prime.

Sieve of Eratosthenes

list all numbers, √ that number, cancel out all integers multiple of num ~~less~~ than prime numbers

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	~~43~~	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	~~89~~	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

2, 3, ~~4~~ 5, 7

Greatest common Divisor :
largest integer d such that d|a and d|b

* choose min powers.

24 = 1, 2, 3, 4, 6, 24, 12, 24
36 = 1, 2, 3, 4, 6, 9, 12, 18, 36 } 12 is largest common divisor

* integers a and b are relatively prime if their gcd is 1.
* integers a, b and c are pairwise relatively prime if their all gcd is 1

Least common multiple
Smallest positive integer that is divisible by both a and b.

* choose max power

$2^3 3^5 7^2$ and $2^4 3^3 = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)}$
$= 2^4 \cdot 3^5 \cdot 7^2 = 190512.$

* $ab = \gcd(a,b) \times \text{lcm}(a,b)$

Euclidean Algorithm:
let $a = bq + r$ then $\gcd(a,b) = \gcd(b,r)$

Q) gcd of 414 and 662 using Euclidean Algorithm

$662 = 414 \cdot 1 + 248$
$414 = 248 \cdot 1 + 166$
$248 = 166 \cdot 1 + 82$
$166 = 82 \cdot 2 + 2$
$82 = 2 \cdot 41 + 0$. gcd = 2
↓ gcd. (last non zero remainder)

Foundation for Advancement of Science & Technology

gcd as linear combination.

gcd of 2 integers can be expressed as $sa + tb$

gcd of 6 and 14 = 2

so $2 = (-2) \cdot 6 + 1 \cdot 14$

Bezout's Theorem: $\gcd(a,b) = sa + tb$

Q) Express $\gcd(252, 198) = 18$ as linear combination of 252 and 198

$$252 = 1 \cdot 198 + 54$$
$$198 = 3 \cdot 54 + 36$$
$$54 = 1 \cdot 36 + 18$$
$$36 = 2 \cdot 18$$

Using next to last division to express as linear combination

$$18 = 54 - 1 \cdot 36$$
$$18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$$
$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$$
$$18 = 4 \cdot 252 - 5 \cdot 198$$

of Science & Technol...

15) Solving Congruences

- Linear Congruences

$ax \equiv b \pmod{m}$

* if a and m are relatively prime integers (gcd=1) then inverse of a modulom exists.

Q) Find inverse of 3 modulo 7

$3 = 1 \cdot 3 \qquad 7 = 1 \cdot 7$

$7 = 2 \cdot 3 + 1$

$1 \cdot 7 - 2 \cdot 3 = 1$

s a t m

gcd = 1 hence inverse exists.

Euclidean algorithm

2 and 1 are Bezout coefficients

-2 is inverse of 3 modulo 7.

* inverse is lesser num's coeff.

Q) Find inverse of 101 modulo 4620

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$gcd = 1$

$1 = 3 - 1 \cdot 2 = 1 \cdot 3 - 1(23 - 7 \cdot 3)$

$= 8 \cdot 3 - 1 \cdot 23 = 8(26 - 1 \cdot 23) - 1 \cdot 23$

$= 8 \cdot 26 - 9 \cdot 23 = 8 \cdot 26 - 9(75 - 2 \cdot 26)$

$= 26 \cdot 26 - 9 \cdot 75 = 26(101 - 1 \cdot 75) - 9 \cdot 75$

$26 \cdot 101 - 35 \cdot 75 = 26 \cdot 101 - 35(4620 - 45 \cdot 101)$

$= 1601 \cdot 101 - 35 \cdot 4620$

$1601 \cdot 101 - 35 \cdot 4620$

inverse = 1601

express in form of Bezout coeff to see inverse

Foundation for Advancement of Science & Technology

+3

Chinese Remainder Theorem

$x \equiv a_1 \pmod{m_1}$ $x \equiv a_2 \pmod{m_2}$ $x \equiv a_3 \pmod{m_3}$ value of x?

m_1, m_2 and m_3 are relatively prime

$$x = (m_1 x_1 a_1 + m_2 x_2 a_2 + m_3 x_3 a_3) \bmod M$$

$$M = m_1 \times m_2 \times m_3$$

$$M_i = \frac{M}{m_i} = \frac{m_i \times m_j \times m_k}{m_i} = m_j \times m_k$$

$$M_i x_i \equiv 1 \pmod{m_i}$$

$a_1 = 1$ $m_1 = 5$
$a_2 = 1$ $m_2 = 7$
$a_3 = 3$ $m_3 = 11$

Q) $x \equiv 1 \pmod 5$ $x \equiv 1 \pmod 7$ $x \equiv 3 \pmod{11}$

1) $m = 5 \times 7 \times 11 = 385$

2) $m_1 = \frac{385}{5} = 77$ $m_2 = \frac{385}{7} = 55$ $m_3 = \frac{385}{11} = 35$

3) $m_1 x_1 \equiv 1 \pmod{m_1}$

$77 x_1 \equiv 1 \pmod 5$

$77 \pmod 5 = 2$

$= 2x_1 \equiv 1 \pmod 5$

choose where u get mod 1

$3(2x_1) \equiv 3(1 \pmod 5)$

$6x_1 \equiv 3 \pmod 5$

$1 x_1 \equiv 3 \pmod 5$

$\boxed{x_1 = 3}$

$m_2 x_2 \equiv 1 \pmod 7$

$55 x_2 \equiv 1 \pmod 7$

$55 \bmod 7 = 6$

$6 x_2 \equiv 1 \pmod 7$

$6(6x_2) \equiv (1 \pmod 7)6$

$36 x_2 \equiv 6 \bmod 7$

$1 x_2 = 6 \bmod 7$

$\boxed{x_2 = 6}$

$m_3 x_3 \equiv 1 \pmod{m_3}$

$35 x_3 = 1 \pmod{11}$

$6(2 x_3) = (1 \pmod{11})6$

$12 x_3 = 6 \pmod{11}$

$1 x_3 = 6 \pmod{11}$

$\boxed{x_3 = 6}$

4) $x = \left[(77 \times 3 \times 1) + (55 \times 6 \times 1) + (35 \times 6 \times 3)\right] \bmod 385$

$= 1191 \bmod 385 = 36$

Fermat's Theorem

$$x^{n-1} \equiv 1 \bmod n \quad = \quad a^{p-1} = 1 \bmod p$$

$2^{16} \bmod 17$

~~$2^{17-1} = 1 \bmod 17$~~

~~$2^{16} \equiv 1 \bmod 17$~~

$5^{2003} \bmod 7$

$p = 7 - 1 = 6$

$2003 = 333 \times 6 + 5$

$= (5^6)^{333} \cdot 5^5$

$= 1^{333} \cdot 3125$

$= 3125 \bmod 7 = 3$

16) ~~Solve~~ Applications of Congruences

Hashing Functions

$h(k) = k \bmod m$

location

Find location of $h(k) = k \bmod 111$ OF 064212848 and 037149212

$064212848 \bmod 111 = 14$

$37149212 \bmod 111 = 65$

Foundation for Advancement of Science & Technology

Psuedorandom numbers

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

Q) $m = 9, a = 7, c = 4$, seed $x_0 = 3$ $\quad x_{n+1} = (7x_n + 4) \bmod 9$

$x_1 = 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7$

$x_2 = 7x_1 + 4 \bmod 9 = 49 + 4 \bmod 9 = 53 \bmod 9 = 6$

$x_3 = 7x_2 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 60 \bmod 9 = 6$ ...

UPCs (Universal Product codes)

remainder should be 0.

$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$

Q) 11 digits 79357343104. check digit.

$(3 \times 7) + 9 + (3 \times 3) + 5 + (3 \times 7) + 3 + (3 \cdot 4) + 3 + (3 \times 1) + 0 + 3 \cdot 4 + x_{12} \equiv 0 \bmod 10$

$98 + x_{12} \equiv 0 \bmod 10$

$x_{12} = 2$

ISBNs

$x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 + 10x_{10} \equiv 0 \pmod{11}$

17) Cryptography

caesar cipher = (p+3) mod 26 ← fixed!

- ~~Caesar~~ Shift cipher
  - encryption $f(p) = (p+K) \bmod 26$
  - decryption $f^{-1}(p) = (p-K) \bmod 26$

A=0, Z=25 (one less than integer)

a) Encrypt STOP GLOBAL WARMING w/ shift K=11

1) text:	S	T	O	P		G	L	O	B	A	L		W	A	R	M	I	N	G
2) numbers:	18	19	14	15		6	11	14	1	0	11		22	0	17	12	8	13	6
3) (p+11) mod 26:	3	4	25	0		17	22	25	12	11	22		7	11	2	23	19	24	17
4) letters	D	E	Z	A		R	W	Z	M	L	W		H	L	C	X	T	Y	R

b) Decrypt w/ L=7

1) text:	L	E	W	L	Y	P	L	U	J	L		P	Z		H		N	Y	L	H	A		A	L	H	J	O	L	Y
2) numbers:	11	4	22	11	24	15	11	20	9	11		15	25	7	13	24	11	7	0	0	11	7	9	14	11	24
3) (L-7) mod 26	4	23	15	4	17	8	4	13	24		8	18	0	6	17	0	19	19	0	27	4	17				
4) letters	E	X	P	E	R	I	E	N	C	E		I	S		A		G	R	E	A	T		T	E	A	C	H	E	R.

- RSA Algorithm

1) choose 2 different prime numbers (p and q)
2) calculate $n = p \times q$
3) calculate $\phi(n) = (p-1) \times (q-1)$ copnme = gcd
4) choose 'e' such that $1 < e < \phi(n)$
   e is coprime to $\phi(n)$, $\gcd(e, \phi n) = 1$
5) calculate d such that $de \equiv 1 \bmod \phi(n)$
6) public key(e,n) private key(d,n)

Foundation for Advancement of Science & Technology

Q) In RSA cryptosystem, A uses 2 prime numbers $p = 13$ and $q = 17$ to generate public & private keys. If public key of A is 35, private key of A is?

1) $p = 13 \quad q = 17$

2) $n = p \times q = 13 \times 17 = 221$

3) $\phi n = (p-1) \times (q-1) = 12 \times 16 = 192$

4) $1 < e < 192$

$e = 35$ (public key) $\quad gcd(35, 192) = 1$

5) $de \equiv 1 \pmod{\phi n}$

$de \bmod (\phi n) = 1$

$d \times 35 \bmod 192 = 1$.

multiply such number by 35 that is mod w/ 192 is 1

$11 \times 35 \bmod 192$

$385 \bmod 192 = 1$

$d = 11$ (private key)

$de = 1 + k\,\phi n$

$d = \frac{1 + k\,\phi n}{e}$ k starts from 0, don't consider decimal

$= \frac{1 + 0 \times 192}{35} = \frac{1}{35}$, $\frac{1 + 192}{35} = \frac{193}{35}$, $\frac{1 + 2(192)}{35} = \frac{385}{35} = 11$

$d = 11$

A	0	G	6	M	12	S	18
B	1	H	7	N	13	T	19
C	2	I	8	O	14	U	20
D	3	J	9	P	15	V	21
E	4	K	10	Q	16	W	22
F	5	L	11	R	17	X	23
						Y	24
						Z	25

Foundation for Advancement of Science & Technology

Chapter 06: Counting

1) Basics of Counting

Product Rule: If there are n_1 ways to do task 1 and n_2 to task 2 then $n_1 n_2$ ways to do procedure (procedure broken down into tasks)

Sum Rule: if task can be done in either n_1 or n_2 ways then $n_1 + n_2$ ways to do task

Q) 2 employees rent floor w/ 12 offices. how many ways are there to assign different offices to these two employees

$$12 \times 11 = 132 \text{ ways}$$

Q) either faculty or student chosen. how many choices if there are 37 faculty and 83 students

$$37 + 83 = 120$$

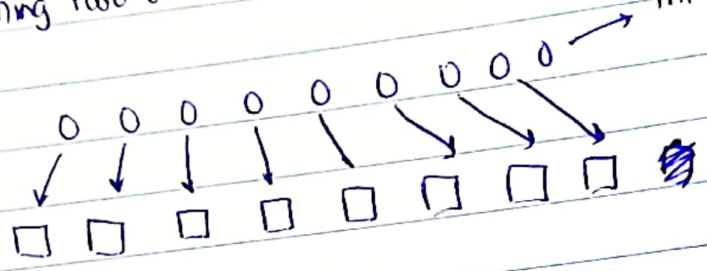
Subtraction Rule: if a task can be done in either n_1 or n_2 ways then number of ways to do task is $n_1 + n_2$ - common.

$$|A + B - A \cap B.|$$

Foundation for Advancement of Science & Technology

20) Pigeonhole Principle

if (N+1) or more objects are placed into N boxes then there is atleast one box containing two or more objects.



Q) If 6 color are used to paint 37 home, show 1 color will be of same color

R G B Y W B
1 1 1 1 1 1
6 6 6 6 6 6

so any one will be from b/w.

$\frac{37}{6} = 6$. 6 home each of color but remainder is 1

7 home may have same cycle

$\frac{37}{6} = 7$ ← greatest integer.

Generalized pigeonhole principle.

(n) pigeonhole : things (boxes)

(kn+1) pigeon = people.

(k+1) = common.

If n pigeonhole are occupied by kn+1 or more pigeons then atleast one pigeonhole is occupied by k+1 or more pigeons.

Q) Find min num of teachers to be sure that 4 of them are born in same month.

$n = 12$ $K+1 = 4$, $k = 3$

$kn + 1 = 12 \times 3 + 1 = 37$

Foundation for Advancement of Science & Technology

A box contains 10 blue balls, 20 red, 8 green, 15 yellow, 25 white. how many balls must we choose to ensure that we have 12 balls of same color

colors (n) = 5

~~knt~~ $k+1 = 12$ $k = 11$

$kn+1 = (11 \times 5) + 1 = 56.$

21) Permutation and Combinations

Permutations

how many ways, arrange, order matters

Q) In how many ways can we select 3 students from 5 to ~~stand~~ stand!

$5 \times 4 \times 3 = 60$ $(5P3) = 60.$

Q) In how many ways can we arrange 5 students to stand,

$5! = 120$ $5P5 = 120.$

Combinations:

chosing, order doesnt matter

Q) how many committees of 3 students can be formed from 4 students

$4C3 = 4$

$$\text{Position} = \frac{n!}{r!(n-r)!}$$

Foundation for Advancement of Science & Technology

22) Binomial Theorem

$(x+y)^n = {}^nC_r \times (x)^{n-r} (y)^r$

Q) $(x+y)^4$

$^4C_0 \quad (x)^4 (y)^0 = 1 \times x^4 \times 1 = x^4$

$^4C_1 \quad (x)^3 (y)^1 = 4 \times x^3 \times y = 4x^3y$

$^4C_2 \quad (x)^2 (y)^2 = 6 \times x^2 \times y^2 = 6x^2y^2$

$^4C_3 \quad (x)^1 (y)^3 = 4 \times x^1 \times y^3 = 4xy^3$

$^4C_4 \quad (x)^0 (y)^4 = 1 \times 1 \times y^4 = y^4$

$x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

23) Generalized Permutation and Combination

Chapter 9: Relations

24) Relations and Properties

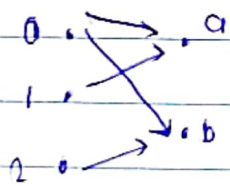
let A and B be sets. A binary relation A to B is subset of $A \times B$

Q) let A be students and B set of courses. let R be relation (a,b) where a is a student enrolled in course B.

Jason and Deborah enrolled in CS518 (Jason, CS518) and (Deborah, CS518)
Jason enrolled in an CS510 (Jason CS510)

$R = \{$ (Jason, CS518), (Deborah (CS518), (Jason, CS510)$\}$

Q) $A = \{0,1,2\}$ $B = \{a,b\}$ $R = \{(0,a),(0,b),(1,a),(2,b)\}$



R	a	b
0	X	X
1	X	
2		X

Relations on sets

Relation on set A is relation from A to A.

Q) $A = \{1,2,3,4\}$ $R = \{(a,b) \mid a \text{ divides } b\}$ $\frac{b}{a}$.

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

Properties

1) Reflexive relations = every element related to itself.

(a,a)

irreflexive = no (a,a)

Foundation for Advancement of Science & Technology

Q) Consider $A = \{1, 2, 3, 4\}$

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$

$R_2 = \{(1,1), (1,2), (2,1)\}$

$R_3 = \{(1,1), (1,2), (1,4), (2,1), (2,2), (3,3), (4,1), (4,4)\}$

$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$

$R_5 = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}$

$R_6 = \{(3,4)\}$

Reflexive (a,a) = R_3 and R_5

2) Symmetric both (a,b) and (b,a) for all elements.

from Qs symmetric? R_2 and R_3

3) antisymmetric if (a,b) then no (b,a) but self loop allowed.

from Qs antisymmetric? R_4, R_5, R_6

4) Transitive if $A \to B$ and $B \to C$ then $A \to C$ (should have all 3 pairs) for all pairs.

from Qs transitive? $(4,2)$ $(2,1)$ $(4,1)$

$(4,3)$ $(3,2)$ $(2,1)$ $(4,2)$

$(3,2), (2,1)$ $(3,1)$

$(4,3), (3,1)$

R_4, R_5, R_6

all empty, single are transitive

Foundation for Advancement of Science & Technology

→ most restricted

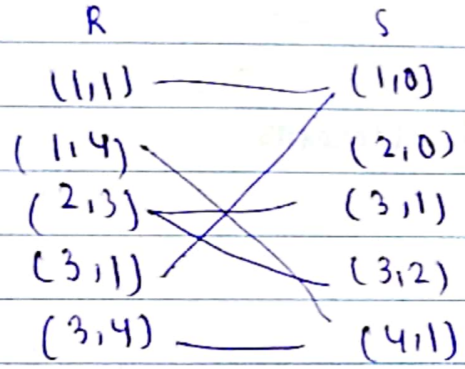
5) Assymetric if (a,b) then no (b,a) and no same.

~~every asymmetric is antisymmetric~~ R4, R6.

Composite Relations

Composition of R and S is represented by $S \circ R$.

$R = \{(1,1)(1,4)(2,3)(3,1)(3,4)\}$ $S = \{(1,0),(2,0)(3,1)(3,2)(4,1)\}$



(1,0), (1,1), (2,1), (3,0), (2,2), (3,1)

2S) Representing Relations

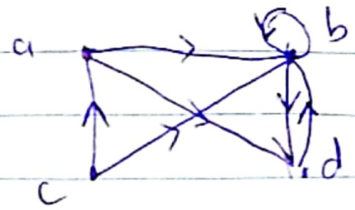
- Using matrices $A_R = [\ ]$ where there is pair in R, 0 when not

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

	1	2
1	0	0
2	1	0
3	1	1

- Using directed graphs.

a) (a,b) (a,d) (b,b) (b,d) (c,a) (c,b) (d,b)



Foundation for Advancement of Science & Technology

26) Equivalence Relation

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

Q) a) {(0,0)(1,1)(2,2)(3,3)

reflexive ✓, symmetric ✓ transitive ✓ → equivalence

b) {(0,0)(0,2)(2,0)(2,2)(2,3)(3,2)(3,3)

not reflexive, symmetric ✓ transitive ✓ → not equivalence

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

reflexive ✓, symmetric ✓, transitive → equivalence

27) Partial Orderings

a relation on set s is partialorder if it is reflexive, antisymmetric and transitive.

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

reflexive ✓ antisymmetric ✓ transitive ✓ → partial ordering

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

reflexive ✓ antisymmetric ✗ transitive ✓ → not partial order

no (3,0)

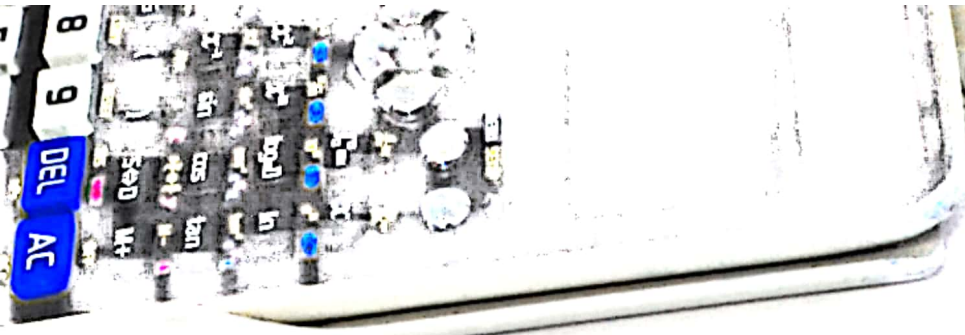
c) {(0,0)(1,1)(1,2)(2,2)(3,3) → partial order

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

(1,2)(2,2) → (1,2) (1,2)(2,3)(1,3) → partial order

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

not partial ordering



RSA Algorithm

1) select 2 prime numbers (p and q) given.
2) calculate $n = p \times q$
3) calculate $\phi n = (p-1) \times (q-1)$
4) choose 'e' such that it is relatively prime to ϕn and $1 < e < \phi n$.
5) calculate $de = 1 \bmod \phi n$
6) public key (e, n) private key (d, n)

encryption
7) convert alphabets in number
8) apply $C = m^e \bmod n$
   ↳ number in group of 4.

decryption
9) $P = C^d \bmod n$.

Foundation for Advancement of Science & Technology

Q) Encrypt STOP using RSA with Key (2537, 13). $2537 = 43 \times 59$

1) $p = 43 \quad q = 59$

2) $n = p \times q = 43 \times 59 = 2537$

3) $\Phi(n) = (43-1)(59-1) = 2436$

4) e (given) $= 13$.

5) $de = 1 \bmod (\Phi(n))$

$d \times 13 = 1 \bmod 2436$

$$d = \frac{1 + K\,\Phi(n)}{e} = \frac{1 + K(2436)}{13}$$

using trial and error to find.

$\frac{1+0(2436)}{13} = 0.07$ ✗

$\frac{1+1(2436)}{13} = 187.4$ ✗

$\frac{1+2(2436)}{13} = 374.8$ ✗

$\frac{1+3(2436)}{13} = 562.2$ ✗

$\frac{1+4(2436)}{13} = 749.6$ ✗

$\frac{1+5(2436)}{13} = 937$ ✓

$d = 937$

6) public key (13, 2537) private key (5, 2537)

7) S T O P = 18 19 14 15 → 1819 1415

$C = 1819^{13} \bmod 2537$

$C = 1415^{13} \bmod 2537$

Foundation for Advancement of Science & Technology

8) Decrypt 0981 0461 with p=43, q=59, e=13, (prev qs)

already calculated terms

n = 2537

$\phi(n)$ = 2436

e = 13

d = 937

~~$C = M^e \bmod n$~~ $P = C^d \bmod n$

$0981^{937} \bmod 2537 = 0704 = HE$

$0461^{937} \bmod 2537 = 1115 = LP$

HELP.

Foundation for Advancement of Science & Technology

Chapter 10 : Graphs

29) Graphs and Graph models

consists of v vertices/nodes and e edges

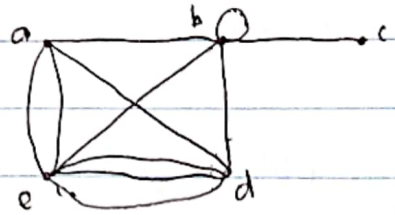
type	edges	multiple edges	loops allowed
simple graph	undirected	no	no
multigraph	undirected	yes	no
pseudograph	undirected	yes	yes
simple directed graph	directed	no	no
directed multigraph	directed	yes	yes
mixed graph	both	yes	yes

30) Graph terminology and special types of graphs

neighbours = when 2 vertices are connected by an edge

neighbourhood $N(v)$ = all vertices connected by edge to a particular vertex

degree = number of edges connecting to a vertex (2 for loop)



$\deg(a) = 4$ $\deg(b) = 6$ $\deg(c) = 1$

$\deg(d) = 5$ $\deg(e) = 6$

$N(a) = \{b, d, e\}$ $N(b) = \{a, b, c, d, e\}$ $N(c) = \{b\}$

$N(d) = \{a, b, e\}$ $N(e) = \{a, b, d\}$

Handshaking Theorem: $2m = \deg$ $(2e = \deg)$

(m = edges)

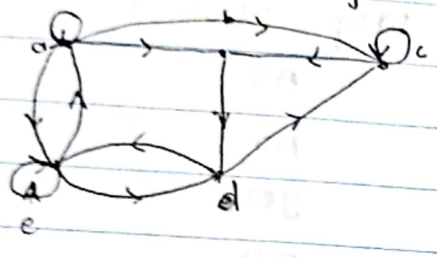
Q) how many edges of graph w/ 10 vertices and degree of 6?

$2m = 10 \times 6$

$m = 30$

- an undirected graph has even number of vertices of odd degree

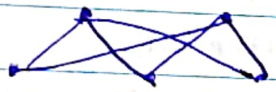
Indegree vertex ($\deg^-(v)$): edges coming in
outdegree vertex ($\deg^+(v)$): edges going out } loop is 1



$\deg^-(a) = 2$ $\deg^-(b) = 2$ $\deg^-(c) = 3$ $\deg^-(d) = 2$ $\deg^-(e) = 3$
$\deg^+(a) = 4$ $\deg^+(b) = 1$ $\deg^+(c) = 2$ $\deg^+(d) = 2$ $\deg^+(e) = 3$

Bipartite Graphs

when vertex set V is divided in 2 sets V_1 and V_2 and each edge in graph connects a vertex in V_1 and V_2 (but not V_1 and V_1 or V_2 and V_2)



New graphs from old

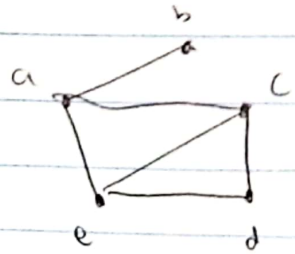
Subgraph where vertices and edges ≤ original graph's

3.1) Isomorphism

* for directed graph only where going

- adjacency list

the list of vertexes with an edge to that particular vertex.

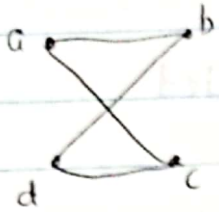


vertex	adjacency ~~list~~ vertices
a	b, c, e
b	a
c	a, d, e
d	c, e
e	a, c, d

Foundation for Advancement of Science & Technology

* in directed only where arrows

Adjacency matrix



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

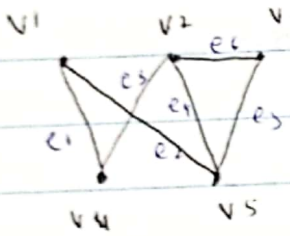
* write according to numbers

eg. if 2 from a → d then 2.

(b/w vertices)

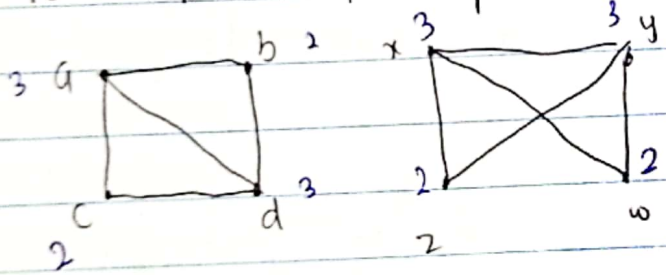
Incidence matrix

b/w vertices and edges



	e1	e2	e3	e4	e5	e6
v1	1	1	0	0	0	0
v2	0	0	1	1	0	1
v3	0	0	0	0	1	1
v4	1	0	1	0	0	0
v5	0	1	0	1	1	0

Isomorphism of Graphs



1) no. of vertex
2) no. of edges
3) degree sequence. (write descending order)
4) mapping of vertex (see how many vertices it is connected to and their degree)
5) validate mapping. (if edge b/w 2 vertex of graph a then should be in b

no of vertex = 4 = 4

edges = 5

abcd(ds): 3322 ✓

xyzw: 3322 ✓

edge ✓ a = x ✓
✓ b = z ✓
✓ c = w
d = y

x — a and b have edge, so does x and y

y — b and c dont have edge, z and w dont

z — c and d have edge, w and y have edge

w — a and c have edge, x and w have edge.

no repitition of edge.

3.2) Euler and Hamilton Paths

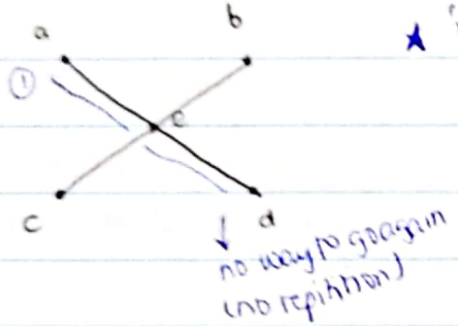
Euler Graph

* vertices can be repeated.

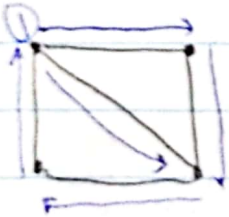
Check Euler path and Euler circuit

if both → Euler graph

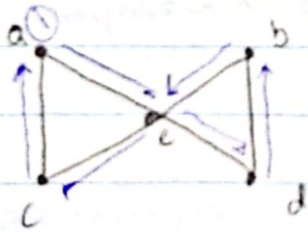
* cover all edges w/out repitition → Euler path
* cover all edges o w/ out repitition and reach starting point again → Euler Circuit



* if path doesnt exists then circuit cannot exist



Euler path
(but not reach at starting point)



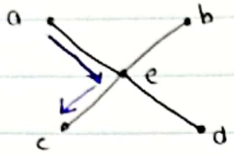
all edges covered
we reach back to a.
Euler circuit.

Foundation for Advancement of Science & Technology

Hamilton Graphs

* no repitition of vertex
* edges can be left out

cover all vertex ~~atleast~~ once → Hamilton path

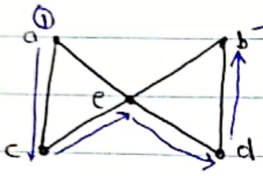


all vertex not covered.

not Hamilton path

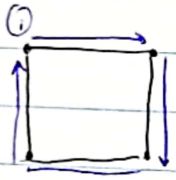
cover all vertex ~~atleast~~ once and reach starting point again → Hamilton circuit

Hamilton path + Hamilton circuit → Hamilton graph



→ all vertex covered here so Hamilton path exists.

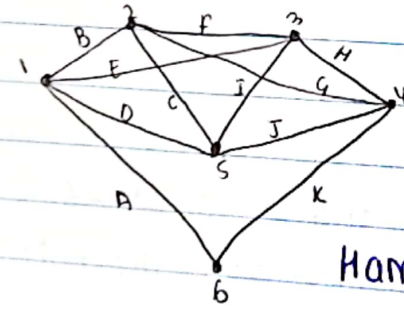
but no vertex left to go till a, so no Hamilton path.



reach starting point

so Hamilton path + circuit → Hamilton graph

Q)



Euler path: ~~E H J I F C~~ E H G F I C B D A K J

Euler Circuit: E H G F I C B D J K A – E

Hamilton : 1 2 5 3 4 6 – 1

so both Hamilton graph and Euler graph!

33) Planar Graphs

A graph is planar when it can be drawn w/out any edges crossing.

K_4 planar K_4

Euler's formula

$$r = e - v + 2$$

r → regions, e → edges, v → vertices

Q) 20 vertices, each of degree 3. how many regions?

$v = 20$

$2m = \deg.$

$2m = (3 \times 20)$

edges $= 30$.

$r = e - v + 2$

$r = 30 - 20 + 2 = 12$.

* if G is connected planar simple graph and $v \geq 3$ then $e \leq 3v - 6$
* If G is connected planar simple graph, then G has vertex of degree not exceeding 5.
* If connected planar simple graph w/ $v \geq 3$ and no circuits of length 3 then $e \leq 2v - 4$