Variable

If a quantifier is used on a variable x we say that x is bound. If no quantifier is used on a variable it is called free.

ex: $P(x,y)$ $\quad x \to$ bound $\quad y \to$ free

We can use negation for quantified expressions.

Let $P(x)$ be a predicate.

$\sim \forall x\, P(x) \equiv \exists x \sim P(x)$

$\sim \exists x\, P(x) \equiv \forall x \sim P(x)$

Proofs

A theorem is a statement that can be shown to be true via proof.

A proof is a sequence of statements that form an argument.

Axioms are statement taken to be self evident or assumed to be true.

A lemma is a theorem useful within the proof of a theorem.

A corollary is a theorem that can be established from theorem that has just been proved.

A proposition is a less important theorem.

A conjecture is a statement whose truth value is not known.

The rules of inference are the means used to draw conclusion from other assertion ~~assertion~~ to derive an argument / proof.

Rules of reference

- If p is true & $p \to q$, then q is true.
  $((p \wedge (p \to q)) \to q$ is tautology
- If q is false & $p \to q$ then p is false
  $(\sim q \wedge (p \to q)) \to \sim p$
- If $p \to q$ & $q \to r$ then $p \to r$
  $((p \to q) \wedge (q \to r)) \to (p \to r)$
- If either p or q is true & p is false then q is true
  $((p \vee q) \wedge \sim p) \to q$
- If p or q is true & not p or r is true then q or r is true
  $((p \vee q) \wedge (\sim p \vee r)) \to (q \vee r)$

#) Assume that $p \to q$, $r \to s$ & $(r \vee p)$ holds
Assume that q is false, show that s must be true.

Diff^n types of proofs

→ **Trivial proof**: A trivial proof can be given if conclusion is always true. Eg if q is true then $p \to q$ is always true.
- If $x > 0$ $(x+1)^2 = 2x > x^2$

→ **Vacuous Proof**: If p is false, then $p \to q$ is always true.
A vacuous proof is a proof that relies on the fact that no element in the domain satisfies the hypothesis.
- If x is a prime no. divisible by 16 then $x^2 < 0$
  & x is domain.

→ **Direct proof**:
In a direct proof you assume the hypothesis p & give a direct seq^n of implications using rules of inference to show the conclusion holds
- If n is even then n^2 is even & vice versa
  ⇒ Let n be even then $n = 2k$
  $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ ⇒ Even

→ **Proof by contrapositive**
$p \to q \equiv \sim q \to \sim p$
Assume the conclusion is false then give a series of implications show that the hypothesis is also false.
- P.T. if $x^3 < 0$ then $x < 0$
  ⇒ the contrapositive is if $x \geq 0$ $x^3 \geq 0$

→ **Proof by contradiction**
Assume the result is false & then proceed to show that such assumption leads to contradiction.

• Pt. $\sqrt{2}$ is irrational.

⇒ Assume $\sqrt{2}$ is rational.

$\sqrt{2}$ can be written as $\frac{p}{q}$ where $\gcd(p,q)=1$

$2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2$

∴ p^2 is even no ⇒ p is an even no.

$p = 2k$

$4k^2 = 2q^2 \Rightarrow q^2 = 2k^2$

∴ q^2 is even & q is even

Then $\gcd(p,q) \neq 1$.

Hence, $\sqrt{2}$ is irrational.

#) Pt. there exist infinitely many prime numbers. by contradiction

⇒ Assume that there are finite no. of prime numbers.

→ Proof by cases :

Sometimes it is easier to prove a theorem by breaking it down into cases & proving each of them seperately.

• let $n \in \mathbb{Z}$. Prove that $3n^2+3n-2$ is even.

⇒ $3n^2+3n-2 = (3n+2)(3n-1)$

1) let $3n+2$ is odd

$3n+2-3$ is even

$3n-1$ is even.

∴, $3n^2+3n-2$ is even //

→ Existential Proof :

• A constructive existence proof asserts a theorem by providing a specific, concrete example of a statement.

It only proves a statement of the form $\exists x\, P(x)$.

• A non-constructive existence proof also shows a statement of the form $\exists x\, P(x)$ but it doesn't necessarily need to give a specific example of x.

#) $P(x) = x^3+x-1$ has exactly 1 real sol.

⇒ $P(0) = -1 \quad P(1) = 1$

There is one real sol^n between 0 & 1. — Non-constructive

$P'(x) = 3x^2+1$

let us assume $p(x)$ has 2 diff roots say x_1 & x_2.

Then $p(x_1) = p(x_2) = 0$. By Roller theorem $\exists\ c \in (x_1, x_2)$

s.t. $p'(c) = 0$. Which is a contradiction.

so there is only 1 real root.

#) S.t. $\exists$ some n s.t. $(n+1)^2 \leq 2^n$ — Constructive

⇒ Here $n=6$ satisfies the cond^n

#) show that ∃ irrational no. x & y st x^y is rational.

Counter-example ⇒

some times you want to disprove a statement with statement of the form $\forall x P(x)$, it suffices to give a counter example, because the existence of element x for which $\sim P(x)$ which is negation of $\forall x P(x)$.

- How to prove statements like $n \le n^n$ or all $n \in N$?
- Common mistakes known as fallacies

→ Fallacy of affirming conc^n

$(q \wedge (p \to q)) \to p$

→ Fallacy of denying the hypothesis

$(\sim p \wedge (p \to q)) \to \sim q$

→ Circular reasoning

Here we use the conc^n as assumption, avoiding an actual proof.

MATHEMATICAL INDUCTION

Induction (Axiom)

Let P(n) be a property of non-negative integers. If

→ P(0) is true (Base case)

→ for all $k \ge 0$ $P(k) \to P(k+1)$ (Induction step)

then P(n) is true for all non-negative

Theorem ⇒ for all integers $n > 1$ $\ln < n^n$

Proof ⇒ Base case: $n = 2$ $\ln 2 < 2^2$

Suppose for some $n = k > 1$, $\ln k < k^k$

then the induction step

$\ln(k+1) = \ln k + \ln(k+1)$

$< k^k + \ln(k+1)$

$< k^k + (k+1)^k$

$< (k+1)^{k+1}$

Hence, $P(k) \Rightarrow P(k+1)$

∴ It is true for all k

#) Prove by induction

1) $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

2) $1^2 - 2^2 + \dots + (-1)^{n-1} n^2 = (-1)^{n-1} \frac{n(n+1)}{2}$

3) 6 divides $n^3 - n$ when n is a non-negative integer

4) 21 divides $4^{n+1} + 5^{2n-1}$, where n is +ve integer.

Interesting fallacy in using induction

→ All horses have the same colour.

Pnf: The case with one horse is trivial.

→ Assume for $n = k$ & have to prove for $k+1$, eg 1, 2, . . ,

- Let k horses are of same colour
- Need consider 2, . . . , k+1 are also of same colour.
- So 2, . . , k horses have same colour as 1 horse & (k+1) horse. So all horses have same colour

Where is the bug ?

⇒ k=2 step does not hold.

• What is the basis for induction ?

⇒ Well Ordering Principal

Every non-empty set of non-negative integers has a smallest element.

• Theorem : WOP implies Induction.

⇒ Suppose P(i) is true & for each $k \geq 0$ $P(k) \Rightarrow P(k+1)$ but P(k) is not true for all non-negative integer.

Consider $S = \{ i \in \mathbb{N} \mid P(i) \text{ is false} \}$

S is a non-empty set of non-negative integers. Then by WOP, S has a smallest element, say $i_0 > 0$.

Then $P(i_0)$ = false

But $i_0 - 1 \notin S$. so $P(i_0 - 1)$ is true.

Then $P(i_0 - 1) \Rightarrow P(i_0)$ which is a contradiction.

• Theorem : WOP iff Induction ⟶ Prove at home

Strong form of induction

Given a statement P concerning integer n. Suppose (i) P is true for some integer n_0

(ii) If $k \geq n_0$ is any integer & P is true for all integer m in the range $n_0 \leq m \leq k$, then it is also true for k+1.

∴ P is true for all integer $n \geq n_0$.

Proof of algorithm using induction

Consider the following integer algorithm

Input : Non-zero real no. a & non-negative int. n

Procedure : if n=0 return f(a,n) = 1

else f(a,n) = a · f(a,n-1)

i) Prove that the algo computes $f(a,n) = a^n$ for all non-negative integers n=0

⇒

11/1/12

Theorem : Any integer n>1 can be written as a product of primes.

Proof by WOP : Let S be the set of all integer >1 that can not be written as a product of prime numbers.

If S is non-empty, then by WOP, there exists a smallest element in S say n_0.

Then n_0 is not a prime no. so $n_0 = a \cdot b$ where $n_0 > a, b > 1$.

Since $a, b < n_0$ & $a, b \notin S$.

So a & b can be written as product of primes. & correspondingly n_0 can also be written as a product of primes.

∴ S is an empty set.

Proof by induction :

Holds for k=2 (Base case)

Let for $n \geq k$, i.e. $k = p_1 p_2 \ldots p_r$

If (k+1) is a prime, we are done.

But if it is not then $k+1 = a \cdot b$ $a, b > 1$

But a, b need not be equal to k so we need strong induction.

Assume $r \leq k$. r can be written as a product of primes.
Therefore by strong induction $a * b$ can be written as product of primes.
Hence $(k+1)$ can be written as product of primes.

= #) An odd no. of people stand at a mutually distinct distance. Every person throws a ball at their nearest neighbour hitting that person. Use induction to prove that there is atleast one left is not hit by any ball.

⇒ Let $P(n)$ be the statement
"There is a survivor in the ball fight with $2n+1$ people"

Base step : $P(1)$ ⇒ There are 3 people A, B & C. Suppose that among them the closest distance is A & B.
The one who > dist. So A & B throw at each other & C survives.

Assume $P(k)$ as true, i.e, with $(2k+1)$ people there is one survivor.
Consider the fight with $2k+3$ people. Let A & B be the closest pair among these people.

I) They are closest pair so they throw at each other. If someone else throws at one of them, then for remaining $(2k+1)$ people there are only $2k$ balls. So someone survives.

II) If no one else throws a ball at them then $(2k+1)$ people play among themselves. So by induction hypothesis there will be a survivors.

SET

→ A set is an unordered collection of objects. The objects in a set are called its elements.

→ Let P be a property. Any collection of objects that are defined by (or satisfy) P is a set
$S = \{x \mid P(x)\}$
The most common examples of sets are $\mathbb{Z}, \mathbb{N}, \mathbb{R}$ etc.

Properties of Sets

→ Let A & B be 2 set..
→ A & B are equal if they contain the same elements, $A = B$
→ A is said to be a subset of B if every element of A is also an element of B, $A \subseteq B$
→ A set with no elements is called empty set / null set, $A = \emptyset$
→ A set that has one element is called singleton set.
→ The power set of a set S denoted by $P(S)$ is the set of all subsets of S.
Let $A = \{a, b, c\}$
$P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{c,a\}, \{a,b,c\}\}$

#) Let S be a set with $|S| = n$, then $|P(S)| = 2^n$

#) Let A, B be 2 sets. The cartesian product of A & B is denoted by

$A \times B = \{(a,b) \mid a \in A, b \in B\}$ is the set of all ordered pairs (a,b).

Set Operations

→ The union of A & B is denoted by $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$

→ The intersection of A & B is denoted by $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$

← 2 sets are disjoint if $A \cap B = \phi$

→ The diff^n of 2 set A & B is denoted by $A \setminus B$ or $A - B = \{x \mid (x \in A) \wedge (x \notin B)\}$

→ The compliment of a set A is denoted by $\bar{A}$ or $A^c = \{x \mid x \in U - A\}$

#) What is the power set of ϕ & $\{\phi\}$?

⇒ The empty set has only one subset namely itself.

$P(\phi) = \{\phi\}$

$P(\{\phi\}) = \{\phi, \{\phi\}\}$

Barber's Paradox

A barber is a man in the town who only shaves those who don't shave themselves.

Does the barber shave himself?

Russell's Paradox

Let the domain be the set of all set & define $S = \{x \mid x \notin x\}$

Then S is the set of all set which are not member of themselves.

Is S a member of itself?

⇒ Suppose S is not a member of itself. Then it satisfies the predicate in the definition & hence S is a member of itself which is a contradiction.

⇒ Now if S is a member of itself, then it doesn't satisfy the predicate & hence S is not a member of itself. Again contradiction.

This can be resolved by having levels of set. This is sometimes called "theory of type". Here sets exist in hierarchy. x can be a member of y only if y is at level one higher than x. Then $x \notin x$ & $x \in x$ has no meaning.

How to compare sets

→ In finite set, count the no. of elmt

HILBERT'S HOTEL PROBLEM

Suppose there is a hotel with infinitely many rooms & they are all full

#) Can yo accomodate finite no of guest.

⇒ Yes. Shift the person from n^{th} room to $(n+1)^{st}$ room

#) What if infinitely many guest arrive?

⇒ Move the guest from the n^{th} room to $2n^{th}$ room.

#) What if infinitely many train arrive with infinitely many passenger?

⇒ Shift the person in the n^{th} room to 2^n th room. Then the n^{th} passenger of first train shifts to 3^n th room.

& the m^{th} train passenger shifts to m^{th} prime no.

FUNCTION

Here we study functions defined on discrete domain.

Let A & B be 2 set. A function f from A to B is an assignment of exactly one element of B to each element of A, i.e. $f: A \to B$ is a subset of R of $A \times B$ s.t.

(i) $\forall a \in A$, $\exists\ b \in B$ s.t. $(a,b) \in R$

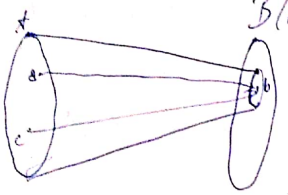
(ii) if $(a,b) \in R$ & $(a,c) \in R$, $b = c$

We write $f(a) = b$ & b is the image of a.

Range $(f) = \{b \in B \mid \exists\ a \in A$ s.t. $f(a) = b\}$

domain $(f) = A$

Visualization



Comparing sets

Surjective or onto : $f: A \to B$ is onto if $\forall y \in B\ \exists x \in A$ s.t. $f(x) = y$

If A & B are finite, $|A| \geq |B|$

Injective or one-one : $f: A \to B$ is injective if $\forall x, y \in A$ if $f(x) = f(y)$, $x = y$

If A & B are finite, $|A| \leq |B|$

Bijective ⇒ If a function is the one-one & ont- it is called bijective

Composition of

If $g: A \to B$ & $f: B \to C$ then

$f \circ g: A \to C$ is defined by $f \circ g(x) = f(g(x))$

$f \circ g$ is defined only if range $(g) \subseteq$ Domain (f)

$f \circ (g \circ h) = (f \circ g) \circ h$

Inverse of a func^n

Let $f: A \to B$ be a bijection. The inverse func^n of f is the func^n $f^{-1}: B \to A$ that assigns an element $b \in B$ to the unique element $a \in A$ s.t. $f(a) = b$

i.e. $f^{-1}(b) = a$.

If f is a bijection then its inverse exists & $f \circ f^{-1} = Id(B)$

$f^{-1} \circ f = Id(A)$

#(i) $f(x) = x^2$, $f: \mathbb{R} \to \mathbb{R}$

→ this is not injective so the inverse does not exist

#) $f(x) = x^2$, $f: \mathbb{N} \to \mathbb{N}$

→ Not surjective

#) $f: \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $f(x) = x^2$

→ f is bijective & has an inverse $f^{-1} = \sqrt{x}$

Relative notion of size using bijection

We say 2 finite/infinite sets have the same size if there exists a bijection between them.

→ For finite sets this is a property that can be shown that for infinite set, this is the def^n.

A set S is

* Infinite

• **Theorem**: The set $\mathbb{N}$ is an infinite set.

⇒ Consider the injective map $f: \mathbb{N} \to \mathbb{N}$ defined by $f(x) = 2x$. Then $f(\mathbb{N}) \subset \mathbb{N}$. ∴ $\mathbb{N}$ is infinite.

#) Can we measure infinite set?

⇒ A set that is either finite or has the same cardinality as $\mathbb{N}$ (∃ a bijection exists between the set & $\mathbb{N}$), then the set is called countable.

A set that is not countable is called uncountable.

• When an infinite set S is countable we denote the cardinality of S by $\aleph_0$ known as aleph knot where aleph is the first letter of the Hebrew alphabet.

Theorem: There is a bijection from $\mathbb{Z}$ to $\mathbb{N}$

⇒
$$f(x) = \begin{cases} -2x + 1 & x \le 0 \\ 2x & x > 0 \end{cases}$$

#) Is there a bijection between $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$? Yes

#) Is there a bijection between $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$? Yes

) Is there a bijection from $\mathbb{Q}$ to $\mathbb{N}$? Yes

Is there a bijection from $\mathbb{R}$ to $\mathbb{N}$? No

Is there a bijection from $\mathcal{P}(\mathbb{N})$ to $\mathbb{N}$? No

Is the set of odd +ve integers countable? Yes

• **Union of 2 countable set is countable**

Let $A = \{a_0, a_1, \dots\}$, $B = \{b_0, b_1, \dots\}$

$A \cup B = \{a_0, a_1, \dots, b_0, b_1, \dots\}$ is countable set.

$f(a_i) = 2i + 1$ $f(b_i) = 2i + 2$

• Let A & B be countable sets then $A \times B$ is also countable.

⇒ (a_0, b_0), (a_0, b_1), (a_0, b_2), (a_0, b_3), (a_0, b_4) ...

(a_1, b_0), (a_1, b_1), (a_1, b_2), (a_1, b_3), (a_1, b_4) ...

(a_2, b_0)

⋮

$$f(a_i, b_j) = \left(\sum_{k=1}^{i+j} k\right) + j + 1$$

#) Show that set of +ve rational no. is countable.

Cantor – Bernstein – Schröeder Theorem

If there are injective maps $f: A \to B$ & $g: B \to A$ then there is a bijection between A & B.

$f(p/q) = 2^p 3^q$

$f: \mathbb{Q} \to \mathbb{N}$ defined by $f(p/q) = 2^p 3^q$ where $\gcd(p, q) = 1$ is injective map & $g: \mathbb{N} \to \mathbb{Q}^+$ defined by $g(n) = n$ is injective.

∴ There is a bijection.

Cantor, 1891

Theorem ⇒ Let S be any set, then there is no bijection between S & $P(S)$. In fact we prove if $f: S \to P(S)$ then f is not surjective.

Let, $S = \mathbb{N}$

$1 \longrightarrow \{1, 2, 3\}$
$2 \longrightarrow \{1, 5, \dots\}$
$3 \longrightarrow \{2, 5, 7, \dots\}$
4
5

Consider $B = \{x \in \mathbb{N} \mid x \notin f(x)\} \subseteq \mathbb{N}$

$\exists$ some $\xi \in \mathbb{N}$ s.t. $f(\xi) = B$

$\xi \in B$ iff $\xi \notin f(\xi) = B$, which is a contradiction.

Proof ⇒ Consider $B = \{x \in S \mid x \notin f(x)\} \subset S$ ie $B \in P(S)$

Let us assume that f is a bijection between S & $P(S)$, ie f is surjective.

Then $\exists$ some $\xi \in S$ s.t. $f(\xi) = B$. But by construction $\xi \in B$ iff $\xi \notin f(\xi) = B$ which is a contradiction so f can't be surjective.

If B is empty set, this means that every element of S has been mapped to set that contain that element. so no element has been mapped to empty set, so it is not surjective.

Thus we conclude that $|S| < |P(S)|$

$|\mathbb{N}| < |P(\mathbb{N})| < |P(P(\mathbb{N}))| < \dots$

there is an infinite hierarchy of larger infinities.

Q) Show that there is a bijection between $(0,1)$ & $\mathbb{R}$

Theorem : $(0,1)$ is uncountable.

Proof ⇒ Suppose that $(0,1)$ is countable. Say the elements are $p_1, p_2, p_3, \dots$

$p_1 = 0 \cdot d_{11} d_{12} d_{13} d_{14} \dots$
$p_2 = 0 \cdot d_{21} d_{22} d_{23} d_{24} \dots$
$p_3 = 0 \cdot d_{31} d_{32} d_{33} d_{34} \dots$

where $d_{ij} \in \{0, 1, \dots, 9\}$

Let us construct a new real no. say

$p = 0 \cdot d_1 d_2 d_3 d_4 \dots$

where $d_i = \begin{cases} 4 & \text{if } d_{ii} \neq 4 \\ 5 & \text{if } d_{ii} = 4 \end{cases}$

$p_1 = 0.14572 \dots$
$p_2 = 0.543 \dots$
$p_3 = 0.210 \dots$

$p = 0.454, \dots$

Then the decimal number r is not equal to the any of the decimal number p_i's in the list as the i^{th} place of r is diff^n from the i^{th} place of p_i for each i.

So there is no surjection between $\mathbb{N}$ & $\mathbb{R}$ & $\mathbb{R}$ is uncountable.

- **Def^n** : A set has cardinality C if there is a bijection from $(0,1)$ to S

⇒ (i) $\aleph_0 < C$

We have seen that there is no bijection from $(0,1)$ to $\mathbb{N}$. But we have an injection from $f: \mathbb{N} \to (0,1)$,

(2) Set of irrational number is uncountable because because if it is countable $\mathbb{R}$ is also countable which is a contradiction.

(3) Is $|\mathbb{R} \times \mathbb{R}|$ & $|\mathbb{R}|$ same?

Theorem $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

Lemma If A is a set, then there is a bijection between $\mathcal{P}(A)$ & $\text{Maps}(A, \{0,1\}) := \{f : A \to \{0,1\} \mid f \text{ is a map}\}$

Proof :

$\mathcal{P}(A) \xrightarrow{F} \text{Maps}(A, \{0,1\})$

$\delta \longrightarrow 1_\delta$ (Characteristic function)

where $1_\delta : A \to \{0,1\}$

$$1_\delta(a) = \begin{cases} 0 & a \notin \delta \\ 1 & a \in \delta \end{cases}$$

F is $1-1$

Let $\delta, \tau \in \mathcal{P}(A)$ st $F(\delta) = F(\tau)$ ie $1_\delta = 1_\tau$

Note : $a \in \delta$ iff $1_\delta(a) = 1$ iff $1_\tau(a) = 1$ iff $a \in \tau$

$\delta = \tau$

F is injective.

F is surjective.

For every $\chi \in \text{Maps}(A, \{0,1\})$ $\exists\ \delta \subseteq A$ st $\chi = 1_\delta$

Let $\delta = \{a \in A \mid \chi(a) = 1\}$

Then check $1_\delta = \chi$

Proof of theorem → By the lemma we have : $|\mathcal{P}(\mathbb{N})| = |\text{Maps}(\mathbb{N}, \{0,1\})|$

Now that there is a bijection between maps $(\mathbb{N}, \{0,1\})$ & $(0,1)$

Note : Maps $(\mathbb{N}, \{0,1\})$ are just sequences with value 0 / 1.

Given a sequence $\{y_n\}_{n=1}^{\infty}$

We produce $\sum_{n=1}^{\infty} y_n 2^{-n}$

Check this gives a bijection

$$|\mathcal{P}(\mathbb{N})| = |\mathbb{R}| = c$$

We know that $\aleph_0 < |\mathbb{R}|$. Whether or not there exist a set A for which $\aleph_0 < |A| < |\mathbb{R}|$? → Continuum Hypothesis

It was suspected that no such set exist but no one was able to prove / disprove this.

RELATION

- A relation R from A to B is a subset of $A \times B$. We say a is related to b by R & the notation aRb.

This relation is a way to relate the elements of 2 sets (not necessarily diff^n)

(i) All func^n are relations

(ii) $R_1(\mathbb{Z}) = \{(a,b) \mid a, b \in \mathbb{Z},\ a - b \text{ is even}\}$

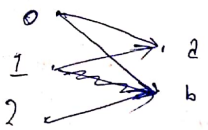
(iii) $R_2(\mathbb{Z}) = \{(a,b) \mid a, b \in \mathbb{Z},\ a \le b\}$

(iv) Let δ be a set. $R_3(\mathcal{P}(\delta)) = \{A, B \mid A, B \subseteq \delta \text{ & } A \subseteq B\}$

Representation of a relation from A to B

$A = \{0, 1, 2\}$ $B = \{a, b\}$

$\therefore R = \{(0,a), (0,b), (1,a), (2,b)\}$



Directed graph representation

	a	b
0	1	1
1	1	0
2	0	0

Matrix representation

- Let M be the matrix representation of a relation from A to B. Then

$$m_{ij} = \begin{cases} 1 & \text{if } a_i \sim b_j \\ 0 & \text{otherwise} \end{cases}$$

where $A = \{a_1, a_2, \dots\}$, $B = \{b_1, b_2, \dots\}$

- Functions were special type of relations that were useful to compose sets.

Equivalence relation & Partial Order Relation

If a set A is finite, we can count the no of relations on A. R is a subset of $A \times A$. If $|A| = n$, then 2^{n^2} relations are possible on A.

Partition of a set (Grouping like elements)

- Natural nos are partitioned into even & odd numbers.
- A partition of a set S is a collection of disjoint non-empty subsets of S that have S on the union. In other words, the collection of subsets A_i form a partition of S iff

(i) $A_i \neq \phi$, $\forall i$

(ii) $A_i \cap A_j = \phi$

(iii) $S = \cup A_i$

Interpreting partition as relation

We define aRb on S if a & b belong to the same set in the partition of S

Properties of relation generated by a partition

(i) All elements must be related to themselves

(ii) If a is 'like' b then b must be 'like' a

(iii) If $a \sim b$ & $b \sim c$ then $a \sim c$

- A relation R(S) is reflexive if $\forall a \in S$. aRa
- R(S) is symmetric if $aRb \Rightarrow bRa \quad \forall a, b \in S$
- R(S) is transitive if aRb & bRc implies aRc.

These 3 properties are defining properties of partition.

#) Consider the relations on $\mathbb{Z}$

(i) $R_1 = \{(a,b) \mid a \leq b\}$

(ii) $R_2 = \{(a,b) \mid a > b\}$

(iii) $R_3 = \{(a,b) \mid a = b \text{ or } a = -b\}$

(iv) $R_4 = \{(a,b) \mid a = b\}$

(v) $R_5 = \{(a,b) \mid a = b+1\}$

(vi) $R_6 = \{(a,b) \mid ab \in \mathbb{Z}\}$

⇒ Reflexive : R_1, R_3, R_4

Symmetric : R_3, R_4, R_6

Transitive : $R_1, R_2, \not{R}_4, R_3$

#) Is the converse true? Can we generate a partition from an equivalence relation?

⇒ Let R be an equivalence relation on a set S & $a \in S$. Then the equivalence class of a is denoted by $[a]$, is the set of all elements which are related to a ie $[a] = \{b \in S \mid (a,b) \in R\}$

Lemma Let R be an equivalence relation on S. Let $a, b \in S$. Then following are equivalent :

(i) aRb

(ii) $[a] = [b]$

(iii) $[a] \cap [b] \neq \phi$

Proof : (1) ⇒ (2). Let aRb WTP $[a] = [b]$

Let $c \in [a]$ then aRc but we have $aRb \Rightarrow bRa$ hence transitivity $bRc \therefore c \in [b]$ //

(2) ⇒ (3) Trivial //

(3) ⇒ (1) : Let $c \in [a] \cap [b]$ then aRc & bRc. $\Rightarrow cRb$ Because of symmetric property. Thus aRb

Theorem: Let R be an equivalence relation on S. Then the equivalence classes of R form a partition of S.

$\Rightarrow S = \bigcup_{a \in S} [a]$

Then by lemma the equivalence classes are either equal or disjoint. Hence proved.

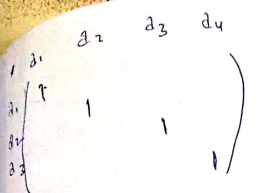
- Define an equivalence relation R on $Z \times Z \setminus \{0\}$ by $(a,b) R (c,d)$ if $ad = bc$

- aRb when $a - b$ is an even number (on Z). Let $[a]$ be an even number, $[a]$ = set of all even numbers.
If a is odd, $[a]$ = set of all odd numbers.

Geometrical Objects using equivalence relation

$[0,1]$

$x \sim x'$ if $\begin{cases} x = x' \\ x = 0, \ x' = 1 \\ x = 1, \ x' = 0 \end{cases}$



→ Reflexive implies diagonal entries are 1.
→ Symmetric means matrix is symmetric

Partial Order Relation

Consider $\{(a,b) \mid a,b \in \mathbb{Z}, a \leq b\}$. This is reflexive & transitive but not symmetric.

Anti-symmetric : A relation R on S is anti-symmetric if $\forall$ $a, b \in S$ aRb & bRa implies $a = b$.

- A partial order is a relation which is reflexive, transitive & anti-symmetric.

- We use $\leq$ to denote partial order.

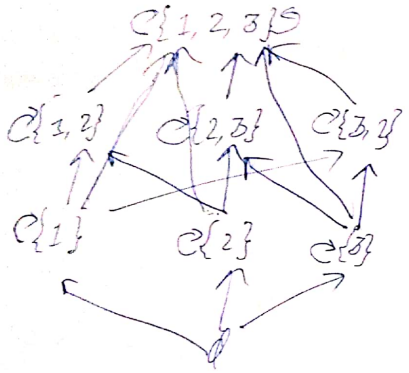
- It is called partial order because not all pairs of elements are comparable.

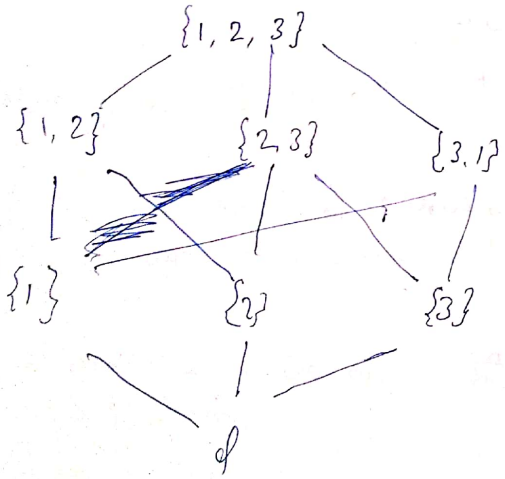
- A total order is a partial order $\leq$ on S in which every pair of element is comparable to each other. $a \leq b$ or $b \leq a$ $\forall a, b \in S$.

- A set S together with a partial order $\leq$ on S is called a partially ordered set or poset. It is denoted by $(S, \leq)$

Representation of Partial Order

Let $S = \{1, 2, 3\}$ & $(P(S), \subseteq)$





Hasse Diagram

Specialities of graph of Poset

→ Must be acyclic ie there is no cycle in the graph.

Constructing Hasse diagram

→ Remove self loops

→ Remove transitive edges.

Maximal & minimal elements

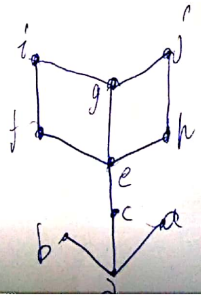
→ An element of poset is called maximal if it is not less than any element of the poset ie a is maximal in poset $(S, \leq)$ if there is no $b \in S$ s.t $a \leq b$ & $a \neq b$.

→ Maximal & minimal elements are the top & bottom elements of Hasse diagram.

In general a poset can have more than one maximal/minimal.

#) Let $(S, \leq)$ be a poset & $A \subseteq S$

→ An element x that is an upper bound of a subset A of S is less than all other upper bounds of A is called the least upper bound of A.



Consider $A = \{c, e\}$

Upper bounds of A are $\{f, g, h, i, j, e\}$

Least upper bound is $\{e\}$.

⇒ Let $(S, \leq)$ be a poset & $A \subseteq S$. If $l \in S$ st $l \leq a \ \forall \ a \in A$ then l is a lower bound of A.

An element x is a lower bound on a subset A & is greater than all other lower bounds on A is called greatest lower bound on A

lower bound of A are $\{A, C\}$ & glb is C.

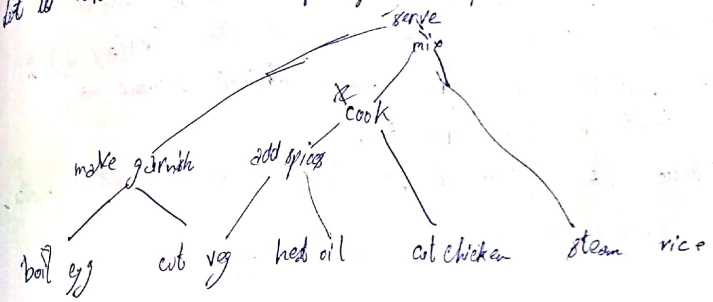
Chain and Anti-chain

⇒ Let $(S, \leq)$ be a poset. A subset $B \subseteq S$ is called a chain if every pair of elements in B is related by $\leq$ ie $\leq$ is a total order on B.

⇒ Let $(S, \leq)$ be a poset. A subset $A \subseteq S$ is called anti-chain if no 2 distinct elements of A are related to each other.

Application

Let us represent the recipe of biryani as poset



- Clearly it has dependencies
- But when you cook an order is required & it must be consistent with partial order.
- This is called linearization & topological sorting

⇒ A topological sort of a poset $(S, \leq)$ is a poset $(S, \leq_t)$ with a total order $\leq_t$ st $x \leq y$ implies $x \leq_t y$

Theorem : Every finite poset has a topological sort.

Lemma : Every finite non-empty poset $(S, \leq)$ has at least one minimal element.

Proof ⇒ Choose an element $a_0 \in S$. If a_0 is non minimal then $\exists\ a_1 \in S$ st $a_1 \leq a_0$. If a_1 is not minimal $\exists\ a_2 \in S$ st $a_2 < a_1$. Continue this process but since S has finite no. of elements it will terminate. Hence $\exists$ a minimal element in S.

Proof (Theorem) ⇒ To define a total ordering on the poset choose a minimal element a_1. Next note that $(X \setminus \{a_1\}, \leq)$ is a poset. If it is non-empty, choose a minimal element a_2 the poset & define $a_2 \leq_t a_2$.

Continue this process & it will give you a total order.

LEL TASK SCHEDULING AND CHAIN

Schedule the task to minimize time? When are there many it is possible.

Every task takes 1 unit of time but we still need 5 units of time as the length of the longest chain present poset is 5.

Fact there is a parallel schedule that runs in t steps the length of longest chain present in poset.

Theorem ⇒ For a finite poset $(S, \leq)$ with the length of the longest chain $= t$. We can partition S into t subsets $S_1, S_2, \ldots, S_t$ st $\forall i \in \{1, \ldots, t\}$ if $a \in S_i$ & $b \neq a$ then $b \in S_1 \cup S_2 \cup \ldots \cup S_{i-1}$.

If we assume the Theorem we can schedule all S_i in time i since we know all previous table were done earlier. Thus each S_i is an anti-chain. This solves the parallel tasking.

Proof ⇒ Put each $a \in S$ in S_i st i is the length of longest chain ending at a. Suppose $\exists\ i$, $a \in S_i$, $b \leq a, b \neq a$. Let $b \notin S_1 \cup \ldots \cup S_{i-1}$. By def^n, $\exists$ chain of length i (i.e. i terms) ending at B. But we have $b \leq a$ which implies we can extend the chain to length $(i+1)$ ending at a which is a contradiction as $a \in S_i$.

Mirsky's Theorem (1971)

If the largest chain in a poset $(S, \leq)$ is of the length t, then S can be partitioned into t-antichains.

Dilworth's Theorem (1950)

If the largest antichain in a poset $(S, \leq)$ is of length n then S can be partitioned into n chains.