Discrete Mathematics

Class: MATH 2410

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: $\{A, B, C\} \subseteq \{B, C, D\}$ $A \subseteq B \Leftrightarrow \forall x$
Proper subset of	$\subset$. Example: $\{A, B, C\} \subset \{A, B, C, D\}$
Intersection	$\bigcap_{i \in I} A_i = \{x \in \mathbb{U} \mid \forall i \in I, x \in A_i\}$ $A \cap B = \{x \in \mathbb{U} \mid x \in A \wedge x \in B\}$
Union	$\bigcup_{i \in I} A_i = \{x \in \mathbb{U} \mid \exists i \in I, x \in A_i\}$ $A \cup B = \{x \in \mathbb{U} \mid x \in A \vee x \in B\}$
Difference	$A \backslash B = \{x \in A \mid x \notin B\}$
Symmetric difference	$A \Delta B = (A \backslash B) \cup (B \backslash A)$
Cartesian Product	$A \times B = \{(x, y) \mid x \in A \wedge y \in B\}$
Complement of	$A^C = \bar{A} = \{x \in \mathbb{U} \mid x \notin A\}$

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 finit or $\|S\| = \|\mathbb{N}\|$.
aleph null.	$\aleph_0 = \|\mathbb{N}\|$ by definition.

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 function(one-to-one) functions $f : A \to B$ and $g : B \to A$, then there is a one-to-one correspondence between A and B. In other words If A and B are set 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 $A = b$.* • $\forall A, A \subseteq A$ • $|\mathcal{P}(A)| = 2^{|A|}$ • $A \cup A = A \cap A = A$ • $A \cup \emptyset = A$ • $A \cap \emptyset = \emptyset$ • $A \cup S = S$ • $A \cap S = A$ • $(A \cup B) \cup C = A \cup (B \cup C)$ • $(A \cap B) \cap C = A \cap (B \cap C)$ • $A \cup B = B \Leftrightarrow A \subseteq B$ • $A \cup B = A \Leftrightarrow A \subseteq B$ • $A \backslash B \neq B \backslash A$ • $A \backslash \emptyset = A$ • $A \backslash S = \emptyset$ • $A \backslash \emptyset = A \Leftrightarrow A \subseteq B$ • $A \backslash S = A^C$ • $A \times (B \cup C) = (A \times B) \cup (A \times C)$ • $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ • $(A \cup B)^C = A^C \cap B^C$ • $(A \cap B) \backslash C = (A \backslash C) \cap (B \backslash C) = A \cap (B \backslash C)$ • $A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C)$

Functions

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

Counting

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

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 apen 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: $P(n, k) = \dfrac{n!}{(n-k)!}$. • 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. • $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ • $\binom{n}{k} = |\mathbf{B}_\mathbf{k}^\mathbf{n}|$ • $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

Theorem 7 (Pigeonhole Principle) *If* n *items are put into* m *containers, then at least one container must contain at least* $\lceil \frac{n}{m} \rceil$ *items.*

Symbolic Logic

Name	Symbol	Translate to
Conjunction	$A \wedge B$	A and B.
Disjonction	$A \vee B$	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

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

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

deMorganLaws

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

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.
Conjuction	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 $n \geq n_0$.
Strong induction: In the inductive step, assume $P(n_0), P(n_0+1), \ldots, P(k)$ to show $P(k+1)$.

Theorem 8 *There are infinitely many prime numbers.*

Graphs

A **graph** is an ordered pair $\boxed{\text{G=(V,E)}}$, where V is a nonempty set of **vertices** and E is a nonempty set of **edges**.
Named Graphs:

K_n	complete graph on n vertices. (every pair of distinct vertices is adjacent)
$K_{m,n}$	complete bipartite graph with parts of sizes m and n. (all possible edges between the first and second sets)
C_n	an n-vertex cycle.
P_n	an n-vertex path.

Directed Vs Undirected Graphs

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

Computing adjacency matrix

Let a graph G with n vertices and the adjacency matrix $A_{n \times n}$. The entry a_{ij} is 1 if there is an edge from vertex i to vertex j, and 0 otherwise.

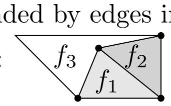
Basic Definitions

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.
loop	an edge that connects a vertex to itself.
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	is the number of edges incident to the vertex. Denoted $\deg(v)$, the biggest degree of any vertex is denoted $\Delta(G)$.
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.
clique	a subset of vertices such that every 2 distinct vertices are adjacent (special induced subgraph).
clique number	the size of the largest clique in a graph G.
complete graph	a graph in which every pair of distinct vertices is connected by a unique edge.

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

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

Special Graphs

simple	a graph with no loops or multiple edges.
multigraph	a graph that is not simple.
acyclic	a graph with no cycles.
tree	a connected graph whith no cycles (acyclic).
forest	an acyclic graph.
spanning tree	a subgraph of a connected graph that is a tree containing all the vertices of G.
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 $\{u, v\} \in E_H$.
bipartite graph	a graph whose vertices form 2 disjoint sets where each edge connects vertices from different sets.
planar graph	a graph that can be drawn without any edges crossing.
faces	the regions bounded by edges in a planar graph. Example: 
Euler's Formula	Consider a planar graph with v vertices, e edges, and f faces, then this graph satisfies: $\boxed{\text{v-e+f=2}}$.

Properties 4 (Tree and Forest) • *A graph T is a tree if and only if there is a unique path between any 2 vertices of T.* • *A graph F is a forest if and oxnly if for every pair of vertices in F, there is at most one path between them.* • *Every connected graph has a spanning tree.* • *K_5 is the smallest non planar complete graph.*

Graph Coloring

vertex coloring	an assignment of colors to the vertices of a G.
edges coloring	an assignment of colors to the edges of a G.
proper coloring	a coloring of a graph such that no 2 adjacent vertices or edges share the same color.
k- colorable	a graph that can be colored with k colors.
chromatic number	the minimum number of colors needed to color the vertices of a graph G. Denoted $\chi(G)$.
chromatic index	the minimum number of colors needed to color the edges of a graph G. Denoted $\chi'(G)$.

Properties 5 • *A graph is 2-colorable if and only if it is bipartite.* • *A clique of size n cannot be colored with less than n colors.* • *The chromatic number of a complete graph K_n is n.*

Theorem 9 (Four Color Theorem) *If G is a planar graph, then its chromatic number is less or equal to 4.*

Theorem 10 (brook's Theorem) *Any graph G satisfies $\chi(G) \leq \Delta(G) + 1$.*

Theorem 11 (vizing's Theorem) *For any simple graph G, the chromatic index $\chi'(G)$ is either $\Delta(G)$ or $\Delta(G) + 1$.*

Theorem 12 *The chromatic number of a graph $G \geq$ the clique number of G.*

Euler and Hamiltonian Graphs

Euler path	a walk through the graph which uses every edge.
Euler circuit	an Euler path that starts and ends at the same vertex.
Hamiltonian path	a path that visits every vertex exactly once.
Hamiltonian cycle	a Hamiltonian path that starts and ends at the same vertex.

Properties 6 • *A graph has an Euler circuit iff the degree of every vertex is even.* • *A graph has an Euler path if and only if there are at most two vertices with odd degrees.*

Theorem 13 (Dirac Thm) *If G is a simple graph with $n \geq 3$ vertices such that the degree of every vertex in G is at least $n/2$, then G has a* ***Hamiltonian circuit****.*

Theorem 14 (Ore Thm) *If G is a simple graph with $n \geq 3$ vertices such that for every pair of non-adjacent vertices u and v, $\deg(u) + \deg(v) \geq n$, then G has a* ***Hamiltonian circuit****.*

General Tips

- $\sqrt{x^2} = |x|, x \in \mathbb{R}$ • $(\sqrt{x})^2 = x, x \geq 0$ • $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ • $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$
- $(a+b)^3 = a^3 + b^3 + 3ab(a+b)$ • $(a-b)^3 = a^3 - b^3 - 3ab(a-b)$ • $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$ • $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$