Chinese Remainder Theorm

* If $GCD(a,b) = 1$; $\forall (r,s)\ \exists\ x$ in mod (ab) such that:-

$$\boxed{x \equiv r \pmod a \quad \text{and} \quad x \equiv S \pmod b}$$

Idea:- Do Skippy clock with 1^{st} clock's hand at arbitrary k.

Now; after 'a' steps it will be back and 2^{nd} will be at $[a]_b$

Repeating; values taken by $b \equiv [ta]_b$

if $GCD = 1 \Rightarrow$ all positions covered.

$GCD = g \Rightarrow$ multiples of 'g' only covered in b'

* By Bezout's; $x = bvr + aus$ where $au + bv = 1$

- Now, because $x = (r,S)$ uniquely; $x = (rem(x,a), rem(x,b))$

Co-ordinate rep. can be used to do Arithmetic!

1) $(r,s) +_m (r',s') = (r +_a r', S +_b S')$ – additive inverses

2) $(r,s) \times_m (r',s') = (r \times_a r', S \times_b S')$ – Mult. inverses

* CRT for arbitrary

$m = a_1 \cdot a_2 \cdot \ldots a_n$ and $GCD(a_i, a_j) = 1$ for $i \neq j$

For any $\{r_1, r_2, \ldots r_n\}$ where $r_i \in [0, a_i)$

$\rightarrow \exists!\ x$ such that $x \equiv r_i \pmod{a_i}$

Prove via Weak Induction from $n = 1$.

Lecture-3G

Friday, September 4, 2020 12:50 PM

$\boxed{\forall a \in Z_m^*;\ \gcd(a,m)=1}$

- Z_m^* is set of elements of Z_m with multiplicative inverse.
  - Elements of Z_m^* = "Units". 0 can never be a unit!
  - number of units for $p^k \Rightarrow p^k - p^{k-1}$ p = prime ; $k \neq 1$

    $\Rightarrow (p-1)$ when $k=1$

    ↳ Now; for $m = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}$

    By Extended CRT; $m = (r_1, r_2, \ldots, r_n)$

    $$\Rightarrow \text{num}(m) = \text{num}(r_1) \cdot \text{num}(r_2) \cdots$$
    $$= \left[p_1^{k_1} - p_1^{k_1-1}\right]\left[p_2^{k_2} - p_2^{k_2-1}\right] \cdots$$
    $$= \underline{m\left[1 - \frac{1}{p_1}\right]\left[1 - \frac{1}{p_2}\right]\left[\ldots\right]}$$

* Euler's Totient Function - $\phi(m)$

- By defn. $|Z_m^*| = \phi(m)$

  if $\underline{\gcd(a,b)=1} \Rightarrow \underline{\phi(ab) = \phi(a)\phi(b)}$

  multiplicative functions!

- We can also prove if $a \in Z_m \cap Z_m^{*!}$; $\exists\, b \in Z_m$ s.t $ab = 0$

  $b = a/\gcd(m,a)$

* Arithmetic Properties

1) if $a \in Z_m^*$; $a^{-1} \in Z_m^*$
2) $\forall (a,b) \in Z_m^*$ $ab \in Z_m^*$ — Closure
3) $\forall a \in Z_m^*$ $a \cdot Z_m^* = Z_m^*$ — Prove by taking a, a^{-1} and show

   $aZ \subseteq Z$ $Z \subseteq aZ$

* Exponentiation:- $a \in Z_m$, $\underline{d \in \mathbb{Z}^+}$ $a^d \triangleq a \times_m \cdots a$ (d times)

↳ not in modular form!

- For Z_m^*; we can extend to $d = \mathbb{Z}$ with $\boxed{a^0 = 1}$; $a^{-d} = (a^{-1})^d$

* Euler's Totient Theorm:- $\phi(m)$ is not smallest d s.t $a^d = 1$

$\forall a \in Z_m^*$; $a^{\phi(m)} = 1 \pmod m$ $\longrightarrow$ m = prime $\Rightarrow$ Fermat's little theorm

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

Proof:- $Z_m^* = \{x_1, x_2, \cdots x_n\}$ where $n = \phi(m)$

$u = x_1 \cdot x_2 \cdots$ and $w = (ax_1)(ax_2)\ldots$ where $a \in Z_m^*$

$\Rightarrow$ $\boxed{w = a^n u}$

However; $w = u$! (Closure prop.) $\Rightarrow \boxed{a^n = 1}$

Important fact:- If p is prime; $\exists g$ such that $\forall a \in Z_p^*$ $a = g^k$ (k is some int.)

Stated w/o proof

- g is called "Generator of Z_p^*" or "a primitive root of Z_p^*"
- We can write Z_p^* as $1, g, g^2, \cdots g^{p-2}$ $\Rightarrow$ $g^{p-1} = 1$ by ETT.

However, notice that the exponents form a Z_{p-1}!

$\Rightarrow$ We can label Z_p^* as Z_{p-1} and do calculations there if 'g' is known.

$$[g^a \cdot g^b]_p = [a+b]_{p-1}$$

- Getting Z_p^* if Z_{p-1} is known is easy; but reverse is not.
- Discrete log:- given 'g' for Z_p^* and $k \in Z_p^*$; the value of $a \in Z_{p-1}$ s.t $\boxed{g^a = k}$

Lecture-3H

Monday, September 7, 2020 4:50 AM

- For $a \in \mathbb{Z}_m^*$; can see that $a^c = a^d$ iff $c \equiv d \pmod{\phi(m)}$ → $\gcd(e, \phi(m)) = 1$

  1) Define e^{th} root :- given x^e find e ⇒ if $\exists d$ s.t $ed \equiv 1 \pmod{\phi(m)}$ then $(x^e)^d = x$

     - $a^{1/e}$ may/may not Exist ; may/may not be unique.

- * Exponentiation, inverse via EEA * — (Note in Sep. Secn maybe)

- If m is a product of distinct primes ; $\forall a \in \mathbb{Z}_m$ (not $a \in \mathbb{Z}_m^*$! no restriction)

  1) $a^{k\phi(m)+1} = a$ CRT for $P_1, P_2, \dots, P_k$; Consider Cases

  2) if $\gcd(e, \phi(m)) = 1$; $a^{1/e}$ exists uniquely. (above, $a \in \mathbb{Z}_m^*$. Here, $a \in \mathbb{Z}_m$)

     ↳ Method to Solve is just like above

* **Squares** :-

- Notice that for all $m > 2$; $\gcd(\phi(m), 2) = 2$ ⇒ Not well defined!

- Elements in $\mathbb{Z}_m$ of the form x^2 are called Quadratic Residues.

↳ Considering $\mathbb{Z}_p^*$; all g^{2n} are Quadratic Residues. ⇒ $\boxed{QR_p^*}$

  1) $z \in QR_p^* \leftrightarrow z^{(p-1)/2} = 1$

— * $ab = 0 \not\Leftrightarrow a = 0$ or $b = 0$!! * —

  holds if $a, b \in \mathbb{Z}_p$; p = prime

$\boxed{\text{In } \mathbb{Z}_p^* ; (a^e)^{1/e} \text{ has } \gcd(e, p-1) \text{ values}}$

↳ If $\frac{p-1}{2}$ is odd ; then $\forall a \in QR_p^* \to a^2 \in QR_p^*$

Lecture-4A

Wednesday, September 9, 2020 5:47 AM

- Let A and B two sets. $A \subseteq B \not\to A \in B$

  for Example, look at $A=\phi$, $B=\mathbb{Z}$:- $\phi \notin \mathbb{Z}$ but $\phi \subseteq B$!

- Predicates can be used to define sets and vice-versa!

  Predicate to Set :- $A = \{x \mid P(x) = T\}$ Set to Predicate :- "Membership Predicate" $\to$ $In(S)$

- From above; we can also define Set operations in terms of prop. calculus.

  1) $\bar{S} \Rightarrow in(\bar{S}(x)) = \neg in(S(x))$ $inS(x) \equiv \{x \in S\}$

  2) $S \cup T \Rightarrow inS(x) \vee inT(x)$ 3) $S \cap T \Rightarrow inS(x) \wedge inT(x)$

  4) $S - T \Rightarrow inS(x) \wedge \neg inT(x) \equiv inS(x) \not\to inT(x)$

  5) $S \Delta T \Rightarrow inS(x) \oplus inT(x)$

  All of Propositional Calculus holds!

- $S \subseteq T$ can be written as $\forall x \; x \in S \to x \in T$; $S = T$ is $\forall x \; x \in S \leftrightarrow x \in T$

  $\bar{T} \subseteq \bar{S}$

* <u>Inclusion-Exclusion</u>:-

↳ $|R+S+T| = |R| + |S| + |T| - [|R \cap S| + |R \cap T| + |S \cap T|] + |R \cap S \cap T|$

* <u>Cartesian Product</u>:-

↳ $R \times S = \{(r,s) \mid r \in R \text{ and } s \in S\}$ $\Rightarrow$ $R \times S = \phi \leftrightarrow \{R = \phi \cup S = \phi\}$

↳ $R \times S \times T \neq (R \times S) \times T$ but Essentially the same.

↳ $(A \cup B) \times C = (A \times C) \cup (B \times C)$ $(A \cap B) \times C = (A \times C) \cap (B \cap C)$ — Distributive!

↳ $\overline{A \times B} = (\bar{A} \times \bar{B}) \cup (\bar{A} \times B) \cup (A \times \bar{B})$ — Complement.

Lecture-4B

Saturday, September 12, 2020 12:23 PM

Relations :-

- A predicate for $S \times S$ (homogenous) $\Rightarrow$ Likes(x,y) , $(x,y) \in S \times S$

  ↳ Subset of $S \times S$ for which predicate is true

- Represented as $x R y$.

- All set operations apply to Relations as well.

* Converse :- $R^T = \{(x,y) \mid (y,x) \in R\}$

* Composition :- $R \circ R' = \{(x,y) \mid \exists \omega, (x,\omega) \in R \text{ and } (\omega, y) \in R'\}$

  - For Bool matrices; $(R \circ R')_{xy} = \bigvee_{\omega} (R_{x\omega} \wedge R'_{\omega y})$

- Reflexive :- $\forall x \in S;\ (x,x) \in R$ | Diagonal of bool matrix = True

  Irreflexive :- $\forall x \in S;\ (x,x) \notin R$ – No edge to self

- Symmetric :- $\forall (x,y) \in S \times S;\ (x,y) \in R \wedge (y,x) \in R$ $(x \neq y)$ | $R = R^T$ for bool

  Asymmetric :- If $(x,y) \in R$ then $(y,x) \notin R$. — No double edges $\rightarrow x, y$ need not be distinct!

  Anti Symmetric :- if $(x,y) \in R$ and $(y,x) \in R$ then $x = y$ $\Rightarrow$ what we usually mean.

- Transitive :- if aRb and bRc, then aRc. Intransitive = Not transitive

  * $R \circ R \subseteq R$ also; $\forall k > 1;\ R^k \subseteq R$

- Equivalence $\equiv$ Reflexive, Sym., transitive

* Given R; we define :-

(1) Reflexive Closure – Smallest $R' \supseteq R$ s.t. R' is reflexive

(1) Reflexive Closure – Smallest $R' \supseteq R$ s.t R' is reflexive

(2) Symmetric Closure – Smallest $R' \supseteq R$ st R' is symmetric

(3) Transitive Closure – " transitive.

All unique!

* <u>Equivalence</u> <u>Class</u>:- $Eq(x) = \{y \mid xRy\}$ here R is Equivalent.

- If $Eq(x) \cap Eq(y) \neq \phi$, then $Eq(x) = Eq(y)$
- Also; $Eq_1(x) \cup Eq_2(x) \ldots = S$

(**)

Lecture-4C

Wednesday, September 16, 2020 1:11 PM

* A transitive - Anti Symmetric Relation is Acyclic
  transitive - Symmetric Relation is Cyclic.

* Partial Order Sets :-

  - We know that transitive - Reflexive - Symmetric ⇒ Equivalence =

  - Similarly :- Transitive - Reflexic - AntiSymmetric ⇒ Partial orders $\geq, \leq$

    if irreflexive, Strict partial Orders $<, >$

  - $\boxed{\text{Transitive + acyclic} \leftrightarrow \text{Partially ordered}}$ — (**)

    acyclic replaces Symmetric! (in case of transitive)

    if Reflexive, PO ; if irreflexive, SPO.

  - Poset is represented like (S,R) :- R is the relation being applied over S

* Maximal & Minimal :-

  - x is maximal for (S,R) iff $\nexists y \in S - \{x\}$ such that $x R y$

    x is minimal for (S,R) iff $\nexists y \in S - \{x\}$ such that $y R x$

    Will write R as $\leq$ for ease!

  - Need not be unique, or even existent.

    However; if S is finite, then they def. Exist! — Will use directly in induction.

    prove by str induction.

  - Greatest Element :- $x \in S$ s.t $\forall y \in S$ $y \leq x$ — Need not Exist..

    Smallest " :- $x \in S$ s.t $\forall y \in S$ $x \leq y$

* Reflexive Reduction of $\leq$:- Relation obtained on removing Self-loops = $<$

  Reflexive Closure of $< \Rightarrow \leq$ SPO

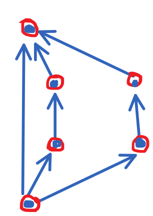
* Transitive Reduction of $\leq$:-

  - $\sqsubseteq$ is trans. reduction iff ⇒ $[a \sqsubseteq b \rightarrow \nexists m \in S - \{a,b\}$ s.t $a \leq m \leq b]$ → No Element is transitive!

  - Transitive Closure of $\sqsubseteq$ = $\leq$

  - Exists for Finite posets :- need not be for ∞.

    Proof By Induction? Try doing by self.



Not a transitive reduction!

* Hasse Diag :- Draw transitive reduction of (S,R) for simplicity.

* Hasse Diag :- Draw transitive reduction of (S,R) for simplicity.

* Bounding Elements :-

  - for $T \subseteq S$; x is upper bound of $T \Rightarrow \forall y \in T,\ y \le x$ $\Rightarrow$ Define greatest LB and Least UB

    for " x is lower bound of $T \Rightarrow \forall y \in T,\ x \le y$

    if it exists, it is unique

* Total / Linear Order :- All pairs are comparable.

* Order Extension :- for $(S, \preccurlyeq)$; (S,R) is extension if $a \preccurlyeq b \rightarrow aRb$

  - We can extend Poset to totally ordered set $\longrightarrow$ Topological Sorting

  - Order Extension Principle is usally taken as an Axiom !

Lecture-4D

Saturday, September 19, 2020 8:53 PM

<u>Chain</u>:-

- Given poset $(S, \leq)$; $O \subseteq S$ is a chain if O is totally ordered.

  i.e., all distinct Elements are related to each other.

- Anti Chain means no two distint Elements are comparable.

  Meaning, self-loops can be present.

- Singular Elements are both chains and anti-chains! ϕ is an Anti-Chain!

* From this; $n(\text{Chain} \cap \text{Anti-Chain}) \leq 1$

* <u>Height of an Element</u>:- $a \in S$

- Height(a) = Max length of chain with 'a' as maximum.

  This will be atleast 1 :- $\{a\}$ → Well defined for finite S, $S \neq \phi$

  Always check if the set you're considering for height is a chain!

- Define height of poset as :- Size of largest chain in poset

  = Max(heights)

** Literally the height of element in Hasse diagram! **

- Let $A_H = \left\{ a \,\middle|\, \text{Height}(a) = H \right\}$:- Set of elements with same height.

  ⇒ A_H is an anti-Chain! → Simple enough, prove by contr.

- Also, from Hasse's diagram :- we can see that all A_h partition S exactly.

  Mirsky's theorm :- A_h are the least number of partitions into Anti-Chains

  ↳ Like, min. number = Height of poset. All partitions need not be A_h, though

We can see that each element in longest chain must be in different sets.

* Dilworth's theorm :- Least number of chains partitioning S = Length of biggest anti-chain.

Mirsky's theorm :- Least number of a.c partitioning S = Length of biggest chain.

Functions :- $f: A \to B$

- Maps elements in Domain to elements in Co-domain.
- Image of $f \Rightarrow \{y \in B \mid \exists x \in A, f(x) = y\}$ $\Rightarrow$ Elements of Co-domain which are used.

- If both domain - Codomain are totally ordered ; plotting it is possible
- Composition of functions $\Rightarrow$ $g \circ f(x) \Leftrightarrow Im(f) \subseteq dom(g)$

* Types of Functions :-

1) Onto — Surjection → Check Co-domain
2) One - One → Check domain - Injective
3) Bijection → Both one-one and onto

* Invertible :-

- $\boxed{\text{Injective} \leftrightarrow \text{Invertible}}$

$f: A \to B$

- f is said to be invertible iff $\exists g$, $g \circ f(x) = x \ \forall x \in A$
- Notice that f^{-1} need not be invertible/unique
  - ↳ becomes unique if f is a bijection.

Graphs

- Have many physical interpretations such as social networks and the such.
- We typically want graphs with few connections but good connectivity.

NP-hard — A class of problems without an efficient Algo.

Definition Simple Graphs

- A simple graph $G = (V, E)$ where V – Non empty and finite set of nodes

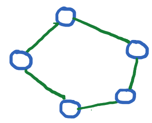
$$E \subseteq \{ \{a,b\} \mid a,b \in V ; a \neq b \}$$

- In terms of relations; a simple graph would be symmetric and irreflexive.

Definition Complete graph K_n — n nodes, all possible edges present.

$$E = \{ \{a,b\} \mid a,b \in V, a \neq b \}$$

Cycle C_n — $V = \{v_1, \dots, v_n\}$, $E = \{ \{v_i, v_j\} \mid j = i+1 \text{ or } (i = n, j = 1) \}$

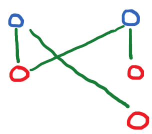


n = number of nodes

$\to C_5$

Bipartite graph – Set V is partitioned into V_1 and V_2 ; no edge within V_1, V_2

$$E \subseteq \{ \{a,b\} \mid a \in V_1, b \in V_2 \}$$



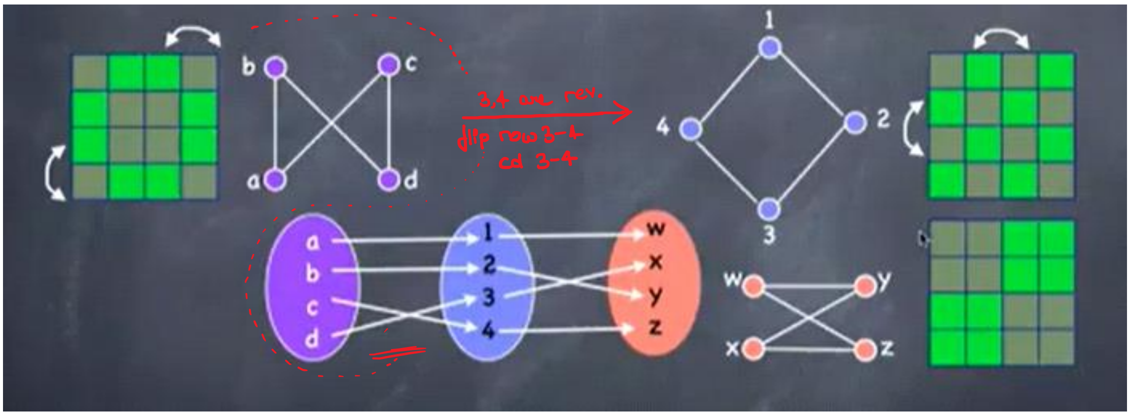
Complete bipartite graph K_{n_1, n_2} — $n(V_1) = n_1$ and $n(V_2) = n_2$

All possible edges are present.

Definition **Graph Isomorphism**

- G_1, G_2 are isomorphic if one is a relabelling of another
- Formally :- $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic iff there is a bijection
  $f : V_1 \to V_2$ such that $\{u, v\} \in E_1$ iff $\{f(u), f(v)\} \in E_2$

- Adjcency matrix :- A boolean matrix keeping track of which vertices are adjacent.



- No efficient algorithm is known to check if two graphs are isomorphic

Definition **Subgraph**

- $G_1 = (V_1, E_1)$ is a subgraph of $G_2(V_2, E_2)$ iff $V_1 \subseteq V_2$ and $E_1 \subseteq E_2$

Definition **Walk** – A walk of length 'k', $k \geq 0$, from node a to node b is a sequence of nodes
$(v_0, v_1, \ldots, v_k)$ such that $v_0 = a$; $v_k = b$ and $\{v_i, v_{i+1}\} \in E$

Path – A walk with no node repeating

Cycle – A walk with $k \geq 3$ where $v_0 = v_k$ and no other repetition occurs.

- A graph is acyclic if no cycle is its subgraph

Definition **Connectivity**

- Let u,v be two nodes. They are said to be connected iff a path/walk exists from u to v.

- The relation connected(u,v) is equivalence in nature.

  every node is related to itself!

- The equivalence classes are called as connected components.

Definition **Degree of a vertex**

- The number of edges incident on the vertex.

$$\deg(v) = \left| \{ u : \{u,v\} \in E \} \right|$$

Lemma $\sum_i \deg(v_i) = 2n(E)$ — every edge is counted twice.

Definition **Degree Sequence**

- Sorted list of degrees of all vertices in a given graph.

- Invariant under isomorphism. $\Rightarrow$ To disprove isomorphism, check this first!

Definition **Eulerian trail**

- A walk which visits every edge exactly once

Theorem Eulerian trail exists $\longrightarrow$ at most 2 odd degree nodes.

Define enter(v) and exit(v) :- for all v other than start and end have |enter(v)| = |exit(v)|

Eulerian circuit - a closed Eulerian trail $\Rightarrow$ start and end nodes are the same

Eulerian circuit Exists $\longleftrightarrow$ No odd degree AND all edges in one connected component

Definition **Hamiltonian Cycle**

- A cycle which visits all $\boxed{\text{nodes}}$ exactly once.
- No efficient algorithm to check if a graph has a hamiltonian cycle.

– NP-hard problem –

Definition **Distance**

- Shortest walk between two nodes is a path. (obviously!)
- The Length of shortest path is called distance. (∞ if no path)
- Graphs can be used to model probalistic processes; with shortest being most likely
- Diameter – the Largest distance in a graph

* Graph Coloring :-

- We know that the partitions of a bi-partite graph can be "coloured" so that no edge exists between two nodes of the same colour. This is said to be proper colouring.

Definition :- a function $C: V \to \{1, \dots, k\}$, $\forall \{x, y\} \in E \to C(x) \neq C(y)$

- 'C' need not be onto, as we dont need to use all colours.

Definition:- Chromatic Number –

- The least number of colours needed to properly colour Graph G.
- Represented as $\chi(G)$

- If a graph can be coloured using 'k' colours; $\chi(G) \leq k \Rightarrow$ used to find upper bound of $\chi(G)$
- Notice that if H is a subgraph of G ; $\chi(H) \leq \chi(G)$

1) If K_n is subgraph of G $\Rightarrow \chi(G) \geq n$

2) If C_n is subgraph with odd $n \Rightarrow \chi(G) \geq 3$

$\Rightarrow$ used to find Lower bound of $\chi(G)$

- Also, notice that $\chi(G)$ is invariant to isomorphism!

- Calculating $\chi(G)$ is an "NP-hard" problem.

- Practical applications refer to a "conflict graph".

* <u>Bipartite Graph</u>:-

Theorem A graph is bipartite $\boxed{\text{iff}}$ it contains no odd cycle. $\Rightarrow$ if $C_{2n+1} \notin G \leftrightarrow \chi(G) \leq 2$

$\leftarrow$ is easy, prove by contradiction. ($\rightarrow$ proof ??)

* <u>Complete graph</u>:- "Clique"

Theorem Let G have 'n' nodes. $\chi(G) = n \leftrightarrow G$ is isomorphic to K_n

$\leftarrow$: Invariability ; $\rightarrow$ prove by contradiction.

Definition Clique Number $\omega(G)$ – The largest subgraph of G which is isomorphic to a complete graph. $\chi(G) \geq \omega(G)$

Independance Number $\alpha(G)$ – The number of nodes in largest subgraph with no edges. $\chi(G) \geq n/\alpha(G)$

- We have two lower bounds for $\chi(G)$. We shall now prove an upper bound for $\chi(G)$.

Theorem:- $\chi(G) \leq \Delta(G) + 1$ where ΔG = max order of a node in graph G.

* prove by induction. Can be proved by contradiction even faster.

- The equality holds for a clique and C_{2n+1} only! —(**)

* Some special graphs

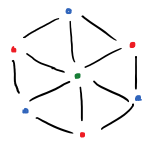
(Defined diff than wikipedia)

1) Path graph $P_n \equiv$ (n=4)

- $V = \{1,2,\ldots n\}$, $E = \{(i,i+1) \mid i \in [1,n)\}$
- $\chi(P_n) = 2$

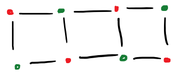
2) Wheel graph W_n $(n \geq 3)$

$\boxed{n=6}$



- $\chi(W_n) = 3$
- $V = \{hub\} \cup \mathbb{Z}_n$; $E = \{(i,i+1) \mid i \in \mathbb{Z}_n\} \cup \{(hub, i)\}$

3) Ladder graph $L_n \equiv$ (n=4)



- $\chi(L_n) = 2$
- $V = \{0,1\} \times \{1,\ldots,n\}$

$E = \{\{(b,i),(b,i+1)\} \mid b = 0,1\} \cup \{\{(0,i),(1,i)\}\}$

4) Circular Ladder graph CL_n :-

- Just connect the ends

$\chi(CL_n) \neq 2$ when $n = $ odd

* Hypercubes :- Q_n

V - all n-bit strings ; E — x,y connected if they differ only at a single bit.

- Clearly visible that the diameter $= n$
- Q_n is n-regular bipartite graph, and Q_{n-1} is a subgraph of Q_n.

partition wrt parity

prefix Q_{n-1} with a '0' and '1' respectively

* Knesser Graph - KG_n

- $V = P(S)$ where $S = \{1,2,\ldots,n\}$

E = disjoint subsets of S.

$\rightarrow$ $\overline{KG_n} \Rightarrow$ Edges b/w non-empty intersections

$\Downarrow$

Erdos-Ko-Rado theorem.

- All set operations can be extended to Graphs as well.

$G_1(V,E_1)$, $G_2(V,E_2) \Rightarrow \cup, \cap, \Delta, (-)$

$G_1(V_1,E_1), G_2(V_2,E_2) \Rightarrow \cup, \cap$

- Power of a graph; $G^2 = (V,E')$, $E' = \{(x,y) \mid (x,z),(z,y) \in E\}$

For $\{x,y\} \in E$ of G^k; a path from x to y of atmost length 'k' should exist.

* Cross product :-

Definition Let $G_1(V_1,E_1)$ and $G_2(V_2,E_2)$. The cross product $G_1 \times G_2$ is defined by $(V_1 \times V_2, E)$ where

$E = \{(u_1,u_2),(v_1,v_2)\}$ where $(u_1,v_1) \in E_1$ and $(u_2,v_2) \in E_2$.

- Bipartite double cover – $G' = G \times K_2$; where K_2 is a bipartite graph.
  - Has all info of G; but in a bipartite space.

* Box product – $G_1 \square G_2 = (V_1 \times V_2, E)$

$E = \{(u_1,u_2),(v_1,v_2)\}$ where $(u_1,v_1) \in E_1$ and $u_2 = v_2$

or $(u_2,v_2) \in E_2$ and $u_1 = v_1$

- Can be seen that $Q_n \square Q_m = Q_{n+m}$
- We use box products in the defn of a Hamming graph.

$H_{nq} = K_q \square \cdots \square K_q$ (n times)

– Can be seen that this gives hypercubes for $q=2$.

Graph Matching

- A set of edges in a graph which donot share any vertex is called as a "matching."

  i.e., every node gets matched with atmost one other node

- Trivially, ϕ is a matching.

- A subset of Edges, M, is said to be a Perfect Matching if all vertices are mapped

  by it, this may or may not exist.

- Finding the largest possible mapping is not NP-hard, and algorithms do exist.

* Matching in Bipartite graphs

Let $G(X,Y,E)$ be the bipartite graph where X,Y are the disjoint sets of vertices.

Definition We define a matching to be a Complete matching from X to Y if all the nodes in X are matched to an element in Y.

* Neighbourhoods:-

Definition Given $G(V,E)$ and $v \in V$; nbd of $v \equiv \Gamma(\{v\}) = \{u \mid \{u,v\} \in E\}$

$$S \subseteq V \text{ ; nbd of } S \equiv \Gamma(S) = \bigcup_{v \in S} \Gamma(v)$$

- Take a bipartite graph $G(X,Y,E)$. For $S \in X$;
  - If $|\Gamma(S)| < |S|$, we say that the neighbourhood is shrinking
  - For some $B \in Y$; If $|\Gamma(S) \cap B| < |S|$, we say that the nbd is shrinking in B.

Theorem **Halls Theorem :-**

- A bipartite graph $G(X, Y, E)$ has a complete matching from X to Y $\boxed{\text{iff}}$ no subset of X is shrinking.

Proof :- complete matching $\rightarrow$ no shrinking subset is easy enough to prove by contradiction.

no shrinking subset $\longrightarrow$ complete matching :- prove via strong induction on $|X|$

Application :- The edge set of any bipartite graph where each vertex has degree 'd', can be partitioned into 'd' matchings.

We prove this by induction on 'd'. It holds for $d=1$.

Hypothesis — For a given $d \geq 1$, this holds

Step :- Given that degree of each $= d+1$. If a single perfect matching is found, by removing these edges and from hypothesis we get the remaining 'd' partitions.

- Take a subset S of X. # of edges coming out of $S = d \cdot |S|$

# of edges incident on $\Gamma(S) = d \cdot |\Gamma(S)|$

and we know that # of edges coming outta $S \leq$ # of edges incident on $\Gamma(S)$

$\Rightarrow$ $|S| \leq |\Gamma(S)|$ $\Rightarrow$ no shrinking $\Rightarrow$ one matching exists!

* Vertex Cover :-

Definition For a given graph $G(V,E)$; $C \subseteq V$ is said to be a vertex cover if all edges in G is incident on atleast 1 vertex in C.

- Trivially, for a graph $G(V,E)$; V is obv. a vertex cover, and so is $V - \{v\}$, $\forall v \in V$
- Finding the smallest possible vertex cover is an NP-hard problem.
- However, we'll be able connect finding the smallest vertex cover with a maximum matching, and this is very strong in the case of bipartite graphs.

Relation 1 :- For a vertex cover C, matching M; $|C| \geq |M|$, for a general graph.

Königs theorem - In a bipartite graph, size of smallest vertex cover equals size of max. matching.

Proof by hall's theorem

Let C be the smallest vertex cover $\Rightarrow$ Let $C \cap X = A$, $C \cap Y = B$; Enough to show for A, as B would hold by symmetry. Looking at $A \to (Y-B)$; we can show that no shrinking subset of A exists in Y-B, by contradiction.

$\Rightarrow$ By hall's theorem; matching from A to Y-B exists. $\Rightarrow$ # edges $= |A|$

Similarly from B to Y-A $\Rightarrow$ # edges $= |B|$

put together, we get a mapping of size $|A| + |B| = |C|$ //.

- We define a Maximal matching to make finding smallest vertex cover a little easier.

Definition A matching, M, is said to be maximal if adding a new edge would cause M to stop being a matching.

- Can be converted to a vertex cover pretty easily, just take both endpoints of all edges in M.

* Independant Set :-

Definition A subset $I \subseteq V$ is independent set if no edge exists between any vertices in I.

Notice that $\overline{I}$ is a vertex cover.

→ Finding the largest independant set is NP-hard as well.

Trees

- A tree is simply a connected acyclic graph.

  Forest is just defined as an acyclic graph. Any subgraph of a forest (or tree) is also forest.

- Leaf – node with degree 1.

Statement ⊢ Every tree with atleast two nodes has atleast two leaves.

(to prove, look at the maximal path of the tree, and prove that the ends are leaves)

- Deleting a leaf from a tree yields another tree. This property is used to have induction on trees.

  ie, use this property during the induction step to get n-node tree from (n+1) nodes.

Example for Induction

Statement – For a tree G(V,E) ; $|E| = |V| - 1$ (Converse also true! If $|E| = |V| - 1 \rightarrow$ Graph is tree)

By induction on $|V|$ ⇒ $|V| = 1$ ⇒ $|E| = 1 - 1 = 0$

Let $|V| = n$; for (n+1) nodes tree, shrink by deleting 1 and use hypothesis.

* Rooted tree :-

- A tree with a special designated node called the "root".
- u is an ancestor of v, and v is desendant of u ; iff path from root to v passes through u.
- Leaf = has no descendants.

- Depth - Length of the path from root to that node.
  - Level i - Set of nodes of depth i .
- Arity - max. number of children for a node
  - Full m-ary tree is a tree with all nodes having same number of childeren
  - Complete tree has all leaves at the same level.