Date: 03/01/2019

Chapter 1: Logic and Proofs [Mathematical Logic/Formal Logic]

Topic 1.1 Propositional Logic [Propositional Calculus]

A) Proposition

Definition:

1) Declarative sentence/statement, either true or false, but not both.

2) Assigned one of the two distinct values, True and False or T and F.

Examples:

1) The integer 20 is a prime.
2) Dhaka is the capital of Bangladesh.

Not examples:

1) What is your name?
2) Solve the problem.

B) Negation of a proposition

Definition:

1) Let p be a proposition.

2) Negation of p is denoted by $\neg p$ and read 'not p'

3) $\neg p$ is True if p is False, and $\neg p$ is False when p is True.

4) 'Not' ($\neg$) is a unary operator.

Examples:

p: '9 is divisible by 3'; $\neg p$: 'It is not the case that 9 is divisible by 3' or '9 is not divisible by 3'

Truth Table:

p	$\neg p$
F	T
T	F

p	$\neg p$	$\neg(\neg p)$
F	T	F
T	F	T

(*) $\neg(\neg p)$ is logically equivalent ($\equiv$) to p,

Scanned by CamScanner

c) Common prepositions involving common Binary Operators or connectives.

1) Conjunction

Definition

1) p, q — propositions.

2) conjunction of p and q is denoted by $p \wedge q$ and read 'p and q'.

3) Proposition which is True only when both p and q are True.

Examples:

1) p: 'The boy prepares his lessons regularly.'

2) q: 'The boy helps his parents everyday.'

3) $p \wedge q$: 'The boy prepares his lessons regularly and [/although / but] helps his parents everyday.'

Truth Table

p	q	p∧q
F	F	F
F	T	F
T	F	F
T	T	T

II) Disjunction

Definition

1) p, q – propositions.

2) Disjunction of p and q is denoted by p∨q and read 'p or q'.

3) Proposition which is False only when both p and q are False.

p	q	p∨q
F	F	F
F	T	T
T	F	T
T	T	T

Scanned by CamScanner

Examples:

1) p : 'You can take Physics this semester.'

2) q : 'You can take chemistry this semester.'

3) $p \vee q$: 'You can take Physics or chemistry [anyone or both of physics and chemistry] this semester.

III) Exclusive disjunction

Definition

1) p, q - propositions

2) Exclusive Disjunction of p and q is denoted by $p \oplus q$ and read 'p exclusive q'.

3) Proposition which is True only when exactly one of p and q is True.

Example

1) p: 'You can take tea'.

2) q: 'You can take coffee'.

3) $p \oplus q$: 'You can take tea or coffee.'

Truth Table

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

Home Work:

Prove using truth tables that $p \oplus q \equiv (p \vee q) \wedge \neg (p \wedge q)$

Date: 07/01/2019

Propositional Logic [Continued]

(D) Conditional Statements or Implications

Definition

1) p, q – propositions.

2) compound proposition, denoted by $p \to q$, and most commonly read 'p implies q', which is False only when p is True, but q is False.

Examples:

If you fall ill, then you miss the examination

p: ~~If~~ 'You fall ill',

q: 'You miss the examination.'

$p \to q$ [p implies q]

p – the antecedent or the premise of the conditional statement.

'implies' বামে True & ডানে False হলে False বাকিগুলো True .

q – the conclusion or the consequence of the conditional statement.

Other common expressions:

If p then q. q, whenever p

q, if p. q follows p

Truth Table

p	q	$p \to q$	$\neg p$	$\neg q$	$p \land \neg q$	$\neg(p \land \neg q)$	$\neg p \lor q$
F	F	T	T	T	F	T	T
F	T	T	T	F	F	T	T
T	F	F	F	T	T	F	F
T	T	T	F	F	F	T	T

Complete the table and be assured that

$p \to q \equiv \neg(p \land \neg q)$

and $p \to q \equiv \neg p \lor q$

If I am elected, then I do all the good things

E) Biconditional Statements or Bi-implications

[২টো T, F হলে T বাকি সব F]

Definition:

1) p, q - propositons.

2) compound propositon, denoted by $p \leftrightarrow q$, and most commonly read 'p if and only if q', which is True only when p and q have the same truth values.

Examples:

The angles of a triangle are equal to each other if and only if the triangle is equilateral

p: 'The angles of a triangle are equal to each other.'

q: 'The triangle is equilateral'.

$p \leftrightarrow q$ [p if and only q.

Other common Expressions:

p iff q

q, whenever p, and p, whenever q.

Truth Table

p	q	$p \leftrightarrow q$	$\neg p$	$\neg q$	$p \to q$	$q \to p$	$\neg p \vee q$	$\neg q \vee p$	$(p \to q) \wedge (q \to p)$	$(\neg p \vee q) \wedge (\neg q \vee p)$
F	F	T	T	T	T	T	T	T	T	T
F	T	F	T	F	T	F	T	F	F	F
T	F	F	F	T	F	T	F	T	F	F
T	T	T	F	F	T	T	T	T	T	T

Complete the table and be assured that

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

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

Date: 08/01/2019

F) Special Propositional Conventions

1) Converse, Inverse and Contrapositive of a Conditional Statement.

p	q	$p \to q$	$q \to p$	$\neg p$	$\neg q$	$\neg p \to \neg q$	$\neg q \to \neg p$
F	F	T	T	T	T	T	T
F	T	T	F	T	F	F	T
T	F	F	T	F	T	T	F
T	T	T	T	F	F	T	T

Complete the table and be assured:

1) Contrapositive is equivalent to the conditional ($\neg q \to \neg p \equiv p \to q$)

2) Converse ($q \to p$) is not

3) inverse ($\neg p \to \neg q$) is also not

But the converse and inverse of a conditional are equivalent to each other ($q \to p \equiv \neg p \to \neg q$).

Exercise on ['You are ill.' → 'You miss the examination']

Implication ($p \to q$): If you are ill, then you miss the examination.

Contrapositive ($\neg q \to \neg p$): If you don't miss the examination, then you are not ill.

Converse ($q \to p$): If you miss the examination then you are ill.

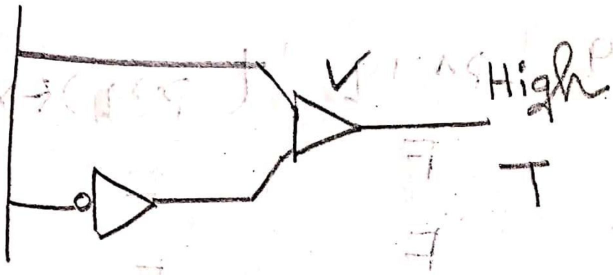
Inverse ($\neg p \to \neg q$): If you are not ill, then you will not miss the examination.

2) Tautology:

Compound proposition, the truth value of which is always True.

For proof: $p \vee \neg p$, $p \leftrightarrow \neg(\neg p)$, $\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$

p	$\neg p$	$p \vee \neg p$
F	T	T
T	F	T



p	$\neg p$	$\neg(\neg p)$	$p \leftrightarrow \neg(\neg p)$
F	T	F	F
T	F	T	F

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$	$\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg$
F	F	T	T	F	T	T	T
F	T	T	F	T	F	F	T
T	F	F	T	T	F	F	T
T	T	F	F	T	F	F	T

3) Contradiction

Compound proposition that is always False

$p \wedge \neg p$, $p \leftrightarrow \neg p$, $(p \to q) \leftrightarrow (p \wedge \neg q)$

p	q	$\neg q$	$p \to q$	$p \wedge \neg q$	$(p \to q) \leftrightarrow (p \wedge \neg q)$
F	F	T	T	F	F
F	T	F	T	F	F
T	F	T	F	T	F
T	T	F	T	F	F

p	$\neg p$	$p \wedge \neg p$
F	T	F
T	F	F

p	$\neg p$	$p \leftrightarrow \neg p$
F	T	F
T	F	F

4) Contingency

Neither tautology nor a contradiction.

5) Order of precedence of logical operators:

$\neg$; $\wedge$, $\vee$; $\rightarrow$, $\leftrightarrow$

6) p is logically equivalent to q if $p \leftrightarrow q$ is tautology.

Date: 10/01/2019

21

G) Common Propositional Equivalences
[Important Laws of propositional Logic]

1) Double negation law: $\neg(\neg p) \equiv p$

2) Idempotent laws: $p \wedge p \equiv p$, $p \vee p \equiv p$

3) Communicative laws $p \wedge q \equiv q \wedge p$, $p \vee q \equiv q \vee p$

4) Associative laws: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$, $(p \vee q) \vee r \equiv p \vee (q \vee r)$

5) Distributive laws $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

6) De Morgan's laws: $\neg(p \wedge q) \equiv \neg p \vee \neg q$, $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Negation of conjunction is proportional to the disjunction of negation.

7) Identity laws: $p \wedge T \equiv p$, $p \vee F \equiv p$

8) Domination laws: $p \wedge F \equiv F$, $p \vee T \equiv T$

9) Complement laws / Negation laws: $p \wedge \neg p \equiv F$; $p \vee \neg p \equiv T$

10) Absorption laws: $p \wedge (p \vee q) \equiv p$, $p \vee (p \wedge q) \equiv p$

Other useful propositional equivalences;

11) $p \rightarrow q \equiv \neg(p \wedge \neg q) \equiv \neg p \vee q$ [Ellimination of conditions]

12) $p \rightarrow q \equiv \neg q \rightarrow \neg p$ [Contrapositive]

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

14. $(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

15. $(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$

16. $(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

17. $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$ [Ellimination of Biconditionals]

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

19. $p \leftrightarrow q \equiv q \leftrightarrow p \equiv \neg p \leftrightarrow \neg q \equiv \neg q \leftrightarrow \neg p$

Exercise

1) Verify the above equivalences using truth tables.

$\leftrightarrow$ corresponding tautology

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

p	q	r	$p \vee q$	$p \vee r$	$q \wedge r$	$p \vee (q \wedge r)$	$(p \vee q) \wedge (p \vee r)$	
F	F	F	F	F	F	F	F	T
F	F	T	F	T	F	F	F	T
F	T	F	T	F	F	F	F	T
F	T	T	T	T	T	T	T	T
T	F	F	T	T	F	T	T	T
T	F	T	T	T	F	T	T	T
T	T	F	T	T	F	T	T	T
T	T	T	T	T	T	T	T	T

2) Verify using only propositional equivalences

i) $(p \land \neg q) \lor (q \land p) \equiv p$

ii) $\neg(\neg p \lor q) \land (\neg p \lor (q \land \neg p)) \equiv F$

iii) $(\neg p \land (\neg q \lor \neg p)) \lor p \equiv T$

iv) $(\neg p \lor \neg q) \land q \land \neg(\neg p) \equiv q \land ((\neg q \lor p) \land \neg q)$

v) $(q \land r) \lor \neg p \leftrightarrow (\neg p \lor q) \land (\neg p \lor r) \equiv T$

iv) L.H.S.

$= (\neg p \lor \neg q) \land q \land \neg(\neg p)$ [~~Double Negati~~

$= (\neg p \lor \neg q) \land q \land p$ [Double Negation]

$= \neg(p \land q) \land q \land p$ [De morgan]

$= \neg(p \land q) \land p \land q$ [Communicative law]

$= \neg(p \land q) \land (p \land q)$ [Association law]

$= \underbrace{\quad}_{x} \quad \underbrace{\quad}_{x}$ [Thinking $x = p \land q$

$= \neg x \land \neg x$

$=$ F [complement law]

Scanned by CamScanner

R.H.S. = $q \wedge ((\neg q \vee p) \wedge \neg q)$

$= q \wedge (\neg q \wedge (\neg q \vee p))$ [Commutative law]

$= (q \wedge \neg q) \wedge (\neg q \vee p)$ [Associative law]

$= F \wedge (\neg q \vee p)$ [complement law]

$= F$ [Dominative law]

LHS = RHS

Date: 14/01/2019

Predicate Logic / Predicate Calculus

A) Predicates

Definition

(1) declarative sentence or statement with one or more variables.

(2) turns into a proposition after assigning values to the variables.

(3) Set of possible values of variables: Universe of discourse (uod) or Domain.

(4) assigning values: binding the variables.

Examples: [Domain / uod: set of integers]

(1) $x-5>8$: $P_1(x)$, say; 1-place predicate;

$P_1(2)$ = False;

(2) ~~x+y~~ $x+y=4$; $P_2(x,y)$, say ; 2- place predicate ,

$P_2(1,3) =$ True

(3) $x+y=z$; $P_3(x,y,z)$, say ; 3- place predicate ;

$P_3(1,2,3) =$ True .

✓ $P_3(2,2,5)$ returns the value of propositional function P_3 at $(2,2,5)$, which is False

✓ Two possible outcome of a propositional function: True, False .

✓ Two possible predicates in the domain 'Set of all people' :

Father (x,y) : 'x is the father of y.'

Male (x) : "x is a male.'

B) Quantified Predicates :

1) When the values of the variable in a predicate are specified in some particular way, then the predicate is said to be quantified.

2) Fully quantified predicates are propositions.

3) Two quantifiers are widely used :

Universal Quantified.

Existential Quantified.

Universal Quantified.

1) Denoted by $\forall$, and read 'for all' / 'for each'

2) Examples : [Domain / uod : Set of integers]

$P_4(x) : x^2 \geq 0$

$\forall x \, P_4(x)$: True

$P_5(x) : x+2 > 10$

$\forall x \, P_5(x)$: False

3. $\forall x P(x) \equiv P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \dots$, when the elements of the UoD can be listed as $x_1, x_2, x_3 \dots$

4) A <u>counterexample</u> is <u>sufficient</u> to show 'falsehood' of a universally quantified predicate, that is, to disprove it.

Existential Quantified

1) Denoted by $\exists$, and read 'for some', meaning 'there is / exists at least one'.

$\exists x P_4(x) =$ True $\qquad \exists x P_5(x) =$ True

2) $\exists x P(x) \equiv P(x_1) \vee P(x_2) \vee P(x_3) \vee \dots$, when the elements of the UoD can be listed as $x_1, x_2, x_3, \dots$

3) To prove of or to show the 'truth' of an existentially quantified predicate <u>one example</u> is <u>sufficient</u>.

* Other quantifiers like 'There is exactly one' (uniqueness quinatifier), 'There is exactly two' etc are not commonly used.

Date: 15.01.2019

Predicate Logic

c) Negation of Quantified Predicates

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

$[\neg(P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \ldots] \equiv \neg P(x_1) \vee \neg P(x_2) \vee \neg P(x_3) \vee \ldots]$

Not for all x ~~seen~~ P(x) ~~is true~~ holds

≡ For some x P(x) doesn't hold.

2) $\neg \exists x\, P(x) = \forall x \neg P(x)$

$[\neg(P(x_1) \vee P(x_2) \vee P(x_3) \vee \ldots] \equiv \neg P(x_1) \wedge \neg P(x_2) \wedge \neg P(x_3) \wedge \ldots]$

Not for some x P(x) holds.

For all some x P(x) doesn't hold.

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

Not for all x P(x) doesn't hold.

For all x P(x) holds.

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

D) Expressing Natural Language Sentences with Quantified Predicates and Logical Connectives

[UoD : $\mathbb{Z}$]

1. There are some odd integers that are not primes.

$\exists x \, (Odd(x) \land \neg Prime(x))$

2. The only even prime is two

$\forall x ((Even(x) \land Prime(x)) \longrightarrow (x = 2))$

3. Not for all cases primes are odd.

$$\neg \forall x\,(Prime(x) \rightarrow odd(x)) \equiv \exists x \neg(Prime(x) \rightarrow odd(x))$$

$$\equiv$$

$$\exists x \neg(\neg Prime(x) \vee odd(x)) \equiv \exists x\,(Prime(x) \wedge \neg odd(x))$$

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

4. The sum of two negative numbers is always negative.

$$\forall x \forall y\,(((x<0) \wedge (y<0)) \rightarrow ((x+y)<0))$$

[UoD: All people]

5. Every guest gets at least one gift.

$$\forall x\,(Guest(x) \longrightarrow \exists y\,(Gift(y) \wedge Gets(x,y)))$$

( ) → scope of x, ( ) — scope of y, ∃ – nested, within the scope of x.

Scanned by CamScanner

6. If x is the father of y and y is the father of z, then x is the grandfather of z.

$$\forall x \forall y \forall z ((Father(x,y) \land Father(y,z)) \to Grandfather(x,z))$$

7. Nobody likes everybody.

$$\neg \exists x \forall y \, Likes(x,y) \equiv \forall x \neg \forall y \, likes(x,y) \equiv \forall x \exists y \neg likes(x,y)$$

Exercise from text book [Section 1.3, Domain: All people]

7. $C(x)$: 'x is a comedian', $F(x)$: 'x is funny'.

a) $\forall x (C(x) \to F(x))$: Every comedian is funny.

b) $\forall x (C(x) \land F(x))$: Everyone is a comedian, and is also funny.

c) $\exists x (C(x) \to F(x))$: Some people, if they are comedians, are funny.

d) $\exists x (C(x) \land F(x))$: Some people are ~~not~~ comedians, and are also funny.

Scanned by CamScanner

25. a) No one is perfect. $\neg \exists x \, Perfect(x) \equiv \forall x \neg Perfect(x)$

b) Not everyone is perfect $\neg \forall x \, Perfect(x) \equiv \exists x \neg Perfect(x)$

c) All your friends are perfect. $\forall x \, (YourFriend(x) \rightarrow Perfect(x))$

d) At least one of your friends is perfect

$$\exists x \, (YourFriend(x) \land Perfect(x))$$

e) Everyone is your friend and is perfect.

$$\forall x \, (YourFriend(x) \land Perfect(x))$$

f) Not everyone is your friend or someone is not perfect

$$\neg \forall x \, YourFriend(x) \lor \exists y \neg Perfect(y)$$

There are paradoxes:

Is the declaration 'I am a liar' a proposition

Date: 17.01.2019.

Topic 1.3 Proofs

A) Basic Concepts:

1) Theorem: Proposition that can be proved to be true

2) Proof: Argument, that is, sequence of propositions that demostrates the 'truth' of a theorem.

A proof may include:

i) Axioms or Postulates: Definitions / Primary assumptions / Facts known to be True apriori / Explicit facts;

ii) Theorems proved earlier;

iii) Hypotheses of the theorem, that is, propositions that are assumed to be true;

iv) Proposition inferred (derived) from given propositions.

* Inference or Reasoning: Process of constructing a proof using some rules.

* Lemma: Simple theorem used to prove complicated ones.

* Corollary: Proposition derived directly from a theorem.

* Conjecture: Proposition with unknown truth value.

Examples:

i) Goldbach's conjecture: Every even integer n, $n>2$, can be shown as the sum of two primes.

ii) Twin prime conjecture: There are infinitely many twin primes (pair of primes that differ by 2), like (3,5), (5,7), ...

B) Rules of Inference of Propositional Logic

1) $P_1, P_2, P_3 \dots P_n \vdash q$ is an inference rule iff $P_1 \wedge P_2 \wedge P_3 \wedge \dots \wedge P_n \rightarrow q$ is a tautology [$\vdash$: infer / proves / derives]

Common Inference rules:

1) Addition : $p \vdash p \vee q$
2) Simplification : $p \wedge q \vdash p$.
3) Conjuction : $p, q \vdash p \wedge q$
4) Modus pones : $p, p \rightarrow q \vdash q$
5) Modus tollens : $\neg q, p \rightarrow q \vdash \neg p$
6) Hypothetical syllogism : $p \rightarrow q, q \rightarrow r \vdash p \rightarrow r$
7) Disjunctive syllogism : $p \vee q, \neg p \vdash q$;

   $p \vee q, \neg q \vdash p$
8) Resolutin : $p \vee q, \neg p \vee r \vdash q \vee r$.

Scanned by CamScanner

Exercise:

1) Prove the tautologies corresponding to the rules of inference described.

i) $p, p \to q \vdash q$

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

p	q	$p \to q$	$p \wedge (p \to q)$	$(p \wedge (p \to q)) \to q$
F	F	T	F	T
F	T	T	F	T
T	F	F	F	T
T	T	T	T	T

2) Derive a fact (proposition) from a given knowledgebase ~~(KB)~~ (KB, set of facts):

i) r from $\{p \to s, q \vee p, s \to r, \neg q\}$;

ii) q from $\{q \leftrightarrow p, p\}$

iii) $p \wedge t$ from $\{r \wedge p, s \vee t, t \to \neg s\}$;

iv) $s \vee u$ from $\{p \to q, t \wedge \neg r, q \to r, p \vee s\}$

i) KB:

To be derived: r

1. $p \to s$
2. $q \vee p$
3. $s \to r$
4. $\neg q$

From 1, 3:

5. $p \to r$ [Hypothetical syllogism]

From 2, 4:

6. p [Disjunctive syllogism]

From 6 & 5:

7. r [Modus pones]

[Derived]

Scanned by CamScanner

Date: 21/01/2019.

A) Basic concepts

* Fallacy: Invalid (incorrect) reasoning, commonly due to improper use of implication.

c) Inferance Rules Involving Quantified Predicates

1. Universal Instantiation

$\forall x P(x) \vdash P(s)$, where s is any specified element of the domain

['Everyone dies' ⊢ 'Karim dies']

2. Universal Generalization

$P(a) \vdash \forall x P(x)$, where a is an arbitrary element of the domain.

['A girl student gets special stipend' ⊢ 'Every girl student gets special stipend.']

Scanned by CamScanner

3. Existential Instantiation

$\exists x\, P(x) \vdash P(c)$, where c is a certain specified element of the domain.

[' Some mammals can fly.' ⊢ ' The bat is a mammal that can fly.']

(4) Existential Generalization

$P(c) \vdash \exists x\, P(x)$, where c is a certain specified element of the domain.

[' The whale is a mammal that lives in water.
⊢ ' Some mammals live in water.']

Scanned by CamScanner

$p \to q \equiv \neg q \to \neg p$

$\neg P(s)$

D) Most Common Combination of inference Rules of Propositional and Predicate Logic

i) Universal Modus Pones

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

$P(s)$, where s is any specified element of the domain.

$\therefore Q(s)$

ii) Universal Modus tollens

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

$\neg Q(s)$, where s is any specified element of the domain.

$\therefore \neg P(s)$

An illustrative example

'Every CSE student takes CSE 1203. Karim is a CSE student.'

Prove: 'Karim takes CSE 1203.'

$\forall$ (CSE . Student(x) $\rightarrow$ Takes(x, CSE 1203))

CSE - Student (karim)

$\therefore$ Takes (karim, CSE 1203)

$\neg$(Rahim, CSE 1203)

$\therefore$ $\neg$ CSE Student (Rahim)

E) Important Deductive Methods of Proving Theorems

Domain: $\mathbb{Z}$; $n, k \in \mathbb{Z}$

1. Direct Proof

- To prove that $p \rightarrow q$ is True, assume that p is True, and then show that q is True.

Example:

If $\underbrace{n \text{ is even}}_{p}$ then $\underbrace{n^2 \text{ is even}}_{q}$. $[p \to q]$

Say p is True, that is, $n = 2k$

Then $n^2 = (2k)^2 = 4k^2 = 2 \cdot 2k^2$

That is, n^2 is even.

q is True.

2. Indirect or Contrapositive Proof

To prove that $p \to q$ is True, assume that $\neg q$ is True, and then show that $\neg p$ is True.

Example:

If $\underbrace{(3n+2) \text{ is odd}}_{p}$ then $\underbrace{n \text{ is odd}}_{q}$. $[p \to q]$

Say $\neg q$ is True.

that is, n is even

$n = 2k$

Then $3n+2 = 3(2k) + 2 = 6k + 2 = 2(3k+1)$, even

That is $\neg p$ is True.

Date: 22/01/2019

3. Proof by Contradiction.

1) To prove that p is ~~tru~~ True, assume that $\neg p$ is True, and then derive an absurdity / contradiction

- Example: $2n+1$ is odd [p]

suppose p is false that is, $(2n+1)$ is ~~true~~ even.

Then $2n+1 = 2k$, for $n, k \in \mathbb{Z}$

$\Rightarrow k = n + \frac{1}{2}$

That is ~~k do~~ $k \notin \mathbb{Z}$

So we get $(k \in \mathbb{Z}) \wedge (k \notin \mathbb{Z})$, which is a contradiction.

Scanned by CamScanner

\# $p \to q$ } Prove
$\neg p \lor q$ }

4. Counter Example method for universally quantified predicates.

Example: Proposed: 'Every bird can fly.'

Countered: 'An ostrich, although is a bird, can't fly.'

$\forall x\,(\mathrm{Bird}(x) \to \mathrm{canFly}(x))$

$\mathrm{Bird}(\mathrm{Ostrich}) \land \neg \mathrm{CanFly}(\mathrm{Ostrich})$ ✓

$\neg \forall x\,(B(x) \to CF(x))$

$= \exists x\, \neg (B(x) \to CF(x))$

$= \exists x\, \neg (\neg B(x) \lor CF(x))$

$= \exists x\, (B(x) \land \neg CF(x))$ ✓

5. One Example Method for an Existentially Quantified Predicate

Example: Proposed: 'Some mammals can fly.'

Cited: 'A bat is a mammal and it can fly.'

$\exists x\ (\text{Mammal}(x) \wedge \text{CanFly}(x))$

$\text{Mammal}(\text{Bat}) \wedge \text{CanFly}(\text{Bat})$

6. Proving logical Equivalences, tautologies and Contradiction using truth tables.

7. Simplication using laws of logical equivalences.

8. Deriving from a knowledgebase using inference rules.

F) Non Deductive Proof Techniques

[Example based]

Mathematical Induction

Example : $1+2+3+ \_\_\_ . +n = (n+1)/2$

- Let $P(n)$ denote $1+2+3+4+\ldots+n = n(n+1)/2$

$1+2+3+4+5$
$5+4+3+2+1$

$6+6+6+6+6$

$6 \times 5 = 30$

$30/2 = 15$

$$\frac{(1+5) \times 5}{2}$$

• Idea: $P(1) = \text{True}$, $P(2) = \text{True}$, ..., So, $P(n) = \text{True}$

$P(1): 1 = 1(1+1)/2$

$P(2): 1+2 = 2(2+1)/2$

Formal inductive proof in three steps.

1) Basis: $P(1)$ holds; Proved True.

2) Hypothesis: Say $P(k) = \text{True}$, for $k \geq 1$

$P(k): 1+2+3+ \cdots + k = k(k+1)/2$

3) Induction Step:

If $P(k) = \text{True}$, then $P(k+1) = \text{True}$, that is,

$P(k) \rightarrow P(k+1)$

Proof of the steps

$P(k+1)$: $1+2+3+\dots+(k+1) = (k+1)(k+2)/2$

$L.H.S = 1+2+3+\dots+(k+1)$

$= 1+2+3+\dots+k+(k+1)$

$= k(k+1)/2 + (k+1)$ [According to hypothesis].

$= \dfrac{k(k+1)+2(k+1)}{2}$

$= \dfrac{(k+1)(k+2)}{2}$

$= R.H.S$.

[We have $P(1)$, $P(k) \rightarrow P(k+1)$ shown True; So, we can take $P(1+1)$ = True, $P(2+1)$ = True ...]

Empirical Induction

Show that, 'About 90% of the Bangladesh population takes interest in politics.'

We can take help of statistical data analysis to prove or disprove it, Analogy

[Induction based on similarity among examples]

Prove that 'Electric current flow at a junction can be computed with the help of water flow at a crossing of water channels.'

** Nondeductive, especially empirical and analogical procedures are not always very accurate, but very useful and common in natural world.

Date: 27/01/2019

Chap: 2
Set Theory

Basic concepts

A) Sets and set notations

Sets
- Unordered collection of objects (distinct objects, if not said otherwise);
- Those objects are elements or members of the set;
- A set is said to contain its elements;
- An object either belongs to ($\in$) or does not belong to ($\notin$) the set;

- Assumed, $S \notin S$, although a set may contain other sets.
- Russell's paradox: $S = \{x \mid x \notin x\}$ does not exist.

Set notations to describe sets
Listing: $S_1 = \{1, 2, 3, 4, \ldots, 9\}$
Set-builder: $S_1 = \{x \mid x$ is a positive integer and $x < 10\}$

Important sets of numbers:

i) $N = \{0, 1, 2, 3 \ldots\}$ – Natural number set

ii) $Z = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ – set of integers.

iii) $Q = \{p/q \mid p, q \in Z \wedge q \neq 0\}$ – set of ~~Rotational~~ Rational numbers.

iv) $[N, Z, Z^+, Q, Q^+, R, R^+]$

v) $Z^+ = \{1, 2, 3 \ldots\}$; R– set of real numbers.

B) Important concepts related to sets

a) Set relations: Subset, $\subseteq$, $A \subseteq A$, Proper subset, $\subset$, Superset, $N \subset Z \subset Q \subset R$, $A \subset B$ if $\forall x (x \in A \rightarrow x \in B)$ $\wedge \exists y (y \in B \wedge y \notin A)$.

Equal sets (if $A \subseteq B \wedge B \subseteq A$).

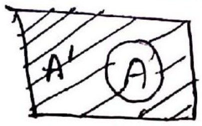
$A = \{5, 7, 9\}$

$B = \{1, 5, 7, 8, 9, 10\}$

$A \subset B$

b) Empty set: $\{\}$, $\emptyset$, $\{x \mid x \in Z \wedge x < 3 \wedge x > 10\}$;

$\{\emptyset\}$, $\{\{\}\}$, $\{a\}$ or $\{\{a, b\}\}$ –



singleto, not empty; $\phi \subseteq A$, for any set A.

c) Universal set : A universal set (U).

d) complement of a set, A', $\{x \mid x \in U \wedge x \notin A\}$,

$\{A'\}' = A$, $\phi' = U$, $\phi = U'$.

e) Finite and infinite sets: Finite sets, Cardinal numbers, $|A|$, Infinite sets may only be compared to each other, may be countable or uncountable

$N \subset Z$:

$N = \{0, 1, 2, 3, 4 \ldots\}$

$Z = \{0, 1, -1, 2, -2 \ldots\}$

R

$S = \{x \mid x \in R \wedge x \in [2.00001, 2.00002]\}$

f) Power set: $P(A)$, $|P(A)| = 2^n$, where $|A| = n$

$P\{\phi\} = \{\phi\}$, $P\{\{\phi\}\} = \{\phi, \{\phi\}\}$, Counting $P(A)$ using

Scanned by CamScanner

bit strings, $P(N)$ or $P(Z)$ is uncountable.

$A = \{a, b, c\}$

$|A| = 3$

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

000 100 010 001

$N = \{0, 1, 2, 3 \ldots\}$

$\phi(N) = \{ \phi$

$\{\{\phi\}, \{1\}, \{2\} \ldots$

$\{0, 1\}, \{0, 2\}, \{0, 3\}, \ldots \{1, 2\} \ldots \{1, 3\} \ldots$

$\{0, 1, 2\}, \{0, 1, 3\} \ldots$

N

g) cartesian product: ordered pairs / n-tuples,

$\times$, $A \times \phi = \phi$, $A \times B \neq B \times A$, except for special cases like ϕ and $A = B$.

$\Sigma\sigma A(T_5^{1} - T^{1})$

$A = \{a, b\}$

$B = \{x, y\}$

$A \times B = \{(a, x), (a, y), (b, x), (b, y)\}$

$|A \times B| = |A| \times |B|$ when $A \neq B$, $A \times B \times C$ – A, B cities and C–airlines providing service, $A_1 \times A_2 \times A_3 \times \cdots A_n$ – contains ordered n–tuples.

Date: 29/01/2019

h) Concatenation of sets: $AB = \{ab \mid a \in A \text{ and } b \in B\}$, $A\phi = \phi = \phi A$, $AB \neq BA$ except for special cases like ϕ and $A = B$.

Topic 2.2 Set Operations

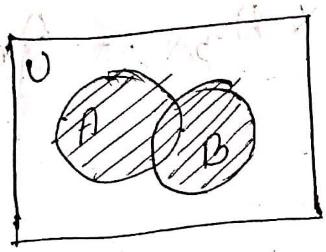
1) Set Union

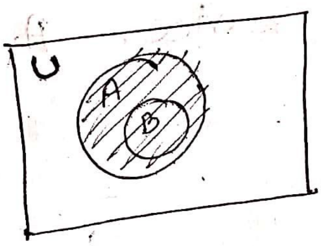
$\cup$, $A \cup B = \{x \mid x \in A \vee x \in B\}$, membership table, Venn diagrams, $A \cup B = B \cup A$, $A \cup \phi = \phi \cup A = A$, $A \cup U = U \cup A = U$, $A \cup A' = U$, $A \cup A = A$

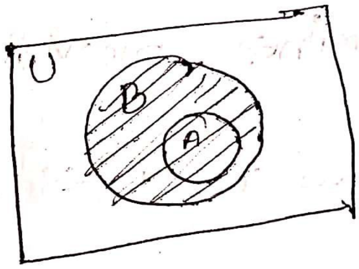
A	B	~~A∩B~~ A∪B
0	0	0
0	1	1
1	0	1
1	1	1

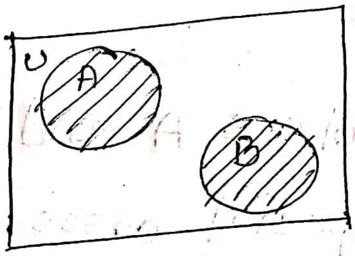
0 = does not belong to

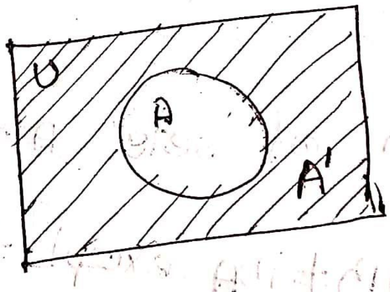
1 = belongs to







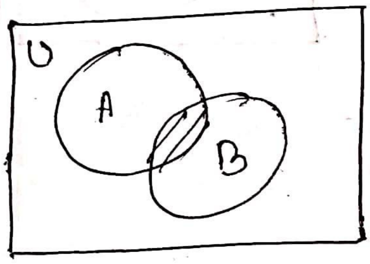


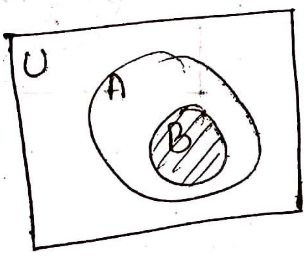


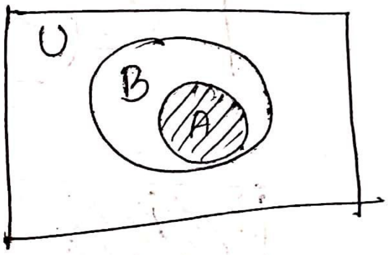
2) Set Interesection

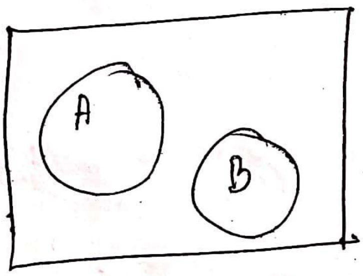
$\cap$, $A \cap B = \{x \mid x \in A \wedge x \in B\}$, membership table, Venn diagrams, $A \cap B = B \cap A$, $A \cap \phi = \phi \cap A = \phi$, $A \cap U = U \cap A = A$, $A \cap A' = \phi$, $A \cap A = A$, disjoint sets: $A \cap B = \phi$, $|A \cup B| = |A| + |B| - |A \cap B|$

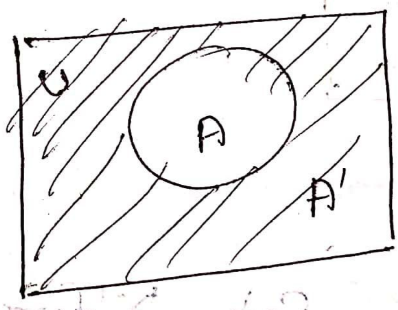
A	B	A∩B
0	0	0
0	1	0
1	0	0
1	1	1







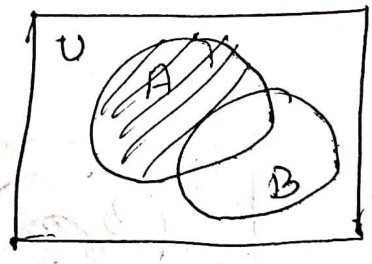


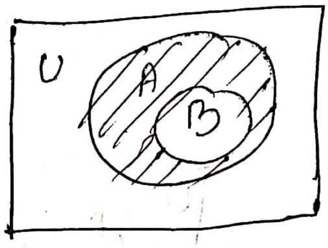


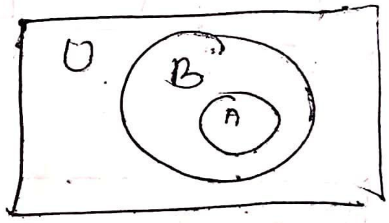
3) Set Difference

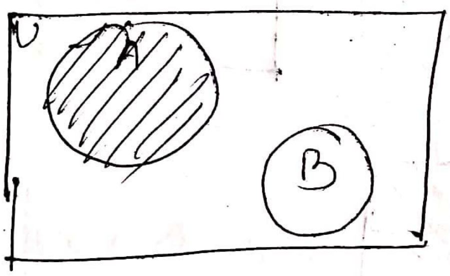
→ Not a basic operation, $A - B = \{x \mid x \in A \wedge x \in B\}$ $= A \cap B'$, membership table, Venn diagrams, $A - B \neq B - A$ except for special cases like ϕ and $A = B$; $A - \phi = A$, $\phi - A = \phi$, $A - U = \phi$, $U - A = A'$, $A - A' = A$, $A - A = \phi$

A	B	A-B
0	0	0
0	1	0
1	0	1
1	1	0





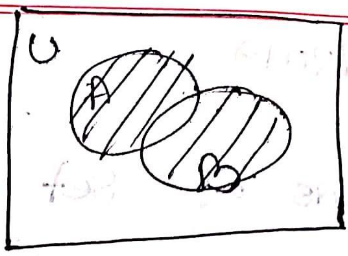


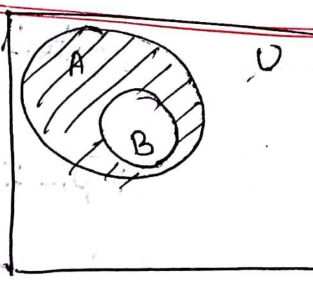


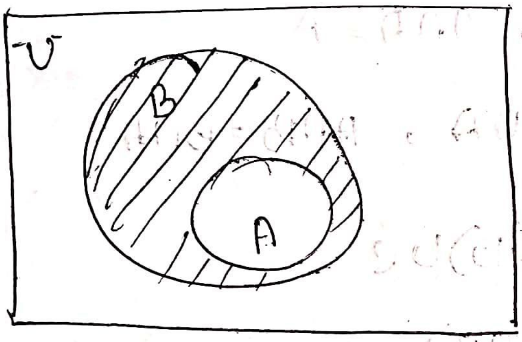
4) Symmetric Set Difference

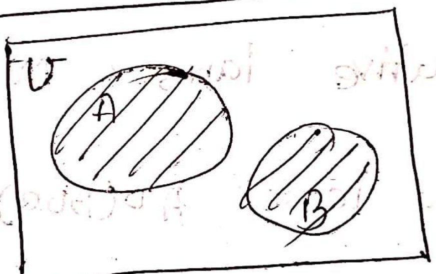
⊕, Not a basic operation, $A \oplus B = \{x \mid x \in A \vee$
(exclusive) $x \in B\} = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$
$= (A \cup B) \cap (A \cap B)' = (A \cup B) \cap (A' \cup B')$, membership
table, Venn diagrams, $A \oplus B = B \oplus A$, $A \oplus \phi = \phi \oplus A = A$,
$A \oplus U = U \oplus A = A'$, $A \oplus A' = U$, $A \oplus A = \phi$

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0









Generalized union and intersection

① $A_1 \cup A_2 \cup A_3 \cup \ldots A_n = \bigcup_{i=1}^{n} A_i$, Contains distinct elements of all A_i

② $A_1 \cap A_2 \cap A_3 \cap A_n$

Scanned by CamScanner

Date: 31/01/2019

Topic 2.3. Laws of Set Operations [Set Identities]

Say A, B and C are subsets of a specific U.

1. Complementation law: $(A')' = A$

2. Idempotent laws: $A \cup A = A$, $A \cap A = A$

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

4. Associative laws: $A \cup (B \cup C) = (A \cup B) \cup C$

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

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

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

6. De Morgan's laws: $(A \cup B)' = A' \cap B'$, $(A \cap B)' = A' \cup B'$

7. Identity laws: $A \cup \phi = A$; $A \cap U = A$

8. Domination laws: $A \cup U = U$, $A \cap \phi = \phi$

9. Complement laws: $A \cup A' = U$, $A \cap A' = \phi$

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

Scanned by CamScanner

Identities are used to simplify and transform expressions, and also to show equivalence of expressions involving set operations.

Exercise

- Verify the laws using membership tables:

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

A	B	$A \cap B$	$A \cup (A \cap B)$
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	1

- Prove the following equalities using only definitions and set identities.

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

(ii) $(A \cap A) \cup (B \cap (B' \cup A))' = U$

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

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

(v) $((A \cup B) \cap A')' \cup B = U$

(vi) $A' \cap (A \oplus B) = A' \cap B$

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

$L.H.S = (A \oplus B) \cup (A \cap B)$

$= ((A \cup B) - (A \cap B)) \cup (A \cap B)$ [Defination]

$= ((A \cup B) \cap (A \cap B)') \cup (A \cap B)$ [Definition]

$= ((A \cup B) \cap (A' \cup B')) \cup (A \cap B)$ [De Morgan's law]

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

[Distributive law]

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

[Distributive law]

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

[Complement law]

$= ((B \cap A') \cup (A \cap B')) \cup (A \cap B)$ [Identity law]

$= (B \cap A') \cup ((A \cap B') \cup (A \cap B))$ [Associative law]

$= (B \cap A') \cup (A \cap B' \cup B))$ [Distributive lab]

$= (B \cap A') \cup (A \cap U)$ [Complement law]

$= (B \cap A') \cup (A \cap U)$ [Identity law]

$= (B \cap A) \cup A \cap (A' \cup A)$ [Distributive law]

$= (B \cup A) \cap U$ [Complement]

$= B \cup A$ [Identity law]

$= A \cup B)$ [Complement law]

$=$ RHS.

Date 04/02/2019

Chapter 3. Relations and Functions

Topic 3.1 Relations

A) Basic concepts

(i) A Binary Relation or Relation, R from a set A to set B is a subset of A×B

Example

$A_1 = \{1, 2, 3, 5\}$, $B_1 = \{4, 6, 9, 15\}$

$R_1 = \{(a,b) \mid a \in A_1 \wedge b \in B_1 \wedge$ 'a is the square root of b'$\}$

$= \{(2,4), (3,9)\}$

R_1 stands for 'is the square root of'.

$R_1 \subseteq A_1 \times B_1$

We write, $2 R_1 4$ and $3 R_1 9$.

(ii) R from A to B may also be ϕ & equal to $A \times B$ (Empty relation & Universal relation).

(iii) Relation R on a set A is a subset of $A \times A$.

Example 1. R_2 standing for 'is greater than', defined on N as follows:

$$R_2 = \{(x,y) \mid x,y \in N \wedge x > y\}$$

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

$1 R_2 0$ $3 R_2 0$ $2 R_2 1$ $4 R_2 1$

Example 2.

R_3: 'is a brother of' on the set of all people

(iv) n-ary ~~recall~~ relation, R on sets $A_1, A_2, A_3, \ldots, A_n$:

$R \subseteq A_1 \times A_2 \times A_3 \ldots \times A_n$

Examples:

Ternary (3-ary), R_4 on $A = \{1, 2, 3, \ldots, 12\}$, defined as follows:

$$R_4 = \{(x,y,z) \mid x,y,z \in A \wedge x^2 + 5y = z\} = \{(1,1,6), (1,2,11), (2,1,9)\}$$

Karim R_3 Rahim

Ternary $R_5 = \{$(Karim, CSE, 1^{st} year), (Rahim, EE, 2^{nd} year) ...... $\}$

[Database application].

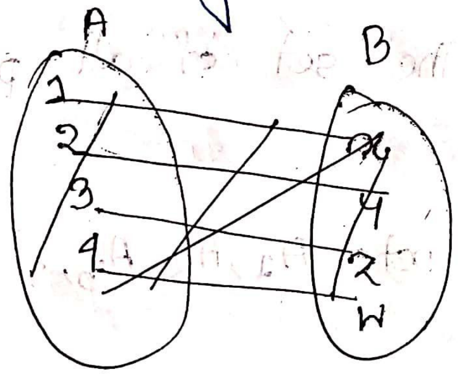
B) Representation of binary relations.

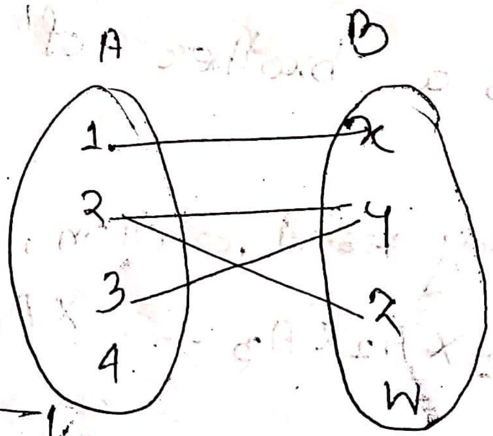
Set representation

Example: $A = \{1, 2, 3, 4\}$, $B = \{x, y, z, w\}$,

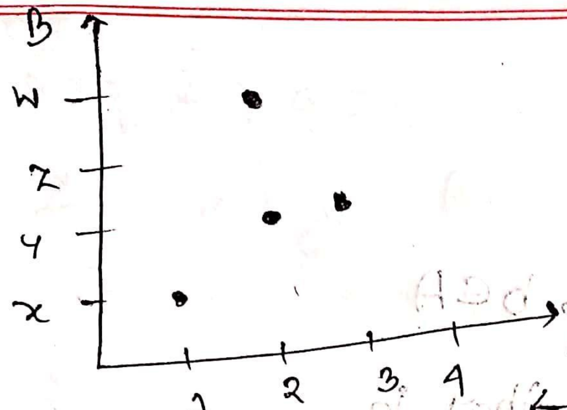
$R = \{(1, x), (2, y), (2, w), (3, y)\}$

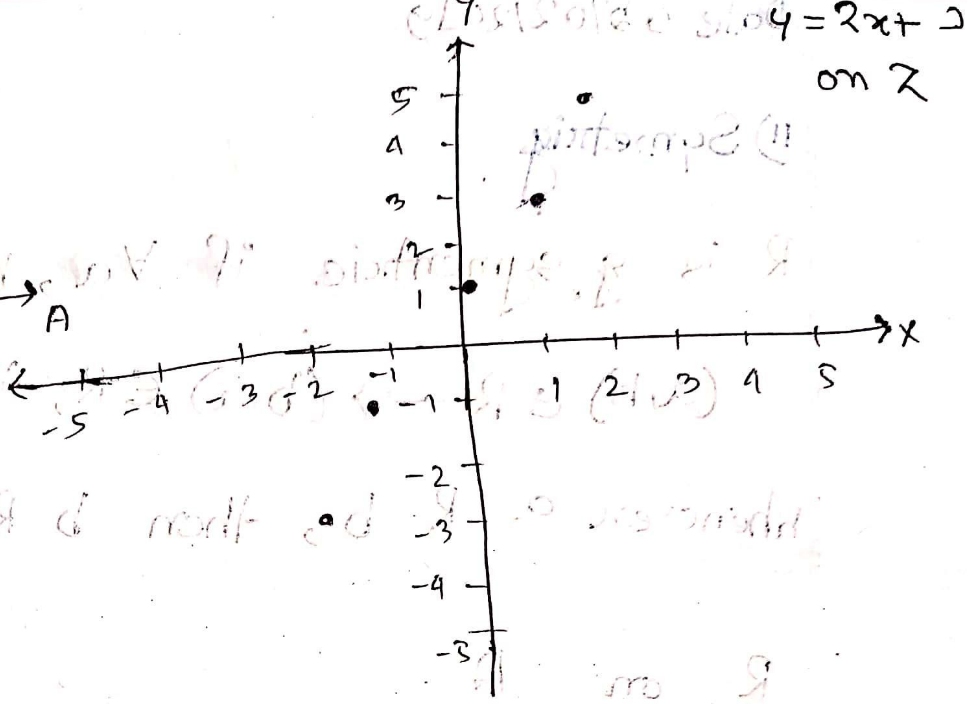
Arrow diagrams





	x	y	z	w
1	1	0	0	0
2	0	1	0	~~0~~ 1
3	0	1	0	0
4	0	0	0	0





B) ~~Representatio~~

2) Tabular / Matrix

3) Coordinate / Graph representation.

c) Important properties of Binary relations.

Say, R is a binary relation on a set A, that is $R \subseteq A \times A$

1) Reflexivity

i) R is a reflexive if $\forall a \in A$,

aRa, that is, $(a,a) \in R$

Examples:

Reflexive: $\leq, \geq, =$ on Z; $\subseteq$ on $P(Z)$

Not Reflexive: $<, >$ on Z; $\subset$ on $P(Z)$

Date 05/02/2019

11) Symetric

R is a symmetric if $\forall a, b \in A$

$(a,b) \in R \rightarrow (b,a) \in R$, that is,

whenever $a \, R \, b$, then $b \, R \, a$.

R on A

$R \subseteq A \times A$

Examples: = in general algebra; ≡ in propositional calclus; 'is a brother of' on the set of all male humans.

Not examples: 'is a brother of' on the set of all humans; $\leq$, $<$ on $\mathbb{Z}$.

=, $\mathbb{R}$

$a = b \longrightarrow b = a^2$

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

Z $5 \leq 10$

$10 \leq 5$ × not symmetric

iii) Antisymmetry

R is antisymmetric if for every distinct $a, b \in A$

$(a,b) \in R \rightarrow (b,a) \notin R$, that is,

whenever $a R b$, then $b \not R a$.

Examples $<, \leq$ on $\mathbb{Z}$; $\subset, \subseteq$ on $P(X)$

Not examples: "is a brother of" on the set of all humans.

Not symmetric is not necessarily antisymmetric

$5 < 9 \longrightarrow 9 \nless 5$

$\{1,3\} \subseteq \{-5,1,3,4\}$

$\{-5,1,3,4\} \subseteq \{1,3\} \longrightarrow$ False

Scanned by CamScanner

iv) Transitivity

R is Transitive if $\forall a, b, c \in A$

$((a,b) \in R \wedge (b,c) \in R) \rightarrow (a,c) \in R$, that is,

Whenever $(a R b)$ and $(b R c)$, then $a R c$.

R on A

$R \subseteq A \times A$

Examples:

$\leq, <$ on $\mathbb{Z}$; $\subset, \subseteq$ on $P(\mathbb{Z})$,

'is a brother of' on the set of all male humans

Not example: 'is the mother of' on the set of all humans.

$5 \leq 10 \wedge 10 \leq 25$

$5 \leq 25$

$\{2,5\} \subset \{1,2,5\}$

$\{1,2,5\} \subset \{-3,1,2,5\}$

$\{2,5\} \subset \{-3,1,2,5\}$

Other properties that are commonly used:
Irreflexive, Asymmetric, Both symmetric and antisymmetric.

Topic 3.1 Relations (Continued)

D) Equivalence Relations and classes

A binary relation R on set A is said to be an equivalence relation if R is reflexive, symmetric and transitive.

Examples:

$=$ in general algebra; $\equiv$ in propositional calculus;
$\equiv_m$ on N for $m \in Z^+$ (congruence modulo m on N for any positive integer m)

[$x \equiv_m y$ reads x 'congruent modulo m' y, which means x and y leave the same remainder after integer division by m, Application: Hashing function]

R on A

$R \subseteq A \times A$

$=$ on $\mathbb{R}$

$a = a$ Reflexive

$a = b \rightarrow b = a$ Symmetric

$\begin{matrix} a = b \\ b = c \end{matrix} \Big| \; a = c$ Transitive

---

$\equiv$ selfstudy.

$p \equiv p$

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

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

N

$\equiv_3$.

$9 \equiv_3 9$ Reflexive

$9 \equiv_3 24$, $24 \equiv_3 9$ Symmetric

$(8 \equiv_3 17) \wedge (17 \equiv_3 32) \rightarrow (8 \equiv_3 32)$

Transitive

Verify $\equiv_3$ on $\mathbf{N}$ for reflexivity, symmetry and transitivity

R on $\mathbf{R}$ such that $(a, b) \in R \longleftrightarrow (a-b) \in \mathbf{Z}$

a	b	a-b
1.2	1.2	0
3.1	-3.9	7

-3.9	3.1	-7
-3.9	5.1	-9

1.2 R 1.2 Reflexive

$\left.\begin{array}{l} 3.1 \; R \; -3.9 \\ -3.9 \; R \; 3.1 \end{array}\right\}$ Symmetric

-3.9 R 3.1

-3.9	-1.9	-2
3.1	5.1	-2

3.1 R 5.1

So Transitive

R on

Date: 07/01/2019

R on the set of English words such that $(x,y) \in R \longleftrightarrow |x| = |y|$, meaning x and y are of equal length.

x		y	
Men a	R	Men a	→ Reflexive
Men a	R	hen b	⇒ Symmetric
hen b	R	Men a	
Self a	R	help b	⇒ Transitive
help b	R	Best c	
Self a	R	best c	

$S = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$,

$L = \{1, 10, 100, 1000, 10000, 100000, \ldots\}$

I_L on such that

$x \, I_L \, y$ iff $\forall z \in S$,

$xz \in L \longrightarrow yz \in L$, and

$xz \notin L \rightarrow yz \notin L$

$\Sigma = \{0, 1\}$ — alphabet

~~$S = \{\epsilon, 0$~~ Empty String

$S = \{\epsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\} = \Sigma^*$

$|\epsilon| = 0$

$L = \{1, 10, 100, 1000, 10000, 100000, \ldots\}$

$= L(10^*)$ - regular language

I_L on S

R

R

x	I_L	y
10		1000
		10000
10		10000
100		
$101 \notin L$		1

$z = \epsilon$

$z = 0$

$z = 1$

$10 \; I_L \; 10 \longrightarrow$ Reflexive

$10_a \; I_L \; \cancel{1}0_a$

$10_a \; I_L \; 1000_b$

$1000_b \; I_L \; 10_a$ Symmetric

$10_a \; J_L \; 1000_b$
$1000_b \; J_L \; 10000000_c$ } Transitive
$10_a \; J_L \; 10000000_a$

Equivalence Classes.

i) An equivalence relation R, on a set, A partitions A into equivalence classes.

Example:

$\equiv_3$ on N

Partition: $\{\{0,3,6,9,12,\ldots\},\{1,4,7,10\ldots\},$
$\{2,5,8,11,\ldots\}\}$

classes: $C_1=\{0,3,6,9,12\ldots\}$, $C_2=\{1,4,7,10,\ldots\}$,
$C_3=\{2,5,8,11,\ldots\}$

$9\equiv_3 3$

ii) If R is an equivalence relation on A, then there are $A_1, A_2, A_3\ldots$ such that

$A_i \subseteq A$,

$\forall a, b \in A_i (a,b) \in R$, that is, $a R b$,

$A_i \cap A_j = \varphi$, for $i \neq j$,

and $A_1 \cup A_2 \cup A_3 \cup \cdots = A$.

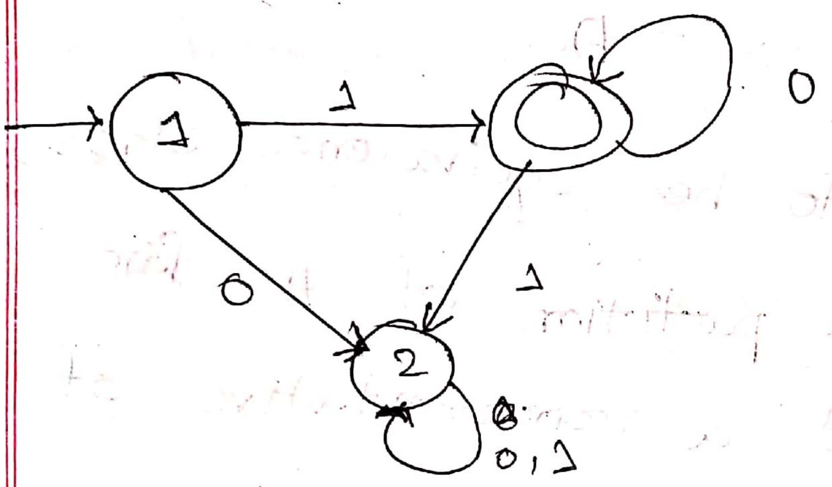
Here A_i is said to be equivalence class, $\{A_1, A_2, A_3 \cdots\}$ - a partition of A for $e \in A_i$, e is called a representative of the class A_i, and representatives of different classes are not equivalent to each other.

Exercise

1. Find the equivalence classes related to I_2, discussed above.

2. Consider the relation $R_1 = \{(a,a), (a,c) (a,f)$ $(b,b), (b,e), (c,a), (c,c), (c,f), (e,b), (e,e), (f,a),$ $(f,c), (f,f)\}$ on $\{a, b, c, e, f\}$.

Demostricate that R_1 is an equivalence relation, and also find the equivalence classes that it yeilds.



DFA — Deterministic Finite Automation

3 states ① ② ③

I_L

① {ε}

② {0, 00,

③ {1, 10, 100, 1000, ...}

Date: 11/02/2019

Topic 3.2 Functions

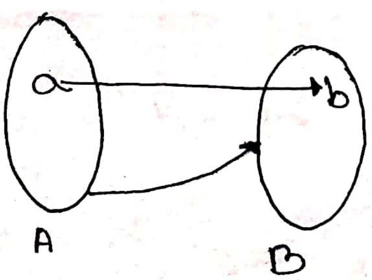
A) Basic Features of functions | Mappings | Transformations

A function f from a set A to a set B associates exactly one element from B to each and every element of A.

In other words, f is a binary relation from A to B in the following way:

$$f = \{(a,b) \mid a \in A \wedge b \in B \wedge \forall a \in A \text{ there is exactly one } b \in B\}.$$

Explanations:



1) f is a function from A to B.

2) We write

$f: A \to B$

[f maps A to B]

$f(a) = b$

[a: argument of f
b: value of f at a]

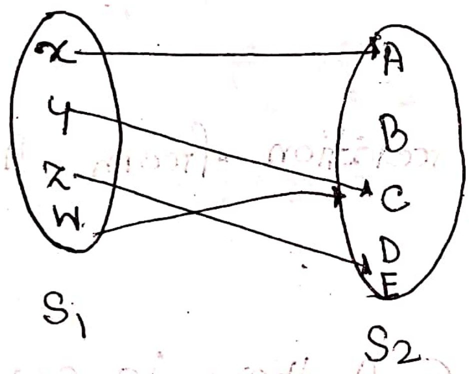
We call,

b: the image of a; a: a Preimage of b;

A: the Domain of f; B: the codomain of f;

Set of all images: Range of f.

Examples:

1. 

S_1: Students;

S_2: Grades obtained in CSE 1203;

$f_1 : S_1 \longrightarrow S_2$;

$f_1(x) = A,\ f_1(y) = C, \ldots$;

S_1: Domain of f_1;

S_2: Codomain of f_1;

$\{A, C, E\}$: Range of f_1.

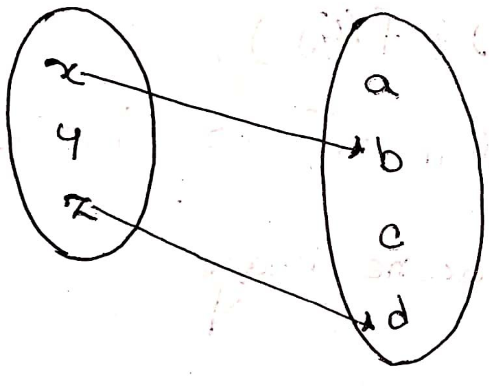
2. f_2 is a function on $\mathbb{Z}$, that is $f_2 : \mathbb{Z} \to \mathbb{Z}$, such that $f_2(x) = x^2$.

$\mathbb{Z}$: the Domain & Codomain of f_2

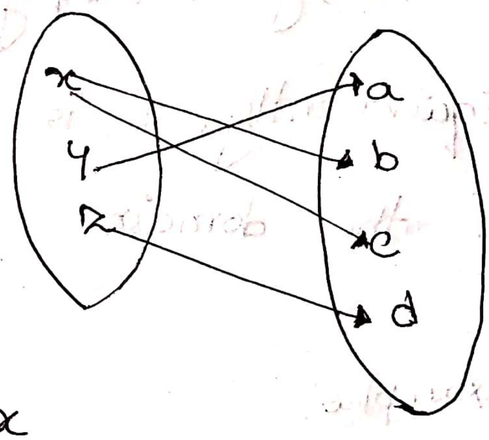
$\{0, 1, 4, 9, 16, \dots\}$: the range of f_2.

Not examples:

1.



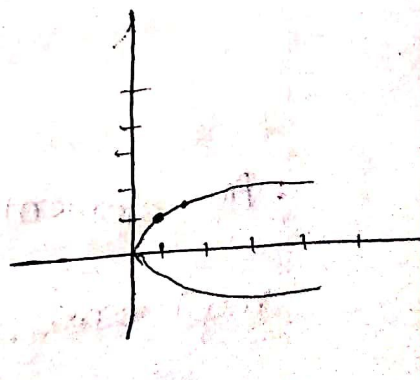
2.



3. $y = f(x)$ is defined as $y^2 = x$

In fact two functions: $f_1(x) = \sqrt{x}$, $f_2(x) = -\sqrt{x}$

$y = \pm\sqrt{x}$



Domain for both $= \{x \mid x \in \mathbb{R} \wedge x \geq 0\}$

Range of $f_1 = \{x \mid x \in \mathbb{R} \wedge x \geq 0\}$

Range of $f_2 = \{x \mid x \in \mathbb{R} \wedge x \leq 0\}$

Topic 3.2 Functions [Continued]

B) Fundamental Classes of Functions

Say, $f: A \to B$

1. One-to-One function / Injective function / Injection

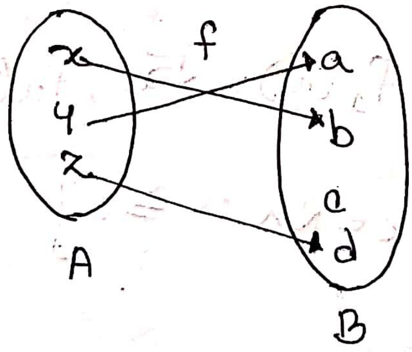
i) f is an injection iff

$$\forall x, y \in A \, (x \neq y \longrightarrow f(x) \neq f(y)).$$

Equivalently, f is an injection iff no two elements of the domain have the same image.

Examples:

1. Idealized



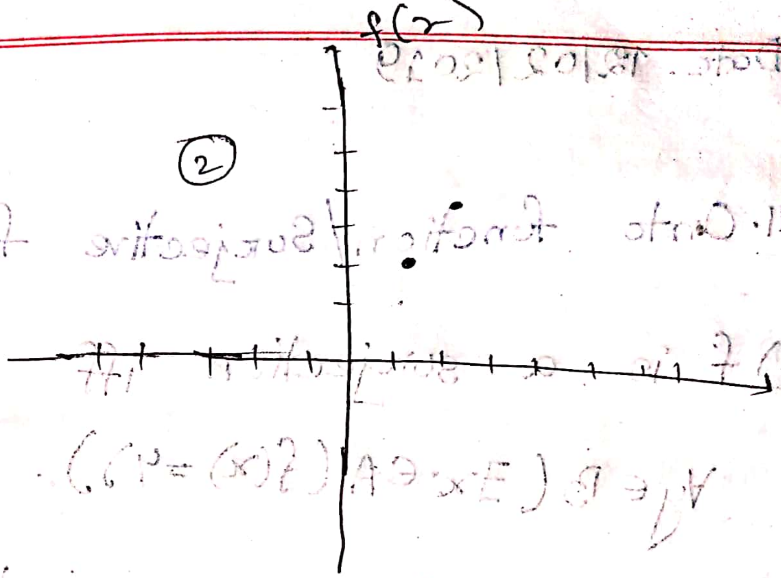
An element of B can be the image of at most one element of A.

[Concrete Examples]

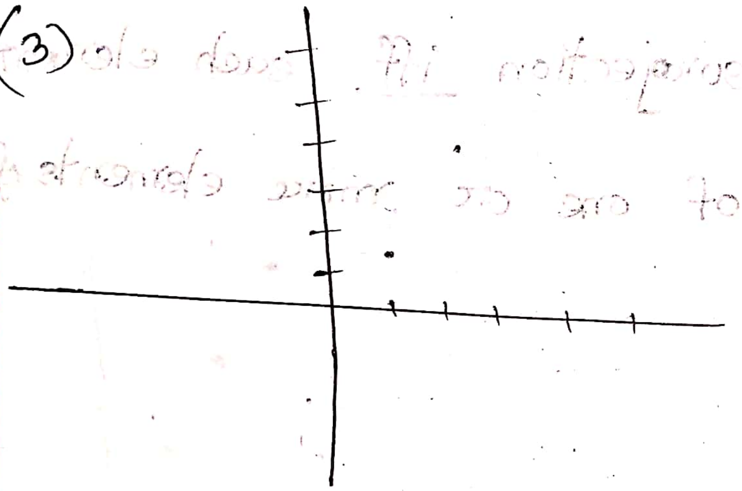
2. $f(x) = x+1$ on $\mathbb{Z}$

3. $f(x) = x^2$ on $\mathbb{Z}^+$

(2)

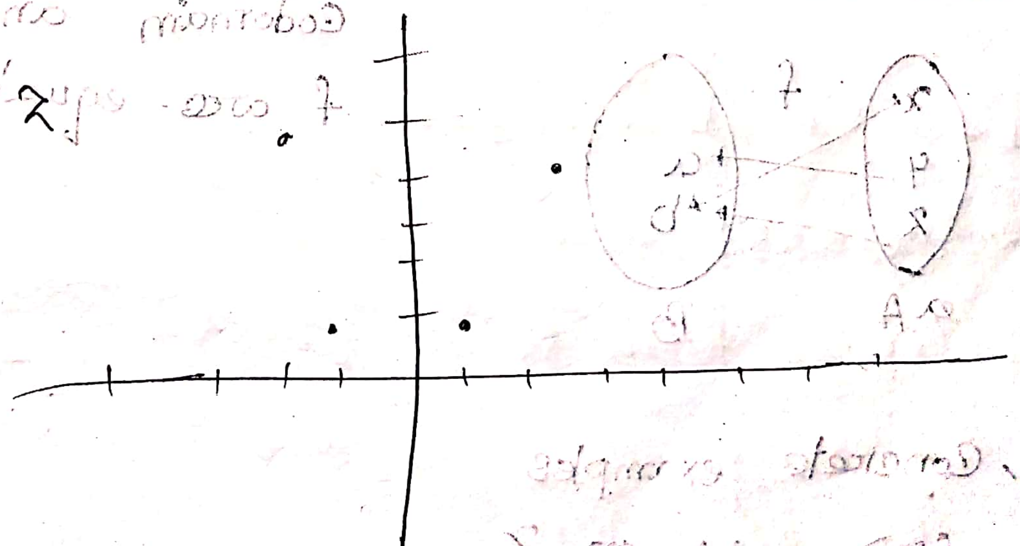


(3)



Not example

$f(x) = x^2$ on $\mathbb{Z}$



Date: 12/02/2019

II. Onto function/Surjective function/surjection

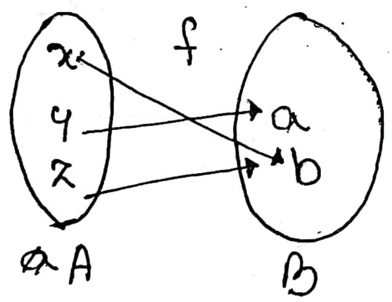
1) f is a surjection iff

$\forall y \in B (\exists x \in A (f(x) = y))$.

Equivalently, f is a surjection <u>iff</u> each element of B is the image of one or more elements of A.

Examples:

1. Idealized



Codomain and range of f are equal.

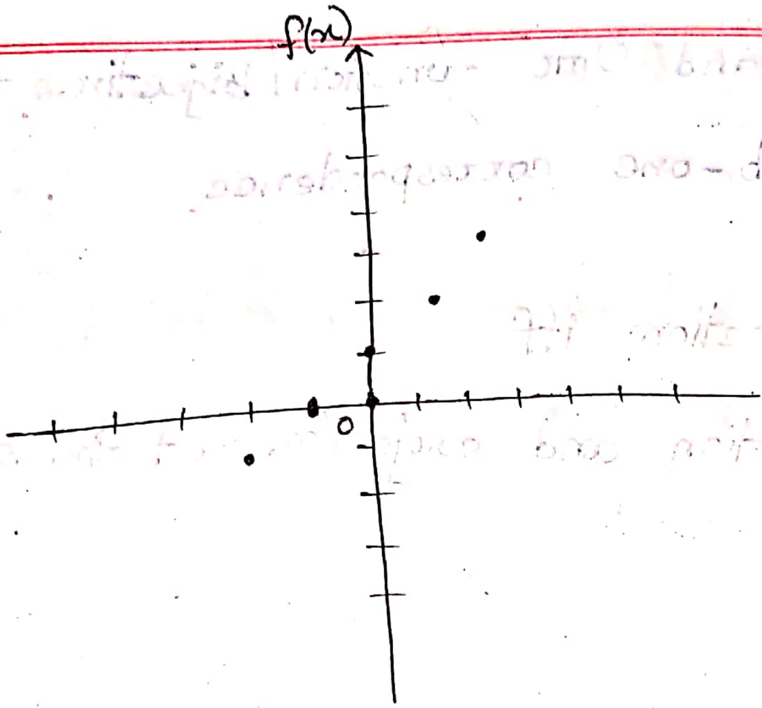
2. Concrete examples

2. $f(x) = x+1$ on Z

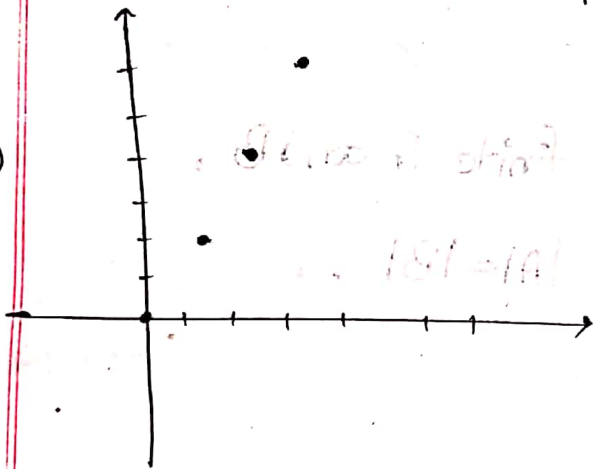
3. $f(x) = 2x$ from N to {0, 2, 4, 6 . . . }

Scanned by CamScanner

(2)

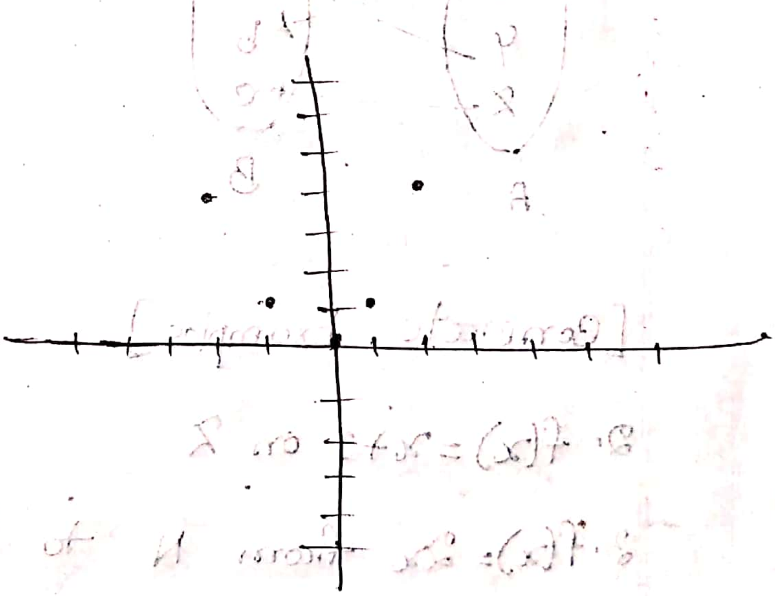


(3)



Not Example

$f(x) = x^2$ on $\mathbb{Z}$

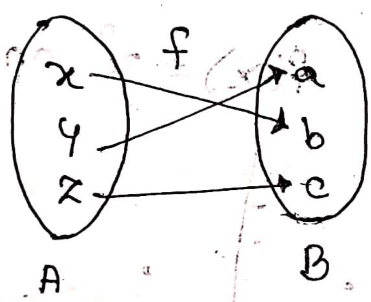


III) One-to-one and Onto function / Bijective function / Bijection / One-to-one correspondence

1) f is a bijection iff it is an injection and surjection at the same time.

Examples

1.) Idealized



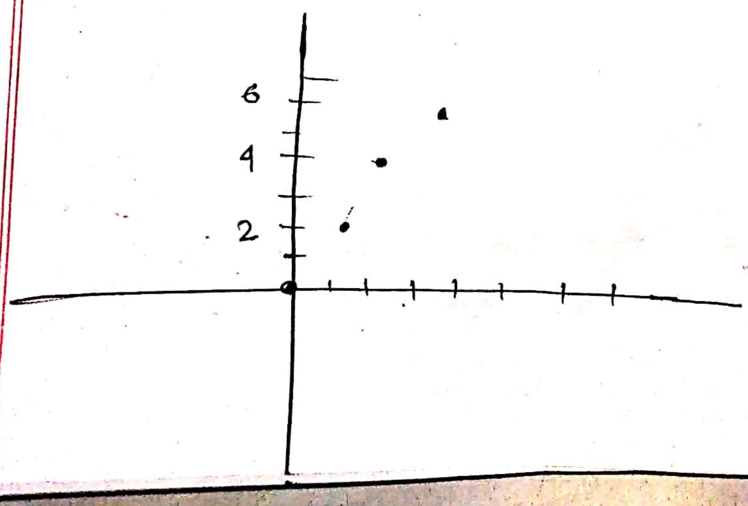
For finite A and B,

$|A| = |B|$.

[Concrete Examples]

2. $f(x) = x+1$ on $\mathbb{Z}$

3. $f(x) = 2x$ from N to $\{0, 2, 4, 6, \ldots\}$



Some important facts about functions and their fundamental classes

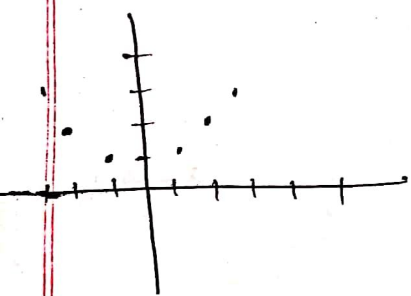
✓ Not all relations are function.

✓ All combination of class properties are possible.

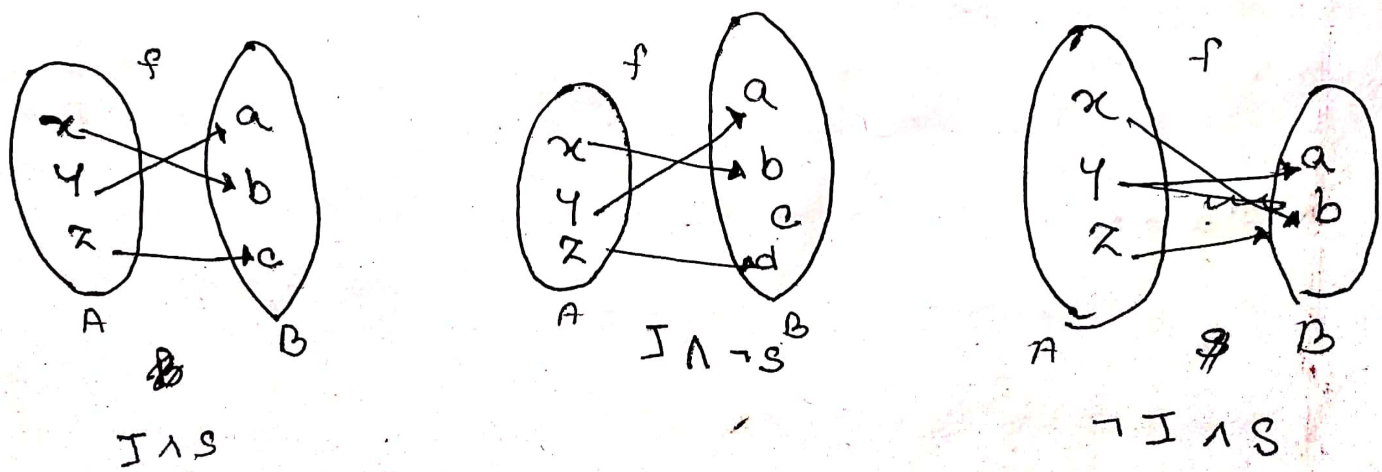
a. $\neg I \wedge \neg S$: $f(x) = x^2$ on $\mathbb{Z}$

b. $I \wedge \neg S$; $f(x) = x^2$ on $\mathbb{N}$

c. $\neg I \wedge S$: $f(x) = |x|$ from $\mathbb{Z}$ to $\mathbb{N}$



d. $I \wedge S$: $f(x) = x+1$ on $\mathbb{Z}$.



$I \wedge S$ $\qquad$ $I \wedge \neg S$ $\qquad$ $\neg I \wedge S$

For finite A and B,

a. f is $I \land S \longrightarrow |A| = |B|$.

b. f is $I \land \neg S \longrightarrow |A| < |B|$.

c. f is $\neg I \land S \longrightarrow |A| > |B|$

d. $|A| = |B| \longrightarrow f$ is injective, iff f is surjective

✓ Identity Function

~~$I_A : A \rightarrow A$ and $I_A(x)$~~

$i_A : A \longrightarrow A$ and $i_A(x) = x$

It is a bijection.

Date: 18.02.2019

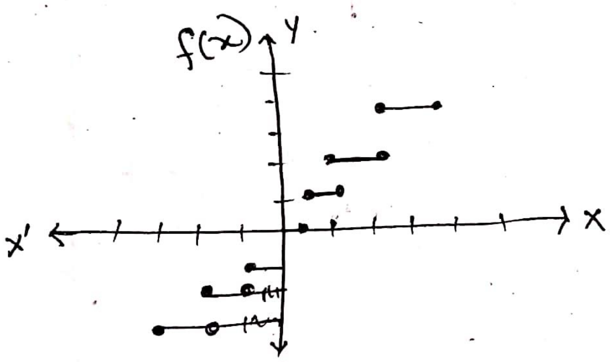
Topic 3.2. Functions (continued)

c) Some Important Discrete Functions

1) Floor function from R to Z

$y = f(x) = \lfloor x \rfloor = n$,

where $n \le x < n+1$, for $x \in R$ and $n \in Z$



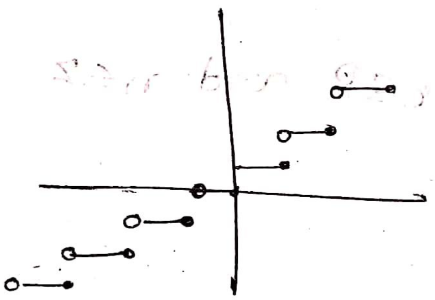
x	y	$x+y$
3.2	1.3	4.5
3	1	4
3.6	1.8	5.4
3	1	5

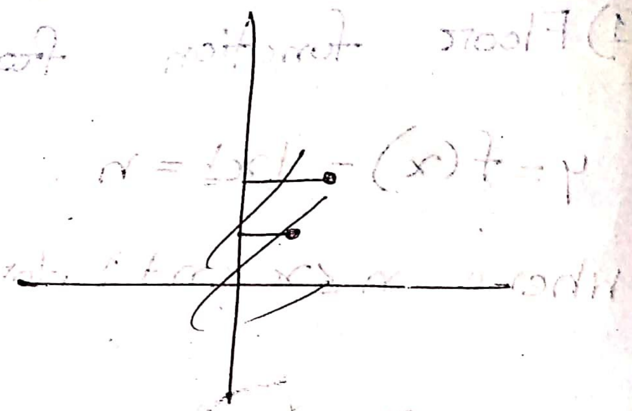
- $\lfloor x \rfloor + \lfloor y \rfloor \le \lfloor x+y \rfloor$
- ......
- $\neg I \wedge S$

2) Ceiling function from R to Z

$y = f(x) = \lceil x \rceil = n+1$, where $n < x \leq n+1$, for $x \in R$ and $n \in Z$

- $\lceil x \rceil + \lceil y \rceil \geq \lceil x+y \rceil$
- .....





x	y	$x+y$
3.2	1.3	4.5
4	2	5
3.6	1.8	5.4
4	2	6

- $\neg I \wedge S$

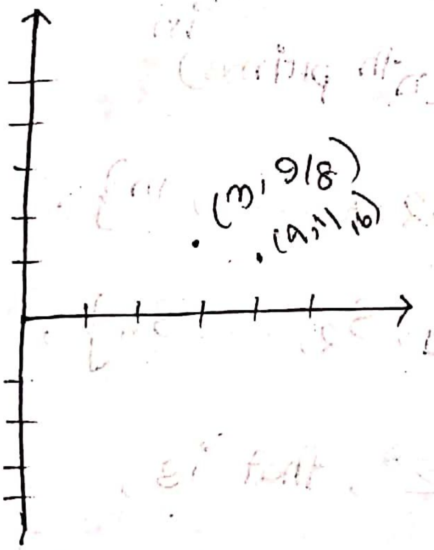
Date: 19/02/2019

3. Discrete numeric functions

Function of the type $f: N \Rightarrow R$

Example: $f(n) = 0$ for $0 \leq n \leq 2$,

$f(n) = 1 + 2^n$, for $n \geq 3$



(4) Functions with Strings as arguments

1) Say, $\Sigma = \{a, b\}$, [Σ . alphabet]

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

Scanned by CamScanner

$L : \Sigma^* \rightarrow N$, such that $L(x) = n$, where n is the number of symbols in x, that is, $|x|$.

$L(\varepsilon) = 0$, $L(a) = 1$, $L(b) = 1$, $L(aa) = 2$, $L(ab) = 2$ . . .

$\neg I \wedge S$.

II) $GN : \Sigma^* \rightarrow N$, such that

$GN(x) = 2^{i1} \times 3^{i2} \times 5^{i3} \times \ldots \times (n^{th} \text{ prime})^{in}$

where $i1, i2, i3, \ldots, in \in \{1, 2, 3, \ldots, m\}$,

for $|\Sigma| = m$, and say, $\Sigma = \{s_1, s_2, \ldots s_n\}$,

[GN - Godel ~~Ho~~ Number, and $x \in \Sigma^*$, that is, x is a string of symbols in Σ, 1^{st} prime = 2]

Suppose, $\Sigma = \{a, b\} = \{s_1, s_2\}$.

$GN(a) = 2^1 = 2$, $GN(b) = 2^2 = 4$,

$GN(aa) = 2^1 \times 3^1 = 6$, $GN(ab) = 2^1 \times 3^2 = 18$

$GN(ba) = 2^2 \times 3^1 = 12$ . . . .

$GN(\varepsilon)$ is taken 1 . $\qquad I \wedge \neg S$

Scanned by CamScanner

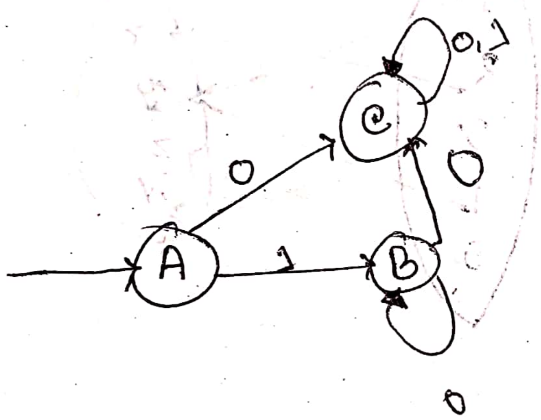
5) Transition function of automata (machines)

Consider the DFA for $L(10^*)$ shown earlier.

States, $S = \{A, B, C\}$, $\Sigma = \{0, 1\}$

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

$\delta(A, 0) = C$, $\delta(A, 1) = B$, $\delta(B, 0) = B$, $\delta(B, 1) = C$, ...



$\neg I \wedge \neg S$

D) Composition and Inverse of functions

✓ Say, f and g are functions such that

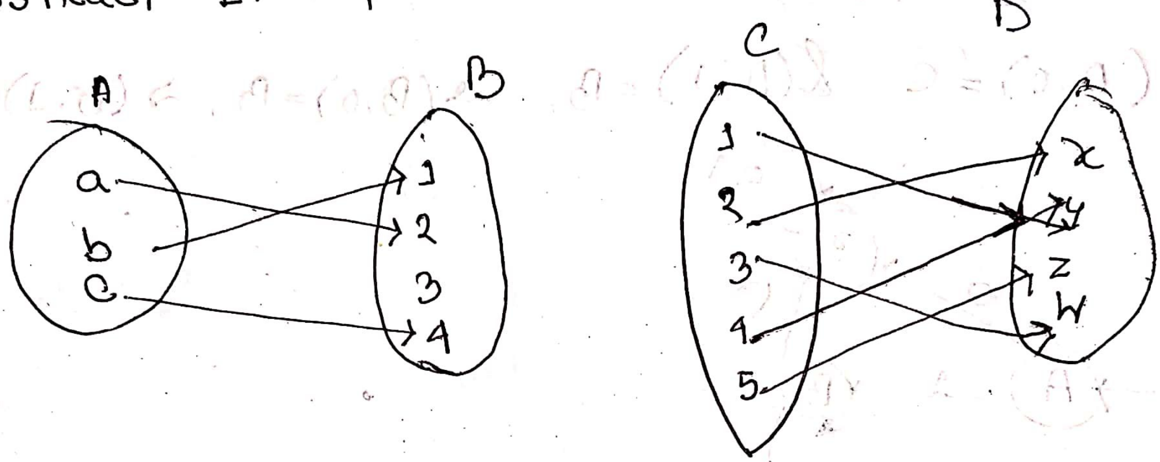
$g : A \rightarrow B$, $f : C \rightarrow D$,

and the range of g is a subset of the domain f [Special case: $B = C$]

Composition of f and g is a function from A to D, denoted by $f \circ g$, such that

$f \circ g(x) = f(g(x))$, for $\forall x \in A$

Abstract Example



$f \circ g(a) = i$, $f \circ g(b) = j$, $f \circ g(c) = i$

Concrete example :

$f_1(x) = 2x+1$ on R , $f_2(x) = x-2$ on R

- $f_1 \circ f_2(x) = f_1(f_2(x)) = f_2(x-2) = 2(x-2)+1 = 2x-3$
- $f_2 \circ f_1(x) = f_2(f_1(x)) = f_2(2x+1) = 2x+1-2 = 2x-1$

✓ Say, $f : X \to Y$, and f is a bijection.

The inverse of f, denoted by f^{-1}, is a function such that $f^{-1} : Y \to X$ and

$f^{-1}(f(x)) = x$, for all $x \in X$, and $f(f^{-1}(y)) = y$ for all $y \in Y$.

* A function is invertible iff it is bijection.

Example:

$f(x) = 2x$ from N to $\{0, 2, 4, 6, \ldots\}$

$f^{-1}(x) = x/2$

I ∧ S.

Date: 04/03/2019

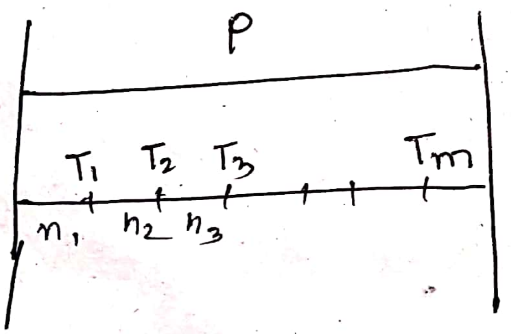
Chapter 4
Counting and Countability

Topic 4.1. Basic Counting Principles

A) The Product Rule

✓ Say, a process P can be broken down to sequence of m tasks,

$T_1, T_2, T_3 \dots, T_m$



and say, T_i can be done in n_i different ways after up to T_{i-1} is done.

- There are $n_1 \times n_2 \times n_3 \times \dots \times n_m$ different ways to execute the process P.

✓ Examples

1) How many 5-length bit strings are possible?

0/1 0/1 0/1 0/1 0/1

2 2 2 2 2

$2 \times 2 \times 2 \times 2 \times 2 = 2^5 = 32$

2) How many 4-digit binary numbers are possible?

3) How many 3-digit numbers (decimal) are possible

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

$\cancel{k^4}\ 2^4 = 16$

0 0 0
0 0 1
0 0 2
⋮
0 0 9
0 1 0
⋮
9 9 9

10 10 10

$10^3 = 1000$

4) How many car license numbers are possible that have 2 capital letters at the beginning, followed by a hyphen, and then by 3 digits?

AB - 099

A-Z	A-Z	-	0-9	0-9	0-9
26	26	1	10	10	10

$26^2 \times 1 \times 10^3$

5) Observe the code fragment below:

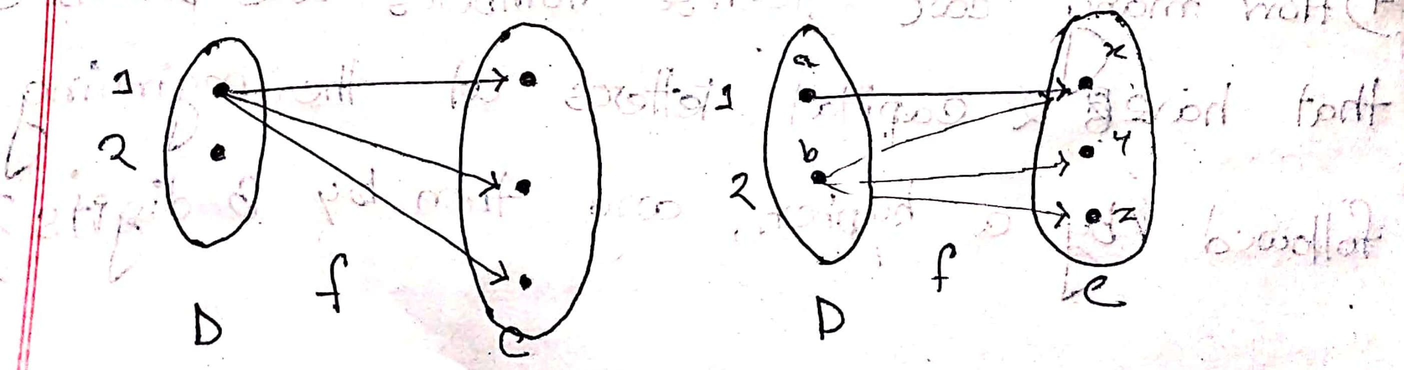
```
k := 0
for i1 = 1 to n1
  for i2 = 1 to n2
    :
    :
    for im = 1 to nm
        k := k+1
```

Value of k after execution of the program fragment:

$n_1 \times n_2 \times n_3 \times \ldots \times n_m$

(6) $f: D \to C$, $|D| = m$, $|C| = n$.

What would be the number of different possible functions of this kind?

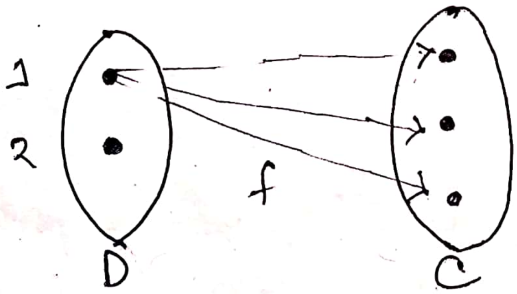


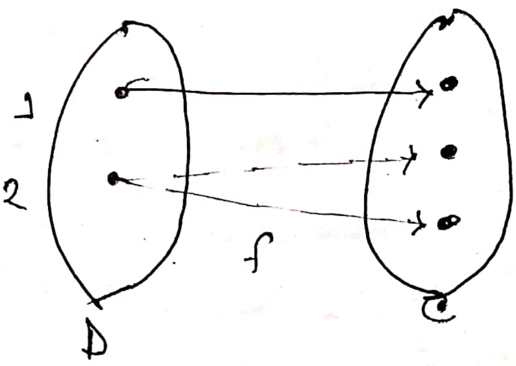
m

$\frac{3}{1}$ $\frac{3}{2}$ $3^2 = n^m$ $|C|^{|D|}$

{(a, x), (b, x)}
{(a, x), (b, y)}
{(a, x), (b, z)}
{(a, y), (b, x)}
{(a, y), (b, y)}
{(a, y), (b, z)}
{(a, z), (b, x)}
{(a, z), (b, y)}
{(a, z), (b, z)}

7) Suppose, $f: D \to C$, $|D| = m$, $|C| = n$, f is an INJS.





$\frac{3}{1}$ $\frac{2}{2}$ 3×2.

In general: $n \times (n-1) \times (n-2) \times \dots \times (n-(m-1))$

3 5

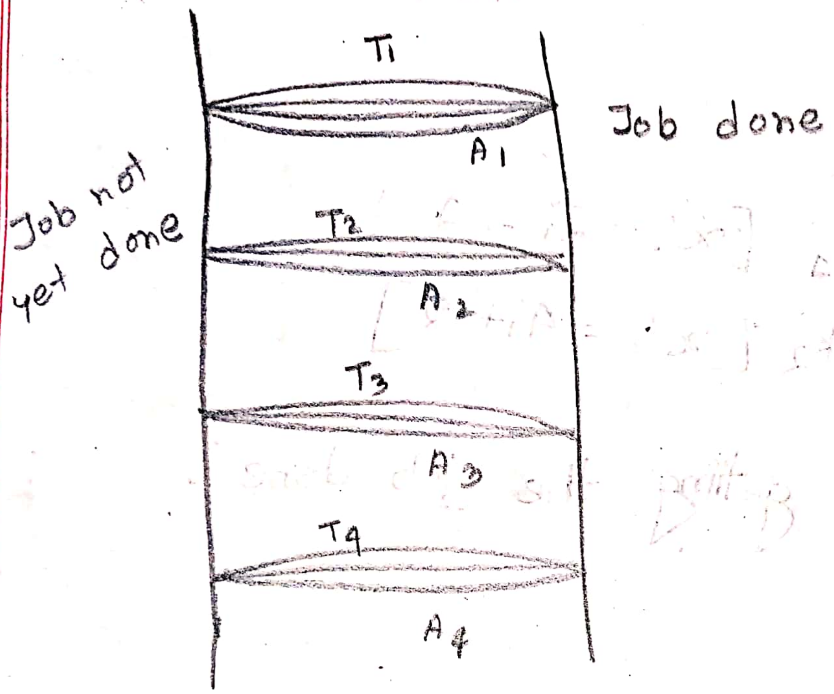
$5 \times 4 \times 3$

If f is an $I \wedge S$, that is f is a bijection,
then $|D| = |C| = n$, and the number is $n \times (n-1) \times (n-2) \times \_\_\_\_ 1 = n!$

B) The Sum Rule

Suppose, one of the tasks, from among m different tasks $T_1, T_2, T_3 \ldots T_m$, is required to be carried out to have a job done.

Date: 04/03/2019



And say, there are $n_1, n_2, n_3 \ldots n_m$ different way to carryout the tasks respectively.

- Then there are $n_1 + n_2 + n_3 + \ldots + n_m$ different ways to get the job done.

Examples:

1) Program fragment for a job:

for $i=1$ to n

if condition = True

then do Task$_1$ $[x := 2i^2 + 1]$

else do Task$_2$ $[x := 4i + 2]$

Possible ways of getting the job done:

$n+n = 2n$

2) Either a teacher or a student may represent the department in a committee.

No. of teachers $= m$,

No. of students $= n$; and nobody is both a teacher and a student.

There are $m+n$ different ways of representing the department.

c) Combination of Product and Sum Rules :

Example 1. How many identifiers are possible under the following conditions:

i) At most 8 letters or digits are used;

ii) 1^{st} symbol is a lowercase letter;

iii) There are 50 reserved words (keyboards) each of 3 lowercase ~~#~~ letters each.

$N_1 = 26$ [of length 1] $\frac{a-z}{26}$

$N_2 = 26 \times (26+26+10)$ $\frac{a-z,\ A-Z,\ 0-9}{26+26+10}$

$N_3 = 26 \times (26+26+10) \times (26+26+10) - 50$

Total $= N_1 + N_2 + N_3$

Example 2: How many passwords of length 6 to 8 are possible if

i) only lowercase letters and digits are used and

ii) a password must contain at least one digit?

$N = N_6 + N_7 + N_8$, where

$N_6 = 36^6 - 26^6$ $\quad$ $\underline{a-z, 0-9}$, $\underline{a-z, 0-9}$ . . . - - - , 8s

$N_7 = 36^7 - 26^7$ $\quad$ $\underline{a-z}$, $\underline{a-z}$, . . .

$N_8 = 36^8 - 26^8$

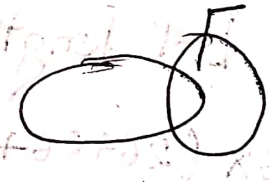
Topic 4.1 Basic Counting Principles (Continued)

D) Principle of Inclusion and Exclusion

* Sample form:

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

included twice in $|A| + |B|$



Example: How many integers from 1 to 20 are divisible by 2 or 3?

Let, A contain those divisible by 2, and B contain those divisible by 3.

So $A \cup B$: divisible by 2 or 3.

$A \cap B$: divisible by 2 and 3.

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

$= 6\lfloor 2012/8 \rfloor + \lfloor 2013/9 \rfloor - \lfloor 2016 \rfloor$

$= 10 + 6 - 3 = 13$

⇒ General form of the principle of inclusion and exclusion

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

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

- $|A_1 \cup A_2 \cup A_3 \cup A_4| = |A_1| + |A_2| + |A_3| + |A_4| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_3| - \dots - |A_3 \cap A_4| + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| - |A_1 \cap A_2 \cap A_3 \cap A_4|$.

Date: 07/03/2019

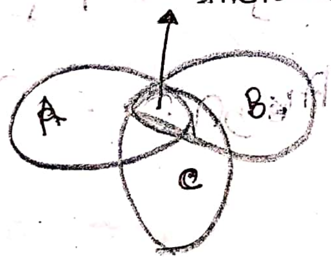
Example: How many binary strings of length 5 begin with 0 or end with 1 or have 1 at the central places?

A. 0   0/1   0/1   0/1   0/1 $|A| = 1\times2\times2\times2\times2 = 16$

B. 0/1   0/1   0/1   0/1   1 $|B| = 2\times2\times2\times2\times1 = 16$

C. 0/1   1   1   1   0/1 $|C| = 2\times1\times1\times1\times2 = 4$

Included thrice in $|A|+|B|+|C|$



$A\cap B$: 0   0/1   0/1   0/1   1 $|A\cap B| = 1\times2\times2\times2\times1 = 8$

$A\cap C$: 0   1   1   1   0/1 $|A\cap \cancel{B}C| = 1\times1\times1\times1\times2 = 2$

$B\cap C$: 0/1   1   1   1   1 $|B\cap C|$ $\cancel{|A\cap B|} = 2\times1\times1\times1\times1 = 2$

$A\cap B\cap C$: 0   1   1   1   1 $|A\cap B\cap C| = 1\times1\times1\times1\times1 = 1$

$|A\cup B\cup C| = 16+16+4-8-2-2+1 = 37-12 = 25$

Exercise: Solve the following problems and name the major counting principles involved.

1) Department: 20 teachers; 250 male students; 150 female students,

i) 1 teacher and 3 male students and 2 female students form a delegation; How many possible delegations? [Hint: Combination+ Product rule]

$N_1 = {}^{20}C_1 = \frac{20!}{1!\,19!}$

$N_2 = {}^{250}C_3$ $\quad N_3 = {}^{150}C_2$

i) $N_1 \times N_2 \times N_3$

ii) 1 teacher or 3 male students or 2 female ~~studen~~ students from a delegation; How many possible delegations? [Hint: Combination + Sum rule]

$\Rightarrow N_1 + N_2 + N_3$

2) How many integers between 21 and 200 (including 21 and 200) are divisible by 3 or 5 or 9?

[Hint x: 1-200, y: 1-20; $x-y$ to be found]

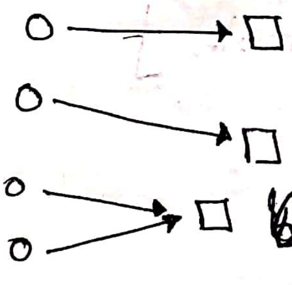
Answer: 84

Topic 4.1. Basic Counting Principles (continued)

E) The Pigeonhole Principle

Sample form:

If there are k boxes to contain more than k objects, then at least one box must contain more than one objects.



3 boxes (holes)

4 objects (pigeon)

Problems:

1) What is the smallest class size, for which it is obvious that at least two students have the same grade in a course, if the set of possible grades,

$G = \{ (A+, A, A-, B+, B, B-, C+, C, D, F) \}$

Boxes: Grades; $|G| = 10$

Objects: Students

10 boxes; so, needed $10+1$, that is, 11 objects.

2) What is the size of the smallest group of people, for whom at least two must have the same birthday according to the English calender?

Boxes: $365+1$ days,

Objects: People.

366 boxes; so needed $366+1$, that is, 367 objects.

3) Say, $f : D \to C$, and $|D| > |C|$, for finite D & C.

Can f be an injection?

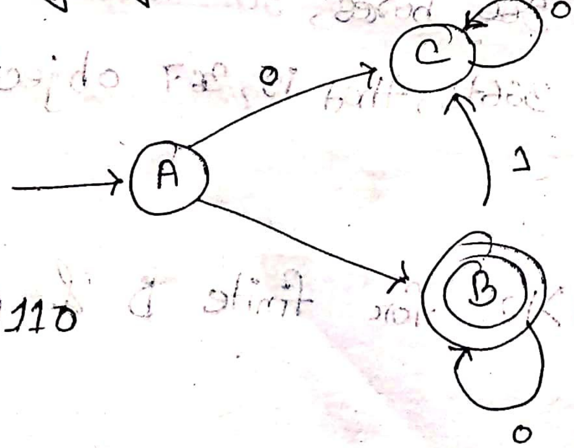
Boxes: $|C|$; Objects: $|D|$

As $|D| > |C|$, at least one of ~~the~~ C is the image of two or more of D. So, f can't be an injection.

4) How many single shoes at least are to be examined from a mess of 100 pairs to find a proper pair for sure?

Boxes: 100, so Objects required: 101

5) If there is a string of length $\geq$ the number of states of a DFA and if it is accepted by the DFA, then there must be a cycle, and the language is infinite.



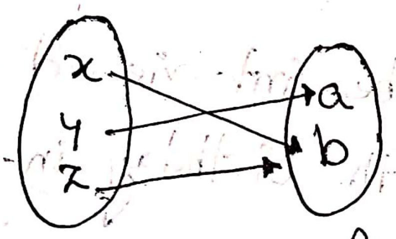
$L = \{1, 10, 100, 1000, \ldots\}$

0110

Date: 11.03.2019

Generalized Pigeonhole Principle

m boxes
n objects $\longrightarrow$ At least one box contains at least $[n/m]$ objects.



objects Boxes

$[3/2] =$

$[1.5] = 2$

Problems:

1) Grades: A, B, C, D, F

Class size: 66

What is the minimum size of the largest group obtaining the same grade?

A	1	2	3
B	1	2	3
C	1	2	3
D	1	2	3
E	1	2	3

Boxes: 5 Objects: 66

$[66/5] = [13.2] = 14$

2) Sample size of a survey: 100 persons.
What is the minimum size of the largest group having month in the same month?

⇒ Boxes: 12 Objects: $\lceil 100/12 \rceil = \lceil 8.33 \rceil = 9$

3) How many people are to be interviewed to find for sure at least 9 with birthday in the same month?

⇒ $\lceil \frac{n}{12} \rceil = 9$ Boxes: 12 objects: n;

$n_{min} = 12 \times (9-1)+1 = 97$

$n_{max} = 12 \times 9 = 108$

Answer: Any number from 97 to 108

Topic 4.2: Reccurrence Relations

✓ Say; a_i, a_{i+1}, a_{i+2}, ..., for an $i \in N$ sequence.

- Recurrence relation: An equation that defines a term, an using one or more ~~predict~~ preceding terms, given one or more term values as initial conditions.

- The solution: The sequence itself.

✓ Example

1) Rabbits and Fibonacci numbers

- Each pair gets matured at the age of 2 months and gives birth to 1 pair every next month.

f_0 : 0

f_1 : 1 $\quad P_1$

f_2 : 1 $\quad P_1$

f_3 : 2 $\quad P_1, P_{11}$

f_4 : 3 $\quad P_1, P_{11}, P_{12}$

f_5 : 5 $\quad P_1, P_{11}, P_{12}, P_{13}, P_{111}$

$f_5 : 8$ $P_1, P_{11}, P_{12}, P_{13}, P_{14}, P_{111}, P_{112}, P_{121}$

• Number of pairs in the n^{th} month, f_n:

$f_n = f_{n-1} + f_{n-2}$, for $n \in N$, $n \geq 2$, $f_0 = 0$, $f_1 = 1$.

2) Tower of Hanoi

Say H_n = Number of moves required to transfer n discs from A to C, with the help of C, if required.

$H_n = 2H_{n-1} + 1$, for $n \in N$, $n \geq 2$, $H_1 = 1$

Solution up to H_6:

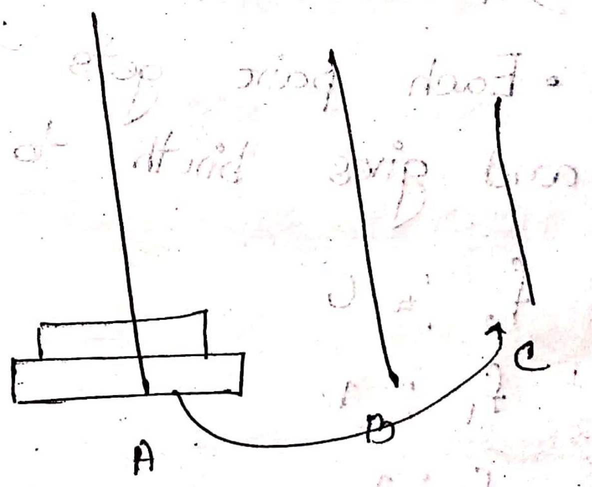
$H_2 = 2H_1 + 1 = 2+1 = 3$

$H_3 = 2H_2 + 1 = 6+1 = 7$

$H_4 = 2H_3 + 1 = 15$

$H_5 = 31$

$H_6 = 63$



3) Find the solution, up to a_8, of the recurrence relation,

$a_n = a_{n-1} + 2a_{n-3}$, for $n \in N$, $n \geq 3$, $a_0 = 1$, $a_1 = 2$, $a_2 = 0$

Sollution: $a_3 = a_2 + 2a_0 = 0 + 2 \times 1 = 2$

$a_8 = 54$ [Must Verify]

a_4 :

a_5 : . . . a_8 :

4) Compound Interest

$P_n = P_{n-1} + 0.11 P_{n-1}$

$= 1.11 P_{n-1}$

$= (1.11)^n \times P_0$

Suppose, P_n - amount after n years with 11% interest and $P_0 = 100000$, for $n \in N$, $n \geq 1$

Exercise

Find the solution up to a_6, of the recurrence relation

i) $a_n = a_{n-1} + (-1)^n a_{n-2}$, for $n \in N$, $n \geq 2$, $a_0 = 0$, $a_1 = 1$.

ii) $a_n = n a_{n-1} + a_{n-2}^2$, for $n \in N$, $n \geq 2$, $a_0 = -1$, $a_1 = 0$.

Scanned by CamScanner

Date: 12/03/2019

Topic 4.3: Countable and Uncountable Sets

✓ A finite set is always said to be countable, because the elements can be indexed or numberred in the way they are described.

✓ An infinite set is not always countable. It is countable, if there is a bijection to it from N or vice-versa, that means, if its elements can be indexed.

✓ Examples of Countable Infinite Sets:

1) $\{1, 3, 5, 7, \ldots\} = O$ $\qquad f: N \to O$

$\{0, 1, 2, 3 \ldots\} = N$ $\qquad f(n) = 2n + 1$

I ∧ S $\quad$ $f^{-1} p$

2) $\{0,2,4,6,\ldots\} = E$ $\quad f: N \rightarrow E$ $\quad$ I^S

$\{0,1,2,3,\ldots\} = N$ $\quad f(n) = 2n$ $\quad f^{-1}$?

3) $\{0,1,-1,2,-2,\ldots\} = Z$ $\quad f: N \rightarrow Z$

$\{0,1,2,3\ldots\} = N$ $\quad f(n) = -n/2$, for $n \in E$.

$= (n+1)/2$, for $n \in O$

I^S

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

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

$N = \{0,1,2,3,4,5,6,7,\ldots\}$

$f: N \rightarrow \Sigma^*$, $f(n) = ?$ [Try using GIN]

✓ Examples of uncountable sets

(1) $P(N) = 2^N = \_$, can't be indexed.

- Power set of an infinite set is uncountable.
- $P(\Sigma^*)$, that is, 2^{Σ^*}, for a nonempty Σ,

is uncountable.

- Languages are uncountable, but computers (Turing Machines) are countable.

2) $\{x \mid x \in R \wedge x > 1.0001 \wedge x < 1.0002\}$

✓ Can we index prime numbers?

■ Primality check of positive integers n:
Divisibility by 2, 3, 5, 7, ... m (prime), such that $m \leq sqrt(n)$.

Not efficient: This is a field of active research in Cryptography, Network Security, etc.

■ $P_1 \times P_2 \times P_3 \times P_4 \times \ldots \times P_m + 1$ is always a prime, where $P_1 = 2$, $P_2 = 3$, ...

[Otherwise, $P_1 \times P_2 \times P_3 \times P_4 \times \ldots \times P_m$ and 1 have common factors other than 1!!!]

■ A new prime can be found using a new known sequence, $P_1, P_2, P_3, P_4, \ldots, P_m$

So, there are infinitely many primes!

■ Not all primes can be written as $P_1 \times P_2 \times P_3 \times P_4 \times \ldots \times P_m + 1$.

For example: 5, 11, 13, 17, 19, 23, 29, ...

* There is always a scope of discovering a new prime!!!

* No general formula yet for primes!!)

* So, the question remains open!!!)

Date: 18/03/2019

Chapter 5

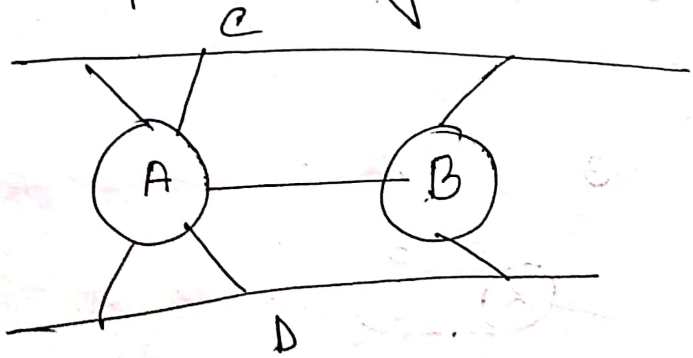
Graph Theory

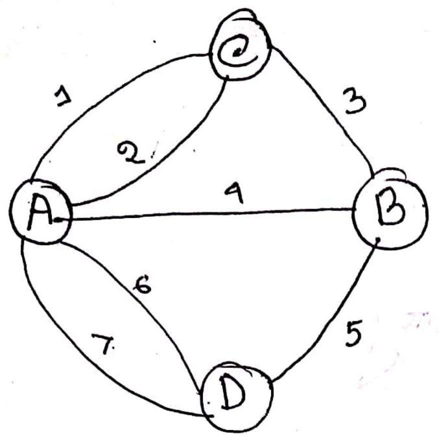
Topic 5.1 Introduction

✓ Graphs - very widely used data structure problem representation and decision making.

✓ Königsburg 7- bridges problem, Euler and Birth of a new science.

Graph Theory.





Vertex / Node

Edge / Arc

(V, E) - system

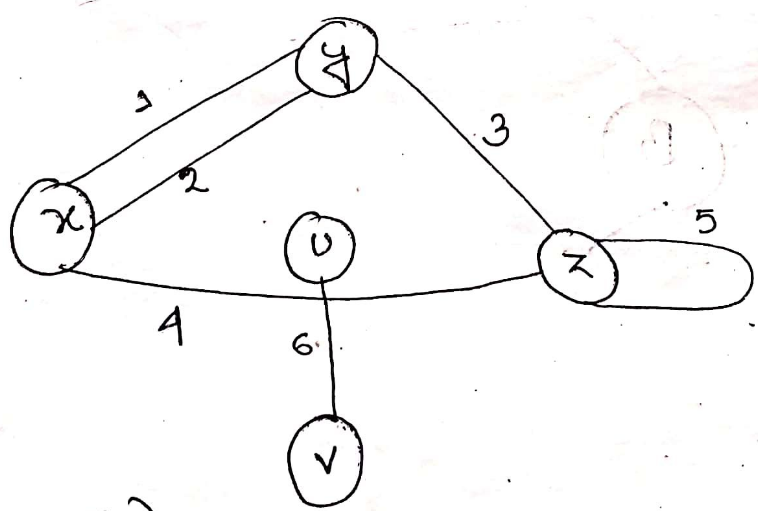
$V = \{A, B, C, D\}$

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

✓ Modeling Computer networks, Transport routes, Chemical structures, ..., Object relationships, All NP-complete problems.

Basic Concepts

1. Graph / Undirected Graph



$G_1 = (V_1, E_1)$

$V_1 = \{x, y, z, u, v\}$ $E_1 = \{1, 2, 3, 4, 5, 6\}$

Scanned by CamScanner

5 - a loop

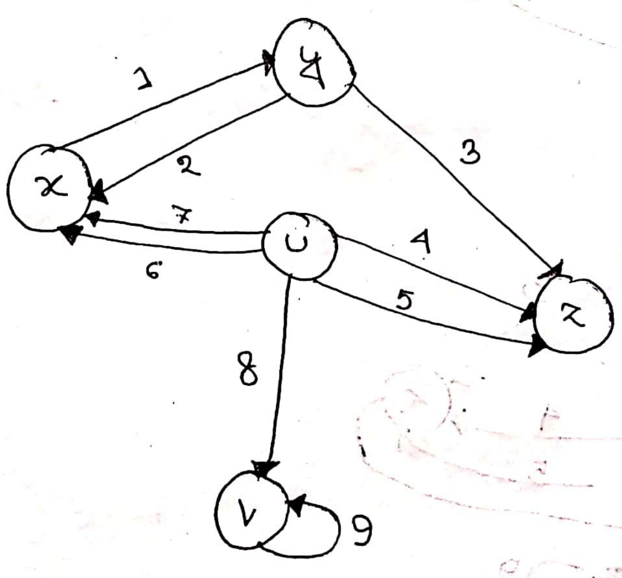
1, 2 - parallel / multiple edges.

$(\{u, v\}, \{6\})$ – an isolated subgraph

- Set of vertices must be nonempty.
- If no loops, no multiple edges and no isolated subgraph, then it is called a simple graph.
- An edge has two ends.
- Edges meet only vertices.

$(\{x, y, z\}, \{1, 2, 3, 4, 5\})$ –

2. Directed Graph



$G_2 = (V_2, E_2)$,

$V_2 = \{x, y, z, u, v\}$

$E_2 = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

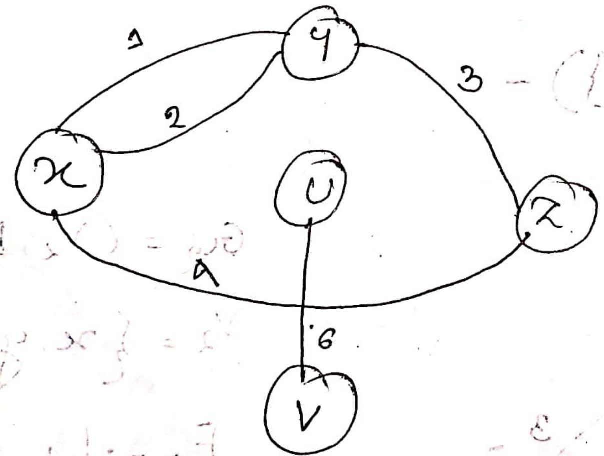
$E_2 = \{ (x, y), (y, x), (y, z),$

9 - a loop

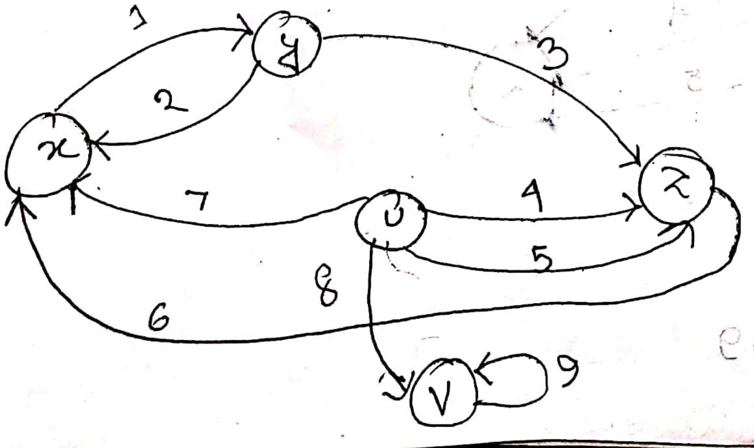
4, 5 - parallel / multiple edges

- Edges are 'directed' or 'pointed to' vertices.
- An edge originates at an end vertex and terminates at another end vertex.
- If no loops, no multiple edges and no isolated subgraph, then it is called a simple directed graph

G_1



G_2



3. Adjacent vertices/neighbors [v is adjacent to u in G_2, not vice-versa]

G_1: x, y | x, u X

y, z

y, x

x, z

G_2: u, v

G_2: x, y – [1]

y, x – [2]

y, z – [3] – z is adjacent to y

z, y – X

4. Degree of a vertex, deg(x) = 3 in G_1 [Number of edges incident with]

5. In-degree in-deg and out-degree (out-deg)

Date: 19/03/2019

6. Disconnected graph - with isolated subgraph.

7. The Handshaking Theorem:

✓ For an undirected graph, $G = (V, E)$,

$\sum_{v \in V} deg(v) = \underline{2|E| = 2e}$ [An edge has two ends; Edges meet at vertices]

✓ For a directed graph, $G = (V, E)$,

$\sum_{v \in V} in\text{-}deg(v) = \sum_{v \in V} out\text{-}deg(v) = \underline{|E| = e}$

and,

$\sum_{v \in V} deg(v) = \sum_{v \in V} (in\text{-}deg(v) + out\text{-}deg(v)) =$

$\underline{2|E| = 2e}$.

Topic 5.2. Special Types of Graphs

1. Complete Graphs

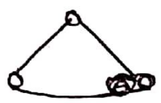
Exactly one edge connect any two vertices,

$K_2, K_3, K_4, K_5, \ldots$

K_2

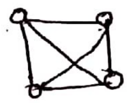
1

K_3



3

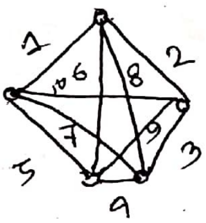
K_4



6

K_5

K_5



10

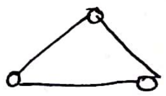
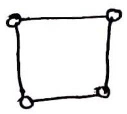
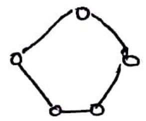
No. of edges of ~~Sum of the degrees~~, $K_n = n(n-1)/2$

2. Cycle Graphs / Cycles

Only one simple cycle or circuit.

$C_3, C_4, C_5 \ldots$

C_3 C_4 C_5

3 4. 5

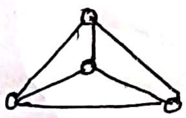
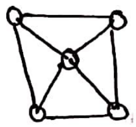
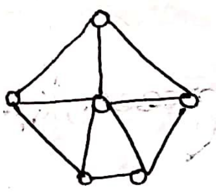
No. of edges of C_n = $2n/2 = n$

3. Wheels

Cycle with one additional vertex that is adjacent to all other.

$W_3, W_4, W_5, \ldots$

V_3 W_4 W_5

No. of edges of W_n = $\frac{3n+n}{2} = 2n$

4. Paths / Path Graphs

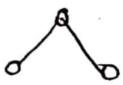
Incomplete simple connected circuit; Single path

$P_2, P_3, P_4, P_5 \ldots$

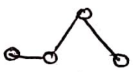
No. of edges of $P_n = n-1$

P_2

P_3



P_4



P_5

$$\frac{1+1+2(n-2)}{2} = \frac{2+2n-4}{2} = \frac{2n-2}{2} = n-1$$

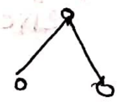
5. Trees

$T_1, T_2, T_3, T_{41}, T_{51}, T_{52}, T_{53}, \ldots$

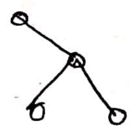
T_1

T_2

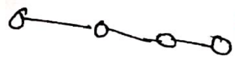
T_3



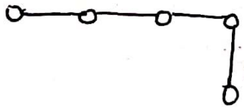
T_{41}



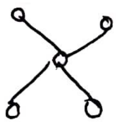
T_{42}



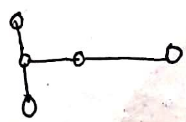
T_{51}



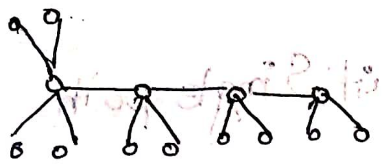
T_{52}

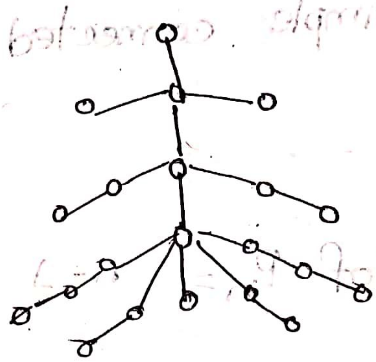


T_{53}



Caterpillar, Christmas Tree, . . .





✓ A tree is a simple graph with no circuits or circles.

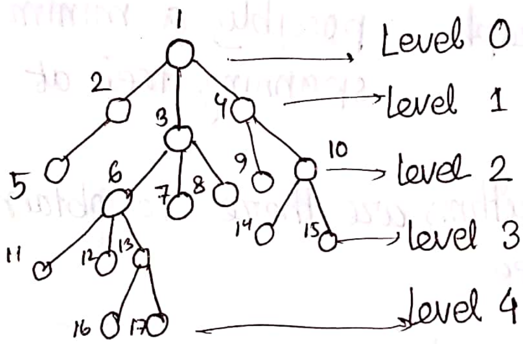
✓ Properties of Trees:

- T_1 has $n-1$ edges;
- There exists a unique path between any two vertices;
- Deleting an edge results in a disconnected graph, which is a 'Forest' with exactly two trees;
- A new edge between any two vertices results in a graph with one circuit.

✓ properties of trees:

- T_n has $n-1$ edges;
- There exists a unique path between any two vertices.
- Deleting an edge results in a disconnected graph, which is a 'Forest' with ~~two~~ exactly two trees.
- A new edge between any two vertices results in a graph with one circuit.

~~5.2~~ ⊞ - Rooted tress



Parent-child : 1-2, 1-3, 1-4, - -

Ancestor of 16 : 13, 6, 3, 1

Root: 1 ; Taken to have no ancestors

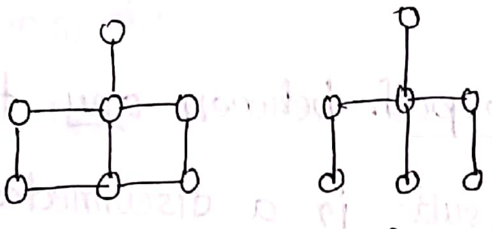
Descendent of 4 : 10, 14, 15

Descendent of 1 : 2–17,

Siblings : 2, 3, 4 ; 11, 12, 13 ; 16, 17 ; 14, 15 ;

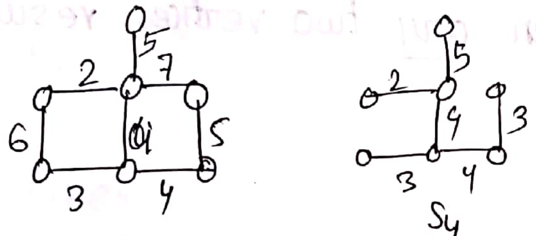
⊞ ☐ leaves ; Internal vertices ; Branching factor : 3 ; Binary trees, ordered (left to right) children or sub trees.

Spanning Trees:



S_1 $\quad$ S_2

- $V(S_2) = V(S_1)$
  $E(S_2) \subseteq E(S_1)$ and S_2 is a tree
- S_2 is a spanning tree at graph S_1.



S_3 $\quad$ S_4

weighted graph $\quad$ possibly a minimum weight spanning tree at graph S_3

~~10^{128}~~ 10^{128}

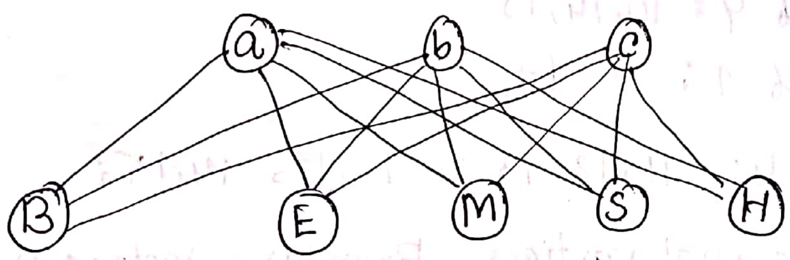
- Various algorithms are there to obtain a minimum weight spannig tree.

6) Bipartite graph:

- Example 1:

  Say: a, b, c – students, B, E, M, S, H – courses

  Each student takes every course.



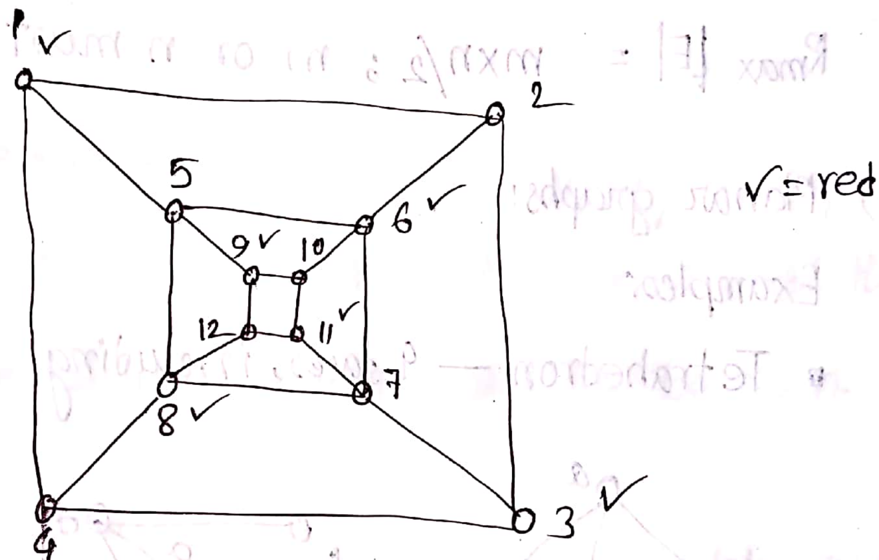
- A partition of V contains 2 sets, where no two elements at the same set are adjacent to each other.
- $K_{3,5}$: Complete bipartite ; $|E| = (5\times3 + 3\times5)/2 = 3\times5$

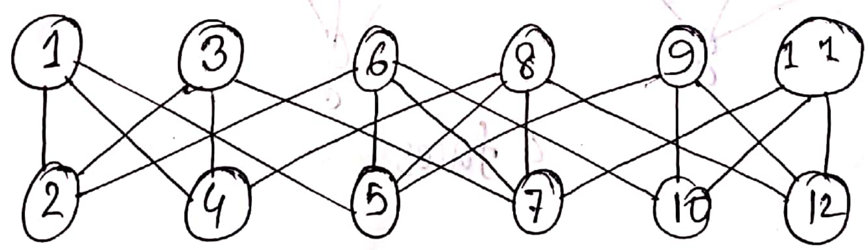
- To determine wheater a given graph is bipartite or not, coloring alternate vertex with same color may be applied.

28/03/2019

- **Example : 2**

3 concentric rectangles, having the corners of one connected to the corresponding corners at inner rectangles.





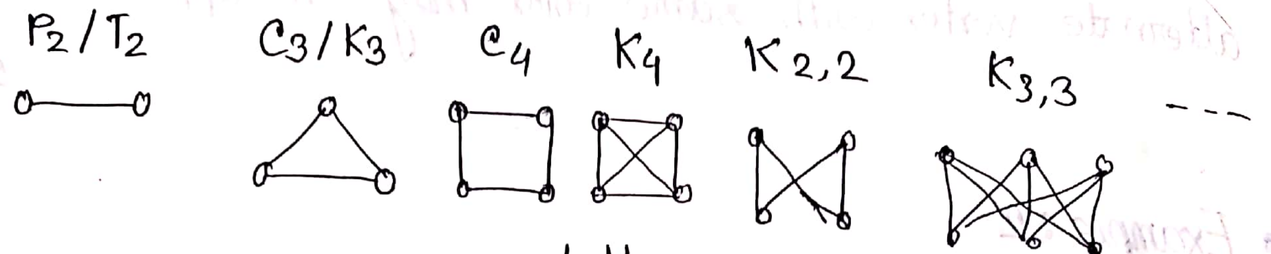
$V = \{1, 2, 3, \ldots, 12\}$

$V_1 = \{1, 3, 6, 8, 9, 11\}$

$V_2 = \{2, 4, 5, 7, 10, 12\}$

After coloring it is found that a partition of B contains 2 sets where no two elements at the same set are adjacent to each other. / Bipartite, but not complete.

(7) Regular graphs:



all the vertices are ~~in~~ of the same degree.

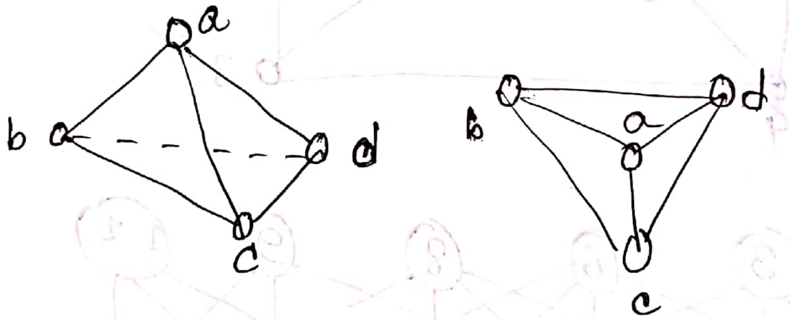
Degree = m, Vertices = n: m-regular with n vertices

R_{max} $|E| = m \times n / 2$; m or n must be even.

(8) Planar graphs:

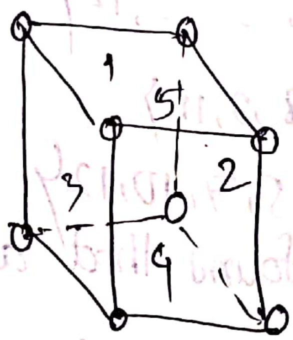
Examples:

- Tetrahedron — 4 faces, including an infinite face.



4 faces

- Cube — 6 faces



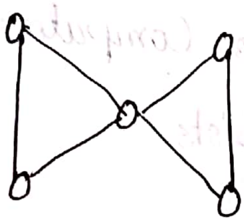
- C_3 — 2 faces

- Any tree — 1 face

✓ can be drawn on a 2D plane with crossing at a vertex only.

✓ Eulers formula for plannar graphs: $e = V + f - 2$

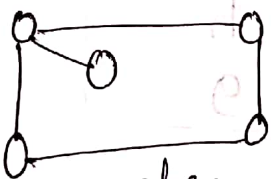
(9) Eulerian Graphs



✓ Eulerian circuit/cycle: Round tour / trial / walk that takes every edge once and visits all the vertices.

Degree at each vertex needs to be even.

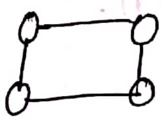
✓ Semi-Eulerian: The circuit is not complete, although each edge taken.

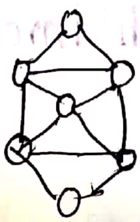


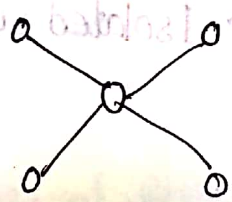
10) Hamiltonian graphs:

Hamiltonian circuit/cycle:

✓ Round tour that takes each vertex once

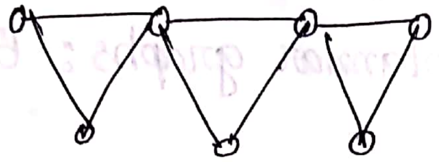






Both E & H

✓ Semi- Hemiltonian : Cycle not complete, althoug each vertex completed.

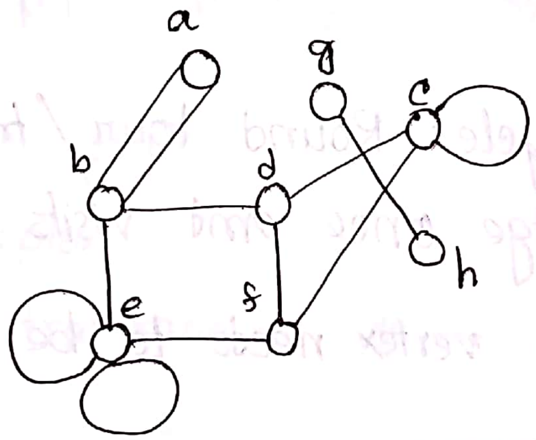


But Eulerian

Topic-5.3: Representation at Graphs in Computers.

01/04/19

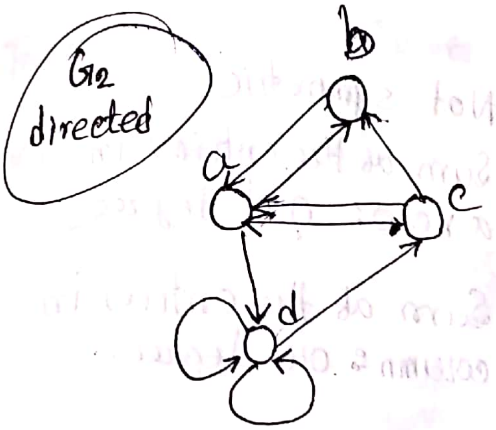
1) Representation using Adjacency Lists



vertex	adjacent vertices	vertex	adjacent verteces
a	b, b	e	b, e, e, f
b	a, a, d, e	f	e, d, e
c	c, d, f	g	h
d	b, c, f	h	g

• Multiple edges between a & b
• Loops : 3
• $|E| = (21+3)/2 = 12$ (edges)
• Isolated sub graph involving g & h.

Scanned by CamScanner



vertex	adjacent vertices
a	b, d
b	a
c	a, a, b
d	c, d, d

- $\sum$ in-degree $= 3+2+1+3 = 9$
- $\sum$ out-degree $= 2+1+3+3 = 9$
- $|E| = 9$

✓ Decisions from the lists: Loops, multiples edges, In-degree, Out-degree, Number of edges, Path / Tour / Cycle between vertices, isolated subgraph etc.

✓ appropriate algorithms are required.

2) Representation using adjacency matrices:

2 4 3 3 4 3 1 1

	a	b	c	d	e	f	g	h	
a	0	2	0	0	0	0	0	0	2
b	2	0	0	1	1	0	0	0	4
c	0	0	$\boxed{1}$	1	0	1	0	0	3 (deg 4)
d	0	1	1	0	0	1	0	0	3
e	0	1	0	0	$\boxed{2}$	1	0	0	4
f	0	0	1	1	1	0	0	0	3
g	0	0	0	0	0	0	0	1	1
h	0	0	0	0	0	0	1	0	1, diagonal loop

✓ Diagonal entries: Number of loops

✓ Simple graph: Completely Boolean and symmetric

✓ Other decisions based on sum of the entries in a row/column with special attention to diagonal entries.

G_2:

	a	b	c	d	
a	0	1	0	1	2
b	1	0	0	0	1
c	2	1	0	0	3
d	0	0	1	2	3
	3	2	1	3	

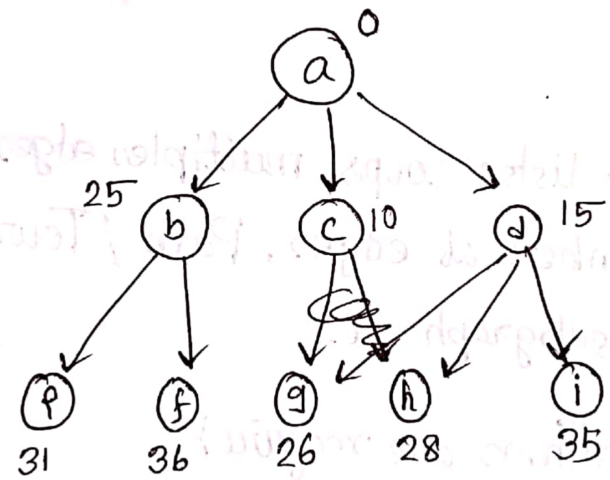
in-degree

out-degree

✓ Not symmetric
✓ Sum of the entries in a row: out degree
✓ Sum of the entries in column: out degree.

02.04.2019

3) Representation of Rooted trees.



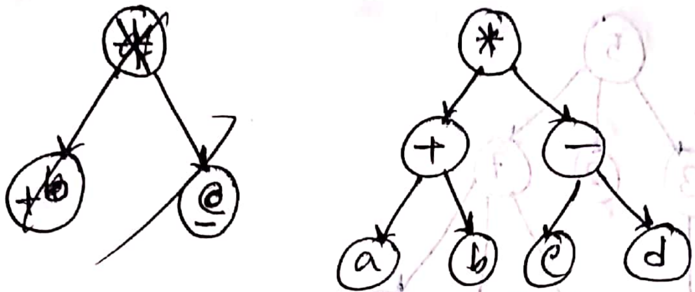
- Node: state
- Characteristics: Evaluation function value

Possible node structure:

Name	Parent	Characteristic
a	Null	0
b	a	25
c	a	10

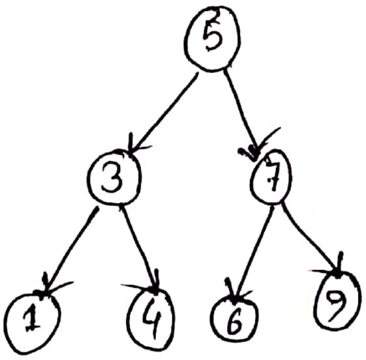
Topic 5.4: Tree Traversals and some use of trees

✓ we may have a binary tree to represent an arithmatic expression.



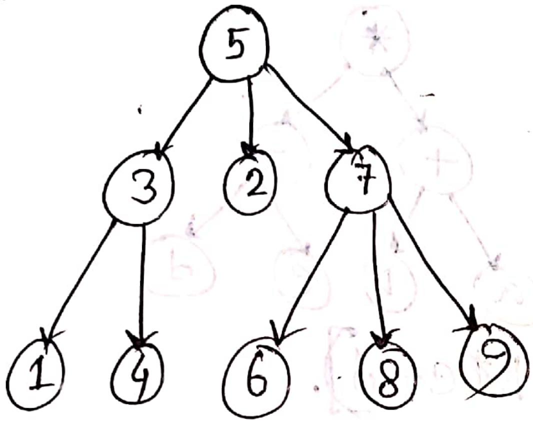
- in-order traversal yields [a+b*c−d].
- It stands for the infix notation (a+b)*(c-d)
- pre-order traversal yeilds [*+ab−cd]
- It stands for the prefix notation *(+(ab)-(cd))
- post-order traversal yeilds [ab+cd−*]
- It stands for the postfix notation ((ab)+(cd)−)*

✓ we may also think of a 'balanced' binary search tree holding search keys in an orderly fashion.



- We may now think of searching for say, 4 or 8.
- The search spaced is reduced to a great extent.

✓ We may think at a tree for visiting nodes in depth-first or breadth first fashion to search for a given value.



- Depth-first strategy yellds : 1, 4, 2, 6, 8, 9, 3, 7, 5
- Breadth-first strategy yeilds : 5, 3, 2, 7, 1, 4, 6, 8, 9

08.04.2019

Chapter: 6 – Algebraic structures and the theory of Groups

Topic 6.1: Basic concepts

✓ Algebra / Algebraic structure / Algebraic System

✓ Examples: $\langle Z, +, 0\rangle$, $\langle P(A), \cup, \cap, \phi, A\rangle$, $\langle R, +, \times, -, 0, 1\rangle$

✓ An algebra has

- a set, S, called the <u>carrier</u> of the algebra ; Z;
- one or more operations, o_i, such that $o_i : S^m \to S$ for $m \in Z$;
- usually, one or more constants, k_i, that are distinguished elements of S.

► And the ~~of~~ carrier is closed under all the operations of the algebra.

✓ signature of an algebra:

- Example: $\langle P(A), \cup, \cap, \phi, A\rangle$ and $\langle R, +, \times, 0, 1\rangle$ have the same signature.
- Number and arity of the operations, along with the constants define the signature of algebra.

✓ Sub algebra :

- Examples: $(N, +, 0)$ of $(Z, +, 0)$
  $(Z, \times, 1)$ of $(R, \times, 1)$
- The carrier is a subset
- The operation and constrains are 'similar'.

✓ Class of algebras

■ Examples:

Boolean algebras:

$\langle P(A), \cup, \cap, ', \phi, A \rangle$

$\langle \{F, T\}, \vee, \wedge, \neg, F, T \rangle$

- Have the same signature
- The operations obey the same axioms or rules like commutativety, associativity etc.

✓ Algebraic system involving common sets of numbers.

田 Natural number systems:

- $\langle N, +, \times, 0, 1 \rangle$
- Commutatively & Associatively of + & X, and Distributivity of X over +.
- Both sided identity elements for + and X.

田 System of integers:

- $\langle Z, +, \times, -, 0, 1 \rangle$
- commutativety & ......;
- Both sided identity elements...;
- Both sided additive inverse elements;

⑪ System of real number:

$\langle R, +, \times, -, ^{-1}, 0, 1 \rangle$ [$^{-1}$ not defined for 0]

commutativety --;

Both sided identity elements --;

Both sided additive inverse elements

Both sided multiplicative inverse element except for the number 0.

11.04.19

Topic-6.2: Elements of group theory

Applications: Coding theory, Higher physics & Mathematics.

A) semigroups:

✓ class of algebras of the form $\langle S, \circ \rangle$, where:

S - carrier, $\circ$ — binary

✓ Examples: $\langle N, + \rangle$, $\langle N, \times \rangle$, $\langle Z, + \rangle$, $\langle Z, \times \rangle$, $\langle R, + \rangle$, $\langle R, \times \rangle$

(not)

✓ Not examples: $\langle R, - \rangle$, where (−) ≡ denotes subtraction, $\langle R - \{0\}, / \rangle$, where (/) ≡ denotes division.

B) Monoids:

✓ Examples: $\langle N, +, 0 \rangle$, $\langle N, \times, 1 \rangle$, $\langle Z, +, 0 \rangle$, $\langle Z, \times, 1 \rangle$, $\langle R, +, 0 \rangle$, $\langle R, \times, 1 \rangle$

✓ class of algebras of the form $\langle S, \circ, i \rangle$, where:

i — both sided identity element for $\circ$.

Scanned by CamScanner

c) Groups:

unary minus

✓ class of algebras of the form $\langle S, \circ, ^{-}, i \rangle$, where $(^{-}) \equiv$ uniary operation that defines inverse elements for every element of S with respect to $\circ$.

✓ Examples: $\langle Z, +, -, 0 \rangle$, $\langle R-\{0\}, \times, ^{-1}, 1 \rangle$.

D) Isomorphic groups:

✓ Groups $\langle S_1, \circ_1, ^{-}_1, i_1 \rangle$ and $\langle S_2, \circ_2, ^{-}_2, i_2 \rangle$ are isomorphic if there is a bijection;

$f: S_1 \rightarrow S_2$, such that for any pair $x, y \in S_1$,

$f(x \circ_1 y) = f(x) \circ_2 f(y)$. [Operation preserving func]

✓ Example

$\langle Z, +, -, 0 \rangle$ and $\langle E, +, -, 0 \rangle$, where $E = \{0, 2, -2, 4, -4, \ldots\}$ are isomorphic for $f: Z \rightarrow E$ such that $f(n) = 2n$.

✓ The bijective function is called an isomorphism.

⊞ When the function f is not necessarily bijective, then the groups are called homomorphic.

⊞ If two groups are isomorphic, then they are homomorphic but not vice versa.

Scanned by CamScanner