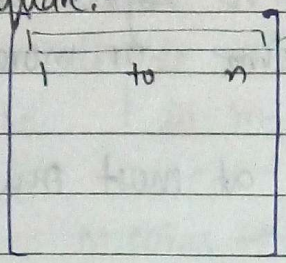
Orion
PAGE:
DATE: 17/10/16

PIGEONHOLE PRINCIPLE (PP)

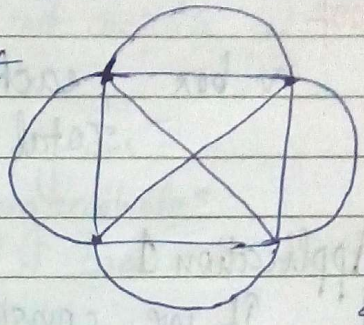
COMBINATORICS

* Magic Square:-



→ Sum upto n^2

(eg Sudoku)

* 

Trace all curves without removing pen from ppr & without repeating.

Combinatorics is concerned with the arrangement of objects in a set satisfying some rules.

1. Existence of arrangement : if it exists?
2. Enumeration or characterization } if at all possible
   - ↳ if possible, count no. of arrangement
     - ↳ diff types / no. of types.
3. * Analysis — Minimise run-time & storage.
4. * Optimization

Combinatorics is concerned with the existence, enumeration, analysis and optimization of arrangement of discrete structures. (finite)

A lot of pigeons fly to not too many pigeonhole then every pigeonhole occupy at least one pigeon.

⇒ Some pigeonhole ↑ two or more pigeons.
will surely contain

Orion
PAGE:
DATE: / /

P.P. Simple Form

Theorem

If $(n+1)$ objects are put in n boxes then at least one box contains two or more objects.

Proof

n box ; each box contains at most one object.
Total n objects.

Application 1

If we consider 13 people then at least two people have birthdays in the same month.

$(n+1)$ nodes, n colors.

Application 2

We consider n no. of couples. Given $2n$ people how many people to be selected so that we get one couple.
↳ $n+1$

$f : X \to Y$

- If X has more no. of elements than Y, then f is not one-to-one.
- If X & Y both have same no. of elements & f is one-to-one then f is onto.
- If ——— onto
  then f is one-to-one.

Application 3

Given m integers $a_1, a_2, \ldots, a_m$ there exist integer k and l with $0 \le k < l \le m$ such that $a_{k+1} + a_{k+2} + \ldots + a_l$ is divisible by m.

Orion
PAGE:
DATE: / /

Consider the following m sums.

a_1, a_1+a_2, $a_1+a_2+a_3$, ..., $a_1+a_2+\dots+a_m$

If we divide each sum by m, then the remainder will be 1 to $m-1$ (we will not consider 0)

m sums → m no. of pigeons
$m-1$ remainders → $(m-1)$ pigeonholes
⇒ Two sums must have same remainders when divided by m.

Let the following two sum have the same remainder r :-

$a_1+a_2+\dots+a_k = pm+r$ — (1)

$a_1+a_2+\dots+a_k+a_{k+1}+\dots+a_l = qm+r$ — (2) $(l>m)$

(2) − (1) $a_{k+1}+a_{k+2}+\dots+a_l = (q-p)m$

→ divisible by m.

Hence, proved.

Application 4

A chess master who has 11 weeks to participate in a tournament decides to play at least one game every day but, in order not to tire himself, he decides not to play more than 12 games during any week. Show that there exists a succession (of consecutive) days during which the chess master will have played exactly 21 games.

Let a_1 is the no. of games played in 1st day.
a_2 — 1st & 2nd days.
a_3 — 1st 2nd & 3rd days
⋮
a_{77} — 1st 2nd ..... 77th days.

Increasing seq. → $1 \le a_1 < a_2 < a_3 < \dots < a_{76} < a_{77} \le 12 \times 11 = 132$

Orion
PAGE:
DATE: / /

Adding 21 :-

In. Sequence → $22 \le a_1+21 < a_2+21 < \dots\dots < a_{77}+21 \le 153$.

(each element is unique.)

If we merge these two increasing sequences
$77 \times 2 = 154$ elements in the sequence ≤ 153.

Value of each element lie between 1 and 153.

⇒ At least two elements in resulting sequence are equal (by PP)

⇒ $a_j = a_i + 21$

$a_j - a_i = 21$

⇒ $a_{i+1} + a_{i+2} + \dots + a_j = 21$

Why we added 21?

$154 - 132 - 1 = 21$ ✓

77×2 = max pigeons required. → pigeonholes

18/10/16

Pigeonhole Principle: Simple form.

related PP simple form.

If n object are put into n boxes and if no box is empty (i.e. no box contains more than one object) then each box contains exactly one object.

Application

CRT (Chinese Remainder Theorem)

Let m and n be relatively prime positive integers, and let a and b be integers where $0 \le a \le m-1$, $0 \le b \le n-1$. Then there is a positive integer x such that the remainder when x is divided by m is a, and when x is divided by

Orion
PAGE:
DATE: / /

n is b, i.e. x can be written in the form:-

$x = pm + a$

$x = qn + b$

⋮

Consider n integer.

$a, m+a, 2m+a, \ldots\ldots, (n-1)m+a$

When divided by m, remainder is a.

Let, the two integers (among these n integers) give some remainder when divided by n.

$0 \le i < j \le m-1 \rightarrow ? \leftarrow x$

$i \le n-1$

$j \le n-1$

$\Rightarrow j - i \le n-1 < n$

$im + a = q_1 n + r$

$jm + a = q_2 n + r$

$\Rightarrow (j-i)m = (q_2 - q_1)n$

Since m and n are relatively prime, so to hold the equation, n must be a factor of $(j-i)$

But this is not possible

n cannot be factor of $(j-i)$ {because $j-i < n$}

$\Rightarrow$ Contradiction.

$\Rightarrow$ No same remainder $\Rightarrow$ They are all different when divided by n.

$x = pm + a$; $0 \le p \le n-1$, $0 \le a \le m-1$

$x = qn + b$; $0 \le q \le m-1$, $0 \le b \le n-1$

$\Downarrow$

$x \bmod m = a$

$x \bmod n = b$

⋮

$x \bmod l = c$.

Congruent equations.

Orion
PAGE:
DATE: / /

Pigeonhole Principle: Strong Form

Theorem: Let $q_1, q_2, \ldots, q_n$ are positive integers.
If $(q_1 + q_2 + q_3 + \ldots + q_n - n + 1)$ objects are distributed among n boxes, then either the 1st box contains at least q_1 objects, or the 2nd box contains atleast q_2 objects, or ...., n^{th} box contains at least q_n objects.

Proof: Let $q_1 + q_2 + \ldots + q_n$ integers are distributed over n boxes, if every box gets a fewer integers

$$(q_1 - 1) + (q_2 - 1) + (q_3 - 1) + \ldots + (q_n - 1) = (q_1 + q_2 + \ldots + q_n - n) \text{ objects}$$

If we add 1 integer more, that integer will go to one of the boxes

But $q_1 = q_2 = \ldots = q_n = 2$

Total no's $= 2n - n + 1 = n + 1$.

$\Rightarrow$ At least one box gets atleast 2 objects.

SPECIAL CASES

If $q_1 = q_2 = \ldots = q_n = r$

* If $n(r-1) + 1$ objects are put into n boxes then atleast one of the boxes contains r or more of the objects.

* If the avg of n non-negative integers $m_1, m_2, \ldots m_n$ is greater than $(r-1)$,

$$\frac{m_1 + m_2 + \ldots + m_n}{n} > r - 1,$$

then at least one of the integers is greater than or equal to r.

$$\text{Avg.} \quad \frac{m_1 + m_2 + \ldots + m_n}{n} = \frac{n(r-1) + 1}{n}$$

VAHSUM : ASI

Orion
PAGE:
DATE: / /

Av. $< \frac{n(r-1)+1}{n} + 1 = \frac{n(r-1)+1+n}{n} = r + 1/n$

$< \frac{n(r-1)+1}{n} + 2 = r+1+1/n$

* If the avg. of n integers $m_1, m_2, \ldots, m_n$ is less than $(r+1)$ i.e $\frac{(m_1+m_2+\ldots+m_n)}{n} < (r+1)$

then atleast one of the integers is less than $(r+1)$.

* If the avg. of n non-negative no.s $m_1, m_2, \ldots m_n$ is at least equal to r then at least one of the integers satisfies $m_i \geq r$.

Application 1

1. A basket of fruit is being arranged out of apples, bananas, and oranges. What is the smallest no. of pieces of fruits that should be put in the basket in order to guarantee that there are atleast 8 apples, atleast 6 bananas, or atleast 9 oranges

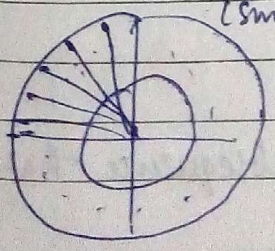
$8+6+9-3+1 = 21$

Application 2

Two disks, one smaller than the other, are each divided into 200 congruent sectors (pie).

L-disk (large) ⇒ 100 sectors are chosen arbitrarily and painted red, 100 painted blue.

S-disk (small) → each sector is painted either red or blue.



Now, s-disk is placed on largest disk such that centers coincide

Orion
PAGE:
DATE: / /

Show that it is possible to align the two disks, so that the no. of sectors of s-disk whose colour matches corresponding sectors of L-disk is at least 100.

sectors of s-disk ← $\frac{200 \times 100}{200}$ = 100 ≡ r → red sectors of L-disk

no. of sectors

Application:

Show that every sequence $a_1, a_2, \ldots, a_{n^2+1}$ of (n^2+1) real no.s contains either an increasing subsequence of length $(n+1)$ or a decreasing subsequence of length $(n+1)$.

Example

8, 11, 9, 1, 4, 6, 12, 10, 5, 7.

$10 = 3^2+1$ (11, 9, 6, 5)

$3+1 = 4$-length subsequence

Proof:

We suppose there does not exist any increasing sequence of length $(n+1)$ and show there must be a decreasing sequence of length $(n+1)$

$a_1, a_2, \ldots, a_{n^2+1}$

m_i = length of subsequence associated with a_i.

For each $k = 1, 2, \ldots n^2+1$

Let m_k be the length of longest subsequence that

begins with a_k.

Suppose $m_k \leq n$ $\quad n+1$.

$m_k \geq 1$

possible length of subsequence have values 1 to n^2+1.
they are put into m_ks whose values lie blw 1 and n.

By P.P.S.F.

$n^2+1, \quad n \cdot n+1$

□ □ . . . □
n boxes.

$\Rightarrow$ At least one box contains $(n+1)$ terms. (i.e $m_i \geq n+1$ for at least 1 $1 \leq i \leq n$)

Let $m_{k_1} = m_{k_2} = \ldots = m_{k_{n+1}}$

Subsequence starting from $a_{k_1} \; a_{k_2} \; \ldots \; a_{k_{n+1}}$

Suppose that for some i, $a_{k_i} < a_{k_{i+1}}$
$(i = 1, 2, \ldots n)$

Since $k_i < k_{i+1}$

$m_{k_i} > m_{k_{i+1}}$

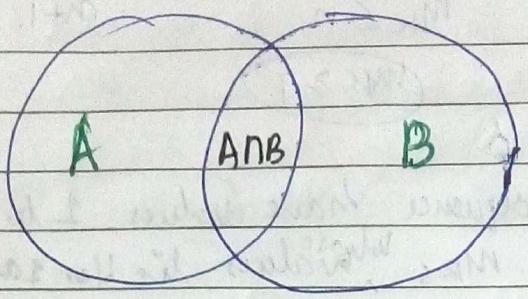
$a_{k_i} \geq a_{k_{i+1}}$

$a_{k_1} \geq a_{k_2} \geq \ldots \geq a_{k_{n+1}}$

where $a_{k_1}, a_{k_2}, \ldots a_{k_{n+1}}$ is a decreasing sequence of length.

Orion
PAGE:
DATE: 24/10/16

The principle of Inclusion Exclusion.



Ex.1 In a D.M (course of Discrete math.), Computer Sc. Major - 25, Mathematics Major - 13, Major in both - 8

all students are in major

How many students? $25+13-8=30$.

Ex.2 How many +ve integers are not exceeding 1000 are divisible by 7 or 11.

$$= \left\lfloor \frac{1000}{7} \right\rfloor + \left\lfloor \frac{1000}{11} \right\rfloor - \left\lfloor \frac{1000}{77} \right\rfloor$$

divisible by 7 — by 11 — by 77 (LCM of 7 & 11) ⇒ divisible by both 7 & 11.

$= 142 + 90 - 12 = 220.$

Ex.3 There are 1807 freshers, 453 in CS, 567 in Math, 299 – both CS & math.

Ex.4. There are 1232 students - Spanish, 879 - French, 114 - Russian

If 2092 students have at least one of Spanish, French, Russian. How many have a course in all three.

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

$2092 = 1232 + 879 + 114 -$ (we get this → we can find this.)

Orion
PAGE:
DATE: / /

Theorem: Let $A_1, A_2, \ldots A_n$ be finite sets

then $$|A_1 \cup A_2 \cup A_3 \ldots \cup A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n+1} |(A_1 \cap A_2 \cap A_3 \ldots \cap A_n)|$$

Proof:- Suppose an element a is a member of exactly 'r' of the sets $A_1, A_2, \ldots, A_n$

$$1 \le r \le n.$$

The element is counted $C(r,1)$ times by $\sum |A_i|$

$C(r,2)$ times by $\sum |A_i \cap A_j|$

$\vdots$

$C(r,m)$ times by $\sum |A_i \cap A_j \cap \ldots A_m|$ (any group of m sets.)

'a' is counted exactly $\rightarrow$ $C(r,1) - C(r,2) + C(r,3) - C(r,4) \ldots$ (these many no.!)

($2^n - 1$ terms.)

$$C(r,0) - C(r,1) + C(r,2) - C(r,3) \ldots = 0$$

$$1 = C(r,1) - C(r,2) - \ldots (-1)^{n+1} C(r,n)$$

Ex.1

$n = 4$

A_1, A_2, A_3, A_4

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = |A_1| + |A_2| + |A_3| + |A_4| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_1 \cap A_4| - |A_2 \cap A_3| - |A_2 \cap A_4| - |A_3 \cap A_4| + |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4| - |A_1 \cap A_2 \cap A_3 \cap A_4|$$

$15 = 2^4 - 1$ terms.

Orion
PAGE:
DATE: / /

Ex:2 $f: A \to B$ (m, n) How many one-to-one f^n's are possible there?

$n > m \Rightarrow$ X

$m > n$

One to one = $n(n-1)(n-2)\ldots 1$

$= n!$

Total possible f^n's $= n^m$

Algebraic Structures

25/10/16

Group, ring, field

Algebra

1. Set
2. Operation on Set
3. Constants, special elements of that set satisfies some specific properties

$A\{S, +, 0\}$

$S \to Z^+$

$a \in S$

$0+a=a$

$a+0=a$

$A\{S, \cdot, 1\}$

$1 \cdot a = a$

$a \cdot 1 = a$

Ex: Set of all strings, constitutes from a set of alphabet Σ (say)

$(\Sigma^*, \text{concatenation}, \lambda)$

Σ^*: set of all strings; concatenation: (concat) operation; λ: empty string

$x \in \Sigma^*$

x concat $\lambda = x$

λ concat $x = x$

$A\{S, +, \cdot, 0, 1\}$

$+$: addition modulo n

$\cdot$: multiplication modulo n

S: $\{0, 1, 2, \ldots, n-1\}$

0, 1: constants

$S^p \to S$

$p \to$ arity of the operation

Orion
PAGE:
DATE: / /

+, ·, binary operators
'−' unary minus

$S^2 \to S$
$S' \to S$

Signature

Given two algebra they are of same signature if they have same no. of op^n, arity is same and same no. of constants.

{Σ*, concat, compare, 0}

{Z+, +, ·, 0}

set of operators
set of constants.

Properties (Axioms) of {S, 0, c}
S · c

1. Commutative
if a, b ∈ S
a · b = b · a

2. Associative
a · (b · c) = (a · b) · c

$S^2 \to S$ → Closure : Inherent property → we do not always define it.
if a, b ∈ S
a o b ∈ S
a operation b → output.

3. Identity
if an element e ∈ S
a · e = a
e · a = a
Left identity
Right identity.

Ex. S - Z+
0 : binary addition +
a + b = b + a
0 : binary subtraction (minus)
a − b ≠ b − a

ANUBHAV JAIN NOTES

if $e_l = e_r = e$, then e is the identity of the algebraic str.

~~$\{$~~ $\rightarrow \{S, +, 0\}$ $\forall a$

If $\cdot = +$ addition

$e = 0$ is the additive identity

$a + 0 = 0 + a = a$, $a \in S$

$\rightarrow \{S, \cdot, 1\}$

$1 \cdot a = a \cdot 1 = a$

1 → multiplicative identity.

$\{\Sigma^*, \text{concatenation}, \lambda\}$

Σ^* $\overset{\infty}{\underset{i=1}{\Sigma}} (a_i s, b_i c)$

→ $a_1\ a_2\ a_3 \ldots a_n$
→ $b_1\ b_2\ b_3 \ldots b_n$
} 2 elements of Σ^*

$\underbrace{a_1 a_2 a_3}_{A} \in \Sigma^*$

$\underbrace{b_1 b_2 b_3}_{B} \in \Sigma^*$

$C = c_1 c_2 c_3$

A concat B $= a_1 a_2 a_3 b_1 b_2 b_3$
B concat A $= b_1 b_2 b_3 a_1 a_2 a_3$
} NOT Commutative

A Concat (B concat C) $= a_1 a_2 a_3 b_1 b_2 b_3 c_1 c_2 c_3$, (A concat B) concat C $= a_1 a_2 a_3 b_1 b_2 b_3 c_1 c_2 c_3$ } Associative

* All structures will not satisfy all the properties.

⇒ we define diff algebraic structures with different properties.

Orion
PAGE:
DATE: / /

Semigroup, Monoid & Group

Algebra : $A\{S, O, C\}$
$A'\{S', O', C'\}$

A' is semialgebra of A if
(i) $S' \subset S$
(ii) each O_i is same as O_i defined to S'
(iii) $C = C'$

Z - set of integers
E - set of even integers.

Axioms :-
A1 Closure
A5 commutative
A2 Associative
A3 Identity
A4 Inverse

Semigroup

G is an algebraic str. defined as $\{G, \cdot\}$ that associates to each ordered pair $a, b \in G$ an element $a \cdot b \in G$ such that the following properties hold

A1 : closure , $a, b \in G \Rightarrow a \cdot b \in G$
A2 : associative , $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

then G is called Semigroup.

Monoid

G is Monoid defined as $\{G, \cdot\}$ that associates to each ordered pair $a, b \in G$ an element $a \cdot b \in G$ such that the following properties hold

A1 : closure , $a, b \in G \Rightarrow a \cdot b \in G$
A2 : associative , $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
A3 : and there exist an element $e \in G$ such that (Identity) $a \cdot e = e \cdot a = a$, $a \in G$

Orion
PAGE:
DATE: / /

Group.

G is a Group defined as $\{G, \cdot\}$ that associates to each ordered pair $a, b \in G$ an element $a \cdot b \in G$ such that the following properties hold

A1 : closure
A2 : Associative
A3 : Identity
A4 : Inverse :-

Inverse element → there exists an element a^{-1}

$a \cdot a^{-1} = e$ $\quad a, a^{-1} \in G$
$a \cdot I_R = e$ $\quad a \cdot b \in G$
$I_L \cdot a = e$
$a^{-1} \cdot a = e$

$\{S, \cdot, c\}$

$\{Z, \cdot, 0, 1\}$

Z → set of integers
· → multiplication

$a, b \in G$
$a \cdot b \in G$
$a \cdot 1 = 1 \cdot a = a$
$\frac{1}{a}$ x → with 2, it does not form a group.

$\{R, \cdot, 1\}$ → Group ✓.

Ex.1 $\{Z_n, \oplus, 0\}$

$Z_n = \{0, 1, \ldots n-1\}$
$\oplus$ = addition modulo n $(n = 8)$
0 = constant

addition modulo 8 ↑ n

⊕	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

A1 - closure ✓
A2 - associative ✓
A3 - Identity ✓ (0 mod 8)
A4 - Inverse ✓ (8 − a) mod 8

⇒ It forms a group

$a + (-a) = 0$ → Identity
Inverse

Orion
PAGE:
DATE: / /

* If group holds A5 also (commutativity) → ABELIAN GROUP.

Ex 2. $\{Z_n, \odot, 0\}$

⊙	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	(1)	2	3	4	5	6	7
→ 2	0	2	4	6	0	2	4	6
3	0	3	6	(1)	4	7	2	5
→ 4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	(1)	6	3
→ 6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	(1)

A1 - Closure ✓
A2 - Assoc. ✓
A3 - Identity ✓ (1 mod 8)
A4 - Inverse ✗

Numbers which are less than n and are coprime will get inverse, others not.

⇒ If we take n prime ⇒ it forms GROUP
if n is not prime ⇒ it does NOT form group

Cyclic Group

A group is cyclic if every element of G can be generated from one particular element $a \in G$ as a power of a^k, k is an integer.

a - generator

Cyclic group is abelian

$\{Z^+, +, 0\}$ Z^+, $a = 1$ / repeated operation

Orion
PAGE:
DATE: / /

Ex: Let N_n denote a set of n distinct symbols $\{1, 2, \cdots n\}$

$a_1\ a_2 \cdots a_n$

		a_2 a_1 a_0
		x^2 x 1
a_1	0	0 0 0
a_2	1	0 0 1
a_3	$1+x$	.
a_4	$1+x+x^2$	1 1 1

$n=3$

$a_2x^2+a_1x^1+a_0x^0$

A permutation of n distinct symbols is a one to one mapping from N_n to N_n. Define S_n to be the set of all permutation of n distinct symbols.
Each element of S_n is represented by a permutation of the integers $\{1, 2, \cdots n\}$
Show that S_n is a group.

S_n, Π

123
132
213
231
312
321

1 2 3
3 2 1

$\Pi\{3, 2, 1\}$
↓
operation

A1 If $\Pi, \rho \in S_n$
$\Pi \cdot \rho$ is formed by permuting the elements of ρ according to permutation Π.

Orion
PAGE:
DATE: 31/10/16

GROUP

A1 Closure — op^n – *
A2 Associative
A3 Identity — Mod n addition – Group
A4 Inverse — mod n multiplication – if n is prime – Group.

Subgroup

We consider a nonempty subset H of group G. H is defined as the subgroup of G if it is closed under the group operation of G and satisfies the other group properties.

Ex. H – set of integers
G – set of rational no.s.
op^n – addition

Theorem: H is a subgroup of G if H is closed under the group operation (*) and inverse exists.

Proof:

A1 If a be an element of H, $a \in H$
A4 Let a^{-1} is the inverse of a
$a * a^{-1} = e$ $e \in H$
A3 So identity exists

A2 Since G is associative then H also holds associativity.
So H is a subgroup of G.

Ex. op^n – mod 16 add^n — binary. op^n → ⊕
G – {0, 1, - - - 15}
Subgroup of G → H = {0, 4, 8, 12}
Total subgroups ~~sets~~ of G → ~~2^{16}~~
H – {1} ~~✓~~

a=3 $3 \oplus h = \{3, 7, 11, 15\}$
a=7 $7 \oplus h = \{7, 11, 15, 3\}$ reordered.

Identical cosets. (cosets are not distinct)

Orion
PAGE:
DATE: / /

Coset

Let a be an element of group G with binary operation *. H is the subgroup of G

The set $a*H = \{a*h ; h \in H\}$ is the left coset of H

and $H*a = \{h*a ; h \in H\}$ is the right coset of H.

If G is commutative $a*h = h*a$ ⇒ coset of H

$0 \oplus H = \{0, 4, 8, 12\}$
$1 \oplus H = \{1, 5, 9, 13\}$
$2 \oplus H = \{2, 6, 10, 14\}$
$3 \oplus H = \{3, 7, 11, 15\}$

Union of distinct cosets forms the group – partition of G.

Theorem 1 Let H be a subgroup of G with binary operation *. No two elements in a coset of H are identical.

Proof:

Let h and h' are the two different elements of H. ~~that are identical~~

Let $a \in G$, $a^{-1} \in G$ {Inverse exists within group}

Let $a*h = a*h'$ {Two elements in a coset of H are identical}

$a^{-1}*(a*h) = a^{-1}*(a*h')$

Associative: $(a^{-1}*a)*h = (a^{-1}*a)*h'$

$e*h = e*h'$; {Identity: $e*h = h$}

$h = h'$

But this is a contradiction since h and h' are diff elements

Hence, our assumption is wrong, $a*h \neq a*h'$ ⇒ No two elements in a coset of H are identical.

Orion
PAGE:
DATE: / /

Theorem 2 No two elements in the different cosets of a subgroup H of a group G are identical.

Proof:

Let $a*H$ & $b*H$ are two different cosets of H with $a, b \in G$.

Let $a*h$ and $b*h'$ be two elements in $a*H$ and $b*H$ $h, h' \in H$.

Suppose,

$a*h = b*h'$

$(a*h)*h^{-1} = (b*h')*h^{-1}$

$a*(h*h^{-1}) = b*(h'*h^{-1})$

$a*e = b*h''$

$a = b*h''$.

Let h^{-1} be the inverse of h.

$\hookrightarrow h^{-1} \in H$

$\Rightarrow (h'*h^{-1}) \in H$

$\Rightarrow h'' \in H$.

$a*H := a*h \quad h \in H$

$= (b*h'')*h$

$(h''*h = h''')$ $= b*(h''*h) = b*h''' =: b*H$

$\rightarrow$ A contradiction since $a*H$ & $b*H$ are diff. cosets.

$\Rightarrow a*h \neq b*h'$

$\Rightarrow a*H$ and $b*H$ are disjoint cosets.

LAGRANGE'S THEOREM

Let G be a group of order (cardinality) n and H (subgroup) be of order m. Then m divides n and the partition G/H consists of n/m cosets of H

Proof:

Let i be the no. of disjoint cosets of H.

$i \cdot m = n$

$i = n/m$.

Properties of Coset:-

1. Every element of G appears in one and only one coset of H.
2. All the distinct cosets of H are disjoint.
3. The union of all the distinct coset of H form the group.

Example- O_{16} mod 16.

Orion
PAGE:
DATE: 01 / 11 / 16

Order of a group is the no. of elements in the group. If there are finite no. of elements in G then it is a finite group, otherwise infinite.

Ex:
Rational no:s, Real no:s, Complex no:s. → Group ✓.
* Set of integers is not a group (Inverse does not exist on multiplication opn.)
↓
It is a group for 'addition opn'

Ex:
$N_n \xrightarrow{P} N_n$ N_n is set of permutation of n distinct symbols

$n=3$

$N_n = \{1,2,3\}, \{3,2,1\}, \{2,1,3\} \ldots$

Π Permutation - $\{3,2,1\}$ → positions.

$\Pi \cdot P = \{3,2,1\} \cdot \{2,1,3\}$

Permutation — one of the elements of N_n

$= \{3,1,2\}$

$a = \{2,3,1\}$

A1 : Closed

A2 - $a.(b.c) = (a.b).c$

LHS $a.(b.c)$
$= \{2,3,1\}\ \{3,1,2\}$
$= \{1,2,3\}$

RHS $a.b = \{2,3,1\} \cdot \{3,2,1\} = \{2,1,3\}$
$(a.b).c = \{2,1,3\} \cdot \{2,1,3\} = \{1,2,3\}$

A3 : $\{1,2,3\}$
$= \{1,2,\ldots\ldots n\}$ (for n symbols)

A4 : $a.b = e$ $\{1,2,3\}$.

$a*e = a$ ✓
$e*a = a$ ✓

Orion
PAGE:
DATE: / /

Group, Ring, Field

$A_1 - A_4 \rightarrow$ Group
$+ A_5$ – commutative $(a \cdot b = b \cdot a) \Rightarrow$ Abelian Group.

Ring: A Set R (R, +, ×) with two binary operations addition and multiplication that satisfies the following axioms

$A_1 - A_5$ – wrt addition & additive identity 0, inverse is (-a), $a \in R$.

M1 – closure under multiplication.
M2 – associative with multiplication $a \times (b \times c) = (a \times b) \times c$
M3 – Distributive (multiplication is distributive over addition).

$a \times (b+c) = a \times b + a \times c$
$(b+c) \times a = b \times a + c \times a$.

M4 – Commutative over multiplication
$a \times b = b \times a$.

Commutative Ring: $A_1 - A_5$, $M_1 - M_4$

Ex. R – a set of n square matrices
Opⁿ – + ×

Set of Real no.	m×m

A5 – holds wrt addition.
– Ring but it is not a commutative Ring as M4 – Matrix Multiplication is not commutative

M5 – Multiplicative identity. $1 \times a = a \times 1 = a$.
M6 – No zero divisors

Orion
PAGE:
DATE: / /

if $a \times b = 0$
then either $a = 0$ or $b = 0$
(but not both.)

A1-A5, M1-M6 - Integral Domain

Field $(F, +, \times)$ is a set of elements with two binary operators, $+, \times$ that satisfies axioms A1-A5, M1-M6 and
M7 - Multiplicative inverse

- addition, subtraction
  $a - b = a + (-b)$
- Multiplication
  a^{-1} $\quad a/b = a \times b^{-1}$

$a, b \in R \Rightarrow c \in R.$
$a \times b = c$

Modulo -n addition

(a+b) modulo 8
= Remainder when (a+b) is divided by 8.
(a×b) modulo 8
= Remainder when (a×b) is divided by 8.

Ex:
Set $\{0, 1\}$ - opn - Modulo-2 addition & multiplication.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	(1)

→ no '1'

additive identity - 0
additive inverse 0, 0
1, 1

Multiplicative identity
$a \times (b \times c) = (a \times b) + (a \times$

$a + a^{-1} = e$
$0 + 0 = 0$
$1 + 1 = 0$

⇒ Inverse does not exist

Orion
PAGE:
DATE: / /

Ex: Op^n – modulo -p addition & multiplication.
Set – $\{0, 1, \ldots p-1\}$, p is prime. – Field

p=7

mod-7 addition

+	0	1	2	3	4	5	6
0	(0)	1	2	3	4	5	6
1	1	2	3	4	5	6	(0)
2	2	3	4	5	6	(0)	1
3	3	4	5	6	(0)	1	2
4	4	5	6	(0)	1	2	3
5	5	6	(0)	1	2	3	4
6	6	(0)	1	2	3	4	5

mod-7 multiplication

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	(1)	2	3	4	5	6
2	0	2	4	6	(1)	3	5
3	0	3	6	2	5	(1)	4
4	0	4	(1)	5	2	6	3
5	0	5	3	(1)	6	4	2
6	0	6	5	4	3	2	(1)

Field:-
1. Commutative group under addition.
2. Commutative group under multiplication.
3. Distributive.

		−a	a^{-1}
→	0	0	–
	1	6	1
	2	5	4
	3	4	5
	4	3	2
	5	2	3
	6	1	6

Additive Inverse | Multiplicative Inverse.

Finite Field: If the no. of elements are finite.
$q = p^m$

Galois Field
↳ GF(p)
↳ GF(p^m) – Extended field – for any +ve integer we get the field GF(p^m).

Consider the sequence of sums

$1 = \sum_{i=1}^{1} 1$, $\sum_{i=1}^{2} 1 = 1+1$, $\sum_{i=1}^{3} 1 = 1+1+1 = 3$, ...

$\therefore \sum_{i=1}^{k} 1 = 1+1+1 \ldots 1$ (k times) $= k$.

Modulo addition + : $1 \in GF(p)$ it will repeat.

Orion
PAGE:
DATE: / /

m, n $\quad \sum_{i=0}^{m} 1 \Rightarrow \sum_{i=1}^{n} 1$

$\sum_{i=1}^{n-m} 1 = 0 \quad = \sum_{i=0}^{n-m} 1 = 0.$

$\lambda \rightarrow$ is called the characteristic of the field.

Theorem 1

The characteristic λ of a prime field is prime.

GF(p) Suppose $\lambda = m,n$, it is not a prime.

$$\sum_{i=1}^{\lambda} 1 = \sum_{i=1}^{mn} 1 = 0$$

$$\sum_{i=1}^{m} 1 \times \sum_{i=1}^{n} 1 = 0$$

$\lambda = mn$ $\quad$ 0 $\quad$ 0

$m, n < \lambda.$

Theorem 2

Let a be a non-zero element of GF(q) then

$$a^{q-1} = 1$$

Order of Field.

a is an element of the set & n is a +ve integer such that $a^n = 1$.

n = order

Proof

Let $b_0, b_1, b_2, \ldots, b_{p-1}$ are the p no. of elements in the set.

p is prime, $\quad 0, 1, 2, \ldots p-1$

Multiply by a.

$a \times b_0, a \times b_1, a \times b_2, \ldots a \times b_{p-1}$.

Orion
PAGE:
DATE: / /

After multiplication, the no.s become the elements of set but in different order.

$b_1, b_2, \ldots b_{p-1}$

Exclude '0' :-

* a is one of b_i

$ab_1 \times ab_2 \times ab_3 \ldots \times ab_{p-1} = b_1 \times b_2 \times \ldots b_{p-1}$

$a^{p-1} \times b_1 \times b_2 \times \ldots \times b_{p-1} = b_1 \times b_2 \times \ldots b_{p-1}$

$\boxed{a^{p-1} = 1}$

$q = 2^8$ $\quad p = 2, \; m = 8$

$q = p^m$

$\{0, 1, 2 \ldots\ldots\ldots p^m - 1\}$

$GF(7)$ $\quad GF(7^8)$

$GF(7)$ — prime. $\quad GF(7^8)$ — extended.

Theorem:

If 'a' is a non zero element of a finite field GF(q) and n is order of the field, then n divides (q-1)

Proof:

* Order n is the smallest integer s.t $a^n = 1$

Suppose n does not divide q-1.

$\Rightarrow q-1 = kn + r$

$a^{q-1} = a^{kn+r} = a^{kn} \cdot a^r$

prev. thm $\Rightarrow 1 = (a^n)^k \cdot a^r$

$\Rightarrow 1 = 1 \cdot a^r \quad (\text{as } a^n = 1)$

Orion
PAGE:
DATE: / /

$\Rightarrow a^r = 1$.

But $r < n$

and n is smallest integer s.t. $a^n = 1$

$\Rightarrow r = 0$

Our assumption was wrong.

$\Rightarrow$ (n divides $(q-1)$) Hence Proved.

Extended version: $p = 7$.

Opⁿ: Modulo 7

[a, e] → $a^e \bmod 7$.

a \ e	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

Integers < 7 as a pow

* as $a^6 = 1$ $\forall$ a's

$\Rightarrow$ order = 6.

for $a = 2, 4$ $a^3 = 1$

$= 3, 5$ $a^6 = 1$

6 $a^2 = 1$

* Some element (one or more) less than q st for them $a^n = a^{q-1} = 1$

is order $n = q-1$.

→ These are primitive members, also called "generator" elements as all other could be obtained using these

Orion
PAGE:
DATE: / /

Modular Arithmetic

a nonzero element.

$\frac{a}{n} = k_1 n + r_a$ $\qquad$ $\frac{b}{n} = k_2 n + r_b$

$r_a = a \bmod n$
$r_b = b \bmod n$

If $a \bmod n = b \bmod n$ → b-a is divisible by n.
then $a \equiv b \bmod n$
a is congruent to b.

1. $(a \bmod n \pm b \bmod n) \bmod n = (a \pm b) \bmod n$
2. $(a \bmod n \times b \bmod n) \bmod n = (a \times b) \bmod n$.

RHS. $(a+b) \bmod n$

$a+b = k_1 n + r_a + k_2 n + r_b$
$= (k_1 + k_2) n + (r_a + r_b)$

$\Rightarrow (a+b) \bmod n = (r_a + r_b) \bmod n$
$= (a \bmod n + b \bmod n) \bmod n = LHS$

Similar for multiplication.

$11^7 \bmod 13$

$11 \bmod 13 = 11$
$11^2 \leftarrow 121 \bmod 13 = 4$
$11^3 \bmod 13 = (11 \times 11^2) \bmod 13 = 44 \bmod 13 = 5.$

$11^4 \bmod 13 = (11^2 \times 11^2) \bmod 13 = 16 \bmod 13 = 3.$
$11^7 \bmod 13 = (11^4 \times 11^3) \bmod 13 = (3 \times 5) \bmod 13 = (2).$

ANUBHAV JAIN NOTES

CT2 → 15/11

Orion

PAGE:
DATE: / /

GF(p) → prime 0, 1, 2, . . ., (p-1)

8-bit 0 to 255 → not prime

↳ nearest prime = 251

GF(256)

GF(pm)

↳ field.

GF(8) = GF(2^3) coefficients of polynomial

a_2 a_1 a_0	
0 0 0	0
0 0 1	1
0 1 0	x
0 1 1	$1+x$
1 0 0	x^2
1 0 1	$1+x^2$
1 1 0	$x+x^2$
1 1 1	$1+x+x^2$

$a_2x^2 + a_1x^1 + a_0x^0$

Group- Ring Field

7/11/16

Isomorphism, Automorphism, Homomorphism.

Let (T, o) and (S, *) be two groups with operation o, *. The groups are isomorphic if there is a bijection f from (T, o) to (S, *) such that for any $a_1, a_2 \in T$,

$$f(a_1 \circ a_2) = f(a_1) * f(a_2)$$

($\circ$: group op^n of (T, o); $*$: (S, *))

$S = \{\alpha, \beta, \gamma\}$ $T = \{a, b, c\}$

T

o	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

S

*	α	β	γ
α	α	β	γ
β	β	γ	α
γ	γ	α	β

Orion
PAGE:
DATE: / /

mappings (operations of $\circ$ & $*$) are similar, only difference is the symbols (elements of the two set).

$f(a) = \alpha$
$f(b) = \beta$
$f(c) = \gamma$

} It could have also been :

$f(a) = \beta$
$f(b) = \gamma$
$f(c) = \alpha$

} → Isomorphism

- $f(a) = b$
  $f(b) = c$
  $f(c) = a$

} Automorphism → get the same element set.
$T \to T$

Properties:-

1. Let $G = (T, \circ)$ be a group of order p.
   Any group of order p is isomorphic to G.
2. Each finite group of order n is a permutation group of degree n.

Let $A(S, \circ, c)$, $A'(S', \circ', c')$
S → set of elements, $\circ$ → opⁿ, c → const.
are two algebraic structures.

There are relations between c and c'.

T, $\circ$
S, $*$

h is the bijection that satisfies
$h(a_1 \circ a_2) = h(a_1) \circ' h(a_2)$
$h(c) = c'$

$$\begin{array}{ccc} S \times S & \xrightarrow{\circ} & S \\ \downarrow h \quad \downarrow h & & \downarrow h \\ S' \times S' & \xrightarrow{\circ'} & S' \end{array}$$

A and A' are homomorphic

Isomorphism is a restricted class, it is a class of homomorphism.

Orion
PAGE:
DATE: / /

Set of elements $\{0, 1, \ldots p-1\}$

Op^n – { modulo-n addition & modulo-n multiplication

⊕ – Group

⊗ – Group

Multiplicative inverse – Field

GF(8)

↓

GF(p) – prime field

GF(q)

$q = p^m$ – extended field

$8 = 2^3$.

Arithmetic Field

$q = p^m$

* Conversion between integer arithmetic to polynomial arithmetic and both follow modular arithmetic $a \bmod n \; (a = k_i n + r_a)$
* To construct the field we need one irreducible polynomial.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} = \sum_{i=0}^{n-1} a_i x^i$$

$p(x) \rightarrow$ irreducible polynomial of degree $(n-1)$.

$$\frac{f(x)}{p(x)} = r_1(x)$$

a_2	a_1	a_0	polynomial
0	0	0	0
0	0	1	1
0	1	0	x
0	1	1	$1+x$
1	0	0	x^2
1	0	1	$1+x^2$
1	1	0	$x+x^2$
1	1	1	$1+x+x^2$

$GF(8) = GF(2^3)$

$0, 1, \ldots 7$

To store this, we need 3 bits.

$a_0, a_1, a_2 \ldots a_{n-1} \in \{0, 1\}$

$f(x) = a_2 x^2 + a_1 x + a_0$.

Orion

PAGE:
DATE: / /

$f(x) = \{0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}$

irreducible → $1+x+x^3$ — $p(x)$

$1+x^2+x^3$

for any deg., at least one irreducible poly. exist.

Let $p(x) = 1+x+x^3$

⊕	0	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
0	0	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
1	1	0	$1+x$	x	$1+x^2$	x^2	$1+x+x^2$	$x+x^2$
x	x	$1+x$	0	1	$x+x^2$	$1+x+x^2$	x^2	$1+x^2$
$1+x$	$1+x$	x	1	0	$1+x+x^2$	$x+x^2$	$1+x^2$	x^2
x^2								
$1+x^2$								
$x+x^2$								
$1+x+x^2$								

→ addition modulo 2 (0, 1 only).

GF(p^n) $n-1$ deg poly.

$f(x) = a_{n-1}x^{n-1} \cdots + a_1 x + a_0$.

$p = 2$ (0,1), $n = 3$ → $f(x) = a_0 + a_1 x + a_2 x^2$

$2^3 = 8$

$p = 3$ (0,1,2), $n = 2$ → $f(x) = a_0 + a_1 x$

$3^2 = 9$ elements.

00	10	20
01	11	21
02	12	22

$0, 1, 2, x, 1+x, 2+x, 2x, 2x+1, 2x+2$.

$\otimes$	0	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
0	0	0	0	0	0	0	0	0
1	0	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
x	0	x	x^2	$x+x^2$	$1+x$	1	$1+x+x^2$	$1+x^2$
$1+x$	0	$1+x$	$x+x^2$	x^2+1	$1+x+x^2$	x^2	1	x
x^2	0	x^2	$1+x$	$1+x+x^2$	$x+x^2$	x	$1+x^2$	1
$1+x^2$	0	$1+x^2$	1	x^2	x	$1+x+x^2$	$1+x$	$x+x^2$
$x+x^2$	0	$x+x^2$	$1+x+x^2$	1	$1+x^2$	$1+x$	x	x^2
$1+x+x^2$	0	$1+x+x^2$	$1+x^2$	x	1	$x+x^2$	x^2	$1+x$

$p(x)$

$1+x+x^3 \overline{)x^3}\,(1$

x^3+x+1

$1+x$

$1+x+x^3 \overline{)x+x^3}\,(x(x^3)$

$x+x^3+1$

1

$x(1+x)$

$x+x^2 = x^4$

$x^2+x^3+x+x^4$

$x^3+x^4+x+x^2$

$x+x^2$

x^2+x^4

a	b	z	−b
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

- Shorter method:-

$p(x) = 1+x+x^3 = 0$

$x^3 = 1+x$

In every row, we get 1 $\Rightarrow$ Multiplicative inverse exists.

10/11/16

Principle & Application (Problems)

Inclusion & Exclusion.

Q. Count the permutations $i_1, i_2, \ldots$ in of $\{1, 2, \ldots n\}$ in which '1' is not in 1st position.

Ex: 1 - 600

no. of integers not divisible by 6?

A = no. of integers divisible by 6. = $\frac{600}{6} = 100$

$\Rightarrow \bar{A} = S - A = 600 - 100$

$\boxed{\bar{A} = 500}$

Let S be a finite set of objects
Let P_1 & P_2 be two properties that each object in S may not possess.

Let A_1 be the no. of objects with property P_1
Let A_2 " P_2.

$$|\overline{A_1 \cup A_2}| = |S| - \underbrace{(|A_1| + |A_2| - |A_1 \cap A_2|)}_{|A_1 \cup A_2|}$$

$\downarrow$

$|\bar{A}_1 \cap \bar{A}_2|$

$$\boxed{|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cdots \bar{A}_m| = |S| - \sum_{i=1}^{m}|A_i| + \sum_{\substack{i=1, j=1 \\ i \neq j}}^{m} (A_i \cap A_j) - \sum (A_i \cap A_j \cap A_k) \cdots \cdots (-1)^m \sum (A_1 \cap A_2 \cap \cdots \cap A_m)}$$

No. of terms = $1 + {}^mC_1 + {}^mC_2 + \cdots + {}^mC_m = \boxed{2^m}$

$- \quad + \quad - \quad + \; - \cdots$

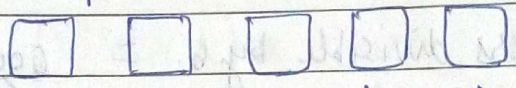
No. of objects of S consists of all these properties which possess at least one of the properties.

$$|A_1 \cup A_2 \cup \cdots A_m| = |S| - |\overline{A_1 \cup A_2 \cup \cdots \cup A_m}|$$
$$= |S| - |\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \cdots \cap \bar{A}_m|$$
$$= \sum A_i - \sum A_i \cap A_j + \sum (A_i \cap A_j \cap A_k) - \cdots (-1)^m \sum (A_1 \cap \cdots A_m)$$

Orion
PAGE:
DATE: / /

Ex: How many integers 0-99999 have among their digits each 2,5,8.

each : 0-9



Total numbers possible $= 10^5 = \alpha_0$.

permutation of Multiple Set

$A_1 \cap A_2 \cap A_3 = \{5\text{-}1, 5\text{-}3, 5\text{-}4, 5\text{-}6, 5\text{-}7, 5\text{-}9\}$ (5-0; 5-0 = no. of repetition; 5-7 = digit)

$= {}^5C_3 \cdot 3! \cdot 10^2 = 6000$

(if only 1 no. is dropped) $\alpha_1 = 9^5$

$\alpha_2 = 8^5$

$\alpha_3 = 7^5$

$$10^5 - \sum_{2,5,8} \alpha_1 + \sum_{(2,5),(5,8),(8,2)} \alpha_2 - \sum_{(2,5,8)} \alpha_3$$

$= 10^5 - 3(9^5) + 3(8^5) - 7^5$

$= 4350$

Combinations with Repetition.

No. of r combinations of a multiset with k-distinct elements each with an infinite repetition — ${}^{r+k-1}C_r$

Ex: Determine the no. of 10 combinations of the multiset $T = \{3\text{-}a, 4\text{-}b, 5\text{-}c\}$

$|S| = {}^{10+3-1}C_{10} = {}^{12}C_{10}$

$|A_1| = {}^{6+3-1}C_6$

${}^{5+3-1}C_5$

${}^{4+3-1}C_4$

⋮

Continued...

Orion
PAGE:
DATE: 15 / 11 / 16

Different Ways of Counting

Theorem 1

Let S be a multiset with objects of k diff" types where each has a infinite repetition number. The no. of r permutations of S is k^r.

Ex. a ternary no. system with 4-digit. / 8 digit

No.: □□□□ → 3^4. / 3^8.

Theorem 2

Let S be a multiset with objects of k diff types with finite repetition $n_1, n_2, \ldots, n_k$. Let the size of S be n

$$n = n_1 + n_2 + \ldots + n_k.$$

No. of permutations of S = $\dfrac{n!}{n_1! \times n_2! \times \ldots \times n_k!}$

$${}^{n}C_{n_1} \times {}^{n-n_1}C_{n_2} \times {}^{n-n_1-n_2}C_{n_3} \times \ldots \times {}^{n-n_1-\ldots-n_{k-1}}C_{n_k}$$

Theorem 3

Let n be a +ve integer and $n = n_1 + n_2 + \ldots + n_k$. The no. of ways to partition a set of n objects with k-labeled boxes $B_1, B_2, \ldots B_k$ equals $\dfrac{n!}{n_1! \times n_2! \times \ldots \times n_k!}$

If the boxes are not labeled and $n = n_1 + n_2 + \ldots + n_k$, $n_1 = n_2 = \ldots = n_k$, then the no. of permutation equals $\dfrac{n!}{k! \times n_1! \times n_2! \times \ldots \times n_k!}$

Combination with Repetition

Let T be a multiset, x of T has a certain type that has a repetition $> r$

Orion
PAGE:
DATE: / /

eg $T = \{3\cdot a, \infty\cdot b, 6\cdot c, \underset{>r}{10\cdot d}, \infty\cdot e\}$

$r=8$ $x = \{a, b, c, d, e\}$

$\{3\cdot a, 8\cdot b, 6\cdot c, 8\cdot d, 8\cdot e\}$

eg $S = \{\underset{1\ 2}{2a}, 1\cdot b, \underset{1\ 2\ 3}{3\cdot c}\}$

r comb^n $(r=3)$

Comb^n := $\{2\cdot a, 1\cdot b\}$ $\{2\cdot a, 1\cdot c\}$ $\{1\cdot a, 2\cdot c\}$ $\{1\cdot b, 2\cdot c\}$ $\{1\cdot a, 1\cdot b, 1\cdot c\}$ $\{3c\}$

Theorem

Let S be the multiset with objects of K-types each with an infinite repetition no. The number of r combination of S equals ${}^{r+k-1}C_r = {}^{r+k-1}C_{k-1}$

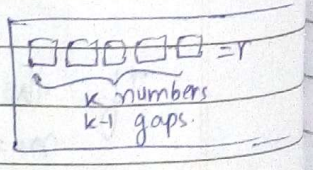
Let $a_1, a_2, \ldots, a_k$

$S = \{\infty\cdot a_1, \infty\cdot a_2, \ldots, \infty\cdot a_k\}$

Let the K no. of objects respect with the no. $x_1, x_2, \ldots, x_k$

$\{x_1\cdot a_1, x_2\cdot a_2, \ldots, x_k\cdot a_k\}$

$x_1 + x_2 + x_3 + \cdots + x_k = r.$



$T = \{\infty\cdot 1, (k-1)\cdot *\}$ $1, *$

$x_1\cdot a_1$ $x_2 a_2$ $x_3 a_3$ $x_4 a_4$

$\_ * 111 * \_ * 11$

$x_1 = 0$
$x_2 = 3$
$x_3 = 0$
$x_4 = 2$

No. of permutations of these $r+k-1$ objects on $r+k-1$ places equals the no. of ways we can choose $x_1, x_2, \ldots x_k$ s.t $\sum x_i = r$

Orion
PAGE:
DATE: / /

Proof

$x_1 + x_2 + \cdots + x_k = r$

We show that the no. of solution equals the no. of permutation of the multiset $T = \{r \cdot 1, (k-1) \cdot *\}$ of objects of two types only.

→ Given a permutation T, the $(k-1)$ *'s divide the r 1's into k groups.

x_1 is to the left of first *
x_2 is between first & 2nd *
⋮
x_k is to right of last *.

We can reverse the preceding steps and construct a permutation of T. No. of r combinations of multiset S = no. of permutations of T.

$$= \frac{(r+k-1)!}{r!\,(k-1)!} = {}^{r+k-1}C_r = {}^{r+k-1}C_{k-1}.$$

Ex. Determine the no. of 10 combination of the multiset

$T = \{3 \cdot a, 4 \cdot b, 5 \cdot c\}$.
(>3, >4, >5)

$T^* = \{\infty \cdot a, \infty \cdot b, \infty \cdot c\}$ is a multiset where 'a' repeats > 3 (atleast 4), b -> 4 (atleast 5), c -> 5 (atleast 6).

Let P_1 be the property that a 10 combination of T^* which has more than 3 a's

P_2 ——— 4 b's

P_3 ——— 5 c's

I.E.P : none of the properties hold for P_1, P_2, P_3, then we get the result.

$A_1 = P_1 \ldots$

$$|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3| = |S| - (|A_1| + |A_2| + |A_3|) + (|A_1 \cap A_2| + |A_2 \cap A_3| + |A_3 \cap A_1|) - |A_1 \cap A_2 \cap A_3|$$

- $|S| = {}^{10+3-1}C_{10} = {}^{12}C_{10} = 66.$

$|A_1| = ?$ | $T^* = 10$, a repeats atleast 4,
→ T^* with remaining others (more a, b & c) are 6 [10-4]

$\Rightarrow |A_1| = {}^{6+3-1}C_6 = {}^{8}C_6 = 28.$
$\Rightarrow |A_2| = {}^{5+3-1}C_5 = {}^{7}C_5 = 21$
$\Rightarrow |A_3| = {}^{4+3-1}C_4 = {}^{6}C_4 = 15$
$\Rightarrow |A_1 \cap A_2| = {}^{1+3-1}C_1 = {}^{3}C_1 = 3$
$\Rightarrow |A_2 \cap A_3| = 0$
$\Rightarrow |A_3 \cap A_1| = {}^{0+3-1}C_0 = 1$
$\Rightarrow |A_1 \cap A_2 \cap A_3| = 0.$

$$|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3| = 66 - (28+21+15) + (3+0+1) - (0)$$
$$= 70 - 64 = \boxed{6}$$

Different ways of Counting

Derangement

Letters → M A D I S O N

□	□	□	□	□	□	□

hats ○ ○ ○ . . . ○ n

heads □ □ □ . . □ n

A derangement of $\{1, 2, 3, \ldots n\}$ is a permutation $i_1, i_2, \ldots i_n$ and $\{1, 2, 3, \ldots n\}$ such that $i_1 \neq 1$, $i_2 \neq 2$ $\ldots$ $i_n \neq n$ no integer is in its natural position.

D_n = derangement of $\{1, 2, 3, \ldots n\}$.

$D_1 = 0$

$D_2 = 1 \rightarrow \begin{matrix} 2 & 1 \\ \_ & \_ \end{matrix}$

$D_3 = 2 \leftarrow \begin{matrix} 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix}$

$D_4 = 9.$

Orion
PAGE:
DATE: / /

Theorem

For $n \geq 1$

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right)$$

Eg. In a party → n-Men
n-women

1. All permutation of Women + Men = $n!$ (Any woman can choose any partner for 1st dance.)

2. 2nd dance → ways of choosing partner such that partner is diff from what it was in 1st dance
$= D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} + \cdots + (-1)^n \frac{1}{n!}\right)$.

Eg. n Men, n Women → each wearing hat.
All mixed.
2 Restrictions → 1. Male gets male hat, female gets female hat.
2. No one gets their own hat.
No. of possible ways?
$D_n \times D_n$; $n! \times n!$

GENERATING FUNCTIONS

17/11/16

Let $h_0, h_1, h_2, \ldots, h_n, \ldots$ be an ∞ sequence.
Its generating function is defined to be the ∞ series:
$g(x) = h_0 + h_1 x + h_2 x^2 + \cdots + h_n x^n + \cdots$

The coeff. of x^n in $g(x)$ is n^{th} term h_n, thus x^n is the placeholder of h^n.

A finite seq: $h_0 + h_1 x + \cdots + h_m x^m$ can be treated as
$g(x) = h_0 + h_1 x + \cdots + h_m x + 0 \cdot x^{m+1} + 0 \cdot x^{m+2} + \cdots$

GF - Galois Field
gf - generating func^n.

Orion
PAGE:
DATE: / /

Ex. 1 Find the gf of infinite sequence $1, 1, 1, \ldots 1, \ldots$

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

Ex. 2 gf of binomial coefficients ${}^mC_0, {}^mC_1, \ldots, {}^mC_m$

$$g(x) = {}^mC_0 + {}^mC_1 x + {}^mC_2 x^2 + \ldots + {}^mC_m x^m$$
$$g(x) = (1+x)^m$$

Ex. 3 For what sequence is $(1+x+x^2+x^3+x^4+x^5)(1+x+x^2)(1+x+x^2+x^3+x^4)$ the gf?

Let $x^{e_1}\ (0 \le e_1 \le 5)$, $x^{e_2}\ (0 \le e_2 \le 2)$, $x^{e_3}\ (0 \le e_3 \le 4)$

$x^{e_1} \cdot x^{e_2} \cdot x^{e_3} = x^n$ provided $e_1 + e_2 + e_3 = n$.

$h_n = 0$ if $n > 5+2+4$

$\Rightarrow n > 11$

$h_0 + h_1 x + \ldots + h_{11} x^{11} + \underbrace{\ldots}_{0}$

Ex. 4 Determine the generating f^n for the number of n-combinations of apples, bananas, oranges & pears where in each combination

the no. of apple - even
bananas - odd
oranges - 0-4
pears - at least one

$$g(x) = (1 + x^2 + x^4 + \ldots)(x + x^3 + x^5 + \ldots)(1 + x + x^2 + x^3 + x^4)(x + x^2 + x^3 + \ldots)$$

Orion
PAGE:
DATE: / /

$$= \frac{1}{1-x^2} \times \frac{x}{1-x^2} \times \frac{1-x^5}{1-x} \times \frac{x}{1-x}$$

$$= \frac{(x^2)(1-x^5)}{(1-x^2)^2(1-x)^2}$$

the coefficients of Taylor series of this function count the combinations of the given problem.

Recurrence and Generating Functions

$$(1-rx)^{-n} = \sum_{k=0}^{\infty} \binom{n}{k} (-rx)^k$$

$$\frac{1}{(1-rx)^n} = \sum_{k=0}^{\infty} (-1)^k \binom{n}{k} r^k x^k$$

$$= \boxed{\sum {}^{n+k-1}C_k \, r^k x^k}$$

Ex: Determine the gf for the sequence of squares
$0, 1, 4, \ldots, n^2, \ldots$

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

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

$(1-x)^2 \to 2x(1-x) \to 1+x$

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

$$\frac{x(1+x)}{(1-x)^3} = 0 + x + 2^2 x^2 + 3^2 x^3 + \ldots + n^2 x^n + \ldots$$

$$\Rightarrow \boxed{g(x) = \frac{x(1+x)}{(1-x)^3}}$$

Orion
PAGE:
DATE: / /

Ex: Solve the recurrence relation

$h_n = 5h_{n-1} - 6h_{n-2}$ $\quad n \geq 2,\ h_0 = 1,\ h_1 = -2$

$h_n - 5h_{n-1} + 6h_{n-2} = 0$

Let $g(x) = h_0 + h_1 x + h_2 x^2 + \dots + h_n x^n$

$-5x\, g(x) = -5h_0 x - 5h_1 x^2 - \dots - 5h_{n-1} x^n - 5h_n x^{n+1}$

$+6x^2 g(x) = 6h_0 x^2 + \dots + 6h_{n-2} x^n + 6h_{n-1} x^{n+1} + 6h_n x^{n+2}$

Add

$(1 - 5x + 6x^2) g(x) = h_0 + (h_1 - 5h_0)x + (h_2 - 5h_1 + 6h_0)x^2 + \dots$
$\dots + (h_n - 5h_{n-1} + 6h_{n-2})x^n + (6h_{n-1} - 5h_n)x^{n+1} + 6h_n x^{n+2}$

$h_0 = 1$, $h_1 = -2$ } initial condn

$(1 - 5x + 6x^2) g(x) = h_0 + (h_1 - 5h_0)x = 1 - 7x$

$g(x) = \dfrac{1 - 7x}{1 - 5x + 6x^2} = \dfrac{1 - 7x}{(1 - 2x)(1 - 3x)}$

$= \dfrac{c_1}{1 - 2x} + \dfrac{c_2}{1 - 3x}$

$c_1 + c_2 = 1$

$-3c_1 + 2c_2 = -7$ $\Rightarrow c_1 = 5,\ c_2 = 4$

$g(x) = \dfrac{5}{1 - 2x} - \dfrac{4}{1 - 3x}$

$= 5(1 + 2x + 2^2 x^2 + \dots + 2^n x^n + \dots) - 4(1 + 3x + 3^2 x^2 + \dots + 3^n x^n + \dots)$

$= 1 + (-2)x + (5 \cdot 2^2 - 4 \cdot 3^2)x^2 + \dots + (5 \cdot 2^n - 4 \cdot 3^n)x^n + \dots$

$h_n = 5 \cdot 2^n - 4 \cdot 3^n$.

$\dfrac{p(x)}{q(x)} = \dfrac{\text{order of } p(x) < k}{\text{order of } q(x) = k}$

$\dfrac{c}{(1 - rx)^t}$

Orion
PAGE:
DATE: / /

Exponential Generating Function

Theorem. Let S be the multiset $\{n_1 a_1, n_2 a_2, \ldots, n_k a_k\}$.
Let h_n be the no. of permutation of S

Then exponential gf $g^{(e)}(x)$ for the seq^n
$h_0, h_1, \ldots, h_n, \ldots$

is

$$g^{(e)}(x) = f_{n_1}(x)\, f_{n_2}(x) \cdots f_{n_k}(x)$$

where $f_{n_i}(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{n_i}}{n_i!}$