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

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 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 $\underline{\quad p \to q \quad}$ $\therefore \quad q$	$(p \land (p \to q)) \to q$	Modus Ponens
$\neg q$ $\underline{\quad p \to q \quad}$ $\therefore \quad q$	$(\neg q \land (p \to q)) \to \neg p$	Modus Tollens
$p \to q$ $\underline{\quad q \to r \quad}$ $\therefore \quad p \to r$	$((p \to q) \land (q \to r)) \to (p \to r)$	Hypothetical Syllogism
$p \lor q$ $\underline{\quad \neg p \quad}$ $\therefore \quad q$	$((p \lor q) \land \neg p) \to q$	Disjunctive Syllogism
p $\underline{\quad\quad}$ $\therefore \quad p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$ $\underline{\quad\quad}$ $\therefore \quad p$	$(p \land q) \to p$	Simplification
p q $\underline{\quad\quad}$ $\therefore \quad p \land q$	$((p) \land (q)) \to (p \land q)$	Conjunction
$p \lor q$ $\underline{\quad \neg p \lor r \quad}$ $\therefore \quad q \lor r$	$((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$	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
$\underline{\quad \forall x P(x) \quad}$ $\therefore \quad P(c)$	Universal Instantiation
$\underline{P(c) \text{ for an arbitrary } c}$ $\therefore \quad \forall x P(x)$	Universal Generalization
$\underline{\quad \exists x P(x) \quad}$ $\therefore \quad P(c) \text{ for some element } c$	Existential Instantiation
$\underline{P(c) \text{ for some element } c}$ $\therefore \quad \exists x P(x)$	Existential Generalization

Figure 11: Rules of Inference for Quantified Statements

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

$$\forall x(P(x) \to Q(x))$$
$$\underline{P(a), \text{ where } a \text{ is a particular element in the domain}}$$
$$\therefore \quad Q(a)$$

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:

$$\sqrt{2} = \frac{a}{b}$$
$$2 = \frac{a^2}{b^2}$$
$$2b^2 = a^2$$

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

$$2b^2 = 4k^2$$
$$b^2 = 2k^2$$

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: $\mathbb{Q} = \left\{ \dfrac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right\}$

- 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
$\displaystyle\sum_{k=0}^{n} ar^k, r \neq 0$	$\dfrac{ar^{n+1} - a}{r - 1}, r \neq 1$
$\displaystyle\sum_{k=1}^{n} k$	$\dfrac{n(n + 1)}{2}$
$\displaystyle\sum_{k=1}^{n} k^2$	$\dfrac{n(n + 1)(2n + 1)}{6}$
$\displaystyle\sum_{k=1}^{n} k^3$	$\dfrac{n^2(n + 1)^2}{4}$
$\displaystyle\sum_{k=0}^{\infty} x^k, |x| < 1$	$\dfrac{1}{1 - x}$
$\displaystyle\sum_{k=1}^{\infty} kx^{k-1}, |x| < 1$	$\dfrac{1}{(1 - x)^2}$

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 2.5.2.1. 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. $\qquad\square$

Example 2.5.2.2. 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. $\qquad\square$

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 2.5.3.1. 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:

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

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. $\square$

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.

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

6.1.2 Basic Counting Principles

Theorem 6.1.2.1. Multiplication Rule: Multiply the number of ways that A can occur by the number of ways that B can occur (where A and B are two events).

- $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_n|$

Theorem 6.1.2.2. Sum Rule: Add the number of ways that A can occur to the number of ways that B can occur (where A and B are two events).

- $|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$ when $A_i \cap A_j =$ for all i, j.

6.1.5 Subtraction Rule (Inclusion-Exclusion For Two Sets)

Theorem 6.1.5.1. Subtraction Rule: If A can be done in either n_1 or n_2 ways, then the number of ways to do the task is $n_1 + n_2$ minus the number of ways to do the task that are common to the two different ways.

- $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$

6.1.6 Division Rule

Theorem 6.1.6.1. Division Rule: There are n/d ways to do a task if it can be done using a procedure that can be carried out in n ways, and for every way w, exactly d of the n ways correspond to way w.

- Useful when it appears that a task can be done in n different ways, but it turns out that for each way of doing the task, there are d equivalent ways of doing it. There are n/d inequivalent ways to do the task.

6.2   Pigeonhole Principle

6.2.1   Introduction

Theorem 6.2.1.1. Pigeonhole Principle: If k is a positive integer and $k + 1$ or more objects are placed into k boxes, then there is at least one box containing two or more of the objects.

Corollary 6.2.1.1. A function f from a set with $k + 1$ or more elements to a set with k elements is not one-to-one.

6.2.2   Generalized Pigeonhole Principle

Theorem 6.2.2.1. Generalized Pigeonhole Principle: If N objects are placed into k boxes, then there is at least one box containing at least $\left\lceil \dfrac{N}{k} \right\rceil$ objects.

Here are some proofs using the pigeonhole principle:

Example 6.2.2.1. Show that for every integer n there is a multiple of n that has only 0s and 1s in its decimal expansion.

Proof. Let n be a positive integer. Consider the $n + 1$ integers $1, 11, 111, \ldots, 11 \ldots 1$ (where the last integer in this list is the integer with $n + 1$ 1s in its decimal expansion). Note that there are n possible remainders when an integer is divided by n. Because there are $n + 1$ integers in this list, by the pigeonhole principle, there must be two with the same remainder when divided by n. The larger of these integers less the smaller one is a multiple of n, which has decimal expansion with only 0s and 1s. $\qquad\square$

Example 6.2.2.2. How many cards must be selected from a standard deck of 62 cards to guarentee that:

a) at least three cards are of the same suit?

b) at least three hearts are selected?

Proof. **a)** Suppose there are 4 boxes, one for each suit, and as cards are selected they are placed in their respective box. Using the generalized pigeonhole principle, we see that if N cards are selected, there is at least 1 box contaning at least $\lceil N/4 \rceil$ cards. Thus, we know that at least 3 cards of 1 suit are selected if $\lceil N/4 \rceil \geq 3$. The smallest integer N to satisfy this inequality is $2 \times 4 + 1 = 9$, so we must select at least 9 cards to guarentee that at least 3 cards are of the same suit. $\qquad\square$

- Note that if 8 cards are selected, it is possible to have 2 cards of each suit, so more than eight cards are needed.

Proof. **b)** We do not use the generalized pigeonhole principle because we want to make sure that there are 3 hearts, not just 3 cards of a suit. Note that in the worst case, we can select all the clubs, diamonds, and spades, 39 cards in all, before we select a single heart. The next 3 cards will all be hearts, so we may need to select 42 cards to get 3 hearts. $\qquad\square$

6.2.3   Some Elegant Applications of the Pigeonhole Principle

Example 6.2.3.1. During a month with 30 days, a baseball team plays at least one game a day, but no more than 45 games. Show that there must be a period fo some number of consecutive days during which the team must play exactly 14 games.

Proof. Let a_j be the number of games played on or before the jth day of the month. Then $a_1, a_2, \ldots, a_{30}$ is an increasing sequence of distinct positive integers, with $1 \leq a_j \leq 45$. Moreover, $a_1 + 14, a_2 + 14, \ldots, a_j + 14$ is also an increasing sequence of distinct positive integers, with $15 \leq a_j + 14 \leq 59$.

The 60 positive integers $a_1, a_2, \ldots, a_{30}, a_1 + 14, a_2 + 14, \ldots, a_j + 14$ are all less than or equal to 59. Hence, by the pigeonhole principle two of these integers must be equal. Because the integers $a_j, j = 1, 2, \ldots, 30$, are all distinct and the integers $a_j + 14, j = 1, 2, \ldots, 30$ are all distinct, there must be indices i and j with $a_i = a_j + 14$. This means that exactly 14 games were played from day $j + 1$ to day i. $\qquad\square$

Example 6.2.3.2. Show that among any $n + 1$ positive integers not exceeding $2n$ there must be an integer that divides one of the other integers.

Proof. Write out each of the $n+1$ integers $a_1, a_2, \ldots, a_{n+1}$ as a power of 2 times an odd integer. In other words, let $a_j = 2^{k_j} q_j$, for $j = 1, 2, \ldots n + 1$, where k_j is a nonnegative integer and q_j is odd. The integers $q_1, q_2, \ldots, q_{n+1}$ are all odd positive integers less than $2n$. Because there are only n odd positive integers less than $2n$, it follows from the pigeonhole principle that two of the integers $q_1, q_2, \ldots, q_{n+1}$ must be equal. Therefore, there are distinct integers i and j such that $q_i = q_j$. Let q be the common value of q_i and q_j. Then $a_i = 2^{k_i} q$ and $a_j = 2^{k_j} q$. It follows that if $k_i < k_j$, then a_i divides a_j; while if $k_i > k_j$, then a_j divides a_i. In either case, there is an integer that divides one of the other integers. $\qquad\square$

Theorem 6.2.3.1. Every sequence of $n^2 + 1$ distinct real numbers contains a subsequence of $n + 1$ that is either strictly increasing or strictly decreasing.

6.3   Permutations and Combinations

6.3.2   Permutations

Definition 6.3.2.1. A **permutation** of a set S is an ordering of the elements of S.

Theorem 6.3.2.1. If n is a positive integer and r is an integer with $1 \leq r \leq n$, then there are:

$$P(n, r) = n(n - 1)(n - 2) \cdots (n - r + 1)$$

r-permutations of a set of n **distinct** elements.

Corollary 6.3.2.1. If n and r are integers with $0 \leq r \leq n$, then:

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

6.3.3   Combinations

Definition 6.3.3.1. An r-combination of a set S is a subset of S with r elements.

Theorem 6.3.3.1. The number of r-combinations of a set with n elements, where n is a nonnegative integer and r is an integer with $0 \le r \le n$, is:

$$C(n, r) = \frac{n!}{r!(n-r)!}$$

Corollary 6.3.3.1. Let n and r be nonnegative integers with $r \le n$. Then:

$$C(n, r) = C(n, n-r)$$

Definition 6.3.3.2. Combinatorial Proof: If this is on the final, doomed. Refer to Homework 3 (Practice Exam 3) Question 13 Part B for an example. Page 438 uses this method to prove the Binomial Theorem.

6.4   Binomial Coefficients and Identities

6.4.1   Binomial Theorem

Theorem 6.4.1.1. Let x and y be variables, and let n be a nonnegative integer. Then:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j} = \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \cdots + \binom{n}{n} x^0 y^n$$

Corollary 6.4.1.1. Let n be a nonnegative integer. Then:

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

Corollary 6.4.1.2. Let n be a positive integer. Then:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

Corollary 6.4.1.3. Let n be a nonnegative integer. Then:

$$\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$$

6.4.2   Pascal's Identity

Theorem 6.4.2.1. Pascal's Identity: Let n and k be positive integers with $n \ge k$. Then:

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

6.4.3   Other Identities Involving Binomial Coefficients

Theorem 6.4.3.1. Vandermonde's Identity: Let m, n, r be nonnegative integers, $r < m, n$. Then:
$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{n}{k}\binom{m}{r-k}$$

Corollary 6.4.3.1. If n is a nonnegative integer, then:
$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$$

Theorem 6.4.3.2. Let n and r be nonnegative integers with $r \leq n$. Then:
$$\binom{n+1}{r+1} = \sum_{j=r}^{n} \binom{j}{r}$$

6.5   Generalized Permutations and Combinations

6.5.2   Permutations with Repetition

Theorem 6.5.2.1. The number of r-permutations of a set of n objects **with repetition** is:
$$P_r(n) = n^r$$

6.5.3   Combinations with Repetition

- STARS AND BARS

Theorem 6.5.3.1. There are $C(n+r-1, r) = C(n+r-1, n-1)$ r-combinations from a set of n elements **with repetition**.

- n stars and r bars. Total positions is $n+r-1$. Number of ways to place r bars is $C(n+r-1, r)$.

- Recall that we can have restrictions for each bar. **At least: Subtract from $n+r-1$ the number of stars. At most, subtract the complement.**

6.5.4   Permutations with Indistinguishable Objects

Theorem 6.5.4.1. The number of different permutations of n objects where there are n_1 indistinguishable objects of type 1, n_2 indistinguishable objects of type 2, ..., n_k indistinguishable objects of type k is:
$$\frac{n!}{n_1! n_2! \cdots n_k!}$$

- Proof on Page 450.

6.5.5　Distributing Objects into Boxes

Theorem 6.5.5.1. The number of ways to distribute n **distinguishable objects** into k **distinguishable boxes** so that n_i objects are placed into box $i, i = 1, 2, \ldots, k$ is:

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

Situation	Formula
n Distinguishable Objects and r Boxes	$\dfrac{n!}{n_1! n_2! \cdots n_k!}$
n Indistinguishable Objects and r Distinguishable Boxes	$\dbinom{n + r - 1}{r}$
n Distinguishable Objects and r Indistinguishable Boxes	Give up. Start writing everything out.

Figure 15: Distributing Objects into Boxes

7　Probability

7.1　Introduction to Discrete Probability

7.2　Probability Theory

7.3　Bayes' Theorem

Theorem 7.3.0.1. Bayes' Theorem: Suppose that E and F are events from a sample space S such that $p(E) \neq 0$ and $p(F) \neq 0$. Then:

$$p(F \mid E) = \frac{p(E \mid F)p(F)}{p(E \mid F)p(F) + p(E \mid \overline{F})p(\overline{F})}$$

7.4　Expected Value and Variance

7.4.2　Expected Values

Definition 7.4.2.1. The **expected value** of the random variable X on the sample space S is:

$$E(X) = \sum_{s \in S} p(s)X(s)$$

The **deviation** of X at $s \in S$ is:

$$d(s) = X(s) - E(X)$$

Theorem 7.4.2.1. If X is a random variable and $p(X = r)$ is the probability that $X = r$, so that $p(X = r) = \displaystyle\sum_{s \in S, X(s)=r} p(s)$, then:

$$E(X) = \sum_{r \in X(s)} p(X = r)r$$

Example 7.4.2.1. Expected Value of a Die:

- Let X be the random variable that represents the number of spots on a die. Then X is a random variable on the sample space $S = \{1, 2, 3, 4, 5, 6\}$.

- Let $p(s) = \dfrac{1}{6}$ for each $s \in S$.

- Then $E(X) = \sum_{s \in S} p(s)X(s) = \sum_{s \in S} \dfrac{1}{6}X(s) = \dfrac{1}{6}\sum_{s \in S} X(s) = \dfrac{1}{6} \cdot 21 = \dfrac{7}{2}$

- The expected value of X is 3.5.

Theorem 7.4.2.2. The expected number of successes when n mutually independent Bernoulli trials are formed, where p is the probability of success on each trial, is:

$$E(X) = np$$

7.4.3   Linearity of Expectations

Theorem 7.4.3.1. If $X_i = 1, 2, \ldots, n$ with n a positive integer, are random variables on S, and if a and b are real numbers:

(i). $E(X_1 + X_2 + \cdots + X_n) = E(X_1) + E(X_2) + \cdots + E(X_n)$

(ii). E(aX + b) = aE(X) + b

7.4.5   Geometric Distribution

Definition 7.4.5.1. TA random variable X has a **geometric distribution with parameter** p if $p(X = k) = (1 - p)^{k-1}p$ for $k = 1, 2, \ldots$, where p is a real number with $0 \leq p \leq 1$.

Theorem 7.4.5.1. If the random variable X has the geometric distribution with parameter p, then:

$$E(X) = \dfrac{1}{p}$$

7.4.6   Independent Random Variables

Theorem 7.4.6.1. The random variables X and Y on the sample space S are **independent** if:

$$p(X = r_1 \text{ and } Y = r_2) = p(X = r_1)p(Y = r_2)$$

or in words, if the probability that $X = r_1$ and $Y = r_2$ equals the product of the probabilities that $X = r_1$ and $Y = r_2$ for all numbers r_1 and r_2.

Theorem 7.4.6.2. If X and Y are independent random variables on the sample space S, then:

$$E(XY) = E(X)E(Y)$$

7.4.7 Variance

Definition 7.4.7.1. Let X be a random variable on a sample space S. The **variance** of X is, denoted by $V(X)$ is:

$$V(X) = \sum_{x \in S} (X(s) - E(X))^2 p(s) = E(X^2) - E(X)^2$$

$V(X)$ is the weighted average of the square of the deviation of X. The **standard deviation** of X, denoted $\sigma(X)$, is:

$$\sigma(X) = \sqrt{V(X)}$$

Example 7.4.7.1. Variance of the Value of a Die
We have $V(X) = E(X^2) - E(X)^2$. From Example 7.4.2.1, we have $E(X) = 7/2$. To find $E(X^2)$ note that X^2 takes the values $i^2, i = 1, 2, \ldots, 6$, each with probability $\frac{1}{6}$. Thus:

$$E(X^2) = \frac{1}{6} \sum_{i=1}^{6} i^2 = \frac{1}{6} \cdot 91 = \frac{91}{6}$$

Thus:

$$V(X) = \frac{91}{6} - \left(\frac{7}{2}\right)^2 = \frac{35}{12}$$

Corollary 7.4.7.1. If X is a random variable on a sample space S and $E(X) = \mu$, then:

$$V(X) = E(X - \mu)^2$$

Theorem 7.4.7.1. Variance of a Bernoulli Trial
Because X takes only the values 0 and 1, it follows that $X^2(t) = X(t)$. Hence:

$$V(X) = E(X^2) - E(X)^2 = p - p^2 = p(1 - p) = pq$$

Where p is the probability of success on a single trial, q is the probability of failure.

Theorem 7.4.7.2. If X and Y are independent random variables on the sample space S, the $V(X + Y) = V(X) + V(Y)$. Furthermore, if $X_i, i = 1, 2, \ldots, n$, with n a positive integer, are pairwise independent random variables on S, then:

$$V(X_1 + X_2 + \cdots + X_n) = V(X_1) + V(X_2) + \cdots + V(X_n)$$

Part I
Exam 4 Study Guide

Study Guide

MATH 163: Discrete Mathematics 1 Fall 2022

Dr. Petrescu

Final:

Valen Li

December 25, 2025

Contents

8   Probability & Combinatorics

8.1   Basic Counting & Complements

Concept: Often, calculating the probability of "at least one" or "at least n" is difficult directly. It is almost always easier to calculate the probability of the *opposite* (complement) event and subtract from 1.

The Strategy:

1. Identify keywords: "At least one", "At least two", "Not all".

2. Define the Total Sample Space size ($|S|$).

3. Define the Complement Event (E^c).

   - Example: "At least one heads" $\rightarrow$ Complement: "Zero heads" (All tails).
   - Example: "At least two consecutive same" $\rightarrow$ Complement: "Alternating perfectly".

4. Calculate $P(E) = 1 - P(E^c) = 1 - \frac{|E^c|}{|S|}$.

8.2   Inclusion-Exclusion Principle

Concept: Used when counting sets with overlapping conditions (e.g., passwords requiring Upper, Lower, AND Digits).

The Strategy:

1. Start with the **Total** possible permutations (ignoring restrictions).

2. Subtract the "Bad" sets (missing one condition).

3. Add back the intersections of "Bad" sets (missing two conditions) because you subtracted them twice.

4. Subtract the intersection of all three (missing all conditions), and so on.

5. **Formula:** $|A \cup B \cup C| = \sum |A| - \sum |A \cap B| + |A \cap B \cap C|$.

8.3   Independence

Concept: Two events A and B are independent if knowing A happened gives you no information about B.

The Test: To prove or disprove independence, calculate these two values separately:

1. $P(A \cap B)$

2. $P(A) \times P(B)$

Conclusion:

- If $P(A \cap B) = P(A)P(B)$, they **are** independent.

- If $P(A \cap B) \neq P(A)P(B)$, they are **dependent**.

9   Conditional Probability & Bayes' Theorem

9.1   Common Pitfall: $P(A|B)$ vs $P(B|A)$

These are **not** the same. Confusing them is often called the "Prosecutor's Fallacy".

- $P(A|B)$: The probability that A is true, given evidence B. (e.g., "Probability you have the virus, given a positive test.")

- $P(B|A)$: The probability of evidence B, given A is true. (e.g., "Probability of testing positive, given you have the virus.")

Example: If $A =$ "It is raining" and $B =$ "It is cloudy":

- $P(B|A) \approx 100\%$ (Rain almost always implies clouds).

- $P(A|B) \approx 10\%$ (Clouds often exist without rain).

9.2   The Formula (Bayes)

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

9.3   Understanding the Denominator (Total Probability)

The denominator $P(B)$ represents the total probability of the evidence occurring, regardless of whether the hypothesis A is true or false. It is the sum of two distinct scenarios:

1. **True Positives:** You have the condition (A) AND test positive.

$$P(B \cap A) = P(B|A)P(A)$$

2. **False Positives:** You do NOT have the condition (A^c) AND test positive.

$$P(B \cap A^c) = P(B|A^c)P(A^c)$$

Thus, the full formula is:

$$P(A|B) = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}}$$

9.4   Step-by-Step Strategy

1. **Identify the Hypothesis (H):** E.g., "Person uses drugs" or "Coin is biased".

2. **Identify the Evidence (E):** E.g., "Test is positive" or "Sequence of flips".

3. **Calculate the Numerator (True Positive):** $P(E|H) \times P(H)$.

4. **Calculate the False Positive Term:** $P(E|H^c) \times P(H^c)$.

5. **Sum for Denominator:** Numerator + False Positive Term.

6. **Divide:** Numerator / Denominator.

Tip: For coin flip sequences, $P(E|H)$ is the product of individual flip probabilities given that specific coin.

10 Number Theory

10.1 Base Expansion & Conversion

Problem Type: Convert $(Hex)_{16}$ to Binary, Octal, or Decimal.
The Strategy:

1. **Hex → Binary:** This is the "Gateway". Convert every single Hex digit into exactly **4 binary bits**.

   - $A \rightarrow 10 \rightarrow 1010$
   - $7 \rightarrow 0111$

2. **Binary → Octal:** Group the binary string into chunks of **3 bits** starting from the **right**. Convert each chunk.

3. **Binary → Base 4:** Group binary string into chunks of **2 bits** from the right.

4. **Any Base → Decimal:** Multiply digit by position power. $(d_2 d_1 d_0)_b = d_2 \cdot b^2 + d_1 \cdot b^1 + d_0 \cdot b^0$.

10.2 Divisors (Count and Sum)

Problem Type: Find how many divisors N has, or their sum.
The Strategy:

1. **Prime Factorization:** Break N down completely. $N = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$.

2. **Count:** Take every exponent, add 1, and multiply them.

$$\text{Count} = (e_1 + 1)(e_2 + 1) \ldots (e_k + 1)$$

3. **Sum:** Use the geometric series formula for each prime part:

$$\text{Sum} = \prod_{i=1}^{k} \left(\frac{p_i^{e_i + 1} - 1}{p_i - 1} \right)$$

10.3 Divisibility Rules (General Bases)

Concept: Rules like "ends in 0 or 5" (Base 10) rely on modular arithmetic. **To find rule for k in Base b:** Look at $b \pmod{k}$.

- If $b \equiv 1 \pmod{k}$: The rule is "Sum of digits is divisible by k".

- If $b \equiv -1 \pmod{k}$: The rule is "Alternating sum of digits is divisible by k".

- If $b \equiv 0 \pmod{k}$: The rule is "Last digit is divisible by k".

10.4   Key GCD Theorems for Proofs

When proving statements involving GCDs, keep these three properties in mind:

1. **Bézout's Identity:** If $d = \gcd(a, b)$, there exist integers s and t such that $sa + tb = d$. Use this when you need to express the GCD algebraically.

2. **Euclid's Lemma:** If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$. This is crucial for proofs involving prime factorization uniqueness or coprime integers.

3. **Euclidean Algorithm Step:** $\gcd(a, b) = \gcd(b, a \pmod{b})$. This generalizes to $\gcd(a, m) = \gcd(a - km, m)$, allowing you to add/subtract multiples of one number from the other without changing the GCD.

11   Modular Arithmetic

11.1   Solving Systems of Congruences

You will likely be asked to solve a system using two specific methods.

11.1.1   Method 1: Chinese Remainder Theorem (Construction)

Use when: You need a formulaic approach for $x \equiv a_i \pmod{m_i}$.

1. Calculate $M = m_1 \times m_2 \times \cdots \times m_k$.

2. For each equation i, calculate $M_i = M/m_i$.

3. Find the modular inverse y_i such that $M_i \cdot y_i \equiv 1 \pmod{m_i}$.

4. **Solution:** $x = \sum(a_i \cdot M_i \cdot y_i) \pmod{M}$.

11.1.2   Method 2: Back Substitution

Use when: You prefer algebra over finding multiple inverses.

1. Take the first equation: $x \equiv a \pmod{m} \implies x = mk + a$.

2. Substitute this expression for x into the **second** equation.

3. Solve for $k \pmod{m_2}$.

4. Substitute k back into the expression for x.

5. Repeat for all equations.

11.2   Fermat's Little Theorem

Problem Type: Find $a^K \pmod{p}$ where p is prime and K is huge.
Theorem: $a^{p-1} \equiv 1 \pmod{p}$ (if $p \nmid a$).
The Strategy:

1. Divide the exponent K by $(p - 1)$.

2. Write $K = q(p-1) + r$.

3. The huge power cancels out: $a^K \equiv a^r \pmod{p}$.

4. Calculate the much smaller $a^r \pmod{p}$.

11.3   Proofs & Disproofs

- **Disproving "For all x..." statements:** You only need **one** counterexample. Try small numbers (primes, 0, 1) or boundary cases.

- **Proving GCD properties:** See Section 3.4 for essential theorems.

12 Self-Check Practice Problems

Problem 1 (Probability): A fair coin is flipped 8 times. What is the probability that at least 2 flips are heads? (Hint: Use the complement).

Problem 2 (Bayes' Theorem): A certain disease affects 1% of the population. A test for the disease is 99% accurate for sick people (True Positive) but has a 2% false positive rate for healthy people. If a person tests positive, what is the probability they actually have the disease?

Problem 3 (Number Theory): Convert the hexadecimal number $(2C5)_{16}$ into Octal (base 8). Show your work using binary as the intermediate step.

Problem 4 (Modular Arithmetic): Solve the system of congruences using back substitution:

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 5$$

13   Answer Key & Explanations

Solution to Problem 1

We use the **Complement Rule**.

- **Total Outcomes:** Since a coin has 2 sides and we flip 8 times, Total $= 2^8 = 256$.

- **Complement Event:** "Less than 2 heads" means exactly 0 heads OR exactly 1 head.

  - Ways to get 0 heads (TTTTTTTT): $\binom{8}{0} = 1$.
  - Ways to get 1 head: $\binom{8}{1} = 8$.
  - Total "Bad" outcomes $= 1 + 8 = 9$.

- **Calculation:** $P(\text{At least } 2) = 1 - \frac{9}{256} = \frac{247}{256}$.

Note: Do not use combinations for the total sample space (like $\binom{8}{2}$) when dealing with sequential coin flips; the sample space grows exponentially (2^n).

Solution to Problem 2

We use Bayes' Theorem. Let $D =$ Disease, $+ =$ Positive Test.

- $P(D) = 0.01 \implies P(D^c) = 0.99$.

- $P(+|D) = 0.99$ (True Positive Rate).

- $P(+|D^c) = 0.02$ (False Positive Rate).

- $P(D|+) = \frac{0.99(0.01)}{0.99(0.01) + 0.02(0.99)}$

- $P(D|+) = \frac{0.0099}{0.0099 + 0.0198} = \frac{0.0099}{0.0297} = \frac{1}{3}$.

Answer: $\approx 33.3\%$.

Solution to Problem 3

- **Step 1: Hex to Binary.**

$$2 \to 0010, \quad C(12) \to 1100, \quad 5 \to 0101$$

  Binary string: 001011000101_2

- **Step 2: Binary to Octal.** Group by 3s from the right.

$$(001) \quad (011) \quad (000) \quad (101)$$

$$1 \quad\quad 3 \quad\quad 0 \quad\quad 5$$

- Answer: 1305_8.

Solution to Problem 4

Using Back Substitution:

1. From $x \equiv 2 \pmod 3$, we write $x = 3k + 2$.

2. Substitute into the second equation:

$$3k + 2 \equiv 3 \pmod 5$$

$$3k \equiv 1 \pmod 5$$

3. Multiply by 2 (the inverse of 3 mod 5, since $2 \times 3 = 6 \equiv 1$):

$$6k \equiv 2 \pmod 5 \implies k \equiv 2 \pmod 5$$

4. Write $k = 5j + 2$.

5. Substitute back into x:

$$x = 3(5j + 2) + 2 = 15j + 6 + 2 = 15j + 8$$

Answer: $x \equiv 8 \pmod{15}$.
Q
Practice Exam 4 Solutions – Discrete Mathematics I

Name: Valen Li **Date**: December 25, 2025

Problem 1. A fair coin is flipped n times. Give an expression for each of the probabilities below as a function of n. Simplify your final expression as much as possible.
(a) At least $n - 1$ flips come up heads.
(b) There are **at least two** consecutive flips that are the same.
(c) Assuming n is even, the number of heads is different from the number of tails.

Solution: (a) **At least $n - 1$ heads:** This implies getting exactly $n - 1$ heads or exactly n heads.

- Ways to get n heads: $\binom{n}{n} = 1$

- Ways to get $n - 1$ heads: $\binom{n}{n-1} = n$

- Total outcomes: 2^n

- **Answer:** $\dfrac{n + 1}{2^n}$

(b) **At least two consecutive same:** We use the complement (no two consecutive flips are the same).

- The only sequences with no consecutive same flips are alternating: $HTHT\ldots$ and $THTH\ldots$ (2 sequences).

- Probability of complement: $\dfrac{2}{2^n} = \dfrac{1}{2^{n-1}}$

- **Answer:** $1 - \dfrac{1}{2^{n-1}}$

(c) **Number of heads $\neq$ number of tails (n is even):** Use the complement (Heads = Tails).

- This occurs only if there are exactly $n/2$ heads.

- Ways to choose $n/2$ heads: $\binom{n}{n/2}$

- **Answer:** $1 - \dfrac{\binom{n}{n/2}}{2^n}$

Problem 2. 10 kids are randomly grouped into an A team with five kids and a B team with five kids. Each grouping is equally likely. There are 3 kids in the group, Alex and his two best friends Jose and Carl. What is the probability that Alex ends up on the same team with at least one of his two best friends?

Solution: We calculate the probability of the complement: Alex is on a team with *neither* of his friends.

- Total ways to pick Alex's 4 teammates from the remaining 9 kids: $\binom{9}{4} = 126$.

- Ways to pick teammates excluding Jose and Carl (picking 4 from remaining 7): $\binom{7}{4} = 35$.

- $P(\text{No Friends}) = \dfrac{35}{126} = \dfrac{5}{18}$.

- $P(\text{At least one}) = 1 - \dfrac{5}{18}$.

- **Answer:** $\dfrac{13}{18}$

Problem 3. An online vendor requires that customers select a password that is a sequence of upper-case letters, lower-case letters and digits. A valid password must be at least 10 characters long, and it must contain at least one character from each of the three sets of characters. What is the probability that a randomly selected string with exactly ten characters results in a valid password? The alphabet for the strings in the sample space from which the string is drawn is the union of the three sets of characters.

Solution: Use Inclusion-Exclusion. Let S be the total set of strings (62^{10}). Let U be strings missing Uppercase, L missing Lowercase, D missing Digits.

- $|U| = (26 + 10)^{10} = 36^{10}$

- $|L| = (26 + 10)^{10} = 36^{10}$

- $|D| = (26 + 26)^{10} = 52^{10}$

- $|U \cap L| = 10^{10}$ (Digits only)

- $|U \cap D| = 26^{10}$ (Lower only)

- $|L \cap D| = 26^{10}$ (Upper only)

Answer: $\dfrac{62^{10} - (2 \cdot 36^{10} + 52^{10}) + (10^{10} + 2 \cdot 26^{10})}{62^{10}}$ _____

Problem 4. A 5-card hand is dealt from a perfectly shuffled deck. Define the events A: the hand is a four of a kind (all four cards of one rank plus a 5th card), B: at least one of the cards in the hand is an ace.

Are the events A and B independent? Prove your answer by showing that one of the conditions for independence is either true or false.

Solution: Events: A (Four of a Kind), B (At least one Ace).

- $|A| = 13 \times 48 = 624$. (13 ranks for the quad $\times$ 48 kickers).

- $A \cap B$: Hand is Four of a Kind AND has an Ace.

    - Case 1: Quad Aces ($AAAA + X$). 48 possibilities.
    - Case 2: Quad Non-Aces ($KKKK + A$). 12 ranks $\times$ 4 suits of Aces $= 48$ possibilities.
    - $|A \cap B| = 96$.

- $P(B|A) = \dfrac{96}{624} = \dfrac{2}{13} \approx 0.15$.

- $P(B) = 1 - \dfrac{\binom{48}{5}}{\binom{52}{5}} \approx 0.34$.

- Since $P(B|A) \neq P(B)$, they are **not independent**.

_____

Problem 5. A wedding party of eight people is lined up in a random order. Every way of lining up the people in the wedding party is equally likely.
(a) What is the probability that the bride is next to the groom?
(b) What is the probability that the maid of honor is in the leftmost position?
(c) Determine whether the two events are independent. Prove your answer by showing that one of the conditions for independence is either true or false.

Solution: Total permutations: 8!.

- (a) Treat Bride and Groom as one block $\{BG\}$. We arrange 7 items. BG can be BG or GB.
  $P = \dfrac{2 \times 7!}{8!} = \dfrac{1}{4}$.

- (b) Maid of Honor fixed in position 1. Arrange remaining 7.
  $P = \dfrac{7!}{8!} = \dfrac{1}{8}$.

- (c) Check $P(A \cap B)$. Maid in pos 1, Bride/Groom adjacent in remaining 7 spots.
  Ways $= 2 \times 6!$ (treating BG as block in the line of 7).
  $P(A \cap B) = \dfrac{2 \times 6!}{8!} = \dfrac{2}{56} = \dfrac{1}{28}$.
  Check Independence: $P(A) \times P(B) = \dfrac{1}{4} \times \dfrac{1}{8} = \dfrac{1}{32}$.
  $\dfrac{1}{28} \neq \dfrac{1}{32}$. **Not Independent.**

Problem 6. A biased coin is flipped 10 times. In a single flip of the coin, the probability of heads is 1/3 and the probability of tails is 2/3. The outcomes of the coin flips are mutually independent. What is the probability of each event?
(a) Every flip comes up heads
(b) The first 5 flips come up heads. The last 5 flips come up tails.
(c) The first flip comes up heads. The rest of the flips come up tails.

Solution: $P(H) = 1/3, P(T) = 2/3$.

- (a) All Heads: $(1/3)^{10} = \dfrac{1}{59049}$.

- (b) 5 Heads, then 5 Tails: $(1/3)^5(2/3)^5 = \dfrac{32}{3^{10}} = \dfrac{32}{59049}$.

- (c) 1 Head, then 9 Tails: $(1/3)^1(2/3)^9 = \dfrac{512}{59049}$.

Problem 7. The national flufferball association decides to implement a drug screening procedure to test its athletes for illegal performance enhancing drugs. 3% of the professional flufferball players actually use performance enhancing drugs. A test for the drugs has a false positive rate of 2% and a false negative rate of 4%. In other words, a person who does not take the drugs will test positive with probability 0.02. A person who does take the drugs will test negative with probability 0.04. A randomly selected player is tested and tests positive. What is the probability that she really does take performance enhancing drugs?

Solution: Bayes' Theorem. Let D be Drug User, $+$ be Positive Test.

- $P(D) = 0.03$. $P(D^c) = 0.97$.

- $P(+|D) = 1 - 0.04 = 0.96$ (Sensitivity).

- $P(+|D^c) = 0.02$ (False Positive).

- $P(D|+) = \dfrac{P(+|D)P(D)}{P(+|D)P(D) + P(+|D^c)P(D^c)}$

- $P(D|+) = \dfrac{0.96(0.03)}{0.96(0.03) + 0.02(0.97)} = \dfrac{0.0288}{0.0288 + 0.0194} = \dfrac{0.0288}{0.0482}$

- **Answer:** ≈ 0.5975 or 59.75%

Problem 8. Sally has two coins. The first coin is a fair coin and the second coin is biased. The biased coin comes up heads with probability .75 and tails with probability .25. She selects a coin at random and flips the coin ten times. The results of the coin flips are mutually independent. The result of the 10 flips is: T,T,H,T,H,T,T,T,H,T. What is the probability that she selected the biased coin?

Solution: Let C_F be Fair Coin (50/50), C_B be Biased (75/25). Data: 3 Heads, 7 Tails.

- $P(Data|C_F) = \binom{10}{3}(0.5)^{10} \approx 0.117$ (Actually since specific sequence given: $0.5^{10} \approx 0.000976$).

- $P(Data|C_B) = 0.75^3 \times 0.25^7 \approx 0.0000257$.

- Priors are equal (0.5).

- $P(C_B|Data) = \dfrac{0.0000257}{0.0000257 + 0.000976} \approx \mathbf{0.0256}$

The sequence is extremely unlikely for a coin biased towards heads. ————————————

Problem 9. Assume 1 person out of 10,000 is infected with HIV, and there is a test in which 2.5% of all people test positive for the virus although they do not have it. If you test negative on this test, then you definitely do not have HIV. What is the chance of having HIV, assuming you test positive for it?

Solution: $P(HIV) = 0.0001$. $P(+|Healthy) = 0.025$. $P(-|HIV) = 0$ (so $P(+|HIV) = 1$).

- $P(HIV|+) = \dfrac{1(0.0001)}{1(0.0001) + 0.025(0.9999)}$

- $P(HIV|+) = \dfrac{0.0001}{0.0001 + 0.0249975} \approx \mathbf{0.00398}$ or 0.4%

————————————————————————————

Problem 10. Consider an experiment in which a red die and a blue die are thrown. Let X be the random variable whose value is the product of the numbers on the red and blue dice.
(a) What is the range of X, i.e. its possible values ?
(b) What is the probability that $X = 6$?

Solution: $X = \text{Red} \times \text{Blue}$.

- (a) **Range:** $\{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 30, 36\}$

- (b) Pairs multiplying to 6: $(1, 6), (2, 3), (3, 2), (6, 1)$. Total 4 outcomes.

- $P(X = 6) = \dfrac{4}{36} = \dfrac{1}{9}$.

————————————————————————————

Problem 11. Certain rules allow us to determine by inspection when a positive integer n is divisible by a positive integer k. For example, in base 10, $5|n$ if and only if n ends in the digit 5 or 0. Similarly, $2|n$ if and only if n ends in one of the digits $0, 2, 4, 6, 8$. There are also rules to determine divisibility by many different integers. Use your knowledge of divisibility rules in base 10, to write divisibility rules for $n = 2, 3, 4, 5, 6, 7, 8$ in base 9

Solution: Divisibility rules in Base 9. Let $N = (d_k \ldots d_1 d_0)_9$.

- $n = 2$: Since $9 \equiv 1 \pmod 2$, sum of digits must be even.

- $n = 3$: Since $9 \equiv 0 \pmod 3$, last digit d_0 must be divisible by 3 $(0, 3, 6)$.

- $n = 4$: Since $9 \equiv 1 \pmod 4$, sum of digits divisible by 4.

- $n = 5$: Since $9 \equiv -1 \pmod 5$, alternating sum of digits divisible by 5.

- $n = 6$: Must satisfy rules for 2 and 3. Last digit $0, 3, 6$ AND sum of digits even.

- $n = 7$: Since $9 \equiv 2 \pmod 7$, $d_0 + 2d_1 + 4d_2 + \dots$ divisible by 7.

- $n = 8$: Since $9 \equiv 1 \pmod 8$, sum of digits divisible by 8.

Problem 12) (a) Find the number of positive integer divisors of 648.
(b) Find the sum of all positive integer divisors of 648.

Solution: $648 = 2^3 \times 3^4$.

- (a) Count: $(3+1)(4+1) = 20$.

- (b) Sum: $\dfrac{2^4 - 1}{2 - 1} \times \dfrac{3^5 - 1}{3 - 1} = 15 \times 121 = \mathbf{1815}$.

Problem 13) Find the decimal, binary, octal and base 4 expansion of $(D5A3)_{16}$.

Solution: Hex: $D5A3_{16}$.

- **Binary:** $1101\ 0101\ 1010\ 0011_2$

- **Base 4:** $11|01|01|01|10|10|00|11 \rightarrow 31112203_4$

- **Octal:** $1|101|010|110|100|011 \rightarrow 152643_8$

- **Decimal:** $13(16^3) + 5(16^2) + 10(16) + 3 = 53248 + 1280 + 160 + 3 = \mathbf{54691}$

Problem 14) Find values a, b, and c (not all 0) such that $(abc)_5 = (cba)_8$, or prove that there are none.

Solution: $(abc)_5 = (cba)_8 \implies 25a + 5b + c = 64c + 8b + a$.

- Simplify: $24a - 3b - 63c = 0 \implies 8a - b - 21c = 0 \implies b = 8a - 21c$.

- Constraints: $1 \le a \le 4$, $0 \le b \le 4$, $1 \le c \le 4$.

- If $c = 1$, $b = 8a - 21$.

- Try $a = 3 \implies b = 24 - 21 = 3$. Valid ($331_5 = 131_{10}$? No. $25(3) + 15 + 1 = 91$. $64(1) + 24 + 3 = 91$).

- **Answer:** $a = 3, b = 3, c = 1$.

Problem 15) Suppose the odd primes 3, 5, 7,11,13,17,... in order of increasing size are $p_1, p_2, p_3, \dots$. Prove or disprove:
$p_1 p_2 p_3 \dots p_k + 2$ is prime, for all $k \ge 1$.

Solution: Disprove: $p_1 \dots p_k + 2$ is prime.

- $k = 1 : 3 + 2 = 5$ (Prime)

- $k = 2 : 3(5) + 2 = 17$ (Prime)

- $k = 3 : 3(5)(7) + 2 = 107$ (Prime)

- $k = 4 : 3(5)(7)(11) + 2 = 1157.$

- Test 1157: $1157 = 13 \times 89$. Not Prime.

- **Answer:** False. Counterexample at $k = 4$.

Problem 16) Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences:
$x \equiv 1 \pmod{2}$,
$x \equiv 2 \pmod{3}$,
$x \equiv 3 \pmod{5}$,
$x \equiv 4 \pmod{11}$

Solution: System: $x \equiv 1(2), x \equiv 2(3), x \equiv 3(5), x \equiv 4(11)$.

- $M = 330$.

- $x = 1(165)(1) + 2(110)(2) + 3(66)(1) + 4(30)(7) = 165 + 440 + 198 + 840 = 1643$.

- $1643 \pmod{330} = 323$.

- **Answer:** $x \equiv 323 \pmod{330}$.

Problem 17) Solve the system of congruences in the previous question using the method of back substitution.

Solution: Back Substitution.

- $x = 2j + 1$. Sub into mod 3: $2j + 1 \equiv 2 \implies 2j \equiv 1 \implies j \equiv 2 \pmod 3$. $j = 3k + 2$.

- $x = 2(3k + 2) + 1 = 6k + 5$. Sub into mod 5: $6k + 5 \equiv 3 \implies k \equiv 3 \pmod 5$. $k = 5m + 3$.

- $x = 6(5m + 3) + 5 = 30m + 23$. Sub into mod 11: $30m + 23 \equiv 4 \implies 8m + 1 \equiv 4 \implies 8m \equiv 3$.

- Multiply by 7 (inverse of 8): $m \equiv 21 \equiv 10 \pmod{11}$. $m = 11n + 10$.

- $x = 30(11n + 10) + 23 = 330n + 300 + 23 = 330n + 323$.

Problem 18) Use Fermat's little theorem to find $23^{1002} \bmod 41$.

Solution: $23^{1002} \pmod{41}$.

- Fermat's Little Theorem: $23^{40} \equiv 1 \pmod{41}$.

- $1002 = 25(40) + 2$.

- $23^{1002} \equiv (23^{40})^{25} \cdot 23^2 \equiv 1 \cdot 529 \pmod{41}$.

- $529 = 12(41) + 37$.

- **Answer:** 37.

Problem 19) Show that if **a** ,**b** , and **m** are integers such that $m \geq 2$ and $a \equiv b \ (mod \ m)$, then $gcd(a, m) = gcd(b, m)$.

Solution: Proof: Let $d = \gcd(a, m)$. Then $d|a$ and $d|m$. Since $a \equiv b \pmod{m}$, $a = b + km$ for some integer k, so $b = a - km$. Since d divides a and m, it divides $a - km$, so $d|b$. Thus d is a common divisor of b and m. Similarly, any common divisor of b and m must divide a. Therefore, $\gcd(a, m) = \gcd(b, m)$.

Problem 20) Find a counterexample to of this statement about congruences:
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where **a, b, c, d** and **m** are integers with **c** and **d** positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$.

Solution: Statement: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a^c \equiv b^d \pmod{m}$. **Counterexample:**

- Let $m = 3$.

- $a = 2, b = 5 \implies 2 \equiv 5 \pmod{3}$.

- $c = 1, d = 4 \implies 1 \equiv 4 \pmod{3}$.

- LHS: $2^1 = 2$.

- RHS: $5^4 = 625 \equiv 1 \pmod{3}$.

- $2 \not\equiv 1 \pmod{3}$.

Part II
Homework Solutions

14   Homework 1

Homework 1

To show that $p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$ using truth table, where $\oplus$ is the XOR conjunction, we write the truth table below:

p	q	$\neg p$	$p \wedge \neg q$	$\neg p \wedge q$	$(p \wedge \neg q) \vee (\neg p \wedge q)$	$\neg q$	$p \oplus q$
True	True	False	False	False	False	False	False
True	False	False	True	True	False	True	True
False	True	True	False	False	True	True	True
False	False	True	True	False	False	False	False

Problem 21. Given the truth table above, write the truth table for $p \vee q \wedge s$ and its negation

p	q	s	$p \vee (q \wedge s)$	$\neg(p \vee (q \wedge s))$
T	T	T	T	F
T	T	F	T	F
T	F	T	T	F
T	F	F	T	F
F	T	T	T	F
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

15   Homework 2

Logical Operators: NAND and NOR

In this document, we address a series of questions to demonstrate the properties and equivalences of logical operators, including the newly introduced NAND ($|$), defined as true when at least one of p or q is false, and NOR ($\downarrow$), defined as true only when both p and q are false. We use truth tables to verify equivalences and construct compound propositions.

Q1: Conjunction, Disjunction, and Conditional using $\neg$ and $\vee$

To express conjunction ($p \wedge q$), disjunction ($p \vee q$), and conditional ($p \rightarrow q$) using only $\neg$ and $\vee$, we use the following equivalences:

- Disjunction: $p \vee q$ (already given).

- Conjunction: $p \wedge q \equiv \neg(\neg p \vee \neg q)$

- Conditional: $p \rightarrow q \equiv \neg p \vee q$.

The truth table verifies these equivalences:

p	q	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(\neg p \vee \neg q)$
T	T	F	F	F	T
T	F	F	T	T	F
F	T	T	F	T	F
F	F	T	T	T	F

The column for $\neg(\neg p \vee \neg q)$ matches $p \wedge q$. For the conditional:

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

The column for $\neg p \vee q$ matches $p \rightarrow q$. Thus, $\neg$ and $\vee$ can express all three.

Q2: Conjunction, Disjunction, and Conditional using $\neg$ and $\wedge$

To express conjunction ($p \wedge q$), disjunction ($p \vee q$), and conditional ($p \rightarrow q$) using only $\neg$ and $\wedge$, we use:

- Conjunction: $p \wedge q$ (already given).

- Disjunction: $p \vee q \equiv \neg(\neg p \wedge \neg q)$

- Conditional: $p \rightarrow q \equiv \neg(p \wedge \neg q)$.

The truth table verifies these:

p	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$\neg(\neg p \wedge \neg q)$	$\neg(p \wedge \neg q)$
T	T	F	F	F	T	T
T	F	F	T	F	T	F
F	T	T	F	F	T	T
F	F	T	T	T	F	T

The column for $\neg(\neg p \wedge \neg q)$ matches $p \vee q$, and $\neg(p \wedge \neg q)$ matches $p \rightarrow q$. Thus, $\neg$ and $\wedge$ can express all three.

Q3: Truth Table for NAND ($p|q$)

The NAND operator ($p|q$) is true when at least one of p or q is false, and false when both are true:

p	q	$p|q$
T	T	F
T	F	T
F	T	T
F	F	T

Q4: Showing $p|q \equiv \neg(p \wedge q)$

We compare $p|q$ with $\neg(p \wedge q)$ using a truth table:

p	q	$p \wedge q$	$\neg(p \wedge q)$	$p|q$
T	T	T	F	F
T	F	F	T	T
F	T	F	T	T
F	F	F	T	T

The columns for $\neg(p \wedge q)$ and $p|q$ are identical, confirming $p|q \equiv \neg(p \wedge q)$.

Q5: Truth Table for NOR ($p \downarrow q$)

The NOR operator ($p \downarrow q$) is true only when both p and q are false:

p	q	$p \downarrow q$
T	T	F
T	F	F
F	T	F
F	F	T

Q6: Showing $p \downarrow q \equiv \neg(p \vee q)$

We compare $p \downarrow q$ with $\neg(p \vee q)$ using a truth table:

p	q	$p \vee q$	$\neg(p \vee q)$	$p \downarrow q$
T	T	T	F	F
T	F	T	F	F
F	T	T	F	F
F	F	F	T	T

The columns for $\neg(p \vee q)$ and $p \downarrow q$ are identical, confirming $p \downarrow q \equiv \neg(p \vee q)$.

Q7: Showing $\{\downarrow\}$ is Functionally Complete

A set of operators is functionally complete if it can express negation, conjunction, and disjunction (or equivalently, $\neg$ and $\vee$ or $\neg$ and $\wedge$). We show this for $\{\downarrow\}$ in two parts.

Q7a: Showing $p \downarrow p \equiv \neg p$

We construct a truth table for $p \downarrow p$:

p	$p \downarrow p$	$\neg p$
T	F	F
F	T	T

Since $p \downarrow p$ matches $\neg p$, we have $p \downarrow p \equiv \neg p$.

Q7b: Showing $(p \downarrow q) \downarrow (p \downarrow q) \equiv p \vee q$

We construct a truth table:

p	q	$p \downarrow q$	$(p \downarrow q) \downarrow (p \downarrow q)$	$p \vee q$
T	T	F	T	T
T	F	F	T	T
F	T	F	T	T
F	F	T	F	F

The column for $(p \downarrow q) \downarrow (p \downarrow q)$ matches $p \vee q$. Since we can express $\neg p$ (from Q7a) and $p \vee q$, and Q1 shows that $\{\neg, \vee\}$ is functionally complete, $\{\downarrow\}$ is functionally complete.

Q8: Expressing $p \rightarrow q$ using only $\downarrow$

We proved $p \rightarrow q \equiv \neg p \vee q$ in class so using this and the work from Q7:

- $\neg p \equiv p \downarrow p$.

- $p \vee q \equiv (p \downarrow q) \downarrow (p \downarrow q)$.

Thus, $p \rightarrow q \equiv \neg p \vee q \equiv (p \downarrow p) \vee q \equiv ((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$. The truth table verifies:

p	q	$p \downarrow p$	$(p \downarrow p) \downarrow q$	$((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$	$p \rightarrow q$
T	T	F	T	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

The columns match, so $p \rightarrow q \equiv ((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$.

Q9: Showing $p|q \equiv q|p$

We compare $p|q$ and $q|p$ using a truth table:

p	q	$p|q$	$q|p$
T	T	F	F
T	F	T	T
F	T	T	T
F	F	T	T

The columns for $p|q$ and $q|p$ are identical, confirming $p|q \equiv q|p$.

16   Homework 3

Show all your work to get credit.

Name: Valen Li

Date: September 21, 2025

Problem 22. Prove that $\neg[r \vee (q \wedge (\neg r \to \neg p))] \equiv \neg r \wedge (p \vee \neg q)$ by using a series of logical equivalences.

Solution:

- Simplify the implication: $\neg r \to \neg p \equiv \neg(\neg r) \vee \neg p \equiv r \vee \neg p$. Thus, the expression becomes:

$$\neg[r \vee (q \wedge (r \vee \neg p))].$$

- Apply De Morgan's Law to the negation of the disjunction:

$$\neg[r \vee (q \wedge (r \vee \neg p))] = \neg r \wedge \neg(q \wedge (r \vee \neg p)).$$

- Apply De Morgan's to the negated conjunction:

$$\neg(q \wedge (r \vee \neg p)) = \neg q \vee \neg(r \vee \neg p).$$

  So the expression is:
$$\neg r \wedge (\neg q \vee \neg(r \vee \neg p)).$$

- Simplify $\neg(r \vee \neg p)$:
$$\neg(r \vee \neg p) = \neg r \wedge \neg(\neg p) = \neg r \wedge p.$$

  Thus:
$$\neg r \wedge (\neg q \vee (\neg r \wedge p)).$$

- Distribute $\neg q \vee (\neg r \wedge p)$:

$$\neg q \vee (\neg r \wedge p) = (\neg q \vee \neg r) \wedge (\neg q \vee p).$$

  So the expression becomes:
$$\neg r \wedge (\neg q \vee \neg r) \wedge (\neg q \vee p).$$

- Apply the absorption law:
$$\neg r \wedge (\neg q \vee \neg r) = \neg r.$$

  Resulting in:
$$\neg r \wedge (\neg q \vee p).$$

- Recognize that $\neg q \vee p = p \vee \neg q$ (commutative property), so:

$$\neg r \wedge (p \vee \neg q).$$

  This matches the right hand side we were given at the start.

Problem 23. Express the following propositions using quantifiers, then express the negation in English and using quantifiers:
(a) Some people have no common sense.
(b) All Swedish movies are boring.
(c) No one can keep a secret.
(d) Someone in this class has a bad attitude.
Make sure you indicate the predicate and its domain.

Solution:

(a) **Proposition:** Some people have no common sense.

  – **Predicate:** $C(x) = $ "x has common sense."
  – **Domain:** All people.
  – **Quantified Form:** $\exists x \neg C(x)$.
  – **Negation (English):** "All people have common sense."
  – **Negation (Quantifiers):** $\neg(\exists x \neg C(x)) \equiv \forall x C(x)$.

(b) **Proposition:** All Swedish movies are boring.

  – **Predicate:** $B(x) = $ "x is boring."
  – **Domain:** All Swedish movies.
  – **Quantified Form:** $\forall x B(x)$.
  – **Negation (English):** "Some Swedish movies are not boring."
  – **Negation (Quantifiers):** $\neg(\forall x B(x)) \equiv \exists x \neg B(x)$.

(c) **Proposition:** No one can keep a secret.

  – **Predicate:** $K(x) = $ "x can keep a secret."
  – **Domain:** All people.
  – **Quantified Form:** $\forall x \neg K(x)$.
  – **Negation (English):** "Someone can keep a secret."
  – **Negation (Quantifiers):** $\neg(\forall x \neg K(x)) \equiv \exists x K(x)$.

(d) **Proposition:** Someone in this class has a bad attitude.

  – **Predicate:** $A(x) = $ "x has a bad attitude."
  – **Domain:** All people in this class.
  – **Quantified Form:** $\exists x A(x)$.
  – **Negation (English):** "No one in this class has a bad attitude."
  – **Negation (Quantifiers):** $\neg(\exists x A(x)) \equiv \forall x \neg A(x)$.

Problem 24. Let $M(x) = $ "x is a millionaire" and $P(x) = $ "x drives a Porsche". The domain is all people. Translate to English:
(a) $\forall x(M(x) \to P(x))$
(b) $\exists x(M(x) \to P(x))$
(c) $\forall x(M(x) \land P(x))$
(d) $\exists x(M(x) \lor P(x))$

Solution:

(a) $\forall x(M(x) \rightarrow P(x))$: "All millionaires drive a Porsche."

(b) $\exists x(M(x) \rightarrow P(x))$: Since $M(x) \rightarrow P(x) \equiv \neg M(x) \vee P(x)$, this translates to: "There exists a person who is either not a millionaire or drives a Porsche."

(c) $\forall x(M(x) \wedge P(x))$: "Everyone is both a millionaire and drives a Porsche."

(d) $\exists x(M(x) \vee P(x))$: "There exists a person who is either a millionaire or drives a Porsche."

Problem 25. Prove that $\cos x$ and $\sin x$ are continuous $\forall x \in \mathbb{R}$.

(I didn't understand how to prove this, so I watched a YouTube video that explained it and I only kinda get it so heres my attempt at the proof)

Solution:
To prove that $\sin x$ is continuous at every point $a \in \mathbb{R}$, we need to show that for every $\epsilon > 0$, there exists a $\delta > 0$ such that if $|x - a| < \delta$, then $|\sin x - \sin a| < \epsilon$.
Start with the trigonometric identity:

$$\sin x - \sin a = 2\cos\left(\frac{x+a}{2}\right)\sin\left(\frac{x-a}{2}\right).$$

Taking the absolute value:

$$|\sin x - \sin a| = 2\left|\cos\left(\frac{x+a}{2}\right)\right|\left|\sin\left(\frac{x-a}{2}\right)\right|.$$

Since $|\cos\theta| \leq 1$ for any θ, this simplifies to:

$$|\sin x - \sin a| \leq 2\left|\sin\left(\frac{x-a}{2}\right)\right|.$$

We use the known inequality $|\sin\theta| \leq |\theta|$ for all real θ (this can be established geometrically: in the unit circle, the vertical distance $\sin\theta$ is less than or equal to the arc length θ for $\theta \geq 0$, and by symmetry for $\theta < 0$):

$$\left|\sin\left(\frac{x-a}{2}\right)\right| \leq \left|\frac{x-a}{2}\right| = \frac{|x-a|}{2}.$$

Substituting back:

$$|\sin x - \sin a| \leq 2 \cdot \frac{|x-a|}{2} = |x-a|.$$

To make $|\sin x - \sin a| < \epsilon$, choose $\delta = \epsilon$. Then, if $|x-a| < \delta = \epsilon$, we have $|\sin x - \sin a| \leq |x-a| < \epsilon$. This δ works for any a, so $\sin x$ is continuous everywhere.

Similarly, for $\cos x$ at $a \in \mathbb{R}$:

$$\cos x - \cos a = -2\sin\left(\frac{x+a}{2}\right)\sin\left(\frac{x-a}{2}\right).$$

Taking the absolute value:

$$|\cos x - \cos a| = 2\left|\sin\left(\frac{x+a}{2}\right)\right|\left|\sin\left(\frac{x-a}{2}\right)\right|.$$

Since $|\sin\theta| \le 1$ for any θ:

$$|\cos x - \cos a| \le 2 \cdot 1 \cdot \left|\sin\left(\frac{x-a}{2}\right)\right| = 2\left|\sin\left(\frac{x-a}{2}\right)\right|.$$

Again, using $|\sin\theta| \le |\theta|$:

$$2\left|\sin\left(\frac{x-a}{2}\right)\right| \le 2 \cdot \frac{|x-a|}{2} = |x-a|.$$

So:

$$|\cos x - \cos a| \le |x-a|.$$

Choose $\delta = \epsilon$. If $|x-a| < \delta = \epsilon$, then $|\cos x - \cos a| < \epsilon$.
This works for any a, so $\cos x$ is continuous everywhere.

17 Homework 4

Practice Exam 1 Discrete Mathematics 1

This is a mandatory homework. Show all your work to get credit.

Name: Valen Li **Due Date**: 10/03/25

Problem 26. The following sign is at the entrance of a restaurant: "No shoes, no shirt, no service." Write this sentence as a conditional proposition.

-Lets set p equal to "The user wears shoes", q equal to "The user wears a shirt", and r equal to "Service is provided". Then $\neg p$ is "No shoes", $\neg q$ is "No shirt", and $\neg r$ is "No service". The requirement for service is (shoes $\wedge$ shirt). The conditional proposition is:

$$(\neg p \wedge \neg q) \to \neg r$$

Problem 27. Write these system specifications in symbols using the propositions:
v: "The user enters a valid password,"
a: "Access is granted to the user,"
c: "The user has contacted the network administrator,"
and logical connectives. Then determine if the system specifications are consistent (i.e. all 3 statements can be simultaneously true).
(i) "The user has contacted the network administrator, but does not enter a valid password."
(ii) "Access is granted whenever the user has contacted the network administrator or enters a valid password."
(iii) "Access is denied if the user has not entered a valid password or has not contacted the network administrator."

i) $C \wedge \neg V$

ii) $(C \vee V) \to A$

iii) $(\neg V \vee \neg C) \to \neg A$

1.For (i) to be True, we must have $C = \mathbf{T}$ and $V = \mathbf{F}$. 2.Substitute $C = T$ and $V = F$ into (iii):

$$(\neg F \vee \neg T) \to \neg A \equiv (T \vee F) \to \neg A \equiv T \to \neg A$$

For (iii) to be True, the conclusion $\neg A$ must be True, so $A = \mathbf{F}$. 3.Now, check if the truth assignment $V = F, A = F, C = T$ satisfies (ii):

$$(C \vee V) \to A \equiv (T \vee F) \to F \equiv T \to F$$

The statement $T \to F$ is False.
Since the requirement for (i) and (iii) to be true ($V = F, A = F, C = T$) makes (ii) false, there is no assignment that makes all three true. Therefore, the system specifications are inconsistent.

Problem 28. Solve this puzzle: You meet two people, A and B. Each person either always tells the truth or always lies. Person A tells you, "We are not both truthtellers."

Determine, if possible, which type of person each one is.

Let P_A be the proposition "A is a truthteller" and P_B be the proposition "B is a truthteller". A's statement S is $\neg(P_A \wedge P_B)$.

1.Assume A is a Liar ($\neg P_A$): A's statement S must be False.

$$\neg S \equiv P_A \wedge P_B$$

For $P_A \wedge P_B$ to be True, P_A must be True. This contradicts our assumption that A is a Liar ($\neg P_A$). Thus, this case is impossible.

2.Assume A is a Truthteller (P_A): A's statement S must be True.

$$S \equiv \neg(P_A \wedge P_B)$$

Since P_A is True, $S \equiv \neg(T \wedge P_B) \equiv \neg P_B$. Since S must be True, $\neg P_B$ must be True. This means P_B is False.

Conclusion: A must be a truthteller (Knight) and B must be a liar (Knave).

Problem 29. Write the following statement and its negation symbolically: "If it is Thursday, then we are going to swim only if it is not raining".

Let p: "It is Thursday", q: "We are going to swim", r: "It is raining". The phrase "A only if B" means $A \rightarrow B$. So, "we are going to swim only if it is not raining" is $q \rightarrow \neg r$. The entire statement is in the form "If p, then $q \rightarrow \neg r$":

$$\text{Statement: } p \rightarrow (q \rightarrow \neg r)$$

To find the negation, we first simplify the statement using logical equivalences:

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

Now negate the simplified form:

$$\text{Negation: } \neg(\neg(p \wedge q \wedge r)) \equiv p \wedge q \wedge r$$

In English, the negation is: "It is Thursday, and we are going to swim, and it is raining."

Problem 30. Prove that $p \rightarrow (q \vee r) \equiv (p \wedge \neg q) \rightarrow r$ by using a series of logical equivalences.

$$
\begin{array}{rcll}
(p \wedge \neg q) \rightarrow r & \equiv & \neg(p \wedge \neg q) \vee r & \text{(Implication Law: } A \rightarrow B \equiv \neg A \vee B) \\
& \equiv & (\neg p \vee \neg(\neg q)) \vee r & \text{(De Morgan's Law)} \\
& \equiv & (\neg p \vee q) \vee r & \text{(Double Negation)} \\
& \equiv & \neg p \vee (q \vee r) & \text{(Associative Law)} \\
& \equiv & p \rightarrow (q \vee r) & \text{(Implication Law)}
\end{array}
$$

The two expressions are equivalent.

Problem 31. Consider this sentence, which is Section 2 of Article I of the U. S. Constitution: "No person shall be a Representative who shall not have attained the age of twenty-five years, and been seven years a citizen of the United States, and who shall not, when elected, be an inhabitant of that state in which he shall be chosen."

(a) Rewrite the sentence in English in the form "If . . . , then . . . ".
(b) Using the predicates A(x): "x is at least twenty-five years old," C(x): "x has been a citizen of the United States for at least seven years," I(x): "x, when elected, is an inhabitant of the state in which he is chosen," and R(x): "x can be a Representative," where the universe for x in all four predicates consists of all people, rewrite the sentence using quantifiers and these predicates. [Note: At the time at which the U. S. Constitution was ratified, the universe for x consisted of landowning males.]

a) If a person is a Representative, then that person is at least 25 years old, has been a citizen of the United States for at least 7 years, and is an inhabitant of the state from which they are chosen when elected.

b) The sentence establishes the necessary conditions for being a Representative. The form is $R(x) \to$ (requirements).

$$\forall x(R(x) \to (A(x) \land C(x) \land I(x)))$$

Problem 32. Suppose that the universe for x and y is $\{1, 2, 3\}$. Also, assume that P(x,y) is a predicate that is true in the following cases, and false otherwise: P(1,3),P(2,1),P(2,2),P(3,1),P(3,2),P(3,3). Determine whether each of the following is true or false:
(a) $\forall y \exists x(x \neq y \land P(x, y))$.
(b) $\forall x \exists y(x \neq y \land \neg P(x, y))$.
(c) $\forall y \exists x(x \neq y \land \neg P(x, y))$.

The false cases $\neg P(x, y)$ are: $(1, 1), (1, 2), (2, 3)$.
a) $\forall y \exists x(x \neq y \land P(x, y))$. (True)

- $y = 1$: $\exists x \neq 1 \mid P(x, 1)$? Yes, $P(2, 1)$ and $P(3, 1)$ are True.

- $y = 2$: $\exists x \neq 2 \mid P(x, 2)$? Yes, $P(3, 2)$ is True.

- $y = 3$: $\exists x \neq 3 \mid P(x, 3)$? Yes, $P(1, 3)$ is True.

b) $\forall x \exists y(x \neq y \land \neg P(x, y))$. (False)

- $x = 1$: $\exists y \neq 1 \mid \neg P(1, y)$? Yes, $\neg P(1, 2)$ is True.

- $x = 2$: $\exists y \neq 2 \mid \neg P(2, y)$? Yes, $\neg P(2, 3)$ is True.

- $x = 3$: $\exists y \neq 3 \mid \neg P(3, y)$? No. $P(3, 1), P(3, 2), P(3, 3)$ are all True, so $\neg P(3, y)$ is never True.

Since it fails for $x = 3$, the statement is False.
c) $\forall y \exists x(x \neq y \land \neg P(x, y))$. (False)

- $y = 1$: $\exists x \neq 1 \mid \neg P(x, 1)$? No. $P(1, 1)$ is False (so $\neg P(1, 1)$ is True, but $x \neq 1$ is required). $P(2, 1)$ and $P(3, 1)$ are True, so $\neg P(2, 1)$ and $\neg P(3, 1)$ are False.

Since it fails for $y = 1$, the statement is False.

Problem 33. Determine whether this argument is valid:
Lynn works part time or full time. $(P \lor F)$
If Lynn does not play on the team, then she does not work part time. $(\neg T \to \neg P)$
If Lynn plays on the team, she is busy. $(T \to B)$
Lynn does not work full time. $(\neg F)$

Therefore, Lynn is busy. $(\therefore B)$

The argument is valid.

$$
\begin{array}{lll}
1. & P \vee F & \text{(Premise 1)} \\
2. & \neg T \to \neg P & \text{(Premise 2)} \\
3. & T \to B & \text{(Premise 3)} \\
4. & \neg F & \text{(Premise 4)} \\
5. & P & \text{(Disjunctive Syllogism from 1 and 4)} \\
6. & P \to T & \text{(Contrapositive from 2)} \\
7. & T & \text{(Modus Ponens from 5 and 6)} \\
8. & B & \text{(Modus Ponens from 7 and 3)}
\end{array}
$$

The conclusion B logically follows from the premises.

Problem 34. Give a proof by contradiction of: "If n is an even integer, then $3n + 7$ is odd."

We want to prove $p \to q$, where p: "n is an even integer" and q: "$3n + 7$ is odd". Assume the negation of the conclusion, $\neg q$, holds: $3n + 7$ is even. Since n is an even integer (premise p), we can write $n = 2k$ for some integer k. Substituting $n = 2k$ into the assumption:

$$3n + 7 = 3(2k) + 7 = 6k + 7$$

By our assumption, $6k + 7$ is even, so $6k + 7 = 2m$ for some integer m.
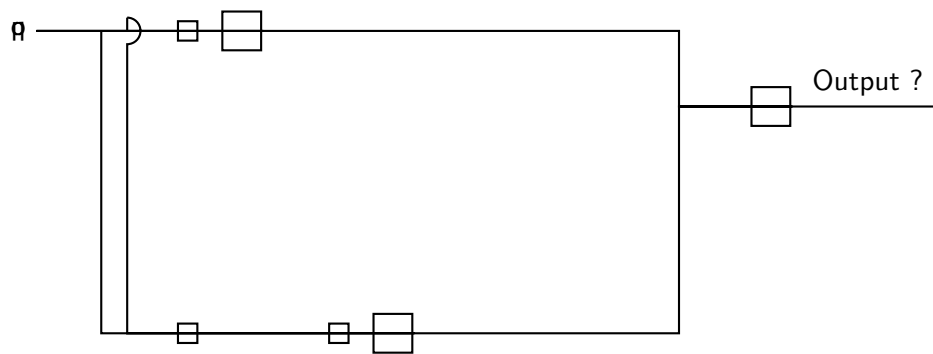
$$6k + 7 = 2m$$

$$6k - 2m = -7$$

$$2(3k - m) = -7$$

Let $j = 3k - m$. Since k and m are integers, j is an integer.

$$2j = -7$$

This equation states that an even integer $2j$ is equal to an odd integer -7. This is a contradiction. Therefore, our assumption ($\neg q$) must be false, and the original conclusion (q) that $3n + 7$ is odd must be true.

Problem 35. Find the output of the following logic gate:

$$(p \wedge \neg q) \vee (\neg p \wedge \neg q)$$

Problem 36. Prove, using whatever method you want, that at least one of the real numbers $a_1, a_2, ..., a_n$ is greater than or equal to the average of these numbers.

1. Let $\bar{a}$ be the average of the n real numbers $a_1, a_2, \ldots, a_n$. 2. By the definition of the average, we have:

$$\bar{a} = \frac{a_1 + a_2 + \cdots + a_n}{n}$$

3. Multiplying by n gives:

$$n\bar{a} = a_1 + a_2 + \cdots + a_n$$

4. Rearranging the terms shows that the sum of the differences between each number and the average is zero:

$$0 = (a_1 - \bar{a}) + (a_2 - \bar{a}) + \cdots + (a_n - \bar{a})$$

For a sum of n real numbers to equal zero, it is impossible for all n numbers to be strictly negative. If $(a_i - \bar{a}) < 0$ for all i, the sum would be strictly less than zero.
Therefore, at least one of the difference terms, say $(a_k - \bar{a})$, must be greater than or equal to zero:

$$a_k - \bar{a} \geq 0$$

Adding $\bar{a}$ to both sides yields the desired result:

$$a_k \geq \bar{a}$$

We conclude that at least one of the numbers is greater than or equal to the average.

Problem 37. Prove by contraposition: $x \in \mathbb{R}, x^2 - 6x + 5 > 0 \rightarrow x \geq 5 \ \lor \ x \leq 1$

Let P be $x^2 - 6x + 5 > 0$ and Q be $x \geq 5 \lor x \leq 1$. We prove the contrapositive $\neg Q \rightarrow \neg P$.

- Hypothesis ($\neg Q$): The negation of $x \geq 5 \lor x \leq 1$ is $x < 5 \land x > 1$, or $1 < x < 5$.

- Conclusion ($\neg P$): The negation of $x^2 - 6x + 5 > 0$ is $x^2 - 6x + 5 \leq 0$.

Proof: Assume $1 < x < 5$. Factor the quadratic: $x^2 - 6x + 5 = (x - 5)(x - 1)$. Since $x < 5$, the factor $(x - 5)$ is negative. Since $x > 1$, the factor $(x - 1)$ is positive. The product of a negative number and a positive number is negative:

$$(x - 5)(x - 1) < 0$$

Thus, $x^2 - 6x + 5 \leq 0$ is true. Since the contrapositive is true, the original statement is also true.

Problem 38. Prove by contradiction $\sqrt{3}$ is irrational

Assume, for the sake of contradiction, that $\sqrt{3}$ is rational. If $\sqrt{3}$ is rational, it can be written as a fraction $\frac{a}{b}$, where a and b are integers, $b \neq 0$, and $\frac{a}{b}$ is in simplest form (a and b have no common factors other than 1).

$$\sqrt{3} = \frac{a}{b}$$

Squaring both sides gives:

$$3 = \frac{a^2}{b^2}$$

$$3b^2 = a^2 \quad (*)$$

Since a^2 equals 3 times an integer (b^2), a^2 must be divisible by 3. By the fundamental theorem of arithmetic, if 3 divides a^2, then 3 must divide a. Therefore, we can write $a = 3k$ for some integer k. Substitute $a = 3k$ back into equation $(*)$:

$$3b^2 = (3k)^2$$

$$3b^2 = 9k^2$$

Divide both sides by 3:

$$b^2 = 3k^2$$

Since b^2 equals 3 times an integer (k^2), b^2 must be divisible by 3. Again, by the fundamental theorem of arithmetic, if 3 divides b^2, then 3 must divide b. We have established that 3 divides a (since $a = 3k$) and 3 divides b. This means that a and b have a common factor of 3. This contradicts our initial assumption that $\dfrac{a}{b}$ was in simplest form (i.e., a and b have no common factors other than 1). Therefore, the initial assumption that $\sqrt{3}$ is rational must be false. Hence, $\sqrt{3}$ is irrational.

18   Homework 5

Exam 2 Discrete Mathematics 1 Solutions

Name: Valen Li **Due Date**: 10/15/25

Code snippet

Problem 39. In this exercise, you prove the Schröder-Bernstein theorem. Suppose that A and B are sets where $|A| \leq |B|$ and $|B| \leq |A|$. This means that there are injections $f : A \to B$ and $g : B \to A$. To prove the theorem, we must show that there is a bijection $h : A \to B$, implying that $|A| = |B|$. To build $h : A \to B$, we construct the chain of an element $a \in A$. This chain contains the elements $a, f(a), g(f(a)), f(g(f(a))), g(f(g(f(a)))), ...$ It also may contain more elements that precede a, extending the chain backwards. So, if there is an element $b \in B$ with $g(b) = a$, then the element b will be the term of the chain just before the element a. Because $g : B \to A$ may not be a surjection, there may not be any such b, so that a is the first element of the chain. If such an element b exists, because $g : B \to A$ is an injection, it is the unique element of B mapped by g to a; hence we denote it by $g^{-1}(a)$. We extend the chain backwards as long as possible in the same way, adding $f^{-1}(g^{-1}(a)), g^{-1}(f^{-1}(g^{-1}(a))), ...$ To construct the proof, complete these five parts.

(a) Each element in $A \cup B$ belongs to exactly one chain. The functions $f : A \to B$ and $g : B \to A$ define a partition of $A \cup B$ into disjoint chains (sequences or cycles). The relationship is defined by $a \to f(a)$ for $a \in A$ and $b \to g(b)$ for $b \in B$. Since f and g are injective, each element has at most one predecessor and one successor, ensuring the set is partitioned into these unique sequences.
(b) Chains are categorized by their backward structure (origin):

- Type 1 (Loop) / Type 2 ($\mathbf{C_\infty}$): Cyclic or infinite both ways.

- Type 3 ($\mathbf{C_A}$): Ends backward at $a_0 \in A$ (no $b \in B$ such that $g(b) = a_0$).

- Type 4 ($\mathbf{C_B}$): Ends backward at $b_0 \in B$ (no $a \in A$ such that $f(a) = b_0$).

Let $\mathcal{C}_f$ be the union of Type 1, 2, 3 chains, and $\mathcal{C}_{g^{-1}}$ be Type 4 chains.
(c) Define the bijection candidate $h : A \to B$:

$$h(a) = \begin{cases} f(a) & \text{if } a \text{ is in } \mathcal{C}_f, \\ g^{-1}(a) & \text{if } a \text{ is in } \mathcal{C}_{g^{-1}}. \end{cases}$$

For $a \in \mathcal{C}_{g^{-1}} = C_B$, a is necessarily of the form $g(b)$ for some $b \in B$ (since the chain begins at $b_0 \in B$, a cannot be the chain's origin), so $g^{-1}(a)$ is well-defined in B.
(d) To show h is injective, let $h(a_1) = h(a_2)$.

- Same Type: If $a_1, a_2 \in \mathcal{C}_f$, $f(a_1) = f(a_2) \implies a_1 = a_2$ (by injectivity of f). If $a_1, a_2 \in \mathcal{C}_{g^{-1}}$, $g^{-1}(a_1) = g^{-1}(a_2) \implies a_1 = a_2$ (by injectivity of g).

- Mixed Types: If $a_1 \in \mathcal{C}_f$ and $a_2 \in \mathcal{C}_{g^{-1}}$, then $f(a_1) = g^{-1}(a_2)$. Applying g gives $g(f(a_1)) = a_2$. This establishes a connection $a_1 \to f(a_1) \to a_2$, meaning a_1 and a_2 are in the same chain. This is a contradiction, as connected elements must be in the same type of chain ($\mathcal{C}_f$ vs $\mathcal{C}_{g^{-1}}$).

Thus, h is one-to-one.
(e) To show h is onto, take $b \in B$.

- If $b \in \mathcal{C}_f$: Every $b \in B$ in these chains must have a predecessor $a \in A$ such that $f(a) = b$. For this a, $h(a) = f(a) = b$.

- If $b \in \mathcal{C}_{g^{-1}}$: Let $a = g(b)$. Then $a \in A$ and a is also in $\mathcal{C}_{g^{-1}}$. By definition, $h(a) = h(g(b)) = g^{-1}(g(b)) = b$.

All $b \in B$ are covered, so h is onto. Thus, h is a bijection, proving $|A| = |B|$.

Problem 40. To show $|(0,1)| = |\mathbb{R}|$, construct a bijection $h : (0,1) \to \mathbb{R}$, defined as:

$$h(x) = \tan\left(\pi x - \frac{\pi}{2}\right).$$

- Domain: For $x \in (0,1)$, $\pi x - \frac{\pi}{2} \in (-\frac{\pi}{2}, \frac{\pi}{2})$, where $\tan$ maps to $\mathbb{R}$.

- Injectivity: If $h(x_1) = h(x_2)$, then $\tan(\pi x_1 - \frac{\pi}{2}) = \tan(\pi x_2 - \frac{\pi}{2})$. Since $\tan$ is injective on $(-\frac{\pi}{2}, \frac{\pi}{2})$, $\pi x_1 - \frac{\pi}{2} = \pi x_2 - \frac{\pi}{2}$, so $x_1 = x_2$.

- Surjectivity: For $y \in \mathbb{R}$, solve $h(x) = y$: $\tan(\pi x - \frac{\pi}{2}) = y$, so $\pi x - \frac{\pi}{2} = \arctan(y)$, hence $x = \frac{\arctan(y) + \frac{\pi}{2}}{\pi}$. Since $\arctan(y) \in (-\frac{\pi}{2}, \frac{\pi}{2})$, $x \in (0,1)$, and $h(x) = y$.

Thus, h is a bijection, so $|(0,1)| = |\mathbb{R}|$.

19   Homework 6

Homework 2 MATH163   Show all your work to get credit.

Name: Valen Li **Due Date**: 10/24/25

Problem 41. Let $S = \{\emptyset, a, \{a\}\}$. Determine whether each of these is an element of S, a subset of S, neither, or both. Justify your answer
(a) {a}
(b) {{a}}
(c) $\emptyset$
(d) $\{\{\emptyset\}, a\}$
(e) $\{\emptyset\}$
(f) $\{\emptyset, a\}$

(a) $\{a\}$ is both an element of S and a subset of S. Since $\{a\}$ appears in S, it is an element of S. Additionally, every element of $\{a\}$ is contained in S (specifically, S contains the element a), so $\{a\}$ is a subset of S.

(b) $\{\{a\}\}$ is not an element of S, but it is a subset of S. The set $\{\{a\}\}$ does not appear in S, so it is not an element of S. However, every element of $\{\{a\}\}$ is contained in S (specifically, S contains the element $\{a\}$), so $\{\{a\}\}$ is a subset of S.

(c) $\emptyset$ is both an element of S and a subset of S. Since $\emptyset$ appears in S, it is an element of S. Moreover, $\emptyset$ contains no elements, so vacuously all its elements are in S. Therefore, $\emptyset$ is a subset of S.

(d) $\{\{\emptyset\}, a\}$ is neither an element of S nor a subset of S. The set $\{\{\emptyset\}, a\}$ does not appear in S, so it is not an element of S. Since $\{\emptyset\}$ is an element of $\{\{\emptyset\}, a\}$ but not of S, the set $\{\{\emptyset\}, a\}$ is not a subset of S.

(e) $\{\emptyset\}$ is not an element of S, but it is a subset of S. The set $\{\emptyset\}$ does not appear in S, so it is not an element of S. However, every element of $\{\emptyset\}$ is contained in S (specifically, S contains the element $\emptyset$), so $\{\emptyset\}$ is a subset of S.

(f) $\{\emptyset, a\}$ is not an element of S, but it is a subset of S. The set $\{\emptyset, a\}$ does not appear in S, so it is not an element of S. However, every element of $\{\emptyset, a\}$ is contained in S (specifically, S contains both $\emptyset$ and a), so $\{\emptyset, a\}$ is a subset of S.

Problem 42. You begin with $1000. You invest it at 5% compounded annually, but at the end of each year you withdraw $100 immediately after the interest is paid.
(a) Set up a recurrence relation and initial condition for the amount you have after n years.
(b) How much is left in the account after you have withdrawn $100 at the end of the third year?
(c) Find a formula for a_n.
(d) Use the formula to determine how long it takes before the last withdrawal reduces the balance in the account to $0.

(a) $S_n = S_{n-1}(1.05) - 100, n \geq 1, S_0 = 1000$

(b)

$$S_0 = 1000 \quad \begin{aligned} S_1 &= S_0(1.05) - 100 \\ &= 1000(1.05) - 100 \\ &= 1050 - 100 \\ &= 950 \end{aligned} \qquad \begin{aligned} S_2 &= S_1(1.05) - 100 \\ &= 950(1.05) - 100 \\ &= 997.5 - 100 \\ &= 897.5 \end{aligned} \qquad \begin{aligned} S_3 &= S_2(1.05) - 100 \\ &= 897.5(1.05) - 100 \\ &= 942.375 - 100 \\ &= 842.375 \end{aligned}$$

After withdrawing $100 at the end of the third year, $842.37 remains in the account.

(c) Let $P = S_0 = 1000, r = 1.05, c = 100$.

$$S_0 = P \qquad S_1 = Pr - c \qquad \begin{aligned} S_2 &= (Pr - c)r - c \\ &= Pr^2 - cr - c \end{aligned} \qquad \begin{aligned} S_3 &= (Pr^2 - cr - c)r - c \\ &= Pr^3 - cr^2 - cr - c \end{aligned}$$

$$\begin{aligned} S_n &= Pr^n - cr^{n-1} - cr^{n-2} - \cdots - cr^1 - c \\ &= Pr^n - c(r^{n-1} + r^{n-2} + \cdots + r + 1) \\ &= Pr^n - c\left(\sum_{i=0}^{n-1} r^i\right) \\ &= Pr^n - c\left(\sum_{i=1}^{n} r^{i-1}\right) \\ &= Pr^n - c\left(\frac{1 - r^n}{1 - r}\right) \\ &= 1000(1.05)^n - 100\left(\frac{1 - 1.05^n}{1 - 1.05}\right) \\ &= 1000(1.05)^n + 2000(1 - 1.05^n) \\ &= 1000(1.05^n + 2 - 2(1.05^n)) \\ &= 1000(-1.05^n + 2) \\ S_n &= -1000(1.05^n - 2) \end{aligned}$$

(d)

$$0 = -1000(1.05^n - 2)$$
$$2 = 1.05^n$$
$$\log_{1.05} 2 = n$$
$$\frac{\log 2}{\log 1.05} = n$$
$$14.21 \approx n$$

It will take 15 years before the last withdrawal reduces the account balance to \$0.

Problem 43. If $P(A)$ means the power set of A,
(a) Prove that $P(A) \cup P(B) \subset P(A \cup B)$ is true for all sets A and B.
(b) Prove that the converse of (a) is not true. That is, prove that:
$P(A \cup B) \subset P(A) \cup P(B)$ is false for some sets A and B.

(a) *Proof.* Let $S \in (P(A) \cup P(B))$ be arbitrary.

Then $S \in P(A) \vee S \in P(B)$. Since S belongs to the power set of A or B, we have $S \subset A \vee S \subset B$.

Now, $P(A \cup B)$ contains all subsets of $A \cup B$, which includes all subsets of A and all subsets of B. Therefore, in either case where $S \subset A$ or $S \subset B$, we have $S \in P(A \cup B)$.

Since S was arbitrary, we conclude that $P(A) \cup P(B) \subset P(A \cup B)$. □

(b) *Proof.* Let $A = \{0\}$ and $B = \{1\}$.

Then $A \cup B = \{0, 1\}$ and $P(A \cup B) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

We have $P(A) = \{\emptyset, \{0\}\}$ and $P(B) = \{\emptyset, \{1\}\}$, so $P(A) \cup P(B) = \{\emptyset, \{0\}, \{1\}\}$.

For $P(A \cup B)$ to be a subset of $P(A) \cup P(B)$, every element of $P(A \cup B)$ must be in $P(A) \cup P(B)$.

However, $\{0, 1\} \in P(A \cup B)$ but $\{0, 1\} \notin P(A) \cup P(B)$. Therefore, $P(A \cup B) \subset P(A) \cup P(B)$ is false for some sets A and B. □

Problem 44. Prove that the following is true for all sets A, B, and C: if $A \cap C \subset B \cap C$ and $A \cup C \subset B \cup C$, then $A \subset B$.

Proof. Let $x \in A$ be arbitrary. We consider two cases:

Case 1: $x \in C$. Then $x \in A \cap C$. Since $A \cap C \subset B \cap C$, we have $x \in B \cap C$. Therefore, $x \in B$.

Case 2: $x \notin C$. Since $x \in A$, we have $x \in A \cup C$. Since $A \cup C \subset B \cup C$, we have $x \in B \cup C$. Because $x \notin C$, it follows that $x \in B$.

In both cases, $x \in B$. Since x was arbitrary, we conclude that $A \subset B$. $\square$

Problem 45. Let $f : R \to R$ have the rule $f(x) = \lceil 3x \rceil + 1$ and $g : R \to R$ have the rule $g(x) = \dfrac{x}{3}$.

(a) Find $(fog)^{-1}(\{2.5\})$.

(b) Find $(fog)^{-1}(\{2\})$.

$$(f \circ g)(x) = \left\lceil 3\left(\frac{x}{3}\right) \right\rceil + 1$$
$$= \lceil x \rceil + 1$$

(a) We need to find all x such that $(f \circ g)(x) = 2.5$. However, since $\lceil x \rceil$ is always an integer and we add 1, $(f \circ g)(x)$ is always an integer. Therefore, $(f \circ g)(x) = 2.5$ has no solutions.

$$(f \circ g)^{-1}(\{2.5\}) = \emptyset$$

(b) We need to find all x such that $(f \circ g)(x) = 2$:

$$\lceil x \rceil + 1 = 2$$
$$\lceil x \rceil = 1$$

The ceiling function equals 1 when $0 < x \leq 1$.

$$(f \circ g)^{-1}(\{2\}) = (0, 1]$$

Problem 46. Find a formula for the recurrence relation $a_n = 2a_{n-1} + 2^n$, $a_0 = 1$, using a recursive method.

$$
\begin{aligned}
a_0 &= a_0 & a_1 &= 2(a_0) + 2^1 & a_2 &= 2(2^1 a_0 + 2^1) + 2^2 & a_3 &= 2(2^2 a_0 + 2(2^2)) + 2^3 \\
&= 1 & &= 2^1 a_0 + 2^1 & &= 2^2 a_0 + 2^2 + 2^2 & &= 2^3 a_0 + 2^3 + 2^3 + 2^3 \\
& & &= 4 & &= 2^2 a_0 + 2(2^2) & &= 2^3 a_0 + 3(2^3) \\
& & & & &= 12 & &= 32
\end{aligned}
$$

Observing the pattern, we obtain:

$$
\begin{aligned}
a_n &= 2^n a_0 + n(2^n) \\
&= 2^n + n(2^n) \\
&= (n+1)2^n
\end{aligned}
$$

Problem 47. Find a formula for an infinite sequence $a_1, a_2, a_3, ...$ that begins with the terms 1,2,1,2,1,2,1 and continues this alternating pattern.

$a_n = 1 + ((n + 1) \bmod 2)$

The expression $(n+1) \bmod 2$ yields 0 when n is odd (since $n+1$ is even) and yields 1 when n is even (since $n+1$ is odd). Adding 1 to this result produces the desired alternating sequence of 1's and 2's.

Problem 48. Find a function $f : \mathbb{Z} \to \mathbb{N}$ that is one-to-one but not onto.

f(x) = $\begin{cases} 2x + 2 & \text{if } x \geq 0 \\ -2x + 3 & \text{if } x < 0 \end{cases}$ This function is one-to-one because no two distinct elements in the domain map to the same element in the codomain. However, it is not onto because the image of f does not equal the entire codomain $\mathbb{N}$ (it misses 1 and 3).

par Find a function $g : \mathbb{N} \to \mathbb{Z}$ that is one-to-one and onto. $g(x) = x/2$ when x is even and $-(x-1)/2$ when x is odd This function is one-to-one because no two distinct elements in the domain map to the same element in the codomain. It is also onto because the image of g equals the entire codomain $\mathbb{Z}$.

Problem 49. Find $1 + x^2 + x^4 + x^6 + x^8 + ...$ assuming $0 < |x| < 1$.

Formula for the sum of a geometric series: $\frac{1}{1-r}$.

Since the common ratio of the sequence above is x^2, the sum is $\frac{1}{1-x^2}$.

Problem 50. Use the Principle of Mathematical Induction to show this inequality is true for all integers $n \geq 2$:
$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} > \sqrt{n}$$

Base Case ($n = 2$):
For $n = 2$, we have:
$$\sum_{i=1}^{2} \frac{1}{\sqrt{i}} = \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} = 1 + \frac{1}{\sqrt{2}}$$

Since $\sqrt{2} < 2$, we have $\frac{1}{\sqrt{2}} > \frac{1}{2}$. Therefore, $1 + \frac{1}{\sqrt{2}} > 1 + \frac{1}{2} = \frac{3}{2}$, which exceeds $\sqrt{2}$. Thus, the base case holds.

Inductive Hypothesis:
Assume that for some positive integer $k \geq 2$, the inequality
$$\sum_{i=1}^{k} \frac{1}{\sqrt{i}} > \sqrt{k}$$

is true.

Inductive Step:
We need to prove that for $n = k + 1$, the inequality
$$\sum_{i=1}^{k+1} \frac{1}{\sqrt{i}} > \sqrt{k+1}$$

holds.
Starting with the left-hand side:
$$\sum_{i=1}^{k+1} \frac{1}{\sqrt{i}} = \left(\sum_{i=1}^{k} \frac{1}{\sqrt{i}} \right) + \frac{1}{\sqrt{k+1}}$$

By the inductive hypothesis, $\sum_{i=1}^{k} \frac{1}{\sqrt{i}} > \sqrt{k}$. Therefore:
$$\sum_{i=1}^{k+1} \frac{1}{\sqrt{i}} > \sqrt{k} + \frac{1}{\sqrt{k+1}}$$

We need to show that $\sqrt{k} + \frac{1}{\sqrt{k+1}} > \sqrt{k+1}$. Squaring both sides:
$$\left(\sqrt{k} + \frac{1}{\sqrt{k+1}} \right)^2 > (\sqrt{k+1})^2$$

Expanding the left-hand side:
$$k + 2\sqrt{k} \cdot \frac{1}{\sqrt{k+1}} + \frac{1}{k+1} > k + 1$$

Subtracting k from both sides:
$$2\sqrt{k} \cdot \frac{1}{\sqrt{k+1}} + \frac{1}{k+1} > 1$$

Simplifying $2\sqrt{k} \cdot \frac{1}{\sqrt{k+1}} = \frac{2\sqrt{k}}{\sqrt{k+1}}$:

$$\frac{2\sqrt{k}}{\sqrt{k+1}} + \frac{1}{k+1} > 1$$

To verify this, multiply through by $\sqrt{k+1}$:

$$2\sqrt{k} + \frac{\sqrt{k+1}}{k+1} > \sqrt{k+1}$$

Squaring $2\sqrt{k} > \sqrt{k+1}$ gives $4k > k+1$, which simplifies to $3k > 1$. Since $k \geq 2$, we have $3k \geq 6 > 1$, confirming the inequality.

Therefore:

$$\sum_{i=1}^{k+1} \frac{1}{\sqrt{i}} > \sqrt{k} + \frac{1}{\sqrt{k+1}} > \sqrt{k+1}$$

By the Principle of Mathematical Induction, the inequality

$$\sum_{i=1}^{n} \frac{1}{\sqrt{i}} > \sqrt{n}$$

holds for all integers $n \geq 2$.

Problem 51. Prove that for all positive integers n, $3^{2^n} - 1$ is divisible by 2^{n+2}.

Base Case: $n = 1$

$$3^{2^1} - 1 = 3^2 - 1 = 9 - 1 = 8 = 2^3 = 2^{1+2}$$

Thus, the base case holds.

Inductive Hypothesis: Assume that for some positive integer k, $3^{2^k} - 1$ is divisible by 2^{k+2}.

Inductive Step: We need to show that for $n = k + 1$, $3^{2^{k+1}} - 1$ is divisible by 2^{k+3}.

$$3^{2^{k+1}} - 1 = (3^{2^k})^2 - 1$$

Using the difference of squares formula $a^2 - b^2 = (a + b)(a - b)$ with $a = 3^{2^k}$ and $b = 1$:

$$3^{2^{k+1}} - 1 = (3^{2^k} + 1)(3^{2^k} - 1)$$

By the inductive hypothesis, $3^{2^k} - 1$ is divisible by 2^{k+2}, so we can write $3^{2^k} - 1 = 2^{k+2} \cdot m$ for some integer m.

$$3^{2^{k+1}} - 1 = (3^{2^k} + 1)(2^{k+2} \cdot m)$$

To prove divisibility by 2^{k+3}, we need to show that $3^{2^k} + 1$ is divisible by 2.

Since 3 is odd, 3^{2^k} is also odd. The sum of an odd number and 1 (which is also odd) gives an even number. Therefore, $3^{2^k} + 1$ is even, meaning it is divisible by 2.

We can write $3^{2^k} + 1 = 2 \cdot \ell$ for some integer ℓ. Thus:

$$3^{2^{k+1}} - 1 = (2 \cdot \ell)(2^{k+2} \cdot m) = 2^{k+3} \cdot \ell m$$

Hence, $3^{2^{k+1}} - 1$ is divisible by 2^{k+3}.

By mathematical induction, for all positive integers n, $3^{2^n} - 1$ is divisible by 2^{n+2}.

Problem 52. Find a formula for

$$(1 - \frac{1}{2^2})(1 - \frac{1}{3^2})(1 - \frac{1}{4^2})(1 - \frac{1}{5^2})...(1 - \frac{1}{n^2})$$

where $n \geq 2$, and use the Principle of Mathematical Induction to prove that the formula is correct.

Proposed Formula: $(1 - \frac{1}{2^2})(1 - \frac{1}{3^2}) \cdots (1 - \frac{1}{n^2}) = \frac{n+1}{2n}$

Base Case $(n = 2)$:
For $n = 2$, the formula gives:

$$\frac{2+1}{2(2)} = \frac{3}{4}$$

The product in the original expression is $(1 - \frac{1}{2^2}) = (1 - \frac{1}{4}) = \frac{3}{4}$. Therefore, the base case holds.

Inductive Hypothesis:
Assume that the formula holds for some positive integer $k \geq 2$:

$$(1 - \frac{1}{2^2})(1 - \frac{1}{3^2}) \cdots (1 - \frac{1}{k^2}) = \frac{k+1}{2k}$$

Inductive Step:
We need to show that the formula holds for $n = k + 1$:

$$(1 - \frac{1}{2^2})(1 - \frac{1}{3^2}) \cdots (1 - \frac{1}{k^2}) \cdot (1 - \frac{1}{(k+1)^2}) = \frac{(k+1)+1}{2(k+1)} = \frac{k+2}{2(k+1)}$$

Starting with the left-hand side and using the inductive hypothesis:

$$(1 - \frac{1}{2^2})(1 - \frac{1}{3^2}) \cdots (1 - \frac{1}{k^2}) \cdot (1 - \frac{1}{(k+1)^2})$$

$$= \frac{k+1}{2k} \cdot (1 - \frac{1}{(k+1)^2})$$

$$= \frac{k+1}{2k} \cdot \frac{(k+1)^2 - 1}{(k+1)^2}$$

$$= \frac{k+1}{2k} \cdot \frac{k^2 + 2k + 1 - 1}{(k+1)^2}$$

$$= \frac{k+1}{2k} \cdot \frac{k^2 + 2k}{(k+1)^2}$$

$$= \frac{k+1}{2k} \cdot \frac{k(k+2)}{(k+1)^2}$$

$$= \frac{(k+1) \cdot k(k+2)}{2k(k+1)^2}$$

$$= \frac{k(k+2)}{2k(k+1)}$$

$$= \frac{k+2}{2(k+1)}$$

This matches our desired result. Therefore, the formula holds for $n = k + 1$.
By mathematical induction, we have shown that the formula

$$(1 - \frac{1}{2^2})(1 - \frac{1}{3^2}) \cdots (1 - \frac{1}{n^2}) = \frac{n+1}{2n}$$

is correct for all positive integers $n \geq 2$.

Problem 53. Which amounts of stamps can be formed using just five cents stamp and nine cents stamp? Prove your answer using strong induction.

We can form any amount of postage greater than or equal to 32 cents using only 5-cent and 9-cent stamps.

Base Cases: We verify that the amounts from 32 to 36 cents can be formed:

- 32 cents: Three 9-cent stamps and one 5-cent stamp ($3 \times 9 + 1 \times 5 = 27 + 5 = 32$).

- 33 cents: Two 9-cent stamps and three 5-cent stamps ($2 \times 9 + 3 \times 5 = 18 + 15 = 33$).

- 34 cents: One 9-cent stamp and five 5-cent stamps ($1 \times 9 + 5 \times 5 = 9 + 25 = 34$).

- 35 cents: Seven 5-cent stamps ($7 \times 5 = 35$).

- 36 cents: Four 9-cent stamps ($4 \times 9 = 36$).

Note that amounts such as 1, 2, 3, 4, 6, 7, 8, 11, 12, 13, 16, 17, 21, 22, 26, 27, 28, 29, 30, and 31 cents cannot be formed, while some smaller amounts like 5, 9, 10, 14, 15, 18, 19, 20, 23, 24, 25 can be formed as previously listed.

Inductive Hypothesis: Assume that for all positive integers k where $32 \leq k \leq n$ (for some $n \geq 36$), we can form k cents using only 5-cent and 9-cent stamps.

Inductive Step: We want to show that we can form $(n + 1)$ cents using these stamps.

Since $n \geq 36$, we have $n - 4 \geq 32$. By the inductive hypothesis, we can form $(n - 4)$ cents. Adding one 5-cent stamp to this gives us $(n - 4) + 5 = n + 1$ cents.

Therefore, we can form $(n + 1)$ cents using only 5-cent and 9-cent stamps.

By strong induction, we have shown that any amount greater than or equal to 32 cents can be formed using 5-cent and 9-cent stamps.

Problem 54. Let P(n) be the statement that a postage of n cents can be formed using just 3-cent stamps and 5- cent stamps. The parts of this exercise outline a strong induction proof that P(n) is true for $n \geq 8$.

a) Show that the statements P(8), P(9), and P(10) are true, completing the basis step of the proof.

We have $3 + 5 = 8$, $3 + 3 + 3 = 9$, and $5 + 5 = 10$, which confirms that P(8), P(9), and P(10) are all true.

b) What is the inductive hypothesis of the proof?

Inductive Hypothesis: $P(k)$ is true for all k where $8 \leq k \leq n$, where $n \geq 10$.

c) What do you need to prove in the inductive step?

We need to prove that $P(n + 1)$ is true.

d) Complete the inductive step for $n \geq 10$.

If $n \geq 10$, then $n + 1 = (n - 2) + 3$. Since $n - 2 \geq 8$, $P(n - 2)$ is true by the inductive hypothesis.

Thus, a postage of $n - 2$ cents can be paid using 3-cent and 5-cent stamps. By adding one 3-cent stamp, we can pay a postage of $n + 1$ cents. Therefore, $P(n + 1)$ is true.

e) Explain why these steps show that this statement is true whenever $n \geq 8$.

The base cases establish that $P(n)$ is true for $n = 8, 9, 10$. The inductive step proves that if $P(k)$ is true for all k in the range $8 \leq k \leq n$ (where $n \geq 10$), then $P(n + 1)$ is also true. By strong induction, this proves $P(n)$ holds for all $n \geq 8$. Specifically, once we have three consecutive values (8, 9, 10), we can generate any subsequent value by adding 3 to a value that is at least 8.

20 Homework 7

Practice for Counting and Discrete Probability

Name: Valen Li

Problem 55. Ten men and ten women are to be put in a row. Find the number of possible rows if no two of the same sex stand adjacent.
Solution:
2 Possible rows: MWMWMWMWM... or WMWMWMWMWM...

For the first slot M or W there are 10 men or 10 women to choose from.
The next slot will have 10 of the alternate gender.
Then 9 then 8...
This is just 10!, so 10! for men and 10! for women = 2 * 10! is the number of possible rows.

Problem 56. In how many ways can 8 of the 9 letters in TETHERING be put in a row?

Solution:

The word TETHERING has letters: T,T,E,T,H,E,R,I,N,G.

Counts: T appears 3 times, E appears 2 times, others 1 time each.

We remove one letter and arrange the remaining 8.

Case 1: Remove one T. Left: T,T,E,E,H,R,I,N,G (2 T, 2 E).

Number of arrangements $= \frac{8!}{2! \cdot 2!} = \frac{40320}{4} = 10080$.

There are 3 T's to remove, so $3 \times 10080 = 30240$.

Case 2: Remove one E. Left: T,T,T,H,R,I,N,G (3 T).

Number of arrangements $= \frac{8!}{3!} = \frac{40320}{6} = 6720$.

There are 2 E's to remove, so $2 \times 6720 = 13440$.

Case 3: Remove H, R, I, N, or G (each appears once).

Left: 8 letters with 3 T and 1 E.

Number of arrangements $= \frac{8!}{3!} = 6720$ each.

5 such letters, so $5 \times 6720 = 33600$.

Total $= 30240 + 13440 + 33600 = 77320$.

Problem 57. Prove the identity

$$\binom{n}{r}\binom{r}{k} = \binom{n-k}{r-k}\binom{n}{k}$$

with $n \geq r \geq k > 0$
a) algebraically
b) using a combinatorial argument.

a) Algebraic proof:

Left side: $\binom{n}{r}\binom{r}{k} = \frac{n!}{r!(n-r)!} \cdot \frac{r!}{k!(r-k)!} = \frac{n!}{k!(r-k)!(n-r)!}$.

Right side: $\binom{n-k}{r-k}\binom{n}{k} = \frac{(n-k)!}{(r-k)!(n-k-r+k)!} \cdot \frac{n!}{k!(n-k)!} = \frac{n!}{k!(r-k)!(n-r)!}$.

Both sides equal.

b) Combinatorial argument:

Left: Choose r people from n, then choose k leaders from those r.

Right: First choose k leaders from n ($\binom{n}{k}$ ways).

Then choose $r - k$ more members from the remaining $n - k$ people ($\binom{n-k}{r-k}$ ways).

Same thing, so equal.

Problem 58. How many solutions are there to the equation $\sum_{i=1}^{i=6} x_i = 31$, where $x_i, (i = 1, 2, 3, 4, 5, 6)$ is a nonnegative integer such that:
a) $x_i > 1$ for $i = 1, 2, 3, 4, 5, 6$?
b) $x_1 \geq 1, x_2 \geq 2, x_3 \geq 3, x_4 \geq 4, x_5 > 5,$ and $x_6 \geq 6$?
c) $x_1 \geq 5$?
d) $x_1 < 8$ and $x_2 > 8$?

a) Let $y_i = x_i - 2$, so $y_i \geq 0$. Then $\sum y_i = 31 - 12 = 19$.

Stars and bars: $\binom{19+6-1}{6-1} = \binom{24}{5}$.

b) Let $y_1 = x_1 - 1, y_2 = x_2 - 2, ..., y_5 = x_5 - 6, y_6 = x_6 - 6$. All $y_i \geq 0$.

Sum: $y_1 + \cdots + y_6 = 31 - (1 + 2 + 3 + 4 + 6 + 6) = 31 - 22 = 9$.

Answer: $\binom{9+6-1}{5} = \binom{14}{5}$.

c) Let $z_1 = x_1 - 5, z_i = x_i$ for $i \geq 2$. All ≥ 0.

Sum: $z_1 + x_2 + \cdots + x_6 = 26$.

Answer: $\binom{26+6-1}{5} = \binom{31}{5}$.

d) $x_1 \leq 7$, $x_2 \geq 9$. Let $w_1 = x_1$, $w_2 = x_2 - 9$.

Sum: $w_1 + w_2 + x_3 + \cdots + x_6 = 31 - 9 = 22$, $0 \leq w_1 \leq 7$, $w_2 \geq 0$.

Total without upper bound: $\binom{22+6-1}{5} = \binom{27}{5}$.

Subtract cases $w_1 \geq 8$: let $w_1' = w_1 - 8$, sum $= 22 - 8 = 14$, $\binom{14+5}{5} = \binom{19}{5}$.

Answer: $\binom{27}{5} - \binom{19}{5}$.

Problem 59. 10 kids are randomly grouped into an A team with five kids and a B team with five kids. Each grouping is equally likely. There are 3 kids in the group, Alex and his two best friends José and Carl. What is the probability that Alex ends up on the same team with at least one of his two best friends?

Total ways to choose teams: $\binom{10}{5} = 256$ (divide by 2, teams unlabeled).

Fix Alex on team A. Choose 4 more from 9 kids.

Cases:

- Both friends with Alex: choose 2 friends + 2 others: $\binom{2}{2}\binom{7}{2} = 21$.

- Exactly one friend: $\binom{2}{1}\binom{7}{3} = 2 \times 35 = 70$.

Favorable: $21 + 70 = 91$.

Probability $= \frac{91}{256} = \frac{13}{36}$.

Problem 60. Sally has two coins. The first coin is a fair coin and the second coin is biased. The biased coin comes up heads with probability .75 and tails with probability .25. She selects a coin at random and flips the coin ten times. The results of the coin flips are mutually independent. The result of the 10 flips is: T,T,H,T,H,T,T,T,H,T. What is the probability that she selected the biased coin?

$P(\text{data} - \text{fair}) = (0.5)^{10} = \frac{1}{1024}$.

$P(\text{data} - \text{biased}) = (0.25)^7(0.75)^3 = \frac{3^3 \cdot 1^7}{4^{10}} = \frac{27}{1048576}$.

$P(\text{biased}) = P(\text{fair}) = 0.5$.

$P(\text{data}) = 0.5 \cdot \frac{1}{1024} + 0.5 \cdot \frac{27}{1048576}$.

$= \frac{512}{1048576} + \frac{27}{1048576} = \frac{539}{1048576}$.

$P(\text{biased} - \text{data}) = \frac{0.5 \cdot 27/1048576}{539/1048576} = \frac{27}{2 \cdot 539} = \frac{27}{1078}$.

Problem 61. You have 40 different books, 20 math books, 15 history books, and 5 geography books.
You pick two books at random, one at a time. What is the probability that the two books are from different disciplines?

Total ways: 40×39.

Favorable:

- Math then not: $20 \times 20 = 400$

- History then not: $15 \times 25 = 375$

- Geography then not: $5 \times 35 = 175$

Total favorable: $400 + 375 + 175 = 950$.

Probability $= \frac{950}{40 \times 39} = \frac{950}{1560} = \frac{95}{156}$

Problem 62. Find the expected value and the variance of the random value k, the number of success, of the binomial distribution.

$E[k] = np$.

$\text{Var}(k) = np(1 - p)$.

Problem 63. Each of 26 cards has a different letter of the alphabet on it. You pick one card at random. A vowel (a, e, i, o, u, y) is worth 3 points and a consonant is worth 0 points. Let X = the value of the card picked. Find E(X), V (X), and the standard deviation of X.

Vowels: 6 (worth 3), consonants: 20 (worth 0).

$E[X] = \frac{6 \cdot 3 + 20 \cdot 0}{26} = \frac{18}{26} = \frac{9}{13}$.

$\text{Var}(X) = E[X^2] - (E[X])^2 = \frac{6 \cdot 9}{26} - \left(\frac{9}{13}\right)^2 = \frac{54}{26} - \frac{81}{169} = \frac{729 - 81}{169 \cdot 13/13}$

$\frac{54}{26} = \frac{27}{13}, so \frac{27}{13} - \frac{81}{169} = \frac{27 \cdot 13 - 81}{169} = \frac{351 - 81}{169} = \frac{270}{169}$.

$$SD = \sqrt{\frac{270}{169}} = \frac{\sqrt{270}}{13} = \frac{3\sqrt{30}}{13}.$$

Problem 64. Urn 1 contains 9 black balls, 6 white balls and 5 green balls; urn 2 contains 12 green balls, 2 black balls and 6 white balls; urn 3 contains 6 green balls, 2 black balls and 2 white balls. You roll a die to determine which urn to choose: if you roll a 1 or 2 you choose urn 1; if you roll a 3 you choose urn 2 and if you roll a 4, 5, or 6 you choose urn 3. Once the urn is chosen, you draw out a ball at random from that urn. Given that the ball is black, what is the probability that the ball came from urn 3?

P(U1) = 2/6 = 1/3, P(U2)=1/6, P(U3)=3/6=1/2.

P(B—U1)=9/20, P(B—U2)=2/20=1/10, P(B—U3)=2/10=1/5.

P(B) = (1/3)(9/20) + (1/6)(1/10) + (1/2)(1/5) = 3/20 + 1/60 + 1/10.

LCM 60: $9/60 + 1/60 + 6/60 = 16/60 = 4/15$.

$P(U3—B) = \frac{(1/2)(1/5)}{4/15} = \frac{1/10}{4/15} = \frac{1}{10} \cdot \frac{15}{4} = \frac{3}{8}.$