

# Study Guide

MATH 163: Discrete Mathematics 1 Fall 2022

Dr. Petrescu

Final: Monday, December 12, 2022

Denny Cao

December 10, 2022

## Contents

<b>1</b>	<b>Logic and Proofs</b>	<b>4</b>
1.1	Propositional Logic . . . . .	4
1.1.2	Propositions . . . . .	4
1.1.3	Conditional Statements . . . . .	4
1.1.5	Precedence of Logical Operators . . . . .	5
1.3	Propositional Equivalences . . . . .	5
1.3.1	Introduction . . . . .	5
1.3.2	Logical Equivalences . . . . .	5
1.3.5	Satisfiability . . . . .	7
1.4	Predicates and Quantifiers . . . . .	7
1.4.2	Predicates . . . . .	7
1.4.3	Quantifiers . . . . .	7
1.4.4	Quantifiers Over Finite Domains . . . . .	8
1.4.6	Precedence of Quantifiers . . . . .	8
1.4.8	Negating Quantified Expressions . . . . .	8
1.5	Nested Quantifiers . . . . .	8
1.6	Rules of Inference . . . . .	9
1.7	Introduction to Proofs . . . . .	10
1.7.5	Direct Proofs . . . . .	10
1.7.6	Proof by Contraposition . . . . .	10
1.7.7	Proof by Contradiction . . . . .	10
1.8	Proof Methods and Strategy . . . . .	11
1.8.2	Exhaustive Proof and Proof by Cases . . . . .	11
<b>2</b>	<b>Basic Structures</b>	<b>11</b>
2.1	Sets . . . . .	11
2.1.1	Introduction . . . . .	11
2.1.3	Subsets . . . . .	11
2.1.4	Size of a Set . . . . .	12
2.1.5	Power Sets . . . . .	12
2.1.6	Cartesian Products . . . . .	12
2.2	Set Operations . . . . .	12
2.2.1	Introduction . . . . .	12
2.2.2	Set Identities . . . . .	13
2.2.3	Generalized Unions and Intersections . . . . .	14
2.3	Functions . . . . .	14
2.3.1	Introduction . . . . .	14
2.3.2	One-to-One and Onto Functions . . . . .	15
2.3.3	Inverse Functions and Composite Functions . . . . .	16
2.4	Sequences and Summations . . . . .	17
2.5	Cardinality of Sets . . . . .	17
2.6	Matrices . . . . .	17

<b>4</b>	<b>Number Theory</b>	<b>17</b>
4.1	Divisibility and Modular Arithmetic . . . . .	17
4.2	Integer Representations and Algorithms . . . . .	17
4.3	Primes and Greatest Common Divisors . . . . .	17
4.4	Solving Congruences . . . . .	17
4.5	Applications of Congruences . . . . .	17
<b>5</b>	<b>Induction and Recursion</b>	<b>17</b>
5.1	Mathematical Induction . . . . .	17
5.2	Strong Induction and Well Ordering Principle . . . . .	17
<b>6</b>	<b>Counting</b>	<b>17</b>
6.1	Basics of Counting . . . . .	17
6.2	Pigeonhole Principle . . . . .	17
6.3	Permutations and Combinations . . . . .	17
6.4	Binomial Coefficients and Identities . . . . .	17
6.5	Generalized Permutations and Combinations . . . . .	17
6.6	Generating Permutations and Combinations . . . . .	17
<b>7</b>	<b>Probability</b>	<b>17</b>
7.1	Introduction to Discrete Probability . . . . .	17
7.2	Probability Theory . . . . .	17
7.3	Bayes' Theorem . . . . .	17
7.4	Expected Value and Variance . . . . .	17

# 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  $p \rightarrow q$ . 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  $q \rightarrow p$  is the converse of the proposition  $p \rightarrow q$ .

$p$	$q$	$q \rightarrow p$
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  $\neg q \rightarrow \neg p$  is the contrapositive of the proposition  $p \rightarrow q$ .

- Same truth value as  $p \rightarrow q$

$p$	$q$	$\neg p$	$\neg q$	$\neg q \rightarrow \neg p$
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  $\neg p \rightarrow \neg q$  is the inverse of the proposition  $p \rightarrow q$ .

$p$	$q$	$\neg p$	$\neg q$	$\neg p \rightarrow \neg q$
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
$\rightarrow$	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
$p \rightarrow q \leftrightarrow \neg p \vee q$

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
$p \rightarrow q \equiv \neg p \vee q$ $p \rightarrow q \equiv \neg q \rightarrow \neg p$ $p \vee q \equiv \neg p \rightarrow q$ $p \wedge q \equiv \neg(\neg p \vee \neg q) \equiv \neg(p \rightarrow \neg q)$ $\neg(p \rightarrow q) \equiv p \wedge \neg q$ $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$ $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$ $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$ $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Logical Equivalences Involving Biconditional 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 contingency).

**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
$\frac{p}{p \rightarrow q}$ $\therefore q$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus Ponens
$\frac{\neg q}{p \rightarrow q}$ $\therefore q$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus Tollens
$\frac{p \rightarrow q}{q \rightarrow r}$ $\therefore p \rightarrow r$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical Syllogism
$\frac{p \vee q}{\neg p}$ $\therefore q$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive Syllogism
$\frac{p}{p \vee q}$ $\therefore p \vee q$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{p}$ $\therefore p$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p}{q}$ $\therefore p \wedge q$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{p \vee q}{\neg p \vee r}$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$	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
$\frac{\forall x P(x)}{\therefore P(c)}$	Universal Instantiation
$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$	Universal Generalization
$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$	Existential Instantiation
$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$	Existential Generalization

Figure 11: Rules of Inference for Quantified Statements

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

$$\frac{\forall x (P(x) \rightarrow Q(x))}{P(a), \text{ where } a \text{ is a particular element in the domain}}$$

$$\therefore Q(a)$$

## 1.7 Introduction to Proofs

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

### 1.7.5 Direct Proofs

Show  $p \rightarrow q$  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  $p \rightarrow q$  by showing  $\neg q \rightarrow \neg p$ .

### 1.7.7 Proof by Contradiction

Another type of indirect proof is **proof by contradiction**. We can prove  $p$  is true by showing that  $\neg p \rightarrow (r \wedge \neg r)$ . 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. Assume  $\neg p$  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.  $\square$

## 1.8 Proof Methods and Strategy

### 1.8.2 Exhaustive Proof and Proof by Cases

**Exhaustive Proof:** Prove that  $p \rightarrow q$  by showing:

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

**Proof by Cases:** Prove that  $p \rightarrow q$  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:  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- 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  $A \not\subseteq B$ , 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  $\bar{A}$ , is the set  $U - A$ . Hence:

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

**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  $f : A \rightarrow B$ .

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

**Definition 2.3.1.2.** Let  $f : A \rightarrow B$  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 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:

$$\begin{aligned}(f_1 + f_2)(x) &= f_1(x) + f_2(x) \\ (f_1 f_2)(x) &= f_1(x) f_2(x)\end{aligned}$$

**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 contrapositive 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:

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



## 2.4 Sequences and Summations

## 2.5 Cardinality of Sets

## 2.6 Matrices

# 4 Number Theory

## 4.1 Divisibility and Modular Arithmetic

## 4.2 Integer Representations and Algorithms

## 4.3 Primes and Greatest Common Divisors

## 4.4 Solving Congruences

## 4.5 Applications of Congruences

# 5 Induction and Recursion

## 5.1 Mathematical Induction

## 5.2 Strong Induction and Well Ordering Principle

# 6 Counting

## 6.1 Basics of Counting

## 6.2 Pigeonhole Principle

## 6.3 Permutations and Combinations

## 6.4 Binomial Coefficients and Identities

## 6.5 Generalized Permutations and Combinations

## 6.6 Generating Permutations and Combinations

# 7 Probability

## 7.1 Introduction to Discrete Probability

## 7.2 Probability Theory

## 7.3 Bayes' Theorem

## 7.4 Expected Value and Variance