Study Guide

MATH 163: Discrete Mathematics 1 Fall 2022

Dr. Petrescu

Final: Monday, December 12, 2022

Denny Cao

December 11, 2022

Contents

1 Logic and Proofs

1.1 Propositional Logic

1.1.2 Propositions

Definition 1.1.2.1. Proposition: A statement that is either true or false.

p	$\neg p$
T	F
F	T

Figure 1: Truth table for **negation**

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$
T	T	T	T	F
T	F	F	T	T
F	T	F	T	T
F	F	F	F	F

Figure 2: Truth table for **bit operations**

1.1.3 Conditional Statements

Definition 1.1.3.1. Conditional Statement: A statement of the form $p \to q$. The conditional statement is called the *hypothesis* (or *antecedent* or *premise*) and q is called the *conclusion* (or *consequence*).

Definition 1.1.3.2. Converse: The proposition $q \to p$ is the converse of the proposition $p \to q$.

p	q	$q \to p$
T	T	T
T	F	T
F	T	F
F	F	T

Figure 3: Truth Table for converse of implication of two propositions p and q

Definition 1.1.3.3. Contrapositive: The proposition $\neg q \to \neg p$ is the contrapositive of the proposition $p \to q$.

- Same truth value as $p \to q$

p	q	$\neg p$	$\neg q$	$\neg q \to \neg p$
T	T	F	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

Figure 4: Truth Table for contrapositive of implication of two propositions p and q

Definition 1.1.3.4. Inverse: The proposition $\neg p \to \neg q$ is the inverse of the proposition $p \to q$.

p	q	$\neg p$	$\neg q$	$\neg p \to \neg q$
T	T	F	F	T
T	F	F	T	T
F	T	T	F	F
F	F	T	T	T

Figure 5: Truth Table for inverse of implication of two propositions p and q

1.1.5 Precedence of Logical Operators

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\to$	4
$\leftrightarrow$	5

Figure 6: Precedence of Logical Operators

1.3 Propositional Equivalences

1.3.1 Introduction

Definition 1.3.1.1. Tautology: A compound proposition that is always true.

Definition 1.3.1.2. Contradiction: A compound proposition that is always false.

Definition 1.3.1.3. Contingency: A compound proposition that is neither a tautology nor a contradiction.

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

Figure 7: Truth Table of an example of a Tautology and Contradiction

1.3.2 Logical Equivalences

Definition 1.3.2.1. Two propositions are **logically equivalent** if $p \leftrightarrow q$ is a tautology.

The following are important logical equivalences:

De Morgan's Laws
$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
$\neg(p \vee q) \leftrightarrow \neg p \wedge \neg q$

Conditional-Disjunction Equivalence
$p \to q \leftrightarrow \neg p \vee q$

Here are some other logical equivalences:

Logical Equivalences	
Equivalence	Name
$p \wedge \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Identity Laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \vee \mathbf{F} \equiv \mathbf{F}$	Domination Laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent Laws
$\neg(\neg p) \equiv p$	Double Negation Law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative Laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative Laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive Laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's Laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption Laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation Laws

Logical Equivalences Involving Conditional Statements
$p \to q \equiv \neg p \vee q$
$p \to q \equiv \neg q \to \neg p$
$p \vee q \equiv \neg p \to q$
$p \wedge q \equiv \neg(\neg p \vee \neg q) \equiv \neg(p \to \neg q)$
$\neg(p \to q) \equiv p \wedge \neg q$
$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$
$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$
$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$
$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

Logical Equivalences Involving Biconditonal Statements
$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$
$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$
$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

$$\bigvee_{i=1}^{n} p_i = p_1 \vee p_2 \vee \cdots \vee p_n$$

$$\bigwedge_{i=1}^{n} p_i = p_1 \wedge p_2 \wedge \cdots \wedge p_n$$

By De Morgan's laws, it follows that:

$$\neg \bigvee_{i=1}^{n} p_i = \bigwedge_{i=1}^{n} \neg p_i$$

1.3.5 Satisfiability

Definition 1.3.5.1. A compound proposition is **satisfiable** if there is an assignment of truth values to its variables that makes it true (When it is a tautology or a contigency).

Definition 1.3.5.2. A compound proposition is **unsatisfiable** if there is no assignment of truth values to its variables that makes it true (When it is a contradiction). To prove this, we can prove that the negation is a tautology.

1.4 Predicates and Quantifiers

1.4.2 Predicates

Definition 1.4.2.1. A **statement** contains 2 parts: a **subject** and a **predicate**.

- In the statement, x is greater than 3, x is the subject and greater than 3 is the predicate.
- The statement $P(x)$ is said to be the value of the **propositional function** P at x.

1.4.3 Quantifiers

Definition 1.4.3.1. Universal Quantifier: $\forall x P(x)$. $P(x)$ for all values of x in the domain.

- An element for which $P(x)$ is false is called a **counterexample**.

Definition 1.4.3.2. Existential Quantifier: $\exists x P(x)$. There exists an element x in the domain such that $P(x)$ is true.

Definition 1.4.3.3. Uniqueness Quantifier: $\exists! x P(x)$. There exists exactly one element x in the domain such that $P(x)$ is true.

A way to think about determining the truth value of quantifiers is to think about looping. To determine if $\forall x P(x)$ is true, we loop through all the elements in the domain and check if $P(x)$ is true for all of them. To determine if $\exists x P(x)$ is true, we loop through all the elements in the domain and check if $P(x)$ is true for at least one of them.

1.4.4 Quantifiers Over Finite Domains

When domain is finite, we can express statements using propositional logic:

$$\forall x P(x) \equiv \bigwedge_{i=1}^{n} P(x)$$

$$\exists x P(x) \equiv \bigvee_{i=1}^{n} P(x)$$

1.4.6 Precedence of Quantifiers

$\forall x$ and $\exists x$ have higher precedence than all logical operators from propositional calculus. For instance, $\forall P(x) \vee Q(x) \equiv (\forall P(x)) \vee Q(x)$.

1.4.8 Negating Quantified Expressions

$$\neg \forall x P(x) \equiv \exists x \neg P(x)$$
$$\neg \exists x P(x) \equiv \forall x \neg P(x)$$

Figure 8: De Morgan's Laws for Quantifiers

1.5 Nested Quantifiers

Statement	When True	When False
$\forall x \forall y P(x, y)$	$P(x, y)$ is true for all values of x and y	$\exists x \exists y \neg P(x, y)$
$\forall x \exists y P(x, y)$	For every x there is a y such that $P(x, y)$ is true	$\exists x \forall y \neg P(x, y)$
$\exists x \forall y P(x, y)$	There is an x such that $P(x, y)$ is true for all values of y	$\forall x \exists y \neg P(x, y)$
$\exists x \exists y P(x, y)$	There is an x and a y such that $P(x, y)$ is true	$\forall x \forall y \neg P(x, y)$

Figure 9: Quantifications of Two Variables

1.6 Rules of Inference

Rule of Inference	Tautology	Name
p $p \to q$ $\therefore \; q$	$(p \wedge (p \to q)) \to q$	Modus Ponens
$\neg q$ $p \to q$ $\therefore \; q$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus Tollens
$p \to q$ $q \to r$ $\therefore \; p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical Syllogism
$p \vee q$ $\neg p$ $\therefore \; q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive Syllogism
p $\therefore \; p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore \; p$	$(p \wedge q) \to p$	Simplification
p q $\therefore \; p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore \; q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution

Figure 10: Rules of Inference for Propositional Logic

Note: Resolution is saying, regardless of what p is, q or r is true.

Rule of Inference	Name
$\forall x P(x)$ $\therefore \; P(c)$	Universal Instantiation
$P(c)$ for an arbitrary c $\therefore \; \forall x P(x)$	Universal Generalization
$\exists x P(x)$ $\therefore \; P(c)$ for some element c	Existential Instantiation
$P(c)$ for some element c $\therefore \; \exists x P(x)$	Existential Generalization

Figure 11: Rules of Inference for Quantified Statements

Universal Modus Ponens: The usage of universal instantiation and modus ponens together.

$$\begin{array}{l} \forall x(P(x) \to Q(x)) \\ P(a), \text{ where } a \text{ is a particular element in the domain} \\ \therefore \; Q(a) \end{array}$$

1.7 Introduction to Proofs

Prove $\forall x(P(x) \to Q(x))$ by showing that $P(c) \to Q(c)$ is true, where c is an arbitrary element of the domain, and then apply universal generalization.

1.7.5 Direct Proofs

Show $p \to q$ by first assuming p is true and then showing that q is true using the rules of inference.

Definition 1.7.5.1. The integer n is **even** if $\exists k \in \mathbb{Z} \mid n = 2k$.

Definition 1.7.5.2. The integer n is **odd** if $\exists k \in \mathbb{Z} \mid n = 2k + 1$.

Definition 1.7.5.3. Two integers have the same **parity** if they are both even or both odd. They have **opposite parity** if one is even and the other is odd.

1.7.6 Proof by Contraposition

Definition 1.7.6.1. An **indirect proof** is a proof that does not start with the premise and ends with the conclusion. One type is **proof by contraposition**. This is a proof that shows $p \to q$ by showing $\neg q \to \neg p$.

1.7.7 Proof by Contradiction

Another type of indirect proof is **proof by contradiction**. We can prove p is true by showing that $\neg p \to (r \wedge \neg r)$. Assume the negation of p is true, and then show that r and $\neg r$ are both true. This is a contradiction, so p must be true.

Important example of proof by contradiction: Prove that $\sqrt{2}$ is irrational.

Proof. By contradiction. Let p be the proposition that $\sqrt{2}$ is irrational. Assum $\neg p$ is true, that is, assume $\sqrt{2}$ is rational. By definition of rational numbers, there exist integers a and b such that $\sqrt{2} = \frac{a}{b}$, where $\frac{a}{b}$ is in simplest terms. Then, we have:

$$\begin{aligned} \sqrt{2} &= \frac{a}{b} \\ 2 &= \frac{a^2}{b^2} \\ 2b^2 &= a^2 \end{aligned}$$

Since a^2 is a multiple of 2, a^2 is even. Therefore, a is even, and $a = 2k$ for some integer k.

$$\begin{aligned} 2b^2 &= 4k^2 \\ b^2 &= 2k^2 \end{aligned}$$

Since b^2 is a multiple of 2, b^2 is even. Therefore, b is even, and $b = 2l$ for some integer l.

$$\sqrt{2} = \frac{2k}{2l}$$

Since both a and b are even, we can divide both the numerator and denominator by 2. Because our assumption of $\neg p$ leads to the contradiction that 2 divides both a and b and 2 does not divide both a and b, $\neg p$ is false. Therefore, p is true. □

1.8 Proof Methods and Strategy

1.8.2 Exhaustive Proof and Proof by Cases

Exhaustive Proof: Prove that $p \to q$ by showing:

$$\bigvee_{i=1}^{n} p_i \to q$$

Proof by Cases: Prove that $p \to q$ by breaking p into cases and showing that q is true in each case.

2 Basic Structures

2.1 Sets

2.1.1 Introduction

Definition 2.1.1.1. A **set** is an unordered collection of distinct objects called **elements** or **members** of the set. A set is said to **contain** its elements. We write $a \in A$ to denote that a is an element of the set A. The notation $a \notin A$ denotes that a is not an element of the set A.

Sets of types of numbers:

- Natural Numbers: $\mathbb{N} = \{0, 1, 2, 3, \dots\} = \{\mathbb{Z}^+ \cup 0\}$
- Integers: $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, \dots\}$
- Positive Integers: $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$
- Rational Numbers: $\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$
- Real Numbers: $\mathbb{R}$
- Positive Real Numbers: $\mathbb{R}^+$
- Complex Numbers: $\mathbb{C}$

Definition 2.1.1.2. Equality of Sets:

$$A = B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B) \leftrightarrow A \subseteq B \wedge B \subseteq A$$

Definition 2.1.1.3. Empty Set: $\emptyset = \{\}$

2.1.3 Subsets

Definition 2.1.3.1. Subset:

$$A \subseteq B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B) \leftrightarrow B \supseteq A$$

To show that $A \nsubseteq B$, show $\exists x(x \in A \wedge x \notin B)$.

Theorem 2.1.3.1. For every set S, $\emptyset \subseteq S$ and $S \subseteq S$.

2.1.4 Size of a Set

Definition 2.1.4.1. Let S be a set. If there are exactly n distinct elements in S, where n is a nonnegative integer, we say that S is a **finite set** and that n is the **cardinality** of S, denoted by $|S|$.

- Note: Theorem 2.1.3.1!

2.1.5 Power Sets

Definition 2.1.5.1. Let S be a set. The **power set** of S, denoted by $\mathcal{P}(S)$, is the set of all subsets of S.

Theorem 2.1.5.1. Cardinality of a power set

$$|\mathcal{P}(S)| = 2^{|S|}$$

2.1.6 Cartesian Products

Definition 2.1.6.1. Let A and B be sets. The **Cartesian product** of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. Hence:

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$$

2.2 Set Operations

2.2.1 Introduction

Definition 2.2.1.1. Let A and B be sets. The **union** of the sets A and B, denoted $A \cup B$, is the set that contains those elements that are in either A or B or both. Hence:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Definition 2.2.1.2. Let A and B be sets. The **intersection** of the sets A and B, denoted $A \cap B$, is the set that contains those elements in both A and B. Hence:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Definition 2.2.1.3. Two sets are called **disjoint** if their intersection is the emptyset.

Definition 2.2.1.4. Let A and B be sets. The **difference** of the sets A and B, denoted $A - B$, is the set that contains those elements in A but not in B. It is also called the **complement of B with respect to A**. Hence:

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

Definition 2.2.1.5. Let U be the universal set. The **complement** of a set A, denoted $\overline{A}$, is the set $U - A$. Hence:

$$\overline{A} = \{x \mid x \in U \wedge x \notin A\}$$

Definition 2.2.1.6. Let A and B be sets. The **symmetric difference** of A and B is the set of elements that are in either A or B but not in both. It is denoted by $A \oplus B$. Hence:

$$A \oplus B = (A \cup B) - (A \cap B)$$

2.2.2 Set Identities

Identity	Name
$A \cap U = A$ $A \cup \emptyset = A$	Identity Laws
$A \cup U = U$ $A \cap \emptyset = \emptyset$	Domination Laws
$A \cup A = A$ $A \cap A = A$	Idempotent Laws
$\overline{(\overline{A})} = A$	Complementation Law
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutative Laws
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	Associative Laws
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributive Laws
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	De Morgan's Laws
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	Absorption Laws
$A \cup \overline{A} = U$ $A \cap \overline{A} = \emptyset$	Complement Laws

Figure 12: Set Identities

There are 3 ways to prove that two sets are equal:

1. Showing that they are subsets of each other. (Definition 2.2)
2. Membership tables.
3. Set identities.

A **membership table** considers each combination of the atomic sets (the original sets used to produce the sets on each side) that an element can belong to and verify that elements in the same combinations of sets belong to both the sets in the identity. Use a 1 to indicate that an element belongs to a set and a 0 to indicate that it does not. For example, consider the following identity:

$$A \cup (A \cap B) = A$$

We can construct a membership table for this identity as follows:

A	B	$A \cup (A \cap B)$
1	1	1
1	0	1
0	1	0
0	0	0

Since the columns are the same, we can conclude that the sets are equal.

2.2.3 Generalized Unions and Intersections

Definition 2.2.3.1. The **union** of a collection of sets is the set that contains those elements that are members of at least one set in the collection. It is denoted by:

$$A_1 \cup A_2 \cup \cdots A_n = \bigcup_{i=1}^{n} A_i$$

Definition 2.2.3.2. The **intersection** of a collection of sets is the set that contains those elements that are members of all sets in the collection. It is denoted by:

$$A_1 \cap A_2 \cap \cdots A_n = \bigcap_{i=1}^{n} A_i$$

2.3 Functions

2.3.1 Introduction

Definition 2.3.1.1. Let A and B be nonempty sets. A **function** f from A to B is an assignment of exactly one element of B to each element of A. We write $f(a) = b$ if b is the unique element of B assigned by the function f to the element a of A. If f is a function from A to B, we write $f : A \to B$.

- Functions are sometimes also called **mappings** or **transformations**

Definition 2.3.1.2. Let $f : A \to B$ be a function. A is the **domain** of f and B is the **codomain** of f. If $f(a) = b$, we say that b is the **image** of a and a is the **preimage** of b. The **range**, or **image** of f is the set of all images of elements of A. Also, if f is a function from A to B, we say that f **maps** A to B.

- Codomain is set of possible values of the function and range is the set of all elements of the codomain that are achieved as the value of f for at least one element of the domain.
- Two functions are **equal** when they have the same domain, same codomain, and map each each element of their common domain to the same element in their common codomain.

Definition 2.3.1.3. Let f_1 and f_2 be functions from A to B. Then $f_1 + f_2$ and $f_1 f_2$ are also functions from A to B defined $\forall x \in A$ by:

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$
$$(f_1 f_2)(x) = f_1(x) f_2(x)$$

Definition 2.3.1.4. Let f be a function from A to B and let $S \subseteq A$. The **image** of S under the function f is the subset of B that consists of the images of the elements of S. We denote the image of S by $f(S)$, so:

$$f(S) = \{t \mid \exists s \in S(t = f(s))\} = \{f(s) \mid s \in S\}$$

2.3.2 One-to-One and Onto Functions

Definition 2.3.2.1. A function f with domain A is **one-to-one** if and only if:

$$\forall a \forall b(a, b \in A \wedge (f(a) = f(b) \rightarrow a = b))$$

- A function f is one-to-one if and only if $f(a) \neq f(b)$ whenever $a \neq b$. This is obtained by taking the contrapositve of the implication in the definition.

Definition 2.3.2.2. A function f whose domain A and codomain B are subsets of the set of real numbers is called **increasing** if $f(x) \leq f(y)$ whenever $x < y$ and $x, y \in A$. Hence:

$$\forall x \forall y(x, y \in A \wedge x < y \rightarrow f(x) \leq f(y))$$

Definition 2.3.2.3. A function f whose domain A and codomain B are subsets of the set of real numbers is called **strictly increasing** if $f(x) < f(y)$ whenever $x < y$ and $x, y \in A$. Hence:

$$\forall x \forall y(x, y \in A \wedge x < y \rightarrow f(x) < f(y))$$

Definition 2.3.2.4. A function f whose domain A and codomain B are subsets of the set of real numbers is called **decreasing** if $f(x) \geq f(y)$ whenever $x < y$ and $x, y \in A$. Hence:

$$\forall x \forall y(x, y \in A \wedge x < y \rightarrow f(x) \geq f(y))$$

Definition 2.3.2.5. A function f whose domain A and codomain B are subsets of the set of real numbers is called **strictly decreasing** if $f(x) > f(y)$ whenever $x < y$ and $x, y \in A$. Hence:

$$\forall x \forall y(x, y \in A \wedge x < y \rightarrow f(x) > f(y))$$

Definition 2.3.2.6. A function f from A to B is **onto**, or a **surjection**, if and only if for every element $y \in B$ there exists an element $x \in A$ such that $f(x) = y$. Hence:

$$\forall y \exists x(f(x) = y)$$

where the domain for x is A and the domain of y is B.

- f is **surjective** if it is onto.

Definition 2.3.2.7. The function f is a **one-to-one correspondence** if it is both one-to-one and onto.

- Such a function is **bijective**

Suppose that $f : A \rightarrow B$.	
Show f is injective:	Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$, then $x = y$
Show f is not injective:	Find particular elements, $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.
Show f is surjective:	Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$.
Show f is not surjective:	Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.
Show f is bijective:	Show that f is both injective and surjective.

2.3.3 Inverse Functions and Composite Functions

Definition 2.3.3.1. Let f be a one-to-one correspondence from the set A to the set B. The **inverse function** of f is denoted by f^{-1}: Hence:

$$f^{-1}(b) = a \text{ when } f(a) = b$$

- A one-to-one correspondence f is **invertible** because we can define an inverse function f^{-1}.
- A function is **invertible** if it is not a one-to-one correspondence, because the inverse of f does not exist.

Definition 2.3.3.2. Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The **composition** of the functions f and g, denoted for all $a \in A$ by $f \circ g$, is the function from A to C defined by:

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

- $f \circ g$ assigns the element a of A the element assigned by f to $g(a)$.
- The domain of $f \circ g$ is the domain of g.
- The range of $f \circ g$ is the image of the range of g with respect to f.
- The composition $f \circ g$ cannot be defined unless the range of g is a subset of the domain of f.
- **Not Commutative!**

$$f \circ g \neq g \circ f$$

- When composing with inverse function, an identity function is obtained:

$$f \circ f^{-1}(a) = f^{-1} \circ f(a) = a$$

2.3.5 Some Important Functions

Definition 2.3.5.1. The **floor function** assigns to the real number x the largest integer that is less than or equal to x. The value of the floor function at x is denoted by $\lfloor x \rfloor$. The **ceiling function** assigns to the real number x the smllest integer that is greater than or equal to x. The value of the ceiling function at x is denoted by $\lceil x \rceil$.

n **is an integer,** x **is a real number**
$\lfloor x \rfloor = n \leftrightarrow n \leq x < n+1$
$\lceil x \rceil = n \leftrightarrow n-1 < x \leq n$
$\lfloor x \rfloor = n \leftrightarrow x-1 < n \leq x$
$\lceil x \rceil = n \leftrightarrow x \leq n < x+1$
$x-1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x+1$
$\lfloor -x \rfloor = -\lceil x \rceil$
$\lceil -x \rceil = -\lfloor x \rfloor$
$\lfloor x+n \rfloor = \lfloor x \rfloor + n$
$\lceil x+n \rceil = \lceil x \rceil + n$

Figure 13: Useful Properties of the Floor and Ceiling Functions

2.4 Sequences and Summations

2.4.2 Sequences

Definition 2.4.2.1. A **sequence** is a function from the set of integers to a set S. We use the notation a_n to denote the image of the integer n. a_n is called a **term** of the sequence.

Definition 2.4.2.2. A **geometric progression** is a sequence of the form:

$$a, ar, ar^2, \ldots, ar^n, \ldots$$

where the **initial term** a and the **common ratio** r are real numbers.

Definition 2.4.2.3. An **arithmetic progression** is a sequence of the form:

$$a, a+d, a+2d, \ldots, a+nd, \ldots$$

where the **initial term** a and the **common difference** d are real numbers.

2.4.3 Recursive Relations

Definition 2.4.3.1. A **recursive relation** for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely, $a_0, a_1, \ldots, a_{n-1}$, for all integers n with $n \geq n_0$, where n_0 is a nonnegative integer. A sequence is called a **solution** of a recurrence relation if its terms satisfy the recurrence relation.

Definition 2.4.3.2. The **Fibonacci sequence** is a sequence of integers defined by the recurrence relation:

$$f_0 = 0, \quad f_1 = 1, \quad f_{n+2} = f_{n+1} + f_n$$

2.4.5 Summations

Definition 2.4.5.1. The **sum** of a sequence $\{a_n\}$ is the real number:

$$\sum_{j=0}^{n} a_j = a_0 + a_1 + a_2 + \ldots$$

Theorem 2.4.5.1. If a and r are real numbers and $r \neq 0$, then:

$$\sum_{j=0}^{n} ar^j = \begin{cases} \dfrac{ar^{n+1} - a}{r-1}, & \text{if } r \neq 1 \\ a(n+1), & \text{if } r = 1 \end{cases}$$

Sum	Closed Form
$\sum_{k=0}^{n} ar^k, r \neq 0$	$\frac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x\rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x\rvert < 1$	$\frac{1}{(1-x)^2}$

Figure 14: Some Useful Summation Formulae

2.5 Cardinality of Sets

2.5.1 Introduction

Definition 2.5.1.1. The sets A and B have the **same cardinality** if and only if there is a one-to-one correspondence from A to B. When A and B have the same cardinality, we write $|A| = |B|$.

- For infinite sets, the definition of cardinality provides a relative measure of the size of two sets, rather than a measure of the size of one particular set.

Definition 2.5.1.2. If there is a one-to-one correspondence from A to B, the cardinality of A is less than or equal to the cardinality of B and we write $|A| \leq |B|$. Moreover, when $|A| \leq |B|$ and A and B have different cardinality, we say that the cardinality of A is less than the cardinality of B and we write $|A| < |B|$.

Remark. Definitions 2.5.1.1 and 2.5.1.2 do not give any separate meaning to $|A|$ and $|B|$ when A and B are arbitrary infinite sets.

2.5.2 Countable Sets

Definition 2.5.2.1. A set that is either finite or has the same cardinality as the set of positive integers is called **countable**. A set that is not countable is called **uncountable**. When an infinite set S is countable, we denote the cardinality of S by $\aleph_0$. We write $|S| = \aleph_0$ and say that S has cardinality "aleph null."

- To prove that a set is countable, we must show that there is a one-to-one correspondence between the set and the set of positive integers (Refer to Definition 2.3.2.7)

The following are examples of how to prove some common sets are countable:

Example 1. Prove that $\mathbb{Z}$ is countable.

Proof. We can list all integers in a sequence by starting with 0 and alternating between positive and negative integers: $0, 1, -1, 2, -2, 3, -3, \ldots$. Let f have the domain $\mathbb{Z}^+$.

$$f(n) = \begin{cases} \dfrac{n}{2}, & \text{if } n \text{ is even} \\ -\dfrac{n-1}{2}, & \text{if } n \text{ is odd} \end{cases}$$

Since when n is even, $f(n)$ maps to all positive integers, and when n is odd, $f(n)$ maps to all negative integers and 0, the codomain of f is $\mathbb{Z}$. Since there is a function f that maps $\mathbb{Z}^+$ to $\mathbb{Z}$, we can conclude that $\mathbb{Z}$ is countable. □

Example 2. Prove that $\mathbb{Q}^+$ is countable.

Proof. Every positive rational number is the quotient p/q of two positive integers. We can arrange the positive rational numbers by listing those with denominator $q = 1$ in the first row, those with denominator $q = 2$ in the second row, and so on:

	1	2	3	4	5	$\cdots$
1	$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{5}{1}$	$\cdots$
2	$\frac{1}{2}$	$\frac{2}{2}$	$\frac{3}{2}$	$\frac{4}{2}$	$\frac{5}{2}$	$\cdots$
3	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{3}$	$\frac{4}{3}$	$\frac{5}{3}$	$\cdots$
4	$\frac{1}{4}$	$\frac{2}{4}$	$\frac{3}{4}$	$\frac{4}{4}$	$\frac{5}{4}$	$\cdots$
5	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{3}{5}$	$\frac{4}{5}$	$\frac{5}{5}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Each rational number can be represented by the ordered pair (i, j) where i is the row number and j is the column number. We can see by snaking a line from $\mathbb{Q}^+_{11}$ to $\mathbb{Q}^+_{21}$ to $\mathbb{Q}^+_{12}$ to $\mathbb{Q}^+_{13}$ to $\mathbb{Q}^+_{31}$ and so forth, such that there is a zigzag-ing enumeration, we can list the element of $\mathbb{Q}^+$ in a sequence indexed by the positive integers, and thus $\mathbb{Q}^+$ is countable. □

Remark. Note that the same proof can be used to show that $\mathbb{Q}^-$ is countable, and thus the union of $\mathbb{Q}^+$ and $\mathbb{Q}^-$ is countable. By using the ordered pair $(0, 0)$, we can show that $\mathbb{Q}$ is countable.

2.5.3 Uncountable Sets

We can utilize the **Cantor diagonalization argument** to prove that the set of real numbers is uncountable.

Example 3. Prove that $\mathbb{R}$ is uncountable.

Proof. By contradiction. Suppose $\mathbb{R}$ is countable. Then, the subset of all real numbers that fall between 0 and 1 would also be countable (The subset of a countable set is countable). Under this

assumption, the real numbers between 0 and can be listed in some order, $r_1, r_2, r_3, \ldots$. Let the decimal representation of these real numbers be:

$$\begin{aligned} r_1 &= 0.d_{11}d_{12}d_{13}d_{14}\ldots \\ r_2 &= 0.d_{21}d_{22}d_{23}d_{24}\ldots \\ r_3 &= 0.d_{31}d_{32}d_{33}d_{34}\ldots \\ r_4 &= 0.d_{41}d_{42}d_{43}d_{44}\ldots \\ &\vdots \end{aligned}$$

where $d_{ij} \in \{x \mid 0 \leq x \leq 9\}$. Then, form a new real number with decimal expansion $r = 0.d_1d_2d_3d_4\ldots$, where the decimal digits are determined by the following rule:

$$d_i = \begin{cases} 4 & \text{if } d_{ii} \neq 4 \\ 5 & \text{if } d_{ii} = 4 \end{cases}$$

For instance, let $r_1 = 0.23794102\ldots, r_2 = 0.44590138\ldots, r_3 = 0.09118764\ldots, r = 4 = 0.80553900\ldots$, and so on. Then we have $r = 0.d_1d_2d_3d_4\cdots = 0.4544$, where $d_1 = 4$ because $d_{11} \neq 4$, $d_2 = 5$ because $d_{21} = 4$, $d_3 = 4$ because $d_{31} \neq 4$, and so on.

Every real number has a unique decimal expansion. Therefore, the real number r is not equal to any of $r_1, r_2, \ldots$ because the decimal expansion of r differs from the decimal expansion of r_i in the ith place to the right of the decimal point, for each i.

Because there is a real number r between 0 and 1 that is not in the list, the assumption that all the real numbers between 0 and 1 could be listed must be false. Therefore, all the real numbers between 0 and 1 cannot be listed, so the set of real numbers between 0 and 1 is uncountable. Any set with an uncountable subset is uncountable. Hence, the set of real numbers is uncountable. □

Remark. What we essentially did in the proof was create a number that is not in the list. We proved that we can infinitely create new numbers, r that are not in the list.

Theorem 2.5.3.1. If A and B are countable sets, then $A \cup B$ is also countable.

- Proof on page 184.

Theorem 2.5.3.2. Schröder-Bernstein Theorem If A and B are sets with $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$. In other words, if there are one-to-one functions f from A to B and g from B to A, then there is a one-to-one correspondence between A and B.