

Naive Set Theory

Set Notation

Universal set	\mathbb{U}
Empty set	$\emptyset = \{\}$, Remember: $\forall A (\emptyset \subset A)$
Power set	$\mathcal{P}(A)$ is the set of all the subsets of A .
Partition of A	A collection of nonempty, pairwise-disjoint subsets whose union is A .
Element of	\in . Example: $2 \in \{1, 2, 3\}$
Subset of	\subseteq . Example: $\{A, B, C\} \subseteq \{B, C, D\}$
Proper subset of	$A \subsetneq B \Leftrightarrow \forall x$
Intersection	\subset . Example: $\{A, B, C\} \subset \{A, B, C, D\}$
Union	$\bigcap_{i \in I} A_i = \{x \in \mathbb{U} \mid \forall i \in I, x \in A_i\}$
Difference	$A \cap B = \{x \in \mathbb{U} \mid x \in A \wedge x \in B\}$
Symmetric difference	$\bigcup_{i \in I} A_i = \{x \in \mathbb{U} \mid \exists i \in I, x \in A_i\}$
Cartesian Product	$A \cup B = \{x \in \mathbb{U} \mid x \in A \vee x \in B\}$
Complement of	$A \setminus B = \{x \in A \mid x \notin B\}$
	$A \Delta B = (A \setminus B) \cup (B \setminus A)$
	$A \times B = \{(x, y) \mid x \in A \wedge y \in B\}$
	$A^C = \bar{A} = \{x \in \mathbb{U} \mid x \notin A\}$

Cardinality

Cardinality($ A $)	The number of elements in a set.
finite set	Let X be a finite set then $ X \in \mathbb{N}$
countable set	A set S is countable if and only if that is finite or $ S = \mathbb{N} $.
aleph null.	$\aleph_0 = \mathbb{N} $

Axiom 1 (Axiom of extensionality) Two sets are equal if and only if they have the same elements.

Theorem 1 Let A and B be sets, then $|A| = |B|$ if and only if there is a one-to-one correspondence from A to B .

Theorem 2 If A and B are countable, then $A \cup B$ is countable.

Theorem 3 (Cantor's Theorem) For every set A , $|A| < |\mathcal{P}(A)|$.

Theorem 4 (Schröder–Bernstein) If there are injective functions $f : A \rightarrow B$ and $g : B \rightarrow A$, then there is a one-to-one correspondence between A and B . In other words If A and B are sets with $|A| \neq |B|$ and $|B| \neq |A|$, then $|A| = |B|$.

Theorem 5 (Well-Ordering Principle) Every nonempty subset of \mathbb{N} has a least element.

Properties 1 Let S be the universal set.

- if $A \subseteq B$ and $B \subseteq A$ then $A = B$.
- $\forall A, A \subseteq A$
- $|\mathcal{P}(A)| = 2^{|A|}$
- $A \cup A = A \cap A = A$
- $A \cup \emptyset = A$
- $A \cap \emptyset = \emptyset$
- $A \cup S = S$
- $A \cap S = A$
- $(A \cup B) \cup C = A \cup (B \cup C)$
- $(A \cap B) \cap C = A \cap (B \cap C)$
- $A \cup B = B \Leftrightarrow A \subseteq B$
- $A \cup B = A \Leftrightarrow A \subseteq B$
- $A \setminus B \neq B \setminus A$
- $A \setminus \emptyset = A$
- $A \setminus S = \emptyset$
- $A \setminus \emptyset = A \Leftrightarrow A \subseteq B$
- $A \setminus S = A^C$
- $A \times (B \cup C) = (A \times B) \cup (A \times C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $(A \cup B)^C = A^C \cap B^C$
- $(A \cap B)^C = (A \setminus C) \cap (B \setminus C) = A \cap (B \setminus C)$
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Functions

Functions	A rule that assigns each input exactly one output.
Domain	The set of all input of a function. (X in $f : X \rightarrow Y$)
Codomain	The set of all output of a function. (Y in $f : X \rightarrow Y$)
Range	Is the subset of Y of elements that have an antecedent in X by f
$f : x \rightarrow y$	a function f with a domain x and a codomain y .
Recursive f.	every element of the codomain is the image of $f(a) = f(b) \Rightarrow a = b$
Injective	at most one element from the domain.
Surjective	every element of the codomain is the image of at least one element from the domain.
Bijective	A function that is Injective and Surjective .
Image	$f(A) = \{f(a) \in Y : a \in A\}$, where $A \subset \text{domain}$.
Inverse Image	$f^{-1}(B) = \{f(b) \in X : b \in B\}$, where $B \subset \text{codomain}$.
Set of Function	B^A contains all functions from A to B ($A \rightarrow B$).

Counting

n-bit string	the number of 1 in a bit string.
bit string weight	the set of all n-bit strings of weight k.
B_k^n	$n! = n \cdot (n - 1) \cdot (n - 2) \cdot \dots \cdot 1$
Factorial	

Additive Principle

General Definition: if event A can occur in m ways, and even B can occur in n disjoint (A and B can't happen at the same time.) ways, then A and B can occur in $m + n$ ways.

Set Definition: Given 2 sets A and B , then $|A \cup B| = |A| + |B| - |A \cap B|$. Given 3 sets A, B and C , then $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |C \cap B| + |A \cap B \cap C|$.

Multiplicative Principle

General Definition: if event A can occur m ways, and each possibility for A allows for exactly n ways for event B , then the event "A and B" can occur $m \cdot n$ ways.

Set Definition: Given 2 sets A and B , we have $|A \times B| = |A| \cdot |B|$.

Permutations

Definition: Ordered selections of k distinct elements drawn from an n -element set.

- Without repetition: $P(n, k) = \frac{n!}{(n-k)!}$
- With repetition of symbols allowed from an alphabet of size m : m^k length- k strings.

Combinations

Definition: Unordered selections of k elements from an n -element set.

- Without repetition: $C(n, k) = \binom{n}{k}$
- With repetition allowed: $C_{\text{rep}}(n, k) = \binom{n+k-1}{k}$

Binomial coefficient

Formula: n choose $k = \binom{n}{k} = \frac{n!}{(n-k)!k!}$

Theorem 6 (Binomial Theorem) $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$

Properties 2 • $\binom{n}{k}$ is the number of subset of size n each of cardinality k . • $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ • $\binom{n}{k} = |\mathbf{B}_k^n|$ • $\sum_{k=0}^n \binom{n}{k} = 2^n$

Symbolic Logic

Name	Symbol	Translate to
Conjunction	$A \wedge B$	A and B .
Disjunction	$A \vee B$	A or B .
Negation	$\neg A$	not A .
Condition/Implication	$A \Rightarrow B$	if A then B .
Bicondition	$A \Leftrightarrow B$	if and only if A then B .
Exclusive Disjunction	$A \oplus B$	Either A or B , but not both.
Universal	$\forall x$	For all x 's.
Existential	$\exists x$	There is at least one x .
Unique Existential	$\exists!x$	There is exactly one x .
Equivalence	$A \equiv B$	A is identical to B .

Converse: $B \Rightarrow A$ is the converse of $A \Rightarrow B$.

Contrapositive: $\neg B \Rightarrow \neg A$ is the Contrapositive of $A \Rightarrow B$.

Important Equivalences & Properties

- $\neg(\neg A) \equiv A$ • $p \wedge T \equiv p$ • $p \wedge \perp \equiv \perp$ • $p \vee T \equiv T$ • $p \vee \perp \equiv p$
- $A \oplus B \equiv (A \vee B) \wedge \neg(A \wedge B)$ • $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$ • $p \Rightarrow q \equiv \neg p \vee q$
- $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$ • $\neg(p \Leftrightarrow q) \equiv \neg p \Leftrightarrow q \equiv p \Leftrightarrow \neg q$
- $\neg B \Rightarrow \neg A \equiv A \Rightarrow B$

Properties 3 • $A \vee B \equiv B \vee A$ • $A \vee (B \vee C) \equiv C \vee (A \vee B)$

- $A \wedge B \equiv B \wedge A$ • $A \wedge (B \wedge C) \equiv C \wedge (A \wedge B)$ • $A \oplus B \equiv B \oplus A$
- $A \oplus (B \oplus C) \equiv C \oplus (A \oplus B)$

deMorgan Laws

- $\neg \forall x P(x) = \exists x \neg P(x)$ • $\neg \exists x P(x) = \forall x \neg P(x)$
- $\neg \exists x \exists y P(x, y) = \forall x \forall y \neg P(x, y)$ • $\neg (\bigwedge_{i=0}^n a_i) = \bigvee_{i=0}^n \neg a_i$
- $\neg (\bigvee_{i=0}^n a_i) \equiv \bigwedge_{i=0}^n \neg a_i$

Proofs

Rules of inference

Modus Ponens	If $p \Rightarrow q$ and p , then q .
Modus Tollens	If $p \Rightarrow q$ and $\neg q$, then $\neg p$.
Hypothetical Syllogism	If $p \Rightarrow q$ and $q \Rightarrow R$, then $p \Rightarrow R$.
Disjunctive Syllogism	If $p \vee q$ and $\neg q$, then p .
Addition	If p , then $p \vee q$.
Simplification	If $p \wedge q$, then p .
Conjunction	If p and q , then $p \wedge q$.
Absorption	If $p \Rightarrow q$, then $p \Rightarrow (p \wedge q)$.
Resolution	If $P \vee Q$ and $\neg P \vee R$, then $Q \vee R$.

Direct Proof

Goal: Prove $p \Rightarrow q$.

Idea: Assume p and use definitions/algebra to derive q .

Proof by Contrapositive

Goal: Prove $p \Rightarrow q$.

Idea: Instead of proving $p \Rightarrow q$, prove $\neg q \Rightarrow \neg p$.

Proof by Counter Example

Goal: Disprove $\forall x P(x)$ (show $\exists x \neg P(x)$).

Idea: Exhibit a specific counterexample x_0 with $\neg P(x_0)$.

Proof by Cases

Goal: Prove the claim.

Idea: Split into exhaustive, mutually exclusive cases and prove the claim in each case.

Proof by Contradiction

Goal: Prove a statement S .

Idea: Assume $\neg S$ and derive a contradiction; conclude S .

Proof by Mathematical Induction

Goal: Prove $\forall n \geq n_0, P(n)$.

Base Case: Verify $P(n_0)$ (and additional initial values if required).

Inductive Step: Assume $P(k)$ holds for an arbitrary $k \geq n_0$ (inductive hypothesis) and show $P(k+1)$ holds.

Conclusion: If both steps succeed, the principle of mathematical induction yields $P(n)$ for all $n \geq n_0$.

Proof by Strong Induction

Goal: Prove $\forall n \geq n_0, P(n)$.

Base Case(s): Establish $P(n_0), P(n_0 + 1), \dots, P(n_0 + r)$ as needed.

Inductive Step: Assume $P(n_0), P(n_0 + 1), \dots, P(k)$ all hold (strong hypothesis) and deduce $P(k+1)$.

Conclusion: By strong induction, $P(n)$ holds for every $n \geq n_0$.

Graphs

A **graph** is an ordered pair $G = (V, E)$, where V is a nonempty set of **vertices** and E is a nonempty set of **edges**.

Vertices	elements of set V in a graph. The dots in the drawing.
edges	connections between vertices (elements of set E). The lines in the drawing.
adjacent	if 2 edges are connected by a vertice.
morphism	a mapping from the vertices and edges of one graph to the vertices and edges of another graph that preserves incidence.
isomorphism	a bijective morphism.
isomorphic	if there is an isomorphism between 2 graphs.
automorphism	is an isomorphism from a graph to itself.
Degree of a vertex	is the number of edges incident to the vertex.
incoming degree	number of edges coming into a vertex.
outgoing degree	number of edges going out of a vertex.
adjacency matrix	is the a matrix representation of a graph. $A = [a_{ij}]$ where a_{ij} equals 1 if $\{i, j\} \in E$ and 0 otherwise, $i \in V, j \in V$ for $G = V, E$.
path	an ordered sequence of successive edges
connected	if there is a path between every pair of vertices.
cycle	a path that starts and ends at the same vertex.
acyclic	a graph with no cycles.
tree	a connected acyclic graph.
subgraph	a graph $H = (V_H, E_H)$ is a subgraph of $G = (V_G, E_G)$ if $V_H \subseteq V_G$ and $E_H \subseteq E_G$.
partial graph	a subgraph that contains all the vertices of G .
Induced subgraph	a subgraph H of G such that if $u, v \in V_H$ and $\{u, v\} \in E_G$, then $\{u, v\} \in E_H$.
bipaetite graph	a graph whose vertices form 2 disjoint sets where each edge connects vertices from different sets. Thos graphs are bi colorable

Directed Vs Undirected Graphs

In a **directed graph**, edges have a direction. Such that $E = \{(\dots), \dots\}$ for **directed graph** and $E = \{\{\dots\}, \dots\}$ for **undirected graph**.

Lemma 1 (Handshaking Lemma) *Let $G = (V, E)$ be a finite undirected graph, then:*

$$\sum_{v \in V} \deg(v) = 2|E|$$