Discrete Mathematics: In-Depth Topics and Advanced Formulas

February 15, 2025

Contents

1 Introduction and Basic Concepts

1.1 Numbers and Sets: Notation

A clear understanding of sets and number systems is fundamental to discrete mathematics. In this section we introduce standard notations and some useful identities.

Definition 1.1 (Common Number Sets)**.**

- $\mathbb{N}$: the set of *natural numbers*. (Note: some authors define $\mathbb{N} = \{0, 1, 2, \dots\}$, while others use $\{1, 2, \dots\}$.)
- $\mathbb{Z}$: the set of *integers* $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
- $\mathbb{Q}$: the set of *rational numbers*.
- $\mathbb{R}$: the set of *real numbers*.
- $\mathbb{C}$: the set of *complex numbers*.

Definition 1.2 (Basic Set Notation)**.** A *set* is a collection of distinct objects (called *elements*). Common notations include:

$$A = \{a, b, c, \dots\},$$

with $a \in A$ meaning a is an element of A. Other important notations are:

- $|A|$: the *cardinality* of A (number of elements).
- $A \subseteq B$: A is a *subset* of B.
- $A \cup B$: the *union* of A and B.
- $A \cap B$: the *intersection* of A and B.
- $A \setminus B$: the *set difference* (elements in A but not in B).
- A^c or $\overline{A}$: the *complement* of A (with respect to a universal set U).
- $\mathcal{P}(A)$: the *power set* of A, which has $|\mathcal{P}(A)| = 2^{|A|}$ when A is finite.

Lemma 1.3 (De Morgan's Laws)**.** *For any two sets A and B (with respect to a universal set U), we have:*

$$(A \cup B)^c = A^c \cap B^c \quad \textit{and} \quad (A \cap B)^c = A^c \cup B^c.$$

Proof. The proof follows directly from the definitions of union, intersection, and complement. □

1.2 Mathematical Induction and Other Proof Techniques

Induction is a key tool for proving statements about natural numbers. In addition to standard induction, strong (complete) induction is also widely used.

Theorem 1.4 (Principle of Mathematical Induction). *Let $P(n)$ be a proposition about $n \in \mathbb{N}$. If*

(i) ***Base Case:*** *$P(1)$ is true.*

(ii) ***Inductive Step:*** *For all $k \in \mathbb{N}$, $P(k)$ true implies $P(k+1)$ is true.*

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Theorem 1.5 (Principle of Strong Induction). *Let $P(n)$ be a proposition about $n \in \mathbb{N}$. If*

(i) ***Base Case:*** *$P(1)$ is true.*

(ii) ***Inductive Step:*** *For all $n \geq 1$, if $P(1), P(2), \ldots, P(n)$ are true, then $P(n+1)$ is true.*

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Example 1.6 (Prime Factorization). **Statement:** Every integer $n > 1$ can be written as a product of primes.

Proof (by strong induction):

- *Base Case:* $n = 2$ is prime.
- *Inductive Step:* Assume every integer $2 \leq k \leq n$ has a prime factorization. For $n+1$: if it is prime, the claim holds; if not, write $n+1 = ab$ with $2 \leq a, b \leq n$. By induction, both a and b have prime factorizations, so $n+1$ does as well.

Other common proof methods include *proof by contradiction* and *proof by contrapositive*.

1.3 Functions

Functions are mappings between sets that play a central role in mathematics.

Definition 1.7 (Function)**.** A *function* f from a set A to a set B, written $f : A \to B$, is a rule that assigns each $a \in A$ a unique element $f(a) \in B$. Here:

- A is the *domain*.
- B is the *codomain*.
- The *image* of f is $\{f(a) \mid a \in A\}$.

Definition 1.8 (Types of Functions)**.** A function $f : A \to B$ is:

- **Injective (one-to-one)** if $f(a_1) = f(a_2)$ implies $a_1 = a_2$.
- **Surjective (onto)** if for every $b \in B$ there is an $a \in A$ with $f(a) = b$.
- **Bijective** if it is both injective and surjective.

Lemma 1.9 (Composition of Functions)**.** *Let $f : A \to B$ and $g : B \to C$. Then the composition $g \circ f : A \to C$ defined by*

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

is a function. Moreover:

- *If f and g are injective, then $g \circ f$ is injective.*
- *If f and g are surjective, then $g \circ f$ is surjective.*
- *If f and g are bijective, then $g \circ f$ is bijective with inverse $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.*

1.4 Relations

Relations generalize the idea of functions and allow us to discuss various types of associations between elements.

Definition 1.10 (Relation)**.** A *relation* R on a set A is a subset of the Cartesian product $A \times A$:

$$R \subseteq A \times A.$$

If $(a, b) \in R$, we write $a \, R \, b$.

Definition 1.11 (Properties of Relations)**.** Let R be a relation on A. Then:

- R is *reflexive* if for every $a \in A$, $a\,R\,a$.
- R is *symmetric* if $a\,R\,b$ implies $b\,R\,a$ for all $a, b \in A$.
- R is *antisymmetric* if $a\,R\,b$ and $b\,R\,a$ imply $a = b$.
- R is *transitive* if $a\,R\,b$ and $b\,R\,c$ imply $a\,R\,c$ for all $a, b, c \in A$.

Example 1.12. The relation $\leq$ on $\mathbb{R}$ is reflexive, antisymmetric, and transitive.

Lemma 1.13 (Composition of Relations)**.** *If R and S are relations on a set A, their composition is defined as:*

$$R \circ S = \{(a, c) \in A \times A \mid \exists\, b \in A \text{ with } (a, b) \in S \text{ and } (b, c) \in R\}.$$

(Note: even if R and S are transitive, $R \circ S$ need not be transitive; one may consider the transitive closure *of a relation.)*

1.5 Equivalence Relations and Partitions

Definition 1.14 (Equivalence Relation)**.** A relation R on a set A is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Lemma 1.15 (Equivalence Relations and Partitions)**.** *Every equivalence relation on A partitions A into disjoint subsets (equivalence classes), where each element of A belongs to exactly one equivalence class. Conversely, any partition of A defines an equivalence relation by declaring two elements equivalent if they lie in the same subset.*

Example 1.16. Define a relation R on $\mathbb{Z}$ by $a\,R\,b$ if and only if $a \equiv b \pmod{n}$ (for some fixed $n \in \mathbb{N}$). Then R is an equivalence relation, and its equivalence classes are the congruence classes modulo n.

2 Ordering and Posets

Ordering relations allow us to compare elements in a set. This section discusses partial orders, total orders, lattices, and related results.

2.1 Partial Orders and Hasse Diagrams

Definition 2.1 (Partial Order)**.** A relation $\preceq$ on a set P is a *partial order* if it is:

- **Reflexive**: For all $a \in P$, $a \preceq a$.
- **Antisymmetric**: For all $a, b \in P$, if $a \preceq b$ and $b \preceq a$, then $a = b$.
- **Transitive**: For all $a, b, c \in P$, if $a \preceq b$ and $b \preceq c$, then $a \preceq c$.

Definition 2.2 (Hasse Diagram)**.** A *Hasse diagram* is a drawing of a finite poset that shows the ordering without including the edges for reflexivity and transitivity. If $a \prec b$ (i.e., $a \preceq b$ and $a \neq b$), then b is drawn above a.

Lemma 2.3. *Every finite, nonempty poset has at least one* minimal *element (an element with no smaller element) and at least one* maximal *element.*

2.2 Total Orders and Chains

Definition 2.4 (Total (or Linear) Order)**.** A partial order $\preceq$ on a set P is a *total order* if for any $a, b \in P$, either $a \preceq b$ or $b \preceq a$; that is, every pair of elements is *comparable*.

Example 2.5. The usual order $\leq$ on $\mathbb{R}$ is a total order. In contrast, the subset relation $\subseteq$ on the power set $\mathcal{P}(S)$ is only a partial order.

A *chain* in a poset is a subset in which every two elements are comparable, while an *antichain* is a subset in which no two distinct elements are comparable.

2.3 Lattices and Boolean Algebras

Definition 2.6 (Lattice)**.** A poset $(L, \preceq)$ is called a *lattice* if every pair $a, b \in L$ has a unique *least upper bound* (join, $a \vee b$) and a unique *greatest lower bound* (meet, $a \wedge b$).

Example 2.7. The power set $\mathcal{P}(S)$ of any set S, ordered by $\subseteq$, forms a lattice where

$$a \vee b = a \cup b \quad \text{and} \quad a \wedge b = a \cap b.$$

Lemma 2.8 (Distributive Law in Lattices). *A lattice L is* distributive *if for all $a, b, c \in L$:*

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

and

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

The lattice $\mathcal{P}(S)$ is distributive.

2.4 Dilworth's Theorem and Related Results

A major topic in the study of posets is the interplay between chains and antichains.

Theorem 2.9 (Dilworth's Theorem). *In any finite poset, the size of the largest antichain equals the minimum number of chains needed to cover the poset.*

Theorem 2.10 (Erdős–Szekeres Theorem). *Any sequence of $n^2 + 1$ distinct real numbers contains a monotonic (increasing or decreasing) subsequence of length $n + 1$.*

These results capture the idea that in a sufficiently large poset, one finds either a long chain ("tall") or a large antichain ("wide").

3 Combinatorial Counting

Counting techniques are at the heart of discrete mathematics. This section covers functions, permutations, binomial coefficients, and more.

3.1 Counting Functions and Subsets

- The number of functions from a finite set A (with $|A| = m$) to a finite set B (with $|B| = n$) is:
$$n^m.$$
- The number of injections from A to B (when $m \leq n$) is:
$$P(n, m) = \frac{n!}{(n - m)!}.$$

- The number of subsets of an n-element set is:

$$2^n.$$

- The number of k-element subsets is given by the binomial coefficient:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Lemma 3.1 (Binomial Sum Identity). *For any non-negative integer n,*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

3.2 Permutations and Factorials

Definition 3.2 (Factorial). For $n \in \mathbb{N}$, the *factorial* $n!$ is defined as:

$$n! = n \cdot (n-1) \cdots 2 \cdot 1, \quad \text{with } 0! = 1.$$

Definition 3.3 (Permutation). A *permutation* of a set of n elements is an ordered arrangement of its elements. The total number of permutations is $n!$. More generally, the number of ways to order k out of n elements is:

$$P(n,k) = \frac{n!}{(n-k)!}.$$

Lemma 3.4 (Permutations with Repetition). *If there are n objects with n_1 of one type, n_2 of another, $\ldots$, n_k of the kth type (with $n_1+n_2+\cdots+n_k = n$), then the number of distinct permutations is:*

$$\frac{n!}{n_1! n_2! \cdots n_k!}.$$

3.3 Binomial Coefficients and the Binomial Theorem

Definition 3.5 (Binomial Coefficient). For non-negative integers n and k with $0 \leq k \leq n$, the binomial coefficient is:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Lemma 3.6 (Pascal's Identity)**.** *For $0 < k < n$,*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Theorem 3.7 (Binomial Theorem)**.** *For any real numbers x and y and any non-negative integer n,*

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

Example 3.8. For $n = 3$:

$$(x+y)^3 = \binom{3}{0} x^0 y^3 + \binom{3}{1} x^1 y^2 + \binom{3}{2} x^2 y^1 + \binom{3}{3} x^3 y^0 = y^3 + 3xy^2 + 3x^2 y + x^3.$$

Definition 3.9 (Multinomial Coefficients)**.** For non-negative integers $n_1, n_2, \ldots, n_k$ satisfying $n_1 + n_2 + \cdots + n_k = n$, the multinomial coefficient is defined by:

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

Theorem 3.10 (Multinomial Theorem)**.** *For any real numbers $x_1, x_2, \ldots, x_k$ and non-negative integer n,*

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{n_1+n_2+\cdots+n_k=n} \binom{n}{n_1, n_2, \ldots, n_k} \prod_{i=1}^{k} x_i^{n_i}.$$

3.4 Inclusion-Exclusion Principle

The inclusion-exclusion principle is an important tool for counting the number of elements in the union of overlapping sets.

Theorem 3.11 (Inclusion-Exclusion Principle)**.** *Let $A_1, A_2, \ldots, A_n$ be finite sets. Then:*

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Example 3.12. For two sets A and B:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

3.5 Derangements and the Hat-Check Problem

A classical problem in combinatorics involves counting derangements.

Definition 3.13 (Derangement)**.** A *derangement* is a permutation σ of $\{1, 2, \ldots, n\}$ with no fixed points; that is, $\sigma(i) \neq i$ for all i.

Let D_n denote the number of derangements of n objects. Using inclusion-exclusion, one obtains:

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

An alternative recurrence for derangements is:

$$D_n = (n-1)(D_{n-1} + D_{n-2}), \quad \text{with } D_0 = 1 \text{ and } D_1 = 0.$$

Example 3.14. For $n = 3$:

$$D_3 = 3!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!}\right) = 6\left(1 - 1 + \frac{1}{2} - \frac{1}{6}\right) = 6\left(\frac{1}{2} - \frac{1}{6}\right) = 6\left(\frac{1}{3}\right) = 2.$$

Another useful expression for D_n is:

$$D_n = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor,$$

where e is the base of the natural logarithm.

3.6

Conclusion

In this document we have explored several core topics in discrete mathematics in greater depth:

- **Numbers and Sets:** We reviewed standard number systems, set operations, and key identities such as De Morgan's laws.
- **Proof Techniques:** Both standard and strong forms of mathematical induction were discussed alongside examples.

- **Functions and Relations:** Definitions, types, and properties (including function composition and inverses) were examined. We also discussed relations, including equivalence relations and the corresponding partitions of sets.
- **Ordering:** Partial and total orders were defined, and the concept of Hasse diagrams, chains, antichains, lattices, and related theorems (such as Dilworth's theorem) were introduced.
- **Combinatorial Counting:** Fundamental counting techniques including functions, permutations (with and without repetition), binomial and multinomial coefficients, the binomial theorem, inclusion-exclusion, and derangements were covered.

These topics form the backbone of combinatorics, graph theory, number theory, and computer science, and provide a solid foundation for advanced studies.