Discrete Mathematics

Benny George K

Department of Computer Science and Engineering

Indian Institute of Technology Guwahati

ben@iitg.ernet.in

September 22, 2011

Elementary Concepts

Let A and B be sets. Let A_i, $i \in \mathcal{I}$ be an indexed family of sets, i.e. for each $i \in \mathcal{I}$ we have sets A_i (Assume $\mathcal{I} \neq \emptyset$)

- Union
$$A \cup B \triangleq \{x | x \in A \text{ or } x \in B\}$$
$$\bigcup_{i \in \mathcal{I}} A_i \triangleq \{x | \exists j, x \in A_j\}$$
- Intersection
$$A \cap B \triangleq \{x | x \in A \text{ and } x \in B\}$$
$$\bigcap_{i \in \mathcal{I}} A_i \triangleq \{x | \forall j, x \in A_j\}$$
- Set Difference (Also written as $A - B$ and called as relative compliment of B relative to A and shortened as B^c when A is clear from the context)
$$A \setminus B \triangleq \{x | x \in A \text{ and } x \notin B\}$$

Elementary Concepts

- Symmetric Difference

$$A \oplus B \triangleq (A \setminus B) \cup (B \setminus A)$$

- Power set of a set S (Written as $\mathcal{P}(S)$ or 2^S)

$$\mathcal{P}(S) \triangleq \{x | x \subseteq S\}$$

- DeMorgan's rule.

$$(A \cup B)^c = A^c \cap B^c$$

$$(A \cap B)^c = A^c \cup B^c$$

Finite and infinite set.

- For any given set A, define A^+ called successor of A as below.

$$A^+ \triangleq A \cup \{A\}$$

- We can start with the empty set $\emptyset$, repeatedly apply the successor operation and construct a sequence of sets.
- The first few sets in this sequence will be $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \ldots$
- We shall name these sets as $0, 1, 2, 3, \ldots$
- Let us now define the set $\mathbb{N}$ to be the set which
  - contains 0.
  - Whenever it contains the element A, it contains A^+ as well.
- $\mathbb{N}$ constructed as above is an "infinite" set but we will formally define that term in the next page.

Finite and Infinite Sets

- A set S is said to be finite if there is a bijection (one to one correspondence) between S and and element of $\mathbb{N}$.
- n is said to be the cardinality or *size* of the set S and is denoted by $|S|$.
- A set S is said to be infinite if it is not finite.
- A set S is said to be countably infinite if there exists a bijection between S and $\mathbb{N}$.
- A set S is said to be countable or enumerable if it is finite or countably infinite. (e.g. $\mathbb{Z}, \mathbb{Q}$).
- A set is said to be uncountable if it is not countable. (e.g. $\mathbb{R}, [0,1]$, set of irrationals etc.)
- We say that two sets S_1 and S_2 are of same cardinality if there is a bijection from S_1 to S_2.

Cardinality of sets

Integers($\mathbb{Z}$) form a countable set

Consider the map f from $\mathbb{Z}$ to $\mathbb{N}$ given by $f(x) = 2x$ if $x \geq 0$ and $f(x) = 2x - 1$ if $x < 0$.

Rationals form a countable set.

Every positive rational number is of the form $p/q, q \neq 0$. List the rationals in increasing order of $p + q$. (We can do this because there are only finitely many positive integral solutions for the equation $p + q = k$ for any fixed k). Negative rationals can be similarly enumerated then can combine these enumerations as we did for integers.

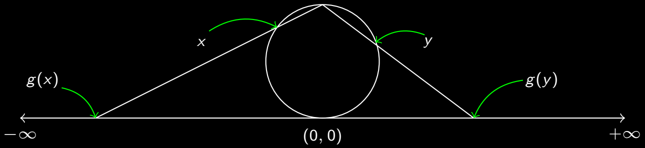
Finite subsets of $\mathbb{N}$ is a countable set.

Enumerate in the increasing order of sum of elements in the subset.

Cardinality of $\mathbb{R}$

Power set of $\mathbb{N}$ is of the same cardinality as $\mathbb{R}$

- We need to exhibit a bijection from $\mathcal{P}(\mathbb{N})$ to $\mathbb{R}$.
- We shall first exhibit a bijection f from $\mathcal{P}(\mathbb{N})$ to $[0,1]$ and then a bijection g from $[0,1]$ to $\mathbb{R}$. $(g \circ f)$ will then be a bijection from $\mathcal{P}(\mathbb{N})$ to $\mathbb{R}$.
- Verify that $f(S) = \sum_{s \in S} 2^{-s}$ is a bijection from $\mathcal{P}(\mathbb{N})$ to $\mathbb{R}$
- The diagram below shows a bijection between $[0,1]$ and $\mathbb{R}$. The circle in the diagram is the [0,1] interval rolled into a circle.



Cantor's theorem

Theorem

Cardinality of $\mathbb{N}$ is not the same as the cardinality of $\mathbb{R}$

Proof

(We will show that there are no bijections from $\mathbb{N}$ to $[0, 1]$).

- For contradiction assume that f is a bijection from $\mathbb{N}$ to $[0, 1]$.
- Let for $n \in \mathbb{N}$, $f(n) = 0.a_{n,1}a_{n,2}a_{n,3}\ldots$ where $a_{n,i}$ stands for the ith digit in the decimal expansion of $f(n)$.
- Consider the number $d = d_1 d_2 d_3 \ldots$ where $d_i = a_{i_i} + 5$
- For each i, $f(i)$ differs from d in the ith digit. Thus d is not the image of any $n \in \mathbb{N}$. Thus f is not a bijection. $\square$

- Cardinality of $\mathbb{N}$ is written as $\aleph_0$ (read as alpeh not).
- Cardinality of $\mathbb{R}$ is written as $\aleph_1$ (read as alpeh one).

Cantor's Theorem

Theorem

For every set S, there is not bijection from S to $\mathcal{P}(S)$

Proof

- For contradiction, assume that f is bijection from S to $\mathcal{P}(S)$.
- For every $s \in S$, $f(s)$ is a subset of S. $f(s)$ may or may not contain the element s.
- Collect all the elements d from S such that the image of d does not contain d and call this set as D.
- Symbolically, $D \triangleq \{d | d \notin f(d)\}$
- Notice that D cannot be the image of any element $x \in S$.
  - $x \in D$ would mean $x \notin f(x) = D$.
  - $x \notin D$ would mean $x \in f(x) = D$. $\square$

Introduction to Propositional Logic

- Propositional Logic is a simple but useful branch of mathematical logic.
- It helps us make inferences about *propositional formulas*.
- Propositions are statements which has a truth value.
- A proposition make take either a truth value $TRUE$ or a truth value $FALSE$.
- We shall denote a proposition symbolically by letters $P, Q, R \ldots$.
- Also we shall abbreviate $TRUTH$ and $FALSE$ to T and F respectively.
- From propositions using connectives, we form more complex statements.

Propositional Connectives

Below we give a list of commonly used propositional connectives and their meanings.

Connective	Usage	Meaning
Negation	$\neg P$	Is true if and only if P is false
Conjunction	$P \wedge Q$	Is true if and only if both P and Q are true
Disjunction	$P \vee Q$	Is false if and only if both P and Q are false
Implication	$P \Rightarrow Q$	Is false if and only if P is true and Q is false
Equivalence	$P \Leftrightarrow Q$	Is true if and only if P and Q has same truth values.

- Implication is also referred to as conditional.
- The meaning of each propositional connective can be summarized in a truthtable.

Truth tables for connectives

P	Q	$\neg P$	$P \vee Q$	$P \wedge Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
T	T	F	T	T	T	T
T	F	F	T	F	F	F
F	T	T	T	F	T	F
F	F	T	F	F	T	T

- Total number of possible connectives on two propostional symbols is $2^4 = 16$.
- Total number of possible connectives on m propostional symbols is 2^{2^m}.

Propositional Formulas and Structural Induction

Using propositional connectives and any set of propositional symbols S we can produce a lot of formulas.

The set of formulas $\mathcal{F}$ consists of

- All the elements in S as well as T and F are in $\mathcal{F}$.
- Let φ and ψ be elements of $\mathcal{F}$ then $(\neg\varphi), (\varphi \vee \psi), (\varphi \wedge \psi)$, $(\varphi \Rightarrow \psi)$ and$(\varphi \Leftrightarrow \psi)$ are also elements of $\mathcal{F}$

To prove theorems about set of formulae, we use principle of structural inductio

Structural Induction

If $A \subseteq \mathcal{F}$ satisfies the following conditions then $A = \mathcal{F}$

- A contains all the propositional symbols as well as T and F.
- If $\alpha, \beta \in A$, then $(\neg\alpha), (\alpha \vee \beta), (\alpha \wedge \beta)$, $(\alpha \Rightarrow \beta)$ and$(\alpha \Leftrightarrow \beta)$ are also elements of A

Introduction

- Binary operation
  A binary operation from a set A to a set B is a function which assigns for each ordered pair of A a unique element in B. Mathematically this is written as below

$$f : A \times A \mapsto B$$

- Examples
  - Addition: $+_{\mathbb{N}} : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$
  - Addition: $+_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \mapsto \mathbb{Q}$
    We use the subscripts under the operation to emphasize the fact that $+$ on $\mathbb{N}$ and $\mathbb{Q}$ are two different functions.
  - Minimum: $\texttt{min}{:}\mathbb{Q} \times \mathbb{Q} \mapsto \mathbb{Q}$
  - Multiplication, division, subtraction, exponentiation, Maximum, Concatenation ...

Properties of operations

Let us consider a binary operations

$$\star : A \times A \mapsto B$$

- Closure: $\star$ is said to be *closed* if the set B is equal to A.
- Associativity: Parentheses doesn't matter.
  $((a \star b) \star c) = (a \star (b \star c))$
- Commutativity: Order doesn't matter. $a \star b = b \star a$
- Existence of Identity: A special element e for every a

  $$e \star a = a \;\text{ (left identity)}$$
  $$a \star e = a \;\text{ (right identity)}$$

  If the left identity and the right identity both exist, then they must be the same (Why?) and it is called simply the *identity*.
- Existence of Inverse An element a^{-1} associated with each a

  $$a^{-1} \star a = e \;\text{ (left inverse of a)}$$
  $$a \star a^{-1} = e \;\text{ (right inverse of a)}$$

Algebraic structures

- A set A equipped with a collection of operators is called an algebraic structure. We shall assume that the operations are all binary operations.

Let $\mathcal{A} = (A, \star)$ be an algebraic structure.

- If $\star$ is closed and associative then $\mathcal{A}$ is a semigroup. e.g., Set of non empty strings with the concatenation operation
- If $\star$ is closed, associative and has an identity then $\mathcal{A}$ is a monoid. e.g., Set of non strings including the empty string with the concatenation operation
- If $\star$ is closed, associative, has an identity and has inverse then $\mathcal{A}$ is a group. e.g., $n \times n$ invertible matrices under matrix multiplication
- If $\star$ is closed, associative, has an identity, has inverse and is commutative then $\mathcal{A}$ is an abelian group. e.g., Integers under addition.

Generators

Let $\mathcal{A} = (A, \star)$ be an algebraic structure such that $\star$ is closed. For $B \subseteq A$, define a set sequence of sets $B_0, B_1, B_2, \ldots$ as below

$$\begin{aligned} B_0 &\triangleq B \\ B_1 &\triangleq \{b | b = b_i \star b_j \text{ where } b_i, b_j \in B_0\} \cup B_0 \\ &\vdots \\ B_{i+1} &\triangleq \{b | b = b_i \star b_j \text{ where } b_i, b_j \in B_i\} \cup B_i \end{aligned}$$

- The set B^* defined as

$$B^* \triangleq \bigcup_{i \in \mathbb{N}} B_i$$

is called as the *set generated by* B. Moreover if $B^* = A$, the B is called the *generator* of A.

Generators

- If $\star$ is an operation such that inverses are well defined then in addition to elements of the form $b_i \star b_j$ we add b^{-1} as well in the process of "generation".

Additive chains

An *additive chain* ending in a n is a sequence $a_1, a_2, \ldots, a_m$ such that for every $1 < i \leq m$, $a_i = a_j + a_k$ where $j, k < i$ and $a_m = n$. m is called the *length* of the chain

Open question

Given an n find the chain of smallest length ending in n.

Subgroup

- Let $(A, \star)$ be a group and let $B \subseteq A$. B is a subgroup of A if B is a group.
- Given set B how do we check if it forms a subgroup of A?
- We need to verify closure, associativity, existence identity and existence of inverse.
- Associativity comes for free.
- Identity of A must be the identity of B. (Why?)
- Inverse of an element in B must exist and be the same as its inverse in the group A. (Why?)

Subgroup

Subgroup criterion

A subset B of a group $(A, \star)$ is a subgroup if and only if

- $B \neq \emptyset$
- For every $x, y \in B,\ x \star y^{-1} \in B$

Proof

- Since B is non empty there must exist an element x. Since $x \star x^{-1}$, the identity of A (therefore the identity B as well) must be present in B.
- Take x to be the identity of A and y any element of B. Thus $e \star y^{-1} = y^{-1}$ is present in B.
- Let $a, b \in B$. Take $x = a$ and $y = b^{-1}$. Since $(b^{-1})^{-1} = b$ we can conclude that $a \star (b^{-1})^{-1} = a \star b \in B$

Cyclic groups

- A group whose generator is a singleton set is called a cyclic group.

Lemma

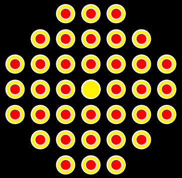
Every finite cyclic group is commutative.

Proof

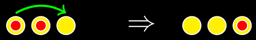
Let G be a finite cyclic group. Let g be the element in it's singleton generator. Therefore G is of the form $\{g^1, g^2, \ldots g^r\}$ where $g^r = \underbrace{g \star \ldots \star g}_{r\ \ times}$. The lemma follows from the fact that

$$g^i \star g^j = g^{i+j} = g^j \star g^i$$

An application of group theory.



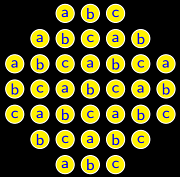
The diagram of left shows a solitaire game. The red circle inside a yellow circle denotes a position of the board with a marble.



- An allowed move is shown in the diagram above. A marble can jump over an adjacent marble (as indicated by the green arrow in figure).
- While jumping over a marble, one should remove that marble. Jumping may be done left to right, right to left, top to bottom and bottom to top.
- The resulting position after the jump in the example is shown on the right of the $\Rightarrow$.
- Can one reach a board configuration with a single marble?

Klein four group

- We shall show that it is impossible to reach a configuration with single coin.
- We will use the Klein four group (K_4) for this purpose.
- K_4 is defined on $\{a, b, c, e\}$. The operation $\star$ is defined as
  - $a \star a = b \star b = c \star c = e$
  - K_4 is commutative.
  - e is the identity.
  - $a \star b = c, b \star c = a, c \star a = b$



- We will mark each yellow circle in the solitaire game described earlier by an element of K_4 as shown in figure above.
- Define value of a configuration to be product of elements at all the circles with marbles (red dots) in it.

Impossibility proof

- Note that the initial value of the board is $a^{12} \star b^{12} \star c^{12}$
- Each move changes the contents of exactly 3 yellow circles.
- Since any move involves 3 consecutive circles, they must be labeled using a, b and c.
- The contribution of these circles to the value of the board before the jump move is one among $\{a \star b = c, b \star c = a, c \star a = b\}$.
- Note that the contribution of these circles to the value of the board after the jump move is the same as its contribution before the jump move i.e. Value of the board is invariant under allowable moves. It will be e.
- No configuration having a single marble on board can have a board value of e. $\square$

Order

- The order of a group G denoted by $|G|$ or $ord\{G\}$ is the number of elements in the underlying set.
- The order of a element g of a group G denoted by $ord\{g\}$ is the smallest positive number n such that g^n is equal to the identity of G. When is is no such positive integer then we say that the order is infinite.
- The set $\{0, 1, \ldots, 9\}$ forms a group under modulo 10 addition. The order of this group is 10. The order of 5 is 1 and the order of 3 is 10.

Lagrange's Theorem

Theorem

Let G be a finite group and H be a subgroup of G. $|H|$ divides $|G|$.

Proof

- Let $g \in G$. The subsets gH and Hg defined as below are the left and right coset of H w.r.t. g.

$$gH \triangleq \{gh|h \in H\}, \; Hg \triangleq \{hg|h \in H\}$$

- Every coset of H has size $|H|$. (if $h_1 \neq h_2$ then $gh_1 \neq gh_2$.)
- If $g_1 H \cap g_2 H \neq \emptyset$, $\exists h_1, h_2 \in H$ such that $g_1 h_1 = g_2 h_2$.
- Since H is a group and $h_1, h_2 \in H$, $g_1 = g_2 h_2 h_1^{-1}$.
- $\therefore \forall h \in H, g_1 h = g_2 h_2 h_1^{-1} h = g_2 h_3,$ for some $h_3 \in H$
- $\therefore g_1 H \subseteq g_2 H$. But as all cosets are of size $|H|$, $g_1 H = g_2 H$
- In other words, there cannot be overlapping cosets unless they are one and the same.

Lagrange's Theorem

Proof (Contd.)

- The union of all distinct cosets of H (overlapping cosets accounted only once) is G as H contains the identity.
- $\therefore$ number of distinct cosets $\times$ size of a coset $= |G|$
- Size of a coset $= |H|$. Thus we have

$$|H| = \frac{|G|}{\text{number of distinct cosets}}$$

$\square$

Symmetric Group S_Ω

- Let Ω be any non empty set. Let S_Ω be the set of all one to one and onto functions (bijections) from Ω to itself. S_Ω forms a group under function composition.
- Suppose $\Omega = \{1, 2, \ldots, n\} = [n]$. Then S_Ω is also referred to as the symmetric group of degree n written as S_n.
- A particular element of S_n can be written as below ($n = 8$).

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 3 & 2 & 4 & 5 & 1 & 8 & 7 \end{pmatrix}$$

- The above representation denotes a function σ where $\sigma(1) = 6, \sigma(2) = 3, \sigma(3) = 2, \sigma(4) = 4, \sigma(5) = 5,$ $\sigma(6) = 1, \sigma(7) = 8 \text{and} \sigma(8) = 7.$

Example S_3

The elements of S_3 are as follows

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

- Note that $\sigma_2(\sigma_3(1)) = 3, \sigma_2(\sigma_3(2)) = 1$ & $\sigma_2(\sigma_3(3)) = 2$
- If we denote the group operation by $\circ$, $\sigma_2 \circ \sigma_3 = \sigma_5$
- As $\sigma_3 \circ \sigma_2 = \sigma_4$, We know that S_3 is not an Abelian group.

Cycle Representation

- Instead of writing an element of S_n in two rows, we may represent it using cycles.
- Consider the permutation σ given below

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 3 & 5 & 4 & 2 & 1 & 8 & 7 & 9 \end{pmatrix}$$

- $\sigma(1) = 6, \sigma(6) = 1$. (This completes a cycle)
- Further, $\sigma(2) = 3, \sigma(3) = 5, \sigma(5) = 2$
- Continuing this way, σ can be broken down into cycles and written as follows $(1, 6), (2, 3, 5), (4), (7, 8)(9)$
- Each $(a_1, a_2, \ldots, a_k)$ denotes a cycle such that $\sigma(a_i) = a_{i+1}$ for all i except k. and $\sigma(a_k) = a_1$.
- We will remove the cycles of length 1, for example in σ given above we shall remove the cycles (4) and (9)
- The representation obtained is called the cycle representation.

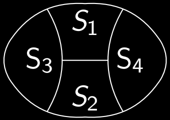
Cycle Representation (Algorithm)

1. From $[n]$ pick the smallest element a which has not yet appeared in any cycle.
2. Add a as the starting element of a new cycle.
3. Compute the value $\sigma(x)$ where x the most recently added element of the cycle and repeat this till the cycle closes. Return to step 1 after cycle closes.
4. Remove cycles of length 1.

Remark: Let n be a permutation of $[n]$. $ord(n)$ will be equal to the l.c.m of the length of cycles in the cycles representation of σ.

Equivalence Relation and Partitions

- Given a set S, A partition of S is set of disjoint subsets of S such that their union is S.



- In Figure above, the set S is shown partitioned into 4 parts.
- An equivalence relation R is a binary relation defined on a set S such that S is
  - *reflexive*: aRa for all $a \in S$.
  - *symmetric*: If aRb then bRa.
  - *transitive*: If aRb and bRc then aRc .
- Partitions and Equivalence relations are one and the same thing.

Equivalence Relations and Partitions

- Given a partition P of S define a relation R such that aRb if and only if a and b belong to the same disjoint subset in the partition P. Verify that this relation R is indeed an equivalence relation.
- Conversely, given an equivalence relation R on a set S, we can define a partition in the following way.
  - For each element a define R_a to be the set of all elements b such that aRb. R_a is called the equivalence class of a.
  - Note that every element is in some equivalence class.
  - Also if two equivalence classes R_a and R_b have an overlap, then one can easily show that $R_a = R_b$ as R is an equivalence relation.
  - The set of all equivalence classes of elements in S thus forms a partition of S.

Homomorphism and Isomorphism

- Let $(G, \star)$ and $(H, \circ)$. be groups. Any function f from G to H such that for all $g_1, g_2 \in G$, $f(g_1 \star g_2) = f(g_1) \circ f(g_2)$ is called a homomorphism.
- For each $h \in H$, all the elements of G mapping to h forms the fiber of f over h.
- For example, the map $x \mapsto e^x$ is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$ because $e^{x+y} = e^x e^y$. ($\mathbb{R}^+$ denotes the set of positive reals.)
- If f is a bijection then the homomorphism becomes an isomorphism.
- f maps the identity of G to the identity of H. $(f(e) \circ f(e) = f(e \star e) = f(e)$. Cancel $(f(e)$ from both sides.)
- Image of the inverse equals the inverse of the image, i.e. $f(x^{-1}) = f(x)^{-1}$. (As $f(x) \circ f(x^{-1}) = f(x \star x^{-1}) = f(e)$)
- Kernel of f is the set of all a such that $f(a) =$ identity of H.

More on Homomorphisms

Theorem

Kernel of f denoted by $Ker(f)$ is a subgroup of G and image of G under f is a subgroup of H.

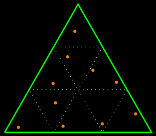
Proof

For any $x, y \in G$ and a homomorphism f,we have $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1}$. Let e_1 be the identity in G and e_2 the identity in H
Consider $x, y \in Ker$. Thus $f(x) = f(y) = f(y)^{-1} = e_1$.
$\therefore f(xy^{-1}) = f(x)f(y)^{-1} = e$. Thus $Ker(f)$ is a group.
Consider $x, y \in$ Image of G Thus $\exists x', y' inG$ such that $f(x') = x$ and $f(y') = y$. Note that $f(x'y'^{-1} = xy^{-1}$ Thus $xy^{-1} \in$ Image of G. Thus image of G is a group.

Quotient Group

- Let f be a homomorphism with K as its kernel. The quotient group G/K (read as G mod K) is the group consisting of fibers of f.
- Suppose G_1 is the fiber above $f(g_1)$ and G_2 the fiber above $f(g_2)$, then the product in G/K is computed by defining G_1G_2 to be the fiber above $f(g_1g_2)$. (Verify that this definition is well defined as f is homomorphism)
- $GL_n(\mathbb{R})$ be the group of all invertible $n \times n$ matrices. Consider the map from $GL_n(\mathbb{R})$ to $\mathbb{R} \setminus \{0\}$ given by $f : A \mapsto det(A)$ where $det(A)$ denotes the determinant of A.
- $Ker(f)$ is all $n \times n$ matrices with determinant one. Fibers are all matrices with determinant $c, c \in \mathbb{R} \setminus \{0\}$

Pigeon Hole Principle



Let 10 points be randomly chosen from an equilateral triangle of side 3. Show that there will be two point within distance 1 cm of each other.

- Observe that there must be at least one small triangle which contains 2 points.
- These points must be within 1 cm of each other.

Pigeon Hole Principle

Suppose there are n objects to be distributed into $n-1$ boxes, then there exists a box with contains more than one object.

Generalized Pigeon Hole Principle

Suppose there are $q_1 + q_2 + \ldots + q_n - n + 1$ objects to be distributed into n boxes,then there exists an i such that the ith box contain at least q_i objects in it.

Applications of PHP

- In every set of people (with more than two people) there exists two persons with same number of friends.

Proof

- Let the set have n people.
- If there is a person with no friends there cannot be a person who friends with everyone.
- If there is a person who is friends with everyone there cannot be a person without friends.
- Thus the number of friends each person can have is either from the set $\{0, 1, \ldots, n-2\}$ or from the set $\{1, \ldots, n-1\}$. In either case the number of distinct elements in the set is $n-1$. Therefore one element must repeat. $\square$

Applications of PHP

Erdös Szekeres Theorem

Every sequence of length $n^2 + 1$ contains a monotone subsequence of length $n + 1$.

Proof

- Let $a_1, a_2, \dots a_{n^2+1}$ be the series we are considering.
- Let m_i denote the length of the maximal increasing sequence starting from the element a_i
- If any m_i is greater than n we have a monotone subsequence of length $n + 1$. So let us assume that every m_i is less than or equal to n.
- Since there are $n^2 + 1$ different m_i, taking values 1 to n, there must exist an L such that $n + 1$ of the m_is takes the value L.

Erdös Szekeres Theorem (Proof)

- Consider the a_is with $m_i = L$.
- Let us write these elements as $b_1, b_2, \ldots, b_k$ (Note that $k \geq n+1$). without changing the order in which they appear in the original sequence.
- If $b_s < b_{s+1}$ for any s, then consider the maximal monotonic increasing sequence starting at b_{s+1} (which is of length L). We can append b_s to the start of this sequence to get an increasing monotonic sequence of length $L+1$ starting at b_s.
- This contradicts the assumption that the maximal increasing monotonic sequence starting at b_s is of length L.
- Thus we have $b_s \geq b_{s+1}$ for all s.
- Considering b_is , we have obtained a monotonic decreasing sequence of length at least $n+1$ $\square$

Principle of Mathematical Induction

Weak Induction

Let $P(n)$ be statement about a natural number n such that

- Base: $P(1)$ is true.
- Induction: $P(n+1)$ true whenever $P(n)$ is true

Then $P(n)$ is true for all $n \in \mathbb{N}$

Strong Induction

Let $P(n)$ be statement about a natural number n such that

- Base: $P(1)$ is true.
- Induction: $P(n+1)$ true whenever $P(m)$ is true for $m \leq n$

Then $P(n)$ is true for all $n \in \mathbb{N}$

Incorrect use of PMI

(Pseudo)Theorem: All horses are of the same color.

(Pseudo) Proof:

$P(n) \triangleq$ Any set of containing n horses have horses of identical color.

- Base case: For $n = 1$ the statement $P(n)$ is certainly true.
- Induction case: Assume that $P(k)$ is true for some k. Now consider a set of $k + 1$ horses.
- The horses numbered 1 to k forms a set of k horses. They are all of the same color say c. In particular the horse numbered k is of color c.
- The horses numbered 2 to $k + 1$ forms a set of k horses. They are all of the same color as the horse numbered k *i.e.* c. Thus all the horses are of the same color.

Question: Where is the mistake in the above "proof"?

Well Ordering Principle

Every non empty subset of $\mathbb{N}$ has a smallest element.

- Well ordering principle is equivalent to PMI.
- We shall first prove that PMI $\Rightarrow$ WOP using strong induction.

$$\mathrm{P}(n) \triangleq \text{Every subset of } \mathbb{N} \text{ containing } n \text{ has a least element}$$

- Base:1 is certainly the least element of any subset of $\mathbb{N}$ containing 1. Thus $P(1)$ is true.
- Induction: Consider any set S containing $k+1$.
- If S contains any element, say m, smaller than $k+1$, then by strong induction,as $P(m)$ is true, we know that S contains a least element.
- If S didn't contain any element smaller than $k+1$, then S contains a smallest element, namely $k+1$. Thus $P(k+1)$ is true. $\square$

Well Ordering Principle

- We shall now show the reverse direction namely WOP $\Rightarrow$ PMI.
- For contradiction, let us assume that there is a property P such that
  - $P(1)$ is true and whenever $P(k)$ is true, $P(k+1)$ is also true.
  - There exists a number m such that $P(m)$ is false.
- Let $S \triangleq \{x \in \mathbb{N} | P(x) \text{ is false}\}$.
- Since $m \in S$, S is a non empty subset of $\mathbb{N}$ and thus has a least element say s.
- $s \neq 1$ because $P(1)$ is true. Since s is the least element of S, $s - 1 \notin S$.
- $\therefore P(s-1)$ is true. But then $P((s-1)+1)$ must also be true and thus $s \notin S$. $\square$

Topics

- Introduction Definitions
- Eulerian Cycles
- Hamiltonian Cycles
- Tournament Graphs
- Minimal Spanning Trees