CS 530 notes

Hao-En Lu

2/1/2023

$\boxed{\text{show}}$ $y = e^x + 5$ is one-to-one.

If a f_n is 1-1 then $f(x_1) = f(x_2)$

$\Rightarrow x_1 = x_2$

$f(x_1) = f(x_2)$

$f(x_1) = e^{x_1} + 5$, $f(x_2) = e^{x_2} + 5$

$f(x_1) = f(x_2) \Rightarrow e^{x_1} + 5 = e^{x_2} + 5$

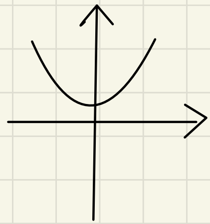
$e^{x_1} = e^{x_2}$

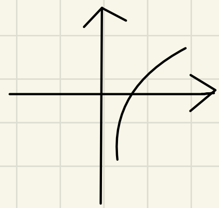
$\frac{e^{x_1}}{e^{x_2}} = 1$

$e^{x_1 - x_2} = 1$

$\therefore x_1 - x_2 = 0$

$\therefore x_1 = x_2$

Domain : X. →  cover all domain

Range : Y. →  cover all range.

Sequence

→ denoted by $\{x_n\}$ to indicate n-th element in an ordered collection

→ infinite number of element

exp:

Integers : $\mathbb{N} = \{1, 2 \dots\}$

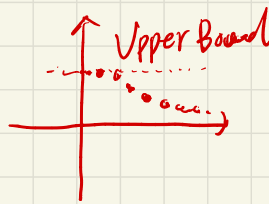
Rational Types

Operations with sequences

End Behavior : $x_n = \{\frac{1}{n}\}$ $n \in \mathbb{N}$

Alternating : $x_n = (-1)^n$ $n \in \mathbb{N}$

Relation to a Series : $S_n = \sum_{n \in \mathbb{N}} x_n$



1-1 (one-to-one) : Injective property

onto : Surjective property

↳ $f: \mathbb{N} \to \mathbb{N}$ $f(n)=n$ OR $f(n)=n+1$ are onto

$f: \mathbb{N} \to \mathbb{N}$

f_1 is neither 1-1 nor onto : f_2 if $n<100$; f_3 if $n \geq 100$

f_2 is 1-1 but NOT onto : $f(n)=n^2+1$

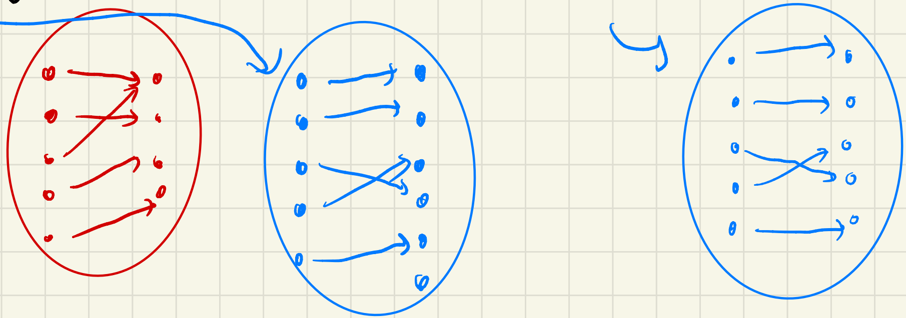
f_3 is onto but NOT 1-1 : $f(n)=n-2$ $f_1(n)=f_3(n)=1$

f_4 is both 1-1 and onto : $f(n)=n$

if A surj B then $|A| \geq |B|$ = onto

if A inj B then $|A| \leq |B|$ = one-to-one

if A bij B then $|A| = |B|$ = both



Modulo Arithmetic

→ a function that restricts the output to certain possible values.

→ $y = x \pmod p$

y is the output and x is the input called modulo p.

exp: $x = 25$ $p = 17$ → $y = 8$

⇒ $25 = 17(1) + 8$

possible value of y is restricted to $\{0, 1, 2, 3, \ldots, 15, 16\}$

$8 \equiv 25 \pmod{17}$

Usage:

Number Theory & Cryptography

Check Errors & Fraud.

Digital Signal Processing.

⇒ $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$

→ a is congruent to b modulo n

$a \equiv b \pmod n$ iff $n \mid (a-b)$

Example $n=4$ then

- $[0] = \{\dots -4, 0, 4, 8 \dots\}$
- $[1] = \{\dots -3, 1, 5, 9 \dots\}$
- $[2] = \{\dots -2, 2, 6, 10 \dots\}$
- $[3] = \{\dots -1, 3, 7, 11 \dots\}$

multiplication

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\downarrow$ $\mathbb{Z}_4$

$2x \equiv 1 \pmod 4$

$x = \emptyset$

$n=5$

multiplication

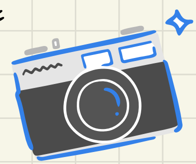
$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_5$

$\rightarrow$ $2x \equiv 1 \pmod 5$

$x = \underline{\underline{3}} = 2^{-1}$

$\longrightarrow$ n congruent classes



Facts:

- $a \equiv b \pmod n$ then $b \equiv a \pmod n$
- $a \equiv b \pmod n$, $c \equiv d \pmod n$ then
  $a + c \equiv b + d \pmod n$
  $a \times c \equiv b \times d \pmod n$

example:

$5 + 8 \equiv 1 \pmod{12}$, $5 \times 8 = 40 \equiv 4 \pmod{12}$ $\quad 5^3 = \underbrace{25}_{1 \pmod{12}} \times 5$
$\equiv 5 \mod (12)$

For all $n \in \mathbb{Z}$, $7 \mid n^3$ OR $7 \mid n^3 \pm 1$

classes of $\mathbb{Z}_7$: $\{0, 1, 2, 3, 4, 5, 6\}$

$4 \equiv -3$, $5 \equiv -2$, $6 \equiv -1$

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

n^3

$\{-27, -8, -1, 0, 1, 8, 27\}$

$-27 \equiv -(-1) \to 1$, $-8 \equiv -1$, $8 \equiv 1$, $27 = 6 \equiv -1$

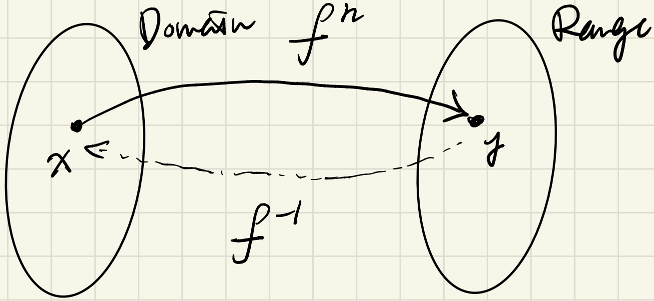
$$\Rightarrow \{1, -1, -1, 0, 1, 1, -1\}$$

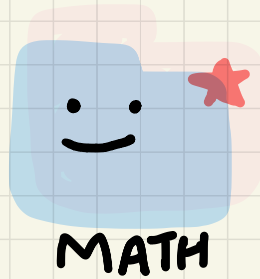
$$\Rightarrow 7 \mid n^3 \quad \text{OR} \quad 7 \mid n^3 \pm 1$$

$\boxed{a \mid (b-c) \Rightarrow a \text{ "divides" } (b-c)}$

a is a divisor of $(b-c)$

Inverse Function





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

If function is not one-to-one or onto

→ no inverse function

Ex.

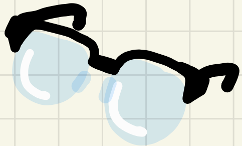
$2y + 5x = 4$

↳ $5x = 4 - 2y \rightarrow x = \frac{4}{5} - \frac{2}{5}y$

(Inverse)

$y = e^x \longleftrightarrow y = \log x$ (Inverse)

Function Composite



$(f \circ g)(x) \neq (f \cdot g)(x)$

$= f(g(x))$

exp.

if $f(x) = 3x + 1$ $\quad g(x) = \sin 2x$

$(f \circ g)(x) = f(g(x)) = 3(\sin 2x) + 1$

$(f \cdot g)(x) = (3x+1)(\sin 2x)$

$(f \circ f^{-1})(x) = 1$

Greatest Common Divisor.

Th^m:

$a \in \mathbb{Z}$. is invertible $\bmod(n)$ iff. $\gcd(a, n) = 1$

Let's check $\mathbb{Z}_6$

$n = 6$

$\{1, 2, 3, 4, 5\}$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Induction

⇒ $\forall n \in \mathbb{N}$, $p(n)$ where $p(n)$ is a preposition about n.

⇒ Use Induction Axiom from Peano Axiom

- Weak Induction
  - → base case : confirm $1 \in S$
  - → Induction step : $p(n+1)$ is True

  < Assumption

- Strong Induction
  - → base case $(n=1)$ is True.
  - → $p(k)$: $a \leq k \leq n$ $p(k)$ is True
  - → $p(n+1)$ is True

Logic:

Complexity Theory:

- O (notation) if $f = O(g(x))$

  $f(x) \le c \cdot g(x)$ c is a constant

  $c \ge 1$

OR $\cup$ **AND** $\wedge$ **Implication** $\Rightarrow$ (if then)

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

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

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

$\equiv$

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

if A then B

$\equiv$ not A or B

Practice: p is T, q is F

$(p \wedge \overset{T}{q}) \vee \overset{T}{p} \longrightarrow$ T

$\overset{T}{p} \Rightarrow (q \overset{T}{\vee} p) \longrightarrow$ T

$\overset{F}{\sim p} \wedge \overset{T}{\sim q} \longrightarrow$ F

$\underbrace{(\underset{F}{\sim p} \vee \underset{F}{q})}_{F} \Rightarrow \underset{T}{p} \longrightarrow$ T if p(s) then q(s), i.e $p \Rightarrow q$ implication

converse $q \Rightarrow p$

inverse $\sim p \Rightarrow \sim q$ same

contapositive $\sim q \Rightarrow \sim p$

NP completeness:

check if the problem can be solved in

. $\boxed{\text{Polynomial Time}}$ and $\boxed{\text{Exponential Time}}$

$P \subseteq NP$

Boolean Algebra

- Boolean Product is "AND"
- Boolean Sum is "OR"
- Priority <u>NOT</u> → <u>AND</u> → <u>OR</u>

exp.

$F(x, y, z) = x + y^c z$

Relational Database.

Cryptography $\longrightarrow$ Number Theory.

- Encryption function $C = m + k \pmod{26}$

Caesar Cipher.

numerical position of text.

Cepher

- Vigenère Cipher.
- Block Cipher.
- Euler Phi Function ϕ.

$\phi(n) = n-1$

$n \Rightarrow$ prime.

$\longrightarrow$ p and q are distinct prime. $N = pq$

$$\phi(N) = \phi(pq) = (p-1)(q-1) = \phi(p)\phi(q)$$

Theorem (Euler Theorem): If $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \bmod (n)$

let $a=15$ and $n=187 \to n=11(17)$ $\begin{array}{r} 12 \\ 15\overline{)187} \\ \underline{15} \\ 37 \end{array}$

$\phi(187)=\phi(11)\phi(17)=10\cdot 16=160$. $gcd(15,187)$ $=gcd(15,7)=1$

$gcd(15,187)=1$

then (By Euler Theorem) $15^{\phi(187)}=15^{160}$
$\equiv 1 \pmod{187}$

Example

$\phi(15)=\phi(3)\phi(5)=2\times 4=8$.

$\phi(200)=\phi(25)\phi(8)=\phi(5^2)\phi(2^3)$
$=(5^2-5^1)(2^3-2^2)=(25-5)(8-4)$
$=20\times 4=80$

$\star$ [$\phi(p^a)=p^a-p^{a-1}$ if p is prime and $a\in\mathbb{Z}$]

$\phi(32)=\phi(2^5)=2^5-2^4=32-16=16$

$\begin{array}{r} 2 \\ 27 \\ \underline{\times\ 2} \\ 54 \end{array}$

$\phi(2^3 3^4 7^2)=\phi(2^3)\phi(3^4)\phi(7^2)$
$=(2^3-2^2)(3^4-3^3)(7^2-7^1)=4\times 54\times 7$
$=28\times 54=1512$

$\begin{array}{r} 54 \\ \underline{\times\ 28} \\ 112 \\ \underline{140\ } \\ 1512 \end{array}$

Polynomial Time Algorithm

- for a constant c : run time is $O(n^c)$

Bipartite Matching

- Graph Theory Problem OR

Linear Programming Flow problem.

Example of NP.

- Traveling Salesman
- 3 Color Problem

exp.
→ Hamiltonian cycle Problem.

hardest problem in NP.

NP-complete , NP-hard.

→ at least as hard as NP-com

Linear Recurrence Relations

$$f_n = f_{n-1} + f_{n-2}$$

Characteristic Polynomial.

$$\begin{cases} f_n = x^2 \\ f_{n-1} = x \\ f_{n-2} = \text{const.} \end{cases}$$

$\Rightarrow \underline{x^2 = x + 1}$

Functions / Sequence / Recurrence.

1-1 ∪ onto
example

$\{x_n\} = (-1)^n$

$\{y_n\} = \frac{1}{n+1}$

$n \in \mathbb{N}^+$

$\left\{\frac{x_n}{y_n}\right\} = (-1)^n (n+1) \Big|_{n=5}$

$= (-1)(6)$

$3x = 1 \quad \mathbb{Z}_7$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0						
3	0	3	6	2	5	1	4
4	0						
5	0						
6	0	6	5	4	3	2	1

Induction : Show that for $n \geq 1$ sum of first n odd numbers is a perfect squares, that is $\sum_{n=1}^{k} 2n-1 = k^2$

$n=1 \quad 1 = 1^2$ TRUE

Assume $n=k$ and result holds.

$$n=k \Rightarrow \sum_{n=1}^{k} 2n-1 = k^2$$

Induction Step $n = 2k+1$

$$k^2 + 2k+1 = (k+1)^2 \longrightarrow \text{TRUE}$$

$$\sum_{n=1}^{k+1} \overline{2(k+1)}^{\,2k+2-1\,=\,2k+1}-1 = \underbrace{\sum_{n=1}^{k} 2n-1}_{= k^2} + (2k+1)$$

$$= k^2 + (2k+1) = (k+1)^2 \longrightarrow \text{TRUE}$$

Public Key Ciphers

- Usage : Internet, Credit card . . .
- Type : RSA, El-Gamal, Diffie-Hellman Key

Cipher Keys :

- Symmetric / Primary key.
- Asymmetric / Public Key.

Caesar Cipher.

$C + (26 - k) \bmod 26$, with $k = 3$.

Euler Phi Function

$\phi(p) = p - 1$, p is prime

$\phi(N) = \phi(pq) = (p-1)(q-1) = \phi(p)\phi(q)$

Euler Theorem

$\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \bmod (n)$

[$\phi(p^a) = p^a - p^{a-1}$ if p is prime and $a \in \mathbb{Z}^+$]

Primitive Root

- Fermat's little Theorem:

  if p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$

  and $a^{p-1} - 1 \equiv 0 \pmod{p}$

exp.

Calculate $2^{345} \bmod (11)$

Note that $2^{10} \equiv 1 \bmod (11)$ (using $a^{p-1} - 1 \equiv 0 \pmod{p}$)

$a = 2 \quad p = 11$

$$2^{345} = \boxed{\underbrace{2^{34(10)}}_{\substack{\shortparallel \\ 1 \pmod{11}}}} + 5 = \underbrace{2^5}_{\substack{\shortparallel \\ 32}} = 10 \bmod (11)$$

$\Rightarrow 2^{345} = 10 \bmod (11)$

Euler's Corollary:

let p, q be distinct primes, for each a not divisible by either p or q, $a^{(p-1)(q-1)} \equiv 1 \bmod (p \cdot q)$

Euler Phi Function: $\phi : \mathbb{N}^+ \Rightarrow \mathbb{N}^+$

$\phi(n) = \{ k \mid 1 \le k \le n, \gcd(k, n) = 1 \}$

exp.

$\phi(2) = \{1\} = 1 \quad \phi(4) = \{1, 3\} = 2 \quad \phi(12) = \{1, 5, 7, 11\} = 4$

Primitive Root

let b be an integer not divisible by prime p.
Find (p-1) be the smallest positive integer. γ.
$b^{\gamma} \equiv 1 \mod p$

$\Rightarrow$ b is called primitive Root mod p.

exp.
let $p=5$ $b=2$

$2^0 = 1 \mod 5$
$2^1 = 2$
$2^2 = 4$
$2^3 = 3$
$2^4 = 1 \mod 5$

The number of Primitive Root is given by ϕ the Euler Phi function.

if b is any primitive root mod p. then set of all primitive root mod p is given by
$\{ b^k \mid \gcd((p-1), k) = 1 \}$

exp.
$p=13$ $\phi(p-1) = \phi(12) = 4$ and 2 is a primitive root b/c $2^{p-1} = 1 \mod (13)$
$\phi(12) = \{1, 5, 7, 11\} \Rightarrow$ Primitive Root $\{2, 2^5, 2^7, 2^{11}\}$

Discrete Logarithm Problem.

Let G be a group. determine the elements $g, h \in G$ such that $\underbrace{g \times g \times g \times g \cdots \times g}_{x \text{ times}} = h$

where x is an integer $\quad g^x = h$

Diffie-Hellman Problem

$g^{ab} \pmod p$ from known $g^a \pmod p$ & $g^b \pmod p$

Collision Algorithms → Find matching element.

- Meet in the middle
- collision algorithms.

Find probable primes or pseudo primes.

$x^{25} \to$ 24 multiplication

$25 \to$ binary $\to 11001 \to$ Remove 1st 1

$\to 1001 \to 1 \leftrightarrow sx, 0 \leftrightarrow s \quad s = \text{square} \quad x = \text{multiply by } x.$

sx, s, s, sx

$\to \underline{x^2, x^3, x^6, x^{12}, x^{24}, x^{25}} \to$ 6 multiplication

Elliptic Curves.

$E[a,b] = y^2 = x^3 + ax + b.$

→ Discrete Logarithm Problem (DLP)

discriminant of Elliptic curve Equation

$\Delta = 4A^3 + B^2$

$f(x,y) = ax^2 + bxy + cy^2 + dx + ey + g.$

$\Delta = \sqrt{b^2 - 4ac}$

Proposition : a statement either true or false.

Theorem : a proposition proved to be correct.

Conjecture : proposition whose truth remains unknown.

Predicate : a proposition whose truth depends on the value of variables.

Natural Numbers = $\{1, 2, 3, 4 \ldots\} = \mathbb{N}^+$

Integers = $\{\ldots, -2, -1, 0, 1, 2, 3 \ldots\} = \mathbb{Z}^+$

Rational Numbers = $\{m/n \mid m, n \in \mathbb{Z}, n \neq 0\} = \mathbb{Q}$

Complex Numbers = $\{a + ib \mid a \in \mathbb{R}, b \in \mathbb{R}\} = \mathbb{C}$

Real Number = $\mathbb{R}$.

Set Operation

Union = $A \cup B$ = A or B

Intercection = $A \cap B$ = A and B.

Difference = A / B = A and not B.

Complement = A^c = not A.

Distributive Law

- A AND (B OR C) = (A AND B) OR (A AND C)
- A OR (B AND C) = (A OR B) AND (A OR C)

Induction Practice : show $\forall n \in \mathbb{N}$, $1+2+4 \cdots +2^n = 2^{n+1}-1$

① Base Case : $n=1$

$1+2 = 3 = 2^{1+1}-1 = 4-3 \longrightarrow$ TRUE

② Assume $1+2+\cdots+2^n = 2^{n+1}-1$ to be TRUE

③ Induction Step : $n = n+1$

$1+2+\cdots+2^n+2^{n+1} = 2^{n+1}-1+2^{n+1} = 2(2^{n+1})-1$

$= 2^{n+2}-1 \longrightarrow$ TRUE

$a_0=1$ $a_1=3$ $a_n=2a_{n-1}-a_{n-2}$ for $n \geq 2$

Prove that for all $n \geq 0$ $a_n = 2n+1$

① Base case : $n=0$ $a_0 = 2\cdot(0)+1 = 1 \rightarrow$ TRUE

$n=1$ $a_1 = 2\cdot(1)+1 = 3 \rightarrow$ TRUE

② Assume $a_n = 2a_{n-1} - a_{n-2} = 2n+1$

③ Induction step : $n = n+1$

$a_{n+1} = 2a_n - a_{n-1} = 2(2n+1) - [2(n-1)+1]$

$= 4n+2-2n+2-1 = 2n+3 = 2(n+1)+1 \rightarrow$ TRUE

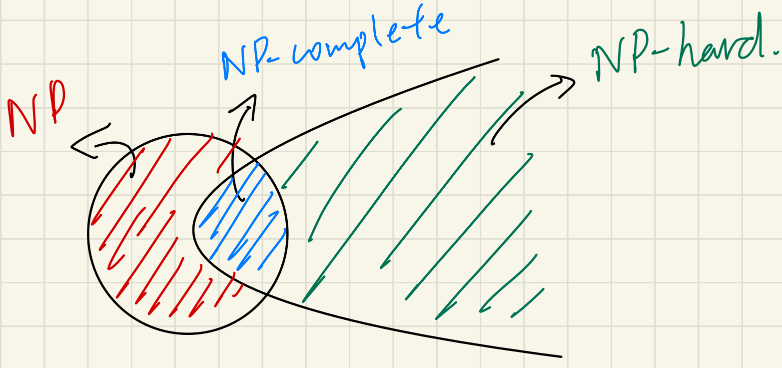
Complexity Theory → Resources needed to solve problem

- Input size = n t_n = maximum time
  S_n = Maximum space

- Worst Case Scenario $t_A(n) = t_n$ & $S_A(n) = S_n$

Logical Formula as a statement $p(s)$

$p(s)$ → Tautology (Valid)
$p(s)$ → Satisfacting
$p(s)$ → Contradiction.



NP - A problem is NP class if it is solvable in polynomial time by a nondeterministic turing machine

NP Problem Example

- Diophantine Equation → Not NP.
- Composite Number Problem → NP.
- Euler Cycle → NP

NP problem can be solved by a time between polynomial and Exponential

Tautology → a statement where the resulting truth table is all true.

exp.

$$p \Rightarrow q \vee q \Rightarrow p.$$

Boolean Function

- Gates
- AND, OR, NOT, XOR, NAND, NOR

By $a^p \equiv a \pmod p$ if p is prime & $\gcd(a,p) = 1$

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

$35^{28} \equiv 1 \mod 29$ $\qquad 86 = 28 \times 3 + 2$

$$\begin{array}{r} 3 \\ 28\overline{)\,86} \\ 84 \\ \hline 2 \end{array} \qquad \underbrace{35}_{1}{}^{28\cdot 3+2} \equiv 35^2 \mod 29$$

$$1 \equiv 3 \mod 29$$

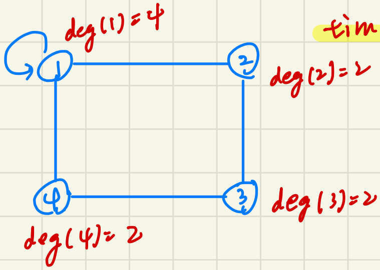
$$\begin{array}{r} 35 \\ \times\ 35 \\ \hline 175 \\ 105\ \ \\ \hline 1225 \end{array} \qquad \begin{array}{r} 42 \\ 29\overline{)\,1225} \\ 116\ \ \\ \hline 65 \\ 58 \\ \hline 3 \end{array}$$

Graph : $G = \langle V, E \rangle$ V - a finite set of vertices

E - a finite set of edges.

exp. $V = \{1, 2, 3, 4\}$ $E = \{(1,2), (2,3), (3,4), (4,1)\}$

Degree of vertex V : degree v, written $\deg(v)$, is the number of non-self loop edges adjacent to v plus two times the number of self loops defined at v.



finite graph : $|V| < \infty$

Simple graph : no two vertices are connected by more than one edge.

no edge connect a vertex to itself.

graph with multiple edges → Multi-Graph.

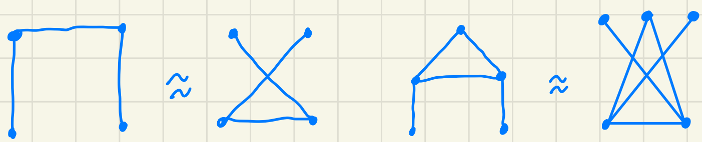
graph with a loop → Pseudo-Graph.

Simple graph Operation :

$G_1 = G_2$: 2 graph have exact same vertex set. and edge set.

G_1 is isomorphic to G_2 $(G_1 \approx G_2)$: if we can find a bijection $\varphi: V(G_1) \to V(G_2)$ such that $V_i V_j$ is an edge of G_1 iff $\varphi(V_i)\varphi(V_j)$ is an edge of G_2

homomorphisms : that is isomorphisms onto itself, as a measure of symmetry.



Graph Operation

- Union : $G_1 = (V_1, E_1)$ $G_2 = (V_2, E_2)$ when $V_1 \neq V_2$. $G_1 \cup G_2$ formed by placing G_1 and G_2 side by side.

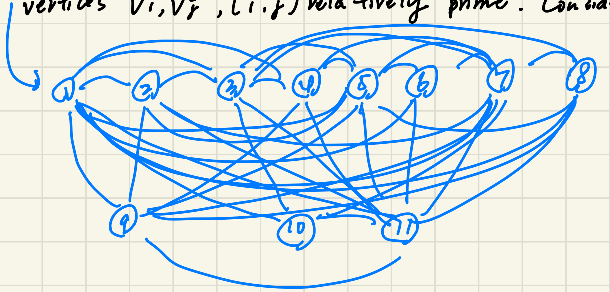
  when $V_1 = V_2$, $G_1 \cup G_2$ contains every edge of both $E_1 . E_2$.
- Complement : G^c of a graph $G = (V, E)$ is a graph with same vertex set. but with the Edge set that are NOT in G.

exp.
If $G = (V_1, E_1)$ and $G^c = (V_2, E_2)$ then $E_1 \cup E_2 = E(K_n)$ and $E_1 \cap E_2 = \emptyset$.
K_n = complete graph with n edges

Example :

(1) $G(V,E)$ has 3 vertices labelled 0, 1, and 2 . An edge exists if the modulo function $V \to V(\text{Mod } 2)$ is non-zero for vertices 1 and 2, starting from vertex 0.

(2) Consider the $G(V,E)$ where an edge exists between any two relatively prime vertices V_i, V_j , (i,j) relatively prime. Consider in Z_{12}



Sub Graph : A sub graph H of graph $G = (V, E)$ is a graph when every vetex of H is a vertex of G and that every edge of H is an edge of G.

→ For the given graphs $G_1 . G_2$, we say $G_2 \subseteq G_1$ if there is a sub graph H of G_1 such that is isomorphic of G_2 .

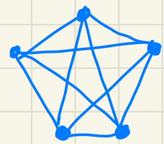
Graph Examples.

- Path graph P_n – has $(n+1)$ vertices.
  → the length of a path is the number of edges in the path. $(= n)$
- Cycle graph C_n – has n vertices.
- Complete Graph K_n – has n edges and there is an edge connecting every pair of distinct vertices.

Planner Graph – a connected graph can be drawn without any edge crossing.

Euler Formula : $v - e + f = 2$ f : faces.

Example: K_5 is NOT planar.



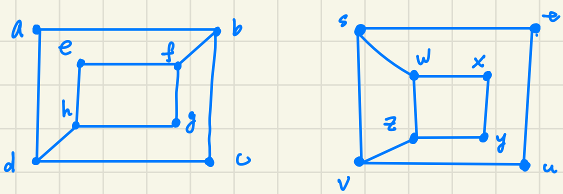
K_5.

ΔG : Maximum degree of a graph, the $\max\{d(v) \mid v \in V(G)\}$

δG : Minimum degree of a graph, the $\min\{d(v) \mid v \in V(G)\}$.

→ for any $v \in G$, $\delta G \le d(v) \le \Delta G$

Determine if the graph is Isomorphic



$|V| = 8$ $|e| = 10$ for both graphs.

But $\deg(a) = 2$ in G.

It can be t, u, x or y in H

But they all adjacent to another deg 2 in H

this is not true for a in G

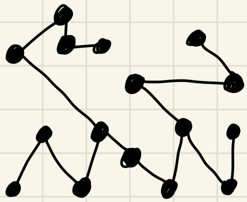
→ they are NOT isomorphic

Theorem : For a graph $G(V, E)$ the following holds:

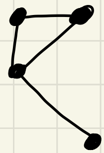
$$\sum_{v \in V(G)} d(v) = 2E$$

Lemma : For any graph $G(V, E)$ the number of odd degree vertices is always even.

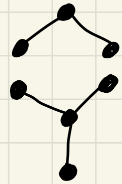
Tree in Graph Theory. : Undirected connected Graph with NO cycles.



Tree



Not a tree
(has cycle)



Not a tree
(not connected)

Tree : if a graph $G(V,E)$ is a tree. then it has $(n-1)$ edges.

→ it has at least 2 vertices of degree 1 ($V \geq 2$)

Theorem : Suppose $G(V,E)$, $|V| = n$, $|E| = n-1$

→ G is connected

→ G is acyclic

→ G is a tree.

Theorem : Show that G, H isomorphic iff G^c and H^c are isomorphic

$\Rightarrow uv \in E(G^c) \Rightarrow uv \notin E(G)$

$\Rightarrow uv \notin E(H)$

$\Rightarrow uv \in E(H^c)$

exp.

Let $G(V,E)$ with n vertices and every vertex has degree k.

what is the number of edges ?

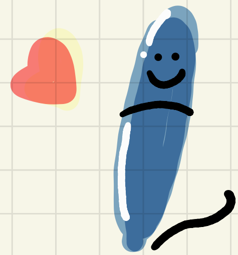
$\Rightarrow 2|E| = nk. \Rightarrow |E| = \frac{nk}{2}$ (handshake lemma)

- Sum of the degree sequence is even if it is graphical.

Graph Invariant : A property of a graph that will be preserved under an Isomophism.

- Number of components
- Number of Edges
- Number of vertices
- Degree sequence of a graph.

Graph Definition :



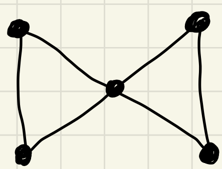
- walk
- tail
- path.
- circuit.
- length
- Eulerian Circuit : a circuit that contains every edge of the graph.
- A Graph $G=(V,E)$ is called <u>Eulerian</u> if it has Euler Circuit.

Theorem: Due to <u>Euler</u>

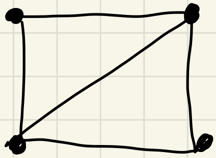
Let $G=(V,E)$. Given an Eulerian Circuit if and only if every vertex in G has even degree. G has an Eulerian trial if and only if G has exactly two vertices with odd degree.

Hamiltonian Circuit.

a circuit where every vertex is visited exactly once.



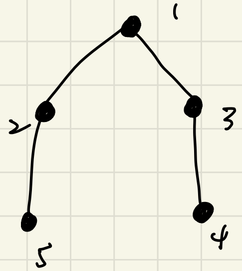
has Euler Circuit.
NO Hamiltonian Circuit.



No Euler Circuit.
has Hamiltonian Circuit.

Adjacency Metrix

$$M = \begin{array}{c|ccccc} & 1 & 2 & 3 & 4 & 5 \\ \hline 1 & 0 & 1 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 \\ 3 & 1 & 0 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 & 0 & 0 \\ 5 & 0 & & 0 & 0 & 0 \end{array}$$



Randomness

an event or an occurrence Is random if the outcome. Is not determined a-priori

Example

Show that if $A \subseteq B$, then $P(A) \leq P(B)$

Assume $A \subseteq B$. Then $B = A + B \setminus A$

Apply the probabilistic function $P(B) = P(A) + P(B \setminus A) \geq P(A)$

When $B \setminus A = \emptyset$, The equality occurs.

Probability Distribution: A descriptive way of writing or showing the possible outcomes.

↳ Discrete Distribution:

has a finite or countable number of outcomes.

- Coin toss (one) Bernoulli trials with probability of success p.
- Many Repeated coin tosses → Binomial trials → Collection of Bernoulli
- Doctor office visit → Poisson Distribution with parameter given by unit arrivals.

Bayes Theorem : Useful in determining conditional probability.

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)}$$ ← normalizing factors.

AI & ML use **Bayes Classifier.**

The Three M's of Probability

Mean. Median. Mode.

Mean: $\frac{\sum x_i}{n}$

Median: $x_1 < x_2 \cdots < x_n$ the middle value

Mode: the highest frequency of data point.

Interquartile Range (IQR) $Q_3 - Q_1$ = difference of quartiles.

Parameter Estimation.

- Maximum Likelihood Estimation (MLE)
- Method of Moments (MoM)
- Percentile Matching
- Simulation

Unbiased Estimator : the expected value of the estimator is same as the true parameter.

if the true parameter value is θ.

$E[T|\theta] = E[\theta] = \theta$.

Bias $\Rightarrow E[T|\theta] - E[\theta]$

Consistent Estimator : an estimator T as given above, perform the estimation process n-times. $T_1, T_2, T_3 \ldots T_n$.

$\lim_{n\to\infty} T_n = \theta$

$\forall \theta$ and $\forall \varepsilon > 0$ $Pr(|T_n - \theta| > \varepsilon) \to 0$ as $n \to \infty$

Efficiency : $T = \min \{T_n$ is unbiased $\forall n \in N\}$

MSE (Mean Squared Error)

$MSE = \mathrm{Var}\, T + \mathrm{Bias}(T|\theta)^2.$

Fréchet - Cramer - Rao Lower Bound.

For an unbiased estimator T of paramater θ.

the variance of T is

$$\mathrm{Var}\, T \geq \frac{1}{nI}$$

where I is the Fisher Information and n is the number of times the experiment is repeated.

Expected Value: $E(x)$

$E(x) = \sum x_i p(x_i)$ → assume the probabilities are discrete.

$E(x) = \int_\Omega x p(x) dx$ → continuous probabilities.

$E(5X) = 5E(X)$

$E(X+Y) = E(X) + E(Y)$

$E(3X+5Y+4) = 3E(X) + 5E(Y) + E(4)$

Variance $\sigma^2 = \frac{\sum(x_i - \mu)^2}{n-1}$ → degree of freedom.

Standard Deviation σ.

$\mathrm{Var}(5X) = 5^2 \mathrm{Var}(X)$

$\mathrm{Var}(5X+4Y) = 5^2\mathrm{Var}(X) + 4^2\mathrm{Var}(Y)$

$\mathrm{Var}(3X-3Y+9) = 3^2\mathrm{Var}(X) + 3^2\mathrm{Var}(Y)$

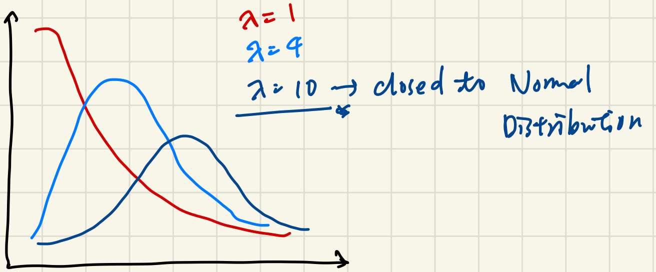
Poisson Distribution.

$$PMF = \frac{\lambda^k e^{-\lambda}}{k!}$$

exp.

$$P_0 = \frac{\lambda^0 e^{-\lambda}}{0!} = e^{-\lambda}.$$

probability of zero is not trivial



λ = average number of events.

$$z\text{-score} = \frac{x-\mu}{\sigma}.$$