Discrete Structures

Discrete data
↳ distinct and seperate
↳ {1,2,3,4}
↳ no. of svojects

Continous Data
↳ measured on a scale
↳ [0 – 70]
↳ time in race

conjunctions(·): both propositions T or F

disjunction(∨): atleas one proposition T

exclusive(⊕): one T and one F (↗ xor)

implication(→): if P, then q

proposition: declarative sentence either true or false
e.g
↳ 1. read this carefully → not P
↳ 2. 1+2 =3 → P
↳ 3. ∩ +1 =2 → not P

- cant be partial T/F
- cant be both T/F

q if P
q when P
q unless ¬P
q whenever P
q is necessary P
sufficient condition q is p
follows
Provided

Implication Table

"if p, then q"	"p implies q"
"if p, q"	"p only if q"
"p is sufficient for q"	"a sufficient condition for q is p"
"q if p"	"q whenever p"
"q when p"	"q is necessary for p"
"a necessary condition for p is q"	"q follows from p"
"q unless $\neg p$"	

$P \rightarrow q$

37

↳ P iff q
↳ if P then q, conversly
↳ P is necessary and sufficient for q
↳ P if and only if q

T=F

P	q	and $P \wedge q$	or $P \vee q$	xor $P \oplus q$	implication $P \rightarrow q$	converse $q \rightarrow P$	contrapositive $\neg q \rightarrow \neg P$	inverse $\neg P \rightarrow \neg q$	bi-implications $P \leftrightarrow q$
T	T	T	T	F	T	T	T		T
T	F	F	T	T	F	T	F		F
F	T	F	T	T	T	F	T		F
F	F	F	F	F	T	T	T		T

→ opposite of xor

= = =

Precedence

1. ¬
2. ∧
3. ∨
4. →
5. ↔

- $(P \rightarrow Q) \equiv (\neg P \vee q)$

tautology: always T

contradiction: always F

contigiency: neither tautology or contradiction

contigiency tautology contradiction

P	¬P	P∨¬P	P∧¬P
T	F	T	F
F	T	T	F

Demorgans law: $\neg(p \wedge q) \equiv \neg p \vee \neg q$; $\neg(p \vee q) \equiv \neg p \wedge \neg q$

Commutative laws: $p \wedge q \equiv q \wedge p$; $p \vee q \equiv q \vee p$

Associative laws: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$; same with opposite operation

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

Identity laws: $p \wedge T \equiv p$ (T: true); $p \vee f \equiv p$ (f: false)

Negation laws: $p \vee \neg p \equiv T$; $p \wedge \neg p \equiv f$

Double negation laws: $\neg(\neg p) \equiv p$

Idempotent laws: $p \wedge p \equiv p$; $p \vee p \equiv p$

Universal bound laws: $p \vee t \equiv t$; $p \wedge F \equiv f$

Absorbtion laws: $p \wedge (p \vee q) \equiv p$; $p \vee (p \wedge q) \equiv p$

Negation of t and f: $\neg t \equiv f$; $\neg f \equiv t$

implication law: $p \rightarrow q \equiv \neg p \vee q$

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

Predicates: statements neither T or F

↳ u is an animal

Variables: x, y, z

Predicates: P(x), M(y)

Propositional functions

let $x + y = z$

$R(3,4,7) = F$

compound expressions (uses connectives ∨, ∧)

$P(x)$; $x > 0$

$P(3) \vee P(-1) = T$

but = ∧

Quantifiers

Universal (∀)

- for all / for every
- conjunctions T/F
- if domain empty the universal
- uses ∨ on ∧

Existential (∃)

- for some
- disjunctions atleast T
- uses ∨ on ∧

negating Quantifiers

not everybody — atleast one somebody

$\neg\forall n\, P(n) = \exists n\, \neg P(n)$

$\neg\exists n\, P(n) = \forall n\, \neg P(n)$

no one — everyone

start sentence with there is

TABLE 1 Quantifiers.

Statement	When True?	When False?
$\forall x P(x)$	$P(x)$ is true for every x.	There is an x for which $P(x)$ is false.
$\exists x P(x)$	There is an x for which $P(x)$ is true.	$P(x)$ is false for every x.

TABLE 2 De Morgan's Laws for Quantifiers.

Negation	Equivalent Statement	When Is Negation True?	When False?
$\neg\exists x P(x)$	$\forall x \neg P(x)$	For every x, $P(x)$ is false.	There is an x for which $P(x)$ is true.
$\neg\forall x P(x)$	$\exists x \neg P(x)$	There is an x for which $P(x)$ is false.	$P(x)$ is true for every x.

nested if's

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

RULES OF Interfernce

Premise: an asumption made to draw a conclusion

Conclusion: reached by given set of premises

$p \to q$

p

$\therefore q$ e.g

$((p \to q) \wedge p) \to q$ this is tautology

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
p $\therefore p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution

- always add '∧' when making tautology
- equate every line true
- if more than 1 implication make conslusion False
  - ↳ if unable to equate every premis T the conclusion valid

MODUS PONENS

Example:
Let p be "It is snowing."
Let q be "I will study discrete math."

"If it is snowing, then I will study discrete math."
"It is snowing."

"Therefore , I will study discrete math."

$$\begin{array}{l} p \to q \\ \underline{p \qquad} \\ \therefore q \end{array}$$

Corresponding Tautology:
$(p \wedge (p \to q)) \to q$

implication
S premise
S conclusion

MODUS TOLLENS

Example:
Let p be "it is snowing."
Let q be "I will study discrete math."

"If it is snowing, then I will study discrete math
"I will not study discrete math."

"Therefore , it is not snowing."

$$\begin{array}{l} p \to q \\ \underline{\neg q \qquad} \\ \therefore \neg p \end{array}$$

Corresponding Tautology:
$(\neg p \wedge (p \to q)) \to \neg q$

implication
¬S premise
¬S conclusion

HYPOTHETICAL SYLLOGISM

Example:
Let p be "it snows."
Let q be "I will study discrete math."
Let r be "I will get an A."

"If it snows, then I will study discrete math.'
"If I study discrete math, I will get an A."

"Therefore , If it snows, I will get an A."

$$\begin{array}{l} p \to q \\ \underline{q \to r \qquad} \\ \therefore p \to r \end{array}$$

Corresponding Tautology:
$((p \to q) \wedge (q \to r)) \to (p \to r)$

hence not valid as false so conclusion valid

multiple directly related implications
implication

DISJUNCTIVE SYLLOGISM

Example:
Let p be "I will study discrete math."
Let q be "I will study English literature."

"I will study discrete math or I will study English literature."
"I will not study discrete math."

"Therefore , I will study English literature."

$$\begin{array}{l} p \vee q \\ \underline{\neg p \qquad} \\ \therefore q \end{array}$$

Corresponding Tautology:
$(\neg p \wedge (p \vee q)) \to q$

connector
¬S premise
S conclusion

ADDITION

Example:
Let p be "I will study discrete math."
Let q be "I will visit Las Vegas."

"I will study discrete math."

"Therefore, I will study discrete math or I will visit Las Vegas."

$$\begin{array}{l} \underline{p \qquad} \\ \therefore p \vee q \end{array}$$

Corresponding Tautology:
$p \to (p \vee q)$

?? if i equate to false will work

S premise
OR

SIMPLIFICATION

Example:
Let p be "I will study discrete math."
Let q be "I will study English literature."

"I will study discrete math and English literature"

"Therefore, I will study discrete math."

$$\begin{array}{l} \underline{p \wedge q \qquad} \\ \therefore q \end{array}$$

Corresponding Tautology:
$(p \wedge q) \to p$

one connector
S conclusion

CONJUNCTION

Example:
Let p be "I will study discrete math."
Let q be "I will study English literature."

"I will study discrete math."
"I will study English literature."

"Therefore, I will study discrete math and I will study English literature."

$$\begin{array}{l} p \\ \underline{q \qquad} \\ \therefore p \wedge q \end{array}$$

Corresponding Tautology:
$((p) \wedge (q)) \to (p \wedge q)$

S premise
S premise
connector

RESOLUTION

Example:
Let p be "I will study discrete math."
Let r be "I will study English literature."
Let q be "I will study databases."

"I will not study discrete math or I will study English literature."
"I will study discrete math or I will study databases."

"Therefore, I will study databases or I will English literature."

$$\begin{array}{l} \neg p \vee r \\ \underline{p \vee q \qquad} \\ \therefore q \vee r \end{array}$$

Corresponding Tautology:
$((\neg p \vee r) \wedge (p \vee q)) \to (q \vee r)$

unable to prove hence valid

¬ connector
connector
connector

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\forall x\, P(x)$ $\therefore\ P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore\ \forall x\, P(x)$	Universal generalization
$\exists x\, P(x)$ $\therefore\ P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore\ \exists x\, P(x)$	Existential generalization

Solution: Let $C(x)$ be "x is in this class," $B(x)$ be "x has read the book," and $P(x)$ be "x passed the first exam." The premises are $\exists x(C(x) \wedge \neg B(x))$ and $\forall x(C(x) \rightarrow P(x))$. The conclusion is $\exists x(P(x) \wedge \neg B(x))$. These steps can be used to establish the conclusion from the premises.

Step	Reason
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	Existential instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	Existential generalization from (8)

◀

∀ ↓ everybody

∃ ↓ somebody

SETS

Set: unordered collection of objects

$a \in A$ — is an element of set A

$a \notin A$ — is not an element of set A

$S = \{a, b, c, d\}$ — order doesn't matter; elements/members

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

$\mathbb{Z}$ = integers $= \{\ldots, -3, -2, 1, 0, 1, 2, 3, \ldots\}$

$\mathbb{R}$ = real numbers

$\mathbb{R}^+$ = +ve real numbers

Universal Set U: contains everything

Empty Set: $\emptyset$ or $\{\}$

$\{\emptyset\} \neq \emptyset$

$|\emptyset| = 0$, $|\{6, 3, 8\}| = 3$ — number of elements

Subsets

- $A \subseteq B$ — subset: all elements of B are in A
- $A \not\subseteq B$ — not subset
- **Proper subset:** $A \subseteq B$ and $A \neq B$ (same number of elements)
- **Power sets:** the set of all subsets
  - ↳ if $A = \{a, b\}$
  - ↳ $P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

2-tuples: ordered pairs

↳ (a, b)

Cartesian Product

$A = \{a, b\}$, $B = \{1, 2, 3\}$

$A \times B = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3)\}$

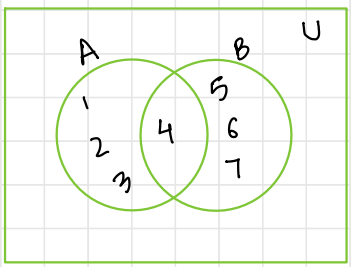
SET OPERATIONS

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

- Union '$\cup$' = combines
  - ↳ $A \cup B = \{1,2,3,4,5,6,7\}$
- Intersection '$\cap$' = common
  - ↳ $A \cap B = \{4\}$
  - ↳ if nothing common then $= \emptyset$
- complement '$\overline{set}$' = opposite
  - ↳ $\bar{A} = \{5,6,7\}$
- Difference 'SetA − setB' = remove all elements of setB from set A
  - ↳ $A - B = \{1,2,3\}$

Example: $U = \{0,1,2,3,4,5,6,7,8,9,10\}$ $A = \{1,2,3,4,5\}$, $B = \{4,5,6,7,8\}$

1. $A \cup B$
   Solution: $\{1,2,3,4,5,6,7,8\}$
2. $A \cap B$
   Solution: $\{4,5\}$
3. $\bar{A}$
   Solution: $\{0,6,7,8,9,10\}$
4. $\bar{B}$
   Solution: $\{0,1,2,3,9,10\}$
5. $A - B$
   Solution: $\{1,2,3\}$
6. $B - A$
   Solution: $\{6,7,8\}$



inclusion - exclusion

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

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

$A \cup \emptyset = A$ (empty set)	$A \cap U = A$ (universal)	identity law
$A \cap \emptyset = \emptyset$	$A \cup U = U$	domination law
$A \cup A = A$	$A \cap A = A$	idempotent law
$\overline{\bar{A}} = A$		complementation law
$A \cup B = B \cup A$	$A \cap B = B \cap A$	commutative law
$A \cup (B \cup C) = (A \cup B) \cup C$	$A \cap (B \cap C) = (A \cap B) \cap C$	Associative law
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) = A \cap (B \cup C)$		Distributive law
$\overline{A \cup B} = \bar{A} \cap \bar{B}$	$\overline{A \cap B} = \bar{A} \cup \bar{B}$	Demorgans law
$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$	Absorption law
$A \cup \bar{A} = U$	$A \cap \bar{A} = \emptyset$	Complement law
$A - B = A \cap \bar{B}$		

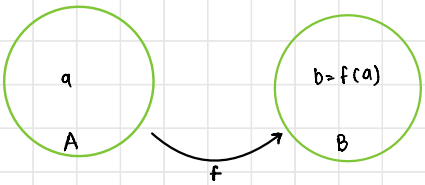
Functions

$A \to B$: f is mapping from A to B

A is domain

B is codomain

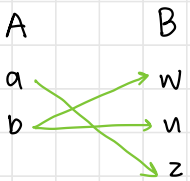
- if $f(a)=b$
  - ↳ b is image of a
  - ↳ a is preimage of b



Equal functions

- ↳ same domain — not equal w e domain changed
- ↳ same codomain — not equal we codomain changed
- ↳ each domain maps to corresponding codomain
  - not equal if mapping changed

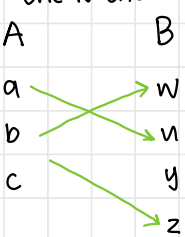
not a function



- domain has only one codomain

Injections

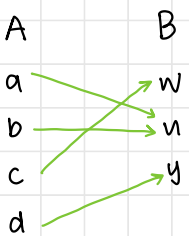
one to one



- all codomain dont need to be used
- no overlaping of codomains

Surjections

onto



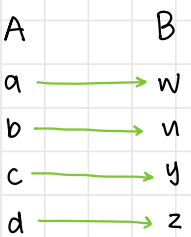
- all codomain elements used
- over laping of codomains

~not invertible~

no inverse

Bijections

one to one AND onto



- all codomain used
- no codomain overlaping

~invertible~

inverseible

inverse functions

- inverse dosent exist unless bijection

$f(x) = x+1$

let $x = y$

$x = y+1$

$y = x-1$

switch

$f^{-1}(x) = y-1$

COMPOSITION

$f(x) = x^2$, $g(x) = 2x+1$

$f(g(x)) = ?$ $\quad$ $g(f(x)) = ?$

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

$(2x+1)^2$ $\quad$ $2x^2+1$

floor function

$f(x) = \lfloor x \rfloor$

↳ $\lfloor 3.5 \rfloor = 3$

↳ $\lfloor -1.5 \rfloor = -2$

Celing function

$f(x) = \lceil x \rceil$

↳ $\lceil 3.5 \rceil = 4$

↳ $\lceil -1.5 \rceil = -1$

Increasing/ decreasing functions

- A function f is
  - increasing if $\forall x \forall y (x < y \rightarrow f(x) \leq f(y))$,
  - strictly increasing if $\forall x \forall y (x < y \rightarrow f(x) < f(y))$,
  - decreasing if $\forall x \forall y (x < y \rightarrow f(x) \geq f(y))$,
  - strictly decreasing if $\forall x \forall y (x < y \rightarrow f(x) > f(y))$,

where the universe of discourse is the domain of f.

- Strictly increasing/decreasing function is one to one/injective

ishma Hafeez notes

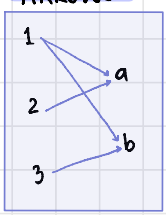
RELATIONS

Binary Relations

A = {1, 2, 3} B = {a, b}

A B relation: {(1,a), (1,b), (2,a), (3,b)}

ARROWS



TABLE

R	a	b
1	X	X
2	X	
3		X

Domain and Range

- domain: all first set values of ordered pairs
- range: all second set values of ordered pairs

EXERCISE:

Let A = {1, 2}, B = {1, 2, 3},

Define a binary relation R from A to B as follows:

R = {(a, b) ∈A × B | a < b} Then

- a. Find the ordered pairs in R.
- b. Find the Domain and Range of R.
- c. Is 1R3, 2R2?

SOLUTION:

Given A = {1, 2}, B = {1, 2, 3},

A × B = {(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)}

- a. R = {(a, b) ∈A × B | a < b}

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

b. Dom(R) = {1,2} and Ran(R) = {2, 3}

c. Since (1, 3)∈R so 1R3.

Since (2, 2)∈R so 2R2.

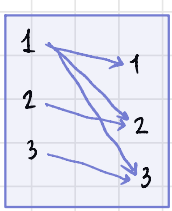
Relations on sets

a relation on a set A is a relation from A to A

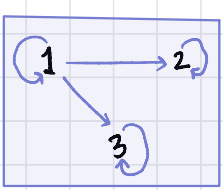
e.g A = {1,2,3} R = {(a,b) | a divides b}

condition 1 condition 2

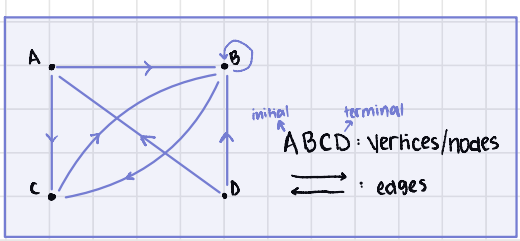
R = {(1,1), (1,2), (1,3), (2,2), (3,3)}



R	1	2	3
1	X	X	X
2		X	
3			X



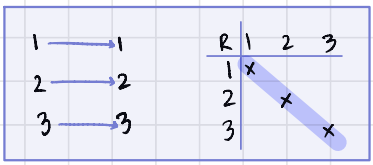
Directed graph



Properties of relations

1. Reflexive relation

- all elements pair with themselves: $\forall a((a,a) \in R)$
- if $A \neq \emptyset$ then reflexive

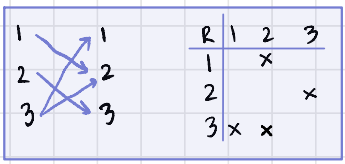


• all diagonals filled

✓ R1 = {(1, 1), (3, 3), (2, 2), (4, 4)}
✗ R2 = {(1, 1), (1, 4), (2, 2), (3, 3), (4, 3)}
✓ R3 = {(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)}
✗ R4 = {(1, 3), (2, 2), (2, 4), (3, 1), (4, 4)}

2. Irreflexive relation

- no same pair element
- $\forall a((a \in R) \rightarrow (a,a) \notin R)$

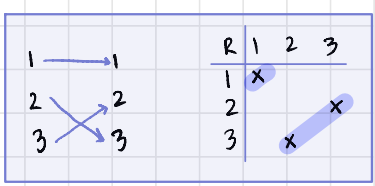


• no diagonals filled

✓ R1 = {(1,3), (1,4), (2,3), (2,4), (3,1), (3,4)}
✗ R2 = {(1,1), (1,2), (2,1), (2,2), (3,3), (4,4)}
✗ R3= {(1,2), (2,3), (3,3), (3,4)}

3. Symmetric relation

- bidirectional
- $\forall a \forall b [(a,b) \in R \rightarrow (b,a) \in R]$



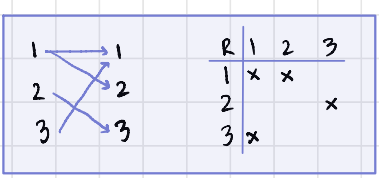
• all across

✓ R1 = {(1, 1), (1, 3), (2, 4), (3, 1), (4,2)}
✓ R2 = {(1, 1), (2, 2), (3, 3), (4, 4)}
✗ R3 = {(2, 2), (2, 3), (3, 4)}
✗ R4 = {(1, 1), (2, 2), (3, 3), (4, 3), (4, 4)}

1. ↔
2. ⇆

4. Antisymmetric relation

- non bidirectional unless of same element
- $\forall a \forall b [((a,b) \in R \wedge (b,a) \in R) \rightarrow (a == b)]$

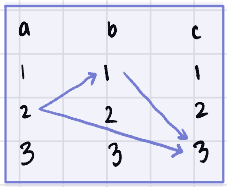


✓ R1 = {(1,1),(2,2),(3,3)}
✓ R2 = {(1,2),(2,2), (2,3), (3,4), (4,1)}
✗ R3={(1,3),(2,2), (2,4), (3,1), (4,2)}
✗ R4={(1,3),(2,4), (3,1), (4,3)}

1. ⇄ ✗
2. ↔ ✓

6. Transisitive relation

- makes a triangle
- a → b → c
- $\forall a \forall b \forall c [((a,b) \in R \wedge (b,c) \in R) \rightarrow (a,c) \in R]$



first check if both true

- (a,b) (b,c) (a,c)
- (a,b) ? = Transisitive
  - T
  - cant find pair

check for false

(a,b) (b,c) but no (a,c) ✗

if false not satisfying then ✓

(1,2) (2,3) (1,3) T

(1,2) (2,3) (4,8) F

(1,2) (3,4) (5,6) T → no pair hence true

(3,4): ?

(5,6): dont care

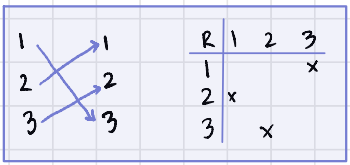
✓ R1 = {(1, 1), (1, 2), (1, 3), (2, 3)}

✗ R2 = {(1, 2), (1, 4), (2, 3), (3, 4)} no (1,3)

✓ R3 = {(2, 1), (2, 4), (2, 3), (3,4)} no (a,b)(b,c) relation hence no need to check false

5. Asymmetric relation

- not bidirectional even if same element
- $\forall a \forall b [((a,b) \in R \rightarrow (b,a) \notin R)]$



✗ R1 = {(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)}

✓ R2 = {(1,2),(2,3),(3,4)}

✗ R3 = {(2,3),(3,3),(3,4)}

1. ↔ x
2. ⇄ x

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

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

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

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

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

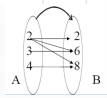
$R_6 = \{(3, 4)\}$. Irreflexsive , Antisymmetric , Asymmetric

Combining Relations

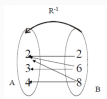
- Union (U)
- Intersection (∩)
- Difference (-)
- Symmetric Complement (⊕)

Inverse of Relation

The relation
R = {(2,2), (2,6), (2,8), (3,6), (4,8)} is represented by the arrow diagram.



Then inverse of the above relation can be obtained simply changing the directions of the arrows and hence the diagram is



Combining Relations

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

R_1 = {(1,1),(2,2),(3,3)},

R_2 = {(1,1),(1,2),(1,3),(1,4)}

- $R_1 \cup R_2$ = {(1,1),(1,2),(1,3),(1,4),(2,2),(3,3)}
- $R_1 \cap R_2$ = {(1,1)}
- $R_1 - R_2$ = {(2,2),(3,3)}
- $R_2 - R_1$ = {(1,2),(1,3),(1,4)}
- $R_1 \oplus R_2$ = {(1,2),(1,3),(1,4),(2,2),(3,3)} → all values of both except common

compliment of common

Equivalence Relation

↳ reflexsive

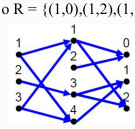
↳ symmetric

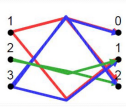
↳ transisitive

Composition of relation

What is the composite of the relations R and S, where

- R is the relation from {1,2,3} to {1,2,3,4} with R = {(1,1),(1,4),(2,3),(3,1),(3,4)}
- S is the relation from {1,2,3,4} to {0,1,2} with S = {(1,0),(1,2),(2,0),(3,1),(3,2),(4,1)}?
- S o R = {(1,0),(1,2),(1,1), (2,2),(2,1), (3,0),(3,2),(3,1)}





no repetition

Partial ordering

↳ Reflexsive

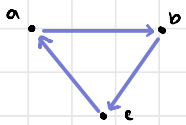
↳ Anti symmetric

↳ Transisitive

GRAPHS

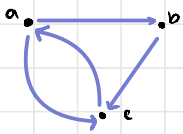
SIMPLE GRAPHS

- no same node edges
- no loop



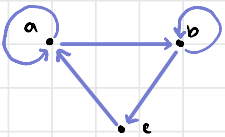
MULTIPLE GRAPHS

- same edges of same nodes



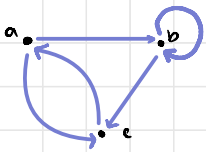
LOOP

- node connects to itself

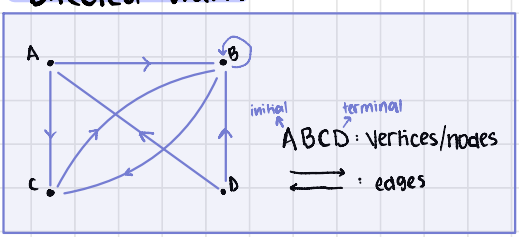


PSEUDOGRAPH

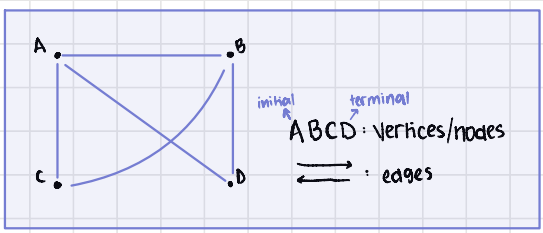
- loops and multiple same node edges



Directed graph



Undirected graph

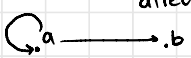


total edges = $\Sigma^{-}(v) + \Sigma^{+}(v)$

indegree = deg⁻(v) $\quad$ ⁻a: 1 $\quad$ ⁻b: 4

outdegree = deg⁺(v) $\quad$ ⁺a = 2 $\quad$ ⁺b: 2

directed

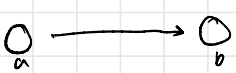


$\deg^{+}(a) = 2$

$\deg^{-}(a) = 1$

$\deg^{-}(b) = 1$

initial



goes out ← out ← $\deg^{+}(a) = 1$

goes in ← in ← $\deg^{-}(b) = 1$

undirected

$\deg(a) = 2$

TABLE 1 Graph Terminology.

Type	*Edges*	*Multiple Edges Allowed?*	*Loops Allowed?*
Simple graph	Undirected	No	No
Multigraph	Undirected	Yes	No
Pseudograph	Undirected	Yes	Yes
Simple directed graph	Directed	No	No
Directed multigraph	Directed	Yes	Yes
Mixed graph	Directed and undirected	Yes	Yes

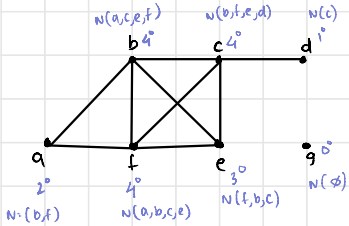
applications of graph

- Social networks
- Communications networks
- Information networks
- Software design
- Transportation networks
- Biological networks

DEGREE / NEIGHBOURS

degree: no of edges connected to node

neighbours: joined edges nodes



HANDSHAKING THEOREM

COMMING IN PAPER

if g is a graph

each degree x total nodes = 2 x total edges

total degree * total nodes = total edges

always even ↙ else graph dosent exist

Corollary: total degree of g is even

undirected graph has even nodes

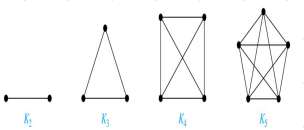
each ↖ $d \times n = 2e$

total ↙ $d \times n = e$

SPECIAL TYPES OF SIMPLE GRAPHS

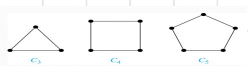
Complete graph

- one edge between nodes
- all connected



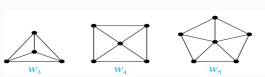
Cycles

- nodes >= 3



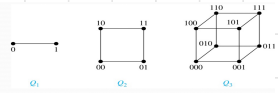
Wheels

- adding a node to cycle
- this node connects all nodes



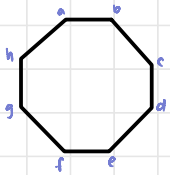
n-cubes

- edge b/w two nodes differs with 1 bit position



Bipnaite graph

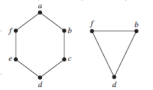
- neighbour nodes in other partition

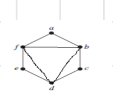


P_1	P_2
a	b
g	h
e	f
c	d

Union

is combining two graphs

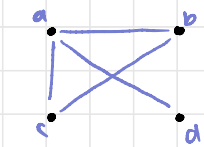




ADJACENCY MATRICES

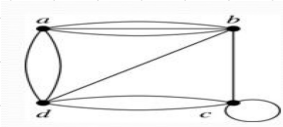
- which vertices are neighbours

adjacency list



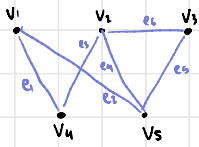
if directed count going out only

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



$$\begin{bmatrix} 0 & 3 & 0 & 2 \\ 3 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 2 & 0 \end{bmatrix}$$

INCIDENCE MATRICE



edges

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

vertices

Path

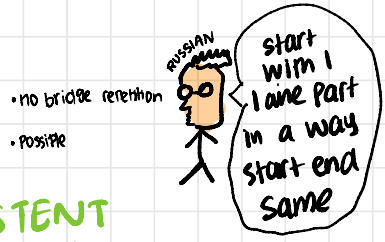
touch all vertices

Simple Path

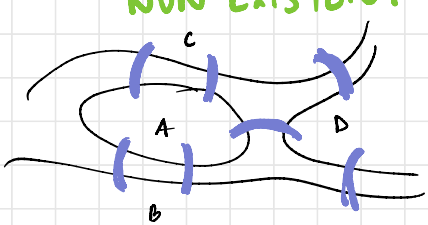
- no repeated vertice
- touches all vertices

circuit

- touches all vertices
- ends where it starts



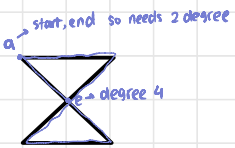
NON EXISTENT



Euler Circuit

- cover all edges once
- cover all vertexes
- repeated vertices allowed
- end where start

- all vertices degree even

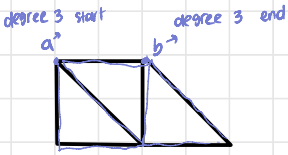


Euler Path → edges

- cover all edges once
- cover all vertexes
- repeated vertices allowed

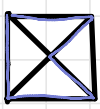
- all vertices degree even
- star and end degree 3

check with degree for euler



Hamilton Circuit

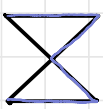
- cover all vertex once
- end where start



Hamilton Path → vertices

always make for hamilton

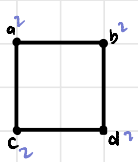
- cover all vertex once
- dont end where start

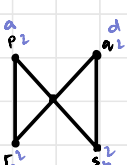


Isomorphisim

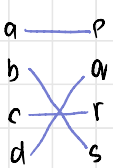
→ 2 WEITAGE QUESTION

- same vertices
- same edges
- same degree vertices
- same max min length
- is connected
- has Euler and Hamilton circuit



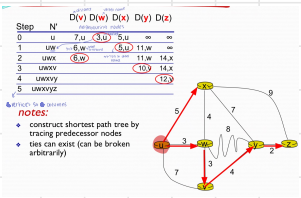


4 vertices
max length = 4
min length = 4



WEIGHTED GRAPH

Dijkstra's Algorithm

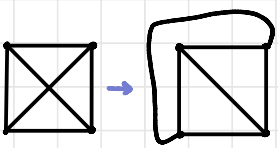


Step	N'	D(v)	D(w)	D(x)	D(y)	D(z)
0	u	7,u	(3,u)	5,u	∞	∞
1	uw	6,w		(5,u)	11,w	∞
2	uwx	(6,w)			11,w	14,x
3	uwxv				(10,v)	14,x
4	uwxvy					(12,y)
5	uwxvyz					

notes:
- construct shortest path tree by tracing predecessor nodes
- ties can exist (can be broken arbitrarily)

Planar graphs

↳ no edge crossing



even if edge crossing exists it can still be considered planar graph as it can be drawn another way with no edge crossings

if Complete graph
↳ all vertices connected once

↳ $n \geq 4$ then planar

disconnect → check every value

self loop remove

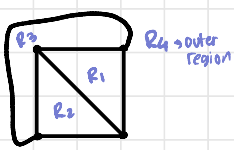
same edges remove

a→b b→c a→c line

Regions

↳ sections

regions: $r = e - v + 2$ (e: edges, v: vertex)



Tree

↳ no loops

↳ connected

↳ unique paths → no multiple edges

↳ no circuit

↳ undirected

Graph

↳ has loop

↳ connected

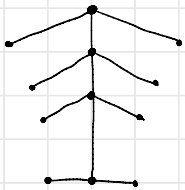
↳ same path exist

↳ circuit

Forest

↳ no simple circuit

↳ not connected



Trees applications

↳ chem bonds

↳ file directories

↳ organise

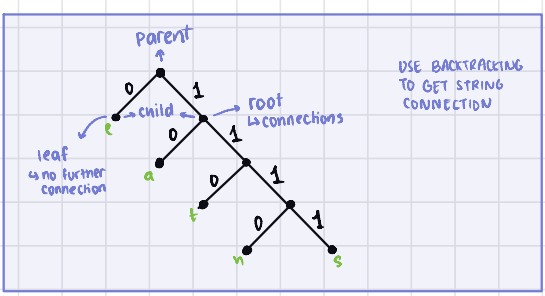
↳ Tik Tac Toe

Prefix code

↳ when char comes

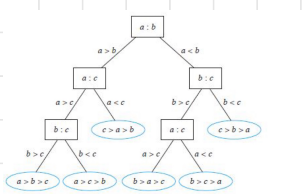
make leaf on left, edge = 0

↳ make root on right, edge = 1



Decision Tree

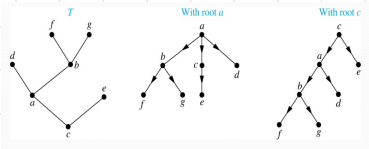
↳ start with one root

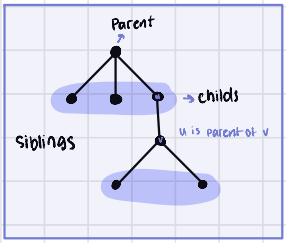


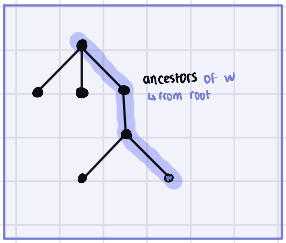
Rooted Tree

↳ one root only

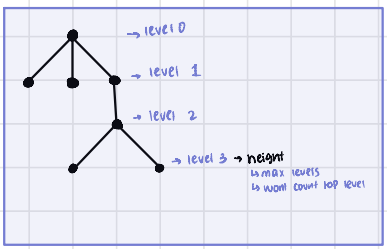
↳ all edges direct away from root

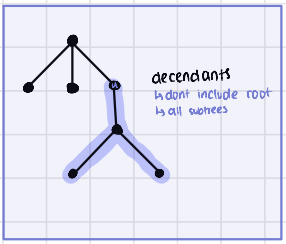


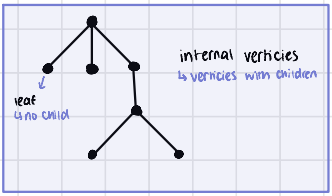




edge: vertices - 1

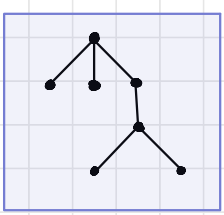






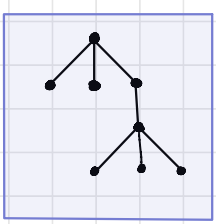
m-ary rooted tree

↳ every internal vertex has <= m children



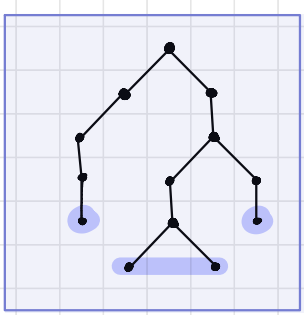
full m-ary tree

↳ every internal vertex has exactly m children



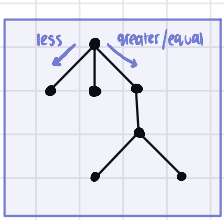
balanced m-ary tree

↳ all leaves are at height h or h-1



Ordered root tree

↳ children are ordered



Binary Tree → WILL COME

- ordered 2 m-ary root tree
- left children: left subtree
- right children: right subtree

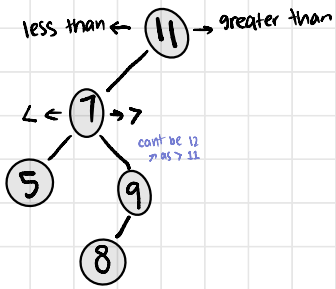
edges, vertices
$e = n - 1$

internal vertices
full m-ary $n = mi + 1$

$e = \frac{n-1}{i}$

Binary Search Tree

2-m-ary

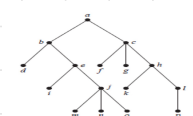


TREE TRAVERSAL

Preorder

- root
- left
- right

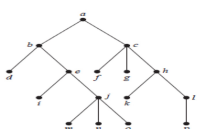
Preorder: a b d e i j m n o c f g h k l p



Inorder

- left leaf
- root
- right

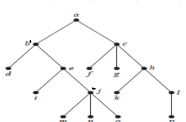
Inorder: d b i e m j n o a f c g k h p l



Postorder

- left leaf
- right leaf
- root

Postorder: d i m n o j e b f g k p l h c a



Expressions Tree

Power
$2 \uparrow 3 = 2^3 = 8$

$((x + y) \uparrow 2) + ((x - 4)/3)$ infix notation

$+ \uparrow + x\ y\ 2\ /\ -\ x\ 4\ 3.$ Prefix notation

move to arithmetic to the left
move left to right

$((x + y) \uparrow 2) + ((x - 4)/3)$ infix notation

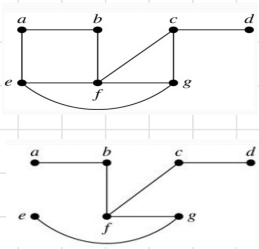
$x\ y + 2 \uparrow x\ 4 - 3\ / +$ Postfix

move arithmetic to the right
move right to left

Spanning Tree

- ↳ connected (every vertex reachable)
- ↳ min edges possible
- ↳ no cycle 
- ↳ not form simple circuit

$e = V - 1$ (edges = vertex − 1)



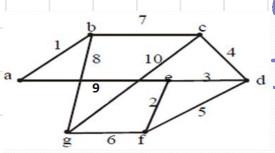
minimum spaning tree

- ↳ connected weighted graph
- ↳ smallest sum of weights of edges

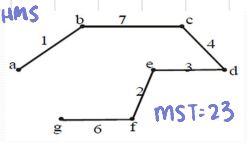
prims algorithm

- ↳ start with any vertex
- ↳ draw smaller adjacent node
- ↳ move connectedly
- ↳ no cycles

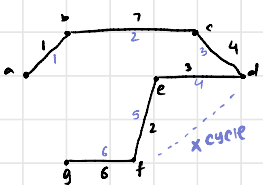
Order of adding the edges:
{a, b}, {b, c}, {c, d}, {d, e}, {e, f}, {f, g}



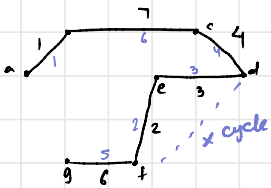
AFTER ALGORITHMS



— adding sequence



— adding sequence



7 − 1 = 6

6 edges used

kruskal's algorithm

- ↳ start with smallest
- ↳ adding order with small to big
- ↳ move disconnectedly (jump to small edges)
- ↳ no cycles

Order of adding the edges:
{a, b}, {e, f}, {e, d}, {c, d}, {g, f}, {b, c}

Sequence AND Series

- a sequence is a function from the subset of arrays
- a sequence whos sign alternates is an alternating sequence

Arithmetic Progression

$$a_n = a + (n-1)d$$

(a_n: nth term; a: first term; n: term number; d: common difference)

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

(S_n: sum of n terms; n: nth term; a: first term; d: difference)

$$S_n = \frac{n}{2}[a + \ell]$$

(ℓ: last term)

$$d = a_2 - a_1$$

Geometric Progression

$$a_n = ar^{n-1}$$

(a_n: nth term; a: first term; r: common ratio; $n-1$: term number)

$$S_n = \frac{a(1-r^n)}{1-r}$$

(S_n: sum of n terms; a: first term; r^n: nth term; r: ratio)

not to important for paper

$$r = \frac{a_2}{a_1}$$

Summation

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} \dots a_n$$

(index: k; lower limit: m; upper limit: n)

$a_0 = 2, a_1 = 3, a_2 = -2, a_3 = 1$ and $a_4 = 0$.

(a) $\sum_{i=0}^{4} a_i = a_0 + a_1 + a_2 + a_3 + a_4 = 2 + 3 + (-2) + 1 + 0 = 4$

(b) $\sum_{j=0}^{2} a_{2j} = a_0 + a_2 + a_4 = 2 + (-2) + 0 = 0$

(c) $\sum_{k=1}^{1} a_k = a_1 = 3$

TABLE 2 Some Useful Summation Formulae.

Sum	*Closed Form*	
$\sum_{k=0}^{n} ar^k \ (r \neq 0)$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$	Geometric Series: We just proved this.
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$	Later we will prove some of these by induction.
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$	
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$	
$\sum_{k=0}^{\infty} x^k, \lvert x \rvert < 1$	$\frac{1}{1-x}$	Proof in text (requires calculus)
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x \rvert < 1$	$\frac{1}{(1-x)^2}$	

ishma hafeez notes

ishma Hafeez notes

Division

Division

$b = ac$ where $a \neq 0$

a divides b

$a \mid b = b/a \rightarrow$ is an integer

$3 \nmid 7$: as not in integer form

$3 \mid 12 = 4$

Properties of divisibility

i $a \mid b$ & $a \mid c = a \mid (b+c)$

ii $a \mid b = a \mid bc$

iii $a \mid b$ & $b \mid c = a \mid c$

Division Algorithm

↳ remainder never negative

$101 = 11 \underline{\ 9\ } + 2$

$-11 = 3 \underline{-4} + 1$

9 → quotient

divisor → 11 | 101 ← dividend

-99

2 → remainder

dividend, divisor, quotient, remainder

$a = dq + r$

$q = a \text{ div } d$

$r = a \text{ mod } d$

Congruence Relation

↳ 3 methods

i	ii	iii
$a \equiv b \pmod m$	$a-b=km$	$a \bmod m = b \bmod m$
↳ a-b	↳ a-b	↳ compare both remainders
↳ check divisibility by m	↳ divide by m	↳ must be same

i) $17 \not\equiv 5 \pmod 6$

$17-5 = 12$ → divisible by 6

hence congurent

i) $17 \not\equiv 5 \pmod 6$

$k = \frac{17-5}{6} = 2$

hence congurent

iii) $17 \not\equiv 5 \pmod 6$

$17 \bmod 6 \equiv 5 \bmod 6$

$5 \equiv 5$

hence congurent

Relation mod

↳ $a \equiv b \pmod m$ (in bracket)

(a: dividend, b: remainder)

↳ check both remainders

$a \bmod m = b \bmod m$

function mod

↳ $a \bmod m = b$ (not in bracket)

Sum: $(a+b) \pmod m = [(a \bmod m) + (b \bmod m)] \bmod m$

Product: $ab \pmod m = [(a \bmod m)(b \bmod m)] \bmod m$

Sum: $a+c \equiv b+d \pmod m$

Product: $ac \equiv bd \pmod m$

Algebric Manipulation of Congruencies

if congurence and

↳ we multiply = still congurent

↳ we add = still congurent

↳ we divide = could change

Q) $7 \overset{a}{\equiv} 2 \overset{b}{\pmod 5}$ and $11 \overset{c}{\equiv} 1 \overset{d}{\pmod 5}$

Sum $18 = 7 + 11 \equiv 2 + 1 = 3 \pmod 5$

Product $77 = 7 \ 11 \equiv 2 \times 1 = 2 \pmod 5$

CALCULATOR MOD SHORTCUT

ans shift S⇄D for -ve value do manually

$\frac{19}{7} = 2\frac{5}{7}$ (quotient, remainder; denominators SAME)

APPLICATIONS OF CONGRUENCIES

Hashing function

↳ not one to one

$h(k) = k \bmod m$ (k: data; m: no. of memory locations)

when collision move to next space

Pseudorandom Numbers

↳ random number generator

↳ found using previous value

↳ 4 needed integers

- m : modulus
- c : increment
- a : multiplier
- x_0 : seed

↳ generation from $0 \leq x_n < m$ recursively

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

(x_n: start value; x_{n+1}: base condition)

↳ if pseudo num b/w 1 and 0 then generated numbers / modulus

x_n / m

↳ pure multiplicative generator ?

Check digits

↳ to check errors in string of numbers

↳ add extra digit at end (generated using function)

↳ if final digit wrong then error

Universal Product codes (UPCs)

↳ 12 digit code 3, 1, 3, 1, 3, 1, ... 1

↳ $\equiv 0 \pmod{10}$ do manually

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

a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

add all 11 digits

$3 \cdot 7 + 9 + 3 \cdot 3 + 5 + 3 \cdot 7 + 3 + 3 \cdot 4 + 3 + 3 \cdot 1 + 0 + 3 \cdot 4 + x_{12} \equiv 0 \pmod{10}$

$21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$

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

$x_{12} \equiv 0 \pmod{10}$ So, the check digit is 2.

↳ x_{12} is 2

- adding 2 to 98 : 100
- 100 mod 10 = 0

b. Is 041331021641 a valid UPC?

$3 \cdot 0 + 4 + 3 \cdot 1 + 3 + 3 \cdot 3 + 1 + 3 \cdot 0 + 2 + 3 \cdot 1 + 6 + 3 \cdot 4 + 1 \equiv 0 \pmod{10}$

$0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1 = 44 \equiv 4 \not\equiv \pmod{10}$

Hence, 041331021641 is not a valid UPC.

International Standard Book Number (ISBN)

↳ 10 digit code 1,2,3,4,...9

↳ $0 \pmod{11}$ use calculator

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}$$ → is given, different for every question

a. Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

1 2 3 4 5 6 7 8 9

$X_{10} \equiv 1\cdot 0 + 2\cdot 0 + 3\cdot 7 + 4\cdot 2 + 5\cdot 8 + 6\cdot 8 + 7\cdot 0 + 8\cdot 0 + 9\cdot 8 \pmod{11}$.
$X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}$.
$X_{10} \equiv 189 \equiv 2 \pmod{11}$. Hence, $X_{10} = 2$.

$189 + x_{10} \equiv 0 \pmod{11}$

$X_{10} = 2$

b. Is 084930149X a valid ISBN10?

written in roman so 10

$1\cdot 0 + 2\cdot 8 + 3\cdot 4 + 4\cdot 9 + 5\cdot 3 + 6\cdot 0 + 7\cdot 1 + 8\cdot 4 + 9\cdot 9 + 10\cdot 10 =$
$0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$
Hence, 084930149X is not a valid ISBN-10.

$299 \pmod{11} = 2$

$2 \neq 0$

so in valid

Arthemetic Modulo m

↳ positive integers $< m$

$a +_m b = (a+b) \bmod m$	addition modulo m
$a \cdot_m b = (a \cdot b) \bmod m$	multiplication modulo m

- $7 +_{11} 9 = (7+9) \bmod 11 = 16 \bmod 11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

If a & b belong to Z_m

1. Closure : $a +_m b$ and $a \cdot_m b$ belong to Z_m

2. Associativity: $(a +_m b) +_m c = a +_m (b +_m c)$
$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$

3. Commutativity : $a +_m b = b +_m a$
$a \cdot_m b = b \cdot_m a$

4. Identity elements: 1 and 0
$a +_m 0 = a$, $a \cdot_m 1 = a$

5. Additive inverse: If $a \neq 0$ belong to Z_m
$a +_m (m-a) = 0$
$0 +_m 0 = 0$

6. Distributivity:
$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$
$(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Caesar Cipher

↳ replace letter by the next 3rd letter → keeps letters in range

↳ encrypt function $f(p) = (p+3) \bmod 26$

↳ decrypt function $f^{-1}(p) = (p-3) \bmod 26$ → find inverse of function for decryption

↳ for encryption use mod

↳ for decryption no need of mod

* whenever range use mod

e.g decrypting B

$= 1-3$ OR $= 1-3+26$ → total letters

$= -2$ $= -2+26$

= check table $= 24$

Y $= Y$

counting starts from D

A	0	-26	H	7	-19	O	14	-12	V	21	-5
B	1	-25	I	8	-18	P	15	-11	W	22	-4
C	2	-24	J	9	-17	Q	16	-10	X	23	-3
D	3	-23	K	10	-16	R	17	-9	Y	24	-2
E	4	-22	L	11	-15	S	18	-8	Z	25	-1
F	5	-21	M	12	-14	T	19	-7			
G	6	-20	N	13	-13	U	20	-6			

$f = k+11 \pmod{26}$

S T O P G L O B A L W A R M I N G

4

D E Z A R W Z M L W H L C X T Y R

Prime are numbers > 1 and divisible only by themselves

Sieve of Erastosthenes

- 1 is not a prime number
- cut all divsible by 2 , keep 2 tho
- cut all divisibble by 3 , keep 3 tho
- cut all divisibble by 5 , keep 5 tho
- cut all divisibble by 7 , keep 7 tho
- the remaining will all be prime

composite integer: opposite of prime

↳ $n = ab$

↳ $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Mersenne Prime

↳ largest known prime numbers

$$2^{p} - 1 \quad (p = \text{Prime number})$$

↳ use the formula

↳ answer = Prime → Mersenne Prime

↳ answer ≠ Prime → not Mersenne Prime

e.g $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$ ✓

$2^{11} - 1 = 2047$ ✗

Least Common Multiple (LCM)

↳ using biggest factor

$$\text{lcm}(2^3 \cdot 3^5 \cdot 7^2, 2^4 \cdot 3^3)$$

$\max(3,4)$ for 2, $\max(5,3)$ for 3, $\max(2,0)$ for 7

$2^4 \cdot 3^5 \cdot 7^2$: LCM

GREATEST COMMON DIVISOR (GCD)

↳ using smallest factor

↳ a b are pairwise relativity prime if their GCD = 1
(a b: pairwise)

Prime Factorization

↳ not efficient cuz no algorithm

gcd(120, 500)

2 | 120
2 | 60
2 | 30
3 | 15
5 | 5
1

$2^3 \cdot 3^1 \cdot 5^1$

2 | 500
2 | 250
5 | 125
5 | 25
5 | 5
1

$2^2 \cdot 5^3$

OR

2	120	500
2	60	250
5	30	125
	6	25

no other number divisible by both

$2 \cdot 2 \cdot 5 = 20$ → GCD

$2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)}$

$2^2 \cdot 3^0 \cdot 5^1 = 20$ → GCD

Euclidean Algorithm

↳ efficient algorithm

$a = dq + r$ (a: dividend, d: divisor, q: quotient, r: remainder)

↳ gcd(91, 287) — greater of both is a

$287 = 91 \times 3 + 14$ (figure out)

↳ gcd(91, 14) — gcd(d, r)

$91 = 14 \times 6 + 7$

↳ gcd(14, 7)

$14 = 7 \times 2 + 0$

gcd = 7

Keep repeating till remainder = 0/1

↳ if remainder = 1 GCD = 1

↳ if remainder = 0 GCD = d

Linear Combination

↳ Bezout's Theorem / extended Euclidean

↳ if a and b are +ve integers

$\gcd(a,b) = sa + tb$ → Bezout's identity

Bezout coefficients of a and b

gcd(252, 198)

↳ first use Euclidean algorithm

i. $252 = 1 \times 198 + 54$ (a = q·d + r; gcd(d, r))

ii. $198 = 3 \times 54 + 36$

iii. $54 = 1 \times 36 + 18$

iv. $36 = 2 \times 18 + 0$ → till 1/0

representation changes from
↳ dq to qd
↳ to make linear combination

↳ backwards from iii to i (ignore 0 remainder)

$18 = 54 - 1 \times 36$ (r = a − qd) → a

$36 = 198 - 3 \times 54$ → b

$54 = 252 - 1 \times 198$ → c

↳ substituting b into a

$18 = 54 - 1(198 - 3 \times 54)$ (consider as variable)

$18 = 4 \times 54 - 1 \times 198$

↳ substituting c into new a

$18 = 4(252 - 1 \times 198) - 1 \times 198$

$18 = \underset{s}{4} \times \underset{a}{252} - \underset{t}{5} \times \underset{b}{198}$ → linear Combination

Linear Congruencies

using inverse to solve solution

$$an \equiv b \pmod{m}$$

linear congruence relation

↳ $\gcd(a, m) = 1$ then inverse exists

↳ Euclidean ← then do

↳ bezouts

↳ consider the coefficient of a given in question

↳ add m if inverse is negative

↳ multiply inverse on both sides of og eq

$\bar{a}$ 5 is inverse of a 3 modulus m 7

↳ **To check inverse**

$$\bar{a}.a \equiv 1 \pmod{m}$$

(inverse)

$5.3 = 15$

$15 \equiv 1 \pmod{7}$

↳ Find inverse of a 3 mod m 7

↳ $\gcd(3,7)$

$7 = 2 \times 3 + 1$

↳ $1 = 7 - 2 \times 3$ (a in question)

-2 is inverse -ve so

$-2 + 7 = 5 \rightarrow$ inverse

positive 5, 12, 19 add mod

negative -2, -9, -16 sub mod

↳ Solve the congruence $3n \equiv 4 \pmod{7}$ (inverse found previously -2)

$3n \equiv 4 \pmod{7}$

$a.\bar{a} = 1$ $3(-2)n \equiv 4(-2) \pmod{7}$ (multiplying inverse)

$n \equiv -8 \bmod 7$

$n = 6 \rightarrow$ ans

$3(6) \equiv 4 \pmod{7}$

$18 \equiv 4 \pmod{7}$

Chinese Remainder Theorem

↳ identify n

↳ all values pairwise relatively prime (gcd = 1) then do

if $\gcd(m_1, m_2), \gcd(m_2, m_3), \gcd(m_1, m_3) = 1$ → relatively prime

$m = m_1 \times m_2 \times m_3$ THEN SOLVE

$M_1 = \frac{m}{m_1}$ $M_2 = \frac{m}{m_2}$ $M_3 = \frac{m}{m_3}$

$Y_1 = \bar{M}_1 \rightarrow \bar{M}_1 M_1 \equiv 1 \pmod m$, ... by trial and error on n

$n = a_1 M_1 Y_1 + a_2 M_2 Y_2 + a_3 M_3 Y_3 \pmod m$

Q $x \equiv 2 \pmod 3$ (a_1, m_1), $x \equiv 3 \pmod 5$ (a_2, m_2), $x \equiv 2 \pmod 7$ (a_3, m_3).

↳ $m = 3 \times 5 \times 7 = 105$

↳ $M_1 = \frac{105}{3} = 35$ $M_2 = \frac{105}{5} = 21$ $M_3 = \frac{105}{7} = 15$

do trial an error on n

↳ $n \cdot 35 \equiv 1 \pmod 3$ $n \cdot 21 \equiv 1 \pmod 5$ $n \cdot 15 \equiv 1 \pmod 7$

$2 \cdot 35$, $\frac{70-1}{3}$ ✓ $\frac{21-1}{5}$ ✓ $\frac{15-1}{7}$ ✓

$Y_1 = 2$ → inverse of M_1 $Y_2 = 1$ → inverse of M_2 $Y_3 = 1$ → inverse of M_3

↳ $n = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 \pmod{105}$

$n = 233 \pmod{105}$

$n = 23$

23 is the smallest possible integer

Q $x \equiv 4 \pmod 5$,
$x \equiv 6 \pmod 8$,
$x \equiv 8 \pmod 9$.

$\gcd(5, 8)$

$8 \equiv 1 \times 5 + 3$

$5 \equiv 1 \times 3 + 2$

$3 \equiv 1 \times 2 + 1$

$\gcd(8, 9)$

$9 \equiv 1 \times 8 + 1$

$\gcd(a, 8)$

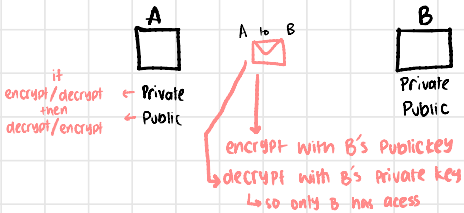
$9 \equiv$

all relatively prime

so possible

Number Theory in Cryptography

Public key cryptosystems



RSA

↳ p and q given

↳ find n, k, e

↳ $n = p * q$ (always prime)

↳ $k = (p-1)(q-1)$

↳ $\gcd(e,k) = 1$ → using trial and error → find e (take smallest value)

↳ $e.\bar{e} \equiv 1 \pmod{k}$ → linear congurencies → find d

encryption

↳ $c = m^e \mod n$ } on each letter

↳ $m = c^d \mod n$

decryption

$m = c^{13} \mod$

Q) $p = 7$, $q = 17$

$n = 7 \times 17 = 119$

$k = (7-1)(17-1) = 96$

$\gcd(e, 96) = 1$

$96 = d \times q + 1$

$96 = 5 \times 19 + 1$

$e = 5$ $(5, 96)$

for d

$1 = 96 - 19 \times 5$

inverse

$5.x \equiv 1 \pmod{96}$

$x = 19$

$-19 + 96$

$d = 77$

Fermat's Little Theorem

↳ large powers of integers

↳ if p is prime and a isn't divisible by p

↳ break in powers of 10

$a^{p-1} \equiv 1 \pmod{p}$

$a^p \equiv a \pmod{p}$

$a^{10} \equiv 1$

Q) Find $7^{222} \pmod{11}$ (break in (11-1) power which is 10)

$= 7^{22 \cdot 10 + 2} \mod 11$

$= 1.7^2 \mod 11$

$= 49 \mod 11$ → if answer too big leave it as it is

$= 5$

TYPES OF PROOFS

Direct Proofs

↳ $P \rightarrow q$ implication

↳ always assume P is true

↳ show q is also true

even	$2k$
odd	$2k+1$
prime	$n>1$, if $n=r.s$ then $r=1 \mid s=1$
composite	$n=r.s$, if $r\neq 1$ & $s\neq 1$
rational	$r=a/b$, $b\neq 0$
perfect square	$n=k^2$
divides	n/d, $d\neq 0$

Q) Prove sum of 2 odd num is even

P assuming is true — q

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

(odd number)

$2k+1+2k+1$

$4k+2$

$2(2k+1)$

$m=2k+1$

$2m$ is even

Q) sum of 3 consecutive num is divisible by 3

$n+(n+1)+(n+2)$

$3n+3$

$3(1+n)$

$k=1+n \rightarrow$ not 0

$3k$

Q) odd integer n^2 is odd integer

$(2k+1)(2k+1)$

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

$4k^2+4k+1$

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

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

$2m+1$ is odd

Q) m and n are both perfect squares

then $m.n$ = perfect square

$s^2 \quad t^2$

$(s.s) \quad (t.t)$

$st \;.\; st$

$(st)^2$

Q) n = odd n^3+n = even

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

$(4k^2+4k+1)2k+1+(2k+1)$

$8k^3+8k^2+2k+4k^2+4k+1+2k+1$

$8k^3+12k^2+8k+2$

$2(4k^3+6k^2+4k+1)$

$m=4k^3+6k^2+4k+1$

$2m$ is even

Q) Sum of 2 rational num = rational

$r=\frac{a}{b} \quad s=\frac{c}{d}$

$b\neq 0 \quad d\neq 0$

$r+s$

$\frac{a}{b}+\frac{c}{d}$

$\frac{ad+cb}{bd} \rightarrow p \;/\; \rightarrow q$

$\frac{p}{q}$ is rational

Indirect proofs

contraposition

↳ $\neg q \rightarrow \neg p$ contrapositive

Q) n is an integer $3n+2$ = odd then n = odd

($\neg q$ n = even → becuz contrapositive so take opposite)

$n = 2k$

$3(2k)+2$

$6k+2$

$2(3k+1)$ ($\rightarrow m$)

$2m$

even

so True

Q) all integ n, if n^2 = even then n = even

($\neg q$ n = odd → $\neg p$ n^2 = odd)

$(2k+1)^2$

$4k^2+2k+1$

$2(2k^2+k)+1$ ($\rightarrow m$)

$2m+1$

True

contradiction

↳ assume statement = false

↳ $\neg q$

↳ if True then statement false (as our wrong assumption is true so it means the statement is false)

↳ if False then statement true

Q) n^2 = even then n = even

n = odd ($\neg q$)

$(2k+1)^2$

$4k^2+4k+1$

$2(2k^2+2k)+1$ ($\rightarrow m$)

$2m+1 \neq$ even (so what we assumed is wrong so statement is true)

hence statement is true

Q) n^3+5 = odd then n = even

n = odd ($\neg q$)

$(2k+1)^3+5$

$(4k^2+4k+1)2k+1$

$8k^3+8k^2+2k+4k^2+4k+1+5$

$8k^3+12k^2+6k+6$

$2(4k^3+6k^2+3k+3)$

$2k \neq$ odd

so statement true

Q) $\sqrt{2}$ is irrational

$\sqrt{2}$ = rational

$\sqrt{2} = \frac{a}{b}$ → as rational

$(\sqrt{2})^2 = a^2/b^2$

$2 = a^2/b^2$

→ b even so take a as $2b^2 = a^2$

$b \neq 0$

$2b^2 = (2k)^2$

$2b^2 = 4k^2$

$b^2 = 2k^2$ so true

hence statement is false

Mathematical induction

↳ check base case

↳ n: first term (LHS), n: range (RHS) → if not given assume 1

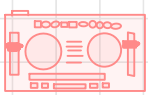
↳ induction step

↳ n=k

↳ n=k+1

↳ replace and prove

a) Prove $1+2+3+4+\dots n = \frac{n(n+1)}{2}$, $n \geq 1$



Basis case

Leftside ↳ n: first term, n=1 — rightside ↳ n: value given as range, n=1 — compare

$1 = 1\frac{(1+1)}{2}$ — since equal move to next step

$1 = 1$ ✓

Induction step:

↳ Assume true n=k

$1+2+3+4+\dots k = \frac{k(k+1)}{2}$

↳ Show true n=k+1 based on above assumption

$1+2+3+4+\dots k+k+1 = \frac{(k+1)(k+1+1)}{2}$

same as above assumption so replace

↳ $\frac{k(k+1)}{2} + k+1 = \frac{(k+1)(k+1+1)}{2}$

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

so we can get same denominator

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

$k^2+k+2k+2 = k^2+2k+k+2$

hence equal so proven

b) $1+2+2^2 \dots 2^n = 2^{n+1}-1$ $n \geq 0$

Basis step

n=1 n=0

$1 = 2^1-1$

$1=1$

Induction step

n=k

$1+2+2^2 \dots 2^k = 2^{k+1}-1$

n=k+1

$1+2+2^2 \dots 2^k + 2^{k+1} = 2^{k+1+1}-1$

$2^{k+1}-1+2^{k+1} = 2^{k+2}-1$

$2^{k+1}(1+1)-1$

$2^{k+1} \cdot 2^1 - 1$

$2^{k+2}-1 = 2^{k+2}-1$

hence equal so proven

Sum Rule

- many groups
- choose 1
- no common element

Subtraction Rule

- many groups
- choose 1
- common element
- way 1 + way 2 − common

Product Rule

- multiple groups
- select 1 task from each group

Pigeonhole Principle

- n boxes
- n+1 objects
- 1 box has 2 or more objects

$N = k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) + 1$ → contradiction

(N: objects, k: boxes)

common: $\left\lceil \frac{N}{k} \right\rceil$

Permutations

- organise
- ways

$${}^{n}P_{r} = \frac{n!}{(n-r)!}$$

Combinations

- different types
- select

$${}^{n}C_{r} = \frac{n!}{(n-r)!\,r!}$$

Binomial Theorem

→ COULD BE GIVEN USING PASCAL

$$(a+b)^{n} = a^{n} + {}^{n}C_{1}\,a^{n-1}b + {}^{n}C_{2}\,a^{n-2}b^{2} + \ldots + b^{n}$$

$$(1+x)^{n} = 1 + nx + \frac{1}{2!}n(n-1)x^{2} + \frac{1}{3!}n(n-1)(n-2)x^{3}\ldots$$

Q) coefficient of $x^{12}y^{13}$ in $(x+y)^{25}$

$$\frac{25!}{13!\cdot 12!} = 5{,}200{,}300$$

Q) coefficient of x^{5} in $(1+x)^{11}$

$${}^{11}C_{5} = 462$$

Q) coefficient of $x^{12}y^{13}$ in $(2x-3y)^{25}$

$${}^{25}C_{13}\,(2)^{25-13}\,(-3)^{13}$$

Pascals Triangle

- ↳ sum of row: 2^r
- ↳ each num = sum of above 2 numbers
- ↳ binomial

↳ $(a+b)^2 = a^2 + 2ab + b^2$

Power/row = 2 coefficients = 1, 2, 1

↳ $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

Power/row = 3 coefficients = 1, 3, 3, 1

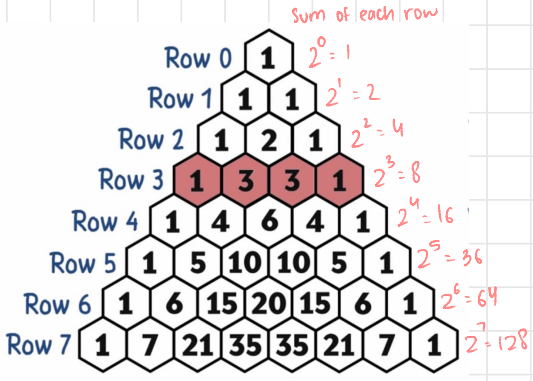


abb meray liyay dua karo ☺

ishma hafeez
notes

Permutation/combination

Interference rules

Binomial

rattafys

implication table

equivalence relation/partial ordering

handshake theorem formula

reison formula

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

but = $\wedge$

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

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

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

negating Quantifiers

not everybody — at least one somebody

$\neg \forall n\, P(n) = \exists n\, \neg P(n)$

$\neg \exists n\, P(n) = \forall n\, \neg P(n)$

no one — everyone

start sentence with there is

Implication Table

"if p, then q"	$p \rightarrow q$	"p implies q"
"if p, q"		"p only if q"
"p is sufficient for q"		"a sufficient condition for q is p"
"q if p"		"q whenever p"
"q when p"		"q is necessary for p"
"a necessary condition for p is q"		"q follows from p"
"q unless $\neg p$"		

37

q if p
q when p
q unless ¬p
q whenever p
q is necessary p
sufficient condition q is p
follows
Provided

↳ P iff q
↳ if P then q, conversly
↳ P is necessary and sufficient for q
↳ P if and only if q

HANDSHAKING THEOREM

COMMING IN PAPER

if g is a graph

each degree x total nodes = 2 x total edges

total degree * total nodes = total edges

always even / else graph dosent exist

Corollary: total degree of g is even

undirected graph has even nodes

each: $d \times n = 2e$

total: $d \times n = e$

Equivalence Relation

↳ reflexsive
↳ symmetric
↳ transisitive

Partial ordering

↳ Reflexsive
↳ Anti symmetric
↳ Transisitive