MAT2520: DISCRETE MATHEMATICS

ADITHYA BHASKARA
PROFESSOR: KENNETH M. MONKS

TEXTBOOK: OSCAR LEVIN & RICHARD HAMMACK

FRONT RANGE COMMUNITY COLLEGE

Contents

1 Statements, Symbolic Logic, and Proofs **1**
1.1 Lecture 1: May 31, 2022 . . . 1
1.1.1 Introduction to Discrete Mathematics . . . 1
1.1.2 Mathematical Statements . . . 1
1.2 Lecture 2: June 2, 2022 . . . 8
1.2.1 Rules of Inference . . . 8
1.2.2 Predicates and Quantifiers . . . 9
1.3 Lecture 3 & Lecture 4: June 7, 2022 & June 9, 2022 . . . 12
1.3.1 Introduction to Proofs . . . 12
1.3.2 Proof by Induction . . . 12
1.3.3 Direct Proofs . . . 20
1.3.4 Proof by Contrapositive . . . 21
1.3.5 Proof by Contradiction . . . 22

2 Sets, Relations, and Functions **23**
2.1 Lecture 5, June 14, 2022 . . . 23
2.1.1 An Introduction to Sets . . . 23
2.2 Lecture 6: June 16, 2022 . . . 27
2.2.1 Relations . . . 27
2.3 Lecture 7: June 21, 2022 . . . 31
2.3.1 Partitions . . . 31
2.4 Lecture 8: June 23, 2022 . . . 34
2.4.1 Functions . . . 34
2.5 Lecture 9: June 30, 2022 . . . 40
2.5.1 The Pigeonhole Principle . . . 40

3 Enumerative Combinatorics **44**
3.1 Lecture 10: July 5, 2022 . . . 44
3.1.1 The Fundamental Principle of Counting . . . 44
3.1.2 Permutations . . . 45
3.1.3 Combinations . . . 46
3.2 Lecture 11: July 7, 2022 . . . 48
3.2.1 Multichoose . . . 48
3.2.2 Selecting k Objects From n Options . . . 49
3.3 Lecture 12, July 12, 2022 . . . 50
3.3.1 Permutations, With Some Repeats . . . 50
3.3.2 The Principle of Inclusion-Exclusion . . . 51
3.4 Lecture 13: July 14, 2022 . . . 52
3.4.1 Combinatorial Proofs . . . 52
3.4.2 Introduction to Probability . . . 54

4 Generating Functions and Recurrence Relations **57**
4.1 Lecture 14: July 19, 2022 57
4.1.1 Generating Functions and Recurrence Relations 57

5 Number Theory **62**
5.1 Lecture 15: July 21, 2022 62

Pure mathematics is, in its way, the poetry of logical ideas.

Albert Einstein

1 Statements, Symbolic Logic, and Proofs

1.1 Lecture 1: May 31, 2022

1.1.1 Introduction to Discrete Mathematics

The word "discrete" means "individually separate and distinct." Discrete Mathematics relates to mathematics pertaining to discrete, or individually separate and distinct, quantities. Informally, mathematics may be divided into "Continuous Mathematics" and "Discrete Mathematics." Among other things, Continuous Mathematics consists of Algebra, Trigonometry, Calculus, and Differential Equations. Discrete Mathematics includes Combinatorics, Set Theory, Number Theory, and Graph Theory.

1.1.2 Mathematical Statements

Logic is the study of statements and the derivation of novel statements from existing statements. In symbolic logic, we will often assign letters to represent statements. Before we delve too much into statements, we must first define what a statement actually is. Consider the following definition.

Definition 1.1.1: Statements

A statement is any declarative sentence which is able to be either true or false. A statement is *atomic* if it cannot be divided into smaller statements, otherwise, it is called *molecular*.

We often use statements to create arguments. Consider the following definition.

Definition 1.1.2: Arguments

An argument is a set of statements, one of which is called the *conclusion* and the rest of which are called *premises*. An argument is said to be *valid* if the conclusion must be true whenever the premises are all true and *invalid* if it is possible for all the premises to be true and the conclusion to be false.

Logical operators may be used to create molecular statements out of atomic statements. Consider the following.

- CONJUNCTION – "P `and` Q" – $\wedge$
  - $P \wedge Q$ is true if and only if both P and Q are true.

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

- DISJUNCTION – "P `or` Q" – $\vee$
  - $P \vee Q$ is true if and only if either P and Q both true, P is true, or Q is true.

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

- IMPLICATION – "`if` P `then` Q" – $\Longrightarrow$
  - $P \Longrightarrow Q$ is true if either P is false, Q is true, or P is false and Q is true.

P	Q	$P \Longrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

- BICONDITIONAL – "P `if and only if` Q" – $\Longleftrightarrow$
  - $P \Longleftrightarrow Q$ is true if P and Q are either both true or both false.

P	Q	$P \Longleftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

- NEGATION – "not P" – $\neg$
  - $\neg P$ is true when P is false.

P	$\neg P$
T	F
F	T

Consider the following examples.

Example 1.1.1: ☢☢☢ Truth Table 1

Compute the truth table for

$$\neg P \implies (P \vee Q).$$

We proceed by computing the truth table sequentially. First, we compute $\neg P$, which produces

P	Q	$\neg P$
T	T	F
T	F	F
F	T	T
F	F	T

.

Then, we find $P \vee Q$, which yields

P	Q	$\neg P$	$P \vee Q$
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	F

.

We finally perform an implication with $\neg P$ as the precondition and $P \vee Q$ as the postcondition. This produces

P	Q	$\neg P$	$P \vee Q$	$\neg P \implies (P \vee Q)$
T	T	F	T	T
T	F	F	T	T
F	T	T	T	T
F	F	T	F	F

.

We now define the principle of logical equivalence.

Definition 1.1.3: Logical Equivalence

Two molecular statements P and Q are logically equivalent provided P is true precisely when Q is true. To verify that two statements are logically equivalent, the truth tables for each statement must be identical. We may use the principle of logical equivalence to gain insight into statements' meanings, or how to prove or refute them.

Example 1.1.2: ☢☢☢ Truth Table 2

Verify that $\neg P \implies Q$ is logically equivalent to $\neg P \implies (P \vee Q)$. That is, verify

$$(\neg P \implies Q) \iff ((\neg P) \implies (P \vee Q)).$$

Recall that $\neg P \implies (P \vee Q)$ produces a truth table of

P	Q	$\neg P \implies (P \vee Q)$
T	T	T
T	F	T
F	T	T
F	F	F

.

We then find the truth table for $\neg P \implies Q$, producing

P	Q	$\neg P$	$\neg P \implies Q$
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	F

.

As the truth tables match, the statements are logically equivalent. That is,

P	Q	$(\neg P \implies Q) \iff (\neg P \implies (P \vee Q))$
T	T	T
T	F	T
F	T	T
F	F	T

.

When given an implication, we can construct three related statements. Consider the following definitions.

Definition 1.1.4: Inverse of a Statement

Given the implication $P \implies Q$, we may construct the statement

$$\neg P \implies \neg Q,$$

which is the associated inverse. The implication is not equivalent to its inverse.

Definition 1.1.5: Contrapositive of a Statement

Given the implication $P \implies Q$, we may construct the statement

$$\neg Q \implies \neg P,$$

which is the associated contrapositive. The implication is logically equivalent to its contrapositive.

Definition 1.1.6: Converse of a Statement

Given the implication $P \implies Q$, we may construct the statement

$$Q \implies P,$$

which is the associated converse. The implication is not equivalent to its converse.

De Morgan's Laws are another useful application of logical equivalence. Consider the following.

Theorem 1.1.1: De Morgan's Laws

Given two statements P and Q,

$$\neg(P \wedge Q) \iff (\neg P \vee \neg Q)$$

and

$$\neg(P \vee Q) \iff (\neg P \wedge \neg Q).$$

We also state another useful theorem.

Theorem 1.1.2: Implications are Disjunctions

Given two statements P and Q,

$$(P \implies Q) \iff (\neg P \vee Q).$$

With the aid of the above theorems, one may take any statement and simplify it such that negations are only applied to atomic statements, understanding that for any statement, P, $\neg\neg P \iff P$.

Consider the following exercise.

Exercise 1.1.1: ☢☢ Logical Equivalence Without Truth Tables

Show that for two statements P and Q,

$$\neg(P \implies Q) \iff (P \wedge \neg Q)$$

without using truth tables.

Proof. We consider the first statement, $\neg(P \implies Q)$, and see that

$$\begin{aligned} \neg(P \implies Q) &\iff \neg(\neg P \vee Q) \\ &\iff (P \wedge \neg Q), \end{aligned}$$

which is precisely the same as the second given statement. □

Just as implications were disjunctions, the negation of an implication is a conjunction. Consider the following theorem.

Theorem 1.1.3: The Negation of an Implication is a Conjunction

Given two statements P and Q,

$$\neg(P \implies Q) \iff (P \wedge \neg Q).$$

To verify that two statements are logically equivalent, truth tables or a transitive chain of logically equivalent statements may be used; however, truth tables can further verify that two statements are *not* logically equivalent. Consider the following exercises.

Exercise 1.1.2: ☢☢ Simplification 1

Simplify $\neg(P \implies \neg Q)$ such that negation is only applied to P or Q.

We proceed by understanding that implications are disjunctions, producing

$$\begin{aligned} \neg(P \implies \neg Q) &\iff \neg(\neg P \vee \neg Q) \\ &\iff P \wedge Q. \end{aligned}$$

Exercise 1.1.3: ☢☢ Simplification 2

Simplify $(\neg P \vee \neg Q) \implies \neg(\neg Q \wedge R)$ such that negation is only applied to P, Q, or R.

We proceed by applying De Morgan's Laws, producing

$$((\neg P \vee \neg Q) \implies \neg(\neg Q \wedge R)) \iff ((\neg P \vee \neg Q) \implies (Q \vee \neg R)).$$

Exercise 1.1.4: ☢☢☢ Simplification 3

Simplify $\neg((\neg P \wedge Q) \vee \neg(R \vee \neg S))$ such that negation is only applied to P, Q, R, or S.

We proceed by applying De Morgan's Laws, producing

$$\begin{aligned}\neg((\neg P \wedge Q) \vee \neg(R \vee \neg S)) &\iff \neg((\neg P \wedge Q) \vee (\neg R \wedge S)) \\ &\iff \neg(\neg P \wedge Q) \wedge \neg(\neg R \wedge S) \\ &\iff (P \vee \neg Q) \wedge (R \vee \neg S).\end{aligned}$$

Exercise 1.1.5: ☢☢☢ Simplification 4

Simplify $\neg((\neg P \implies \neg Q) \wedge (\neg Q \implies R))$ such that negation is only applied to P, Q, or R.

We proceed by applying De Morgan's Laws, as well as rewriting a statement into its equivalent contrapositive, producing

$$\begin{aligned}\neg((\neg P \implies \neg Q) \wedge (\neg Q \implies R)) &\iff \neg((Q \implies P) \wedge (\neg Q \implies R)) \\ &\iff \neg((\neg Q \vee P) \wedge (Q \vee R)) \\ &\iff \neg(\neg Q \vee P) \vee \neg(Q \vee R) \\ &\iff (Q \wedge \neg P) \vee (\neg Q \wedge \neg R).\end{aligned}$$

1.2 Lecture 2: June 2, 2022

1.2.1 Rules of Inference

Rules of Inference are constructed in the following manner.

$$\begin{array}{l} \hline \text{PREMISE 1} \\ \text{PREMISE 2} \\ \quad\vdots \\ \text{PREMISE } n \\ \hline \therefore \text{ CONCLUSION} \\ \hline \end{array}.$$

Consider the following example.

Example 1.2.1: ☢ The Contrapositive as a Rule of Inference

Write the Contrapositive as a Rule of Inference.

$$\begin{array}{l} \hline P \implies Q \\ \hline \therefore \neg Q \implies \neg P \\ \hline \end{array}.$$

To determine the validity of a Rule of Inference, one may build the Rule of Inference as a statement in the form

$$(\text{PREMISE 1} \wedge \text{PREMISE 2} \wedge \cdots \wedge \text{PREMISE } n) \implies \text{CONCLUSION}.$$

Then, one may build a truth table. If the truth table yields a tautology, the Rule of Inference is valid. Consider the following exercises.

Exercise 1.2.1: ☢ Determine the Validity of a Rule of Inference 1

Determine the validity of

$$\begin{array}{l} \hline \neg(P \vee Q) \\ \hline \therefore \neg P \vee \neg Q \\ \hline \end{array}.$$

We may rewrite $\neg(P \vee Q)$ as $\neg P \wedge \neg Q$.

P	Q	$\neg P \wedge \neg Q$	$\neg P \vee \neg Q$	$(\neg P \wedge \neg Q) \implies (\neg P \vee \neg Q)$
T	T	F	F	T
T	F	F	T	T
F	T	F	T	T
F	F	T	T	T

.

Therefore, the Rule of Inference is valid.

Exercise 1.2.2: ☢ Determine the Validity of a Rule of Inference 2

Determine the validity of

$$\begin{array}{c} P \implies Q \\ P \implies \neg Q \\ \hline \therefore \neg P \end{array}.$$

We consider the truth table

P	Q	$P \implies Q$	$P \implies \neg Q$	$(P \implies Q) \wedge (P \implies \neg Q)$
T	T	T	F	F
T	F	F	T	F
F	T	T	T	T
F	F	T	T	T

.

Then, we consider

P	Q	$((P \implies Q) \wedge (P \implies \neg Q)) \implies \neg P$
T	T	T
T	F	T
F	T	T
F	F	T

.

Therefore, the Rule of Inference is valid.

1.2.2 Predicates and Quantifiers

In mathematics, we use two main quantifiers: the existential and universal quantifiers. Consider the following definition.

Definition 1.2.1: Universal and Existential Quantifiers

The existential quantifier, $\exists$, is read "there exists," or "there is." The universal quantifier, $\forall$, is read "for all."

Recall the Intermediate Value Theorem from Calculus, stating that

> Given a continuous function $f(x)$ on a closed interval $[a, b]$. If K is some real number between $f(a)$ and $f(b)$, there exists some c between a and b such that $f(c) = K$.

We may rewrite the Intermediate Value Theorem, using quantifiers, as

> Given a continuous function $f(x)$ on a closed interval $[a, b]$,
>
> $$\forall K \in [f(a), f(b)], \exists c \in [a, b], f(c) = K.$$

Consider the following exercise.

Exercise 1.2.3: ☢☢ Quantifiers and Validity

Let S be the set of all people. Determine the validity of the following statements.

- $\forall x \in S, \exists y \in S$, x is the mother of y.
  - This is untrue. Not all people are mothers.
- $\exists x \in S, \forall y \in S$, x is the mother of y.
  - This is untrue. There does not exist some person that is the mother to everyone.
- $\exists y \in S, \forall x \in S$, x is the mother of y.
  - This is untrue. There does not exist some person who is the child of everyone, including themself.

The correct statement is $\forall y \in S, \exists x \in S$, x is the mother of y.

Quantifiers may be negated; consider the following theorem relating negation to quantifiers.

Theorem 1.2.1: Quantifiers and Negation

For a predicate, or a sentence containing variables, $P(x)$,

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

and

$$\neg \exists x P(x) \iff \forall x \neg P(x).$$

This relation can be thought of as a Corollary to De Morgan's Laws, stated in Theorem 1.1.1.

Consider the following exercises.

Exercise 1.2.4: ☢☢ The $N-\epsilon$ Definition of the Limit of a Sequence

Recall the $N-\epsilon$ definition of the limit of a sequence. That is, for a sequence a_n and a real number L,

$$\left(\lim_{n\to\infty} a_n = L\right) \iff (\forall \epsilon > 0, \exists N, \forall n \in \mathbb{N}, n > N \implies |a_n - L| < \epsilon).$$

Define $\lim_{n\to\infty} \neq L$.

We simply negate the above quantified statement. This produces

$$\begin{aligned}
\neg\left(\lim_{n\to\infty} a_n = L\right) &\iff \left(\lim_{n\to\infty} a_n \neq L\right) \\
&\iff \neg(\forall \epsilon > 0, \exists N, \forall n \in \mathbb{N}, n > N \implies |a_n - L| < \epsilon) \\
&\iff (\exists \epsilon > 0, \forall N, \exists n \in \mathbb{N}, \neg(n > N \implies |a_n - L| < \epsilon)) \\
&\iff (\exists \epsilon > 0, \forall N, \exists n \in \mathbb{N}, (n > N \wedge |a_n - L| \geq \epsilon)).
\end{aligned}$$

Exercise 1.2.5: ☢☢ A Proof With the Definition of the Limit of a Sequence

Prove that for $a_n = (-1)^n$,

$$\lim_{n\to\infty} a_n \neq 0.$$

Proof. Recall that

$$\left(\lim_{n\to\infty} a_n \neq L\right) \iff (\exists \epsilon > 0, \forall N, \exists n \in \mathbb{N}, (n > N \wedge |a_n - L| \geq \epsilon)).$$

Applying the above definition to the current exercise produces

$$\left(\lim_{n\to\infty} a_n \neq 0\right) \iff (\exists \epsilon > 0, \forall N, \exists n \in \mathbb{N}, (n > N \wedge |a_n| \geq \epsilon)).$$

As $0 < \frac{1}{2} < 1$, we let $\epsilon = \frac{1}{2}$. Let N be an arbitrarily large real number. Let $n = \lceil N \rceil + 1$. Therefore, $n > N$, satisfying the first statement in the above conjunction. We also note that $\forall n, |a_n| = 1$. Therefore, $|a_n| \geq \epsilon$. Both statements of the conjunction are satisfied. □

1.3 Lecture 3 & Lecture 4: June 7, 2022 & June 9, 2022

1.3.1 Introduction to Proofs

Before we delve into techniques to write proofs, let us first define what a proof is.

Definition 1.3.1: Proofs

Mathematical proofs are logical arguments to show that stated premises guarantee that a mathematical statement must be true.

There are multiple techniques to write proofs, but here, we will explore the Proof by Induction, the Direct Proof, the Proof by Contrapositive, the Proof by Contradiction, and the Proof by Cases.

1.3.2 Proof by Induction

We will use quantifiers to state induction.

Let $P(n)$ be a statement with $n \in \mathbb{N}$. Consider the following Rule of Inference.

$$\frac{\begin{array}{c} P(0) \\ P(0) \implies P(1) \\ P(1) \implies P(2) \\ \vdots \\ P(n) \implies P(n+1) \end{array}}{\therefore \forall n \in \mathbb{N}, P(n).}$$

This may be further collapsed into

$$\frac{\begin{array}{c} P(0) \\ \forall k \in \mathbb{N}, P(k) \implies P(k+1) \end{array}}{\therefore \forall n \in \mathbb{N}, P(n).}$$

Generally, in Proofs by Induction, we follow the following steps.

- Start with an iterative propostition that depends on some $n \in \mathbb{N}$, or $P(n)$.
- Prove that the proposition is true for some base case $n = n_0$. That is, show that the proposition is true for the smallest fixed number that the proposition makes sense for.
- Prove the inductive step. Suppose that the proposition holds true for $n = k$, and then prove that the proposition holds for $n = k + 1$. Essentially, suppose $P(k)$ is true, and prove that $P(k + 1)$ is true.
- Then, the proposition is proved $\forall n \in \mathbb{N}$, where $n \geq n_0$.

Consider the following examples and exercises.

Example 1.3.1: ☢☢ Gauss' Formula

Prove that the sum of consecutive integers starting at 1 can be found by Gauss' formula. That is,

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

Proof. Consider the base case $n=1$. Then the left hand side is 1, and the right hand side is

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

Therefore, the left hand side is equal to the right hand side, proving the case base.

We suppose that the relationship is true for $n=k$ where $k\in\mathbb{N}$. That is, we suppose that

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

If we add $k+1$ to both sides, we obtain

$$\begin{aligned}1+2+3+\cdots+k+k+1&=\frac{k(k+1)}{2}+k+1\\&=\frac{k(k+1)+2k+2}{2}\\&=\frac{k^2+3k+2}{2}\\&=\frac{(k+2)(k+1)}{2}\\&=\frac{(k+1)((k+1)+1)}{2}.\end{aligned}$$

This result is the proposition where $n=k+1$. Therefore, the inductive step is true. Therefore, Gauss' formula is true for all $n\in\mathbb{N}$ where $n\geq 1$. □

Example 1.3.2: ☢☢ Sum of Consequtive Squares

Prove that for all $n \in \mathbb{N}, n \geq 1$,

$$1^2 + 2^2 + 3^2 \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof. Consider the base case $n = 1$. Then the left hand side is 1, and the right hand side is

$$\frac{1(1+1)(2+1)}{6} = 1.$$

Therefore, the left hand side is equal to the right hand side, proving the base case.

We suppose that the relationship is true for $n = k$ where $k \in \mathbb{N}$. That is, we suppose that

$$1^2 + 2^2 + 3^2 \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

If we add $k+1$ to both sides, we obtain

$$\begin{aligned}
1^2 + 2^2 + 3^2 \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + k^2 + 2k + 1 \\
&= \frac{k(k+1)(2k+1) + 6k^2 + 12k + 6}{6} \\
&= \frac{2k^3 + 9k^2 + 13k + 6}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.
\end{aligned}$$

This result is the proposition where $n = k+1$. Therefore, the inductive step is true. Therefore, the above formula is true for all $n \in \mathbb{N}$ where $n \geq 1$. □

Exercise 1.3.1: ☢☢ The Power Rule for Derivatives

Prove that for all $n \in \mathbb{N}$, $n \geq 0$,

$$\frac{\mathrm{d}}{\mathrm{d}x} x^n = nx^{n-1}.$$

Proof. Consider the base case $n = 0$. Then the left hand side is 0, as the derivative of any constant is zero, and the right hand side is

$$0x^{0-1} = 0.$$

Therefore, the left hand side is equal to the right hand side, proving the base case.

We suppose that the relationship is true for $n = k$ where $k \in \mathbb{N}$. That is, we suppose that

$$\frac{\mathrm{d}}{\mathrm{d}x} x^k = kx^{k-1}.$$

Consider $\frac{\mathrm{d}}{\mathrm{d}x}[x^{k+1}]$, or $\frac{\mathrm{d}}{\mathrm{d}x}[xx^k]$. Then we have

$$\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}x}[x^{k+1}] &= \frac{\mathrm{d}}{\mathrm{d}x}[xx^k] \\
&= x^k + x(kx^{k-1}) \\
&= x^k + kx^k \\
&= (k+1)x^k.
\end{aligned}$$

This result is the proposition where $n = k + 1$. Therefore, the inductive step is true. Therefore, the power rule for derivatives is true for all $n \in \mathbb{N}$ where $n \geq 0$. □

Exercise 1.3.2: ☢☢ *n*th Derivative

Prove that the nth Derivative of $f(x) = \frac{1}{x}$ is

$$f^{(n)}(x) = \frac{(-1)^n n!}{x^{n+1}}.$$

Proof. Consider the base case $n = 0$. The zeroth derivative of $f(x)$ is $f(x)$ itself. Using the formula, we have

$$\begin{aligned} f^{(0)}(x) &= \frac{(-1)^0 0!}{x^{0+1}} \\ &= \frac{1}{x} \\ &= f(x). \end{aligned}$$

Therefore, the base case is true. We suppose that the relationship is true for $n = k$ where $k \in \mathbb{N}$. That is, we suppose that

$$f^{(k)}(x) = \frac{(-1)^k k!}{x^{k+1}}.$$

To find the $(k+1)$th derivative, we differentiate $f^{(k)}$, producing

$$\begin{aligned} f^{(k+1)}(x) &= \frac{\mathrm{d}}{\mathrm{d}x} \frac{(-1)^k k!}{x^{k+1}} \\ &= \frac{(-1)^k k!}{x^{k+1+1}}(-(k+1)) \\ &= \frac{(-1)^{(k+1)}(k+1)!}{x^{(k+1)+1}}. \end{aligned}$$

This result is the proposition where $n = k + 1$. Therefore, the inductive step is true. Therefore, the proposition is proved for all $n \in \mathbb{N}$ where $n \geq 0$. □

Exercise 1.3.3: ☢☢☢ Reduction

Prove that for all $n \in \mathbb{N}$, $n \geq 0$,

$$\int x^n e^{-x}\,\mathrm{d}x = -e^{-x}\left(x^n + nx^{n-1} + n(n-1)x^{n-2} + n(n-1)(n-2)x^{n-3} + \cdots + n!\right) + C.$$

Proof. Consider the base case $n = 0$. Then, the left hand side is equal to

$$\int e^{-x}\,\mathrm{d}x = -e^{-x} + C.$$

The right hand side is equal to $-e^{-x} + C$. Therefore, the left hand side is equal to the right hand side, proving the base case.

We assume that the relationship is true for $n = k$. That is, we assume that

$$\int x^k e^{-x}\,\mathrm{d}x = -e^{-x}(x^k + kx^{k-1} + k(k-1)x^{k-2} + k(k-1)(k-2)x^{k-3} + \cdots + k!) + C.$$

Let

$$u = e^{-x}(x^k + kx^{k-1} + k(k-1)x^{k-2} + k(k-1)(k-2)x^{k-3} + \cdots + k!).$$

Then,

$$\begin{aligned}
\int x^{k+1}e^{-x}\,\mathrm{d}x &= -x^{k+1}e^{-x} - \int -e^{-x}x^k(k+1)\,\mathrm{d}x \\
&= -x^{k+1}e^{-x} - (k+1)\int -x^k e^{-x}\,\mathrm{d}x \\
&= -x^{k+1}e^{-x} + (k+1)\int x^k e^{-x}\,\mathrm{d}x \\
&= -x^{k+1}e^{-x} - e^{-x}(k+1)\frac{u}{e^{-x}} + C \\
&= -e^{-x}\left(x^{k+1} + \frac{u(k+1)}{e^{-x}}\right) + C \\
&= -e^{-x}\left(x^{k+1} + (k+1)x^k + k(k+1)x^{k-1} + \cdots + (k+1)!\right) + C.
\end{aligned}$$

This result is the proposition where $n = k + 1$. Therefore, the inductive step is true. Therefore, the above formula is true for all $n \in \mathbb{N}$ where $n \geq 0$. □

Exercise 1.3.4: ☢☢☢ The Shoelace Lemma

The following is a statement of the Shoelace Lemma.

> Consider a simple polygon with vertices $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$, oriented clockwise. Let $(x_{n+1}, y_{n+1}) = (x_1, y_1)$. The area of the polygon is given by
>
> $$A_n = \frac{1}{2}\left[\sum_{i=1}^{n} x_i y_{i+1} - x_{i+1} y_i\right].$$

Prove the above proposition.

Proof. Consider a polygon with three vertices: (x_1, y_1), (x_2, y_2), and (x_3, y_3). The area, given by the Shoelace Lemma, is

$$A_3 = \frac{1}{2}\left[\sum_{i=1}^{3} x_i y_{i+1} - x_{i+1} y_i\right] = \frac{1}{2}\left[x_1 y_2 - x_2 y_1 + x_2 y_3 - x_3 y_2 + x_3 y_1 - y_3 x_1\right].$$

Then, if we define two vectors $(\vec{v}, \vec{w}) \in \mathbb{R}^3$ such that

$$\vec{v} = (x_2 - x_1, y_2 - y_1, 0), \quad \vec{w} = (x_3 - x_1, y_3 - y_1, 0),$$

we may see that the area of the parallelogram formed by the two vectors is given by

$$A_{||GRAM} = ||\vec{v} \times \vec{w}||$$

Either of the two triangles formed by the parallelogram's diagonals correspond to our polygon. The area is then given by

$$\begin{aligned} A_3 &= \frac{1}{2}||\vec{v} \times \vec{w}|| \\ &= \frac{1}{2}\,||(0, 0, x_1 y_2 - x_2 y_1 + x_2 y_3 - x_3 y_2 + x_3 y_1 - y_3 x_1)|| \\ &= \frac{1}{2}\left[x_1 y_2 - x_2 y_1 + x_2 y_3 - x_3 y_2 + x_3 y_1 - y_3 x_1\right]. \end{aligned}$$

Therefore, we have proved the Shoelace Lemma in the case of a polygon with three vertices. By induction, we suppose that for a polygon with k vertices $(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)$, the area is

$$A_k = \frac{1}{2}\left[\sum_{i=1}^{k} x_i y_{i+1} - x_{i+1} y_i\right].$$

The area of a polygon with vertices $(x_1, y_1), (x_2, y_2), \dots, (x_{k+1}, y_{k+1})$ is given by the sum of the area of the polygon with vertices $(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)$ and the area of the polygon with vertices (x_1, y_1), (x_k, y_k), and (x_{k+1}, y_{k+1}). That is,

$$\begin{aligned} A_{k+1} &= \frac{1}{2}\left[\sum_{i=1}^{k} x_i y_{i+1} - x_{i+1} y_i\right] + \frac{1}{2}\left[x_1 y_k - x_k y_1 + x_k y_{k+1} - x_{k+1} y_k + x_{k+1} y_1 - y_{k+1} x_1\right] \\ &= \frac{1}{2}\left[\sum_{i=1}^{k+1} x_i y_{i+1} - x_{i+1} y_i\right]. \end{aligned}$$

The above result is the consequence of the Shoelace Lemma in the case of a polygon with $k + 1$ vertices. Therefore, the Shoelace Lemma is proved. □

Exercise 1.3.5: ☢☢☢ Fibonacci

Let f_n represent the sequence of Fibonacci numbers, which is defined recursively as

$$f_0 = 1,\ f_1 = 1,\ f_n = f_{n-1} + f_{n-2}.$$

Prove that

$$\sum_{i=0}^{n} (f_i)^2 = f_n f_{n+1}.$$

Proof. Consider the base case $n = 0$. Then the left hand side is equal to 1, and the right hand side is

$$(1)f_1 = 1.$$

Therefore, the left hand side is equal to the right hand side, proving the first base case. Then, consider the base case $n = 1$. The left hand side is equal to 2, and the right hand side is $1 \cdot f_2$ where $f_2 = f_1 + f_0 = 2$. Therefore the right hand side is 2 and is equal to the left hand side proving the second base case.

We suppose that the relationship is true for $n = k$ where $k \in \mathbb{N}$. That is, we suppose that

$$\sum_{i=0}^{k} (f_i)^2 = f_k f_{k+1}.$$

If we add $(f_{k+1})^2$ to both sides, we have

$$\begin{aligned}(f_{k+1})^2 + \sum_{i=0}^{k} (f_i)^2 &= f_k f_{k+1} + (f_{k+1})^2 \\ &= f_{k+1}(f_k + f_{k+1}) \\ &= f_{k+1} f_{k+2}.\end{aligned}$$

This result is the proposition where $n = k + 1$. Therefore, the inductive step is true. Therefore, the above formula is true for all $n \in \mathbb{N}$ where $n \geq 0$. □

1.3.3 Direct Proofs

Direct Proofs are the simplest style of proofs, and are especially useful when proving implications. Consider the following examples.

Example 1.3.3: ☢☢ Direct Proof 1

Prove that for all integers n, if n is even, then n^2 is even.

Proof. Let $n \in \mathbb{Z}$ and suppose that n is even. Let $m \in \mathbb{Z}$. Thus, $n = 2m$. Then, $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$. Because $2m^2 \in \mathbb{Z}$, n^2 is even. □

Example 1.3.4: ☢☢ Direct Proof 2

Prove that for all integers a, b, and c, if $a|b$ and $b|c$, then $a|c$.

Proof. Let $(a, b, c, p, q, r) \in \mathbb{Z}$ and suppose that $a|b$ and$b|c$. Because $a|b$, $b = pa$. Because $b|c$, $c = qb = pqa$. Because c is an integer multiple of a, $a|c$. □

Consider the following exercises.

Exercise 1.3.6: ☢☢ Direct Proof 1

Prove that for any two odd integers, their sum is even.

Proof. Let $(m, n) \in \mathbb{Z} : m \bmod 2 \neq 0 : n \bmod 2 \neq 0$ and let $(p, q) \in \mathbb{Z}$. Because m and n are odd, $m = 2p + 1$ and $n = 2q + 1$. Therefore,

$$\begin{aligned} m + n &= (2p + 1) + (2q + 1) \\ &= 2p + 2q + 2 \\ &= 2(p + q + 1). \end{aligned}$$

Because $(p + q + 1) \in \mathbb{Z}$, $m + n$ is even. □

Exercise 1.3.7: ☢☢ Direct Proof 2

Prove that for all integers n, if n is odd, then n^2 is odd.

Proof. Let $n \in \mathbb{Z} : n \bmod 2 \neq 0$ and let $p \in \mathbb{Z}$. Because n is odd, $n = 2p + 1$. Therefore,

$$\begin{aligned} n^2 &= (2p + 1)^2 \\ &= 4p^2 + 4p + 1 \\ &= 2(2p^2 + 2p) + 1. \end{aligned}$$

Because $(2p^2 + 2p) \in \mathbb{Z}$, n^2 is odd. □

1.3.4 Proof by Contrapositive

Recall that for two statements P and Q, $(P \implies Q) \iff (\neg Q \implies \neg P)$. In a Proof by Contrapositive, we produce a direct proof of the contrapositive of the implication. This is equivalent to proving the implication, because the implication is logically equivalent to the contrapositive. Consider the following examples.

Example 1.3.5: ☢☢ Proof by Contrapositive 1

Prove that for all integers n, if n^2 is even, then n is even.

Proof. Let $n \in \mathbb{Z} : n \bmod 2 \neq 0$. By Exercise 1.3.7, n^2 is odd. □

Example 1.3.6: ☢☢ Proof by Contrapositive 2

Prove that for all integers a and b, if $a + b$ is odd, then a is odd or b is odd.

Proof. Let $(a, b, p, q) \in \mathbb{Z}$. Suppose that a is even and b is even. Then, $a = 2p$ and $b = 2q$. We see that

$$\begin{aligned} a + b &= 2p + 2q \\ &= 2(p + q). \end{aligned}$$

Because $(p + q) \in \mathbb{Z}$, $a + b$ is even. □

Consider the following exercises.

Exercise 1.3.8: ☢☢ Proof by Contrapositive 1

Prove that for real numbers a and b, if ab is irrational, then a or b must be an irrational number.

Proof. Let $(p, q, r, s) \in \mathbb{Z}$. Suppose that $(a, b) \in \mathbb{Q}$. Therefore, $a = \frac{p}{q}$ and $b = \frac{r}{s}$. We see that

$$ab = \frac{pr}{qs} \in \mathbb{Q}$$

Therefore ab is rational. □

Exercise 1.3.9: ☢☢ Proof by Contrapositive 2

Prove that for integers a and b, if ab is even, then a or b must be even.

Proof. Let $(a, b, p, q) \in \mathbb{Z}$. Suppose that $a = 2p + 1$ and $b = 2q + 1$. We see that

$$\begin{aligned} ab &= (2p + 1)(2q + 1) \\ &= 4pq + 2p + 2q + 1 \\ &= 2(2pq + p + q) + 1 \end{aligned}$$

Because $(2pq + p + q) \in \mathbb{Z}$, ab is odd. □

Exercise 1.3.10: ☢☢ Proof by Contrapositive 3

Prove that for any integer a, if a^2 is not divisible by 4, then a is odd.

Proof. Let $a, p \in \mathbb{Z}$. Suppose that a is even, and $a = 2p$. Then, $a^2 = 4p^2$, and $4|4p^2$, so $4|a^2$. □

1.3.5 Proof by Contradiction

Sometimes, a statement, P cannot be rephrased as an implication. In these cases, it may be useful to prove that $P \implies Q$, and also prove that $P \implies \neg Q$. Then, we conclude $\neg P$. One may scrutinize Exercise 1.2.2 for further explanation. Consider the following example.

Example 1.3.7: ☢☢ Proof by Contradiction 1

Prove that $\sqrt{2}$ is irrational.

Proof. Suppose that $\sqrt{2}$ is rational. Then,

$$\sqrt{2} = \frac{p}{q}$$

where $(p, q) \in \mathbb{Z}$ and $\frac{p}{q}$ is in lowest terms. By squaring both sides of the equation, we have

$$2 = \frac{p^2}{q^2}.$$

This means that

$$2q^2 = p^2,$$

and as $q^2 \in \mathbb{Z}$, p^2 is even, which means that by Example 1.3.5, p is even. We see that $p = 2k$ for some $k \in \mathbb{Z}$. Then, we have

$$2q^2 = (2k)^2 = 4k^2$$

meaning that

$$q^2 = 2k^2.$$

Therefore, q is even. If p and q are both even, $\frac{p}{q}$ is not in lowest terms. Therefore, $\sqrt{2}$ is irrational. □

A set is a many that allows itself to be thought of as a one.

Georg Cantor

2 Sets, Relations, and Functions

2.1 Lecture 5, June 14, 2022

2.1.1 An Introduction to Sets

We will first define a set.

Definition 2.1.1: Sets

A set is an unordered collection of distinct objects.

We use curly braces to enclose elements of sets. For example, $A = \{1, 2, 3\}$ means that A is a set containing the elements 1, 2, and 3. We also use $\in$ to mean "is an element of." For example, $1 \in A$. Similarly we use $\notin$ to mean "is not an element of." For example, $4 \notin A$.

Sometimes, simply listing the elements of a set is difficult. For example, let the set of all even natural numbers be B. The set B has infinitely many elements, so we may write

$$B = \{n \in \mathbb{N} : \exists k \in \mathbb{N}, n = 2k\}.$$

The above is read as "B is the set of natural numbers n, such that there exists a natural number k such that $n = 2k$. This notation is *set builder notation*.

We now define the following special sets.

Definition 2.1.2: Special Sets

The set $\emptyset$ is the set which contains no elements.

The set $\mathcal{U}$ is the set of all elements.

The set $\mathbb{N}$ is the set of all natural numbers.

The set $\mathbb{Z}$ is the set of all integers.

The set $\mathbb{Q}$ is the set of all rational numbers.

The set $\mathbb{R}$ is the set of all real numbers.

The set $\mathbb{C}$ is the set of all complex numbers.

The set $\mathcal{P}(A)$, the power set of A, is the set of all subsets of A.

We will also define the following notation.

Definition 2.1.3: Set Theory Notation

The statement $A \subseteq B$ asserts that A is a subset of B. That is, every element of A is also an element of B.

The statement $A \subset B$ asserts that A is a proper subset of B. That is, every element of A is also an element of B and $A \neq B$.

The operation $A \cap B$ is the intersection of A and B, or the set containing all elements that are elements of both A and B.

The operation $A \cup B$ is the union of A and B, or the set containing all elements that are elements of A or B or both.

The operation $A \times B$ is the Cartesian product of A and B, or the set of all ordered pairs (a, b), such that $a \in A$ and $b \in B$.

The operation $A \backslash B$ is the set difference between A and B, or the set containing all elements of A which are not elements of B.

The operation $\overline{A}$ is the complement of A, or the set of everything that is not an element of A.

The operation $|A|$ is the cardinality of A, or the number of elements in A.

Consider the following exercises.

Exercise 2.1.1: ☢☢ Set Statements

Let $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 6\}$, $C = \{1, 2, 3\}$, and $D = \{7, 8, 9\}$. Complete the table

Statement	Validity
$A \subset B$	F
$B \subset A$	T
$B \in C$	F
$\emptyset \in A$	F
$\emptyset \subset A$	T
$3 \in C$	T
$\{3\} \subset C$	T

Exercise 2.1.2: ☢☢ Power Sets

Let $A = \{1, 2, 3\}$. Find $\mathcal{P}(A)$.

The set $\mathcal{P}(A)$ is the set of all subsets of A. That is,

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$$

Note that $\{1, 2, 3\} \in \mathcal{P}(A)$, as $\mathcal{P}(A)$ includes non-proper subsets.

Consider the following theorem related to a set A and its power set $\mathcal{P}(A)$.

Theorem 2.1.1: 🛑 Cardinality of a Power Set

Given a set A, $|\mathcal{P}(A)| = 2^{|A|}$.

Consider the following exercise.

Exercise 2.1.3: ☢☢ Set Operations

Let $A = \{1, 2, 3, 4, 5, 6\}$, $B = \{2, 4, 6\}$, $C = \{1, 2, 3\}$, and $D = \{7, 8, 9\}$. Complete the table

Operation	Result
$A \cup B$	A
$B \cap A$	B
$B \cap C$	$\{2\}$
$A \cap D$	$\emptyset$
$\overline{B \cup C}$	$\{5, 7, 8, 9, 10\}$
$A \backslash B$	$\{1, 3, 5\}$
$(D \cap \overline{C}) \cup (\overline{A \cap B})$	$\{1, 3, 5, 7, 8, 9, 10\}$
$\emptyset \cup C$	C
$\emptyset \cap C$	$\emptyset$

We see that $\cup$ and $\cap$ behave similarly to $\vee$ and $\wedge$, respectively. We formally relate these operations in the following theorem.

Theorem 2.1.2: Unions are Disjunctions and Intersections are Conjunctions

Given two sets A and B,

$$x \in A \cup B \iff (x \in A) \vee (x \in B),$$

$$x \in A \cap B \iff (x \in A) \wedge (x \in B),$$

and

$$x \in \overline{A} \iff \neg(x \in A).$$

2.2 Lecture 6: June 16, 2022

2.2.1 Relations

Although we briefly covered Cartesian products in the previous section, here we state a more mathematical definition. If A and B are sets,

$$A \times B = \{(a, b) : a \in A \land b \in B\}.$$

We provide the following definition of a relation between two sets.

Definition 2.2.1: Relations

A relation between two sets A and B is a subset of their Cartesian product. If the relation is R,

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

If $(a, b) \in R$, with $a \in A \land b \in B$, we write $a \sim_R b$.

Often, we consider a special case of Definition 2.2.1.

Definition 2.2.2: A Special Relation

A relation R on a set A is a relation from A to itself. That is,

$$R \subseteq A \times A,$$

and for if $(a_1, a_2) \in R$, with $a_1 \in A \land a_2 \in A$, we write $a_1 \sim_R a_2$.

Consider the following example.

Example 2.2.1: Divisibility of the Natural Numbers

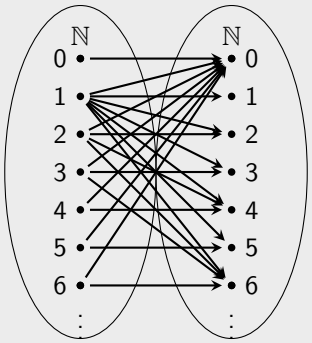
Let R represent divisibility, and let $A = \mathbb{N}$. For $(a, b) \in \mathbb{N}$,

$$a \sim_R b \iff \exists k \in \mathbb{N}, b = ka.$$

That is,

$$a|b \iff \exists k \in \mathbb{N}, b = ka.$$

Consider the following diagram.



We now consider various properties of relations. Consider the following.

- $R : A \to B$ is *reflexive* if and only if $\forall a \in A, a \sim_R a$
- $R : A \to B$ is *symmetric* if and only if $\forall (a, b) \in A, a \sim_R b \implies b \sim_R a$.
- $R : A \to B$ is *transitive* if and only if $\forall (a, b, c) \in A, (a \sim_R b \land b \sim_R c) \implies a \sim_R c$.
- $R : A \to B$ is *asymmetric* if and only if $\forall (a, b) \in A, a \sim_R b \implies b \nsim_R a$.
- $R : A \to B$ is *antisymmetric* if and only if $\forall (a, b) \in A, (a \sim_R b \land b \sim_R a) \implies a = b$.

Consider the following example.

Example 2.2.2: ☢☢ Properties of a Relation

Consider the relation $R : \mathbb{Z} \to \mathbb{Z}$ given by $a \sim_R b \iff a < b + 1$.

- R is reflexive, $\forall a \in \mathbb{Z}, a \sim_R a$.
- R is not symmetric, $\exists (a, b) \in \mathbb{Z}, a \sim_R b \land b \nsim_R a$.
- R is transitive, $\forall (a, b, c) \in \mathbb{Z}, (a \sim_R b \land b \sim_R c) \implies a \sim_R c$.
  - Note that if the same relation were on $\mathbb{R} \times \mathbb{R}$, it would not be transitive. Consider the counterexample $a = 1$, $b = \frac{1}{2}$, and $c = 0$.
- R is not asymmetric, $\exists (a, b) \in A, a \sim_R b \land b \sim_R a$.
- R is antisymmetric, $\forall (a, b) \in A, (a \sim_R b \land b \sim_R a) \implies a = b$.

We may use the properties of relations to define equivalence relations and equivalence classes. Consider the following definition.

Definition 2.2.3: Equivalence Relations

A relation R on a set A is an equivalence relation on A if and only if R is reflexive, symmetric, and transitive.

To see how frequently equivalence relations are used, define the set F to be

$$F = \left\{ \frac{m}{n} : (m, n) \in \mathbb{Z}, n \neq 0 \right\}.$$

Note that this set is not $\mathbb{Q}$, but instead, the set of all possible distinct fractions. For example, both $\frac{1}{2}$, and $\frac{2}{4}$ are elements of F.

Define a relation $\doteq$ on F, we say that $\frac{a}{b} \doteq \frac{c}{d}$ if $ad = bc$. We have defined the relation $\doteq$ such that $\frac{a}{b} \doteq \frac{c}{d}$ if and only if $\frac{a}{b}$ and $\frac{c}{d}$ are equal. We note that $\doteq$ is an equivalence relation.

Proof. For all $\frac{a}{b} \in F$, the equation $ab = ab$ means that $\frac{a}{b} \doteq \frac{a}{b}$. Therefore, $\doteq$ is reflexive.

For all $\left(\frac{a}{b}, \frac{c}{d}\right) \in F$, suppose that $\frac{a}{b} \doteq \frac{c}{d}$. This means that $ad = bc$, so $cb = da$. This implies that $\frac{c}{d} \doteq \frac{a}{b}$. Therefore, $\doteq$ is symmetric.

For all $\left(\frac{a}{b}, \frac{c}{d}, \frac{e}{f}\right)$, suppose that $\frac{a}{b} \doteq \frac{c}{d}$, meaning that $ad = bc$. Then, suppose that $\frac{c}{d} \doteq \frac{e}{f}$, meaning that $cf = de$. We wish to show that $\frac{a}{b} \doteq \frac{e}{f}$. That is, we wish to show that $af = be$. We multiply the first two equations, producing $adcf = bcde$. As we see that cd is on both sides, we see that $af = be$. Therefore, $\doteq$ is transitive. □

Any distinct rational number is contained in an equivalence class. For example, the equivalence class containing $\frac{2}{3}$ is the set $\left\{\frac{2n}{3n}\right\} : n \in \mathbb{Z}, n \neq 0$ of all fractions numerically equal to $\frac{2}{3}$.

Consider the following exercises.

Exercise 2.2.1: ☢☢ Properties of a Relation 1

Consider the relation $R : \mathbb{R}^2 \to \mathbb{R}^2$ given by $(x_1, y_1) \sim_R (x_2, y_2) \iff x_1^2 + y_1^2 = x_2^2 + y_2^2$.

- R is reflexive, $\forall (x_1, y_1) \in \mathbb{R}^2, (x_1, y_1) \sim_R (x_1, y_1)$.
- R is symmetric, $\forall ((x_1, y_1), (x_2, y_2)) \in \mathbb{R}^2, (x_1, y_1) \sim_R (x_2, y_2) \implies (x_2, y_2) \sim_R (x_1, y_1)$.
- R is transitive, $\forall ((x_1, y_1), (x_2, y_2), (x_3, y_3)) \in \mathbb{R}^2, ((x_1, y_1) \sim_R (x_2, y_2) \wedge (x_2, y_2) \sim_R (x_3, y_3)) \implies (x_1, y_1) \sim_R (x_3, y_3)$.
- R is not asymmetric, $\exists ((x_1, y_1), (x_2, y_2)) \in \mathbb{R}^2, (x_1, y_1) \sim_R (x_2, y_2) \wedge (x_2, y_2) \sim_R (x_1, y_1)$.
- R is not antisymmetric, $\exists ((x_1, y_1), (x_2, y_2)) \in \mathbb{R}^2, ((x_1, y_1) \sim_R (x_2, y_2) \wedge (x_2, y_2) \sim_R (x_1, y_1)) \wedge ((x_1, y_1) \neq (x_2, y_2))$.
- R is an equivalence relation.

Exercise 2.2.2: ☢☢ Properties of a Relation 2

Consider the relation $R : A \to A$, where A is the set of infinitely differentiable functions on $\mathbb{R}$, given by $f \sim_R g \iff f'(x) = g'(x)$.

- R is reflexive, $\forall f \in A, f \sim_R f$.
- R is symmetric, $\forall (f, g) \in A, f \sim_R g \implies g \sim_R f$.
- R is transitive, $\forall (f, g, h) \in A, (f \sim_R g \wedge g \sim_R h) \implies f \sim_R h$.
- R is not asymmetric, $\exists (f, g) \in A, f \sim_R g \wedge g \sim_R f$.
- R is not antisymmetric, $\exists (f, g) \in A, (f \sim_R g \wedge g \sim_R f) \wedge (f \neq g)$.
- R is an equivalence relation.

Exercise 2.2.3: ☢☢ Properties of a Relation 3

Consider the relation $R : A \to A$, where A is the set of all triangles in the plane. Triangle T_1 is related to Triangle T_2 if and only if $\triangle T_1$ has at least one side equal to a side of $\triangle T_2$.

- R is reflexive, $\forall T_1 \in A, T_1 \sim_R T_1$.
- R is symmetric, $\forall (T_1, T_2) \in A, T_1 \sim_R T_2 \implies T_2 \sim_R T_1$.
- R is not transitive, $\exists (T_1, T_2, T_3) \in A, (T_1 \sim_R T_2 \wedge T_2 \sim_R T_3) \wedge T_1 \nsim_R T_3$.
- R is not asymmetric, $\exists (T_1, T_2) \in A, T_1 \sim_R T_2 \wedge T_2 \sim_R T_1$.
- R is not antisymmetric, $\exists (T_1, T_2) \in A, (T_1 \sim_R T_2 \wedge T_2 \sim_R T_1) \wedge (T_1 \neq T_2)$.
- R is not an equivalence relation.

Exercise 2.2.4: ☢☢ Properties of a Relation 4

Consider the relation $R : A \to A$, where A is the set of all sets. Sets S_1 and S_2 are related if and only if $S_1 \subseteq S_2$.

- R is reflexive, $\forall S_1 \in A, S_1 \sim_R S_1$.
- R is not symmetric, $\exists (S_1, S_2) \in A, S_1 \sim_R S_2 \wedge S_2 \nsim_R S_1$.
- R is transitive, $\forall (S_1, S_2, S_3) \in A, (S_1 \sim_R S_2 \wedge S_2 \sim_R S_3) \implies S_1 \sim_R S_3$.
- R is not asymmetric, $\exists (S_1, S_2) \in A, S_1 \sim_R S_2 \wedge S_2 \sim_R S_1$.
- R is antisymmetric, $\forall (S_1, S_2) \in A, (S_1 \sim_R S_2 \wedge S_2 \sim_R S_1) \implies (S_1 = S_2)$.
- R is not an equivalence relation.

2.3 Lecture 7: June 21, 2022

2.3.1 Partitions

We begin by stating the following definitions.

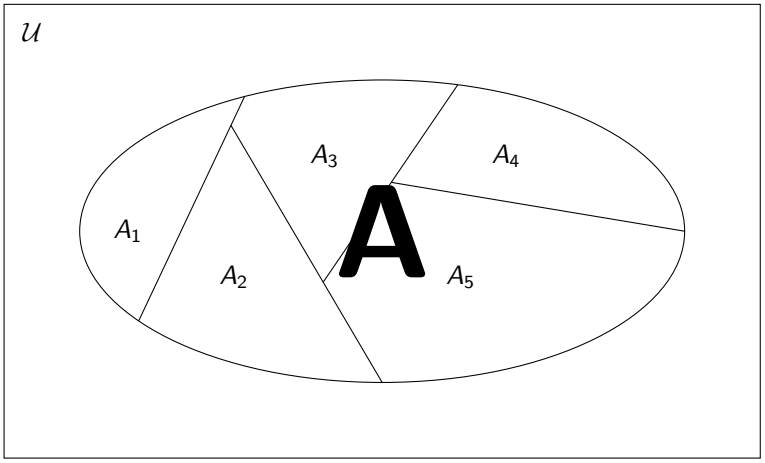
Definition 2.3.1: Partitions

A partition of a set A is a collection of subsets of A, A_1, A_2, ..., A_n such that

$$\underbrace{\left(A = \bigcup_{i=1}^{n} A_i\right)}_{A = A_1 \cup A_2 \cup \cdots \cup A_n} \wedge (A_i \cap A_j = \emptyset),$$

where $i \neq j$. That is, A is the union of the disjoint sets A, A_1, A_2, ..., A_n.

Consider the following example of a 5-part partition.



Consider the following example.

Example 2.3.1: A Partition of the Integers

Let $S = \mathbb{Z}$. Find a partition for S.

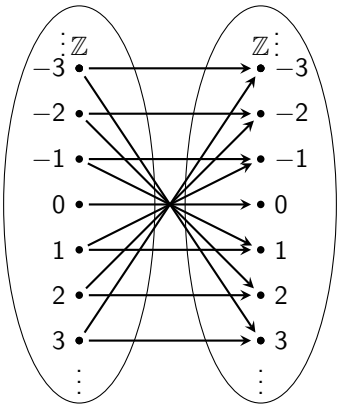
There are infinitely many answers, of which we provide one. Let

$$S_1 = \{a \in \mathbb{Z} : a > 0\}, \quad S_2 = \{0\}, \quad \{a \in \mathbb{Z} : a < 0\}.$$

Note that $\mathbb{Z} = S_1 \cup S_2 \cup S_3$ and $S_1 \cap S_2 = S_2 \cap S_3 = S_1 \cap S_3 = \emptyset$.

Consider the following diagram that corresponds with the equivalence relation $R : \mathbb{Z} \to \mathbb{Z}$, where for $(a, b) \in \mathbb{Z}$,

$$a \sim_R b \iff |a| = |b|.$$



Instead of tediously creating the above diagram, perhaps using TikZ, we may, instead, represent the relation as a partition of $\mathbb{Z}$, where all subsets are comprised of elements of $\mathbb{Z}$ related to each other. This idea brings us to our next definition.

Definition 2.3.2: Equivalence Classes

Suppose R is an equivalence relation on a set A. For any element $a \in A$, the equivalence class containing a is the subset $\{x \in A : x \sim_R a\}$ of A consisting of all the elements of A that relate to a. This set is denoted as $[a]$ or A_a. Therefore, the equivalence class containing a is the set

$$[a] = \{x \in A : x \sim_R a\}.$$

Therefore, the parts of the partition described earlier are the equivalence classes of the equivalence relation. Consider the following theorem.

Theorem 2.3.1: Equivalence Relations and Partitions

Every equivalence relation induces a partition, and every partition induces an equivalence relation, where two elements x and y are related if and only if x and y are found in the same part of the partition.

Consider the following example.

Example 2.3.2: ☢☢ Conmeasurable Numbers

Given the equivalence relation $R : \mathbb{R} - \{0\}$ defined by

$$a \sim_R b \iff \frac{a}{b} \in \mathbb{Q}$$

for $(a, b) \in \mathbb{R}$. The relation R is reflexive, as for all $a \in R$, $\frac{a}{a} = 1 \in \mathbb{Q}$. Similarly, R is symmetric, as

$$\frac{a}{b} \in \mathbb{Q} \implies \frac{b}{a} \in Q.$$

Finally, R is transitive, because

$$\frac{a}{b} \in \mathbb{Q} \land \frac{b}{c} \in \mathbb{Q} \implies \frac{a}{c} \in \mathbb{Q}$$

This is because $\frac{a}{b} \cdot \frac{b}{c} = \frac{a}{c}$. We may then build a partition on $\mathbb{R} - \{0\}$.

We will closely examine the equivalence classes for two elements of $\mathbb{R} - \{0\}$. We see that $[\pi] = \{k\pi : k \in \mathbb{Q}\}$ and $[1] = \mathbb{Q}$.

Consider the following examples.

Exercise 2.3.1: ☢☢ Equivalence Classes 1

Refer to the equivalence relation scrutinized in Exercise 2.2.1. Describe the equivalence classes.

After testing various points in a graphing utility, such as $(1, 0)$, $(1, 1)$, and $(1, 2)$, we come to the conclusion that the equivalence class containing the ordered pair (x, y) is the set of all points on the circle, centered at the origin, with radius $\sqrt{x^2 + y^2}$.

Exercise 2.3.2: ☢☢ Equivalence Classes 2

Refer to the equivalence relation scrutinized in Exercise 2.2.2. Describe the equivalence classes.

The equivalence class containing a function $f(x)$ will be

$$[f(x)] = \{f(x) + C\}, \quad C \in \mathbb{R}.$$

2.4 Lecture 8: June 23, 2022

2.4.1 Functions

Consider the following definition.

Definition 2.4.1: Functions

A relation $R : A \to B$ is a function if and only if

$$\forall a \in A, \exists! b \in B, a \sim_R b.$$

That is,

$$\forall a \in A, \exists b \in B, (a \sim_R b \wedge \forall c \in B, a \sim_R c) \implies b = c.$$

Consider the function $F : A \to B$. We call A the domain of F, and B is called the codomain. All elements of the codomain may not be used. Instead, we form a new construction, called the range. The range of F is

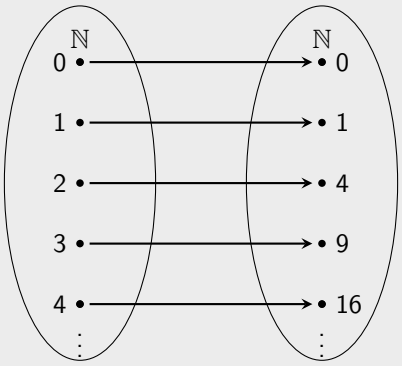
$$\text{range}\, F = \{b \in B : \exists a \in A, F(a) = b\}.$$

There are many notations to describe the way a function maps a given input to an output, one of which we just used. Consider the following example.

Example 2.4.1: Function Analysis

Define $R : \mathbb{N} \to \mathbb{N}$ where for $(a, b) \in \mathbb{N}$, $a \sim_R b \iff b = a^2$. Determine if R is a function. State the domain, codomain, and range of R.

Consider the following diagram.



We recognize that R is a function, as each output only has one input. Notice that if R were a relation on $\mathbb{Z}$, this would not be true. Furthermore, the domain and codomain of R is $\mathbb{N}$. The range of R is the set of all perfect squares.

There are three major classifications of functions. Consider the following definitions.

Definition 2.4.2: Injective Functions

Given a function $F : A \to B$, F is injective, or one-to-one, if and only if

$$\forall (a_1, a_2) \in A, a_1 \neq a_2 \implies F(a_1) \neq F(a_2).$$

That is, F is injective if and only if

$$\forall (a_1, a_2) \in A, F(a_1) = F(a_2) \implies a_1 = a_2.$$

Definition 2.4.3: Surjective Functions

Given a function $F : A \to B$, F is surjective, or onto, if and only if

$$\operatorname{range} F = B.$$

That is, F is surjective if and only if

$$\forall b \in B, \exists a \in A, F(a) = b.$$

Definition 2.4.4: Bijective Functions

Given a function $F : A \to B$, F is bijective, if and only if F is both injective and surjective. That is, F is bijective if and only if

$$(\forall (a_1, a_2) \in A, F(a_1) = F(a_2) \implies a_1 = a_2) \wedge (\forall b \in B, \exists a \in A, F(a) = b).$$

Consider the following example.

Example 2.4.2: The Arctangent: Part I

Consider $F : \mathbb{R}^2 \to \mathbb{R}^2$ given by $F(x) = \arctan x$. Determine if F is injective, surjective, or bijective.

- Injective: F is injective.
  - Suppose $\arctan(a_1) = \arctan(a_2)$. If we take the tangent of both sides, we see that $a_1 = a_2$.
  - Alternatively, if $a_1 \neq a_2$, we observe that $\arctan(a_1) \neq \arctan(a_2)$ because $\arctan x$ is monotonically increasing.
- Surjective: F is not surjective.
  - We see that $\operatorname{range} F = \left\{x : -\frac{\pi}{2} < x < \frac{\pi}{2}\right\}$.
- Bijective: F is not bijective.

Consider the following exercise.

Example 2.4.3: ☢☢ The Arctangent: Part II

Consider $F : \mathbb{R}^2 \to \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ given by $F(x) = \arctan x$. Determine if F is injective, surjective, or bijective.

- Injective: F is injective.
- Surjective: F is surjective.
- Bijective: F is bijective.

Consider the following definition.

Definition 2.4.5: Inverse Functions

Given a function $F : A \to B$, the inverse of F, $F^{-1} : B \to A$, is defined by

$$F^{-1}(b) = a \iff F(a) = b$$

for $a \in A$ and $b \in B$. The inverse of F, F^{-1}, is a function if and only if F is a bijection.

We will define an inverse relation in a similar manner to how we defined inverse functions in Definition 2.4.5.

Definition 2.4.6: Inverse Relations

If $R : A \to B$ is a relation, the inverse relation $R^{-1} : B \to A$ is defined by

$$R^{-1} = \{(b, a) : (a, b) \in R\}.$$

That is,

$$b \sim_{R^{-1}} a \iff a \sim_R b.$$

To alter a function to make it a bijection, we may restrict the domain to make it injective, and we may restrict the codomain to make it surjective.

Consider the following exercise.

Exercise 2.4.1: ☢☢ Compositions

Let A, B, and C be sets and $F : A \to B$ and $G : B \to C$ be functions.

- If F and G are both injective, is $G \circ F$ necessarily injective?
  - Yes. Each $b \in B$ "provided" to G will be different and therefore each $c \in C$ that G generates will be different.
- If F and G are both surjective, is $G \circ F$ necessarily surjective?
  - Yes. All $b \in B$ will be generated by F and therefore will be used by G to generate all $c \in C$.
- If F and G are both bijective, is $G \circ F$ necessarily bijective?
  - Yes. See the above justifications.

We now introduce a theorem explaining what it means for two sets to have the same size.

Theorem 2.4.1: Equal Cardinalities of Two Sets

For two sets A and B, $|A| = |B|$ if and only if there exists a bijection $F : A \to B$.

Theorem 2.4.1 allows us to both consider sets of both finite and infinite cardinality. We examine the latter case.

Example 2.4.4: ☢☢ Natural Numbers and Positive Natural Numbers

Prove that $|\mathbb{N}| = |\mathbb{N}^+|$.

Proof. Let $F : \mathbb{N} \to \mathbb{N}^+$ be defined by $F(n) = n + 1$. We see that F is a bijection between the two sets. □

Example 2.4.4 provides a very interesting result. For finite sets A and B,

$$A \subset B \implies |A| \neq |B|.$$

For infinite sets, the above equality is not necessarily true. Here, we will also define the notion of countable sets.

Definition 2.4.7: Countable Sets

An infinite set A is countable if and only if $|A| = |\mathbb{N}|$.

Consider the following exercise.

Exercise 2.4.2: ☢☢ Natural Numbers and Integers

Prove that $|\mathbb{N}| = |\mathbb{Z}|$.

Proof. We wish to essentially map half of the natural numbers to the positive integers and the other half to the negative integers. Here, we map the positive integers to the even natural numbers and the negative integers to the odd natural numbers. Let $F : \mathbb{Z} \to \mathbb{N}$ be defined by

$$F(n) = \begin{cases} 2n & n \geq 0 \\ -2n-1 & n < 0 \end{cases}.$$

We see that F is a bijection between te two sets. □

We will now provide a few nontrivial examples.

Example 2.4.5: ☢☢ Natural Numbers and Rational Numbers

Prove that $|\mathbb{N}| = |\mathbb{Q}|$.

Proof. We wish to write $\mathbb{Q}$ in bijection with $\mathbb{N}$. We will start at $(0, 0)$ and visit all points of $\mathbb{Z} \times \mathbb{Z}$ in an outward counterclockwise spiral. At each point (a, b), calculate the slope to the origin, namely $\frac{b}{a}$. If the slope is undefined or already used, discard it. Otherwise, fill in the following table accordingly.

$\mathbb{N}$	0	1	2	3	4	5	6	$\cdots$
$\mathbb{Q}$	0	1	-1	$-\frac{1}{2}$	$\frac{1}{2}$	2	-2	$\cdots$

This method will generate all rational numbers once and only once an is a bijective map from $\mathbb{N}$ to $\mathbb{Q}$. □

Example 2.4.6: ☢☢☢☢ Natural Numbers and Real Numbers

Prove that $|\mathbb{N}| \neq |\mathbb{R}|$.

Proof. To prove that there does not exist a bijection between $\mathbb{N}$ and $\mathbb{R}$, implying that $\mathbb{R}$ is uncountable, we must show that for all functions $F : \mathbb{N} \to \mathbb{R}$, F is not bijective. That is, for all F, F is not injective, or F is not surjective. We will show that all functions F are not surjective. We do so by Georg Cantor's Diagonal Argument.

Let $F : \mathbb{N} \to \mathbb{R}$ be a function given by the following table. We list the decimal expansions of all outputs, in order.

$\mathbb{N}$	$\mathbb{R}$	
n	$F(n)$	
0	$b_0.\boxed{a_{00}}a_{01}a_{02}a_{03}a_{04}a_{05}$	$\cdots$
1	$b_1.a_{10}\boxed{a_{11}}a_{12}a_{13}a_{14}a_{15}$	$\cdots$
2	$b_2.a_{20}a_{21}\boxed{a_{22}}a_{23}a_{24}a_{25}$	$\cdots$
3	$b_3.a_{30}a_{31}a_{32}\boxed{a_{33}}a_{34}a_{35}$	$\cdots$
4	$b_4.a_{40}a_{41}a_{42}a_{43}\boxed{a_{44}}a_{45}$	$\cdots$
5	$b_5.a_{50}a_{51}a_{52}a_{53}a_{54}\boxed{a_{55}}$	$\cdots$
$\vdots$	$\vdots$	$\ddots$

Here, b_n is the integer part of $F(n)$ and a_{ij} is the jth digit past the decimal in the number $f(i)$. We wish to show that there exists some real number m not in the range of F. We construct

$$m = 0.m_0m_1m_2m_3m_4m_5 \ldots$$

where

$$m_0 = \begin{cases} 4 & a_{00} \neq 4 \\ 7 & a_{00} = 4 \end{cases}, \quad m_1 = \begin{cases} 4 & a_{11} \neq 4 \\ 7 & a_{11} = 4 \end{cases}, \ldots, m_n = \begin{cases} 4 & a_{nn} \neq 4 \\ 7 & a_{nn} = 4 \end{cases}.$$

By this construction, m will differ from $F(n)$ in at least digit n past the decimal point. Therefore, $\forall n \in \mathbb{N}, m \neq F(n)$. Therefore m is not present in the range of $F(n)$ and $F(n)$ is therefore not surjective. Therefore, there does not exist a bijection between $\mathbb{N}$ and $\mathbb{R}$; therefore, $\mathbb{R}$ is uncountable. □

We will now pose Cantor's Continuum Hypothesis. That is, for set B,

$$\exists B, |\mathbb{N}| < |B| < |\mathbb{R}|?$$

The answer is undecidable.

Now, we pose two applications of Example 2.4.5 and the Continuum Hypothesis to computer science. It is impossible to represent all real numbers in binary; any particular string of zeroes and ones is countable. Also, the halting problem is another famous example of an undecidable problem.

2.5 Lecture 9: June 30, 2022

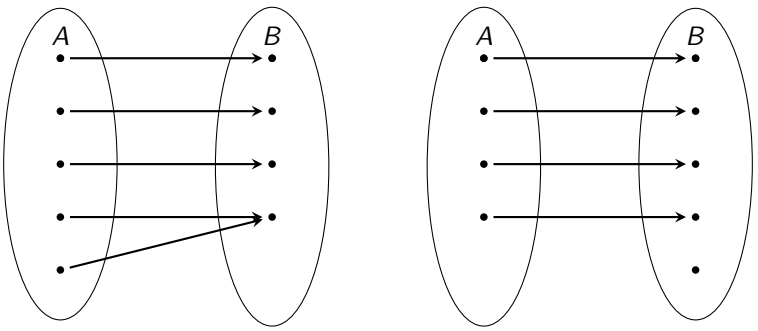
2.5.1 The Pigeonhole Principle

Consider the following theorem.

Theorem 2.5.1: The Pigeonhole Principle

Let $F : A \to B$ be a function with finite sets A and B. If $|A| > |B|$, F is not injective.

The above result gets its name from the conceptual problem of a function that maps pigeons to holes. If there are more pigeons than holes, there exists a hole with more than one pigeon. To visualize this, consider the following diagrams.



While the Pigeonhole Principle may seem trivial, it may be used to construct various proofs. Consider the following examples.

Example 2.5.1: Pairs of Integers

Prove that among any three distinct integers, there exists a pair whose difference is even.

Proof. Let $(p, q, r) \in \mathbb{Z}$. Let A be the set defined by

$$A = \{p, q, r\}.$$

We note that $|A| = 3$. Let B be the set defined by $\{\text{EVEN}, \text{ODD}\}$, with $|B| = 2$. Let $F : A \to B$ where $a \in A$.

$$F(a) = \begin{cases} \text{EVEN} & a \bmod 2 = 0 \\ \text{ODD} & a \bmod 2 \neq 0 \end{cases}.$$

As $|A| > |B|$, F is non-injective. Therefore, there must either exist two odd integers and an even integer, or two even integers and an odd integer. In the first case, the pair whose difference is even is the pair of integers that are odd. In the second case, the corresponding pair is the pair of numbers that are even. □

Example 2.5.2: ☢☢☢ 1978 Putnam

Prove that any 20 distinct integers chosen from the set $S = \{1, 4, 7, 10, \ldots, 100\}$ will contain a pair that sums to 104.

Before delving into the proof itself, we will proceed with some informal experimentation. Consider the following pairs S that sum to 104.

$$\begin{aligned} 104 &= \underbrace{4}_{1+1(3)} + 100 \\ &= \underbrace{7}_{1+2(3)} + 97 \\ &= \underbrace{10}_{1+3(3)} + 94 \\ &= \underbrace{13}_{1+4(3)} + 91 \\ &\vdots \\ &= \underbrace{49}_{1+16(3)} + 55. \end{aligned}$$

Note that there are 16 pairs of numbers that add to 104. Also, 1 and 52 are not able to be used in a pair that sums to 104. Therefore, any choice of 20 distinct integers from S will contain at least 18 distinct integers selected from $S - \{1, 52\}$. We are now ready to begin our proof.

Proof. Let A be 18 distinct integers chosen from $S - \{1, 52\}$. Let B be the set of pairs of integers that sum to 104. That is,

$$\begin{aligned} B &= \{\{4, 100\}, \{7, 97\}, \{10, 94\}, \ldots, \{49, 55\}\} \\ &= \{\{1 + 3n, 103 - 3n\} : n \in \{1, 2, 3, \ldots, 16\}\}. \end{aligned}$$

Note that $|A| = 18$ and $|B| = 16$. Let $F : A \to B$ be given by

$$F(a) = \{a, 104 - a\}.$$

for $a \in A$. The function F is non-injective by the Pigeonhole Principle, so there are two distinct elements of A that are mapped to the same element of B. These two elements are the pair that will sum to 104. □

There are three parts to every Pigeonhole argument.

1. Define A, the set of pigeons.
2. Define B, the set of pigeonholes, such that $A > B$.
3. Define $F : A \to B$, the method of assigning pigeons to pigeonholes.

We may then conclude that

$$\exists (a_1, a_2) \in A, a_1 \neq a_2 \wedge F(a_1) = F(a_2).$$

Consider the following exercises.

Exercise 2.5.1: ☢☢☢ Hairs

Prove that two people from the state of Colorado have the same number of hairs on their head.

Proof. The state of Colorado, at the time of writing, has roughly 5.8×10^6 people, and it is safe to assume that the number of human hairs is less than 5×10^5. Let A be the set of people in Colorado, with $|A| = 5.8 \times 10^6$ and let B be the set of all integers from 0 to 5×10^5, inclusive, noninclusive. We note that $|B| = 5 \times 10^5$. Let the function $F : A \to B$ be the function that maps a given person to the number of hairs on their head. We see that F is non-injective, therefore, at least two people from the state of Colorado must have the same number of hairs on their head. □

Exercise 2.5.2: ☢☢☢ Sphere

Prove that given 5 points on the surface of a sphere, there exists a hemisphere containing at least four of them. Any point on the boundary between the hemispheres is simultaneously in both hemispheres.

Proof. Pick two points, and cut the sphere in half such that the two points lie on the cut. Let A be the set of the three remaining points, and let B be the set of the two pieces of the sphere–the hemispheres. Let $F : A \to B$ map the points to their corresponding hemisphere. As $|A| = 3$ and $|B| = 2$, we see that F is non-injective, meaning that at least two remaining points will fall on the same hemisphere. These two points add to the two points that lie on the cut, giving four points in the hemisphere. □

The Extended Pigeonhole Principle is, well, an extended form of the Pigeonhole Principle. Consider the following statement.

Theorem 2.5.2: The Extended Pigeonhole Principle

If n "pigeons" land into k "pigeonholes," there exists at least one pigeonhole with at least $\lfloor \frac{n-1}{k} \rfloor = \lceil \frac{n}{k} \rceil$ pigeons.

We may use Theorem 2.5.2 to better quantify the "population" of the holes. Consider the following exercise.

Exercise 2.5.3: Equilateral Triangle

Prove that given 9 points in an equilateral triangle with unit sides, there exist 3 that define a triangle of area less than or equal to $\frac{\sqrt{3}}{8}$.

Proof. Let A be the set of the nine points in the triangle. Let B be the set of four equilateral triangles given by the first iteration of Sierpinski's Triangle. Let $F : A \to B$ map each point to the triangle that contains the point. There must exist a triangle containing $\lceil \frac{9}{4} \rceil = 3$ points. The four equilateral triangles have area $\frac{\sqrt{3}}{4 \cdot 2}$, and the triangle formed by the three points is therefore less than or equal to $\frac{\sqrt{3}}{4 \cdot 2}$. □

[This] is the city I chose to live in for 6 years of grad school lol Combintoropolis.

Kenneth M. Monks

3 Enumerative Combinatorics

3.1 Lecture 10: July 5, 2022

3.1.1 The Fundamental Principle of Counting

Consider the following theorem.

Theorem 3.1.1: The Fundamental Principle of Counting

If A and B are finite sets,

$$|A \times B| = |A| \cdot |B|.$$

Alternatively, if A and B are independent events, with A and B having m and n outcomes respectively, then A and B together have mn different outcomes. Independent events refer to the notion that A and B are not impacted by each other.

Consider the following examples.

Example 3.1.1: A Basic Example

If $A = \{1, 2, 3\}$ and $B = \{m, n\}$, consider the table

	m	n
1	$(1, m)$	$(1, n)$
2	$(2, m)$	$(2, n)$
3	$(2, m)$	$(2, n)$

representing $A \times B$. It is trivial to then conclude, $|A \times B| = 6$, which aligns with Theorem 3.1.1.

Example 3.1.2: ☢ Ken's Favorite Deli

Kenneth M. Monks is at a popular sandwich deli. Event A represents Ken picking a certain type of bread. Event B refers to Ken picking a certain meat. Ken's favorite deli has rye, white, and wheat bread, as well as turkey and ham. How many sandwich orders are possible?

Ken has the option to order 6 sandwiches. This example is essentially Example 3.1.1 in words.

Example 3.1.3: ☢☢ Four Digit Passcodes

How many four digit passcodes exist?

For each digit, A, B, C, and D, ten independent outcomes exist. Therefore, $10 \cdot 10 \cdot 10 \cdot 10 = 10^4$ passcodes exist.

3.1.2 Permutations

Consider the following theorem.

Theorem 3.1.2: Permutations

A permutation is an ordered list of k distinct objects chosen from n options. The number of permutations of k objects selected from n options is given by

$$ {}^nP_k = n(n-1)(n-2)\cdots(n-k+1) = \frac{n!}{(n-k)!}. $$

Permutations are used very often in "combination locks." Consider the following example.

Example 3.1.4: ☢☢ "Combination Locks"

Combination locks are actually permutation locks–the order of each number matters. How many ways can one choose 3 numbers, the standard for a "combination lock," from 40 options. Each number must be unique.

This problem asks us to compute ${}^{40}P_3$. By the formula in Theorem 3.1.2,

$$ {}^{40}P_3 = \frac{40!}{(40-3)!} = 59280. $$

Therefore, there are 59280 possible permutations of selecting 3 digits from 40 options.

We now revisit Example 3.1.3.

Example 3.1.5: ☢☢ Four Digit Passcodes Without Repeats

How many four digit passcodes exist where each digit must be distinct? If one were to randomly pick a four digit passcode x, what is the probability that $\underbrace{x \text{ has no repeated digits}}_{U(x)}$?

This problem asks us to compute ${}^{10}P_4 = 5040$. Therefore, there are 5040 passcodes. Note that this is actually less secure than the scenario given in Example 3.1.3. The probability that a random four digit passcode has no repeated digits is simply the ratio

$$P(U(x)) = \frac{{}^{10}P_4}{10^4} = 50.4\%.$$

3.1.3 Combinations

Consider the following theorem.

Theorem 3.1.3: 🛑 Combinations

A combination is an unordered list of k distinct objects chosen from n options. The number of combinations of k objects selected from n options is given by

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

Consider the following example.

Example 3.1.6: ☢☢ Comparisons

Consider both ways of selecting 3 letters from the first five letters $\{A, B, C, D, E\}$.

We first start with ${}^{5}P_3 = \frac{5!}{(5-3)!} = 60$. This means that when order is considered, there are 60 ways to select 3 objects from five.

We also see that ${}^{5}C_3 = \frac{5!}{3!(5-3)!} = 10$. This means that when order is not considered, there are 10 ways to select 3 objects from five.

There is a very important connection between combinations and binomials, the Binomial Theorem, which we state below.

Theorem 3.1.4: The Binomial Theorem

Binomials may be expanded by the identities

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n$$
$$(x-y)^n = \binom{n}{0}x^n - \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 - \cdots \pm \binom{n}{n-1}xy^{n-1} \mp \binom{n}{n}y^n,$$

or equivalently,

$$(x+y)^n = x^n + nx^{n-1}y + \frac{n(n-1)}{2!}x^{n-2}y^2 + \cdots + nxy^{n-1} + y^n$$
$$(x-y)^n = x^n - nx^{n-1}y + \frac{n(n-1)}{2!}x^{n-2}y^2 - \cdots \pm nxy^{n-1} \mp y^n.$$

As a Corollary to Theorem 3.1.4, the Binomial Series is often presented in Calculus II as

$$(1+x)^n = \sum_{k=0}^{\infty}\binom{n}{k}x^k.$$

This series converges when $|x| < 1$. The convergence of series at the endpoints, though, depend on the value of n. If $-1 < n \leq 0$, the series converges at 1, and if $n \geq 0$, the series converges at both endpoints.

3.2 Lecture 11: July 7, 2022

3.2.1 Multichoose

This technique is designed to answer the question

> How many different three-scoop blended milkshakes can be made at an ice cream shop that carries chocolate, vanilla, strawberry, and pistachio ice cream?

and its variants.

The answer is not given by ${}^4P_3$ or ${}^4C_3$ because to create milkshakes, the order in which the flavors are chosen does not matter, and multiple flavors can be chosen repeatedly. We may start listing out possible milkshakes with $n = 4$ options and $k = 3$ objects:

Scoop Combination	Equivalent Stars and Bars
CCC	$\star\star\star\vert\vert\vert$
CCP	$\star\star\vert\star\vert\vert$
CCS	$\star\star\vert\vert\star\vert$
CCV	$\star\star\vert\vert\vert\star$
CPP	$\star\vert\star\star\vert\vert$
CPS	$\star\vert\star\vert\star\vert$
CPV	$\star\vert\star\vert\vert\star$
CSS	$\star\vert\vert\star\star\vert$
CSV	$\star\vert\vert\star\vert\star$
CVV	$\star\vert\vert\vert\star\star$
$\vdots$	$\vdots$
VVV	$\vert\vert\vert\star\star\star$

To generalize this problem of selecting k objects from n options where order does not matter and repeats are allowed, we may use the "Stars and Bars," technique. A star represents a scoop of ice cream, and a bar changes the type of ice cream being scooped. Consider the above table for examples. Notice that there are $n + k - 1 = 6$ characters in each string in the second column. We wish to select $k = 3$ to be stars, so the rest are bars. How many ways can we do this? Well, the answer is ${}^6C_3 = 20$. This question is equivalent to our first question, as the method of assigning scoop combinations to strings of stars and bars is a bijection. Therefore, there are precisely 20 milkshakes that can be created! With this, we present the Multichoose Theorem.

Theorem 3.2.1: The Multichoose Theorem

The number of ways to select k objects from n options, where order does not matter and repeats are allowed, is given by

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

3.2.2 Selecting k Objects From n Options

In this section, we wish to provide a summary of selecting k objects from n options and provide some mixed practice. Consider the table

Selecting k Objects From n Options	Ordered	Unordered
Repeats Allowed	$\prod_{i=1}^{k} n = n^k$	$\binom{n+k-1}{k}$
Repeats Not Allowed	${}^nP_k$	${}^nC_k$

that represents the four possible options. Consider the following exercises.

Exercise 3.2.1: ☢☢ Lottery

What is the probability of winning the lottery by correctly bubbling in 5 numbers out of 50. The numbers are provided in ascending order on a lottery card.

Here, order does not matter, as in the end, all five numbers will be bubbled in. Also, repeats are not allowed, because a number may only be bubbled in once. Therefore, the answer is given by $\frac{1}{{}^{50}C_5} = \frac{1}{2118760}$.

Exercise 3.2.2: ☢☢ Burger-Eating Competition

Ken, Faith, and Rocco are going to a burger-eating competition. Between the three of them, they have to collectively eat 10 burgers. How many ways are there to do this?

Here, order does not matter, as each person may eat a burger at any time, just as long as ten burgers are eaten in the end. Also, repeats are allowed, because any one person may eat more than one burger. Therefore, we may apply the Multichoose Theorem, Theorem 3.2.1, to obtain $\binom{3+10-1}{10} = 66$.

3.3 Lecture 12, July 12, 2022

3.3.1 Permutations, With Some Repeats

This technique is designed to answer the question

> How many ways are there to rearrange the letters of the word "MISSISSIPPI?"

and its variants. Notice that "MISSISSIPPI" has 1 "M," 4 "I"s, 4 "S"s, and 2 "P"s. Not all letters are repeated, and the ones that are, are repeated a different number of times.

Before answering the above question, we consider a few simpler ones.

Example 3.3.1: ☢ Ways to Rearrange "FACE"

How may ways are there to rearrange the letters of the word "FACE?"

Here, order matters and repeats are not allowed. Therefore, the answer is given by ${}^4P_4 = 4! = 24$.

Example 3.3.2: ☢ Ways to Rearrange "CHEESE"

How may ways are there to rearrange the letters of the word "CHEESE"

Here, order matters, but we have some repeats, namely the three "E"s. For a moment, let's consider those three "E"s to be different. That is, let "$CHE_1E_2SE_3$" be a different string to "$CHE_3E_2SE_1$." Now, all the letters are different, so we may use the same technique shown in Example 3.3.1 to find the number of rearrangements. This number is ${}^6P_6 = 6! = 720$. Now, we must divide by the number of ways of rearranging the three "E"s. This is simply 3!, because there are three "E"s that can go into three positions. Therefore, there are $\frac{720}{3!} = 120$ ways of rearranging the letters in "CHEESE."

Finally, we will answer the original question.

Exercise 3.3.1: ☢☢ Ways to Rearrange "MISSISSIPPI"

How may ways are there to rearrange the letters of the word "MISSISSIPPI"

Here, order matters, but we have some repeats, namely the 4 "I"s, 4 "S"s, and 2 "P"s. If we consider these repetitions to be distinct, as we did in Example 3.3.2, we get ${}^{11}P_{11}$ rearrangements; however, we must divide by 4!, 4!, and 2! to account for the number of ways of rearranging the repetitions. Therefore, there are $\frac{{}^{11}P_{11}}{4!\cdot 4!\cdot 2!} = 34650$ ways of rearranging the letters in "MISSISSIPPI."

3.3.2 The Principle of Inclusion-Exclusion

The Principle of Inclusion-Exclusion is a result describing the cardinality of a union of n sets. For two sets, consider the following theorem.

Theorem 3.3.1: The Principle of Inclusion-Exclusion for 2 Sets

If A and B are finite sets,

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

This result is fairly intuitive. Consider a Venn Diagram of the two sets. Shade in A and B, and note that $A \cap B$ gets double counted. This is why $A \cap B$ is subtracted from $|A| + |B|$. Consider the following exercise.

Exercise 3.3.2: Divisibility

How many integers from 1 to 100, inclusive, are divisible by 2 or 3.

Let A be the set of all integers from 1 to 100, inclusive, that are divisible by 2 and note that $|A| = 50$. Let B be the set of all integers from 1 to 100, inclusive, that are divisible by 3 and note that $|B| = 33$. The set of all integers from 1 to 100, inclusive, that are divisible by both 2 and 3 is the set of all integers from 1 to 100, inclusive, that are divisible by 6. This third set has cardinality 16. Therefore, by the Principle of Inclusion-Exclusion, there are $50 + 33 - 16 = 67$ integers from 1 to 100, inclusive, that are divisible by 2 or 3.

For three sets, the Principle of Inclusion-Exclusion is provided below.

Theorem 3.3.2: The Principle of Inclusion-Exclusion for 3 Sets

If A, B, and C are finite sets,

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

3.4 Lecture 13: July 14, 2022

3.4.1 Combinatorial Proofs

We start with a visual exercise.

Exercise 3.4.1: ☢ Visual Analysis of Pascal's Triangle

Consider the first six rows of Pascal's Triangle, provided below.

$n=0$						1						
$n=1$					1		1					
$n=2$				1		2		1				
$n=3$			1		3		3		1			
$n=4$		1		4		6		4		1		
$n=5$	1		5		10		10		5		1	
$n=6$	1	6		15		20		15		6		1

Name, without proof, some patterns that are visible.

- Border entries are all 1.
- Non-border entries are the sum of the two entries above.
- The triangle is symmetric.
- The sum of all entries on any row is a power of 2.

Recall that each entry in Pascal's Triangle can be written as a binomial coefficient. The kth entry in the nth row, where both k and n are zero-indexed, is $\binom{n}{k}$. That is, the first six rows are

$n=0$						$\binom{0}{0}$						
$n=1$					$\binom{1}{0}$		$\binom{1}{1}$					
$n=2$				$\binom{2}{0}$		$\binom{2}{1}$		$\binom{2}{2}$				
$n=3$			$\binom{3}{0}$		$\binom{3}{1}$		$\binom{3}{2}$		$\binom{3}{3}$			
$n=4$		$\binom{4}{0}$		$\binom{4}{1}$		$\binom{4}{2}$		$\binom{4}{3}$		$\binom{4}{4}$		
$n=5$		$\binom{5}{0}$		$\binom{5}{1}$		$\binom{5}{2}$		$\binom{5}{3}$		$\binom{5}{4}$		$\binom{5}{5}$
$n=6$	$\binom{6}{0}$		$\binom{6}{1}$		$\binom{6}{2}$		$\binom{6}{3}$		$\binom{6}{4}$		$\binom{6}{5}$		$\binom{6}{6}$.

Consider the following exercise.

Exercise 3.4.2: ☢☢ Rewriting Hypotheses in Pascal's Triangle

Rewrite the patterns discovered in Exercise 3.4.1 in terms of binomial coefficients.

- $\binom{n}{0} = \binom{n}{n} = 1$.
- $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
- $\binom{n}{k} = \binom{n}{n-k}$.
- $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$.

The above identities were given without proof. To prove the identities, methods of either algebraic or combinatorial proof may be used. While algebraic proof certainly can show that an identity is true, it would not show *why*. Instead, combinatorial proof is based precisely on *why*. In general, combinatorial proofs for binomial identities are in the following format.

1. Find a counting problem that can be answered in two ways.
2. Explain why one answer to the counting problem is the left hand side of the identity.
3. Explain why one answer to the counting problem is the right hand side of the identity.
4. Conclude that the left hand side is equal to the right hand side because they are both answers to the same question.

Consider the following examples and exercises.

Example 3.4.1: ☢☢☢ Pascal Proof 1

Prove the binomial identity

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n.$$

Proof. Consider a set S with cardinality n. We note that $|\mathcal{P}(S)| = 2^n$, which is precisely the right hand side of the statement. We wish to show that the left hand side also produces the cardinality of $\mathcal{P}(S)$. The term $\binom{n}{0}$ corresponds to the fact that $\emptyset \in \mathcal{P}(S)$, and the term $\binom{n}{n}$ corresponds to the fact that $S \in \mathcal{P}(S)$. The quantities $\binom{n}{0}$ and $\binom{n}{n}$ together provide 2 sets in $\mathcal{P}(S)$. The terms $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$ correspond to the sets of cardinality $1, 2, \ldots, n-1$ in $\mathcal{P}(S)$. In $\mathcal{P}(S)$ there are $\binom{n}{1} = \frac{n!}{1!(n-1)!} = n$ sets of cardinality 1, $\binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2!}$ sets of cardinality 2, $\binom{n}{3} = \frac{n!}{3!(n-3)!} = \frac{n(n-1)(n-2)}{3!}$ sets of cardinality 3, etc. until we get to $\binom{n}{n-1} = \frac{n!}{(n-1)!(n-n+1)!} = n!$ sets of cardinality $n-1$. It is now clear that the left hand side also proves the cardinality of $\mathcal{P}(S)$. The left hand side sums the number of sets with cardinality $0, 1, \ldots, n$ in $\mathcal{P}(S)$. In contrast, the right hand side is the result of allowing each element of the set to "choose" to be in an n-length subset of S. □

3.4.2 Introduction to Probability

Before we present any information, we will first say that the definitions and theorems herein are simplified and abridged. In future classes, the statements will be revised. With that consider the following definitions and theorems.

Definition 3.4.1: Probability

The probability of an event with finitely many equally likely possible outcomes is the number of successful outcomes divided by the total number of possible outcomes. If event X has outcome n, write $X = n$. Then, the probability of outcome n is written $P(X = n)$.

Theorem 3.4.1: Sum of Probabilities

The sum of probabilities of event X with all outcomes is 1. That is,

$$\sum_{n=0}^{\infty} P(X = n) = 1.$$

Definition 3.4.2: Expected Value

The expected value of event X is

$$\sum_{n=0}^{\infty} nP(X = n).$$

Conceptually, the expected value is a weighted average of all possible outcomes. The expected value is not necessarily the most likely outcome.

Consider the following examples and exercises.

Example 3.4.2: Expected Value of Rolling a Die

What is the expected value of rolling one six-sided die?

We may use the equation provided in Definition 3.4.2. The expected value is then

$$1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 0 + \cdots = 3.5.$$

We may interpret this as "if the die is rolled ten times, the sum of the rolls would be approximately 35."

Example 3.4.3: ☢☢ A Full House 1

Recall that a full house, in five card poker, is when one has three cards of the one denomination and two cards of another denomination. For example "QQQ77" would be a full house. What is the probability of a full house?

We must first count the number of possible hands. A standard deck of cards has 52 cards, and we must select 5 to form a hand. Order does not matter and repeats are not allowed, so we have $\binom{52}{5}$ hands. To count the number of possible full houses, we must first pick the 2 denominations from a set of 13. Again, order does not matter and repeats are not allowed, so we have $\binom{13}{12}$. Out of those two denominations, we must pick one that has three cards and the other that has two card, giving us $\binom{2}{1}$. There are also four suits for the first denomination that has three cards and four suits for the second denomination that has two cards. This gives us $\binom{4}{3}$ and $\binom{4}{2}$. To find the probability, we evaluate

$$\frac{\binom{13}{12}\binom{2}{1}\binom{4}{3}\binom{4}{2}}{\binom{52}{5}} \approx 0.00144.$$

Example 3.4.4: ☢☢ A Full House 2

Consider a game where the player first pays \$10 to play and is then dealt 5 cards. If the player has a full house, they win \$5000. Otherwise, nothing happens. What is the expected value of the game?

$$\begin{aligned}\sum_{n=0}^{\infty} nP(X=n) &= (5000-10)P(\text{WIN}) + (-10)P(\text{LOSE}) \\ &= 4990\left(\frac{\binom{13}{12}\binom{2}{1}\binom{4}{3}\binom{4}{2}}{\binom{52}{5}}\right) - 10\left(1 - \frac{\binom{13}{12}\binom{2}{1}\binom{4}{3}\binom{4}{2}}{\binom{52}{5}}\right) \\ &= 2.8\end{aligned}$$

This means that if this game were to be set up in a casino, the casino would make approximately \$3 per player considering both wins and losses.

Exercise 3.4.3: ☢☢ A Four of a Kind

In five card poker, a four of a kind is a set of four cards of the same denomination with the remaining card being anything else. We first pick the 2 denominations from a set of 13. Order does not matter and repeats are not allowed, so we have $\binom{13}{2}$. From there, there are two more outcomes. Either there are four of the first card picked and one of the second card picked or there are four of the second card picked and one of the first card pick. Then, we must consider the suits. For the denomination that has four occurrences, there is nothing to pick. But, there are four possibilities for the remaining card. This means that there are $\binom{13}{2} \cdot 2 \cdot 4 = 624$ ways to form a four of a kind.

Exercise 3.4.4: ☢☢ A Two Pair

In five card poker, a two pair is two sets of two cards of the same denomination with the remaining card being anything else. The remaining card must be of a different denomination than the previous cards. We first pick the 3 denominations used in the hand, which gives $\binom{13}{3}$. Then, for each outcome, there are 3 ways for each denomination to go: the first set of two, the second set of two, and the lone card. We must also account for suits. For each set of two, we pick 2 suits from 4, and the lone card has four suits as possibilities. This means that there are $\binom{13}{3} \cdot 3 \cdot \binom{4}{2} \cdot \binom{4}{2} \cdot 4 = 123552$ ways to form a two pair.

Counting poker hands is simply one application of the tools we have discussed so far; however, it is very useful to demonstrate the concepts of probability and expected value.

A generating function is a clothesline on which we hang up a sequence of numbers for display.

Herbert Wilf

4

Generating Functions and Recurrence Relations

4.1 Lecture 14: July 19, 2022

4.1.1 Generating Functions and Recurrence Relations

Generating Functions are situated in another branch of combinatorics: algebraic combinatorics. Consider the following definition.

Definition 4.1.1: Generating Functions

Given a sequence of real numbers, a_n, the associated generating function is

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

Consider the following example.

Example 4.1.1: A Generating Function for a Constant Sequence

Find a generating function for $a_n = 1, 1, 1, \ldots$.

We find that

$$f(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

Consider the following exercise.

Exercise 4.1.1: ☢☢ A Generating Function With Zeroes

Find a generating function for $a_n = 1, 0, 1, 0 \ldots$.

We find that

$$f(x) = \sum_{n=0}^{\infty} x^{2n} = \frac{1}{1-x^2}.$$

We will now show a much more beautiful example.

Example 4.1.2: ☢☢ A Generating Function for the Fibonacci Sequence

Find a generating function for

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}.$$

We find that

$$f(x) = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \cdots .$$

To find a closed form, we multiply both sides by x and x^2, producing

$$xf(x) = x^2 + x^3 + 2x^4 + 3x^5 + 5x^6 + 8x^7 + \cdots$$

and

$$x^2 f(x) = x^3 + x^4 + 2x^5 + 3x^6 + 5x^7 + 8x^8 + \cdots$$

We see that $x^2 f(x) + xf(x) = f(x) - x$. Now, we simply solve for x, which provides

$$f(x) = -\frac{x}{x^2 + x - 1} = \frac{x}{1 - x - x^2}.$$

Generating functions can be used to solve recurrence relations, defined below.

Definition 4.1.2: Recurrence Relations

An equation, used in recursive definitions of sequences, that relates a term of a sequence a_n to previous terms.

To illustrate the utility of generating functions, we will use the result of Example 4.1.2 to build an explicit formula for the Fibonacci sequence F_n. The function

$$f(x) = \frac{x}{1 - x - x^2}$$

has asymptotes at $x = -\frac{1\pm\sqrt{5}}{2}$. We perform partial fraction decomposition, resulting in

$$x = A\left(1 - \frac{x}{-\frac{1-\sqrt{5}}{2}}\right) + B\left(1 - \frac{x}{-\frac{1+\sqrt{5}}{2}}\right).$$

Using normal techniques produces $A = -\frac{\sqrt{5}}{5}$ and $B = \frac{\sqrt{5}}{5}$. Therefore,

$$\begin{aligned}
f(x) &= \frac{-\sqrt{5}}{5\left(1 - \frac{x}{-\frac{1+\sqrt{5}}{2}}\right)} + \frac{\sqrt{5}}{5\left(1 - \frac{x}{-\frac{1-\sqrt{5}}{2}}\right)} \\
&= -\frac{\sqrt{5}}{5}\sum_{n=0}^{\infty}\left(\frac{x}{-\frac{1+\sqrt{5}}{2}}\right)^n + \frac{\sqrt{5}}{5}\sum_{n=0}^{\infty}\left(\frac{x}{-\frac{1-\sqrt{5}}{2}}\right)^n \\
&= \sum_{n=0}^{\infty}\left(-\frac{\sqrt{5}}{5}\left(-\frac{2}{1+\sqrt{5}}\right)^n x^n + \frac{\sqrt{5}}{5}\left(-\frac{2}{1-\sqrt{5}}\right)^n x^n\right) \\
&= \sum_{n=0}^{\infty}\underbrace{\left(-\frac{\sqrt{5}}{5}\left(-\frac{2}{1+\sqrt{5}}\right)^n + \frac{\sqrt{5}}{5}\left(-\frac{2}{1-\sqrt{5}}\right)^n\right)}_{F_n} x^n.
\end{aligned}$$

By algebraic simplification, we find

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

This is quite stunning, we have just found an explicit formula for the Fibonacci sequence! This formula has a special name and is known as Binet's Formula. Finding explicit formulas for recurrence relations is a key application of generating functions. We provide a few exercises on the next page.

For clarity, consider the following exercises.

Exercise 4.1.2: ☢☢☢ Finding an Explicit Formula 1

Find an explicit formula for $a_n = 1, 1, -1, -1, 1, 1, -1, -1, \ldots$.

The recurrence is $a_0 = a_1 = 1$ and $a_n = -a_{n-2}$. Here, we see a second depth recursion. The generating function is

$$f(x) = 1 + x - x^2 - x^3 + x^4 + x^5 + \cdots .$$

We will multiply both sides by x and x^2, producing

$$xf(x) = x + x^2 - x^3 - x^4 + x^5 + x^6 + \cdots$$

and

$$x^2 f(x) = x^2 + x^3 - x^4 - x^5 + x^6 + x^7 + \cdots .$$

We see that $x^2 f(x) = -(f(x) - x - 1)$ and $f(x) = \frac{1+x}{1+x^2}$. By partial fraction decomposition over the complex numbers, we have

$$1 + x = A(x + i) + B(x - i).$$

By standard techniques, we obtain

$$\begin{aligned}
\frac{1+x}{1+x^2} &= \frac{1-i}{-2i(x+i)} + \frac{1+i}{2i(x-i)} \\
&= \frac{1-i}{2}\frac{1}{1-ix} + \frac{1+i}{2}\frac{1}{1-(-ix)} \\
&= \frac{1-i}{2}\sum_{n=0}^{\infty}(ix)^n + \frac{1+i}{2}\sum_{n=0}^{\infty}(-ix)^n \\
&= \sum_{n=0}^{\infty}\left(\frac{1-i}{2}i^n + \frac{1+i}{2}(-i)^n\right)x^n
\end{aligned}$$

Therefore,

$$a_n = \frac{1-i}{2}i^n + \frac{1+i}{2}(-i)^n.$$

Exercise 4.1.3: ☢☢☢ Finding an Explicit Formula 2

Consider the recurrence relation

$$a_0 = 1, \quad a_1 = 5, \quad a_n = 3a_{n-1} - a_{n-2}.$$

Use a generating function to find an explicit formula for the sequence.

We list a few terms of a_n, producing

$$a_n = \{1, 5, 14, 37, 97, 254, 665, 1741, 4558, 11993, ...\}.$$

The corresponding generating function is

$$f(x) = 1 + 5x + 14x^2 + 37x^3 + 97x^4 + 254x^5 + \cdots .$$

We also see that

$$-3xf(x) = -3x - 15x^2 - 42x^3 - 111x^4 - 291x^5 - 762x^6 - \cdots$$

and

$$x^2 f(x) = x^2 + 5x^3 + 14x^4 + 37x^5 + 97x^6 + 254x^7 + \cdots .$$

That means that $f(x) - 3xf(x) + x^2 f(x) = 1 + 2x$. That is,

$$f(x) = \frac{1 + 2x}{1 - 3x + x^2}.$$

By partial fraction decomposition that was done on paper because doing LaTeX for that would be cumbersome, we have

$$\begin{aligned}
f(x) &= \frac{4+\sqrt{5}}{\sqrt{5}\left(x + \frac{-3-\sqrt{5}}{2}\right)} - \frac{4-\sqrt{5}}{\sqrt{5}\left(x + \frac{-3+\sqrt{5}}{2}\right)} \\
&= \frac{4+\sqrt{5}}{\sqrt{5}\frac{-3-\sqrt{5}}{2}\left(\frac{x}{\frac{-3-\sqrt{5}}{2}} + 1\right)} - \frac{4-\sqrt{5}}{\sqrt{5}\frac{-3+\sqrt{5}}{2}\left(\frac{x}{\frac{-3+\sqrt{5}}{2}} + 1\right)} \\
&= \frac{4+\sqrt{5}}{\frac{-3\sqrt{5}-5}{2}\left(1 + \frac{x}{\frac{-3-\sqrt{5}}{2}}\right)} - \frac{4-\sqrt{5}}{\frac{-3\sqrt{5}+5}{2}\left(1 + \frac{x}{\frac{-3+\sqrt{5}}{2}}\right)} \\
&= \frac{8+2\sqrt{5}}{-3\sqrt{5}-5}\sum_{n=0}^{\infty}(-1)^n\left(\frac{2x}{-3-\sqrt{5}}\right)^n - \frac{8-2\sqrt{5}}{-3\sqrt{5}+5}\sum_{n=0}^{\infty}(-1)^n\left(\frac{2x}{-3+\sqrt{5}}\right)^n \\
&= \sum_{n=0}^{\infty}\frac{8+2\sqrt{5}}{-3\sqrt{5}-5}\left(-\frac{2}{-3-\sqrt{5}}\right)^n x^n - \sum_{n=0}^{\infty}\frac{8-2\sqrt{5}}{-3\sqrt{5}+5}\left(-\frac{2}{-3+\sqrt{5}}\right)^n x^n \\
&= \sum_{n=0}^{\infty}\left(\frac{8+2\sqrt{5}}{-3\sqrt{5}-5}\left(-\frac{2}{-3-\sqrt{5}}\right)^n - \frac{8-2\sqrt{5}}{-3\sqrt{5}+5}\left(-\frac{2}{-3+\sqrt{5}}\right)^n\right)x^n.
\end{aligned}$$

We now have an explicit formula for the recurrence. We see that

$$a_n = \frac{8+2\sqrt{5}}{-3\sqrt{5}-5}\left(-\frac{2}{-3-\sqrt{5}}\right)^n - \frac{8-2\sqrt{5}}{-3\sqrt{5}+5}\left(-\frac{2}{-3+\sqrt{5}}\right)^n.$$

Why are numbers beautiful? It's like asking why is Beethoven's Ninth Symphony beautiful. If you don't see why, someone can't tell you. I know numbers are beautiful. If they aren't beautiful, nothing is.

Paul Erdös

5 Number Theory

5.1 Lecture 15: July 21, 2022

Natural numbers are used to solve problems in mathematics quite frequently; therefore, it is always beneficial to make discoveries about the natural numbers themselves. We now define number theory.

Definition 5.1.1: Number Theory

Number theory is the study of $\mathbb{N}$ and $\mathbb{Z}$ with, at first, a focus on divisibility, primality, and modular arithmetic.

A critical component of number theory is the divisibility relation, a concept first seen in Example 2.2.1. Here, we provide a more formal definition and a theorem.

Definition 5.1.2: Divisibility

Consider a relation $R : \mathbb{Z} \to \mathbb{Z}$ such that for $(a, b) \in \mathbb{Z}$,

$$a \sim_R b \iff \exists k \in \mathbb{Z}, b = ka.$$

Theorem 5.1.1: Divisibility & Primality

We provide the statement

$$\forall p \in \mathbb{Z}, 1|p \wedge p|p$$

without proof. If 1 and p are the only divisors of p, p is prime.

We now present the division algorithm.

Theorem 5.1.2: The Division Algorithm

We provide the statement

$$\forall (a, b) \in \mathbb{Z}, \exists q, a = qb + r$$

where $r \in \mathbb{Z}, 0 \leq r < |b|$, without proof.

Theorem 5.1.2 provides that there are only b possible remainders when dividing any integer by b. If we fix the divisor b, we may group integers by the remainder r. Each group is called a remainder class modulo b. Some sources refer to the same concept as a residue class. Consider the following example.

Example 5.1.1: Remainder Classes

Describe the remainder classes modulo 5.

We know that there are only 5 remainder classes, since $0 \leq r < 5$.

- If $r = 0$, we look for all integers divisible by 5. We get $\{\dots, -10, -5, 0, 5, 10, \dots\}$.
- If $r = 1$, we look for all integers, when divided by 5, have remainder 1. We get the set $\{\dots, -9, -4, 1, 6, 11, \dots\}$.
- If $r = 2$, we look for all integers, when divided by 5, have remainder 2. We get the set $\{\dots, -8, -3, 2, 7, 12, \dots\}$.
- If $r = 3$, we look for all integers, when divided by 5, have remainder 3. We get the set $\{\dots, -7, -2, 3, 8, 13, \dots\}$.
- If $r = 4$, we look for all integers, when divided by 5, have remainder 4. We get the set $\{\dots, -6, -1, 4, 9, 14, \dots\}$.

These remainder classes are actually equivalence classes for the following equivalence relation.

Definition 5.1.3: Congruence

Consider a relation $R : \mathbb{Z} \to \mathbb{Z}$ such that for $(a, b) \in \mathbb{Z}$,

$$a \equiv b \pmod{n}$$

if and only if a and b are seen in the same remainder class modulo n. That is, a and b have the same remainder when divided by n.

In the construction of Definition 5.1.3, we used Theorem 2.3.1. Consider the following exercise.

Exercise 5.1.1: ☢☢ Defining Congruence

Many sources define congruence in a different manner. Prove that the definition provided in Definition 5.1.3 is equivalent to the following alternate definition of congruence:

$$a \equiv b \pmod{n} \iff n|a-b.$$

Proof. Definition 5.1.3 essentially means for integers a and b,

$$a = q_1 n + r, \quad b = q_2 n + r.$$

When we subtract b from a, we obtain

$$a - b = q_1 n + r - q_2 n - r = n(q_1 - q_2).$$

This means that $n|a-b$. We have proved $a \equiv b \pmod{n} \implies n|a-b$. Now, we wish to show that $n|a-b \implies a \equiv b \pmod{n}$. We recognize that

$$a - b = kn$$

for some integer k. If we divide both sides by n, the right hand side will have zero remainder. On the left hand side, a will have some remainder, and b will have some remainder. But because the right hand side has zero remainder, the remainders of a and b must be the same. Therefore,

$$(a \equiv b \pmod{n} \implies n|a-b) \wedge (n|a-b \implies a \equiv b \pmod{n})$$

which means

$$a \equiv b \pmod{n} \iff n|a-b.$$

That is, both definitions are equal. □

If Exercise 5.1.1, we used the equation $a - b = kn$. This, when rewritten as $a = b + kn$, provides us a helpful tool to convert between congruences and regular equations and vice versa. We will now provide a theorem about arithmetic with congruences.

Theorem 5.1.3: Congruence and Arithmetic

Suppose $(a \equiv b \pmod{n}) \wedge (c \equiv \pmod{n})$. Then,

- $a + c \equiv b + d \pmod{n}$.
- $a - c \equiv b - d \pmod{n}$.
- $ac \equiv bc \pmod{n}$.

This allows us to, essentially, replace every number in a congruence with any other number it is congruent to. Consider the following exercises.

Exercise 5.1.2: ☢☢ Find the Remainder 1

Find the remainder of 3491 divided by 9.

This is equivalent to solving

$$\begin{aligned} x &\equiv 3491 \pmod 9 \\ &\equiv 3000 + 400 + 90 + 1 \pmod 9. \end{aligned}$$

We know that $90 \equiv 0 \pmod 9$, so we may replace 90 with 0. We also know that $400 = 4(100)$ and $100 \equiv 1 \pmod 9$. This means we can replace 400 with $4(1) = 4$. Similarly, we can replace 3000 with $3(1) = 3$ because $3000 = 3(1000)$ and $1000 \equiv 1 \pmod 9$. That means

$$\begin{aligned} x &\equiv 3 + 4 + 0 + 1 \pmod 9 \\ &\equiv 8 \pmod 9. \end{aligned}$$

That is, the remainder of 3491 divided by 9 is 8.

Exercise 5.1.3: ☢☢ Find the Remainder 2

Find the remainder of 3^{123} divided by 7.

This is equivalent to solving

$$\begin{aligned} x &\equiv 3^{123} \pmod 7 \\ &\equiv (3^3)^{41} \\ &\equiv 27^{41}. \end{aligned}$$

We know that $27 \equiv 6 \pmod 7$, so

$$x \equiv 6^{41} \pmod 7.$$

We also know $6^2 = 36$ is congruent to 1 modulo 7, so

$$\begin{aligned} x &\equiv 6(6^2)^{20} \pmod 7 \\ &\equiv 6(1^{20}) \pmod 7. \end{aligned}$$

Therefore,

$$x \equiv 6 \pmod 7.$$

That is, the remainder of 3^{123} divided by 7 is 6.

We now note that even if $ad \equiv bd \pmod{n}$, we cannot conclude that $a \equiv b \pmod{n}$. For example, while $18 \equiv 42 \pmod{8}$, $3 \not\equiv 7 \pmod{8}$. Instead, we present the following theorem.

Theorem 5.1.4: Congruence and Division

Suppose $ad \equiv bd \pmod{n}$. Then,

$$a \equiv b \pmod{n(\gcd(d, n))^{-1}}$$

We will now take a break from the language of congruences and turn to solving linear Diophantine equations, defined below.

Definition 5.1.4: Diophantine Equations

An equation in two or more variables is called a Diophantine equation if only integer solutions are of interest. A linear Diophantine equation takes the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

for constants $a_1, \ldots, a_n, b$. A solution to a Diophantine equation is a solution to the equation consisting only of integers.

To solve linear Diophantine equations, we will use the Euclidean Algorithm, Bezout's Identity, and the Extended Euclidean Algorithm, shown below.

Theorem 5.1.5: The Euclidean Algorithm

For two integers, a and b where $a \geq b$, the Euclidean Algorithm can be stated as

$$\gcd(a, b) = \begin{cases} a & b = 0 \\ \gcd(b, a \bmod b) & b \neq 0. \end{cases}$$

It may be difficult to understand the Euclidean Algorithm, but often, writing an implementation assists. Consider the following exercise.

Exercise 5.1.4: ☢☢ Euclidean in Python

Write a function to implement the Euclidean Algorithm in Python.

```
1 def gcd(a, b):
2
3   if b == 0: return a
4   return gcd(b, a % b)
```

We will now provide a few computational exercises.

Exercise 5.1.5: ☢☢ Computational Euclidean 1

Find $\gcd(254, 32)$.

By the Euclidean Algorithm,

$$\begin{aligned}\gcd(254, 32) &= \gcd(32, 30)\\ &= \gcd(30, 2)\\ &= \gcd(2, 0)\\ &= 2.\end{aligned}$$

We may also write this as

n	a_n	q_n	b_n	r_n
0	254	7	32	30
1	32	1	30	2
2	30	15	2	0

.

Exercise 5.1.6: ☢☢ Computational Euclidean 2

Find $\gcd(254, 32)$.

By the Euclidean Algorithm,

$$\begin{aligned}\gcd(74, 383) &= \gcd(383, 74)\\ &= \gcd(74, 13)\\ &= \gcd(13, 9)\\ &= \gcd(9, 4)\\ &= \gcd(4, 1)\\ &= \gcd(1, 0)\\ &= 1.\end{aligned}$$

We may also write this as

n	a_n	q_n	b_n	r_n
0	383	5	74	13
1	74	5	13	9
2	13	1	9	4
3	9	2	4	1
4	4	4	1	0

.

Exercise 5.1.7: ☢☢ Computational Euclidean 3

Find $\gcd(7544, 115)$.

By the Euclidean Algorithm,

$$\begin{aligned}\gcd(7544, 115) &= \gcd(115, 69)\\ &= \gcd(69, 46)\\ &= \gcd(46, 23)\\ &= \gcd(23, 0)\\ &= 23.\end{aligned}$$

We may also write this as

n	a_n	q_n	b_n	r_n
0	7544	65	115	69
1	115	1	69	46
2	69	1	46	23
3	46	2	23	0

.

Exercise 5.1.8: ☢☢ Computational Euclidean 4

Find $\gcd(687, 24)$.

By the Euclidean Algorithm,

$$\begin{aligned}\gcd(687, 24) &= \gcd(24, 15)\\ &= \gcd(15, 9)\\ &= \gcd(9, 6)\\ &= \gcd(6, 3)\\ &= \gcd(3, 0)\\ &= 3.\end{aligned}$$

We may also write this as

n	a_n	q_n	b_n	r_n
0	687	28	24	15
1	24	1	15	9
2	15	1	9	6
3	9	1	6	3
4	6	2	3	0

.

Now that we have some experience using the Euclidean Algorithm, we present Bézout's Lemma and the Extended Euclidean Algorithm.

Theorem 5.1.6: Bézout's Lemma

Let a and b be integers or polynomial such that $\gcd(a, b) = d$. Then, there exist integers x and y such that

$$ax + by = d.$$

Theorem 5.1.7: The Extended Euclidean Algorithm

The integers x and y given in Theorem 5.1.6 may be found by solving

$$a_{n-1} = q_{n-1}b_{n-1} + r_{n-1}$$

for r_n, then making substitutions to form a linear combination of a and b.

To apply Theorem 5.1.7, it will be much easier to use the tabular approach shown in Exercises 5.1.5, 5.1.6, 5.1.7, and 5.1.8. Consider the following exercises.

Exercise 5.1.9: ☢☢ Computational Extended Euclidean 1

Find an integer solution to

$$81x + 14y = 1.$$

We start by using the Euclidean Algorithm to obtain the table

n	a_n	q_n	b_n	r_n
0	81	5	14	11
1	14	1	11	3
2	11	3	3	2
3	3	1	2	1
4	2	2	1	0

.

Then, we solve for r_{n-1} and traverse the table upwards, producing

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (11 - 3 \cdot 3) \\
&= 3 - 11 + 3 \cdot 3 \\
&= 4 \cdot 3 - 11 \\
&= 4 \cdot (14 - 11) - (81 - 5 \cdot 14) \\
&= 4 \cdot (14 - (81 - 5 \cdot 14)) - (81 - 5 \cdot 14) \\
&= 4 \cdot (-81 - 9 \cdot 14) - 81 + 5 \cdot 14 \\
&= -4 \cdot 81 - 36 \cdot 14 - 81 + 5 \cdot 14 \\
&= -5 \cdot 81 - 29 \cdot 14.
\end{aligned}$$

Therefore, $x = -5$ and $y = 29$.

Exercise 5.1.10: ☢☢ Computational Extended Euclidean 2

Find an integer solution to

$$1398x + 324y = 6.$$

We start by using the Euclidean Algorithm to obtain the table

n	a_n	q_n	b_n	r_n
0	1398	4	324	102
1	324	3	102	18
2	102	5	18	12
3	18	1	12	6
4	12	2	6	0

.

Then, we solve for r_{n-1} and traverse the table upwards, producing

$$\begin{aligned}
6 &= 18 - 12 \\
&= 18 - 102 + 5 \cdot 18 \\
&= 324 - 3 \cdot 102 - 102 + 5(324 - 3 \cdot 102) \\
&= 324 - 4 \cdot 102 + 5 \cdot 324 - 15 \cdot 102 \\
&= 6 \cdot 324 - 19 \cdot 102 \\
&= 6 \cdot 324 - 19(1398 - 4 \cdot 324) \\
&= 6 \cdot 324 - 19 \cdot 1398 + 76 \cdot 324 \\
&= 82 \cdot 324 - 19 \cdot 1398.
\end{aligned}$$

Therefore, $x = -19$ and $y = 82$.

Exercise 5.1.11: ☢☢ Computational Extended Euclidean 3

Find an integer solution to

$$1398x + 324y = 60.$$

We first solve

$$1398x + 324y = 6,$$

which, coincidentally, was the result of Exercise 5.1.10. We see that for this equation, $x = -19$ and $y = 82$. That is,

$$6 = -19 \cdot 1398 + 82 \cdot 324.$$

We multiply both sides by 10 to produce

$$60 = -190 \cdot 1398 + 820 \cdot 324.$$

Therefore, the solution to the original equation is $x = -190$ and $y = 820$.

Exercise 5.1.12: ☢☢ Computational Extended Euclidean 4

Find an integer solution to

$$6x + 10y = 32$$

We start by using the Euclidean Algorithm to obtain the table

n	a_n	q_n	b_n	r_n
0	10	1	6	4
1	6	1	4	2
2	4	2	2	0

.

Then, we solve for r_{n-1} and traverse the table upwards, producing

$$\begin{aligned} 2 &= 6 - 4 \\ &= 6 - 10 + 6 \\ &= 2 \cdot 6 - 10. \end{aligned}$$

We now multiply both sides by 16 to see that

$$32 = 32 \cdot 6 - 16 \cdot 10.$$

Therefore, $x = 32$ and $y = -16$.