Discrete Structures

Daksh Maahor

September 2025

Contents

1 Introduction : Propositions

1.1 Propositions

A proposition is a statement which is either true or false (but not both).

Ex :- "It is raining in Mumbai today!!!" is a proposition, most probably true :(
Ex :- $x + 3 = 8$ is not a proposition, as it cannot be determined to be true or false without fixing a value for x.

Similarly, since we use variables $x, y, z, \ldots$ for numbers, we will use $p, q, r, \ldots$ for propositions.

1.2 Combining Propositions

The propositions can be combined using Boolean operators such as $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\longleftrightarrow$, etc.

$$\begin{aligned} p &: \text{It is raining} \\ \neg p &: \text{It is not raining} \\ q &: \text{I will go to class} \\ p \wedge \neg q &: \text{It is raining and I will not go to class} \\ \neg p \rightarrow q &: \text{If it is not raining then I will go to class} \end{aligned}$$

1.3 Truth Tables!

A Truth Table is a table that lists all the possible combinations of inputs and their corresponding outputs. For example:

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Table 1: Truth table for $p \wedge q$

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Table 2: Truth table for $p \vee q$

p	q	$p \bigoplus q$
0	0	0
0	1	1
1	0	1
1	1	0

Table 3: Truth table for $p \bigoplus q$

1.3.1 Important logical equivalences

Logical equivalence means that the truth tables of two statements are identical. Some important logical equivalences are:

- $p \rightarrow q$ is equivalent to $\neg p \vee q$
- $p \longleftrightarrow q$ is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$

1.3.2 Operator Precedence

The Operator Precedence of the Logical Operators follows the given order:

$$\neg \text{ then } \wedge \text{ then } \vee \text{ then } \rightarrow \text{ then } \longleftrightarrow$$

Eg: Construct the truth table for $(p \vee \neg q) \to (p \wedge q)$

p	q	$\neg q$	$p \vee \neg q$	$p \wedge q$	$(p \vee \neg q) \to (p \wedge q)$
0	0	1	1	0	0
0	1	0	0	0	1
1	0	1	1	0	0
1	1	0	1	1	1

Table 4: Truth table for $(p \vee \neg q) \to (p \wedge q)$

1.4 Negation, Converse and Contrapositive

Take the following propositions:

$$\begin{aligned} p &: \text{It will rain today} \\ q &: \text{The match will be canceled} \\ p \to q &: \text{If it will rain today then the match will be canceled} \end{aligned}$$

The negation of an implication is given as:

$$\neg(p \to q) \equiv \neg(\neg p \vee q) \equiv p \wedge \neg q$$

For the above statements:

$$\neg(p \to q): \text{ It will rain today and the match will not be canceled}$$

The converse of an implication is given as:

$$\text{Converse of } (p \to q) \text{ is } (q \to p)$$

For the above statements:

$$q \to p: \text{ If the match will be canceled then it will rain today}$$

The contrapositive of an implication is given as:

$$\text{Contrapositive of } (p \to q) \text{ is } (\neg q \to \neg p)$$

For the above statements:

$\neg q \to \neg p$: If the match won't be canceled then it won't rain today.

$p \to q \equiv \neg q \to \neg p$, that is an implication is logically equivalent to its contrapositive.

1.5 Quantifiers

Quantifiers are additional statements that provide context-specific information, such as the domain of discourse. Some common quantifiers are the following.

- $\forall n$ stands for all values of n in the given domain
- $\exists n$ stands for there exists a value of n in the given domain
- $\in$ is "the element of" symbol

The negation of $\forall$ is $\exists$ and vice versa.

Ex : The negation of $\forall x\ P(x)$ is $\exists x\ \neg P(x)$

Ex : The negation of $\forall x\ (x^2 \geq x)$ is $\exists x\ (x^2 < x)$

2 Theorems and Proofs

A theorem is a proposition that can be proved or disproved. At the basic level, there are two basic methods of proving theorems, Induction and Contradiction.

2.1 Examples of some proofs

Theorem 1. *For all $x \in \mathbb{N}$, x is even $\longleftrightarrow x + x^2 - x^3$ is even.*

Proof. The proof proceeds in two directions.

- Forward direction : $\forall x \in \mathbb{N}$, x is even $\rightarrow x + x^2 - x^3$ is even.

  Let $x \in \mathbb{N}$ and x be even.

  So, $\exists k \in \mathbb{N}$, $x = 2k$.

  Then, $x + x^2 - x^3 = 2k + (2k)^2 - (2k)^3 = 2k + 4k^2 - 8k^3 = 2(k + 2k^2 - 4k^3) = 2m$

  where, $m = k + 2k^2 - 4k^3$, thus $m \in \mathbb{Z}$, ie, $2 \mid x + x^2 - x^3$.

  So, $x + x^2 - x^3$ is even.

- Reverse direction : $\forall x \in \mathbb{N}$, $x + x^2 - x^3$ is even $\rightarrow x$ is even.

  It is easier to prove the contrapositive,

  $\forall x \in \mathbb{N}$, x is odd $\rightarrow x + x^2 - x^3$ is odd.

  Let $x \in \mathbb{N}$ and x be odd.

So, $\exists k \in \mathbb{N}$, $x = 2k + 1$.

Then $x + x^2 - x^3 = (2k+1) + (2k+1)^2 - (2k+1)^3 = (2k+1) + (4k^2+4k+1) - (8k^3+12k^2+6k+1) = (-8k^3 - 8k^2 + 1) = 2m+1$ where $m = -4k^3 - 4k^2$, thus $m \in \mathbb{Z}$, i.e. $x + x^2 - x^3$ is odd.

So, $x + x^2 - x^3$ is odd.

Hence, Proved. $\square$

Theorem 2. *There are infinitely many primes.*

Proof. Suppose that there are finitely many primes, say, $p_1 < p_2 < p_3 < \cdots < p_n$. We call the set of those primes $\mathbb{S}$.

Now, let $k = (p_1 p_2 p_3 \ldots p_n) + 1$.

Then, k when divided by any p_r returns a remainder of 1. So k is not divisible by any of the p_r's.

Also, $k > 1$ and $k > p_n$, so k must not be prime. So, by the fundamental theorem of arithmetic, k can be written as a product of primes.

Now take any prime p in that product. Since p divides k, therefore $p \neq p_i$ for any $i \in \{1, 2, \ldots, n\}$.

So p is a prime that is not in $\mathbb{S}$. But this contradicts our assumption that $\mathbb{S}$ is the set of all primes.

This means that our assumption was wrong, and thus, there are infinitely many primes. $\square$

Theorem 3. *$\sqrt{2}$ is irrational.*

Proof. Let us assume, for the sake of contradiction, that $\sqrt{2}$ is rational.

That is,

$$\sqrt{2} = \frac{p}{q}$$

for some

$$p, q \in \mathbb{N}, q \neq 0$$

where p and q are co-prime.

Then,

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

Thus p^2 is divisible by 2. Since 2 is prime, this implies that p is divisible by 2. So,

$$\exists k \in \mathbb{N}, p = 2k$$

$$(2k)^2 = 2q^2$$
$$4k^2 = 2q^2$$
$$q^2 = 2k^2$$

Thus q^2 is divisible by 2. Since 2 is prime, this implies that q is divisible by 2.

Thus, both p and q are divisible by 2. This contradicts the statement that p and q are co-prime. So, our assumption that $\sqrt{2}$ is rational is false.

So, $\sqrt{2}$ is irrational. $\square$

Theorem 4. *There exist irrational numbers x and y, such that x^y is rational.*

Proof. We have already proved that $\sqrt{2}$ is irrational.

Let $x = y = \sqrt{2}$, consider $z = x^y$.

- If z is rational, then we have found a pair of irrational (x, y) such that x^y is rational.
- If z is irrational, then let $x = z$ and $y = \sqrt{2}$. Then, $x^y = ((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$, which is rational, then we have found a pair of irrational (x, y) such that x^y is rational.

$\square$

The above proof is a non-constructive proof. It establishes that a mathematical object exists without providing a method to construct or identify it. Such proof techniques are quite powerful.

Theorem 5. 21 *divides* $4^{n+1} + 5^{2n-1}$ *whenever* $n \in \mathbb{Z}^+$.

Proof.

- Base Case: For $n = 1$

$$4^{n+1} + 5^{2n-1} = 4^2 + 5^1 = 16 + 5 = 21 = 21 \times 1$$

  Thus, 21 divides $4^{n+1} + 5^{2n-1}$ for $n = 1$

- Induction Hypothesis: Let for $n = k$, $k \geq 1$, we have

$$21 \text{ divides } 4^{k+1} + 5^{2k-1}$$

  So,

$$4^{k+1} + 5^{2k-1} = 21m \text{ for some } m \in \mathbb{Z}$$

- Induction Step: For $n = k + 1$

$$4^{n+1} + 5^{2n-1} = 4^{(k+1)+1} + 5^{2(k+1)-1}$$

$$4^{k+2} + 5^{2k+1} = 4(4^{k+1}) + 25(5^{2k-1})$$
$$4^{k+2} + 5^{2k+1} = 4(21m - 5^{2k-1}) + 25(5^{2k-1})$$
$$4^{k+2} + 5^{2k+1} = 4(21m) + 21(5^{2k-1})$$
$$4^{k+2} + 5^{2k+1} = 21(4m + 5^{2k-1}) = 21p$$

  for

$$p = 4m + 5^{2k-1}$$

Thus, by induction, we have 21 divides $4^{n+1} + 5^{2n-1}$ $\forall n \in \mathbb{Z}^+$ □

The above proof technique is another powerful tool known as mathematical induction.

2.2 Mathematical Induction as an Axiom

We can define the induction axiom as follows.

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

- $P(i)$ is true (Base case)
- $\forall k \geq i$, $P(k) \rightarrow P(k+1)$

Then, $P(n)$ holds $\forall n \in \mathbb{Z}^+, n \geq i$

Induction axiom can then be used to prove an important theorem in computer science known as the Well Ordering Principle.

2.3 The Well Ordering Principle

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

Proof.

- Base Case: For a set of 1 non-negative integer, the integer itself is obviously the smallest element.
- Induction Hypothesis: For any set of k non-negative integers, let there exist a smallest element.
- Induction Step: Consider any set of $k+1$ non-negative integers, say S_0. Let $n_0 \in S_0$. Now consider the set $S_1 = S_0 - \{n_0\}$. S_1 is a set of k non-negative integers, thus S_1 has a smallest element, say n_1.

  Now, if $n_1 < n_0$, then n_1 will be the smallest element of the set

S_0. Else n_0 will be the smallest element of S_0. In either case, S_0 will have a smallest element.

Thus, $\forall n \in \mathbb{Z}^+$, any finite set of n non-negative integers will have a smallest element.

For an infinite set of non negative integers $\mathbb{X}$, take for any n, $\mathbb{X}_n = \mathbb{X} \cap \{0, \ldots, n\}$. Now since $\mathbb{X}$ is not ϕ and $\bigcup_{i=0}^{\infty} \mathbb{X}_i = \mathbb{X}$, there exists $n \in \mathbb{N}$ such that $\mathbb{X}_n \neq \phi$.

Then by above proof, $\exists x \in \mathbb{X}_n, \forall u \in \mathbb{X}_n, x \leq u$. Also if $u \in \mathbb{X} - \mathbb{X}_n$, we have $u \notin \{0, \ldots, n\}$ and thus, $x \leq n < u$ so $x \leq u \; \forall \; u \in \mathbb{X}$ □

2.4 Induction as a theorem : WOP implies Induction

Theorem 6. *Let $P(n)$ be a property of non-negative integers. If*

- *$P(i)$ is true (Base case)*
- *$\forall k \geq i$, $P(k) \rightarrow P(k+1)$*

Then, $P(n)$ holds $\forall n \in \mathbb{Z}^+, n \geq i$

Proof. We will use contradiction. Let us assume induction is not true. This means that,

- $P(i)$ is true (Base case)
- $\forall k \geq i$, $P(k) \rightarrow P(k+1)$

But, $\exists n \in \mathbb{Z}^+, n \geq i$, such that $P(n)$ is not true.

Then consider $\mathbb{S} = \{i \in \mathbb{N} | P(i) \text{ is not true}\}$

Since $\mathbb{S}$ is non-empty, by WOP it must have a smallest element. Let that element be n_0. So, $P(n_0)$ is not true. This implies that $P(i)$ is true $\forall i < n_0$. Thus $P(n_0 - 1)$ is true. Using our induction step, $P(n_0 - 1) \rightarrow P(n_0)$, so $P(n_0)$ is true. This is a contradiction, and thus our assumption must be wrong.

Thus, $\forall n \in \mathbb{Z}^+, n \geq i, P(n)$ is true. □

Theorem 7. *Any integer* > 1 *can be written as a product of prime numbers.*

Proof. Proof by Contradiction.

Let us assume there exist
$\mathbb{S} = \{n \in \mathbb{Z}^+, n > 1 \mid n \text{ cannot be written as a product of primes}\}$

Since $\mathbb{S}$ is non empty, there exists a smallest element in $\mathbb{S}$. Call it n_0.

First n_0 can't be prime, as then it can be written as a product of primes as $n_0 = n_0$.

So, n_0 can be written as

$n_0 = a \times b$, where $1 < a, b < n$

Since a and b are smaller than n, they can be written as a product of one or more primes.

$a = p_1 p_2 p_3 \ldots p_k$ and $b = q_1 q_2 q_3 \ldots q_m$ for $k, m \geq 1$

But then $n_0 = p_1 p_2 p_3 \ldots p_k . q_1 q_2 q_3 \ldots q_m$ which is a contradiction.

Thus, any integer > 1 can be written as a product of prime numbers.
$\square$

Theorem 8. *Any integer > 1 can be written as a "unique" product of one or more primes.*

Proof. Let us assume that there exists an integer > 1 that cannot be written as a "unique" product of one or more primes.

Let us call the set of all such integers $\mathbb{S}$. Clearly, $\mathbb{S} \neq \phi$

By WOP, there exists a smallest element in $\mathbb{S}$, say s.

Then, $s = p_1 \ldots \ldots p_n = q_1 \ldots \ldots q_m$,

where each $p_i \neq q_j \ \forall i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, m\}$

Without loss of generality, assume $p_1 < q_1$. Then, $s = p_1 \times P = q_1 \times Q$ for some $P > Q$.

Then, $s - p_1Q = p_1(P - Q) = (q_1 - p_1)Q < s$, which implies that $(q_1 - p_1) < s$ and $Q < s$.

So $(q_1 - p_1)$ and Q must have a unique prime factorization, and thus p_1 must occur in it.

If p_1 occurs in the factorization of Q, then $p_1 = q_j$ violates our hypothesis.

If p_1 occurs in the factorization of $q_1 - p_1$, then p_1 must divide q_1 which contradicts the fact that both p_1 and q_1 are prime.

Hence, we have a contradiction, which means that our original claim was false. Thus, any integer > 1 can be written as a unique product of one or more primes. $\square$

Theorem 9. *For any* $m, n \in \mathbb{N},\ m \neq 0,$ *, there exists a quotient* q *and remainder* r $(q, r \in \mathbb{N})$*, such that*

$$n = q \times m + r, \quad 0 \leq r < m$$

Proof. Fix any $m > 0$, we use strong induction on n.

- Base case : for $n = \{0, \ldots, m-1\}$ we have $n = 0 \times m + n$.

  Thus Base case follows.

- Induction Step : We will prove for all $k \geq m$

  Hypothesis : Let $\forall n \in \mathbb{N},\ n \leq k,\ \exists q, r \in \mathbb{N}$ such that
  $n = q \times m + r,\ 0 \leq r < m$

  Then consider $0 \leq k - m + 1 \leq k$, thus we can use the induction hypothesis on $k - m + 1$.

  $k - m + 1 = q' \times m + r',\ 0 \leq r' < m$

  Now select $q^* = q' + 1$ and $r^* = r'$, then

  $k + 1 = q^* \times m + r^*,\ 0 \leq r^* < m$

Thus, by induction, for any $m, n \in \mathbb{N},\ m \neq 0,$, there exists a quotient q and remainder r $(q, r \in \mathbb{N})$, such that

$$n = q \times m + r, \quad 0 \leq r < m$$

$\square$

3 Basic Structures : Sets and Functions

3.1 Sets

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

Formally, let P be a property. Then, any collection of objects that satisfy P is a set, i.e., $\mathbb{S} = \{x \mid P(x)\}$

3.2 Some properties of sets

- $\mathbb{A} \subseteq \mathbb{B} \longleftrightarrow \forall x \in \mathbb{A}, (x \in \mathbb{B})$
- $\mathbb{A} \times \mathbb{B} = \{(a, b) \mid a \in \mathbb{A} \wedge b \in \mathbb{B}\}$
- $\mathbb{A} \cup \mathbb{B} = \{x \mid x \in \mathbb{A} \vee x \in \mathbb{B}\}$
- $\mathbb{A} \cap \mathbb{B} = \{x \mid x \in \mathbb{A} \wedge x \in \mathbb{B}\}$
- Empty set is denoted by ϕ
- Power set of $\mathbb{A} = \mathcal{P}(\mathbb{A}) = \{X \mid X \subseteq \mathbb{A}\}$
- If U is the universal set, then $\mathbb{A}^C = U - \mathbb{A} = \{x \mid x \in U \wedge x \notin \mathbb{A}\}$

3.3 Functions

Let $\mathbb{A}$ and $\mathbb{B}$ be two sets. A function f from $\mathbb{A}$ to $\mathbb{B}$ is an assignment of exactly one element of $\mathbb{B}$ to each element of $\mathbb{A}$.

$f : \mathbb{A} \to \mathbb{B}$ is a subset R of $\mathbb{A} \times \mathbb{B}$ such that

1. $\forall a \in \mathbb{A}, \exists b \in \mathbb{B}$ such that $(a, b) \in R$
2. If $(a, b) \in R$ and $(a, c) \in R$ then $b = c$

If $f : \mathbb{A} \to \mathbb{B}$ is a bijective function, then we can define its inverse $f^{-1} : \mathbb{B} \to \mathbb{A}$, defined as $f^{-1}(b) = a \longleftrightarrow f(a) = b$

If f is a bijection, then $f^{-1}(f(x)) = f(f^{-1}(x)) = x$, i.e. $fof^{-1}(x) = f^{-1}of(x) = x$

3.3.1 Functions on finite sets

If $\mathbb{A}$ and $\mathbb{B}$ are two finite sets such that $f : \mathbb{A} \to \mathbb{B}$ is a function from $\mathbb{A}$ to $\mathbb{B}$ then,

- f is injective $\to |\mathbb{A}| \leq |\mathbb{B}|$
- f is surjective $\to |\mathbb{A}| \geq |\mathbb{B}|$
- f is bijective $\to |\mathbb{A}| = |\mathbb{B}|$

3.3.2 Some important theorems : True for both finite and infinite sets

- $(\exists$ **bij** from $\mathbb{A} \to \mathbb{B} \wedge \exists$ **bij** from $\mathbb{B} \to C) \to (\exists$ **bij** from $\mathbb{A} \to C)$
- $(\exists$ **bij** from $\mathbb{A} \to \mathbb{B}) \to (\exists$ **bij** from $\mathbb{B} \to \mathbb{A})$

Theorem 10 (Schroder-Bernstein Theorem)**.**

$$(\exists \boldsymbol{inj} \textit{ from } \mathbb{A} \to \mathbb{B} \wedge \exists \boldsymbol{inj} \textit{ from } \mathbb{B} \to \mathbb{A}) \to (\exists \boldsymbol{bij} \textit{ from } \mathbb{A} \to \mathbb{B})$$

$$(\exists \boldsymbol{surj} \textit{ from } \mathbb{A} \to \mathbb{B} \wedge \exists \boldsymbol{surj} \textit{ from } \mathbb{B} \to \mathbb{A}) \to (\exists \boldsymbol{bij} \textit{ from } \mathbb{A} \to \mathbb{B})$$

3.4 Infinite Sets

3.4.1 Definition of Infinite Set

Theorem 11. *Let $\mathbb{A}$ be a set, and $b \notin \mathbb{A}$. $\mathbb{A}$ is infinite $\longleftrightarrow \exists \boldsymbol{bij}$ from $\mathbb{A} \to \mathbb{A} \ \cup \ \{b\}$*

Proof. If $\mathbb{A}$ is infinite, then $\mathbb{A} \neq \phi$, so let $a_0 \in \mathbb{A}$. Define $f(a_0) = b$.

Now $\mathbb{A} - \{a_0\}$ is infinite, so $\mathbb{A} - \{a_0\} \neq \phi$, so let $a_1 \in \mathbb{A} - \{a_0\}$. Define $f(a_1) = a_0$.

$\forall i \in \mathbb{N},\ i \geq 1,\ \mathbb{A} - \{a_0, \ldots, a_{i-1}\}$ is infinite and hence non-empty. Then, define $f(a_i) = a_{i-1}$.

Collecting all such a_i's, we get $\mathbb{A}' = \{a_i \in \mathbb{A} \mid i \in \mathbb{N}\}$, $\mathbb{A}' \subseteq \mathbb{A}$.

Now, if $\forall a \in \mathbb{A}, a \notin \mathbb{A}'$, we define $f(a) = a$, then f will become a bijection. □

3.4.2 Important Takeaways

- Even if $\mathbb{A}, \mathbb{B}$ are infinite, $\mathbb{A} \subsetneq \mathbb{B}$, there can be a bijection from $\mathbb{A} \to \mathbb{B}$. That is, $\mathbb{A}$ and $\mathbb{B}$ will have the same "cardinality".

- From any set $\mathbb{A}$, there is a surjection from $\mathbb{A} \to \mathbb{N}$ (Most Important).

- Finite unions of countable sets are countable.

- To show that an infinite set $\mathbb{S}$ is countable, it is enough to show that:

  - either $\exists$**inj** from $\mathbb{S} \to \mathbb{N}$

  - or $\exists$**surj** from $\mathbb{N} \to \mathbb{S}$

3.5 Some Important Bijections on Infinite Sets

3.5.1 Bijection from $\mathbb{Z} \to \mathbb{N}$

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

3.5.2 Bijection from $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$f(a, b) = \frac{(a + b)(a + b + 1)}{2} + b$$

3.5.3 Bijection from $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$

$$f(x) = (a, b)$$

where

$$x = 2^a(2b+1) - 1$$

3.5.4 Bijection from $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}$

$$f(a,b,c) = \frac{\left(\frac{(a+b)(a+b+1)}{2} + b + c\right)\left(\frac{(a+b)(a+b+1)}{2} + b + c + 1\right)}{2} + c$$

3.5.5 Bijection from $\mathbb{N} \to \mathbb{N} \times \mathbb{N} \times \mathbb{N}$

$$f(x) = (a,b,c)$$

where

$$x = 2^{(2^a(2b+1)-1)}(2c+1) - 1$$

3.5.6 Proving the inexistence of a bijection

Theorem 12. *There does not exist any bijection from* $\mathbb{R} \to \mathbb{N}$

Proof. For the sake of contradiction, let us say that there exists a bijection, namely $f : \mathbb{R} \to \mathbb{N}$. This means that we can enumerate all the real numbers in a table side by side of natural numbers. ie,

$$\forall y \in \mathbb{R}\ \exists x \in \mathbb{N}, f(x) = y$$

Let a_i denote the digit at $10^{-(i+1)}$th place in $f(i)$, $i \in \mathbb{N}$. Define b_i as

$$b_i = \begin{cases} a_i + 1 & a_i < 9 \\ 0 & a_i = 9 \end{cases}$$

and then define a real number p as

$$p = \sum_{i=0}^{\infty} b_i \times 10^{-(i+1)}$$

Then, $p - f(i) \neq 0$, ie, $p \neq f(i)\ \forall i \in \mathbb{N}$

But this contradicts our original claim that f is a bijection. Thus, our assumption must be wrong, and so, there does not exist any bijection from $\mathbb{R} \to \mathbb{N}$ $\square$

Similarly we can prove the inexistence of bijection from $\mathcal{P}(\mathbb{N}) \to \mathbb{N}$.

3.5.7 Proving the existence of a bijection

Theorem 13. *There exists a bijection from* $\mathbb{R} \to \mathcal{P}(\mathbb{N})$.

Proof. First we show there exists a bijection from $\mathbb{R} \to (0,\ 1)$.

Consider the function:

$$f(x) = \frac{1}{2} + \frac{1}{\pi}\tan^{-1}(x)$$

This function is continuous, strictly increasing and maps $\mathbb{R}$ to $(0,\ 1)$. Thus, this function is a bijection.

Next we construct a bijection from $(0,\ 1) \to (0,\ 1) \cup \mathbb{N}$ as:

$$g(x) = \begin{cases} n-1 & x = \dfrac{1}{n+1};\ n \in \mathbb{N},\ n \geq 1 \\ \dfrac{(k-1)n+1}{kn+1} & x = \dfrac{kn+1}{(k+1)n+1};\ k,\ n \in \mathbb{N},\ n \geq 1,\ k \geq 1 \\ x & \text{otherwise} \end{cases}$$

This function basically creates partitions of rationals into sets of all such $\frac{p}{q}$ whose $q-p=c$ is constant. Then it maps the smallest element of each partition to $c-1$, and then progressively maps the next element to the current element. For irrationals, it maps the number to itself.

Proving that the function is well defined and indeed a bijection is left as an exercise to the reader :)

Next we create a bijection from $(0,\ 1) \cup \mathbb{N} \to \mathcal{P}(\mathbb{N})$

Define a function $h : (0,\ 1) \cup \mathbb{N} \to \mathcal{P}(\mathbb{N})$ as:

- $h(0) = \phi$, $h(1) = \mathbb{N}$
- For $n \in \mathbb{N},\ n > 1$, construct a set $\mathbb{S}_n$ as:

  $$\mathbb{S}_n = \{k \mid (k+1)^{th} \text{ bit from the right of n in base 2 is 1.}\}$$

  Eg: For 37, base 2 representation is $(100101)_2$, and thus the set $S_{37} = \{0,\ 2,\ 5\}$
- For $x \in (0,\ 1)$, we use the non terminating binary representation of x. Every number in $(0,\ 1)$ can be represented in binary as $0.b_0b_1b_2\ldots$ where $b_i \in \{0,\ 1\}$. We then construct the set as:

  $$\mathbb{S}_x = \{k \mid b_k = 1\}$$

  Note : If the binary representation has only finite significant digits, we will enforce it to have infinite. Eg: $(0.65625)_{10} = 0.10101 = 0.1010011111111\ldots$ Thus, $S_{0.65625} = \{0, 2, 5, 6, 7, \ldots\}$

Finally,

$$h(x) = \begin{cases} \phi & x = 0 \\ \mathbb{N} & x = 1 \\ \mathbb{S}_n & x = n,\ n \in \mathbb{N}, n \geq 2 \\ \mathbb{S}_x & x \in (0,\ 1) \end{cases}$$

Then the required bijection from $\mathbb{R} \to \mathcal{P}(\mathbb{N})$ will be given as $\mathcal{H}(x) = h(g(f(x))) : \mathbb{R} \to \mathcal{P}(\mathbb{N})$ □

3.5.8 Cartesian product of countable sets

Theorem 14. *Cartesian product of countable sets is countable.*

Proof. Let $\mathbb{A}$ and $\mathbb{B}$ be countably infinite. Then define a bijection $f : \mathbb{A} \times \mathbb{B} \to \mathbb{N}$ as

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

□

3.5.9 Are Rationals countable??

Theorem 15. *There exists a bijection from* $\mathbb{Q} \to \mathbb{N}$

Proof. First, we will show that there exists an injection from $\mathbb{Q} \to \mathbb{N}$.

Let the rational number be given as $s \times \frac{p}{q}$ where $p,\ q \in \mathbb{N}$ and are co-prime, $q \neq 0$ and $s = -1$ or 1 depending on the sign of the rational number.

Consider the mapping,

$$f(s \times \frac{p}{q}) = 2^p 3^q 5^{s+1}$$

The fundamental theorem of arithmetic guarantees that the above mapping is injective. So, there exists an injection from $\mathbb{Q} \to \mathbb{N}$.

Also, since Q is infinite, we also know that there exists an injection from $\mathbb{N} \to \mathbb{Q}$. Thus by Schroder-Bernstein Theorem, there exists a bijection from $\mathbb{Q} \to \mathbb{N}$.

Thus, rationals are countable. $\square$

3.6 Cantor's Theorem and Cantor's Continuum Hypothesis

Theorem 16 (Cantor's Theorem)**.** *There exists no bijection from* $\mathbb{N} \to \mathcal{P}(\mathbb{N})$*. Since there exists a surjection from* $\mathcal{P}(\mathbb{N}) \to \mathbb{N}$*, the cardinality of* $\mathcal{P}(\mathbb{N})$ *is strictly greater than that of* $\mathbb{N}$*.*

Cantor's continuum hypothesis states that there exists no set whose cardinality is strictly between $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$.

3.7 Relations

A Relation R from $\mathbb{A} \to \mathbb{B}$ is a subset of $\mathbb{A} \times \mathbb{B}$. If $(a,\ b) \in R$, then we can write it as $a\ R\ b$. All functions are relations but not all relations are functions.

3.7.1 Partitions of a set

A partition of a set $\mathbb{S}$ is a set $\mathbb{P} \subset \mathcal{P}(\mathbb{S})$ such that:

- $\mathbb{S}' \in \mathbb{P} \rightarrow \mathbb{S}' \neq \phi$
- $\bigcup\limits_{\mathbb{S}' \in \mathbb{P}} \mathbb{S}' = \mathbb{S}$, ie, the union of the elements of a partition covers the entire set.
- If $\mathbb{S}_1,\ \mathbb{S}_2 \in \mathbb{P}$, then $\mathbb{S}_1 \cap \mathbb{S}_2 = \phi$, ie, the sets are disjoint.

If we define a partition on a set and then define a relation such that all elements in a partition are related to each other, we get a special type of relation.

3.7.2 Relation generated by partitions

Relations generated by partitions follow some special properties :

- Reflexivity : $\forall a \in \mathbb{A},\ (a,\ a) \in R$
- Symmetry : $\forall a,\ b \in \mathbb{A},\ (a,\ b) \in R \rightarrow (b,\ a) \in R$
- Transitivity : $\forall a,\ b,\ c \in \mathbb{A},\ (a,\ b) \in R \land (b,\ c) \in R \rightarrow (a,\ c) \in R$

A relation satisfying the above conditions is called an equivalence relation. Thus, from a partition we get an equivalence relation.

3.7.3 Equivalence Classes

Let R be an equivalence relation on set $\mathbb{S}$, and let $a \in \mathbb{S}$. The equivalence class of a, denoted as $[a]$ is defined as,

$$[a] = \{b \in \mathbb{S} \mid (a,\ b) \in R\}$$

Theorem 17.

$$aRb \longleftrightarrow [a] = [b] \longleftrightarrow [a] \cap [b] \neq \phi$$

Theorem 18. *If R is an equivalence relation on $\mathbb{S}$, then the equivalence classes of R form a partition of $\mathbb{S}$. In contrast, given a partition P of a set $\mathbb{S}$, there exists an equivalence relation R whose equivalence classes are exactly the sets of P.*

The proof of above theorem is quite simple and hence, left as an exercise to the reader.

3.7.4 Defining new Objects through equivalence relations

- Consider $R = \{((a,\ b),\ (c,\ d) \mid (a,\ b),\ (c,\ d) \in \mathbb{Z} \times \mathbb{Z}/\{0\},\ (ad = bc)\}$

  Then the equivalence classes of R define rational numbers. Eg: $(2,\ 4) \in [(1,\ 2)]$ is equivalent to saying $\frac{2}{4} = \frac{1}{2}$

  Similarly, equivalence classes of $R = \{((a,\ b),\ (c,\ d) \mid (a,\ b),\ (c,\ d) \in \mathbb{N} \times \mathbb{N},\ (a + d = b + c)\}$ define integers.

- Consider the relation $R([0, 1]) = \{aRb \mid a, b \in [0, 1], a = b \text{ or } (a, b) = (0, 1) \text{ or } (1, 0)\}$

  If we imagine the interval $[0, 1]$ as a thread of length 1, then the above relation describes a loop where we have glued the ends of the thread.

- Consider the relation
  $R([0,1] \times [0,1]) = \{(a,b)R(c,d) \mid (a,b) = (c,d) \text{ or } b = d, c = 0, a = 1 \text{ or } b = d, a = 0, c = 1\}$

  Imagining $[0,1] \times [0,1]$ as a square of side 1, the above relation describes joining the two vertical sides of the square together to form a cylinder.

- Similarly we can describe a torus through relations. Give it a try!

  Spoiler:

  Consider the relation
  $R([0,1] \times [0,1]) = \{(a,b)R(c,d) \mid (a,b) = (c,d) \text{ or } b = d, c = 0, a = 1 \text{ or } b = d, a = 0, c = 1 \text{ or } a = c, b = 0, d = 1 \text{ or } a = c, d = 0, b = 1 \text{ or } a, b, c, d \in \{0,1\}\}$

4 Basic Structures : Posets

4.1 Anti-Symmetry

Consider the relation $R = \{(a, b) \mid a, b \in \mathbb{Z}, a \leq b\}$. This relation is reflexive and transitive but not symmetric. In fact, it is "Anti-Symmetric".

A relation R on a set $\mathbb{S}$ is called anti-symmetric if $\forall\ a, b \in \mathbb{S}$, $(aRb\ \wedge bRa) \rightarrow a = b$.

Examples of anti-symmetric relations are:

- $R(\mathbb{Z}) = \{(a, b) \mid a, b \in \mathbb{Z},\ a \leq b\}$
- $R(\mathcal{P}(\mathbb{S})) = \{(\mathbb{A}, \mathbb{B}) \mid \mathbb{A}, \mathbb{B} \in \mathcal{P}(\mathbb{S}),\ \mathbb{A} \subseteq \mathbb{B}\}$

4.2 Partial Orders

A Partial Order is a relation which is reflexive, transitive and anti-symmetric. Partial orders are denoted by $a \preceq b$ instead of aRb.

There can be a case where some elements in a partial order may not be comparable by the operator defined by the order. That is why it is called a partial order.

A Total Order is then a Partial Order $\preceq$ on a set $\mathbb{S}$ in which every pair of elements is comparable.

In the above two examples, the first one is a total order while the second one is not (can you see why?).

4.3 Partially Ordered Sets : Posets

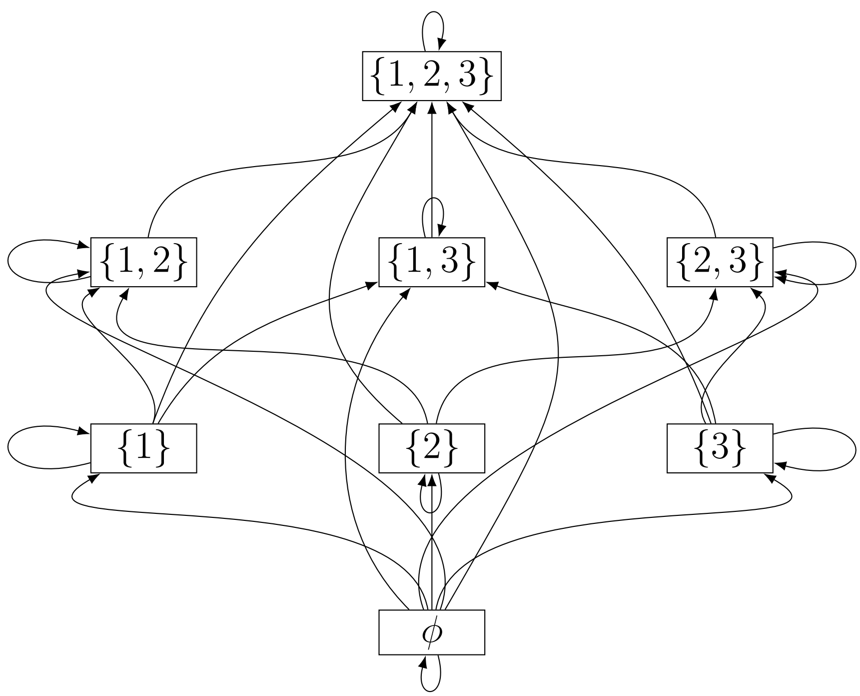
A set $\mathbb{S}$ together with a partial order $\preceq$ defined on it, is called a partially ordered set, or a poset, denoted as $(\mathbb{S}, \preceq)$.

Examples of Posets : $(\mathbb{Z},\ \leq)$, $(\mathbb{Z}^+,\ |\ )$, $(\mathcal{P}(\mathbb{S}),\ \subseteq)$ etc.

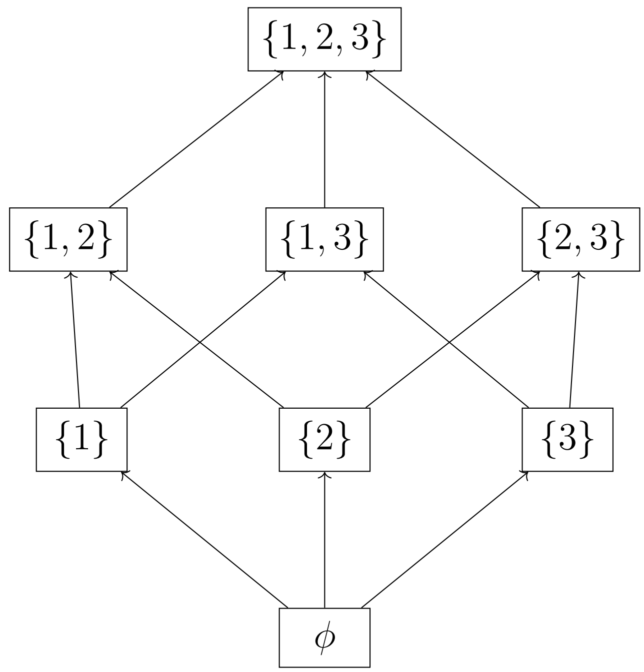
4.3.1 Graphical Representation of a Poset

Posets can be represented graphically as shown :

Graph of the Poset $(\mathcal{P}(\{1,2,3\}),\ \subseteq)$



The above directed tree becomes a bit messy for bigger posets. Thus we draw what is called a "Hasse Diagram" to keep things neat.



In a Hasse diagram, the edges showing reflexivity and transitivity are omitted. We show only those $x \preceq y$ where there exists no z such that $x \preceq z \preceq y$. The reflexive-transitive closure of the Hasse diagram gives back the original graph of the poset.

4.4 Chains and Anti-Chains

4.4.1 Chains

Let $(\mathbb{S}, \preceq)$ be a poset. Then a subset $\mathbb{A} \subseteq \mathbb{S}$ is called a chain if

$$\forall a,\ b \in \mathbb{A},\ a \preceq b\ \vee\ b \preceq a$$

That is, all pair of elements must be related to each other through the partial order. In other words, **a chain is a totally ordered subset of some partial order.**

4.4.2 Anti-Chains

Let $(\mathbb{S}, \preceq)$ be a poset. Then a subset $\mathbb{A} \subseteq \mathbb{S}$ is called an anti-chain if

$$\forall a,\ b \in \mathbb{A}, a \neq b,\ \neg(a \preceq b)\ \wedge\ \neg(b \preceq a)$$

That is, none of the elements in an anti-chain are related to each other through the partial order.

Example : In poset $(\{1,2,3\},\ \subseteq)$, the set $\{\ \phi, \{1\}, \{1,2\}, \{1,2,3\}\ \}$ is a chain while the set $\{\ \{1,2\}, \{2,3\}, \{1,3\}\ \}$ is an antichain.

4.5 Topological Sort

A Topological Sort or Linearization of a poset $(\mathbb{S}, \preceq)$ is a totally ordered set $(\mathbb{S}, \preceq_t)$ with a total order $\preceq_t$ defined on it such that $x \preceq y \rightarrow x \preceq_t y$.

4.5.1 Minimal Element

An element x in a poset is called a minimal element if there is no element $\nexists y \in \mathbb{S}, y \prec x$.

Theorem 19. *Every finite non-empty poset has a set of minimal elements.*

Proof. We will prove this theorem using induction.

- Base case : Consider a poset of 1 element, $(\mathbb{S}_1 = \{a_1\}, \preceq)$

  Here a_1 is the minimal element $\nexists b \in \mathbb{S}_1,\ b \prec a_1$.

  Thus, the base case is satisfied.

- Induction hypothesis : Let any poset of k elements, $(\mathbb{S}_k = \{a_1, \ldots, a_k\}, \preceq),\ k \geq 1$ have a set of minimal elements.

- Induction step : Consider any poset of k+1 elements, $(\mathbb{S}_{k+1} = \{a_1, \ldots, a_k, a_{k+1}\}, \preceq)$

  Now consider the poset obtained by removing the element a_{k+1} from this poset, ie, $(\mathbb{S}'_{k+1} = \mathbb{S}_{k+1} - \{a_{k+1}\} = \{a_1, \ldots, a_k\}, \preceq)$

  By our induction hypothesis, there exists a set of minimal elements in $\mathbb{S}'_{k+1}$, let that be $\mathbb{X} = \{l_1, \ldots, l_n\}$, ie, $\forall b \in \mathbb{S}'_{k+1}\ \exists l_i \in \mathbb{X}, l_i \preceq b$.

  Now, there are the following cases:

  1. $\exists l_i \in \mathbb{X},\ l_i \preceq a_{k+1}$, in which case, that l_i will still be a minimal element.

  2. Either a_i and a_{k+1} are incomparable in the poset $\mathbb{S}_{k+1}$. In that case a_i would still be a minimal element as both $a_{k+1} \preceq a_i$ and $a_i \preceq a_{k+1}$ are false, and thus $\nexists b \in \mathbb{S}_{k+1}, b \prec a_i$.

  3. $a_i \preceq a_{k+1}$ in which case a_i would still be a minimal element as $\nexists b \in \mathbb{S}_{k+1}, b \prec a_i$.

  4. $a_{k+1} \preceq a_i$ in which case a_{k+1} would become a minimal element as, by transitivity, $a_{k+1} \preceq a_i\ \rightarrow\ \forall b \in \mathbb{S}_{k+1}, (a_i \preceq b \rightarrow a_{k+1} \preceq b)$, and thus $\nexists b \in \mathbb{S}_{k+1},\ b \prec a_{k+1}$.

  Thus, if a poset of size k has a minimal element, then a poset of size k+1 also has a minimal element.

Thus, by induction, we conclude that every finite non-empty poset has a minimal element. □

The above lemma can then be used to prove another important theorem.

Theorem 20. *Every finite non-empty poset has a topological sort.*

Proof. Let there be a finite non-empty poset $(\mathbb{S}, \preceq)$ of n elements. We give an inductive algorithm to construct a topological sort:

- Start with the minimal element of $\mathbb{S}$, say x_1. This is a chain consistent with $\preceq$.
- Suppose that we have already constructed a chain of k elements $(1 \leq k < n)$ consistent with $\preceq$, $x_1 \preceq_t \ldots \preceq_t x_k$.
- Consider the poset $\mathbb{S}' = \mathbb{S} - \{a_1, \ldots, a_k\}$. Let us say its minimal element is x_{k+1}.
- Then $x_1 \preceq_t \ldots \preceq_t x_k \preceq_t x_{k+1}$ is a chain of $k + 1$ elements consistent with $\preceq$. If not, then $\exists i \in \{1, \ldots, k\}$, $x_{k+1} \preceq x_i$, but $x_i \preceq_t x_{k+1}$, but then it violates the minimality of x_i at the i^{th} step.
- Thus, after n steps we get a chain of n elements $x_1 \preceq_t \ldots \preceq_t x_n$ consistent with our partial order $\preceq$.

Using this algorithm, we can generate a topological sort of any finite non-empty poset, and hence there must exist a topological sort on every finite non-empty poset. □

4.5.2 Parallel Task Scheduling

For any non-empty and finite poset, there is a legal parallel schedule that runs in t steps, where t is the size of the longest chain.

This result is infact the consequence of the following theorem:

Theorem 21. *For a non-empty, finite poset* $(\mathbb{S}, \preceq)$ *with size of longest chain* $= t$*, we can partition* $\mathbb{S}$ *into* t *subsets* $\mathbb{S}_1, \ldots, \mathbb{S}_t$ *such that* $\forall i \in \{1, \ldots, t\}$, $\forall a \in \mathbb{S}_i$, $b \prec a \to b \in \mathbb{S}_1 \cup \cdots \cup \mathbb{S}_{i-1}$

Proof. Place each $a \in \mathbb{S}$ in $\mathbb{S}_i$ where i is the length of the longest chain that ends at a.

Now suppose $\exists i, a \in S_i,\ b \prec a$ but $b \notin \mathbb{S}_1 \cup \cdots \cup \mathbb{S}_{i-1}$.

By the definition of $\mathbb{S}_i$, $\exists$ a chain of size at least i that ends at b.

But then $b \prec a$ implies that we can extend that chain to another chain of size $i + 1$ ending at a.

But that contradicts the fact that $a \in \mathbb{S}_i$

Thus $\forall a \in \mathbb{S}_i$, $b \prec a \to b \in \mathbb{S}_1 \cup \cdots \cup \mathbb{S}_{i-1}$ □

Using this theorem, we can then schedule all tasks in $\mathbb{S}_i$ at time i (since all previous tasks were done earlier!). So, each $\mathbb{S}_i$ is an anti-chain.

Since each $\mathbb{S}_i$ is an anti-chain, the above theorem was restated in a different way as Mirsky's Theorem.

Theorem 22 (Mirsky's Theorem)**.** *If the largest chain in a poset* $(\mathbb{S}, \preceq)$ *is of size* t*, then* $\mathbb{S}$ *can be partitioned into* t *anti-chains.*

And as a consequence of the above theorem comes the below corollary.

Theorem 23 (Dilworth's Lemma)**.** $\forall t > 0$ *any poset with* n *elements must have either a chain of size greater than* t *or an anti chain with at least* $\lceil \frac{n}{t} \rceil$ *elements.*

The proofs of the above theorems are trivial and hence left as an exercise to the reader :)

4.6 Minimal and maximal elements

Let $(\mathbb{S}, \preceq)$ be a poset.

An element a of $\mathbb{S}$ is a minimal element of the poset if $\forall b \in \mathbb{S}, b \preceq a \to b = a$.

An element a of $\mathbb{S}$ is a maximal element of the poset if $\forall b \in \mathbb{S}, a \preceq b \to a = b$.

An element a of $\mathbb{S}$ is the least element of the poset if $\forall b \in \mathbb{S}, a \preceq b$.

An element a of $\mathbb{S}$ is the greatest element of the poset if $\forall b \in \mathbb{S}, b \preceq a$.

4.6.1 Upper Bounds and Lower Bounds

Let $(\mathbb{S}, \preceq)$ be a partially ordered set, and $\mathbb{A} \subseteq \mathbb{S}$.

An element $u \in \mathbb{S}$ is called an upper bound for $\mathbb{A}$ if $\forall a \in \mathbb{A}, a \preceq u$.

An element $l \in \mathbb{S}$ is called a lower bound for $\mathbb{A}$ if $\forall a \in \mathbb{A}, l \preceq a$.

An element $u \in \mathbb{S}$ is called a least upper bound for $\mathbb{A}$ if it is an upper bound and for all upper bounds u', $u \preceq u'$.

An element $l \in \mathbb{S}$ is called a greatest lower bound for $\mathbb{A}$ if it is a lower bound and for all lower bounds l', $l' \preceq l$.