5. GROUP THEORY

//GP : Lecture 1

Group theory is part of abstract algebra.

Abstract Concept	Specific Concept
Boolean Algebra or boolean lattice	Proposition logic, subset
LUB, GLB	union, LCM, intersection, GCD

So, instead of going through all the structure we can consider one common structure i.e. without going through definition or meaning of specific concept we can study only operations on them (that is what abstract means).

// GP : Lecture 2

Who discovered abstract algebra ? – Evariste Glois, while studying polynomial of different degree. He got stuck at 5th degree polynomial and found that there is no formula for finding roots of degree 5 polynomial and he proved that using group theory.

// GP : Lecture 3

5.1) Introduction to group theory :

(Base set, operation) ← Algebraic structure

(Z, +) (N, +, ×) (set of matrix, product) (Z, +, ×, −)

algebraic structure

But in GATE syllabus we have only simple binary operation.

Example of algebraic structures with a single binary operation are : magma, quasigroup, monoid, semigroup, group, lattice, Boolean algebra.

// Lecture 4

Operation table/ Multiplication table/ Cayley table :

Consider ({a, b}, *)

read from up to right

*	a	b
a	a	b
b	a	a

means

$a * a = a$
$a * b = b$
$b * a = a$
$b * b = a$

5.1.1) The property of closure :

A set has the closure property under a particular operation <u>if the result of the operation is always an element in the set</u>. We say that the set is "*closed under the operation*".

S → (S, #) $a \# b = c$

Consider ({1, 2, 3}, +) and (R, /)

We know that 2+3 = 5 which does not belong to base set {1, 2, 3} which means set is not closed under addition operation. Same for second structure we have 0/0 which is not defined means do not belong to set R.

In terms of operation table, we can say that set is closed under operation when the entries in operation table belongs to that set.

In normal math, we can say *binary operation* is nothing but some operation between two operands but in abstract algebra we make everything precise.

In abstract algebra, binary operation is structure which satisfy closure property. Or # is binary operation on set S iff (s, #) is closed. We can also say that # is function which maps two elements of set to one value of same set, i.e. # : $S \times S \rightarrow S$

// Lecture 5

5.1.2) The Associative property :

(S, #) is associative iff $\forall_{a,b,c} \in S$ (a # b) # c = a # (b # c)

For example, (N, +) satisfies associative property.

// Lecture 6

5.1.3) The identity property :

Identity element "e" is element from same set if $\forall a \in S$, **a # e = a and e # a = a**.

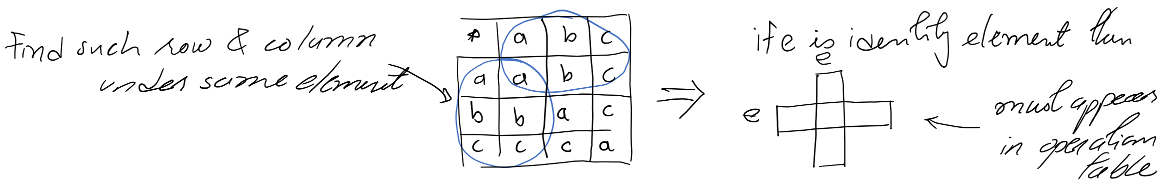
(N, +) – no identity element but (W, +) has identity element 0 while (Z, -) do not have identity element either but it has identity element 0 why ? a – 0 = a but 0 – a = -a so 0 is not identity element stupid.

//Lecture 7

Q : Can we have more than one identity element ? – let e and f are two identity elements. If e is identity element then e # f = f and if f is identity element then f # e = e. Which means f = e. Thus, always unique identity element if exists.

//Lecture 8

Q : How can you find identity element from operation table ? – Consider following operation table,



// Lecture 9

5.1.4) The Inverse Property :

Let we have (S, #) then inverse of element a is b such that $a, b \in S$ iff a # b = e and b # a = e where e is identity element. We say b = a^{-1}.

We can say more formally that **(S, #) has inverse property iff** $\forall_{a \in S} \exists_{b \in S} ((\boldsymbol{a\#b = e}) \wedge (\boldsymbol{b\#a = e}))$

Q : Do (R, x) satisfies inverse property ? – yes, because here identity element is 1 so 5 x something = 1. And something is 1/5 and so on. But you are wrong, 0 x something = 1; something = 1/0 ? absolutely not. 0 does not have any inverse which means (R, x) does not satisfy inverse property.

Without identity element inverse property cannot be defined

Q : if $a^{-1} = b$ then $b^{-1} = a$? – simply apply definition, a # b = e and b # a = e which means $a^{-1} = b$ but it also means $b^{-1} = a$. and we can also prove that $e^{-1} = e$.

Q : Is it possible for an element to have more than one inverse ? – Yes, possible consider following,

*	a	b	c	e
a	e	e	e	a
b	e	e	e	b
c	e	e	e	c
e	a	b	c	e

$a^{-1} = a, b, c$
$b^{-1} = a, b, c$
$c^{-1} = a, b, c$
$e^{-1} = e$

//Lecture 10

5.1.5) The commutative property :

Commutative property is satisfied by some structure (S, #) iff $\forall_{a,b\in S}(a\#b = b\#a)$

//Lecture 11

5.2) Classification of structures (with binary operation) :

	Algebraic Structure	Properties
1	Magma (Groupoid)	Closure property
2	Semigroup	Closure + Associative
3	Monoid	Closure + Associative + Identity
4	Group	Closure + Associative + Identity + Inverse

From above we can say that every algebraic structure with simple binary operation is magma because all algebraic structure with binary operation satisfies closure property.

Moreover, in group theory there was a famous mathematician named *Abel* from which *Abelian* is derived which simply means commutative. So, Abelian semigroup means semigroup with one additional property of commutative and same for other algebraic structure.

5.2.1) Groupoid / Magma :

G be a non-empty set and * be a binary operation, then the structure (G, *) is called a groupoid, if a * b ∈ G, $\forall a, b \in G$. The set N is not a groupoid with respect to operation "-".

5.2.2) Semigroup : A groupoid with associative property is semigroup.

5.2.3) Monoid : A semigroup with identity property. Sometimes monoid structure is represented as (S, *, e) where * is binary operation and e is identity element.

Q : Consider one structure (Z, *) such that a * b = a + b – 3 : – This is abelian group.

1) closure : If $a, b \in Z$ then $a+b-3 \in Z$ ← True

2) Asso : $(a*b)*c = a*(b*c)$

$\therefore (a+b-3)*c = a*(b+c-3)$

$\Rightarrow a+b-3+c-3 = a+b+c-3-3$ ← True

3) Identity : $a*e = a$ & $e*a = a$

$a+e-3 = a \Rightarrow \boxed{e=3}$ $\quad e+a-3 = a \Rightarrow \boxed{e=3}$

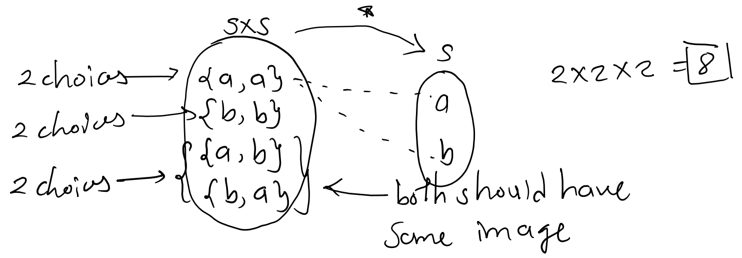
4) Inverse : $a * b = e$ & $b * a = e$ then $a^{-1} = b$

$a + b = 6 \implies \boxed{b = 6 - a}$ ✓

//Lecture 12

Q : (S, *) for this structure no. of binary operation ? – We know that each binary operation is nothing but some function so it is basic question of no. of function which is nothing but $(\text{codomain})^{(\text{domain})}$. In this case domain = S x S and codomain is S.

Q : Consider previous question S with cardinality of n but now we have to find out <u>no. of commutative</u> binary operation ? – First consider one beautiful example, ({a, b}, *) be the structure then



Similarly, for $|S| = n$

domain	codomain
(1,1)	→ n choices
(2,2)	→ n choice
(3,3)	⋮
⋮	
(n,n)	→ n choices

$\Rightarrow n^n$

domain	codomain
(1,2)(2,1)	→ n choices
⋮	⋮
(n,n-1)(n-1,n)	→ n choices

$\Rightarrow n^{{}^nC_2}$

$\#$ of function $= n^{{}^nC_2 + n} = \boxed{n^{\frac{n^2+n}{2}}}$

NOTE :

1) **When operation "*" is NOT associative, we cannot write a * b * c because it is ambiguous. We should put parentheses to disambiguate.**
2) **In any structure, there is at most one identity element.**
3) **When we say some structure does not satisfy commutative property then we are not saying $\forall_{x,y \in S}(x * y) \neq (y * x)$ this is not true in any case. Because we have one case where this commutative property satisfies i.e. e*a = a*e where e is identity element. But not all element is satisfying that is why we can say that commutative property does not satisfy.**
4) **We denote nonzero real number by R^0 and similarly we denote any other set of number with nonzero values as N^0, Z^0, Q^0…**

Q : Example of function with associative or commutative property –

- *Associative and commutative* : $+, \times$ ← Number theory; $\wedge\ \vee\ \oplus\ \leftrightarrow$ ← prop. logic; $\cup\ \cap$ ← set theory
- *Associative but not commutative* : Matrix multiplication, **(N, #) where a#b = a**.
- *Not associative but commutative* : operation **(x, y) -> xy + 1** on the integer, NAND ↑
- *Not associative and not commutative* : -, / ← Number theory; $\rightarrow$ ← logic; $-$ ← set difference

//Lecture 13

Properties of monoid :

Left cancellation property : If a # b = a # c then b = c (meaning we can cancel a)

Right cancellation property : if b # a = c # a then b = c (meaning we can cancel a from right side)

- In a monoid, we don't have left, right property.

Proof. $(N, *) \Rightarrow a * b = \max(a, b)$ / $3 * 1 = 3 * 2$ but $1 \neq 2$

$1 * 3 = 2 * 3$ but $1 \neq 2$

//Lecture 16

5.2.4) Group :

Order of a group : *The number of elements in a group is called order of the group*.

By now we all know about definition of group. So, let's explore more about groups.

Some important groups :

- ***Set of nth Roots of unity, under multiplication*** :

Consider, equation x = 1 how many roots it has ? only 1 i.e. roots = {1} now consider x^2 = 1 then roots = {-1, 1} and these roots are called roots of unity and we do same operation till nth root of unity. One thing to observe is that these roots set with multiplication operation forms a group of order equal to no. of roots …

$x^3 = 1 \Rightarrow (x-1)(x^2+x+1) = 0 \Rightarrow x = 1$ & $x = \frac{1+i\sqrt{3}}{2}$, $x = \frac{1-i\sqrt{3}}{2}$

$\therefore x = \{1, \omega, \omega^2\}$ $\quad 1 \quad \omega \quad \omega^2$

This are called cube roots of unity. And this set under multiplication is also group. Not only that this structure is also abelian group. And again, all the nth roots of unity form a set which in under multiplication is abelian group.

//Lecture 17

- ***Addition modulo n*** :

The group Z_n consists of the elements {0, 1, 2, …, n-1} with addition mod n as the operation. You can also multiply elements of Z_n, but you do not obtain a group. The element 0 does not have multiplicative inverse.

Base set : Z_n consists of all the remainders of n when a number is divided by n.

Operation : addition module n denoted as $\oplus_n$ $\qquad a \oplus_n b = (a+b) \bmod n$

In general, for structure $(Z_n, \oplus_n)$ or $(\{0,1,2,3,\ldots,n-1\}, \oplus_n)$ $n \in N$

Closed, associative, Identity, commutative, inverse ? $\rightarrow (a + ?) \bmod n = 0$

✓ ✓ ✓ 0 ✓ $\quad n-a \quad \forall a \neq 0$ because $0^{-1} = 0$

You know we have already discussed right and left cancellation. Group satisfies right as well as left cancellation. BUT we cannot do a * c = b * a → c = b because of absence of commutative property in group. But if we have Abelian group then this is also true.

//Lecture 21

Q : We know that in group (G, *), $a*a^{-1} = a^{-1}*a$ and ae = ea do these imply abelian property ? – First statement is $aa^{-1} = a^{-1}a$ which is nothing but equal to e. This is inverse property so does not imply abelian property. Now, talking about second ae = ea is the property specifying identity. So, both of these statement does not imply abelian.

Checking associative property in the Cayley table :

In general, it is not possible to check for associativity simply by glancing at the Cayley table. This is in part, because associativity is determined from a three termed equation a(bc) = (ab)c whilst the Cayley table shows two-term products only. But you can check commutative property. Thus, they will never ask you about checking associative property. But if you want to check Cayley table for associativity then never check for identity element or formula including identity element because (a * e) * b = a * (e * b) ➔ ab = ab (identity element with any element is element itself so no point)

//Lecture 23A

If * is a binary operation on a finite set S, then properties of * often correspond to properties of the Cayley table. In group,

- Each element g ∈ G appears *exactly once* in each row and in each column.
- So, every row/column is simply a permutation of all elements i.e. *every element appears exactly once*.
- Row and column of identity element is exactly same as the header.

Proof : Consider if one is repeating,

	b
a	a
c	a

Then ab=cb then a=c

Which means cayley table of group $\underset{\times}{\overset{\checkmark}{\rightleftarrows}}$ No Reapeating elements in Row/column

//Lecture 24

Monoid	Group
⇒ Unique identity	⇒ Unique identity
⇒ Inverse may not exist for some element	⇒ Unique inverse
⇒ left, Right cancellation ✗	⇒ left, Right cancellation ✓

// Lecture 25A

Groups of small order :

Q : How many different binary operations we can have with order 1 structure ? – we know that order is nothing but no. of element in base set. And we also know that binary operation is nothing but function which means no. of binary operations is $\text{codomain}^{\text{domain}}$. So only 1 binary operation is possible.

But wait we have binary operations which has order 1 for example, ({T}, Λ), ({T}, V), ({1}, x), ({0}, +) so there are infinite many binary operations then why we proved that 1 binary operation is possible. Here one thing to note that if you look at operation of first structure it is nothing but T Λ T = T is the only operation and as same for other we can say they have same structure and that is why only 1 binary operation with order 1 structure is there. Which means if you study one structure it is equivalent to study all structure with order 1.

We call them isomorphic structure. So, question we are really interested is how many non-isomorphic groups of order 1 are there ? – so answer is 1.

Let's generalize this to order n, here we are talking about groups so we have to take in count of group's properties.

order 2 group :

	e	a
e	e	a
a	a	e

order 3 grups :

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

order 4 groups :
↳ 2 non-Isomorphic Group
⇕
2 Templetes

We noticed that **non-isomorphic group ≡ Different templets ≡ up to isomorphism** (this simply means consider non-isomorphic)

Let's look at order 4 groups (non-isomorphic groups) :

	e	a	b	c
e	e	a	b	c
a	a	a		
b	b			
c	c			

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

≡

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	e	b	a	b

Iso-morphic

2nd and 3rd are iso-morphic because in both Cayley table. One element is there which is inverse of itself and two elements are inverse of each other.

//Lecture 26

Power of an element in a group :

We introduce the concept of integral exponents of elements in a group. The concept plays an important role in the theory of *cyclic groups*.

Definition : *For any* $a \in G$ *we define*

$$a^0 = e$$

$$a^n = a^{n-1}a, for\ n \geq 1$$

$$a^{-n} = (a^{-1})^n\ for\ n \geq 1$$

Some properties are consequences of these fundamental definition namely, $a^n a^{-n} = e, a^m a^n = a^{m+n}, (a^m)^n = a^{mn}$

We can create beautiful example by using property of inverse is that if $a^n = e$ then $a^{-1} = a^{n-1}$. Because $a^n = a^{n-1}a = e$ so here a^{n-1} working as a^{-1}.

Q : If G is a group of even order, then show that there exists an element $a \neq e$, the identity in G, such that $a^2 = e$? – Question says if |G| = 2n then there is an element which is $a^2 = e$ ➔ $a = a^{-1}$ (which is inverse of itself). We know that identity element is there in every group so we throw out of the base set. Then we know that every element has unique inverse, consider a has unique inverse as b then we throw both out of base set. We do this thing untill nothing left. So, if nothing left means no element is inverse of itself and if one element left then it is inverse of itself because it is property of group. Here we have 2n-1 element (after removing e) and we will get one element at last.

//Lecture 27A

5.2.5) Subgroups :

Definition : *Let (G, *) be a group. A subgroup of G is a subset H ⊂ G such that*

- $e \in H$
- $x, y \in H \rightarrow x * y \in H$
- $x \in H \rightarrow x^{-1} \in H$

"Subgroup of group G" is a subset which is also a group under same operation.

Example, ({1, -1, i, -i}, x) is a group with identity element is 1.

$(\{1,-1\}, \times)$ ✓ $\cancel{(\{1, i\}, \times)}$ Not group $\cancel{(\{1, 0\}, \times)}$ Not in base set $\cancel{(\{0\}, +)}$ Nonsense

//Lecture 27B

1) Subgroup generated by an element :

Let (Z, +) is group and if we say subgroup generated by 2 is equivalent of saying smallest subgroup that contains element 2.

We know that 0 must be there in this group because of definition of subgroup. And 2 must be there if we do 2+2 = 4 so 4 must be there likewise 6, 8, 10, all odd positive number should be there. 2-2 = 0 then we say -2 is inverse of 2 so it must be there in group as well and -4, -6,… are inverse of 4, 6,… respectively. Therefore, smallest subgroup that contains element 2 will be all even numbers or integer which are multiple of 2.

Similarly consider ({1, -1, I, -i}, x) group here if we say subgroup generated by i is equivalent to saying smallest subgroup that contains element i. We know that it should contain i and 1 and all power of i which is nothing but group itself. Which means i can generate whole group. We say that i is generator of group ({1, -1, I, -i}, x). similarly -i also a generator of group. 1 and -1 is not generator of G.

//Lecture 31

Notations : Let Group be (G, *) ; a ∈ G

<a> = *subgroup of G generated by a* **OR** *Smallest subgroup of G containing a*.

<a> = {a^n | n ∈ Z} … look at carefully n is not natural number.

If we say H is subgroup of G, we denote it by $H \leq G$ and |G| = order of G is equal to number of elements in base set

Q : Let G be a group which can be generated by an element "a" which is inverse of itself. Then what is order of G ? – question is asking |<a>| = ?. <a> = { a^0, a^1, a^2, a^3,…} = {e, a, e, a,…} = {e, a}. |G|=2. But one more case is possible, what if a is identity element itself then |G|=1 so if G is generated by an element a which is inverse of itself then order of G will be 1 or 2. These two possible groups are non-isomorphic.

//Lecture 32A

2) Order of an element : (size of subgroup generated by an element)

The order of a finite group is the number of elements. If a group is not finite, one says that its order is infinite. *The order of an element* of a group (also called period length or period) is the order of the subgroup generated by the element.

consider ({1, -1, I, -i}, x) group, we know that order of G = |G| = 4

Order of 1 (by definition) = |<1>|=|{1}|… because 1 can only generate 1 and |{1}| = 1

Similarly, |<-1>|=|{-1, 1}|=2, |<i>| = 4, |<-i>| = 4.

One thing to note that order of identity element is always one as it can create only itself through any operation in group.

Now, let's make some wonderful observations :

Consider a group (G, *), where a,b ∈ G and a ≠ e and <a> = { a^0, a^1, a^2, a^3,…} = {e, a, b, e,…}

If you observe carefully a^3 = e means there is no point of calculating a^4, a^5, a^6,… because it will repeat a b e pattern. So, order will be 3 (in this case only). Which means here order of element "a" is least power of "a" till we get identity element after a^0 (because it is e only). As a0 = e and it is true for all element of any group. Thus, we can ignore a^0.

Similarly, we can say that ***Order of an element*** *a∈G is the* ***least positive*** *integers n such that a^n = e, where e is the identity of G.*

We can make 1 more observation that when *order of an element is equal to order of group then that element is generator.*

NOTE :

1) **While creating "subgroup generated by an element a", inverses are only needed if the group is infinite; In a finite group, the inverse of an element can be expressed as a positive power of that element.**
2) **Order of x = O(x) = O(a^{-1} x a) how ? whenever something about order is given apply definition**

Q : if i^{16} = i^{28}, we know that i^{12} = e then 12 is order of element i ? – Answer is no, because order is smallest integer such that i^n = e but multiple of n can also generate e that does not mean that n is order. More specifically we can say that $1 \leq order\ of\ i \leq 12$.

Q : It is possible that an infinite group has No generator ? – Yes, it can possible, see (C, *) be any operation which is infinite group. We select one element then try to find its subgroup we keep multiplying its power till 1 appears but never occurs but we are getting distinct element of C. and one proof is that we know simple thing that not every group has generator i.e. not every group is cyclic.

Q : If group is commutative then its subgroup is also abelian ? – because according to the definition of subgroup look at second point it says when x and y is in H then x * y should also be in H and y * x should be also be in H and we now that in G, x*y = y*x so in H also if same pairs should be there then they also satisfy commutative.

//Lecture 28

5.3) Types of groups and it's properties :

Coprime or relatively prime : In number theory, two integer a and b are coprime or relatively prime or mutually prime if the only positive integer that is a divisor of both of them is 1.

In previous section we have encountered addition modulo n group which is abelian group. Similarly, here we are introducing new structure namely *multiplication modulo n group*. We know that it has closure property, associativity, identity, communicative but it does not have inverse property as 0 does not have inverse. We can say it is *abelian monoid*.

//Lecture 29

5.3.1) Unit group :

But can we convert it into group ? – Answer is yes, we can by removing elements who do not have inverse. for example, (Z_4, mul mod 4). Z_4 = {0, 1, 2, 3}

0^{-1} = DNE $\quad 1^{-1} = 1$

2^{-1} = DNE $\quad 3^{-1} = 3$

$(\{1, 3\}, \otimes_4)$ ← Unit

↑ This is group but it's not Z

We obtained new set we cannot call it Z or something because it is not consecutive integer, we can denote it by new notation U_4. (we call it **Unit Group**)

Thus, $\quad (U_4, \otimes_4)$ ← Abelian Group

But what makes other elements to remain in set ? – if you note carefully 1, 3 are called units and all units are coprime to 4. For example, 1 and 3 is coprime to 4. Means in unit group we have only those elements in base set who are coprime to n.

$$U_n(Unit\ group) = \{m | m \in Z_n, m\ and\ n\ are\ coprime\}$$

//Lecture 30

Now, let's look at some unit group,

$(U_8, \otimes_8)$		$(U_{10}, \otimes_{10})$		$(U_{12}, \otimes_{12})$
$U_8 = \{1, 3, 5, 7\}$		$U_{10} = \{1, 3, 7, 9\}$		$U_{12} = \{1, 5, 7, 11\}$
$1^{-1} = 1$		$1^{-1} = 1$		$1^{-1} = 1$
$3^{-1} = 3$	← same structure →	$3^{-1} = 7$	← Different structure →	$5^{-1} = 5$
$5^{-1} = 5$		$7^{-1} = 3$		$7^{-1} = 7$
$7^{-1} = 7$		$9^{-1} = 9$		$11^{-1} = 11$

We observed two templets in group of order 4 :

- {e, x, y, z} → $e^{-1} = e, \; z = z^{-1}, \; x^{-1} = y, \; y^{-1} = x$
- {e, x, y, z} → $e^{-1} = e, \; z = z^{-1}, \; x^{-1} = x, \; y^{-1} = y$

Which means if we have more than 2-unit group of order 4 at least 2 of them are isomorphic.

// Lecture 33

5.3.2) Cyclic group :

Definition : Group that can be generated by a single element. **OR** Group with <u>at least</u> one generator.

Example, $(Z_n, \oplus_n)$ is addition modulo n group and it is cyclic with generator 1 (how?)

Q : Order of smallest group that is not cyclic ? – if you have order 1 then it is cyclic. If you have order of 2 group then also cyclic (you can check by cayley table). If you try with 4 then you will get one namely $(U_8, \otimes_8)$ is group which is not cyclic so answer is 4.

Q : If two cyclic group have same order then it is isomorphic ? – yes possible, take nth root of unity under multiplication and addition modulo n. they are isomorphic because same pattern…

nth root of unity $\rightarrow (\{1, \theta^1, \theta^2, \theta^3, ---, \theta^{n-1}\}, \times)$

Addition mod n $\rightarrow (\{1^0, 1^1, 1^2, 1^3, 1^4, ---, 1^{n-1}\}, \oplus_n)$

Theorem : *Any cyclic group is isomorphic to either Z or Z_n*.

For infinite cyclic group → Z, + and for finite cyclic group of order n → Z_n, $\oplus_n$

From above example of nth root of unity and addition mod n we can also conclude that *every cyclic group is also abelian*.

Now, let's look at order 4 groups we know that 2 groups are possible and both of them are abelian and if you look back you will realize that a is generator in first diagram and second diagram has no generator which means one is cyclic and one is non-cyclic group of order 4.

//Lecture 36

5.3.3) Lagrange's theorem :

It says If G is a finite group and $H \leq G$ then |H| divides |G|. or in other words **order of every subgroup of finite group G divide order of G**.

Element is also a subgroup so *order of an element of finite group divides order of group*.

But converse is not true, here converse is "if n (a number) divides order of G then there exists a subgroup of order n". (not necessarily true for group)

But if G is abelian group then above statement is true. i.e. If n (a number) divides order of G then there exists a subgroup of order n.

Q : What if order of G is prime (p) ? – then if subgroup exists then there will be only two subgroups of G. i.e. one identity element and other is subgroup with order p. Which means subgroup can generate G with power p which means it is cyclic group. We can say that *if order of G is prime **then** G is cyclic*. Which means *every subgroup of a cyclic group is cyclic*.

//Lecture 39

5.3.4) properties of subgroups :

For any group G, union of two subgroups may not be a subgroup.

For example, consider group (Z, +) and subgroup (3Z, +) and (4Z, +) then (3Z ∪ 4Z, +) is not subgroup because of closure property 3 + 4 ∉ (3Z ∪ 4Z)

Q : for any group G, intersection of two subgroups is always be a subgroup ? – to prove subgroup we take two subgroups of G and then we find closure, identity, inverse of intersection of two subgroup. So,

So, let's start with closure property, if we know that $a, b \in H, a * b \in H$ and $a, b \in L, a * b \in L$ then $a, b \in H \cap L, a * b \in H \cap L$ this is also true. Now, second is identity property. So, all subgroup contains it so intersection will definitely contain it. Talking about inverse of so same as identity, we know that is $a \in H$ then $a^{-1} \in H$, also $a \in L$ then $a^{-1} \in L$ (third point of definition of subgroup). Thus, if both contains a^{-1} so intersection will also contain a^{-1}. We conclude our proof here.

If Group have order of 6 then we know order of its subgroup will be {1, 2, 3, 6} here subgroup with order 2 or 3 is called **non-trivial subgroup**. And with 1 or 6 will be **trivial subgroup**.

Alternative definition of subgroup :

Our first definition was

*Let (G, *) be a group. A subgroup of G is a subset H ⊂ G such that*

- $e \in H$
- $x, y \in H \rightarrow x * y \in H$
- $x \in H \rightarrow x^{-1} \in H$

Now, we can remove first point i.e. $e \in H$ and instead we can write "non-empty subset H and combine second the third point" combining second and third point will give us. $xy^{-1} \in H$ and when x = y then $x.x^{-1} \in H$ which guarantees the presence of identity element in subgroup H. so, in short, we can say that

A non-empty subset H of a group is a subgroup of G if, for any $x, y \in H$, we have $xy^{-1} \in H$.

Existence of element in subgroup :

Suppose we have group G = <a> and consider two elements a^v and a^u from G. Now, we know that power of this element should be present in group or subgroup generated by that element i.e. $a^{vx} \in G$ and a^{uy}. Thus, $a^{vx}a^{uy} = a^{vx+uy} \in G$.

Now, we know u and v are some random natural number which may or may not contains common term. Which means $a^{\gcd(v,u)(sx+ty)} \in G$, gcd is nothing but some common term between v and u. Then, $a^{\gcd(v,u)} \in G$. Which is the smallest subgroup of G which contains both a^v and a^u.

Lemma : If $O(g) = n$ then $O(g^k) = \frac{n}{\gcd(n,k)}$

Q : Let G is cyclic group of order 48, then how many elements of order 8 are in G ? – from above lemma we know that O(g) = 48 and let $O(g^k) = 8 = \frac{48}{\gcd(48,k)}$ which indirectly means $\gcd(48, k) = 6$. We found that k = 6, 18, 30, 42.

NOTE :

1) **A group (finite or infinite) is never the union of two of its proper subgroups.**
2) **Every group of order p^2 or p where p is prime is abelian. Which implies every group of order less than 6 is abelian.**
3) **Number of different non-isomorphic abelian groups of order P^k (P is prime) is the number of partitions of k.**

Silly mistake :

Let G be a finite group. Let "1" denote the identity element of G. If g is an element of a finite group G, then the order of g is the smallest positive integer n such that $g^n = 1$, and it is denoted $o(g) = n$. The order of group G is denoted by $o(\mathrm{G})$ or $|\mathrm{G}|$.

Which of the following statements is necessarily true?

A. If $g^m = 1$, for some $g \in \mathrm{G}$, then $o(g) \mid m$.
B. If $g^m = 1$, for some $g \in \mathrm{G}$, then $o(g) = m$.
C. If $g^m = 1$, for some g $\in \mathrm{G}$, then $m \mid o(g)$.
D. If $g^m = 1$, for some $g \in \mathrm{G}$, then $m \mid o(\mathrm{G})$.

Here m could be k*O(g)>>O(G) so option D will not be always true

Your Answer: D | Correct Answer: A | Incorrect | Discuss

⇨ If $\forall x \in G, x^2 = e$ then it is abelian because $(xy)^2 = e \rightarrow xy.xy = e \rightarrow xy = y^{-1}x^{-1} = yx$.

6. COMBINATORICS

//Lecture 1

In this module we address only one problem : How to count without counting OR more specifically how to figure out how many things are there with a certain property without actually enumerating all of them.

In this module we will study following :

1) Basic counting principles : Addition, multiplication, subtraction, bijection, pigeonhole principle and double counting
2) Ordered arrangements – strings, maps and products : permutations
3) The twelvefold way – balls in boxes : "n" unlabeled balls or labeled balls in "k" unlabeled or labeled boxes.
4) Inclusion-exclusion principle
5) Generating functions and recurrence relation

//Lecture 2

6.1) Basic counting principles :

6.1.1) The sum rule : Consider we have one task to select one person from group of students and teachers.

$S_1, \dots, S_n$ $\qquad$ $T_1, T_2, \dots, T_m$

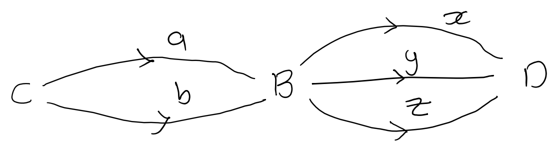
both groups are disjoint $\rightarrow$ $n+m$ ways to select person

Mutually disjoint condition is required because if there exists some common person between them then we are counting it twice.

Rule : If there are n(A) ways to do A and distinct from them, n(B) ways to do B, then the number of ways to do A or B is n(A) + n(B).

//Lecture 3A,3B

6.1.2) The product rule : Consider a problem of finding different type of routes from Chennai to Delhi via Bangalore.



$2 \times 3 = 6$

From C, you have two choices and after reaching B we have 3 choices so in total 6 routes are possible.

One thing you have notice that whole task was depend upon C to B **and** B to D. In sum rule if we select person from student then our task is over. But here in product rule task depend upon several tasks.

Q : 4 Letter English word; How many ? -

Task : $T_1 \cap T_2 \cap T_3 \cap T_4$ $\qquad$ $\cap$ = and

26	26	26	26

$= 26^4$

Only doing task T1 cannot do whole task.

That is why we have not applied sum or addition rule.

Q : How many different bit strings of length seven are there ? – bit string means sequences of 0's or 1's or both. 7 length is given and each place have 2 choices so 2^7.

//Lecture 4

6.1.3) The subtraction rule : If a task can be done in either n1 ways or n2 ways, then the number of ways to do the task n1 + n2 minus the number of ways to do the task that are common to the two different ways.

Q : How many bit strings of length eight either begin with 00 or end with 101 ? -

8 length

$\boxed{00------} + \boxed{-----101} - \boxed{00---101}$

$2^6 + 2^5 - 2^3 = 88$

Number of K length English palindromes : $26^{\lceil \frac{k}{2} \rceil}$ (why?)

//Lecture 6

6.1.4) Counting by case : Mutually exclusive, exhaustive cases

Take an example A student ID is made up of 3 letters followed by two digits. How many student ID's are possible with an even number of A's ? – In such problem we can create two cases, one in which number of A's is 0 and another in which number of A's is 2. Both cases are mutually exclusive meaning we are not overcounting anything. As these are mutually exclusive, we can apply addition rule. Number of A's is 0 + number of A's is 2 = even number of A's.

Case 1 : # A's = 0

L L L D D

25	25	25	10	10

$= (25)^3 \times 100$

+

Case 2 : # of A's = 2

L L L D D

A	A	25	10	10

+

25	A	A	10	10

+

A	25	A	10	10

$3 \times 25 \times 100$

$= 157 \times 10^4$

In case 2 you can see we have covered all the possible cases in which no. of A's is 2. Which means we have exhausted all the cases. In short,

Mutually exclusive & Exhaustive cases

Don't count same thing more than one time

Count every desired cases

Q : Flamingos fanny and Freddy have three offspring : Happy, Glee, and Joy. These five flamingos are to be distributed to seven different zoos so that no zoo gets both a parent and a child. It is not required that every zoo gets a flamingo. In how many different ways can this be done ? – Underlined statement has importance it is saying one of the parents (father or mother or both) and child cannot be in same zoo.

case 1 : both parents together

$\boxed{F + F_R}$ H G J

7 choices 6 6 6

$= 7 \times 6^3$

+

Case 2 : Parents not together

F | F_R H G J

7 choices 6 choices 5 5 5

$= 7 \times 6 \times 5^3$

$= 6762$

//Lecture 7

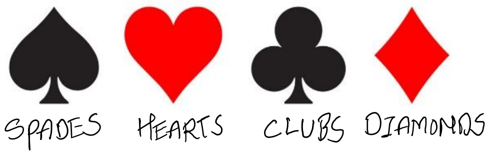
6.1.5) The complement rule : It is sometimes easier to calculate the undesired cases.

Desired = Total – Undesired

Q : Each user on a computer system has a password, which is six to eight characters long, where each character is an uppercase letter or a digit. Each password must contain at least one digit. How many possible passwords are there ? – we can first create three cases, password having length six, length seven and length eight. Now, each must contain at least one digit. This is same as saying total – no digit. Thus, we solve for each case and add them to get required results.

About cards : (basic info)

Standard deck of card contains 52 cards. Each card belongs to one of the 4 suits namely.



Q : How many 4-digit numbers are there, not starting with 0, without repetition, also must be an odd number ? – you got 6 x 8 x 9 x 5 as answer but it is wrong as you are undercounting.

Guideline 1 : while applying product rule start with the most restricted place.

Here most restricted place is last place i.e. it should be odd number so we have 5 choices for last digit. Now we move one to first digit because there is one more restriction of not starting with 0. Like that now, answer is 8 x 8 x 7 x 5.

Guideline 2 : Just because some information is given, doesn't mean it is useful.

//Lecture 8A

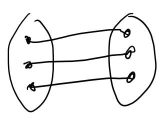
6.1.6) Division Rule : To count the number of cows in your field, first count the number of legs and then divide by four.

//Lecture 8B

We know that one to one correspondence means bijection meaning it is one to one and onto. Similarly, we can extend this to k to one correspondence meaning it is k to one and onto function.

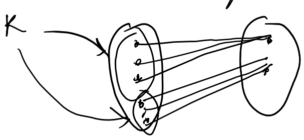
A k to 1 correspondence is an onto mapping in which every B object is the image of exactly k A objects.

1 to 1 correspondence



Here $|A| = |B|$

k to 1 correspondence

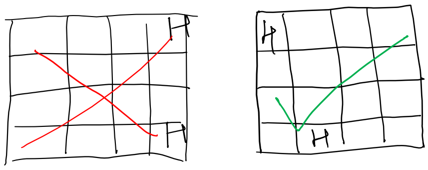


Here $|A| = k * |B|$ or $|B| = |A|/k$

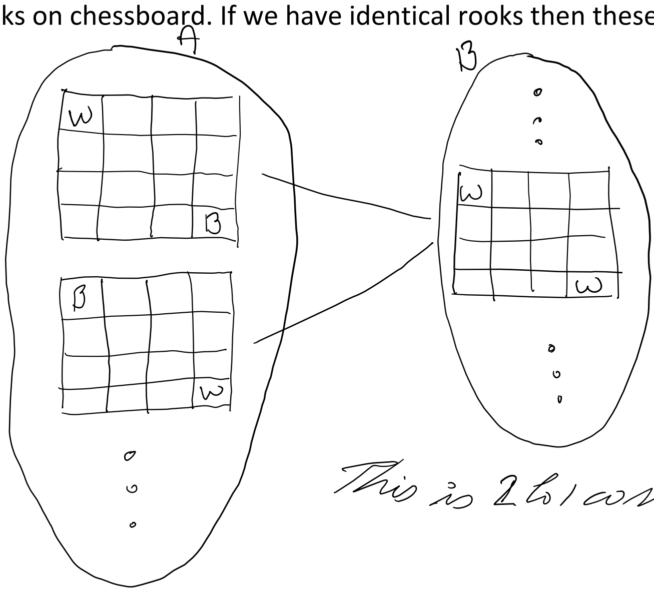
So why we have covered this in division rule, let's answer this by following question.

Q : In how many ways can we place two identical rooks (elephant) on an 8 by 8 chessboard so that they occupy different rows and different columns ? –

If we place one rook (black or while) we cannot place other rooks at same row or column.



In question it is asked that identical rooks, first let's find if rooks are not identity meaning they are different. If we have one rook (say white) there are 64 possible places. And then we take another rook (say black) so for that we have 49 possible places (64 – 15). And similar case for first rook being black and second rook being white is also possible. So, in total we have 64 x 49 ways to place two different rooks on chessboard. If we have identical rooks then these two combinations are same.



we know that in k to 1

$|A| = k * |B|$

similarly in 2 to 1

$|A| = 2 * |B|$

$64 \times 49 = 2 * |B|$

$|B| = 32 \times 49$

This is what we have to find

This is 2 to 1 correspondence

Similarly, you can solve problems like possible strings of length 6 in which a should occur before b where possible alphabet of strings is a, b, c, d, e, f.

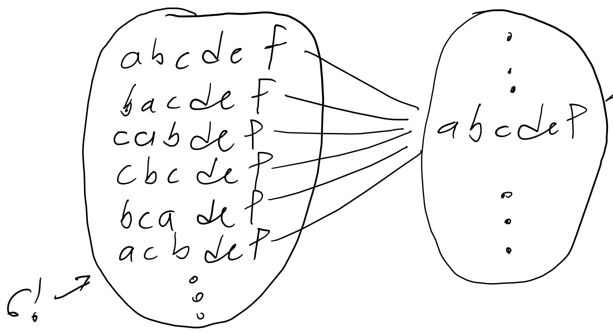
Subsequences : A subsequence of a string is a new string that is formed from the original string by deleting some (can be more) of the characters without disturbing the relative positions of the remaining characters. (i.e., "acd" is a subsequence of "abcde" while "aec" is not).

If W = A B C D then

1) A C – subsequence ✓ ; substring ✗
2) B C – Substring ✓
3) C B – Substring ✗ ; subsequence ✗

substring $\xrightarrow{\checkmark}$ subsequence, subsequence $\xrightarrow{\times}$ substring

Q : how many linear orders of 6 elements a, b, c, d, e, f is there such that "a" comes before "b", and "b" comes before "c" (not necessarily immediately) ? – here not necessarily immediately means abc is subsequence. "a" comes before "b" and "b" comes before "c" can happen in only sequence. Let's take one instant.



$\boxed{\frac{6!}{6}}$ ← answer

because 6 sequences map to one sequence.

NOTE : Mostly, division principle is not used directly but in the form of combination this is used.

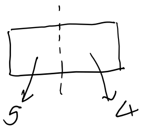
//Lecture 10

Now, will see permutation and combination which are consequences of product rule and division principle. Difference between permutation and combination is - in permutation *picking first, second and third place winners*. And in combination *picking three winners*.

1) **Permutation** : (A fancy application of product rule)

Q : Number of permutations/orderings/arrangements of n distinct elements = n! = P(n, n)

Q : Number of permutations/orderings/arrangements of 2 distinct elements from a set of 5 elements are there? –



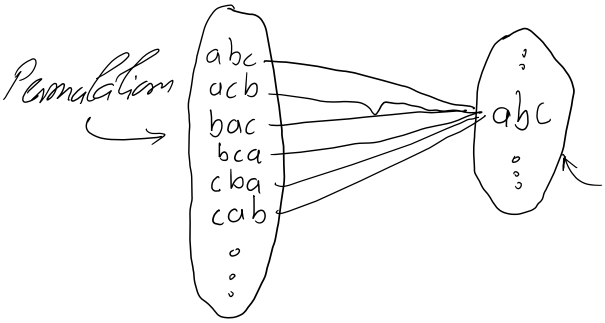
$= 20 = P(5, 2)$

Permutation of r object from n objects (distinct) = $P(n, r) = \frac{n!}{(n-r)!}$

//Lecture 11

2) **Combination** : (A fancy application of division rule)

Q : Number of ways to select 3 people from a class of 5 people. – forget about combination we will use division rule. We have to select 3 people say a, b, c. so if I select abc in this sequence is same as select bca or cba because here order does not matter. So, such 3! Permutation exists of abc. Thus, all 3! Strings map to 1 string abc.



$= \frac{5P_3}{3!} = {}^5C_3$ or $C(5,3)$

combination

${}^nC_r$ = n choose r

${}^nP_r$ = n Permute r

Q : How many poker hands of five cards be dealt from a standard deck of 52 cards ? Also, how many ways are there to select 47 cards from a standard deck of 52 cards ? – answer of first question is C(52, 5) very simple, and second is C(52, 47) both are same because selecting 5 cards from 52 cards is same as selecting 47 cards for rejecting from 52 cards.

$$C(n, r) = C(n, n - r) \;\; 0 \le r \le n$$

It is pretty obvious that we cannot select r(>n) objects from n objects.

//Lecture 13

Now we are going to discuss some templets(cases) of combination and permutation :

- **Some elements always together** :

If some elements are always together then consider them as a single element or box and then permute. For example, total number of permutations of the letters ABCDEFG contains strings ABC and DE –

$\boxed{ABC}\boxed{DE}$ FG $\longrightarrow$ 4! permutation

- **Some element never together** :

In such case we first place element which may or may not be together. Then in gaps we will place element which should never be together. For example,

Q : How many ways are there for eight men and five women to stand in a line so that no two women stand next to each other ? – First position the men (m_i) and then consider possible positions for the women(w_i).

Gaps

$$\circ\, m_1 \circ m_2 \circ m_3 \circ m_4 \circ m_5 \circ m_6 \circ m_7 \circ m_8 \circ$$

$${}^{Gaps}C_5 \times 5! \longrightarrow \boxed{w_1 \quad w_2 \quad w_3 \quad w_4 \quad w_5} \qquad = 8! \times {}^9C_5 \times 5!$$

//Lecture 14a

6.2) Combinatorial Arguments :

In this section we are going to see combinational arguments with making stories and proving identities with pure logic.

6.2.1) Combinational identities :

1) **Pascal's identity** : let n and K be positive integers with n>=k. Then $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

Proof. This is same as you have n+1 student in class and you have to select k students. Consider a random student Bunty. Now, if you are selecting k student from n+1, in selected k student bunty will be there or bunty will not be there. So, we have two cases, if Bunty is already selected then we will have C(n, k-1) ways for selecting remaining student and if bunty is not included in selected student then there will be C(n, k) because now sample space will reduce from n+1 to n and we still have to select k students. ■

Similarly, we can extent this idea to two already selecting two student or rejecting two students.

$${}^{n+1}C_K = \underbrace{{}^{n-1}C_{K-2}}_{\text{both selected}} + \underbrace{{}^{n-1}C_K}_{\text{both rejected}} + 2\,\underbrace{{}^{n-1}C_{K-1}}_{\text{1 student is selected and 1 student rejected}}$$

Above all formula are called **recursive definition of <u>binomial coefficient</u>**.

//Lecture 14b

2) **Vandermonde's Identity** : $\binom{n+m}{r} = \sum_{k=0}^{r}\binom{n}{k}\binom{m}{r-k}$

Similarly, by creating stories we can prove other identity for example,

$$\binom{n+m}{r} = \binom{n}{0}\binom{m}{r} + \binom{n}{1}\binom{m}{r-1} + \binom{n}{2}\binom{m}{r-2} + \cdots + \binom{n}{r}\binom{m}{0}$$

This same as selecting r person from n males and m females. First, we can select all r man + we can select 1 man and r-1 women to form r and so on.

Let's prove another identity by creating stories, For any nonnegative integer n, $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$

First look at LHS it says $\sum_{k=0}^{r} k\binom{n}{k}$ we can break it down $\sum_{k=0}^{r}\binom{n}{k}$ this is saying subsets of n people. Or we can say number of different committees from n people. Then we are multiplying it with k. this is same as first making committee of k people from n and then selecting 1 chairperson from selected k people. Thus, meaning of LHS is form different committee from n people with a chairperson.

This is same as first selecting chairperson from n and then forming subset or different group with remaining n-1 people. i.e. n * 2^{n-1}.

//Lecture 14c

Q : Prove that $C(n,r) + C(n-1,r) + C(n-2,r) + \cdots + C(r,r) = C(n+1,r+1)$ – RHS says select r+1 people from n+1 people. And LHS is saying first take r+1 and then put aside one number from already taken r+1. You can prove this by pascal's identity also (try).

Hockey-Stick identity : $\binom{n+1}{r+1} = \binom{n}{r} + \binom{n-1}{r} + \binom{n-2}{r} + \cdots + \binom{r+1}{r} + \binom{r}{r}\ for\ n, r \in N, n > r$

//Lecture 15

6.2.2) Binomial Theorem :

Binomial means summation of two terms. Binomial theorem is our childhood theorem. Take an example,

Consider, $(a+b)^2 = \underset{1}{(a+b)}\underset{2}{(a+b)}$

$a.a + a.b + b.a + b.b$ = numbers of combination of terms selected from different set

This is same set consisting of same elements and selecting one element from different sets such that no two elements belongs to same set.

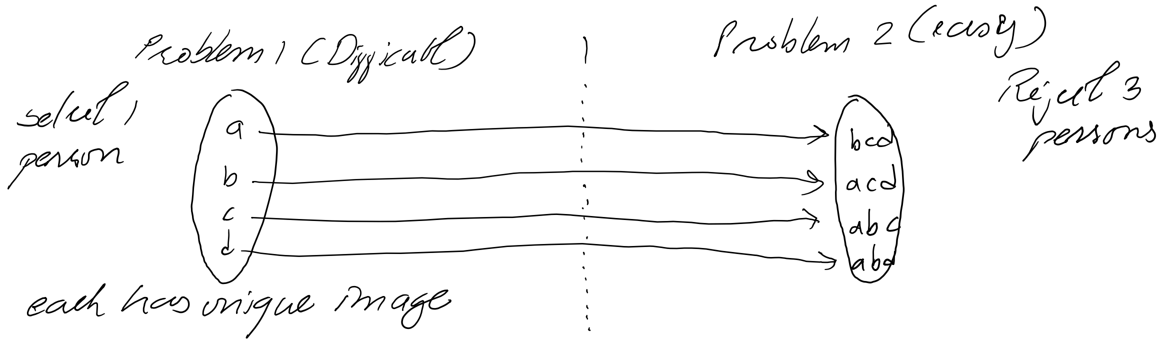
Similarly, $(a+b)^n = (a+b)(a+b)(a+b) \ldots n\ times\ (a+b)$ how many times $a^r b^{n-r}$ can occur ? – first select r sets from which you will select a and from remaining you will select b. we can either select 0 a at minimum and at maximum we can select n a's. We can write this in summation form as,

$$(a+b)^n = \sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r}$$

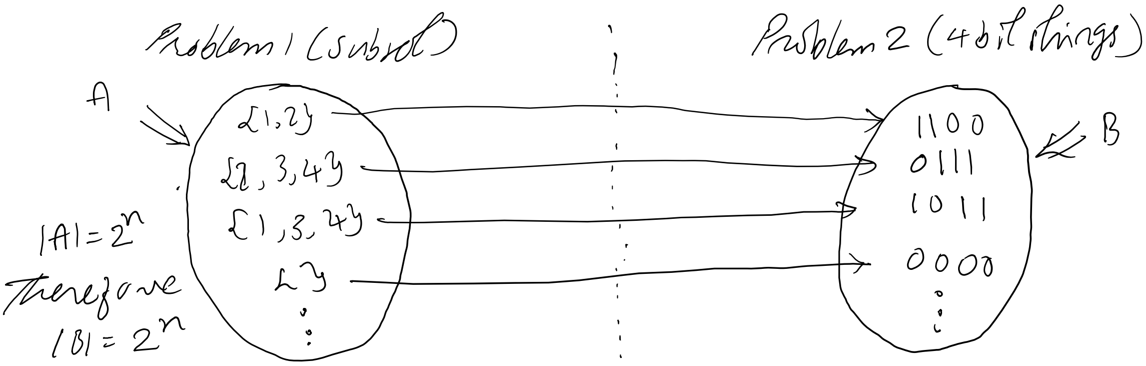
//Lecture 16

Bijective proofs : A bijective proof in combinatorics just means that you transfer one counting problem that seems "difficult" to another "easier" one by putting the two sets into exact correspondence. Let's take one example,

Task of selecting 1 person from 4 people (a, b, c, d) .



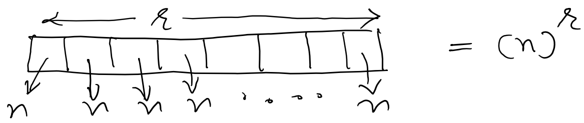
Another example, ask yourself which of the following is easier for you ? – counting bitstrings of length of n or counting number of subsets of a set of size n.



//lecture 17

6.2.3) Permutation with repetition :

Consider one problem of creating three-digit number using two digits (let's say 1, 2). It is obvious that without repetition it is not possible. We know that for each three position of digits 2 choices are there so in short, we can create 2^3 numbers.

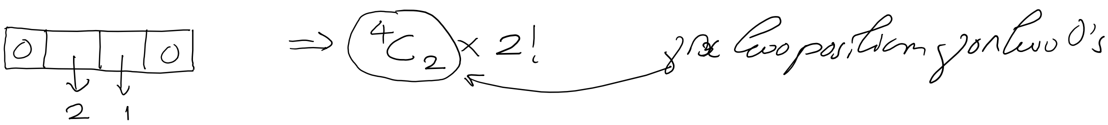


In general, the number of r-permutations of a set of n objects with repetition allowed is n^r.

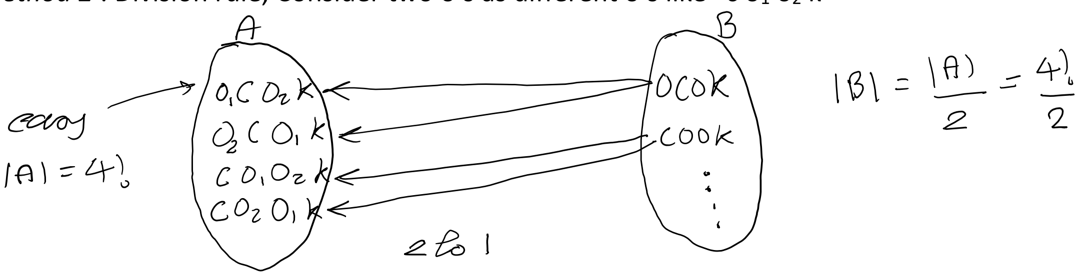
- **Permutation with repeated elements** : A permutation of a set of objects in an ordering of those objects. When some of those objects are identical, the situation is transformed into a problem about permutations with repeated elements.

Q : How many permutations of "cook" are there ? –

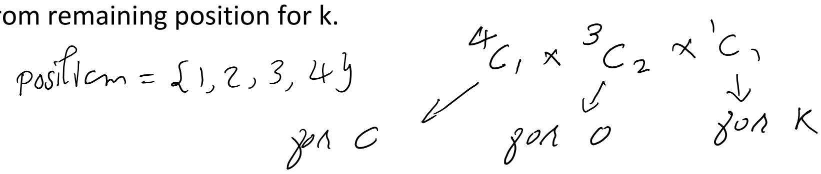
Method 1 : First select two position fixed for two o's and then permute remaining two letter.



Method 2 : Division rule, Consider two o's as different o's like "c o_1 o_2 k"



Method 3 : we first select one position for C and two position from remaining position and 1 position from remaining position for k.



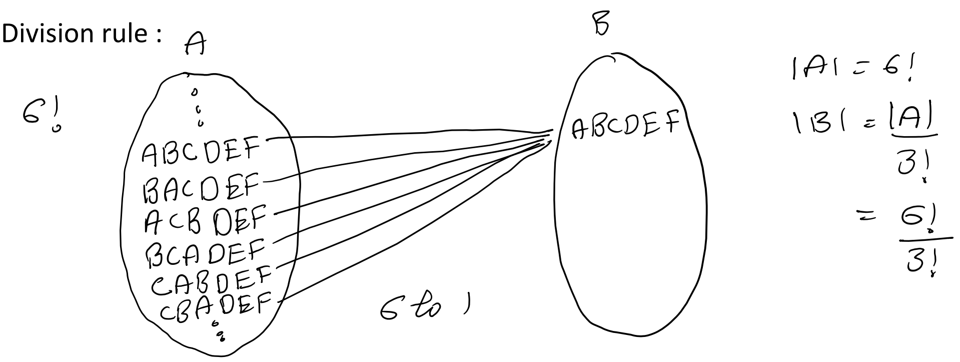
So, from now on if permutation with repeated elements is given you have to solve using all 3 methods (good practice for gate)

In short we can say that, If n elements are consists of n_1 of type 1, n_2 of type 2, n_3 of type 3,…, n_k of type k then permutation with repeated element will be $\frac{n!}{n_1!n_2!n_3!\dots n_k!}$

//lecture 18

Q : Number of permutations of word ABCDEF in which A comes before B and B comes before C (not necessarily immediately) – This question is same as counting word which have ABC subsequences. We will see two methods of solving this question.

Method 1 : Division rule :

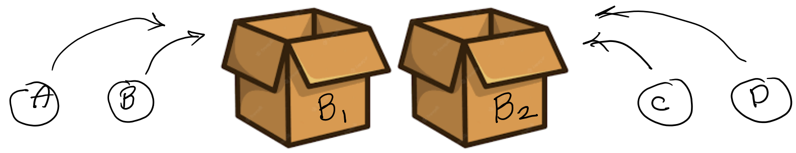


Method 2 : First select three position for ABC. Once you have selected position you cannot change the order as A must come before B and C. So, we can permute remaining element.

$$^6C_3 \times 3!$$

//Lecture 19A

6.3) Distributing objects into boxes :



We may encounter four cases :

- Distinguishable objects into Distinguishable boxes (DODB)
- Indistinguishable objects into distinguishable boxes (IODB)
- Distinguishable objects into indistinguishable boxes (DOIB)
- Indistinguishable objects into indistinguishable boxes (IOIB)

6.3.1) Distinguishable objects into distinguishable boxes : (DODB)

Q : How many ways are there to distribute hands of 5 cards to each of four players from the standard deck of 52 cards ? -

a, b, c, d ← players

5 5 5 5 ← 5 cards to each from 52

$$^{52}C_5 \times {}^{47}C_5 \times {}^{42}C_5 \times {}^{37}C_5 = \frac{52!}{5!\,5!\,5!\,5!\,32!}$$

But why we are getting such pattern ? – Because you can consider this problem like this. We know that 5 cards will definitely be for A, B, C, D. so we write AAAAA on five cards and same for B, C, D. and for remaining 32 cards will not be distributed to anyone else so we write TTTT…32 times. Now, this problem reduces to permuting string AAAAABBBBBCCCCCDDDDDTTTT…32 times T.

//Lecture 19B

Objects to be placed into boxes where the order these objects are placed into the boxes does not matter

//Lecture 20A

6.3.2) Indistinguishable objects into Distinguishable boxes : (IODB – star bar problem)

Consider giving 5 chocolates to 3 children. What mattes here ? – number or order ?

○○○○○ A B C

number matters

A | B | C

○○ | ○ | ○○

$^7C_2$

Above problem is same as selecting position of 2 bars among 5 chocolates.

star bar		IODB
r stars n-1 bars	$\Rightarrow \boxed{^{n+r-1}C_r} \Leftarrow$	r objects n boxes

Q : How many ways are there of distributing 30 identical objects into 3 distinct boxes if each box must have at least 5 items ? – This problem is saying at least 5 items which means each box already have 5 items we just have to put remaining items into 3 boxes. So, 30-15 = 15 items remaining. Now, we convert this problem to star bar problem, we will get, 15 star and 2 bars => C(17, 2)

Using IODB we can create five types of problems. Let's explore…

//Lecture 20B

1) **Problems related to star bar/ IODB** :

Q : The number of ways to distribute 8 identical balls to 12 urns is the same as the number of ways to distribute 11 identical biscuits to 9 dogs. – This statement is true how ? First, we write object and box and then we convert this problem to star-bar problem.

8 identical balls, 12 urns
8 stars, 11 lines
$^{19}C_8$

=

11 biscuits, 9 dogs
11 stars, 8 bars
$^{19}C_8$

2) **Combination with repetition** :

Imagine you are in market and you want to buy 4 fruits from apples, mangoes, oranges. Here in what order I select fruits does not matter. And this is problem of combination in which I can have more than one apple, mangoes, oranges. This is the problem of combination with repetition. How this is connected to star bar or IODB problem ?

We can deduce this problem to following :

Here star is number of objects and bar is fruits(distint) - 1.

apples	oranges	mangoes
2	1	1
1	2	1
3	1	0

- Combination help us to answer the question "In how many ways can we choose r objects from n objects ?"
- And combination with repetition ask us "In how many ways can we choose r objects from n kinds of objects?" in apple, orange exmple, n kinds of objects means type of fruits.

//Lecture 20C

3) **Non-negative integer solution** :

Consider one equation x + y + z = 10 and We ask "How many non-negative integer solutions are there?" To tackle this problem, we use IODB format.

x	y	z
5	5	0
5	0	5

diff. = star bar problems

This is same as star-bar problem where + sign is bar and 10 number is number of stars.

If we ask "How many positive integer solutions are there?" then 0 is not allowed, so we allocate 1 to all the variable to make them positive and as a result our star will gets reduced by same amount.

Q : But in real we can have some restriction on numbers that x, y and z can take just like asking "How many solutions to x + y + z = 10 such that a>=2, b>=-2, c>=0 ?" – In previous example we handled the condition of positive solutions by giving each variable 1 number. Just like that we can handle a>=2 situation by already giving a, 2 numbers. To handle b>=-2 condition we have to take 2 numbers from b and add them to total. And c is already in sync with our problem. So, in the end we will have equation like x' + y' + z = 10 such that x', y', z>=0 where x' = x+2 and y' = y – 2. Final answer is C(12, 2)

Q : In reality we can also have inequalities associated with variable so we ask another question "How many non-negative solutions can x + y + z <=8 have ?" – we can always convert inequalities by converting them to equal to sign by introducing a new variable. x + y + z + w = 8. Problem solved !

//Lecture 20G

Integer compositions of n :

In mathematics, a composition of an integer n is a way of writing n as the sum of a sequence of positive integers. Example, composition of 4 would be $\underbrace{1 + 3, 3 + 1}_{\text{Diff}}$, 2 + 2, $\underbrace{1 + 1 + 2, 1 + 2 + 1}_{\text{Diff}}$,…

We can say that composition of n is ordered summation of positive integer. You can also specify more info as such, composition of 4 into 3 parts. This is equivalent to positive integer solution.

The set of compositions of n into k parts =

$B_1 + B_2 + B_3 + \dots + B_k = n$, $B_i \geq 1$

remaining stars $n-k$

Bar $= k-1$

$$\binom{n-k+k-1}{k-1} = \binom{n-1}{k-1}$$

This formula represents composition of n into k parts. From this we can have formula for distributing n distinct objects into k distinct boxes so that no boxes are empty. here in integer compositions of n we have considered that objects are indistinguishable. We can make them distinguishable by multiplying n!.

So, Ways of distributing n distinct objects into k distinct boxes so that no boxes are empty is,

$$\binom{n-1}{k-1} n!$$

What if we ask "What is the total no. of composition?" – This means taking value of k from 1 to n. Thus, total no. of composition of n would be $\sum_{k=1}^{n}\binom{n-1}{k-1}$. But

$$\sum_{k=1}^{n}\binom{n-1}{k-1}=\sum_{k=0}^{n-1}\binom{n-1}{k}=\mathbf{2^{n-1}}$$

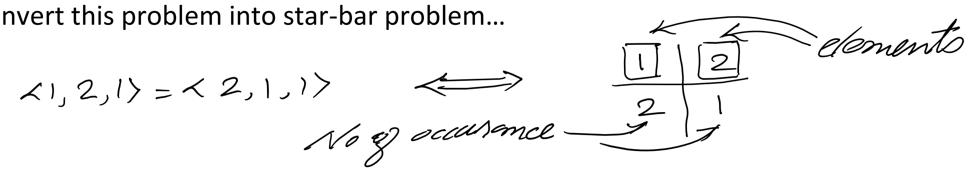
//Lecture 20D

4) Multiset Problem :

Multiset is a set with repetition allowed. For example, in set {1, 2} = {2, 1, 2} but in multiset <1, 2> != <2, 1, 2> but {1, 2} = {2, 1} in set and <1, 2> = <2, 1> in multiset meaning order doesn't matter.

Problem is "*If elements are 1, 2 then how many multisets of size of 3 can be constructed ?*"

We can convert this problem into star-bar problem…

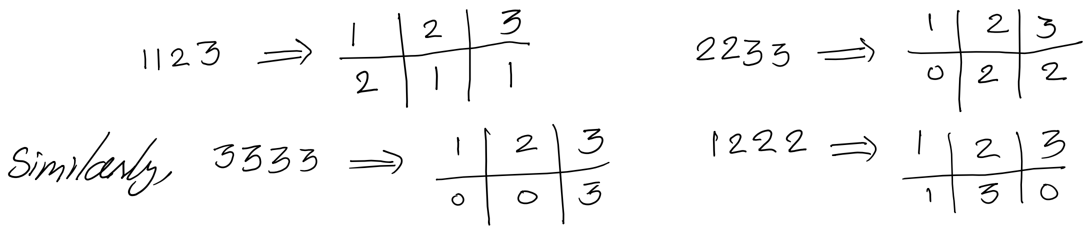


Here, star = 3 (size of multiset) and bar = 1 (no. of distinct elements – 1)

//Lecture 20E

5) Non-decreasing integer sequences :

Q : The number of 4-digit numbers having their digits in non-decreasing order (from left to right) constructed by using digits belonging to the set {1, 2, 3} is ? – We can convert this problem to star-bar problem like below…



Here star = 4 = number of digits in (here 4-digit number) and bar = 2 = number of elements in set – 1 (here 1, 2, 3 so total 3 elements)

In general, problem "find the number of non-decreasing sequences of length-n sequences from {1, 2,…, m}" is equal to star = n and bar = m-1. Thus, C(n+m-1, n).

//Lecture 20F

Q : How many non-decreasing sequences of 6 integer from set {0, 1, 2, 3} ? – $\binom{6+4-1}{3}-1$ why -1 because of 000000 can occur but you're wrong, Read the question carefully it says sequences of 6 integer not number or digit. So, 000000 will also count.

Notation : $\left(\binom{n}{k}\right)=\binom{n+k-1}{k}$ selecting k objects from n kinds of objects. i.e. k star and n - 1 bar

In short, we can say that,

	Order matters	*Order does not matter*
Repetition is not allowed	$P(n,k)$	$\binom{n}{k}$

Repetition is allowed	n^k	$\binom{n+k-1}{k}$

//Lecture 21

6.3.3) Distinguishable objects into indistinguishable boxes :

Analogy used "Friends trips to haunted hotel with same rooms" == Number of equivalence classes of set. == number of partitions

Q : 5 friends, creating two groups, of size 3 and size 2. How many ways ? – let's say 5 friends are a, b, c, d, e. size 3 and size 2 groups can have abc, de or bcd, ae but one thing to note is that abc, de and de, abc are same here order of group doesn't matter we are only concern about element of group. Answer is C(5 ,3) * C(2, 2).

Q : 8 friends. Creating three groups, of size 3, size 3, size 2. How many ways ? – similar to above question answer should be C(8, 2) * C(6, 3) * C(3, 3). But this is wrong why we are overcounting cases like,

123 456 78
456 123 78 } same $\Rightarrow \dfrac{{}^8C_2 \times {}^6C_3 \times {}^3C_3}{2!}$

Q : 9 friends. Creating four groups, of size 2, size 2, size 2 and size 3. How many ways ? – First, we choose size 3 from 9 friends. Then we have three size 2 groups which we can overcount so we divide it by 3!. Thus, C(9, 3) * C(6, 2) * C(4, 2) / 3!.

Q : 3 Friends. How many ways partition can be created ? – here partition is same as groups but size is not given so we can have group of 1, 2, 3 friends. And we know that it is bell number with n = 3. But let's solve it following way.

1 part : abc ← 1 ways
2 parts : (2, 1) ← ${}^3C_2$ ← 3 ways = 5 partitions
3 parts : a, b, c ← 1 ways

But this only works for partition and we do not have any generalize formula for DOIB templet.

Q : How many partitions of 5 elements are there ? – from bell number it is 52. Partition means non-empty so **bell no. = no. of non empty partition**

1 part partition → 1 way
2 part partition : (1, 4) → ${}^5C_1$
(2, 3) → ${}^5C_2$
3 part partition : (1, 1, 3) → ${}^5C_3 \times {}^2C_1 / 2!$
(2, 2, 1) → ${}^5C_1 \times {}^4C_2 / 2!$
4 part partition : (1, 1, 1, 2) → ${}^5C_2 \times {}^3C_1 \times {}^2C_1 / 3!$
5 part partition : 1 way
} 52

Q : If prime factorization of X is $p_1^{c1}\ p_2^{c2}\ p_3^{c3} \dots p_k^{ck}$. Then what is the number of ways for which X can be resolved as a product of two factors, such that those two factors are relatively prime ? – Relatively prime means gcd of two number is 1. Question asks for number of ways such that X = mn where m, n are relatively prime. Here we have k distinguishable objects and two boxes. Same as partition of k objects into two part. This is same as binomial expansion of $(1+1)^k/2$. Why 2 because we are overcounting (x, k-x), (k-x, x) cases. Final answer 2^{k-1}.

//Lecture 22

6.3.4) Indistinguishable objects into indistinguishable boxes (IOIB) :

Q : How many ways to put 7 balls in 4 identical bins ? – We can create 4 cases because of 4 bins,

Case 1 : only 1 bin is used = (7, 0, 0, 0)

same

Case 2 : only 2 bins is used = (6, 1, 0, 0), (5, 2, 0, 0), (0, 5, 2, 0), (4, 3, 0, 0)

Case 3 : only 3 bins is used = (5, 1, 1, 0), (4, 2, 1, 0), (3, 2, 2, 0), (3, 3, 1, 0)

Case 4 : only 4 bins is used = (4, 1, 1, 1), (3, 2, 1, 1), (2, 2, 2, 1) … So, in total 11 ways.

Remember this is not same as integer composition, in integer composition order matters as it belongs to IODB template. but above question is same as partition of 5. Seven partition of 5 are :

5, 4 + 1, 3 + 2, 3 + 1 + 1, 2 + 2 + 1, 2 + 1 + 1 + 1, 1 + 1 + 1 + 1 + 1.

What is integer partition ? – If n is a positive integer, than a partition of n is a non-increasing sequence of positive integers p1, p2, p3,…, pk whose sum is n. Each pi is called a part of the partition. We let the function p(n) denote the number of partitions of the integer n. example, P(5) = 7 as we saw previously.

This is different from integer composition and partition of set. In integer composition you have distinguishable boxes and in partition of set you have distinguishable element. But in integer partition boxes and elements both are indistinguishable. In short,

Composition of natural number = IODB template

Partition of a set = DOIB template

Partition of Natural number = IOIB template

//Lecture 24A

6.4) Inclusion – Exclusion principle :

A *tool* to find union of a finite number of sets.

Q : How many integers from "a" to "b" (inclusive) are multiples of n(i.e. divisible by n) ? –

1 ——— $\boxed{a \text{ ——— } b}$ ← we want this

a-1

$$\left\lfloor \frac{b}{n} \right\rfloor - \left\lfloor \frac{a-1}{n} \right\rfloor$$

Q : Line up of 7 people – Mother, father, 3 sons, 2 daughters. How many line-ups are there in which the mother is next to at least one of her 3 sons ? –

Method 1 : using complement rule

case 1 :

M _ _ _ _ _ _

$3 \times 5!$

Case 2 :

_ _ _ _ _ _ M

$5! \times 3$

Case 3 :

_ M _ _ _ _ _

$5 \times \boxed{3 \times 2} \times 4!$

$$\Rightarrow 7! - \{3 \times 5! \times 2 + 5 \times 3 \times 2 \times 4!\}$$

Method 2 : Using inclusion-exclusion principle, Question asks for $\underbrace{\text{(MS1/S1M)}}_{\text{same}}$ or (MS2/S2M) or (MS3/S3M) here M represents mother and S1, S2, S3 represents son.

$$= MS_1 + MS_2 + MS_3 - S_1MS_2 - S_2MS_3 - S_1MS_3$$

$$(\_MS_1\_ / \_S_1M\_) \Rightarrow MS_1 \leftarrow \text{as one element}$$

$$= 3 \times (6! \times 2!) - 3(5! \times 2!)$$

//Lecture 24b

Q : How many solutions does $x_1 + x_2 + x_3 = 11$ have, where x_1, x_2 *and* x_3 are nonnegative integers with $x_1 \le 3, x_2 \le 4$ and $x_3 \le 6$? – Here we use Total – unfavorable case = Favorable case. But what is total here so all variable should be nonnegative integers which means total = C(11+2, 2) = C(13, 2) all the non-negative solution. Now, talking about unfavorable case which would be $(x_1 \ge 4$ *or* $x_2 \ge 5$ *or* $x \ge 7)$ this is negation of constraints given in question.

$$(x_1 \ge 4 \text{ or } x_2 \ge 5 \text{ or } x_3 \ge 7) = (x_1 \ge 4) + (x_2 \ge 5) + (x_3 \ge 7)$$
$$- (x_1 \ge 4 \,\&\, x_2 \ge 5) - (x_2 \ge 5 \,\&\, x_3 \ge 7) - (x_1 \ge 4 \,\&\, x_3 \ge 7)$$
$$+ (x_1 \ge 4 \,\&\, x_2 \ge 5 \,\&\, x_3 \ge 7)$$
$$= {}^9C_2 + {}^8C_2 + {}^6C_2 - {}^4C_2 - 0 - {}^2C_2 + 0$$

Final answer : ${}^{13}C_2 - {}^9C_2 - {}^8C_2 - {}^6C_2 + {}^4C_2 + {}^2C_2$

//Lecture 24c

6.4.1) Derangement : No one in their own place

A derangement is a permutation of the elements of 1, 2, 3, …, n such that none of the elements appears in their original position. Consider word consists of abc,

Permutations : abc, acb, bac, bca, cba, cab

Derangment : ✗ ✗ ✗ ✓ ✗ ✓

$\boxed{D_3 = 2}$

Similarly, D_2 = 1. Which means derangement = $\bar{a} \wedge \bar{b} \wedge \bar{c}$

'a' is not in its own place

So, let's find general formula, D_n = ?

#Derangement = n! – (at least one number should be its own place)

Let, [1] represents 1 (a number) is its own place. Thus,

At least one number should be its own place = [1] + [2] + … +[n] – [1][2] – [1][3] + … + [1][2][3] + [1][2][4] + … + $(-1)^{n-1}$ ([1][2]…[n]).

Now, [1] : $\underbrace{\boxed{1}\,\_\_\_\_}_{(n-1)!}$ & [2] : $\underbrace{\boxed{2}\,\_\_\_\_}_{(n-1)!}$ …

[1][2] : $\underbrace{\boxed{1}\boxed{2}\,\_\_\_\_}_{(n-2)!}$ & [1][3] : $\underbrace{\boxed{1}\,\_\boxed{3}\,\_\_\_}_{(n-2)!}$

At least one number should be in its own place = $n \times (n-1)! - C(n,2) \times (n-2)! + C(n,3) \ldots$

Derangement = $n! - \underbrace{n \times (n-1)!}_{\frac{n!}{1!}} + \underbrace{C(n,2) \times (n-2)!}_{\frac{n!}{2!}} - \underbrace{C(n,3) \times (n-3)!}_{n!/3!} + \cdots$

 # Derangement = $\boldsymbol{n! \times \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + \frac{(-1)^n}{n!}\right)}$

Derangement with repetition :

Consider derangement of word "BOTTLE" here simply !6 contains overcounting cases like OT_1BLET_2 OT_2BLET_1

case 1 : BOTTLE first T goes to 2nd T position and 2nd T goes to position other than 1st T position.

case 2 : BOTTLE 2nd T goes to 1st T position & 1st T goes to position other than 2nd T position

case 3 : BOTTLE Both goes to alternate position.

We need to subtract all these three cases from !6 ➔ !6 - !5 - !5 - !4 and as both T are same we need to divide it by 2! . So, correct answer is $\frac{!6-!5-!5-!4}{2!}$.

NOTE :

1) **If you observe carefully, boxes which we have taken in calculation are distinct if they were not distinct then there is no point of position. And elements are also distinct. Which means the formula of D_n works iff n distinct elements in n distinct positions.**

//Lecture 24D

6.4.2) The number of onto function :

A function $f: A \to B$ is onto iff every element of B has preimage.

We want to know the total number of possible onto function from A to B. We use complement rule to simplify this problem to

#onto function = Total – Not onto function

$|codomain|^{|domain|}$

Consider one example, let $f: \{1,2,3,4\} \to \{a,b\}$ then # of onto function = 2^4 – (a does not have preimage(*a) ∪ b does not have preimage (*b))

(*a) ∪ (*b) = *a + *b - *a*b → 0 = 2

1^4 1^4

# of onto function = 16 – 2 = 14.

Q : How many ways are there to assign five different jobs to four different employees if every employee is assigned at least one job ? – This is DODB templet so we use our usual method,

Method 1 : Employee

A	B	C	D	
2	1	1	1	← let x
1	2	1	1	← x
1	1	2	1	← x
1	1	1	2	← x

final ans = 4x
= 4×5×4×3
= 240

A B C D
2 1 1 1 $\Longrightarrow \frac{5!}{2!(1!)^3} = 5\times4\times3$

Method 2 : Here it is written as every employee is assigned at least one job. Meaning every employee have at least one preimage this is same as saying $f: job \rightarrow employee$ and we have to find # of onto functions.

# of onto function = $4^5 - (4.\ 3^5 - C(4,2).\ 2^5 + C(4, 3).\ 1^5 - 0) = 1024 - 784 = 240$.

NOTE :

1) **If we reduce some problem into finding no. of onto function then if |B| = |A| - 2 then apply DODB and if |B| < |A| - 2 then apply inclusion-exclusion principle.**

INTO function : function which are not ONTO. i.e. Total function – Onto function

//Lecture 25A

6.5) Generating function :

Generating function is tool which converts sequence into function.

Let's say sequence S = $a_0, a_1, a_2, a_3, a_4, \ldots$

0^{th} term $\quad 1^{st}$ term

G(S) = $a_0x^0 + a_1x^1 + a_2x^2 + a_3x^3 + \ldots = \sum_{n\geq 0} a_n x^n$. This power series is the generating function of sequence S. Our task is to find a_n i.e. coefficient of x here x is just a dummy variable meaning we do not care about x. We have taken power series just to express sequence into some math function. In generating function, we never put value of x like 1, 2 and conclude anything related to convergence.

There are many types of generating function but in gate we have only ordinary generating function. So, if we say generating function it means ordinary generating function. (for simplicity)

//Lecture 25B

For upcoming content, we need some knowledge of AP, GP, and **infinite** AGP. One formula which we use frequently is

If S = a + (a+d)r + (a+2d)r2 + (a+3d)r3 + … $\Rightarrow rS = 0 + ar + (a+d)r^2 + (a+2d)r^3 + \ldots$

$(1-r)S = a + dr + dr^2 + \ldots = a + \frac{dr}{1-r}$

$$S = \frac{a}{1-r} + \frac{dr}{(1-r)^2} \ldots for\ infinite\ AGP$$

For example, Let $G(S) = 1 + 2x + 3x^2 + 4x^3 + \ldots = \frac{1}{1-x} + \frac{1.x}{(1-x)^2}$

For finite AGP, we follow our standard procedure of multiplying by r and subtract and then sum.

Here don't worry about x = 1. We don't care we only care about sequence.

As generating function is function, we can also do differentiation.

//Lecture 25D

Q : How can I determine the sequence generated by a generating function $f(x) = (2x - 3)^3$? – We know that this series will be in the form of

$$f(x) = a_0 + a_1x + a_2x^2 + \dots$$

It is very obvious that if we put x = 0 then we will get a0 but in that matter if we put x = 1 do we get a1 ? Absolutely not. But if we take derivative of f(x) and then put x = 0 then we will get a1 also. Here in this example, we put x = 0 to get a0 term, a0 = -27. If we take derivative, we will get $f'(x) = 6(2x - 3)^2$. Then put x = 0, a1 = 54. Similarly,

$$f''(x) = 24(2x - 3) \xrightarrow{x=0} a_2 = -72$$

But in gate we don't do this, we simply expand this formula.

//Lecture 25E

Q : Let m be a positive integer. Let ak = C(m, k), for k = 0, 1, 2, …, m what is the generating function for the sequence a0, a1, …, am. ? -

Sequence is $\binom{m}{0}, \binom{m}{1}, \binom{m}{2}, \binom{m}{3}, \dots, \binom{m}{m}$

$$G(x) = \binom{m}{0} + \binom{m}{1}x + \binom{m}{2}x^2 + \dots + \binom{m}{m}x^m = (1+x)^m$$

What if we do not limit the value of k in previous question, then k = 0, 1, 2, 3, … then sequence will become,

$$\binom{m}{0}, \binom{m}{1}, \binom{m}{2}, \dots \binom{m}{m}, \underbrace{\binom{m}{m+1}, \binom{m}{m+2}, \dots}_{0} \quad \text{because } r > n, C = 0$$

But it still would be same as previous

//Lecture 25F

6.5.1) Extended binomial coefficient :

We know that C(n, r) is defined only for 0<=r<=n where n is whole number but we extend n to take real number also. For example, C(1/2, 2) = (1/2)*(1/2-1)/2! = -1/8. This is called *extended binomial coefficient*.

But some properties are not common between normal binomial and extended binomial coefficient. i.e. ${}^nC_r = {}^nC_{n-r}$ iff n ∈ N which means below equation is not true.

$${}^{-1/2}C_2 \neq {}^{-1/2}C_{-1/2-2}$$

But why we need extended binomial coefficient. We need this to solve problem such as

Q : What is the coefficient of x^4 in the expansion of $(1+x)^{-2}$? – This is same as asking C(n, 4) = C(-2, 4).

And in extended binomial coefficient we cannot handle expansion of $(a+b)^n$ where n ∈ Z. in such case we have to take a^n outside to get $a^n(1+(b/a))^n$. and then we solve.

We know that $${}^{-n}C_r = \frac{(-n)(-n-1)(-n-2)(-n-3)\dots(-n-r+1)}{r!} \leftarrow r \text{ terms}$$

$$= (-1)^r \frac{(n+r-1)\dots(n+1)n}{r!} = (-1)^r \frac{(n+r-1)\dots n \times (n-1)!}{r! \times (n-1)!}$$

$$= (-1)^r \frac{(n+r-1)!}{r! \times (n-1)!} = (-1)^r \times {}^{n+r-1}C_r$$

$$C(-n, r) = (-1)^r \times ^{n+r-1} C_r$$

//Lecture 25G

Similar to ordinary generating function, we also have *exponential generating function*. If we have sequence S = a_0, a_1, a_2, a_3, a_4,... then exponential generating function will be,

$$EG(x) = \frac{a_0 x^0}{0!} + \frac{a_1 x^1}{1!} + \frac{a_2 x^2}{2!} + \cdots$$

TABLE 1 Useful Generating Functions.

$G(x)$	a_k
$(1+x)^n = \sum_{k=0}^{n} C(n,k)x^k = 1 + C(n,1)x + C(n,2)x^2 + \cdots + x^n$	$C(n,k)$
$(1+ax)^n = \sum_{k=0}^{n} C(n,k)a^k x^k = 1 + C(n,1)ax + C(n,2)a^2x^2 + \cdots + a^n x^n$	$C(n,k)a^k$
$(1+x^r)^n = \sum_{k=0}^{n} C(n,k)x^{rk} = 1 + C(n,1)x^r + C(n,2)x^{2r} + \cdots + x^{rn}$	$C(n, k/r)$ if $r \mid k$; 0 otherwise
$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n$	1 if $k \le n$; 0 otherwise
$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots$	1
$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^k x^k = 1 + ax + a^2x^2 + \cdots$	a^k
$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \cdots$	1 if $r \mid k$; 0 otherwise
$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + \cdots$	$k+1$
$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)x^k = 1 + C(n,1)x + C(n+1,2)x^2 + \cdots$	$C(n+k-1,k) = C(n+k-1,n-1)$
$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)(-1)^k x^k = 1 - C(n,1)x + C(n+1,2)x^2 - \cdots$	$(-1)^k C(n+k-1,k) = (-1)^k C(n+k-1,n-1)$
$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)a^k x^k = 1 + C(n,1)ax + C(n+1,2)a^2x^2 + \cdots$	$C(n+k-1,k)a^k = C(n+k-1,n-1)a^k$
$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$	$1/k!$
$\ln(1+x) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$	$(-1)^{k+1}/k$

//Lecture 26 (playlist)

6.6) Recurrence relations :

Recurrence relations occur when some term in a sequence depends on the previous terms of the sequence. For example, Sequence : arithmetic sequence <3, 8, 13, 18, 23, 28, …> here $\underbrace{a_{n+1} = a_n + 5}_{\text{Recurrence Relation}}$ and $\underbrace{a_0 = 3}_{\text{Initial condition}}$

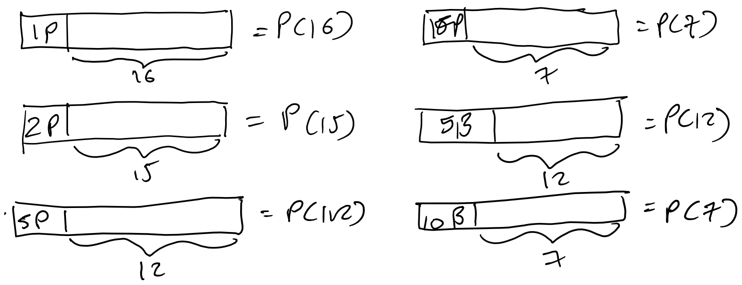
Initial conditions are required to specify terms that proceed the first term where the relation takes effect. One thing to note that every **recurrence relation (equation) + initial conditions = unique sequence** if we alter any of these things, we will get another unique sequence.

Q : Find a recurrence relation and give initial conditions for the number of bit strings of length n that do not have two consecutive 0s. How many such bit strings are there of length five ? – Let this RF (recurrence function) be f(n). Now, we know that if last bit of n string is 1 problem reduce to not finding out consecutive 0s in n-1 length of string. And if last bit is 0 then two cases are possible either second last string is 0 or 1. If it is 1 then problem reduce to n-2 string. And if 0 occurs then we do not accept string. Which means f(n) = f(n-1) + f(n-2). Now, for f(5) we want initial condition. 0

$$f(0) = 0,\ F(1) \longrightarrow \{0, 1\} = 2,\ f(2) \longrightarrow \{01, 10, 11\} = 3$$

Q : find recurrence relation and give initial conditions for the number of bit string of length n that have consecutive 0s ? – First, we find initial conditions, f(0) = 0, f(1) -> {0, 1} = 0, f(2) -> {00} = 2. Now, we know that if last bit is 1 our problem reduce to n-1 and if last bit is 0 then we again have two cases, (i) second last bit is 1 then we find in n-2, (ii) second last bit is 0 then we have found meaning whatever n-2 remaining string takes value we don't care meaning 2^{n-2}. $f(n) = f(n-1) + f(n-2) + 2^{n-2}$.

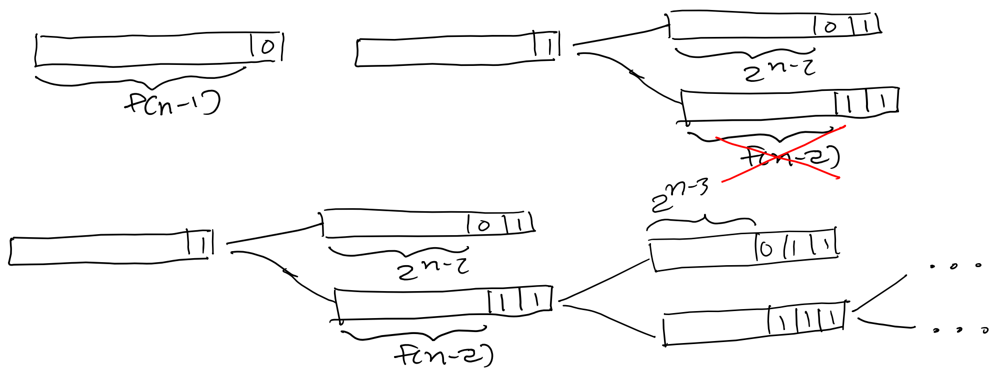
Q : How many ways are there to pay a bill of 17 pesos using a currency with coins of values of 1 peso, 2 pesos, 5 pesos, and 10 pesos, and with bills with value of 5 pesos and 10 pesos ? If the order in which the coins and bills are paid matters. – Let's represents ways to pay a bill of 17 pesos by P(17).



$$\boxed{P(17) = P(16) + P(15) + 2P(12) + 2P(7)}$$

Recurrence Relation

Q : Find a recurrence relation for the number of bit strings of length n that contain the string 01. – You first draw diagram and found that $f(n) = f(n-1) + f(n-2) + 2^{n-2}$.



We saw how our first answer is false. Answer should be $f(n) = f(n-1) + 2^{n-2} + 2^{n-3} + 2^{n-4} + \ldots + 2^1 + 1$ ➔ $\mathbf{f(n) = f(n-1) + 2^{n-1} - 1}$.

Derangement using recurrence relation :

We fix one element say k and thus for each n-1 remaining position and we check if element in that n-1 position takes position at index-k or not.

Case 1 : takes the kth position

$$\underbrace{1\ \ 2\ \ 3\ \ 4 \ldots \boxed{k} \ldots n-1,\ n}_{D_{n-2}}$$

Case 2 : doesn't take kth position

$$\underbrace{1\ \ 2\ \ 3\ \ 4 \ldots \boxed{k} \ldots n-1,\ n}_{D_{n-1}}$$

somewhere acept k^{th}

Here we have taken 1 then we take 2, 3 so on upto n (excluding k) total of n-1 iteration.

$$\boldsymbol{D_n = (n-1)(D_{n-1} + D_{n-2})}$$

We can simplify this formula to the following,

$$D_n - nD_{n-1} = -D_{n-1} + (n-1)D_{n-2} = (-1)\left[D_{n-1} - (n-1)D_{n-2}\right]$$
$$= (-1)\left[(n-2)D_{n-2} + (n-2)D_{n-3} - (n-1)D_{n-2}\right]$$
$$= (-1)\left[-D_{n-2} + (n-2)D_{n-3}\right] = (-1)^2\left[D_{n-2} - (n-2)D_{n-3}\right]$$
$$= (-1)^{n-2}\left[D_{n-(n-2)} - (n-(n-2))D_{n-(n-2+1)}\right] = \frac{(-1)^n}{(-1)^2}\left[D_2 - 2D_1\right]$$

$$\boldsymbol{D_n - nD_{n-1} = (-1)^n}$$

Proving bell number using recurrence relation :

Let B_{n+1} represents number of ways to partition n+1 elements. Consider a set S = {1, 2, 3, 4,…, n, n+1) and now consider one set A1 such that it includes (n+1)th element. |A1| = k+1 where 0<=k<=n. i.e. A1 can contains some or all elements which compulsorily including (n+1)th element. If we have chosen k+1 element from S to form A1 remaining elements are n-k. Number of ways to choose those k elements (not k+1 because 1 element is surely (n+1)th element) C(n, k) why n because we have already chosen (n+1) th element. And remaining n-k element can form their own partition in B_{n-k} ways.

$$B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_{n-k} = \sum_{k=0}^{n}\binom{n}{n-k}B_{n-k} = \binom{n}{n}B_n + \binom{n}{n-1}B_{n-1} + \binom{n}{n-2}B_{n-2} + \ldots$$

$$\boldsymbol{B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_k}$$

1.6.1) Limit of recursive sequence :

A **fixed point** of a function is a point x so that f(x) = x. For recursive sequences this translate as if the sequence $\{a_n\}$ is can be given as $a_{n+1} = f(a_n)$ and if a is a fixed point for f(x), then if $a_n = a$ is equal to the fixed point for some k, the all successive values of a_n are also equal to a for k > n.

For example, let $a_{n+1} = \frac{1}{4}a_n + \frac{3}{4}$. Fixed points for the recursion thus would satisfy $a = \frac{1}{4}a + \frac{3}{4}$, $a = 1$. This we have limiting point. But this will not always be the case : A fixed point is only a candidate for a limit; a sequence does not have to converge to a given fixed point (unless a_0 is already equal to the fixed point). The next two recurrence relation illustrate convergence and non-convergence, respectively.

1) $\lim_{n\to\infty} a_n$ for $a_{n+1} = \sqrt{3a_n}$ with $a_0 = 2$. Converges to value 3.

2) $\lim_{n\to\infty} a_n$ for $a_{n+1} = \frac{3}{a_n}$ with a_0 is not equal to a fixed point. This diverges.

This leaves us with the question of how do we know when a recursive sequence is going to converge. We refer to theorem known as *Monotonic sequence Theorem*.

Theorem : *Every bounded, monotonic sequence converges*.

Step 1 : find the fixed point.

Step 2 : check if function is bounded

Step 3 : check for monotonicity by procedure given below :

If by putting value of fixed point into f'(x) results in negative value meaning function is decreasing at that point and thus converges to that fixed point, next we again take double derivative check if graph is concave up. If graph is concave up meaning it must lie below line y = x if it does then lower value of fixed point is convergent value and if f"(x) is negative then function must lie above line means higher value of fixed point is convergent value. For example,

Example 1.8. Consider the recursive sequence $a_{n+1} = \frac{5}{6-a_n}$ with $a_1 = 4$. We want to show that $\{a_n\}$ converges and find its limit.

First, we look at the function: $f(x) = \frac{5}{6-x}$. Note that we have that $a_{n+1} = f(a_n)$ for all $n = 1, 2, 3, \ldots$, so this function generates our sequence.

Step 1 Find the fixed points.

$$\frac{5}{6-x} = x \Rightarrow 6x - x^2 = 5 \Rightarrow x^2 - 6x + 5 = 0 \Rightarrow x = 1 \text{ or } x = 5.$$

Step 2 Note that for $x > 1$ (which are the only values in which we are interested) we have that $1 \le f(x) < 6$ on $(1, 5)$. Thus, the function and hence the sequence are bounded.

Step 3 Note that for all $1 < x < 5$ we have that $1 < f(x) < 5$, so the function maps the interval $(1, 5)$ to itself.

Step 4 Note that the initial point a_1 lies between the two fixed points, so we only need to know that the sequence is monotonic on the interval $(1, 5)$, between the fixed points. This is easy since $f'(x) = \frac{5}{(6-x)^2} > 0$ for all $x \neq 6$. Hence, f is increasing. Also, $f''(x) = 10/(6-x)^3$ and the graph is concave up. Thus, the graph must lie below the line $y = x$ and the sequence is decreasing. Thus, since we start at 4, the limit will be 1.

n	1	2	3	4	5	6	7	8	9	10
a_n	4	2.50	1.429	1.094	1.019	1.004	1.001	1.000	1.000	1.000006

Source : RecursiveSequences.pdf (uky.edu)

//Lecture 27a

6.7) Pigeonhole Principle :

The pigeonhole principle : If m pigeons occupy n pigeonhole and m > n, then at least one pigeonhole has two or more pigeons roosting in it.

The best way to solve question which ask for "Guarantee" of even X is to try to prevent event x to happening.

//Lecture 27B – 020753

6.7.1) Generalized pigeonhole principle :

The idea is the best way to prevent "too much" in a room… is to uniformly distribute items in all rooms. Example, if you have 100 people in room then at least how many will have birthday in same month ? – Here we know that 12 months are there so we first uniformly distribute people in 12 months.

$\left\lceil \frac{100}{12} \right\rceil$

J	F	M	A	M	J	J	A	…	O
8	8	8	8	8	8	8	8	…	8

$= 12 \times 8 = 96$ 4 people are left

So, if we distribute 12 to those remaining 4 people, we will have 9 or more than 9 people in at least one month. So, at least 9 people have birthday in same month. Here answer is not 8 because if 8 is true then at least 7 is also true, at least 6 is also true so there is no point of using at least here. That is why we take maximum value.

Principle : If you distribute m objects into n bins, then some bin will have at least $\left\lceil \frac{m}{n} \right\rceil$ objects in it, and some bin will have at most $\left\lfloor \frac{m}{n} \right\rfloor$.

//Lecture 27c

Q : Let d be a positive integer. Show that among any group of d + 1 (not necessarily consecutive) integers there are two with exactly the same remainder when they are divided by d – when randomly chosen number is divided by d then possible remainder are {0, 1, 2, …, d-1} which are d in total. So if we add one more number to this d then the remainder of that number always matches with one of the d total. So, d + 1 number guarantees that at least two integers have same remainder.

Theorem : *For any natural number n, there is a nonzero multiple of n whose digits are all 0s and 1s.*

For example, 2|10, 3|111, 4|100, 5|100 and so on. Here 10 and all are not binary numbers they are natural number.

This theorem is consequences of previous question. Let's prove this theorem for every natural number separately,

- For any natural number n>= 2 generates the numbers 1, 11, 111, … until n+1 number are generated.
- There are n possible remainders module n, so two of these number must have the same remainder.
- So, there difference is a multiple of n.
- And we know their difference consists of just 1s and 0s.

Silly mistakes :

There are 16 points in a 2D plane of which 7 are collinear. If X number of triangles are formed and Y number of lines are formed by these given points, then which of the following statement is/are true?

(a) The value of X + Y is perfect square.

(b) The value of $\sqrt[4]{(X+Y)}$ is prime number.

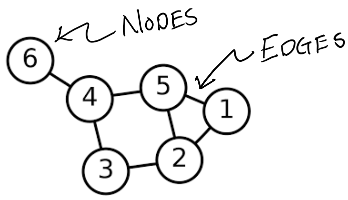
(c) The value of Y is perfect square.

(d) $\sqrt{(X+51)}$, $\sqrt{(X+Y)}$, $\sqrt{(X+Y+51)}$ are three consecutive integers.

Here $Y = {}^{16}C_2 - {}^{7}C_2 + 1$

Don't forget to add main line

7. Graph Theory



//Graph theory lecture 1

7.1) Basic Terminology :

Here graph is different from math function graph. Here graph is →

Graph is structure consists of nodes and edges connecting those nodes. Leonhard Euler in 1736 laid the foundations of graph theory.

//Lecture 2a

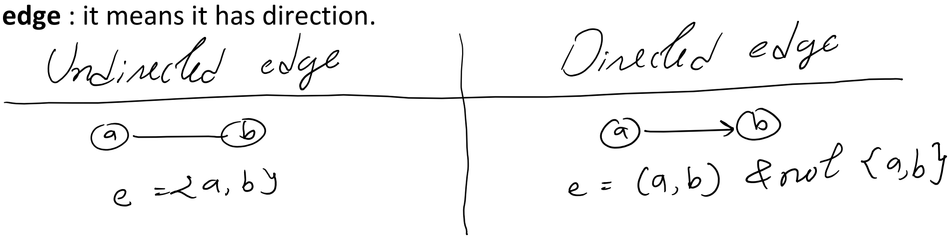
A graph G = (V, E) consists of two sets V and E. The element of V is called the vertices and the elements of E the edges of G. Each edge is a pair of vertices. For instance, the sets V = {1, 2, 3, 4, 5, 6} and E = {{1, 2}, {2, 3}, …{4, 6}} but why {1, 2} and not (1, 2) because (1, 2) implies order pair but edge is unordered pairs of vertices in undirected graph.

Number of edges are sometimes called **size of graph** and **number of vertices** are also known as **order of graph**.

7.1.1) Types of edges :

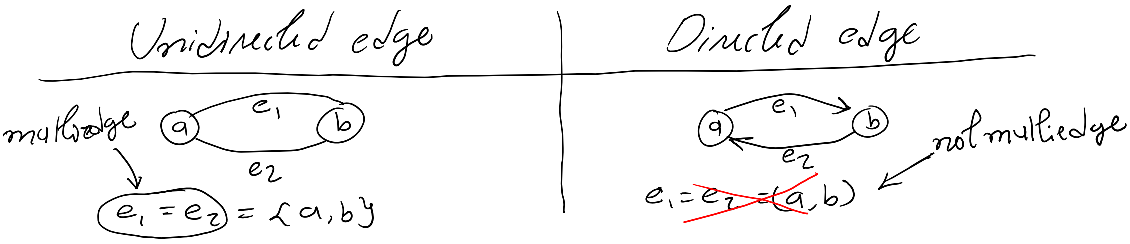
Undirected edge : It simply means it has no direction.

Directed edge : it means it has direction.



Self-loop : edges whose both end points are same.

Multi-edges/ Parallel edges : Exactly same edges.



7.1.2) Types of graph : based on types of edges

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

Undirected graph : every edge should be undirected.

G = (V, E)
set of vertices
multiset of edges

Directed graph : Every edge should be directed.

Multigraph: it should be undirected graph with no self-loops.

Pseudograph : Any undirected graph. Meaning multi-edges and self-loops are also allowed.

Directed Multigraph : It should be directed with multi-edges and self-loops are also allowed.

Simple graph : It should be undirected with no self-loops and no multi-edges.

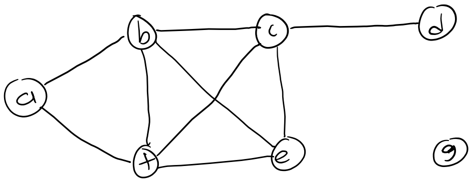
//Lecture 2b

7.1.3) Adjacency, degree of a vertex :

All adjacency and degree of a vertex concepts are only defined for undirected graph.

If {a, b} ∈ E then we say a, b is adjacent nodes/neighbors' nodes. If self-loop is present on some vertex then that vertex is neighbor of itself. Similarly, we have adjacent edges, *two edges are adjacent iff they both shares some common end points.*

1) **Degree of a vertex** : The degree of a vertex in an undirected graph is the number of edges incident with it, except that a loop at a vertex contributes twice to the degree of that vertex (but self-loop only happens in pseudograph). The degree of the vertex v is denoted by deg(v).



deg(a) = 2
deg(b) = 4
deg(c) = 4
deg(d) = 1
deg(e) = 3
deg(f) = 4
deg(g) = 0

A vertex of degree zero is called isolated. Vertex g in graph is **isolated**. A vertex is pendant if and only if it has degree one. Vertex d in graph is **pendant**.

//Lecture 2c

We can also have some terms such as *min-deg(G), max-deg(G), Total-deg(G)* representing min degree in graph G, max degree in graph G and total summation of all degrees respectively. *Avg-deg(G) = Total-deg(G) / no. of vertices*.

Degree sequence of graph : the degree sequence of a graph of order n is the n-term sequence (usually written in descending order) of the vertex degrees.

//Lecture 3A

2) ***Handshaking theorem*** : Total degree = 2 * |E|. This is fact from below observation

You may have noticed that in undirected graph inserting one edge will increase total degree by two.

Q : How many edges are there in a graph with 10 vertices each of degree six ? - every vertex has 6 degree meaning total degree is 10*6 = 60 and by handshaking theorem, 60 = 2 * |E| → |E| = 30.

Q : Can you create odd number of odd-deg vertices ? – We know that Total degree of even-degree vertices + total degree of odd-degree vertices = total degree = 2 * |E| which means it should be even. Now, Total degree of even-degree vertices => is always even as it is summation of even term(degree) so, even + x = even. Here x is total degree of odd -degree vertices. Which means x should be even. It means total degree of odd-degree vertices are even. So, we cannot have odd number of odd-degree vertices in graph.

An undirected graph has an even number of vertices of odd degree

We know that for undirected graph, $\sum_{\forall v \in V} \deg(v) = 2 \times |E|$ and there are n vertices then n*avg. degree = 2*|E|. This is true because suppose, a + b + c = t. now if you replace a, b, c by (a+b+c)/3 then result would remain same.

//Lecture 3B

3) Handshaking theorem for directed graphs :

initial vertex → $a \rightarrow b$ ← terminated ver. means a is adj to b
a is neighbour of b
a, ~~b are adjacent~~

In directed graph we have concept of in-degree and out-degree as edges are directed.

Indegree : denoted by $\deg^-(v)$, is the number of edges with v as their terminated vertex.

Outdegree : denoted by $\deg^+(v)$, is the number of edges with v as their initial vertex.

Note that a loop at a vertex contributes 1 to both the indegree and the out-degree of this vertex.

It means for every edge we have one indegree and one outdegree. It also means that if we add one edge to any graph its indegree and out degree will increase by 1.

$$\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E|$$

//Lecture 4A

7.1.4) Walk, Trail, path, cycle and circuits :

Walk : A *walk* in a graph is a sequence of alternating vertices and edges $v_1e_1v_2e_2...v_ne_nv_{n+1}$ with n>=0. If $v_1 = v_{n+1}$ then the walk is *closed*. The **length** of the walk is the number of edges in the walk. A walk if length zero is a **trivial walk**. Repetition of edges and vertices is allowed in walk.

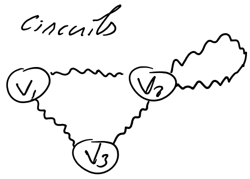
Trail : It is a walk where repetition of edges is not allowed. We also have *closed trail* which also known as *circuits*. **Trivial circuit** has a single vertex and no edges.

Path : It is a walk, in which repetition of edges and vertices are not allowed. Here we can omit saying repetition of edge because

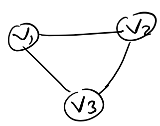
No vertex repetitions → *no edge repetition*, because there always exists one edge between two vertices in simple graph so if in sequence if vertices is not repeating then it means edges are also not repeating.

Cycle : It is a sequence of alternating distinct vertices (except first and last vertices) and distinct edges $v_1e_1v_2e_2...v_ne_nv_{n+1}$ with n => 3 and $v_1 = v_{n+1}$. We can say it is non-trivial circuits in which the only repeated vertex is the first/last one. Note that cycle only exists in graph when no. of distinct vertices are at least 3. Note that cycle is not path and path is not cycle.

Circuits



Cycle



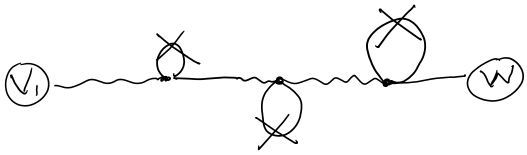
Here only one cycle is there not 3 cycles.

Let's summarize all things in table,

Repeated vertex	Repeated edge	open	closed	Name
✅	✅	✅		Walk(open)
✅	✅		✅	Walk (closed)
✅	❌	✅		Trail
✅	❌		✅	Circuit
❌	❌	✅		Path
✅ (only first/last))	❌		✅	Cycle

//Lecture 4B

Q : In a graph, if there is a walk from v to w then there is a path from v to w. – This can be obtained by deleting loops.



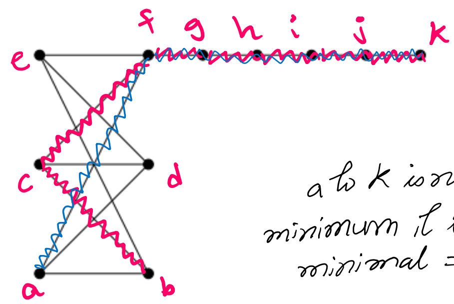
//Lecture 4C

1) **Connected graph :** A graph G is connected iff there is path between every two vertices.
2) **Distance and diameter** :

Length of path : number of edges in the path. *Distance* between two vertices is the length of shortest path between a, b. *Diameter* is the longest shortest distance between two vertices. For example, diameter of Indian is 3214km, it means no distance between two points can exceeds diameter.

This line is longest among all shortest Distance

Here longest shortest distance is between b & K = 7



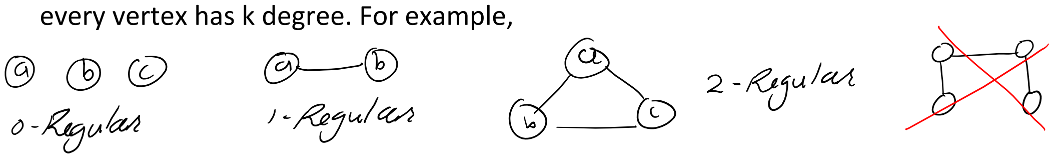
a to k is not minimum it is minimal = 6

Diameter in disconnected graph : ∞

//Lecture 5A

7.1.5) Special type of graphs :

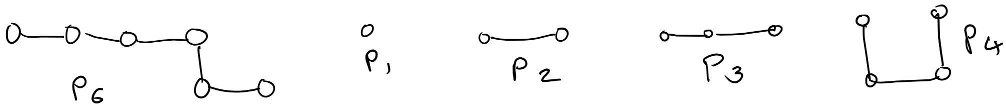
1) **Regular graph** : Every vertex has same degree. A more generalized k-regular graph in which every vertex has k degree. For example,



2) **Complete graph** : A complete graph on n vertices, denoted by K_n, is a simple graph that contains exactly one edge between each pair of distinct vertices. Has $\frac{n(n-1)}{2}$ edges.
3) **Empty/ Null/ Edgeless graph** : Graph without edges. Denoted by E_n.

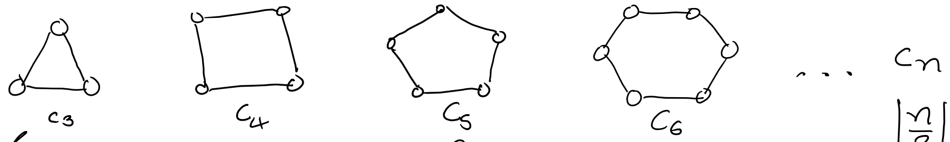
Similarly, we cannot classify graph with no vertices. Every graph should contain at least one vertex.

4) **Path graph** : Denoted by P_n, it is a straight-line graph with n vertices.



//Lecture 5B

5) **Cycle graph** : Denoted by C_n, for n>=3. Every vertex has degree 2 meaning its 2-regular.

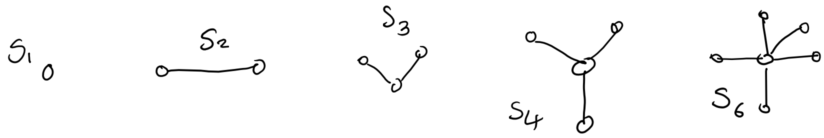


Diameter = 1 2 2 3 $\lfloor \frac{n}{2} \rfloor$

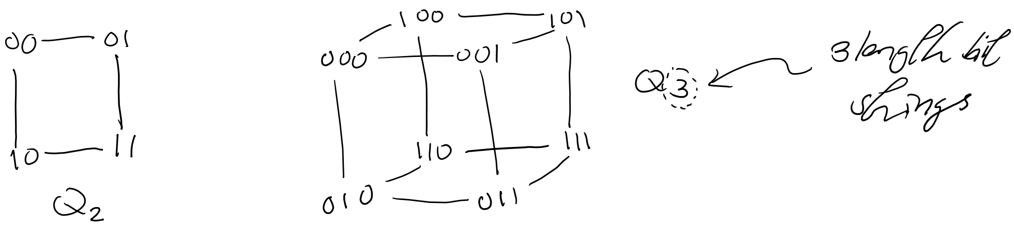
6) **Wheel graph** : If create edges from all vertices and join them then we will have wheel graph.

W3 not W4 because derived from C3

7) **Star Graph** : A special type of graph in which n-1 vertices have degree 1 and a single vertex have degree n – 1. Start graph of order n denoted by Sn



8) **Hypercube graph** : Denoted by Qn, where (u, v) ∈ E iff hamming distance of (u, v) = 1.



It is also called n-cube graph or n-dimensional graph. As you may have noticed…

$|V| = 2^n$, $|E| = n \times 2^{n-1}$, Degree $= n$, Diameter $= n$, T. degree $= n \times 2^n$

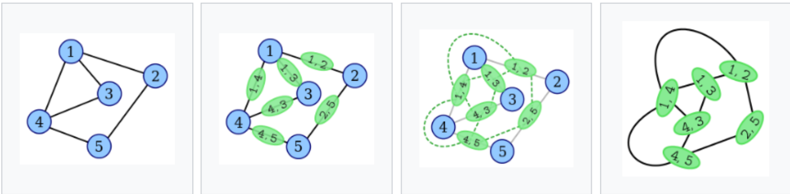
9) **Nullity of graph (N)** : Nullity of graph is the number of closed region so r = e – v + 2 here closed region is r_c = e – v + 1 and r_o = 1. So, by adding we get r = r_c + r_o. So, nullity can be calculated by r_c = e – v + 1.
10) **Line graph** :

The line graph L(G) of a simple graph G is defined as follows :

There is exactly one vertex v(e) in L(G) for each edge e in G.

For any two edges e and e’ in G, L(G) has an edge between v(e) and v(e’), if and only if e and e’ are incident with the same vertex in G.

Conversion of graph to line graph.



Graph G | Vertices in L(G) constructed from edges in G | Added edges in L(G) | The line graph L(G)

In line graph, number of vertices = numver of edges in G and number of edges = sum of square of degree of vertices in G divided by 2 minus number of edges in G.

//Lecture 7

7.2) More graph terminology :

If you delete on edge from a graph only that edge will be deleted. But if you delete a vertex from a graph then all edges incident on that vertex is also gets deleted.

7.2.1) Subgraph :

Graph G $\xrightarrow[\text{Deletion of 0 or more edges OR both}]{\text{Deletion of 0 or more vertices OR}}$ Graph (H) subgraph of G

Definition :

Given two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_3)$, the graph G_1 is said to be

- A ***subgraph*** of $G_2 = (V_2, E_2)$ if $V_1 \subseteq V_2$ and $E_1 \subseteq E_2$, i.e. G_1 can be obtained from G_2 by deleting some vertices and some edges;
- A ***spanning subgraph*** of G_2 if $V_1 = V_2$ and $E_1 \subseteq E_2$. i.e. G_1 can be obtained from G_2 by deleting some edges but not vertices;
- An ***induced subgraph*** of G_2 if G_1 is a subgraph of G_2 and every edge of G_2 with both endpoints in V_1 is also an edge of G_1, i.e. G_1 can be obtained from G_2 by adding some vertices but not edges. Meaning it is opposite of spanning subgraph in which vertex deletion is not allowed and here in induced subgraph edge deletion is not allowed. We say G_1 is induced by G_2.

//Lecture 7

The **union** of two simple graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ is the simple graph with vertex set $V_1 \cup V_2$ and edges set $E_1 \cup E_2$. The union of G_1 and G_2 is denoted by $G_1 \cup G_2$.

//Lecture 8a

7.2.2) Graph Isomorphism :

Graph having abstractly same structure.

Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic iff there exists a bijection between V_1, V_2 which preserves edges.

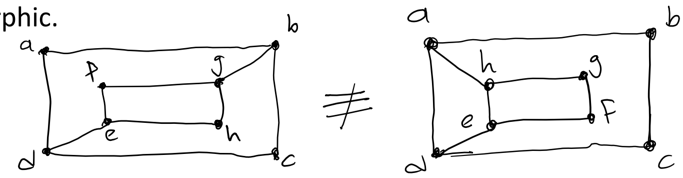
Showing "two graphs are isomorphic" is NP hard problem. But showing "Not isomorphic" can be done using "**Graph Invariant**". Graph invariants are properties which should be same in isomorphic graph.

Graph invariants includes :

1. order of graph should be same
2. size of graph " " "
3. Degree sequences
4. Δ, δ, Diameter
5. Number of 3-length cycles
6. Number of k-length cycles

etc....

There can be many such properties of graph which two graphs must follow in order to have isomorphism. But what if all these 6 properties are satisfy by two graphs then can we say they are isomorphic ? – No. because there can be other property (unknown) for which graph should not be equal that is why it is hard to prove that two graphs are isomorphic but it is easy prove whether two graphs are non-isomorphic.



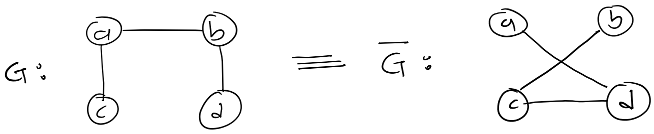
Here all number of vertices are same, edges are same, degree sequence is same, diameter is same. But 4-length cycles are not same (in first 2 cycles, in second 3 cycles).

//Lecture 8d

7.2.3) Complement and self-complementary graph :

We know that every graph on n-vertices is a subgraph of Kn (complete graph). Because Kn work as universal set graph. If G(V,E) then it's complement will be G'(V, E'). Where E' = Edges in Kn – E. we can also say that |E'| = n(n-1)/2 - |E|.

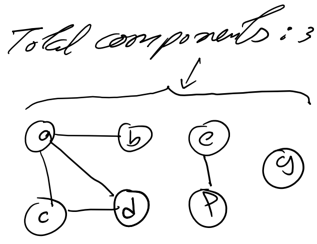
Self-complementary graph : A graph is self-complementary iff graph and its complement is isomorphic. Example,



One interesting fact that every path graph is self-complementary.

//Lecture 9A

1) Connected components :



Component means it is a maximal connected graph. Why not maximum ?

Here you can see maximum connected graph is G({a, b, c, d}, E)

And maximal connected graph is a set of connected components of graph.

Here graph made by a, b, c, d is one component. Similarly, here e is not component rather it is a part of component.

When we say vertices are connected it means there is a path from one vertex to another.

An undirected graph is connected if there is path between every pair of distinct vertices. A connected component of a graph G is a connected subgraph of G that is not contained in any other connected subgraph of G. (that is maximal connected subgraph)

We can say if there is relation R on V such that a R b iff there exists a path between a and b. Then relation is equivalence and number of equivalence class = number of connected components.

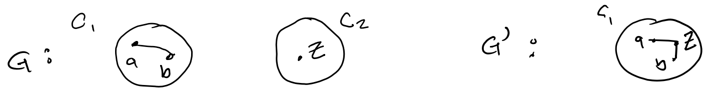
//Lecture 9B

2) Complement of disconnected graph : we know that the complement of connected graph may be connected or disconnected. But complement of disconnected graph implies what ?

Let's take two vertices from G (a disconnected graph) say a, b two things can happen :

Case 1 : a, b are not adjacent means they either belong to different components or connected through some sequence of graph means they are indirectly connected. So, its complement will be G' such that a and b are connected.

Case 2 : a, b are adjacent means they belongs to same component. In complement G' they must be connected.

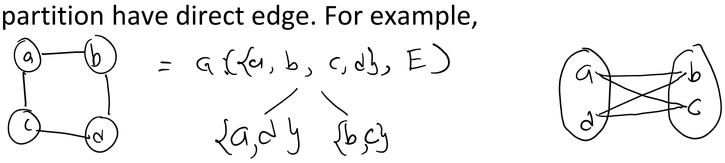


Complement of disconnected graph will always be connected

//Lecture 10A

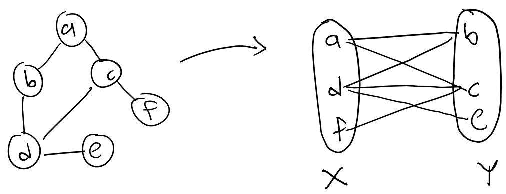
7.2.4) Bipartite graphs :

Bipartite graph is a graph in which you can always make partition of vertices of size 2 such that no two vertices of same partition have direct edge. For example,



More formally, graph G(V, E) is bipartite iff ∃a bipartition X, Y of V such that

- $X \cap Y = \emptyset$
- $\forall_{a,b \in X}\ (a, b) \notin E(G)$
  $\forall_{a,b \in Y}(a, b) \notin E(G)$
- $X \cup Y = V$
- $\boldsymbol{X, Y}$ **can be empty**

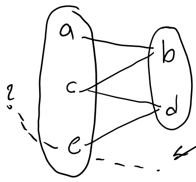


Theorem : ***A graph is bipartite if and only if it doesn't have an odd cycle***.

We will not see proof but little idea is enough,

This theorem also means

If we have odd cycle then graph is not bipartite.



This is not possible else it will not in partition.

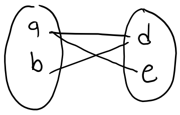
Lemma. *If G is a bipartite graph and the bipartition of G is X and Y, then* $\sum_{v \in X} deg\ (v) = \sum_{v \in y} deg\ (v)$.

Because every edge leaving one partition goes to other partition. So, edge distribution is same.

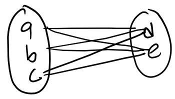
//Lecture 10B

Complete bipartite graph : denoted by $k_{m,n}$

As the name indicate it should be bipartite with all possible edges maintaining bipartite property.



Bipartite but not complete



This is complete Bipartite $K_{3,2}$

For every complete bipartite graph,

|V| = m + n, |E| = mn, *degree sequence* : n, n, n,…, m times , m, m, m, …, n times

Every hypercube graph is bipartite graph

Because we can always divide hypercube graph into even parity and odd parity (parity means no. of 1's) vertices. Meaning no two vertices of same parity is connected.

//Lecture 10c

You may have observed one pattern that when the size of both partitions is nearly same, we get maximum edges. We can say that if a graph on n vertices has edges greater than $\left\lfloor \frac{n^2}{4} \right\rfloor$ then it cannot be bipartite.

//Lecture 11A

7.2.5) Cyclic and Acyclic graph :

There is a difference between cycle graph and **cyclic graph**. *Cycle graph* means all vertices should form one cycle while cyclic graph is a graph containing at least one cycle.

Conversely, a graph with no cycle in it is known as *acyclic graph*.

Definition 2 : there are at least two vertices which have more than one path between them.

Definition 3 : There is some vertex where we can start off, follow a non-empty trail, and come back to the original vertex without repeating edges.

Opposite to this is *acyclic graph* which is also called **forest** when it is *not necessarily connected*. If acyclic graph is connected then it is called **tree**. Components of forest is tree.

1) **Tree :** it is an undirected, acyclic, connected graph.

//Lecture 11C

Number of edges in tree having n vertices is n – 1. Because at start we were having only one vertex and if we add one vertex to this tree, we have to join this vertex through edge. Again, we repeat the

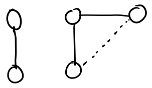
Tree $\underset{\not\longleftarrow}{\longrightarrow}$ |E| = |V| − 1 same procedure. After one vertex we will have equal number of vertex and edges. No. edges will be e + 1 = n ➔ n – 1 edges.

Different definitions of tree :

- T is tree.
- Any two vertices on T are connected by a unique path.
- T is minimally connected, i.e. T is connected but T – e is disconnected for any edge e of T.
- T is maximally acyclic, i.e. T is acyclic but T + uv contains a cycle for any two non-adjacent vertices u, v of T.
- T is connected and |E(T)|=|V(T)|- 1.
- T is acyclic and |E(T)|=|V(T)|- 1.

//Lecture 11E

Q : If G has no cycle but by adding one edge between any two vertices will create a cycle then G is tree ? – Counterexample,

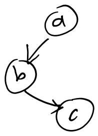


← by adding edge it can create a cycle but it is not tree

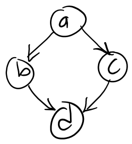
//Lecture 12A

2) Rooted tree : it is a special type of DAGs (directed acyclic graph)

It is a directed acyclic graph with one property that from root to every other node we will have unique path. For example,

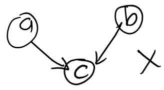


✓



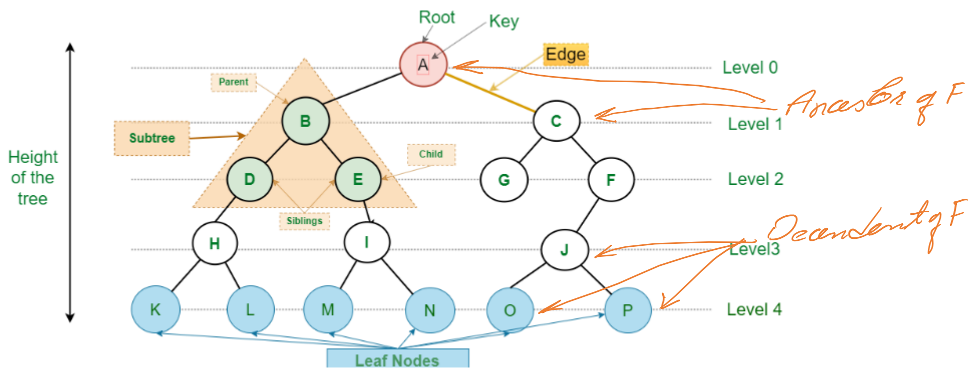
X

It is acyclic but a to d path is not unique



X ← No root present

So, n-ary tree learned in DS is nothing but this rooted tree only but we omit arrow by giving each node level. Therefore, all the terminology remains the same as taught in DS related to rooted tree.



Height of a node in rooted tree : is the number of edges encountered from x to the farthest leaf.

Depth of a node in rooted tree : is the number of edges encountered from root to x.

Tree	Rooted Tree
i) Undirected	i) Directed
Not applicable here ←	Concepts : Root, internal nodes, leaf, height, Depth, Siblings, etc,...

//Lecture 12B

In directed graph we have concept of +ve and -ve degree and rooted tree is also directed graph but it is a special kind of graph which heavily used in many fields so degree in rooted has different analogy.

The **degree of a node** is the number of its children and the **degree of a tree** is the maximum degree of any of its nodes.

3) **Binary tree** : is a rooted binary tree in which every vertex has at most two children.

In binary tree, no. of leaf = (nodes with degree 2 node) + 1.

Proof. We know that Binary tree → rooted tree → directed graph → total indeg = total outdeg = |E|

And |E| = n – 1. Now,

Suppose, L represents no. of leaves, D' represents no. of nodes with degree 1, D'' represents no. of nodes with degree 2.

Total out degree = $L \times 0 + D' \times 1 + D'' \times 2 = D' + 2D'' = n - 1$ but $n = L + D' + D''$ on solving we get $L = D'' + 1$. QED

Full binary tree : is a binary tree with every node either have 0 or 2 children.

In full binary tree we do not have degree 1 node. Therefore, n = L + D'' ➔ n = 2L – 1 using D'' = L – 1

//Lecture 13A

Q : What will be number of maximum and min edges in disconnected graph ? – If we want max |E| then no. of component will be as min as possible. We have two option

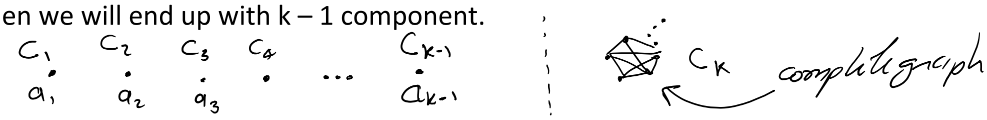
option 1: First component contains n-1 vertices & second contains 1 vertex
In this case no. of maximum edges will be $(n-1)(n-2)/2$
option 2: Both component contains $n/2$ vertices, In that case no. of maximum edges will be $n(n-2)/4$
clearly option 1 edges > option 2 edges $\therefore$ max $|E| = \frac{(n-1)(n-2)}{2}$

For min |E|, all component will contain only one vertex in that case edges will be 0.

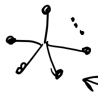
Q : The maximum number of possible edges in an undirected graph with n vertices and k components is – This can be achieved by distributing k-1 vertices from n and remaining n-k+1 vertices in one component. As maximum edges are asked so total C(n-k+1,2) are possible.

tree with n-k+1 vertices → $\boxed{n-k} < no. edges < C(n-k+1, 2)$ ← complete graph with n-k+1 vertices

Q : Let G be an arbitrary graph with n nodes and k components. If a vertex is removed from G, the number of components in the resultant graph must necessarily lie down between ? – Here we want limit, so minimum number of components will be when (k-1) components will have 1 node and 1 component have n-k+1 nodes and forming complete graph with those nodes. If we remove one of the (k-1) components then we will end up with k – 1 component.



For, maximum number of components we distribute (k-1) nodes per components and from n-k+1 nodes we will form

c_1 c_2 c_3 c_4 ... c_{k-1}  c_k star graph

a_1 a_2 a_3 c_4 ... c_{k-1}

$\Rightarrow \boxed{k-1 < x < n-1}$

Counting no. of n-length cycle :

EXAMPLE 15 How many paths of length four are there from a to d in the simple graph G in Figure 8?

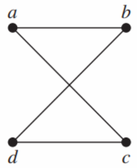
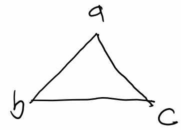


FIGURE 8 **The graph G.**

Solution: The adjacency matrix of G (ordering the vertices as a, b, c, d) is

$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}.$$

overcounting



abc
bac → abc
cba

Hence, the number of paths of length four from a to d is the (1, 4)th entry of $\mathbf{A}^4$. Because

$$\mathbf{A}^4 = \begin{bmatrix} 8 & 0 & 0 & 8 \\ 0 & 8 & 8 & 0 \\ 0 & 8 & 8 & 0 \\ 8 & 0 & 0 & 8 \end{bmatrix},$$

Extra Examples

there are exactly eight paths of length four from a to d. By inspection of the graph, we see that a, b, a, b, d; a, b, a, c, d; a, b, d, b, d; a, b, d, c, d; a, c, a, b, d; a, c, a, c, d; a, c, d, b, d; and a, c, d, c, d are the eight paths of length four from a to d.

Total no. n-length cycle = traceof(A^n) but we are overcounting some cycle. For example, we are counting same cycle in clockwise and anticlockwise direction. And we divide by 2n (why?)

$$\textbf{Total no. n-length cycle} = \frac{traceof(A^n)}{2n}$$

//Lecture 14A

7.3) Connectivity and Coloring :

To properly understand connectivity, we first have to explore few mis-conceptual terms…

Maximal Vs Maximum : *A set is maximal with respect to some property P if nothing new can be added to S keeping the property P preserve*. For example, Let's say we have set S = {1, 2, 3, 4, 5} and we have property P : "No two elements consecutive".

{1, 2} ← Not satisfying P so not mal & mum   {1, 3} ← following P but not maximal

{2, 4} ← following P & maximal   {1, 3, 5} ← following P & maximal

{2, 4} and {1, 3, 5} are possible maximal set which satisfy P but {1, 3, 5} is the maximum set.

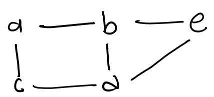
Maximal means no new addition is possible and maximum is the maximum amongst maximal.

7.3.1) Clique, Independent set :

Clique : In a graph, a set of pairwise adjacent vertices is called a clique.

Independent set : A set of pairwise non-adjacent vertices is called an independent set.

For example,



clique : {a, b} ✓ {b, e, d} ✓ {a, d, e} ✗

Ind. set : {a, e} ✓ {a} ✓ {a, d, c} ✗

The size of a maximum clique in G is called the **clique number** of G and is denoted by $\omega(G)$. We can say it is also equal to size of maximum complete subgraph formed in G.

The size of a maximum independent set in G is called the **independent number** (also known as stability number) of g and is denoted by $\alpha(G)$.

For example, for cycle graph Cn : Clique number $\omega(C_n)$ = 2 as at max only two vertices are adjacent. And Stability or independent number $\alpha(C_n) = \left\lfloor \frac{n}{2} \right\rfloor$ as for 5 we have 2 and 6 we have 3.

For hypercube graph, clique number $\omega(Q_n) = 2$ (from observation) and stability number $\alpha(Q_n) = 2^{n-1}$. Because there are total 2^n vertices in Q_n graph and as hypercube graph is bipartite, we can always have partition each partition contains 2^{n-1} vertices (even and odd parity).

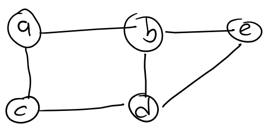
But why we are learning this clique number and independent number together. Because

S is maximum ind. Set in G ↔ S is maximum clique in G'

//Lecture 15A

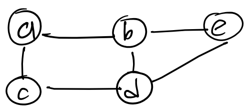
7.3.2) Vertex cover, edge cover :

Vertex cover : set of Vertices which covers all edges.



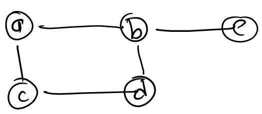
vertex	Edges covered
a	ab, ac
b	ab, be, bd
c	ca, cd
d	cd, bd, de
e	be, de

Edge cover : Edges covering all vertices.



edges	vertex covered
ab	a, b
cd	c, d

Now, interesting problem to ask is minimum vertex cover and edge cover.

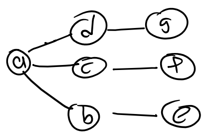


minimum VC = { b, c }
minimum edge cover = { be, ac, cd }

Consider a graph with one isolated vertex then edge cover will be "does not exists" because there are no edges which covers isolated vertex. So, edge cover exists iff no isolated vertex. We can say that **Edge cover exists iff $\delta > 0$ (δ means minimum degree of a node in graph)**

Size of minimum vertex cover is called vertex covering number (β) and size of minimum edge cover is called edge covering number (β').

Q : The maximum degree vertex must be in minimum VC ? – Answer is no, here's the counter,



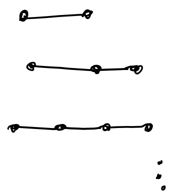
mvc = { b, c, d }
a is maximum degree vertex but not in mvc

//Lecture 15B

Minimum edge cover in any graph is at least $\left\lceil \frac{n}{2} \right\rceil$ because one edge covers 2 vertices at max so to cover n vertices, we should have at least n/2 edges in edge cover.

For example, for P_n graph,

for $n \geq 2$ because if $n=1$ then β' does not defined



	β	β'
	1	1
	1	2
	2	2
	⋮	

$\rightarrow \quad \left\lfloor \frac{n}{2} \right\rfloor \quad \left\lceil \frac{n}{2} \right\rceil$

Relation between vertex cover and independent set :

Let graph $G(V, E)$ have vertex cover S then (V – S) is independent set

Above statement is true because in independent set, we have those vertices which are in between two vertices so edges connected with them is counted in vertices in S And by that logic we can also say that

Let graph $G(V, E)$ have independent set I then (V – I) is vertex cover

maximum independent set → $\boldsymbol{\alpha + \beta = n}$ ← no. of vertices in graph

minimum vertex cover

//Lecture 16A

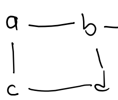
7.3.3) Matching :

Matching == edge independent set

Edge independent set means no two edge should have common vertex we call non-adjacent edges.

Definition : A set of pairwise non-adjacent edges in a graph is called a matching. The maximum number of edges in a matching in a graph G is called the **matching number of G** and denoted by $\mu(G)$ or $\alpha'(G)$.

G:



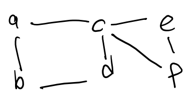
$\mu(G) = 2$

matching: {ab} ✓ {ab, cd} ✓ ← largest matching

{ab, bc} ✗ {ad, be} ✗ ← not edge

vertex	edges
vertex cover (β) ⟷	edge cover (β')
Independent set ⟷	Matching
↓	↓
vertex Ind. set (α)	edge Ind. set (α')

Perfect matching : Matching which covers all vertices.



matching : {ab} ✓ {ab, cd, ef} ✓ → PM (because it covers all vertices)

{ab, ef} ✓

{cd} ✓

You can see that any matching covers even number of vertices because every edge consists of two vertices.

NOTE : With complete graph with 2n vertices have (2n-1)!! Perfect matching.

Q : for every graph, $\mu(G) \leq \left\lfloor \frac{n}{2} \right\rfloor$? – True because every edge in matching consists of two vertices. At max we can connect all pairs of vertices by edge (considering only non-adjacent edges as definition says).

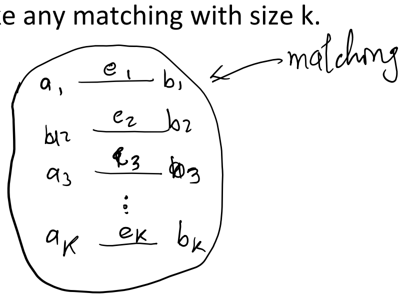
//Lecture 16B

Relationship between matching and vertex cover :

$$|matching| \leq |Vertex\ Cover|$$

Meaning the cardinality of <u>any matching</u> is less than or equal to the cardinality of <u>any vertex cover</u>.

Proof. Take any matching with size k.



should covers all edges

vertex cover = $\{a_1/b_1, a_2/b_2, a_3/b_3, \ldots\}$

for e_1 for e_2 for e_3

As you can see to cover e1 edge any vertices from a1 and b1 should be there in vertex cover. And similarly, for other we can say that at least we want k vertices in vertex cover to cover all edges. *QED*

NOTE :

1) **If S is <u>maximum matching</u> then <u>every edge of the graph</u> is incident on <u>some vertex</u> covered by S. This means vertices covered by S will cover all edges (why ?) which is the definition of vertex cover so vertices in S (maximum matching) is actually a vertex cover (it can be minimum or maximum vertex cover we don't know). Therefore, |Vertex Cover| = $2|\mu|$. Now, if vertex cover is minimum then $\beta(G) \leq 2\mu(G)$. QED**

So, we can say that for every graph $\mu \leq \beta \leq 2\mu$ (here second μ is maximum matching)

We have seen that $\alpha + \beta = n$ similarly, $\boldsymbol{\alpha' + \beta' = n}$

Summery,

$\alpha + \beta = n$	$\alpha' + \beta' = n$	$\beta' \geq \lceil n/2 \rceil$
$\mu \leq \beta \leq 2\mu$	$\alpha' = \mu \leq \lfloor n/2 \rfloor$	$\alpha \leq \beta'$
Bipartite $\rightarrow (\mu = \beta)$		

//Lecture 17A

7.3.4) Graph coloring :

1) Vertex coloring :

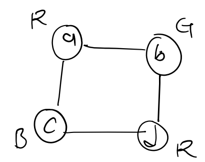
Graph coloring == vertex coloring.

A graph coloring is an assignment of labels, called colors, to the vertices of a graph such that **no two adjacent vertices share the same color**.

Proper coloring : every pair of adjacent vertices must get different color/label.

K – colorable : Using at most k colors, we can color.

For example,

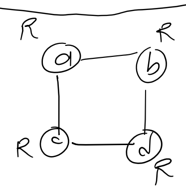


4-colorable ? ✓ ← Trivial coloring

3-colorable ? ✓

2-colorable ? ✓

1-colorable ? ✗



→ Not a proper colouring

Minimum number of colors needed is 2 ← this is called **chromatic number** denoted by $\chi(G) = 2$.

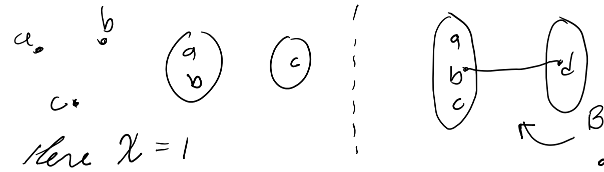
For K_n, $\chi(K_n) = n$

For E_n (Edgeless), $\chi(E_n) = 1$

For P_n (Path graph), $\chi(P_n) = 2$

For C_n, if n is even then $\chi(C_n) = 2$ otherwise $\chi(C_n) = 3$

For Bipartite graph (Iff no odd cycle)



$\therefore \chi(\text{Bipartite}) \le 2$

Similarly, we know that Q_n is bipartite graph, $\therefore \chi = \begin{cases} 2 & n \ge 1 \\ 1 & n = 0 \end{cases}$

//Lecture 17B

Greedy algorithm for vertex coloring : It does not always succeed in finding the minimum.

Let N = {1, 2, 3, ..} denote the set of all possible colors. Then greedy strategy will be

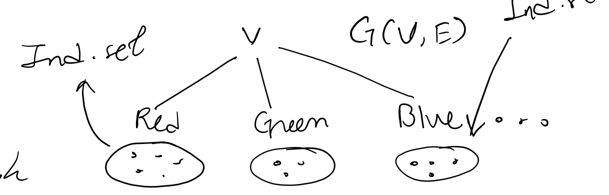
$$\boldsymbol{color(V_i) = \min \{j \in N : No\ neighbour\ of\ V_i\ is\ colored\ j\}}$$

Note that if maximum degree of graph i.e. $\Delta(G) = d$ then $\chi(G) \le d + 1$.

Example, Cn with n = odd. Here d = 2 and $\chi(C_{odd}) = 3$ clearly following above equation. And second example would be kn where d = n – 1 and $\chi(k_n) = n$. And third example is ? Nothing ! because these are only two graphs that satisfy $\chi(G) = d + 1$.

This is called **brooks' theorem**, it says "all connected graph have $\chi(G) \le \Delta(G)$, except for k_n and odd cycles."

"colour" classes :



If G has $\chi = m$ then

$|E| \ge {}^mC_2$ ← from complete graph

$\alpha \ge \frac{n}{\chi}$ ← Avg size of colour class (which is ind set but not confirm whether it is maximum)

Intuition behind above formula : If we can color a graph using k colors then it means every set of k vertices are dependent (or adjacent) to each other so total size of independent set will be at least n/k.

$$\boldsymbol{\Delta(G) + 1 \geq \chi(G) \geq \omega(G)}$$

//Lecture 17E

2) Edge coloring :

No two adjacent vertices share same color. It is denoted by $\chi'(G)$. It is the smallest edge coloring possible also known as **edge chromatic number** or **chromatic index**.

We can definitely say that $\chi'(G) \geq \Delta(G)$.

Vizing's theorem for edge coloring : it says $\chi'(G) = \Delta \; or \; \Delta + 1$

Konig's edge coloring theorem : for any bipartite graph, $\chi'(G) = \Delta(G)$

//Lecture 18

7.3.5) Graph realization problem :

Graph realization problem means we look at the list of degrees to get some information on the graph. We also look at what list of nonnegative integers can be the degree sequence of some graph.

For example, given degree sequence for some graph : 4, 3, 2, 2 can this be complete ? – answer is no because every complete graph has vertex degree = n – 1. Where n is no. of vertices.

This is called Graph Realization condition for K_n

For pseudo-graph, the nonnegative integers are the degree sequence of some graph if and only if their sum is even. This is true because one edge contributes 2 to degree.

Graphic sequence : is a list of nonnegative integers that is the degree sequence of some simple graph. A simple graph with degree sequence d realizes d.

Havel Hakimi theorem : *The nonincreasing sequence of nonnegative integers d1, d2, …, dn can be realized by simple graph, if and only if $d_1 \leq n - 1$ and the sequence*

$$d_2 - 1, d_3 - 1, \ldots, d_{d_1+1} - 1, d_{d_1+2}, d_{d_1+3}, \ldots, d_n$$

Can be realized by simple graph (after reordering the sequence in nonincreasing order).

example,

If 8 was there then invalid sequence

$$\begin{array}{rcl} s & : & 5,4,3,2,2,2,2,2 \\ delete & : & 3,2,1,1,1,2,2 \\ reorder & : & 3,2,2,2,1,1,1 \\ delete & : & 1,1,1,1,1,1 \\ delete & : & 0,1,1,1,1 \\ reorder & : & 1,1,1,1,0 \\ delete & : & 0,1,1,0 \\ reorder & : & 1,1,0,0 \\ delete & : & 0,0,0 \end{array}$$

For tree we can have condition for graph realization, **for n ≥ 2, the nonincreasing sequence $d_1, \dots, d_n$ of nonnegative integers can be realized by tree if and only if $\sum_{i=1}^{n} d_i = 2(n-1)$ holds and $d_i > 0$ for all i.**

As tree is always connected

//Lecture 19A

7.4) More on connectivity :

7.4.1) Cut vertex, cut edge :

Cut vertex = articulation point = removal of vertex creates more components of graph.

Cut edge = bridge = Removal of edge creates more components of graph.

In any graph there are two types of edge : 1) cycle edges : part of some cycle, 2) Non-cycle edges : not part of any cycle.

cycle edges : Not bridge

Non-cycle edges : Bridge or cut edges

All non-cycle edges are cut edges or bridges

Let G be a graph containing a bridge e incident with vertex v then vertex v is cut vertex if and only if deg v >= 2.

//Lecture 19B

7.4.2) Connectivity number, vertex cut, edge cut :

Previously we saw that cut vertex is the vertex whose removal increases the number of components. But **vertex cut** is a set of vertices whose removal increases the number of components.

Similarly, edge cut is a set whose removal increases the number of components.

But there is slight difference that vertex cut and edge cut only define for connected graph unlike cut vertex and bridge which is defined for all graph (connected and disconnected).

So, here we can say that Vertex cut is a set of vertices whose removal disconnects the graph. And similarly, for edge cut.

But we are not interested in vertex cut, we are interested in smallest vertex cut. Denoted by $\kappa(G)$

This number expresses how difficult it is to disconnect the graph by removing vertex.

For tree : $K(G) = 1$ & For Complete graph K_n : $\boxed{K(K_n) = n-1}$

Therefore, we modify our definition : **In a connected graph, a vertex cut is a subset of vertices whose removal either disconnects graph OR single vertex remains**.

For disconnected graph $\kappa(G) = 0$.

	cut vertex	Vs.	Vertex cut
K_2 : a — b	NONE		{b}

k-connected graph : $\kappa(G) \geq k$ here k is variable. **OR** removal of any $\leq$ k – 1 vertices doesn't disconnect the graph or leaves a single vertex.

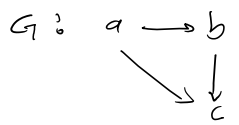
//lecture 20A

7.4.3) Strongly and weakly connected components :

A directed graph G = (V, E) is **singly connected** if $u \rightarrow v$ implies that G contains at most one simple path from u to v from all vertices $u, v \in V$.

We saw concept of components for undirected graph but for directed graph we have strongly and weakly connected components concept.

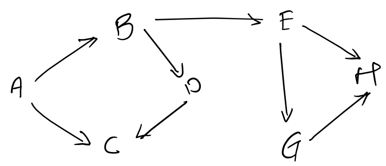
Q : is this graph connected ? -



Not connected!
because no path from c to a

But for directed we do not use connected terminology we say it is not strongly connected.

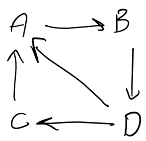
Strongly connected : In a directed graph G = (V, E), two nodes u and v are strongly connected if and only if there is a path from u to v and a path from v to u. (below is wrongly marked just to test)



strongly connected vertices :
A, B ✓ (look carefully)
A, F ✗ ; B, D ✓ ; G, H ✗ ; E, H ✗

In directed graph G(V, E) relation R on V, aRb iff a, b are (strongly) connected is equivalence relation

For example,
$[A]_R = \{A, B, C, D\}$
only one equi. class



{A, B, C, D} This represents strongly connected components

Every equivalence class of "Strongly connected relation R" is called strongly connected component

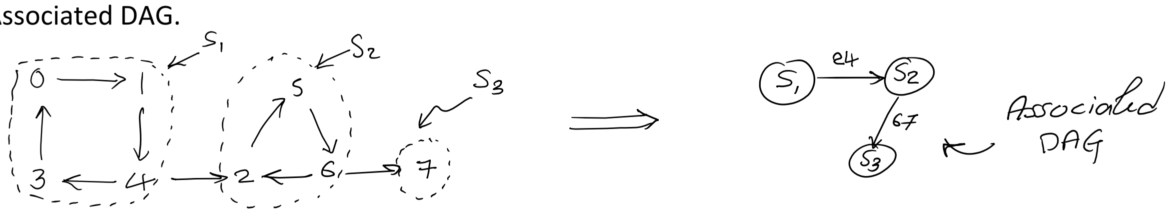
//Lecture 20B

A directed graph is **weakly connected** if there is a path between every two vertices in the underlying undirected graph, *which is the undirected graph S obtained by ignoring the directions of the edges of the directed graph*.

That means **every strongly connected graph is weakly connected graph**.

//Lecture 20C

Associated DAG : In directed graph G(V, E), if we shrink each of these strongly connected components down to a single node, and draw an edge between two of them if there is an edge from some node in the first to some node in the second, we call this new graph as associated directed acyclic graph i.e. Associated DAG.



//Lecture 21A

7.5) Euler and Hamiltonian graph :

A few centuries ago, people were trying to solve a problem that today is called the seven bridges of Konigsberg. Inspired by a real place and situation :

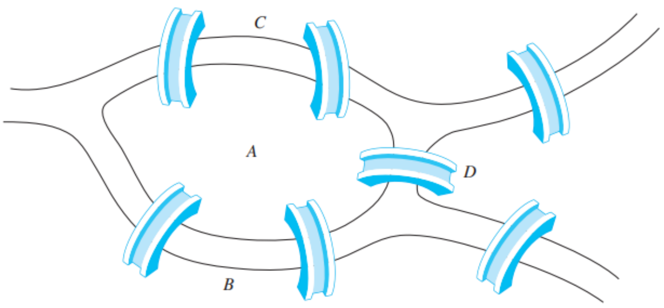


FIGURE 1 The seven bridges of Königsberg.

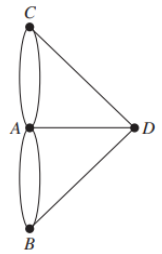


FIGURE 2 Multigraph model of the town of Königsberg.

Problem statement : Is it possible to start at some location in the town, travel across all the bridges once without crossing any bridge twice, and return to the starting point.

Later Euler solved this problem.

7.5.1) Euler path and circuit :

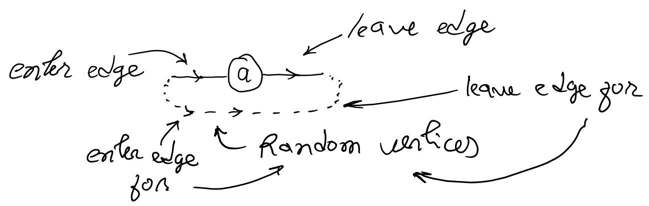
Definition : A **Euler circuit** in a graph G is a simple circuit containing every edge of G. A **Euler path** in G is a simple path containing every edge of G.

Euler graph : A connected graph with Euler circuit. Which means A connected graph is Euler graph if and only if Euler circuit exists.

We know that cycle and circuits is not same but Euler circuit = Euler cycle.

Q : Which graph is Eulerian ? – Connected graph with even degree vertices.

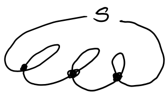
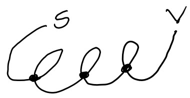
Proof. first note that an Euler circuit begins with a vertex a and continues with an edge incident with a, say {a, b}. The edge {a, b} contributes one to deg(a). Each time the circuit passes through a vertex it contributes two to the vertex's degree, because the circuit enters via an edge incident with this vertex and leaves via another such edge. Finally, the circuit terminates where it started, contributing one to deg(a). Therefore, deg(a) must be even, because the circuit contributes one when it begins, one when it ends, and two every time it passes through a (if it ever does).



A vertex other than a has even degree because the circuit contributes two to its degree each time it passes through the vertex. We conclude that if a connected graph has an Euler circuit, then every vertex must have even degree.

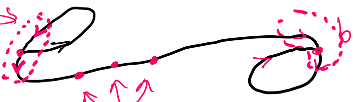
Euler path : An open trail which goes through every edge exactly once.

starting ≠ ending

Euler Circuit	Euler Path
Closed trail 	Open trail 
But both should cover Every edge exactly once	

Theorem : A connected multigraph has an Euler path but not an Euler circuit if and only if it has exactly two vertices of odd degree.

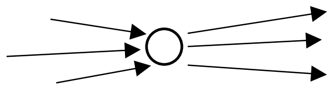
Proof. First, suppose that a connected multigraph does have an Euler path from a to b, but not an Euler circuit. The first edge of the path contributes one to the degree of a. A contribution of two to the degree of a is made every time the path passes through a. The last edge in the path contributes one to the degree of b. Every time the path goes through b there is a contribution of two to its degree.



Consequently, both a and b have odd degree. Every other vertex has even degree, because the path contributes two to the degree of a vertex whenever it passes through it.

Back to Euler graph,

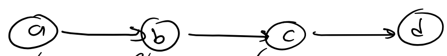
In the undirected case, we wanted an even degree at each node so that we could leave any node we enter. So, with the same logic in directed case, we accomplish this by requiring each node's indegree to equal its outdegree.



Theorem : A directed graph G is Eulerian if and only if it is strongly connected and every node's indegree equals its outdegree.

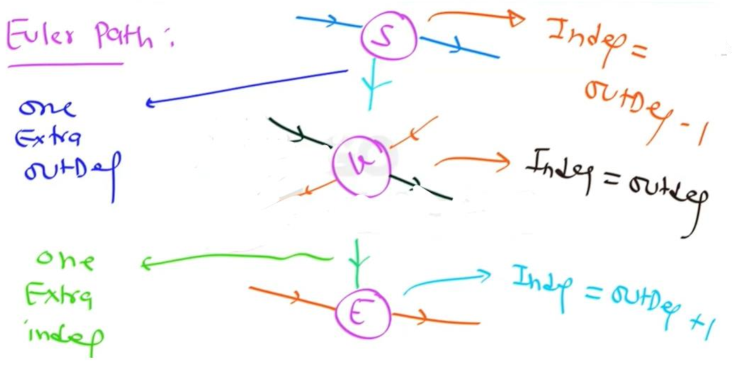
Talking about Euler path in directed. So, we don't need strongly connected condition here because

Not strongly connected but still euler path exist.



But one thing you may have noticed that one vertex has indegree = outdegree + 1 and other have indegree = outdegree – 1 and rest all other vertices have indegree = outdegree.

Thus, we say *A directed graph has Eulerian path if and only if it is weakly connected and one vertex should have indegree = outdegree – 1; one vertex should have indegree = outdegree + 1 and rest all the vertices must have indegree = outdegree*.



//Lecture 21B

7.5.2) Hamiltonian Graph :

Euler cycle === visit every edge exactly once

Euler
Edge

Hamiltonian cycle === visit every vertex exactly once

Hamiltonian graph : G is HG if and only if there exists **Hamiltonian cycle** (cycle which covers every vertex exactly once).

Similarly, **Hamiltonian path** is path made by visiting every vertex exactly once and starting ≠ ending.

For connected graph,	**Euler Circuit/ Euler Cycle**	**Hamiltonian Cycle/circuit**
Can vertex repeat	✅	❌
Can edge repeat	❌	❌

If vertex does not repeat then edge cannot repeat.

For connected graph,	**Euler circuit/ Euler cycle**	**Hamiltonian cycle/Circuit**
Can a vertex remain untouched	❌	❌
Can an edge remain untouched	❌	✅

Similar to Euler circuit is same as Euler cycle, Hamiltonian cycle is same as Hamiltonian circuit.

But only circuit is not same as cycle.

Sadly, there is no efficient method to determine Hamiltonian cycle unlike Euler cycle.

Stupid facts which are true :

- If Hamiltonian cycle exists then Hamiltonian path exists but inverse is not true.
- If Euler circuit exists then Euler path cannot exist because for Euler path to exists G (|V|>2) must have 2 odd deg. Vertices.

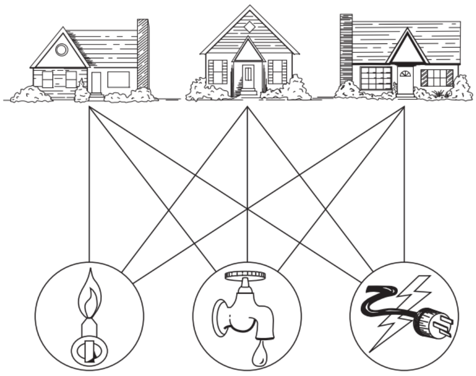
Dirac theorem : If min degree of any vertices in any simple connected undirected graph is greater than or equal to n/2 then Hamiltonian cycle exists provided |V|>=3.

//from Kenath Rozen

7.6) Planar graphs :

In this section we will study the question of whether a graph can be drawn in the plane without edges crossing. In particular, we will answer the houses-and-utilities problem.

Is it possible to join these houses and utilities so that none of the connections cross?

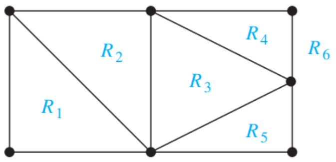


Definition : A graph is called **planar** if it can be drawn in the plane without any edges crossing (where a crossing of edges is the intersection of the lines or arcs representing them at a point other than their common endpoint). Such a drawing is called a **planar representation** of the graph.

Q : is $K_{3,3}$ is planar graph ? – No, you can flip the V1, V4 to reduce the cross edges and then you can flip v3 and v6 but that will cause previous cross edges.

7.6.1) Euler formula :

A planar representation of a graph splits the plane into **regions**, including an unbounded region. For instance, the planar representation of the graph shown in Figure splits the plane into six regions.



Statement : Let G be a connected planar simple graph with e edges and v vertices. Let r be the number of regions in a planar representation of G. Then **r = e − v + 2**.

You can easily prove this result using induction.

Degree of a region, which is defined to be the number of edges on the boundary of this region. When an edge occurs twice on the boundary (so that it is traced out twice when the boundary is traced out), it contributes two to the degree. We denote the degree of a region R by deg(R).

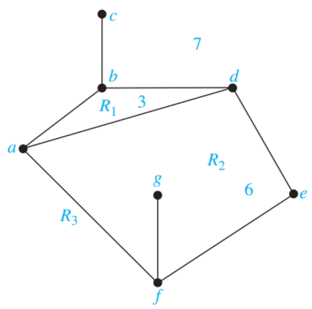


FIGURE 11 The degrees of regions.

Corollary 1 : *If G is a connected planar simple graph with e edges and v vertices, where v ≥ 3, then e ≤ 3v − 6.*

Proof. One thing to note that the degree of each region is at least three (for a graph with vertices at least 3).

$$\therefore \boldsymbol{2e} = \sum_{\boldsymbol{all\ regions\ R}} \mathbf{deg}\ (\boldsymbol{R}) \geq \boldsymbol{3r}$$... why 3r because 3x1 + 3x1 + ... r times

Hence, $\left(\frac{2}{3}\right) e \geq r$ and now using Euler's formula, we obtain

$e - v + 2 \leq \left(\frac{2}{3}\right) e \Rightarrow e \leq 3v - 6.$

Corollary 2 : *If G is a connected planar simple graph, then G has a vertex of degree not exceeding five.*

Proof. If G has one or two vertices, the result is true. If G has at least three vertices from above corollary we know that $e \leq 3v - 6$. Now, what if the degree of every vertex were at least six, then because $2e$ will be sum of all deg(v), we would have $2e \geq 6v$. But this contradicts $e \leq 3v - 6$. It follows that there must be a vertex with degree no greater than five.

Example, K_5 is nonplanar using corollary 1 because the graph of K_5 has five vertices and 10 edges. However, the inequality $e \leq 3v - 6$ is not satisfied for this graph. Therefore, K_5 is not planar.

Corollary 3 : *If a connected planar simple graph has 3 edges and v vertices with v ≤ 3 and no circuits of length three, then $e \leq 2v - 4$.*

The proof of this corollary is same as corollary 1 except that in this case the fact that there are no circuits of length three implies that the degrees of a region must be at least four.

NOTE : here u can also find average degree. Consider $2e \leq 6v - 12$. 2e means sum of degree and if u divide it by v i.e. total number of vertices then u will get 6 – 12/v, this is at most degree of vertices.

7.6.2) Kuratowski's Theorem :

We saw that K3,3 and K5 are not planar. Clearly, a graph is not planar is it contains either of these two graphs as subgraph.

If a graph is planar, so will be any graph obtained by removing an edge {u, v} and adding a new vertex w together with edges {u, w} and {w, v}. Such an operation is called an **elementary subdivision**. The graph $G_1 = (V_1, E_1)$ and $G_2(V_2, E_2)$ are called **Homeomorphic** if they can be obtained from the same graph by a sequence of elementary subdivisions.

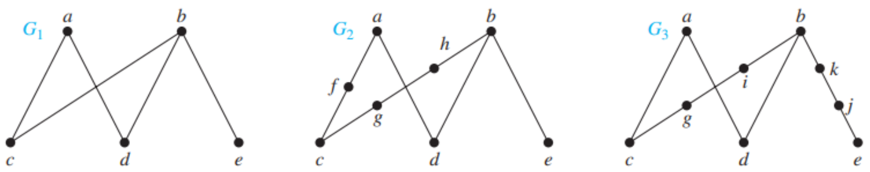


FIGURE 12 **Homeomorphic graphs.**

Theorem : *A graph is nonplanar if and only if contains a subgraph homeomorphic to $K_{3,3}$ or K_5.*

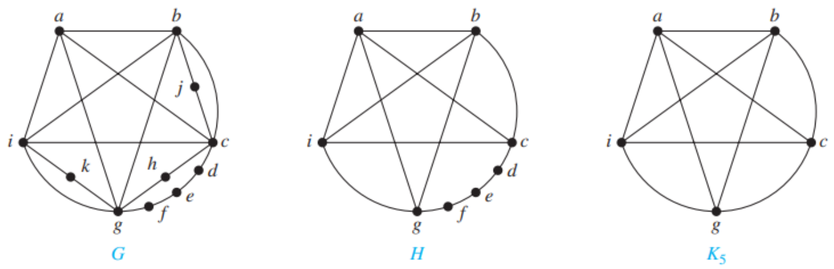


FIGURE 13 The undirected graph G, a subgraph H homeomorphic to K_5, and K_5.

//Lecture 23A

7.7) POWERS OF ADJACENCY MATRIX OF A GRAPH :

Q : Find the number of walks of length 3 from vertex a to vertex a in the following undirected graph ?

-

a — b, a — c   0 walks of length 3

a — b, a — c, b — c (loop at a)   7 walks

a — a — b — a } same for c
a — b — a — a
a — a — a — a
a — b — c — a } ← 2 combi

If we convert undirected graph G to a new graph G' by putting self-loops on all vertices then If there is a walk of length 1 to n – 1 in G between any two vertices then there is walk of length **exactly** n – 1 in G'.

G : a — b — c — d   G' : a — b — c — d (self-loops on all vertices)

a — b – c ⇐ length 2 walk
only possible between a to c but here →
a → a — b — c
a — b — b — c } ← length 3 walk

7.7.1) Power of adjacency matrix of a graph :

Adjacency matrix of a graph will give u walk of length 1.

Let M represents adjacency matrix of a graph G. Thus, M^2 gives you <u>no. of walks of length 2</u> between every pair of vertices.

Every i, j in M^n gives the number of walks from i to j of length n

⇨ ***Find degree of every vertex*** :

Idea 1 : v [row] → # 1's is the degree of v

Idea 2 : In M^2, the main diagonal is degree of all vertices.

$M^2 =$ (row a, column a) ← neighbors of a = degree of a

G : a — b   ↖ a — b — a

simple undirected only ⟶
$$trace(M^2) = \sum_{v \in V} \deg(v) = 2|E|$$

NOTE : If n is the smallest nonnegative integer, such that for some i, j the element (i, j) of A^n is positive, then n is the distance between vertex i and vertex j.

//Lecture 24B

7.7.2) More application of powers of adjacency matrix of a graph :

1) Undirected graph is connected or not :

Method 1 : $M^1 + M^2 + \cdots + M^{n-1}$ where n is no. of vertices >= 3.

All entry non-zero $\Longleftrightarrow$ connected

This method is nothing but finding walks of length 1 to n-1 between every pair of vertices.

Method 2 : put all self loops and then find walks of length n – 1 between every pair of vertices.

G is connected if and only if the matrix $(I_n + A)^{n-1}$ has no 0's

2) Directed graph is connected (strongly off course) or not :

Method 1 : $M^1 + M^2 + \cdots + M^{n-1} + M^n$ where n is no. of vertices >= 3

All entry non-zero $\Longleftrightarrow$ connected

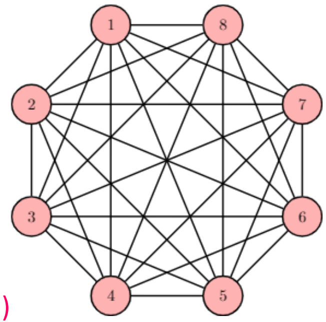
G (Directed) is connected if and only if the matrix $(I_n + A)^n$ has no 0's

3) Finding number of 3 – length cycles :

Directed simple graph with no self-loops # $\mathbf{3 - \textit{length cycles}} = \frac{Trace(M^3)}{3}$.

4) Finding transitive closure of a relation :

Silly mistakes :

1) 

In this problem you have to find number of Hamiltonian cycles. You answered 8! But you have overcounted some cases like clockwise and anticlockwise cycle then cycle forming same sequences for example, 12345678 and 23456781… such 7 sequences should be mapped to 1. So, final answer should be 8!/(2x7).

2)The maximum number of edges in a bipartite graph with 19 vertices is _________. – this is one of the simplest answers is 90 but you have selected 90/2 because you thought 10x9 would count some edges twice but logic is there are one set containing 10 and other containing 9 so for each 10 vertices you have 9 possible edges.