Discrete Mathematics Summary

Mathematical Notes

October 19, 2025

Contents

1 Logic and Proofs

1.1 Propositional Logic

Definition 1.1. A **proposition** is a declarative sentence that is either true or false, but not both.

1.2 Logical Connectives

- **Negation**: $\neg p$ (not p)
- **Conjunction**: $p \wedge q$ (p and q)
- **Disjunction**: $p \vee q$ (p or q)
- **Implication**: $p \rightarrow q$ (if p then q)
- **Biconditional**: $p \leftrightarrow q$ (p if and only if q)

1.3 Truth Tables

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \rightarrow q$
T	T	F	T	T	T
T	F	F	F	T	F
F	T	T	F	T	T
F	F	T	F	F	T

1.4 Logical Equivalences

- **Double Negation**: $\neg(\neg p) \equiv p$
- **De Morgan's Laws**:
  - $\neg(p \wedge q) \equiv \neg p \vee \neg q$
  - $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- **Commutative Laws**: $p \wedge q \equiv q \wedge p$, $p \vee q \equiv q \vee p$
- **Associative Laws**: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- **Distributive Laws**:
  - $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  - $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- **Implication**: $p \rightarrow q \equiv \neg p \vee q$
- **Contrapositive**: $p \rightarrow q \equiv \neg q \rightarrow \neg p$

1.5 Predicate Logic

Definition 1.2. A **predicate** is a statement involving variables that becomes a proposition when specific values are substituted for the variables.

1.6 Quantifiers

- **Universal Quantifier**: $\forall x P(x)$ (for all x, $P(x)$)
- **Existential Quantifier**: $\exists x P(x)$ (there exists an x such that $P(x)$)

1.7 Methods of Proof

- **Direct Proof**: Assume p is true, show q is true
- **Proof by Contraposition**: Prove $\neg q \to \neg p$
- **Proof by Contradiction**: Assume $\neg(p \to q)$, derive a contradiction
- **Proof by Cases**: Consider all possible cases
- **Mathematical Induction**:
  1. Base case: Show $P(1)$ is true
  2. Inductive step: Show $P(k) \to P(k+1)$ for all $k \geq 1$

2 Sets

2.1 Basic Definitions

Definition 2.1. A **set** is an unordered collection of distinct objects called elements.

2.2 Set Operations

- **Union**: $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- **Intersection**: $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- **Complement**: $\overline{A} = \{x : x \notin A\}$
- **Difference**: $A - B = \{x : x \in A \text{ and } x \notin B\}$
- **Symmetric Difference**: $A \triangle B = (A - B) \cup (B - A)$

2.3 Set Identities

- **Commutative Laws**: $A \cup B = B \cup A$, $A \cap B = B \cap A$
- **Associative Laws**: $(A \cup B) \cup C = A \cup (B \cup C)$
- **Distributive Laws**:
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- **De Morgan's Laws**:
  - $\overline{A \cup B} = \overline{A} \cap \overline{B}$
  - $\overline{A \cap B} = \overline{A} \cup \overline{B}$

2.4 Cardinality

Definition 2.2. The **cardinality** of a set A, denoted $|A|$, is the number of elements in A.

2.5 Power Set

Definition 2.3. The **power set** of a set S, denoted $\mathcal{P}(S)$, is the set of all subsets of S.

Theorem 2.1. If $|S| = n$, then $|\mathcal{P}(S)| = 2^n$.

3 Functions

3.1 Basic Definitions

Definition 3.1. A **function** f from set A to set B is a relation that assigns to each element $a \in A$ exactly one element $b \in B$. We write $f : A \to B$.

3.2 Types of Functions

- **One-to-one (Injective)**: $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$
- **Onto (Surjective)**: For every $b \in B$, there exists $a \in A$ such that $f(a) = b$
- **Bijective**: Both one-to-one and onto

3.3 Composition and Inverse

- **Composition**: $(g \circ f)(x) = g(f(x))$
- **Inverse**: $f^{-1}(y) = x$ if and only if $f(x) = y$

4 Relations

4.1 Basic Definitions

Definition 4.1. A **relation** R from set A to set B is a subset of $A \times B$.

4.2 Properties of Relations

For a relation R on set A:

- **Reflexive**: $(a, a) \in R$ for all $a \in A$
- **Symmetric**: $(a, b) \in R \Rightarrow (b, a) \in R$
- **Antisymmetric**: $(a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$
- **Transitive**: $(a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$

4.3 Equivalence Relations

Definition 4.2. An **equivalence relation** is a relation that is reflexive, symmetric, and transitive.

4.4 Partial Orders

Definition 4.3. A **partial order** is a relation that is reflexive, antisymmetric, and transitive.

5 Combinatorics

5.1 Basic Counting Principles

- **Sum Rule**: If task can be done in m ways and another in n ways, then one or the other can be done in $m+n$ ways
- **Product Rule**: If task can be done in m ways and another in n ways, then both can be done in $m \times n$ ways

5.2 Permutations

Definition 5.1. A **permutation** is an ordered arrangement of objects.

- **Permutations of n objects**: $P(n,n) = n!$
- **Permutations of r objects from n**: $P(n,r) = \frac{n!}{(n-r)!}$

5.3 Combinations

Definition 5.2. A **combination** is an unordered selection of objects.

- **Combinations of r objects from n**: $C(n,r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}$

5.4 Binomial Theorem

Theorem 5.1.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

5.5 Pigeonhole Principle

Theorem 5.2. If n objects are placed into m boxes where $n > m$, then at least one box contains more than one object.

6 Graph Theory

6.1 Basic Definitions

Definition 6.1. A **graph** $G = (V, E)$ consists of a set V of vertices and a set E of edges.

6.2 Types of Graphs

- **Simple Graph**: No loops or multiple edges
- **Multigraph**: May have multiple edges
- **Pseudograph**: May have loops and multiple edges
- **Directed Graph**: Edges have direction
- **Complete Graph**: Every pair of vertices is connected
- **Bipartite Graph**: Vertices can be partitioned into two sets with no edges within each set

6.3 Graph Terminology

- **Degree**: Number of edges incident to a vertex
- **Path**: Sequence of vertices connected by edges
- **Circuit**: Path that starts and ends at the same vertex
- **Connected**: Path exists between any two vertices
- **Tree**: Connected graph with no circuits

6.4 Handshaking Theorem

Theorem 6.1. The sum of the degrees of all vertices in a graph equals twice the number of edges.

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

6.5 Euler and Hamiltonian Paths

- **Euler Path**: Uses every edge exactly once
- **Euler Circuit**: Euler path that starts and ends at the same vertex
- **Hamiltonian Path**: Visits every vertex exactly once
- **Hamiltonian Circuit**: Hamiltonian path that starts and ends at the same vertex

6.6 Planar Graphs

Definition 6.2. A graph is **planar** if it can be drawn in the plane without edge crossings.

Theorem 6.2 (Euler's Formula)**.** For a connected planar graph with V vertices, E edges, and F faces:

$$V - E + F = 2$$

7 Number Theory

7.1 Divisibility

Definition 7.1. An integer a **divides** an integer b (written $a|b$) if there exists an integer c such that $b = ac$.

7.2 Properties of Divisibility

- If $a|b$ and $b|c$, then $a|c$
- If $a|b$ and $a|c$, then $a|(b + c)$
- If $a|b$, then $a|bc$ for any integer c

7.3 Division Algorithm

Theorem 7.1. For integers a and b with $b > 0$, there exist unique integers q and r such that:

$$a = bq + r \quad \text{where } 0 \leq r < b$$

7.4 Greatest Common Divisor

Definition 7.2. The **greatest common divisor** of integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b.

7.5 Euclidean Algorithm

To find $\gcd(a, b)$:

1. If $b = 0$, then $\gcd(a, b) = a$
2. Otherwise, $\gcd(a, b) = \gcd(b, a \bmod b)$

7.6 Prime Numbers

Definition 7.3. A **prime number** is an integer greater than 1 whose only positive divisors are 1 and itself.

7.7 Fundamental Theorem of Arithmetic

Theorem 7.2. Every integer greater than 1 can be expressed uniquely as a product of primes.

7.8 Congruence

Definition 7.4. Integers a and b are **congruent modulo** m (written $a \equiv b \pmod{m}$) if $m|(a - b)$.

7.9 Properties of Congruence

- $a \equiv a \pmod{m}$ (reflexive)
- $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ (symmetric)
- $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ (transitive)

8 Recurrence Relations

8.1 Definition

Definition 8.1. A **recurrence relation** is an equation that defines a sequence recursively.

8.2 Linear Homogeneous Recurrence Relations

A recurrence relation of the form:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

where $c_1, c_2, \ldots, c_k$ are constants.

8.3 Solving Linear Homogeneous Recurrence Relations

1. Find the characteristic equation: $r^k - c_1 r^{k-1} - c_2 r^{k-2} - \cdots - c_k = 0$
2. Find the roots $r_1, r_2, \ldots, r_k$
3. If all roots are distinct: $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$
4. If root r has multiplicity m: include terms $\alpha_1 r^n, \alpha_2 n r^n, \ldots, \alpha_m n^{m-1} r^n$

8.4 Common Recurrence Relations

- **Fibonacci**: $F_n = F_{n-1} + F_{n-2}$ with $F_0 = 0, F_1 = 1$
- **Geometric**: $a_n = r a_{n-1}$ with solution $a_n = a_0 r^n$
- **Arithmetic**: $a_n = a_{n-1} + d$ with solution $a_n = a_0 + nd$

9 Generating Functions

9.1 Definition

Definition 9.1. The **generating function** for sequence $\{a_n\}$ is:

$$G(x) = \sum_{n=0}^{\infty} a_n x^n$$

9.2 Common Generating Functions

- $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ for $|x| < 1$
- $\frac{1}{1-ax} = \sum_{n=0}^{\infty} a^n x^n$ for $|ax| < 1$
- $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$ (binomial theorem)
- $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$

10 Boolean Algebra

10.1 Definition

Definition 10.1. A **Boolean algebra** is a set B with operations $\wedge$ (AND), $\vee$ (OR), and $\neg$ (NOT) satisfying certain axioms.

10.2 Boolean Identities

- **Identity Laws**: $x \wedge 1 = x$, $x \vee 0 = x$
- **Domination Laws**: $x \wedge 0 = 0$, $x \vee 1 = 1$
- **Idempotent Laws**: $x \wedge x = x$, $x \vee x = x$
- **Double Complement**: $\neg(\neg x) = x$
- **Commutative Laws**: $x \wedge y = y \wedge x$, $x \vee y = y \vee x$
- **Associative Laws**: $(x \wedge y) \wedge z = x \wedge (y \wedge z)$
- **Distributive Laws**: $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
- **De Morgan's Laws**: $\neg(x \wedge y) = \neg x \vee \neg y$, $\neg(x \vee y) = \neg x \wedge \neg y$

11 Algorithms and Complexity

11.1 Algorithm Analysis

- **Time Complexity**: How running time grows with input size
- **Space Complexity**: How memory usage grows with input size

11.2 Big-O Notation

Definition 11.1. $f(n) = O(g(n))$ if there exist constants c and n_0 such that $f(n) \leq c \cdot g(n)$ for all $n \geq n_0$.

11.3 Common Complexity Classes

- **Constant**: $O(1)$
- **Logarithmic**: $O(\log n)$
- **Linear**: $O(n)$
- **Linearithmic**: $O(n \log n)$
- **Quadratic**: $O(n^2)$
- **Exponential**: $O(2^n)$
- **Factorial**: $O(n!)$

12 Probability

12.1 Basic Definitions

Definition 12.1. The **sample space** S is the set of all possible outcomes of an experiment.

Definition 12.2. An **event** is a subset of the sample space.

12.2 Probability Axioms

For any event E:

- $0 \leq P(E) \leq 1$
- $P(S) = 1$
- For mutually exclusive events: $P(E_1 \cup E_2 \cup \cdots) = P(E_1) + P(E_2) + \cdots$

12.3 Conditional Probability

Definition 12.3.

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \quad \text{where } P(B) > 0$$

12.4 Bayes' Theorem

Theorem 12.1.

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$$

12.5 Independent Events

Definition 12.4. Events A and B are **independent** if $P(A \cap B) = P(A) \cdot P(B)$.

13 Important Theorems and Results

13.1 Inclusion-Exclusion Principle

Theorem 13.1. For finite sets $A_1, A_2, \ldots, A_n$:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

13.2 Chinese Remainder Theorem

Theorem 13.2. If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime integers, then the system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} && (1) \\ x &\equiv a_2 \pmod{m_2} && (2) \\ &\vdots && (3) \\ x &\equiv a_k \pmod{m_k} && (4) \end{aligned}$$

has a unique solution modulo $m_1 m_2 \cdots m_k$.

13.3 Fermat's Little Theorem

Theorem 13.3. If p is prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

13.4 Wilson's Theorem

Theorem 13.4. A positive integer $n > 1$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.