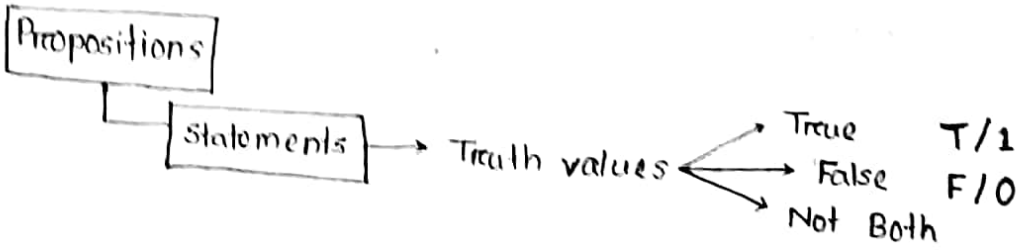
Discrete Mathematics

Reference Books:

(i) Discrete Math — 7th edition
Kenneth H. Rosen

Chapter 1:

The Fundamentals



propositional variables

P = {Donald Trump is a good guy}

x+y=z → not a proposition

but, x=2, y=3, z=5 then x+y=z is a proposition

(To convert a non-proposition into a proposition, we've to assign values to variables)

Propositional calculus:

Compound propositions

→ New propositions, are formed by combining one or more propositions

→ These are formed from existing propositions using logical operators

→ The newly formed propositions are termed as compound propositions.

Binary operators :

① AND / Conjunction

$p \wedge q$

② OR / Disjunction

$p \vee q$

Truth Table :

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0

③ Exclusive OR → only one of the variables is true

$p \oplus q$ then $p \oplus q$ is true

if both of them are ~~fa~~ true then $p \oplus q$ is false

Unary Operators :

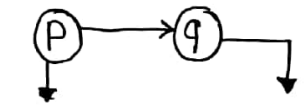
① Negation → $\neg p$

p	$\neg p$
0	1
1	0

Finding the combination for binary propositions

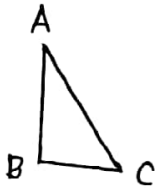
$= 2^n$

Conditionals / Implications :



hypothesis
antecedent
premise

consequence
conclusion



p = $AB^2+BC^2 > AC^2$

q = Right angle Δ

p	q	p→q
0	0	1
0	1	1
1	0	0
1	1	1

p → He is a lecturer.

q → He works at an educational institution

p→q

q follows from p

conclusion follows from hypothesis

(→) q unless (¬) ¬p

q if p

P only if q

hypothesis conclusion

p	q	p→q
0	0	1
0	1	1
1	0	0
1	1	1

p	q	p→q
0	0	1
0	1	1
1	0	0
1	1	1

Google classroom - ωu0kvfh

20 06 19

conditionals :

p = Richard learns Discrete Math

q = Richard will get a good job

$p \rightarrow q$

if (p) then (q)

if Richard learns discrete math, then he will get a good job

Equivalence :

if $(p \rightarrow q)$

- Inverse → $\neg p \rightarrow \neg q$
- converse → $q \rightarrow p$
- contrapositive → $\neg q \rightarrow \neg p$

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

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

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

① The home team wins whenever it is raining

q whenever p

② p = it is raining
q = The home team wins > $p \rightarrow q$

If it is raining then the home team win's.

③ Converse : $(q \rightarrow p)$ If the home team wins, then it is raining

Inverse : $(\neg p \rightarrow \neg q)$ If it is not raining, then the home team is not wins

contrapositive : $(\neg q \rightarrow \neg p)$ If the home team is not wins then it is not raining

Bi-conditionals :

[if and only if]

$p \longleftrightarrow q = p \rightarrow q$ and $q \rightarrow p$

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

p = you take the flight

q = you have to buy a ticket

$p \rightarrow q$: If you take the flight, you have to buy a ticket

$q \rightarrow p$: If you buy a ticket then you can take the flight

$p \leftrightarrow q$

You can take the flight if and only if you buy a ticket.

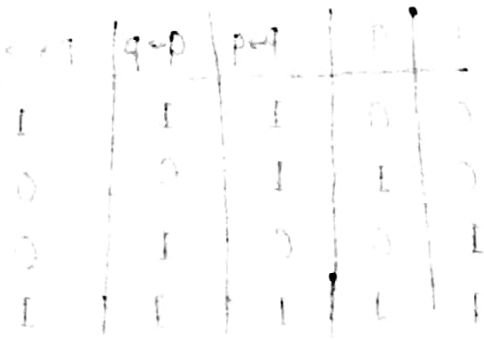
precedence of logical operators :

operators	precedence value	
$\neg$	1	→ Highest precedence
$\wedge$	2	
$\vee$	3	
$\rightarrow$	4	precedence $\propto \frac{1}{P_v}$
$\leftrightarrow$	5	

Bit- strings :

↳ a collection of 0 & 1

a :	101	1111	1111
b :	011	0101	0110
a^b :	001	0101	0110



Quiz # 01
3rd July
Topics : 1.1, 1.2
@ 2.00 pm

a : 1101
b : 0011

a ∧ b : 0001

a ⊕ b : 1110

—— x ——

25.06.19

Translate into logical expressions :

⟶ you can access the internet from campus only if you are a computer science major or you are not a freshman.

a = you can access the internet from campus

c = you are a cs major

f = you are a freshman

$a \rightarrow (c \vee \neg f)$

⟶ The automated reply cannot be sent when the file system is full.

r = automated reply can be sent

$\neg r$ = cannot be sent

$f \rightarrow \neg r$

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

r = you can ride the roller coaster

$\neg r$ = cannot

t = you are under 4 feet tall

o = you are older than 16 years old

for unless $\neg o$

$$(t \wedge \neg o) \rightarrow \neg r$$

- Consistent Systems :

→ should not contain conflicting requirements that could

p = buffer q = diagnostic

① $p \vee q$

② $\neg p$

③ $p \rightarrow q$

p	q	$p \vee q$	$\neg p$	$p \rightarrow q$
0	0	0	1	1
0	1	1	1	1
1	0	1	0	0
1	1	1	0	1

consistent.

* (i) $p \vee q$

(ii) $\neg p$

(iii) $p \rightarrow q$

(iv) $\neg q$

p	q	$p \vee q$	$\neg p$	$p \rightarrow q$	$\neg q$
0	0	0	1	1	1
0	1	1	1	1	0
1	0	1	0	0	1
1	1	1	0	1	0

not - consistent

* knights → always tell the truth

knaves → " lie

A → B is a knight

B → Two of us are opposite

p = A is a knight

q = B " " "

$\neg p$ = A " " knave

$\neg q$ = B " " "

(i) q

(ii) $(p \wedge \neg q) \vee (\neg p \wedge q)$

p	q	$\neg p$	$\neg q$	$p \wedge \neg q$	$\neg p \wedge q$	q	$(p \wedge \neg q) \vee (\neg p \wedge q)$
0	0	1	1	0	0	0	0
0	1	1	0	0	1	1	1
1	0	0	1	1	0	0	1
1	1	0	0	0	0	1	0

Sol^n : A is a knave ✗
B is a knight
contradictory

Sol^n : A is a knave ✓
B " " "

* S ⟶ son's muddy forehead

D ⟶ daughter's muddy forehead

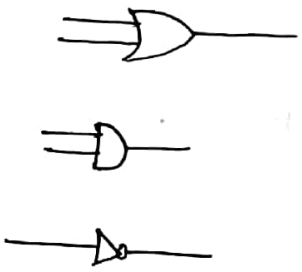
(i) S ∨ D

Logic Gates :

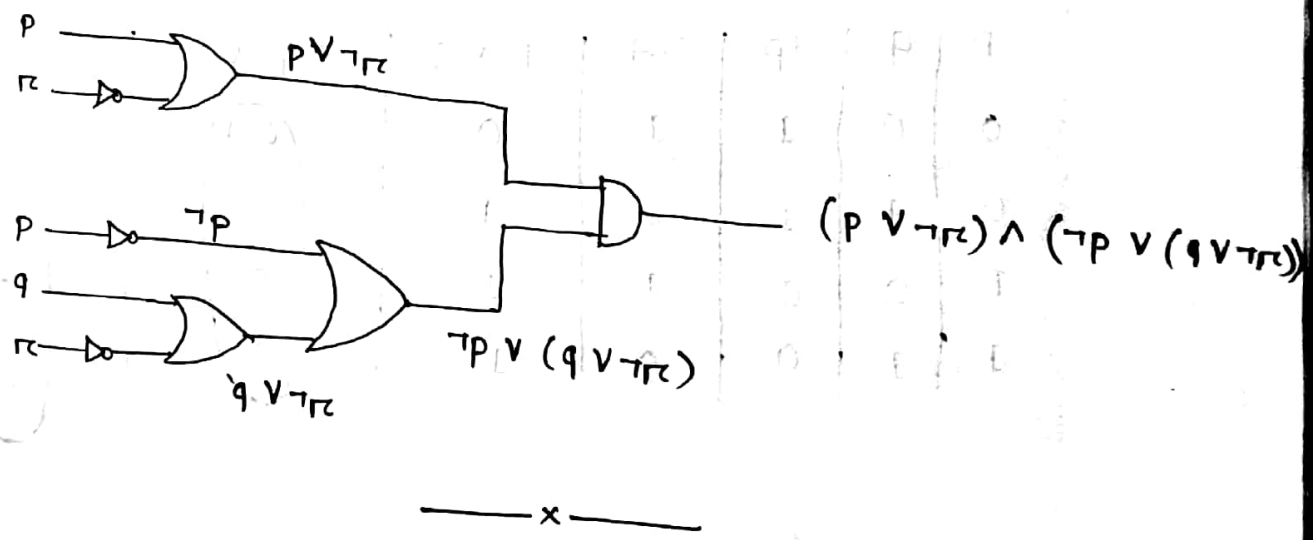
$\vee$ (Disjunction/OR)

$\wedge$

$\neg$



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



x

Propositional Equivalences : 02.07.19

Tautology Contradiction Contingency

$$\begin{matrix} T & & F \\ p & \vee & \neg p \\ F & & T \end{matrix} = T \quad \Big\} \text{ Tautology}$$

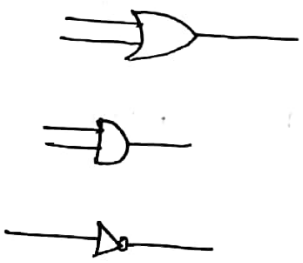
$$\begin{matrix} F & & T \\ p & \wedge & \neg p \\ T & & F \end{matrix} = F \quad \Big\} \text{ contradiction}$$

Logic Gates :

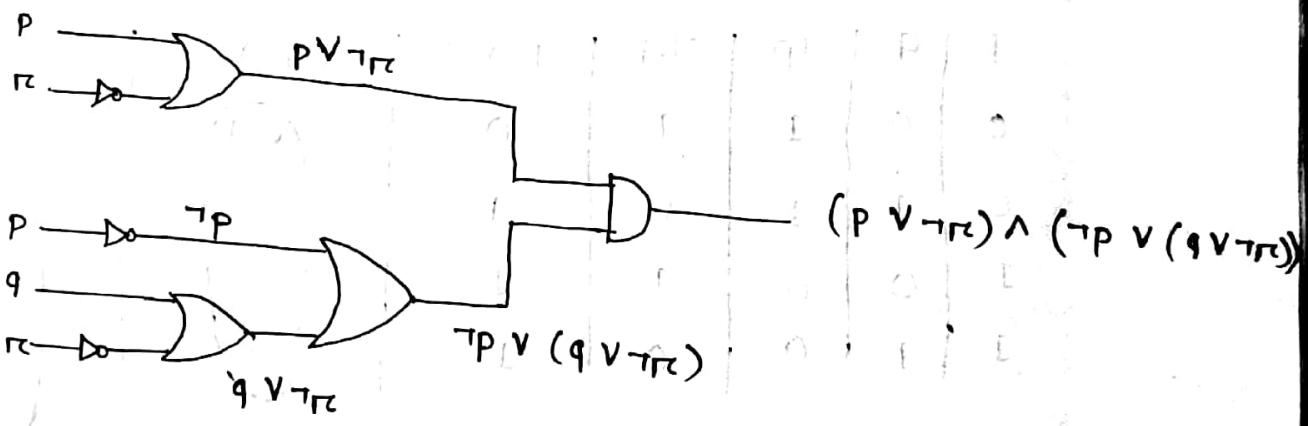
$\vee$ (Disjunction/OR)

$\wedge$

$\neg$



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



x

02.07.19

Propositional Equivalences :

Tautology Contradiction Contingency

$\overset{T}{p} \vee \overset{F}{\neg p} = T$ } Tautology

$\overset{F}{p} \wedge \overset{T}{\neg p} = F$ } contradiction

- The compound propositions p & q are called logically equivalent if $p \leftrightarrow q$ is a tautology
- The notation $p \equiv q$ denotes that p & q are logically equivalent.

• Show that $\neg(p \vee q)$ & $(\neg p \wedge \neg q)$ are logically equivalent.

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q)$	$(\neg p \wedge \neg q)$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

• $p \rightarrow q$ & $\neg p \vee q$

p	q	$p \rightarrow q$	$\neg p$	$\neg p \vee q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

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

p	q	r	$p \vee q$	$p \vee r$	$q \wedge r$	$p \vee (q \wedge r)$	$(p \vee q) \wedge (q \vee r)$
0	0	0	0	0	0		
0	0	1	0	1	0		
0	0	1	0	1	0		
0	1	1	1	1	1		
1	0	0	1	1	0		
1	0	1	1	1	0		
1	1	0	1	1	0		
1	1	1	1	1	1		

Identity Laws : $p \wedge T \equiv p$

$p \vee F \equiv p$

Domination Laws : $p \vee T \equiv T$

$p \wedge F \equiv F$

$p \wedge p \equiv p$

$p \vee p \equiv p$

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

$p \vee q \equiv q \vee p$

$p \wedge q \equiv$

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

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

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

$\equiv p \wedge \neg q$

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

$\equiv \neg p \wedge \neg(\neg p \wedge q)$ second de morgan law

$\equiv \neg p \wedge [\neg(\neg p) \vee \neg q]$ first " "

$\equiv \neg p \wedge (p \vee \neg q)$ double negation "

$\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q)$ second distributive "

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

$\equiv \neg p \wedge \neg q$

- $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

$\equiv \neg(p \wedge q) \vee (p \vee q)$ law of conditional

$\equiv (\neg p \vee \neg q) \vee (p \vee q)$ first de morgan

$\equiv (\neg p \vee p) \vee (\neg q \vee q)$ associative & commutative

$\equiv T \vee T$

$\equiv T$

Propositional Satisfiability :

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

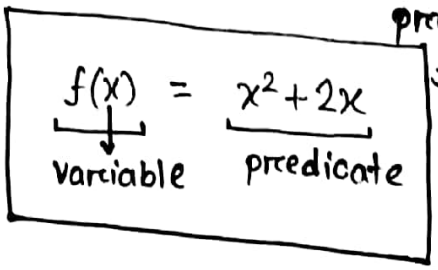
p	q	r	¬p	¬q	¬r

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

p	q	r	¬p	¬q	¬r	p ∨ q ∨ r	¬p ∨ ¬q ∨ ¬r	S
0	0	0	1					
0	0	1						
0	1	0						
0	1	1						
1	0	0						
1	0	1						
1	1	0						
1	1	1						

Predicates & Quantifiers :

- helps in converting a non propositional statement into a proposition.



pre-conditions & post-conditionals :

↓ valid inputs

↓ swap two values

```
x = a, y = b;
temp = x ;   → x = a, temp = a, y = b
x = y ;      → x = b, temp = a, y = b
y = temp ;   → x = b, temp = a, y = a
```

preconditions hold

postconditions hold

Quantification :

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

all, some, many, none and few

Universal Quantification

Extential "

$\forall$ – Universal quantifiers

$\exists$ – existential quantifiers

⑤

② ⟶ A^+ in DM

③ ⟶ A^+ in C } Existential $\exists x\ P(x)$

⑤ ⟶ B in TC — Universal

$\forall x\ P(x)$

$\forall x\ P(x)$ ⟵ (^)

- T for all
- F when a x for which P(x) is F

$\exists x\ P(x)$ ⟵ (v)

- T for at least 1 x
- F(x) is false for every x.

———x———

04.07.19

$\forall x\ P(x)$ — universal

$\exists x\ P(x)$ — existential

$P(x) = x<2 \quad ; x \in \mathbb{R}$

$\forall x\ P(x) \longrightarrow F$

$\exists x\ P(x) \longrightarrow T$

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

$P(x) = x^2 < 10$

$\forall x\ P(x) \longrightarrow F$

$\exists x\ P(x) \longrightarrow T$

Universal :

$$P(1) \wedge P(2) \wedge P(3) \wedge P(4)$$

Existential : $P(1) \vee P(2) \vee P(3) \vee P(4)$

- $N(x)$ = Computers x is connected to the network
  D_x = All computers

- $\forall$ & $\exists$ have higher precedence than all logical operators

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

$$= (\forall x\, P(x)) \vee Q(x)$$

- $P(x) \rightarrow x$ has taken a course in calculus

  $\forall x\, P(x) \rightarrow$ Every student is the class has . . . . .

Equivalent

Its not the case " " "

$$\neg \forall x\, P(x)$$

There is student in the class who has not taken a course in calculus.

$$\exists x \neg P(x)$$

Thus :

$$\boxed{\neg \forall x\, P(x) \equiv \exists x \neg P(x)}$$

There is a student in the class who has taken a course in calculus.

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

Equivalent:

It is not the case that " " " "

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

Every student in the class has not taken calculus.

$$\forall x \neg P(x)$$

$$\boxed{\neg \exists x\, P(x) \equiv \forall x \neg P(x)}$$

De Morgan's Law for quantification :

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

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

- There is an honest politician.

$H(x)$ = x is honest

$\exists x\, H(x)$ = There is an honest politician

$\downarrow$

$\neg \exists x\, H(x)$

$\equiv$

$\forall x \neg P(x)$ = All politicians are not honest

* $\neg \forall x (P(x) \rightarrow Q(x)) \equiv \exists x [P(x) \wedge \neg Q(x)]$

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

$= \exists x \neg [P(x) \rightarrow Q(x)]$ [De Morgan]

$= \exists x \neg (\neg P(x) \vee Q(x))$ [$P \rightarrow q \equiv \neg P \vee q$]

$= \exists x (\neg(\neg P(x)) \wedge \neg Q(x))$ [$(A \vee B)' = A' \wedge B'$]

$= \exists x (P(x) \wedge \neg Q(x))$

$P(x) \rightarrow$ students
- in your class (local domain)
- world (global domain)

11.07.19

• Some students in this class have visited Mexico.

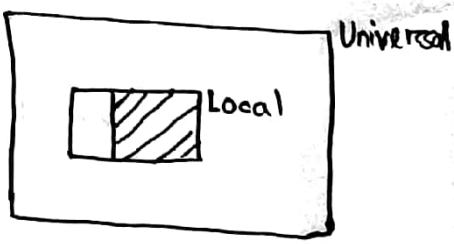
$P(x) = x$ (") have visited mexico.

$\exists x P(x)$

$S(x) = x$ is a student in this class.

$\exists x (S(x) \rightarrow P(x))$ ✗

✓ $\exists x (S(x) \wedge P(x))$



Existential

- Local → predicate represented as it is
- Universal
  - ⊢→ $\exists x$ (Domain $\wedge$ Predicate)

- Every student in this class has visited Mexico.

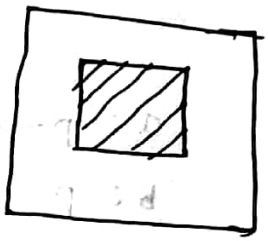
  $P(x)$ = student x has visited Mexico

  $\forall x (P(x)$ → Local

  $S(x)$ = student in this class

  $\forall x (S(x) \rightarrow P(x))$

  $\forall x$ (Domain → Predicate)



- Some student in this class have visited Canada ($C(x)$) or Mexico ($M(x)$).

Local → $\exists x (C(x) \vee M(x))$

Universal → $\exists x (S(x) \wedge (C(x) \vee M(x)))$ ($S(x)$)

For every student :

Local → $\forall x (C(x) \vee M(x))$

Universal → $\forall x (S(x) \rightarrow (C(x) \vee M(x)))$

16.07.19

Quiz #02

Next Thursday @ 2.00 pm

Syllabus : 1.3 — Upto this week.

Rules of inference :

infer

argument { ⓐ, ⓑ } — premises

ⓒ — conclusion

a = If you have access to the network, then you can browse the net

b = You have access to the net

p : you have access to the net

q : You can browse the net

a : $p \rightarrow q$

b : p

---

q (Modus ponens)

* $p = \sqrt{2} > \frac{3}{2}$

$q = (\sqrt{2})^2 > \left(\frac{3}{2}\right)^2$

a : $p \rightarrow q$

b : p

$\therefore q$

* It is below freezing point. Therefore it is either below freezing point or raining now.

p : It is below freezing point

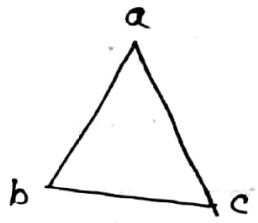
q : " raining.

$\frac{P}{P \vee q}$ Addition

* (i) $p \rightarrow q$

(ii) $q \rightarrow r$

$p \rightarrow r$ (Hypothetical syllogism)



$ab = ac$
$ac = bc$ } $ab = bc$

* (i) $\neg p \wedge q$

(ii) ~~$p \rightarrow r$~~ $r \rightarrow p$.

(iii) $\neg r \rightarrow t$

(iv) $t \rightarrow e$

$\neg p \wedge q$

Modus tollens { $\neg p$ (simplification)
$r \rightarrow p$

Modus ponens { $\neg r$
$\neg r \rightarrow t$

{ t
$t \rightarrow e$

e (Modus ponens)

* a = you send me an e-mail

b = I will finish writing the program

c = I will go to sleep early

d = I will wake up . . . .

(i) $a \rightarrow b$

(ii) $\neg a \rightarrow c$

(iii) $c \rightarrow d$

} conclusion : $\neg q \rightarrow s$

$p \rightarrow q$

$\neg q \rightarrow \neg p$ (contrapositive)

$\neg p \rightarrow r$

$\neg q \rightarrow r$ (hypothetical syllogism)

$r \rightarrow s$

$\neg q \rightarrow s$

"

—— x ——

Rules of Interference for Quantifiers: 23.07.19

$P(x) = x^2 < 10$

$D_1 = \{1, 2, 3\}$

$c \in D_1$

$\forall x\, P(x) \longrightarrow P(c)$ Universal instantiation

Universal generalization

$\exists x\, P(x) \longrightarrow P(c)$ Existential instantiation

Existential generalization

$D(x)$ = x has taken DM

$C(x)$ = x is in CSE

(i) $\forall x \left(D(x) \rightarrow C(x)\right)$

(ii) $D(\text{Marla})$

Quiz : 1.3 – 1.5

$\forall x\ (D(x) \rightarrow C(x))$

↳ $D(M) \rightarrow C(M)$

$D(M)$

$C(M)$

* $C(x) \rightarrow x$ is in the class

$B(x) \rightarrow x$ has read the book

$P(x) \rightarrow x$ passed the first exam

① $\exists x (C(x) \rightarrow \neg B(x))$

② $\forall x (C(x) \rightarrow P(x))$

$\exists x (C(x) \rightarrow \neg B(x))$

↳ $C(a) \wedge \neg B(a)$

↳ $C(a)$

↳ $\neg B(a)$

$\forall x (C(x) \rightarrow P(x))$

↳ $C(a) \rightarrow P(a)$

↳ $P(a)$

↳ $P(a) \wedge \neg B(a)$

↳ $\exists x (P(x) \wedge \neg B(x))$

$A = \{\}$ element = 0

$A' = \{\emptyset\}$ " = 1 ⟶ singleton set

Power set,

$A = \{1, 2\}$ $|A| = 2$

2^n

$n = 2$

↳ cardinality

$P(A) = \{\{1\}, \{2\}, \{1, 2\}, \emptyset\}$

Venn Diagram

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

cartesian product :

$a < b$

$A \times B = \{(1,3), (1,4), (4,3), (4,4)\}$

Representing a set :

① $A = \{1,4,9\}$ Roster method

② $A = \{x \mid x \in \mathbb{R} \text{ and } x^2 < 10\}$

set builder method

Set Operations :

25.07.19

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

$B = \{3,4,5\}$

$C = \{4,5,6\}$

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

$A \cap B = \{3\}$

$A \cap C = \emptyset$

Disjoint sets

$A - B = \{1,2\}$

$A - C = \{1,2,3\}$

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

if $x_i \in A$

$x_i \in U$

$A' = U - A$

$= \{4, 5, 6\}$

- Prove that, $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Let, $x \in \overline{A \cap B}$

$= x \notin A$ or $x \notin B$

$= x \in \bar{A}$ or $x \in \bar{B}$

$= x \in (\bar{A} \cup \bar{B})$.

$\therefore \overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$

computer representation :

$U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$|U| = 10$

(Odd) $O = \{1, 3, 5, 7, 9\}$

$E = \{2, 4, 6, 8, 10\}$

$U = 11111\ 11111$

$O = 10101\ 01010$

1.7 : Intro to proof

Axioms Lemma Corollary conjecture

Direct proof :

If n is odd, then n^2 is odd.

$n = 2k+1$

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

$= 4k^2+4k+1$

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

$= 2N+1$

———x———

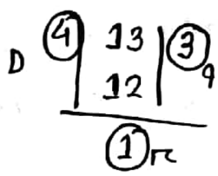
Number Theory & Cryptography : 03.09.19

Section-4.1

$12 = 4 \times 3$

Def^n-1 : $a, b \in \mathbb{Z}$ and $a \neq 0$ and there is an integer c such that $b = ac$ then a divides $b \rightarrow \frac{b}{a}$ or $a \mid b$

Def^n-2 :



Dividend $= Dq + r$

Def^n-3 : If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ then

$a \equiv b \pmod{m}$ if $m \mid (a-b)$

$101 \equiv 2 \pmod{11}$

$11 \mid (101-2) \Rightarrow 11 \mid 99$

Def^n-4: if $a, b \in Z$ and $m \in Z^+$ then

$a \equiv b \pmod{m}$ if & only if $[a \bmod m = b \bmod m]$

$101 \equiv 2 \pmod{11}$

$101 \% 11 = 2$

$2 \% 11 = 2$

$a \% m = b \% m$

Def^n-5: if $a, b \in Z$ and $m \in Z^+$ then a, b are congruent modulo m if there exists an integer k such that

$a = b + km$

$a \equiv b \Rightarrow m \mid (a-b)$

$a - b = km \rightarrow a = b + km$

Def^n-6: Let $m \in Z^+$ and $a \equiv b \pmod{m}$

$c \equiv d \pmod{m}$

then $(a+c) = (b+d) \pmod{m}$

$ac = bd \pmod{m}$

$a \equiv b \pmod{m}$ $\quad\quad$ $c \equiv d \pmod{m}$

$a = b + km$ — (i) $\quad\quad$ $c = d + k_2 m$ — (ii)

(i)+(ii)

$$a + c = (b + d) + (k_1 + k_2)m$$

$$\therefore (a + c) = (b + d) + Km$$

$$\Rightarrow (a + c) \equiv (b + d) \pmod{m}$$

(i)*(ii) :

$$ac = bd + (\quad) m$$

$$\Rightarrow ac = bd + km$$

$$\Rightarrow ac \equiv bd \pmod{m}$$

$$101 \equiv 2 \pmod{11}$$

$$102 \equiv 3 \pmod{11}$$

$$(101 + 102) \equiv (2 + 3) \pmod{11}$$

$$\Rightarrow 203 \equiv 5 \pmod{11}$$

$11 \mid 198$ $\quad$ $r = 0$, $q = 18$

Arithmatic Modulo :

Let, Z_m ∈ set of non-negative integers less than m

i.e $Z_m = \{0, 1, 2, \ldots, m-1\}$ then,

Addition = $a +_m b = (a+b) \pmod m$

Multiplication = $a \cdot_m b = (ab) \pmod m$

$7 +_{11} 9 = (7+9) \pmod{11}$

$= 16 \mod 11 = 5$

$7 \cdot_{11} 9 = 63 \mod 11 = 8$

Section - 4.2

Algorithm for binary addition :

$a = (1110)_2$

$b = (1011)_2$

$$\begin{array}{r} 1110 \\ 1011 \\ \hline (11001)_2 \end{array}$$

$\rightarrow a_0 + b_0 = c_0 \cdot 2 + s_0$

$0 + 1 = 0 \cdot 2 + 1$

$\rightarrow a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$

$1 + 1 + 0 = 1 \cdot 2 + 0$

$\rightarrow a_2 + b_2 + c_1 = c_2 \cdot 2 + s_2$

$1 + 0 + 1 = 1 \cdot 2 + 0$

$\left[a_n + b_n + c_{n-1} = c_n \cdot 2 + s_n \right]$

$\rightarrow a_3 + b_3 + c_2 = c_3 \cdot 2 + s_3$

$1 + 1 + 1 = 1 \cdot 2 + 1$

12/09/19

Section 4.2

Multiplication Algorithm :

$$
\begin{array}{r}
1\ 1\ 0 \\
\times\ 1\ 0\ 1 \\
\hline
1\ 1\ 0 \\
0\ 0\ 0\ 0 \\
1\ 1\ 0\ 0\ 0 \\
\hline
1\ 1\ 1\ 1\ 0
\end{array}
$$

$$ab = a\left(b_0 2^0 + b_1 2^1 + b_2 2^2 + \ldots\ldots + b_{n-1} 2^{n-1}\right)$$

$$= ab_0 2^0 + ab_1 2^1 + ab_2 2^2 + \ldots\ldots$$

$a = 110 \qquad b = 101$

$3 \mid 11 \mid 3$, 9, 2

$3 \mid -11 \mid -4$, -12, 1

$ab_0 2^0 \longrightarrow (110)_2 \cdot 1 \cdot 2^0 \longrightarrow (110)_2$

$ab_1 2^1 \longrightarrow (110)_2 \cdot 0 \cdot 2^1 \longrightarrow (0000)_2$

$ab_2 2^2 \longrightarrow (110)_2 \cdot 1 \cdot 2^2 \longrightarrow (11000)_2$

$(11110)_2$

Division Algorithm :

Let, $a, d \in \mathbb{Z}$ $d > 0$ then $q = d|a$ $r = a \bmod d$

$q = 0$

$r = |a|$

while $r \geq d$

$r = r - d$

$q = q + 1$

← if $a < 0$ & $r > 0$ then

$r = d - r$

$q = -(q+1)$

- Now $a = -11$ $d = 3$

$q = 0$ $r = |a| = 11$

$r > d$, → $r = r - d = 11 - 3 = 8$

$q = q + 1 = 1$

$r > d$, → $r = r - d = 8 - 3 = 5$

$q = q + 1 = 2$

$r > d$, → $r = r - d = 5 - 3 = 2$

$q = q + 1 = 3$

since $a < 0$ & $r > 0$ → $r = d - r = 3 - 2 = 1$

$q = -(q+1) = -4$

Section 4.6

Cryptography

→ Encryption

Decryption

Caesar's Cipher

↓

English Alphabets

key = 3

A, B, C, D . . . . . .
↓ ↓ ↓ ↓
D E F G . . . . .

value = position − 1

for A, v = 1 − 1
= 0

D = 3

HELLO
7 4 11 11 14

+3 → 10 7 14 14 17 ← −3

K H O O P

Encryption :

$$C = f(p) = (p+k) \bmod 26$$

Decryption :

$$p = f^{-1}(c) = (p-k) \bmod 26$$

Block Cipher

HELLO WORLD

Chunk Transposition function

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

(E)
$$\begin{cases} \sigma(1) = 4 \\ \sigma(2) = 3 \\ \sigma(3) = 1 \\ \sigma(4) = 2 \end{cases} \quad \Big| \quad \begin{cases} \sigma^{-1}(4) = 1 \\ \sigma^{-1}(3) = 2 \\ \sigma^{-1}(1) = 3 \\ \sigma^{-1}(2) = 4 \end{cases}$$ (D)

RSA
SHA

random

HELL OWOR LDAC

→ [illegible]

(E) → LLE H

(D) → HELL

———x———

Ch-5.1

17.09.19

Mathematical Induction

Used to prove statements that assert P(x) is true for all positive integers n, where P(x) is a propositional function.

P(x)

① → x = 1 —— (i)

② Suppose,

P(x) → x = m ∈ Z⁺ —— (ii)

③ P(x) → iff P(x) x = (m+1) ∈ Z⁺ —— (iii)

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

① P(n) is true for n = 1

LHS = 1 RHS = $\frac{1 \cdot 2}{2} = 1$

② Let, n = m ∈ Z⁺

$P(m) = 1+2+\ldots+m = \frac{m(m+1)}{2}$ —— (ii)

③ $P(n) \longrightarrow P(m+1)$ where $n=(m+1) \in Z^+$ is true.

$$P(m+1) = 1+2+\ldots+(m+1) = \frac{(m+1)(m+2)}{2} \quad \text{—— (iii)}$$

Adding $(m+1)$ with (ii) :

$$1+2+3\ldots+m+(m+1) = \frac{m(m+1)}{2} + (m+1)$$

$$\Rightarrow 1+2+3+\ldots+(m+1) = (m+1)\left(\frac{m}{2}+1\right)$$

$$= \frac{(m+1)(m+2)}{2}$$

• If $n \in Z$ show that $n < 2^n$

Proof by MI

① Let, $n=1$ $\quad 1 < 2^1 \longrightarrow 1<2$

② $n = m \in Z$ $\quad m < 2^m$ —— (ii)

③ $n = (m+1) \in Z$ $\quad P(m+1) \longrightarrow (m+1) < 2^{(m+1)}$ —— (iii)

Add 1 both sides of (ii) :

$$(m+1) < 2^m + 1$$

$$\Rightarrow (m+1) < 2^m + 2^m$$

$$\Rightarrow (m+1) < 2 \cdot 2^m$$

$$\Rightarrow (m+1) < 2^{(m+1)}$$

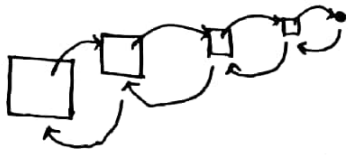
As, $1 < 2^1$

then $1 < 2^m$

$m = 1, 2, 3 \ldots \infty$

Ch - 5.3 :

Recursive Defⁿ :



→ Give a recursive defⁿ for computing GCD → HCF of two non-neg integeres a, b where a < b

a = 5
b = 8

$a_1 \rightarrow 5 \mid \overset{b_1}{\downarrow} 8 \mid 1$
5

$a_2 = b_1 \,\%\, a_1 \rightarrow 3 \mid 5 \mid 1$ → $b_2 = a_1$
3

$a_3 = b_2 \,\%\, a_2 \rightarrow 2 \mid 3 \mid 1$ → $b_3 = a_2$
2

$a_4 = b_3 \,\%\, a_3 \rightarrow 1 \mid 2 \mid 2$ → $b_4 = a_3$
2

0

$a_n = b_{n-1} \,\%\, a_{n-1}$

$b_n = a_{n-1}$

procedure gcd (a, b)
    if a == 0 return b
    else return gcd (b%.a, a)

→ 3! = 3 X 2 X 1 X 0!

0! = 1

n = n X (n-1)!

```
procedure fact (n)
        if n==0 return 1
        else return n * fact(n-1)
```

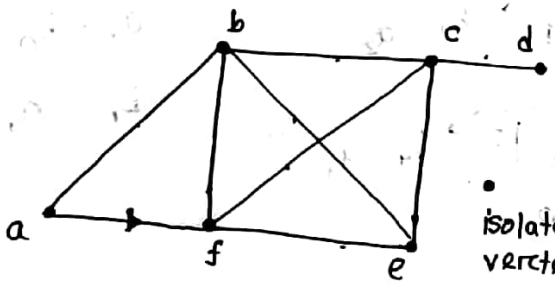
———— x ————

24.09.19

10.1 : Graphs and features

Def^n-1 : A Graph G1(V, E)

- V → set of ~~vel~~ vertices
- E → set of edges. Each edge has 1/two vertices called endpoints.



V = {a, b, c, d, e, f}

E = { (a, b), (a, f), (b, a) ~~(f, a)~~

Def^n-2 : Directed Graph

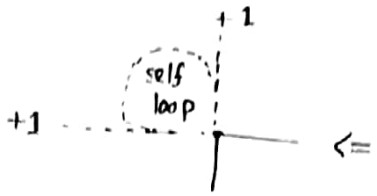
- V
- E

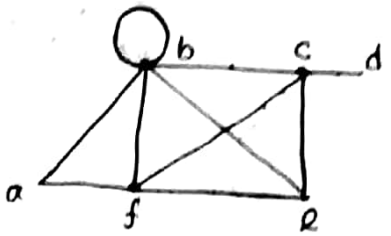
Adjacent nodes, N(a) → {f, b} (Neighbourhood)

N(f) → {a, b, c, e}

Degree of vertiex :

deg(b) = 4





$\therefore$ $Deg'(b) = deg(b) + 2$

(directed) V → starting point of an edge → (out degree) $deg^+(v)$

∴ end point of an edge → (in degree) $deg^-(v)$

Example (1):

$deg(a) = 2$
$deg(b) = 4$
$deg(c) = 4$
$deg(d) = 1$
$deg(e) = 3$
$deg(f) = 4$

} $\Sigma = 18$

Theorem - 1:

$$\sum_{v \in V} deg(v) = 2m$$ → number of edges

$\Rightarrow 18 = 2m \quad \Rightarrow m = 9$

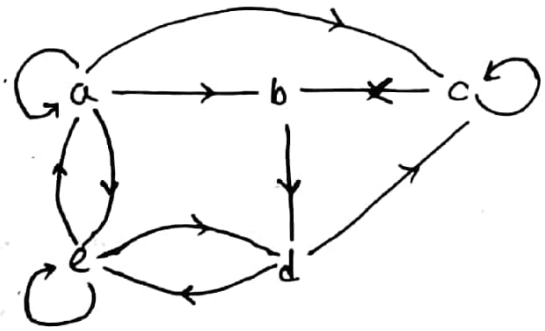
Theorem - 2: in any undirected graph $G(V, E)$, there will always be an even number of vertices with odd degree.

V < V_1 - even
V < V_2 - odd

e + o → o
e + e → e
o + o → e

$$\sum_{v \in V} \deg(v) = 2m$$

$$\sum_{v_1 \in V} \deg(v_1) + \sum_{v_2 \in V} \deg(v_2) = 2m$$



(v)	$\deg^-(v)$	$\deg^+(v)$
a	2	4
b	2	1
c	3	2
d	2	2
e	3	3
	12	12

Theorem – 3:

$$\sum \deg^-(v_i) = \sum \deg^+(v_i) = |E|$$

Types of graphs :

① Complete graphs ⟶ K_n ⟶ n = # of vertices

K_1 K_2 K_3 K_4

[All vertex will be connected with each other]

② Cycles ⟶ C_n ⟶ n = # of vertices, $n \geq 3$

[closed area]

n = 3

C_3

C_4

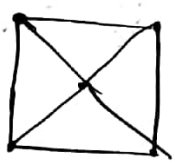
$V = \{a, b, c, d\}$

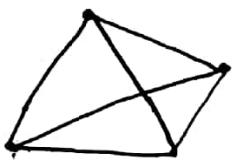
$= \{v_1, v_2, v_3, v_4\}$

$[V_{n-1}, V_n, V_{n+1}]$

relation

③ Wheels ⟶ $W_n = C_n + 1$

C_4  W_4

C_3  W_3

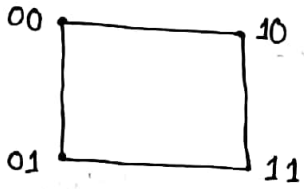
4. n - dim hyperc cubes

$Q_n \rightarrow V \rightarrow$ bit string $\rightarrow |bs| = n$

$|V| = 2^n$

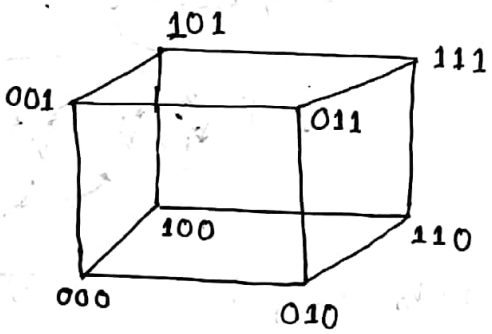
Adjacent vertices

$Q_2 \longrightarrow 2^2 = 4$



$Q_1 \longrightarrow 2^1 = 2$

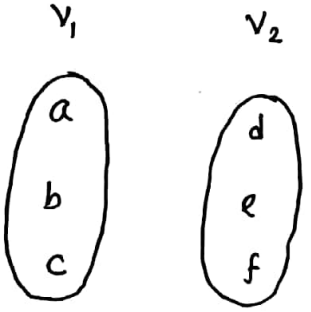
$Q_3 \longrightarrow 2^3 = 8$



5. Bipartite graphs

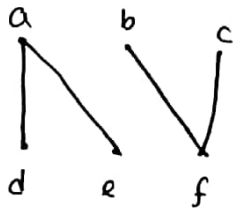
$V = \{a, b, c, d, e, f\}$

$V < V_1 \cap V_2 = \emptyset$



✓ interedges

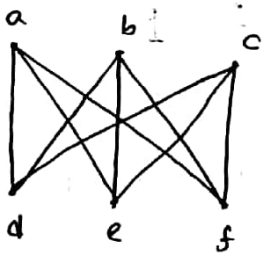
✗ intra edges



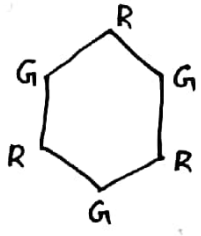
Complete bipartite graph :

$K_{m,n}$

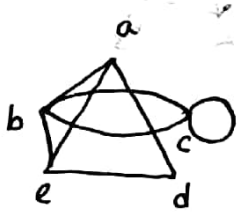
$K_{4,2}$

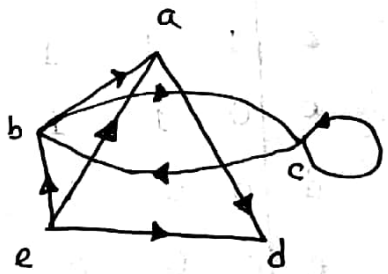


$K_{3,3}$



10.3 : Graph Representation :





Adjacency List :

(UG)

V_i	Adj Vertices
a	b, d, e
b	a, c, e, c
c	b, b, c
d	a, e
e	a, b, d

V_i	TV
a	d
b	a, c
c	b, c
d	—
e	a, b, d

(DG)

Adjacency Matrix : $|V| \times |V|$

UG :

	a	b	c	d	e
a	0	1	0	1	1
b	1	0	2	0	1
c	0	2	1	0	0
d	1	0	0	0	1
e	1	1	0	1	0

DG :

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

Incidence Matrix :

$|V| \times |E|$

	1	2	3	4	5	6	7	8
a	1	0	0	1	0	0	1	0
b	1	1	1	0	0	1	0	0
c	0	1	1	0	1	0	0	0
d	0	0	0	1	0	0	0	1
e	0	0	0	0	0	1	1	1