DM ESE

20 November 2023 04:13 PM

Order Relations

A binary relation R defined on a set A is an order relation if it is transitive & it helps compare two elements of a set.

Partial OR $\langle \overset{\text{set}}{A}, \overset{\text{relation}}{R} \rangle \rightarrow$ poset

$\langle P(A), \subseteq \rangle$

→ binary relation

→ transitive $(a,b) \wedge (b,c) \Rightarrow (a,c)$

→ antisymmetric $(a,b) \wedge (b,a) \Rightarrow (a=b)$

→ reflexive (a,a)

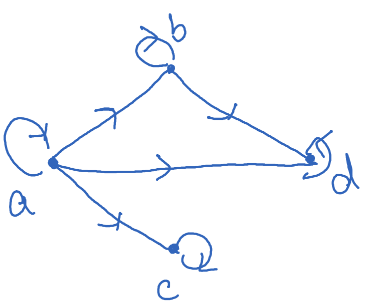
Hash Diagram

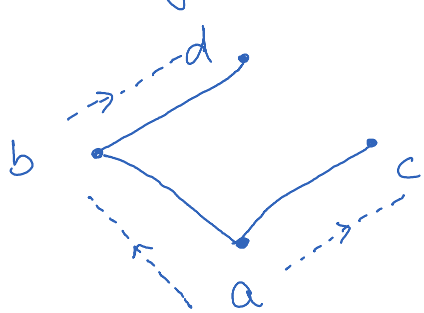
→ using relations like reflexive, antisymmetric, transitive we can make minimal paths. Rest can be found out using this relation.

if (a,b) $a \longrightarrow b$

We put the direc^n of nodes from top to bottom

if ignore self loops





bottom most node origin of direc^ns

Topological Sort

A set of tasks and a dependency relation R st $(a,b) \in R$ then task b must start after task a is finished.

b must start after task a is finished.

→ Can give multiple correct outputs.

Topological Set (S, n, R)

$K = 1$

while $S \neq \emptyset$

a_K = minimal element of S

$S = S \setminus \{a_K\}$

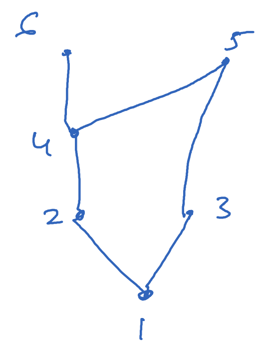
$K = K+1$

output = $\{a_1\ a_2 \dots\}$

minimal element → not unique

minimum element → unique.

Notation : $\langle A, \preccurlyeq \rangle$



1 2 3 4 5 6

1 3 2 4 5 6

1 2 3 4 6 5

1 3 2 4 6 5

Quasi OR

→ ordinary relation

→ transitive

→ irreflexive

→ Antisymmetric (implicit)

since antisymmetric relations are implicit they are not considered in hash diagram.

Linear / Total OR

→ Posets ie partial OR

→ $\forall a, b \left(a, b \in A \Rightarrow aRb \vee bRa \right)$

A ↓ set

R = relation

$\langle P(A), \subseteq \rangle$ is not a total OR

Well Order Relation $\langle A, R \rangle$

→ Linear OR

→ every non-empty subset of A has a minimum element.

$\langle \mathbb{Z}, \leq \rangle$ is not a Well order relation.

$\langle \mathbb{N}, \leq \rangle$ is a W.O.R.

Graphs $G(V, E)$

$|E| \geq 0$ but $|V| > 0$

simple graph: no self loops & parallel edges.

degree (u) = # edges $\underbrace{\text{incident}}$ on u in $G(V,E)$

e incident on u if $e \in (u,v)$

Hand shaking theorem.

$G(V,E)$ undirected graph $|E| = m$

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

* any undirected graph has even number of vertices with odd degree

Simple Graphs:

1) Complete : each pair of vertices will have an edge between them.
(denoted by K_n) $n = \#$ vertices.

2) Cyclic : has a loop.
denoted by C_n $n \geq 3$ $n = \#$ vertices.

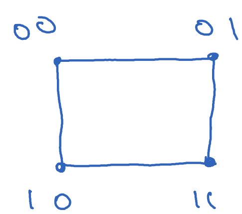
3) Wheel : An vertex (V_n) added in center of C_{n-1}
V_n is adjacent to all $V_1 \dots V_{n-1}$

denoted by W_n

4) n-cube / hyper cube Q_n

$Q_n = 2Q_{n-1}$ attach vertices differing at one bit only.

Q_1



Q_2

Walk in a graph.

Alternating sequence of vertices and edges.

Start & end with vertices

a walk = path if all vertices are distinct

a walk = trail if all edges are distinct.

Regular Graph

A graph is called k-regular if all vertices of K_n have same degree

A cycle = 2-regular

Connected Graph.

there is a path b/w every two vertices.

Subgraph

Maximally connected components of a graph.

$G'(V', E')$ $\quad V' \subseteq V$ & $E' \subseteq E$

Theorem.

Let $G(V, E)$ of order n ie $|V| = n$ if

$\deg(u) + \deg(v) \geq n-1$ for any two non-adjacent vertices u & v

then $G(V, E)$ is connected graph.

from pigeon hole principal.

Bipartite Graph.

$G(V, E)$ if partitions of $V \to V_1$ & V_2 exists such that $V_1 \cup V_2 = V$

$V_1 \cap V_2 = \phi$

$\forall e (e = (v_i, v_j) \to v_i \in V_1 \wedge v_j \in V_2)$

$$\sum_{v \in V_1} \deg(v) = \sum_{v \in V_2} \deg(v)$$

C_n n = even are bipartite.

Complete bipartite graph $\forall e \left(e \in (v_i, v_j) \Leftrightarrow v_i \in V_1 \wedge v_j \in V_2 \right)$

Isomorphic Graph.

if there is one-to-one correspondence b/w vertices of graph & vertices preserve the incident relation.

H, G = isomorphic graph iff there exists bijective mapping

$\phi : V(E) \to V(H)$ st $(u,v) \in E(G)$ iff $(\phi(u), \phi(v)) \in E(H)$

→ have same $|V|$, $|E|$

→ have same no. of vertices with same degree & same connectivity.

Euler Graph.

if some closed (start & end at same vertex) walk in a graph contains all of the edges of the graph, the walk = Euler Line & the graph is Euler Graph.

theorem: if $\forall e$ (deg(e) ≥ 2 & deg(e) is even) then euler graph.

Fleur's Algorithm.

At each iteration, we can move across an edge where deletion does not occur in disconnected graph until & unless no choice left. the sequence of deleted gives us Eulerian trail

Vertex Induced Subgraph.

→ subgraph

→ follows adjancy relationship

Complement of a Graph $\bar{G}(V, \bar{E})$

$\bar{G}(V, E')$ $E' = \forall\, u, v \left(u \in V(G) \wedge v \in V(G) \wedge (u,v) \notin E(G) \right)$

Theorem: If $G(V, \bar{E})$ is disconnected graph, then $\bar{G}(V, E')$ is a connected graph.

proof by cases: same component u & v → adjacent / non adjacent

diff component u & v → adjacent

Hamiltonian Graph.

Hamiltonian cycle in a graph is a cycle that include each vertex of G exactly once. (traverses through each vertex once)

theorem: G = simple graph $|V| \geq 3$ $\deg(v) \geq \frac{n}{2}$ for $\forall\, v \in V$

then G is hamiltonian graph.

Trees

Acyclic directed graph with non-empty set of nodes such that

→ there is only one node called root with indegree = 0 (# edges incoming to the vertex)

→ every node other than root has indegree = 1

→ for every node a_i, there exists a unique path from root to a_i

Height: length of the longest path from root to leaf

Height: length of the longest path from root to leaf

T = binary tree   n = # nodes   h = height of T

$$h+1 \leq n \leq 2^{h+1} - 1$$

$$h \geq \lfloor \log_2(n) \rfloor$$

Complete binary tree: each node has 0 or 2 children.

Full binary tree: Complete BT with leafs at same level.

Theorem

every tree with # nodes ≥ 2 has atleast 2 leaf nodes

$v_0 \dots v_k$ longest path $\deg(v_0) = \deg(v_k) = 1$ leafs

vertices = # edges − 1

Forest

→ An undirected acyclic graph whose connected components are trees.

→ disjoint union of trees

→ Any two vertices are connected by atmost one path.

Theorem.

1) In a forest with V vertices & K components

   # edges = V − K

2) A graph is bipartite iff it doesn't have an odd cycle in it.

Diameter

diam (G) is the max dist b/w any two vertices $\max\limits_{u,v \in V} d(u,v)$

Theorem: G is a simple graph then $\text{diam}(G) \geq 3 \Rightarrow \text{diam}(\bar{G}) \leq 3$

Peterson graph: $\text{diam}(G) = 2$

Pigeon hole Principal (Simple form)

n+1 objects in n boxes. Atleast one box with objects ≥ 2

Pigeon hole Principal (Strong form)

$q_1 \ldots q_n$ = n +ve integers.

$q_1 + q_2 + \ldots q_n + n - 1$ objects in n boxes then

either first box contains atleast q_1 objects

" " second " " " q_2

⋮

" " nth " " " q_n objects

imp: $N = r\,2^K$ $r, K \geq 0$ $K = 0$ N = odd

$K \neq 0$ N = even.

$N = CK + r$ $r = 0 \ldots c-1$

COUNTABLE UNCOUNTABLE SETS

two sets have same cardinality iff there is a bijective mapping from X to Y or Y to X $|X| = |Y|$

Countable: 1) finite set
2) infinite set with same cardinality of $\mathbb{Z}^+$

1) odd integers
2) integers
3) prime numbers
4) rational numbers

$\Bigg\}$ Countable.

Theorem: An infinite set is countable iff it is possible to list the elements of the set in a specific sequence (indexed by positive integers) such that no element is repeated & no element is omitted.

To show countable, prove one:

1) finite set
2) if infinite, bijection with $\mathbb{Z}^+$
3) A well defined sequence for the elements of the set.

Binary Strings

$\Pi = \{0,1\}$ $\quad \Pi^{(i)}$ = strings of length i made from Π

$$\Pi^* = \bigcup_{i = \mathbb{Z} \setminus \mathbb{Z}^-} \Pi^{(i)}$$ Countable

Sequence = $\Pi^{(0)}, \Pi^{(1)}, \ldots$

a string of length i will be eventually listed.

Theorem: A, B = countable then $A \cup B$ = countable

C1 = A finite B finite

$a_1 \cdots a_n \quad b_1 \cdots b_n$

C2 = A finite B infinite WLOG B finite A infinite

$a_1 \cdots a_n \quad b_1 \cdots b_\infty$ $\quad b_1 \cdots b_m \; a_1 \cdots a_\infty$

C3 = A, B infinite

$a_1 b_1 \; a_2 b_2 \cdots$

Theorem: if $|A| \leq |B|$ & $|B| \leq |A|$ then $|A| = |B|$

1) if $|A| \leq |B|$ injective mapping $f: A \to B$

2) if $|B| \leq |A|$ injective mapping $g: B \to A$

if we can define injective mapping $f: A \to B$ & $g: B \to A$

then we can define bijective mapping $h: A \to B$

Theorem: if A is countable, then $B \subseteq A$ is also countable

C1 : A = finite

C2 : A = infinite (define sequence)

ordering for binary strings: $str_{i,j}$ $\quad i$ = length of str

j = order in $\pi(i)$

$S(m) = str_{i,j}$ st $i + j = m$ sequence.

RECURRENCE RELATIONS

$$H_n = \underbrace{H_{n-1}}_{\text{making arrangement for the last disc}} + \underbrace{\overset{\text{putting last disc}}{1}} + \underbrace{H_{n-1}}_{\text{remaining problem}}$$

tower of hanoi

$H_1 = 1$

$\therefore H_n = 2^n - 1$

degree: $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}$ $\quad c_k \neq 0$

if initial Cond^n given then we can find unique sol^n

$$a_{k+1} = f(a_0, a_1, \dots a_k)$$

STEPS to obtain particular Sol^n (Homogeneous)

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots c_k a_{n-k} \quad c_k \neq 0$$

Step 1: characteristic eq^n

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \dots c_k = 0$$

roots $= r_1 \; r_2 \dots r_k$

Step 2: if roots distinct.

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n \dots \alpha_k r_k^n$$

if r_1 occurs m_1 times

$\vdots$

r_n occurs m_n times

$$m_1 + m_2 + \dots m_n = k$$

$$a_n = (\alpha_{1,1} + \alpha_{2,1} n + \alpha_{3,1} n^2 \dots \alpha_{m_1,1} n^{m_1 - 1}) r_1^n + \dots$$

$$(\alpha_{1,n} + \alpha_{2,n} n + \dots \alpha_{m_n,n} n^{m_n - 1}) r_n^n$$

Step 3 : particular sol^n

use the initial $Cond^n s$ to find values of α

Linear Non Homogeneous Recurrence Relation.

$a_n = c_1 a_{n-1} + \dots \; C_k a_{n-k} + F(n)$

association homogeneous recurrence relation $\{\dots a_n^{(h)} \dots\}$

$a_n^h = c_1 a_{n-1} + c_2 a_{n-2} \dots \; c_k a_{n-k}$

Let $\{\dots a_n^{(p)} \dots\}$ be a particular sol^n for this non-homogeneous equation $a_n^{(p)} = c_1 a_{n-1} + c_2 a_{n-2} + \dots c_k a_{n-k} + F(n)$

theorem: every sol^n of the recurrence relation $\{\dots b_n \dots\}$ is of the form $\{\dots a_n^{(h)} + a_n^{(p)} \dots\}$

Steps to find general sol^n of non-homogeneous Eq^n.

Step 1 : find $\{\dots a_n^{(h)} \dots\}$

Step 2 : find $\{\dots a_n^{(p)} \dots\}$ using trial and error

Step 3 : general $sol^n = \{\dots a_n^{(h)} + a_n^{(p)} \dots\}$

Linear Congruence

$ax \equiv b \bmod N$ $\qquad ax \% N = b \% N$ $\qquad (ax - b) \% N = 0$

Z_8 =	0	1	2	3	4	5	6	7
additive =	0	7	6	5	4	3	2	1

additive inverse = 0 7 6 5 4 3 2 1

multiplicative inverse = - 1 - 3 - 5 - 7

multiplicative inverse exists only for n coprime with 8

Eucledian Algorithm

$ax \equiv b \bmod N$ & $\gcd(a, N) = 1$ then

$a^{-1} a x \equiv a^{-1} b \bmod N$

$x \equiv a^{-1} b \bmod N$

Chinese remainder theorem.

$ax \equiv b \bmod N$ if $\gcd(a, N) \neq 1$

example: find x st

$ax = b_1 \bmod m_1$ $\quad ax = b_2 \bmod m_2$ $\quad \ldots \quad ax = b_K \bmod m_K$

cond^n: m_1 m_2 ... m_K are all relatively co-prime

$M = m_1 m_2 \cdots m_K$

then in $[0, M]$ x has a unique sol^n

other sol^{n}s : $x + KM$ $\quad K \in \mathbb{Z}$

define: $x = c_1 b_1 m_1 + c_2 b_2 m_2 + \cdots c_K b_K m_K$

such that

$c_i \bmod m_i = 1 \qquad c_j \bmod m_i = 0 \quad \forall j \neq i$

$\therefore x \bmod m_1 = c_1 b_1 \bmod m_1 = b_1$

define: $M_i = \prod_{j=1}^{n} m_j \quad j \neq i$

$\gcd(m_K, M_K) = 1$

define: Let y_K be multiplicative inverse of $M_K \bmod m_K$

$y_K M_K = 1 \bmod m_K \qquad y_K M_K = 0 \bmod m_j \ \forall j \neq K$

Soln: $x = y_1 M_1 b_1 + y_2 M_2 b_2 + \dots y_K M_K b_K$

y_1: multiplicative inverse of $M_K \bmod m_K$

M_1: $\prod_{j=1}^{n} m_j \quad j \neq i$

Abstract Algebra (Graph Theory)

G = set

$\circ$ = operation defined over G

$(G, \circ)$ is called a group if it is:

1) Clossure: $\forall a, b \in G \quad a \circ b \in G$
2) Associativity: $\forall a, b, c \in G \quad a \circ (b \circ c) = (a \circ b) \circ c$
3) Existence of Identity: $\exists$ a unique element $e \in G$ st $\forall a \in G \quad a \circ e = e \circ a$ holds
4) Existence of inverse: $\forall a \in G$ there exists a unique a^{-1} st $a^{-1} \circ a = e = a \circ a^{-1}$

Addition Module ($+_N$)

define: $\mathbb{Z}_N = \{0, 1, \dots (N-1)\}$

$\forall a, b \in \mathbb{Z}_N$

$a +_N b = (a+b) \bmod N$

$(\mathbb{Z}_N, +_N)$ is a group.

Multiplication Module. ($\cdot_N$)

define: $\mathbb{Z}_N^* = \{ a \in \mathbb{Z}_N : \gcd(a, N) = 1 \}$

$a \cdot_N b = (a \cdot b) \bmod N$

$\gcd(a, b) = \gcd(a-b, b)$

$\gcd(a, N) = 1 \ \wedge \ \gcd(b, N) = 1 \Rightarrow \gcd(ab, N) = 1$

Permutations

S_n = Set of n numbers

P_n = permutation of all elements of S_n

$|P_n| = n!$

$S_3 = \langle 1, 2, 3 \rangle \qquad P_3 = \left\{ \begin{array}{ll} \langle 1, 2, 3 \rangle & \langle 1, 3, 2 \rangle \\ \langle 2, 1, 3 \rangle & \langle 2, 3, 1 \rangle \\ \langle 3, 2, 1 \rangle & \langle 3, 1, 2 \rangle \end{array} \right\}$

define: operation $\circ$: permutation of sequences.

$\pi = \langle 3\ 2\ 1 \rangle$ $\quad$ $\pi \circ \rho$ applied on $\langle 1\ 2\ 3 \rangle$ gives

$\rho = \langle 1\ 3\ 2 \rangle$ $\quad$ $\langle 2\ 3\ 1 \rangle$

Cancellation rules

$x, y, a, b, z \in G$

1) $x \circ y = x \circ z \implies y = z$ $\quad$ Left cancellation rule
2) $a \circ x = b \circ x \implies a = b$ $\quad$ right cancellation rule.

Corollary of Cancellation Rules

$G = \{ g_1\ g_2\ g_3\ \cdots\ g_n \}$

for any $g_i \in G$ $\quad$ $(g_1 \circ g_i), (g_2 \circ g_i) \ldots (g_n \circ g_i)$ are all distinct.

proof: $g_s \neq g_t$ $\quad$ $g_s \circ g_i = g_s \circ g_i$ $\quad$ right cancel

$g_s = g_t \implies \Leftarrow$

Abelian Group

if $(G, \circ)$ is a group & operation '$\circ$' is commutative then it is called Abelian group.

$\forall a, b \in G \quad a \circ b = b \circ a$ $\quad$ $(\mathbb{Z}, +)$ is abelian group.

Existence of Unique Identity element

$(G, \circ)$ = group, then it has a unique identity element e

$e_1 \neq e_2 \quad e_1 \circ a = a \;\wedge\; e_2 \circ a = a \Rightarrow e_2 \circ a = e_1 \circ a \Rightarrow e_1 = e_2$

Existence of Unique Inverse

$(G, \circ)$ be group & $a \in G$. a has an unique inverse a^{-1}

suppose a_1^{-1} a_2^{-1} st $a \circ a_1^{-1} = e$ $\quad a \circ a_2^{-1} = e$

$$a \circ a_1^{-1} = a \circ a_2^{-1} \Rightarrow a_1^{-1} = a_2^{-1}$$

Group Exponential

$(G, \circ)$ group. operator $\circ$ be multiplicative

Let 'e' be identity element

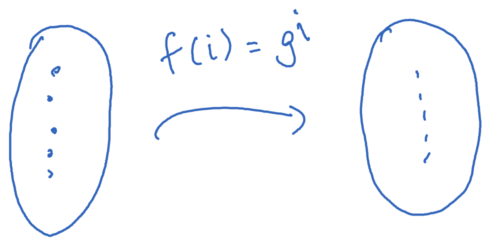
$$g^0 = e \qquad g^2 = g \circ g \qquad g^3 = g \circ g^2 \qquad g^m = g \circ g^{m-1}$$

$$g^{-m} = g^{-1} \circ g^{-(m-1)} \qquad g^{-1} = \text{inverse of } g$$

Rules

$$g^m \circ g^n = g^{m+n} \qquad \forall g \in G \qquad \forall m, n \in \mathbb{Z}$$

Order of element.



$g^i \in G$

$i \in \mathbb{N}$ $\qquad$ G

∞ set $\qquad$ finite set

$\exists\, a, b \quad a > b > 0$

$g^a = g^b$ $\qquad$ finite set

$g^a \circ g^{-b} = g^b \circ g^{-b} = g^0 = 1$

$g^{a-b} = 1$

$n = a - b \in \mathbb{Z}^+$ st $g^n = 1$

Smallest such n is called order of element g.

Subgroup: $H \subseteq G$ H is a group too under the same opr o

then H is a subgroup

$(\mathbb{Z}, +)$ is subgroup of $(\mathbb{R}, +)$

How to check?

$\forall\, x, y \in H$ $x o y \in H$ then H is a subgroup.

$\forall\, x \in H$ $x^{-1} \in H$

Hasse Diagram Elements:

1) Maximal Element: elements in hasse diag which do not have any element above them.

2) Maximum Element: if # maximal element = 1. That is maximum.

3) Minimal Element: elements in hasse diag which do not have any element below them.

4) Minimum Element: if # minimal element = 1. This is minimum.

bijective = injective + surjective

injective $\downarrow$ one to one funcn

surjective $\downarrow$ onto (domain is fully used)

if there exist a bijective mapping from $X \to Y$ then $|X| = |Y|$

* Euler requires all edges $deg(v) =$ even
* Hamiltonian requires all vertices $deg(v) \geq \frac{n}{2}$

Theorem: If n integers $m_1, m_2 \ldots m_n$ have an avg $\geq r-1$ then atleast one of the integers is $\geq r$