Writing Mathematical Proofs

"I don't draw a tombstone until I know I'm right."

Dr. Justin Wright
Mathematics Department, Plymouth State University

Licensing

This text is meant as a companion work to Dr. Richard Hammack's *Book of Proof* and has been produced with permission. *Book of Proof* is available for free download at the author's website: `http://www.people.vcu.edu/~rhammack/BookOfProof/`.

To the Reader

Why this text?
I never had an introductory proof writing course as an undergraduate student. Through a stroke of luck (the jury's still out on good or bad), a Discrete Mathematics course transferred and earned me credit for the requirement despite it not really covering proofs. As a result, I had to learn to write proofs the hard way. I read a lot of proofs in my textbooks and emulated my instructors when I could. I think I was a little more willing to dive in and *try* to write proofs than some of classmates, I was a little more willing to be wrong, and I spent more time trying to make sure my proofs were right on my own.

I don't exactly recommend this path to anyone. Even into my graduate school years I was haunted my lack of some fundamental skills. Simply put, I developed the general technique of proof writing and critical thinking, but I was unaware of many common conventions and approaches. For instance, many students learn that proving sets A and B are equal is most often done by showing that $A \subseteq B$ and $B \subseteq A$. While I probably wrote many proofs as an undergraduate that boiled down to this technique, it wasn't until my graduate years that I learned it as an approach that could almost always get me to where I wanted to go.

With this text I've tried to deliver what worked in my favor while eliminating the troubles I was faced with. This inquiry based approach forces students to think of proof writing as something other than a formulaic process. At the same time, I've provided more structure and instruction than I've seen in other inquiry based approaches to proof writing so that students still get the exposure to common proof writing conventions. This approach is admittedly slower and more painstaking, but most of my own students come out of the experience with the skills and confidence they need to write proofs on their own.

To instructors:
This workbook was developed over a period of several years. It began as class notes to go along with Dr. Richard Hammack's *Book of Proof*, but I realized early that students retained the class material the most when they were asked to work with it rather than just recording notes. Over time activities were added and refined based on student learning and feedback. It's reached a level at which it can probably serve as a solo text, but it is still intended as a companion to *Book of Proof*. If you choose to adopt this work, please let me know and I'll pass your message along to Dr. Hammack as well.

In the past these materials were distributed to students in class, but this, invariably, led to problems. Students often lost their old materials, it was difficult to get materials to students that had been absent, and it was difficult to move forward if the class finished something early. Having the students purchase a printed version of this text or print it themselves eliminates this problem, although it does unfortunately transfer a small cost to the students.

At Plymouth State University we split the traditional introductory proof writing course into two 3-credit courses. The first focuses on sets, logic, and relations and the second focuses entirely on proof writing. Together the two courses place an enormous emphasis on cohort building, presentations, writing, and student self-assessment. We use Richard Hammack's *Book of Proof* during both semesters and only use this text during the second course. We generally cover a chapter per day during the course with roughly one third of class meetings devoted entirely to presentations. There are definitely chapters like 1 through 3 that can be combined into a single day. Keep in mind that students are expected to generate 100% of the work on their own, so even shorter chapters can take one or two class periods.

If you adopt this text, some adaptation is recommended. I've often referred to myself and colleagues in this work and the name of the course. I've tried to use LaTeXcommands to do so to make overall changes easier. You might also want to expand chapters 1 through 3 as they are really only used as a review in our course. You also may need to add some material to adjust the difficulty level. Students take our introductory proof writing course in their first year, so mention of topics from higher level calculus, linear algebra, and geometries is mostly omitted.

Chapters 4 through 14 cover the fundamental material for proof writing. Individual chapters may be able to stand on their own, but I wouldn't recommend it without making changes. Chapters 15 through 19 are all related, so it would be hard to skip around in these chapters. Otherwise, Chapters 15 through 19 could be potentially be left out all together.

A penultimate version of this text will include homework exercises and appendices with former student work to be corrected by students taking the course. Many of the homework exercises I use come from *Book of Proof* with some additional original claims to be proven. If you choose to make additions as you adapt this work, you're encouraged to share them with others and me. I also welcome any feedback you may have and would appreciate you letting me know about any errors.

To students:
This is not a textbook. Textbooks give you a lot of information and examples and then have a few exercises for you to try. Textbooks are great and there are plenty of textbooks out there that cover all the material you need to know to learn to write proofs. Unfortunately, students often fool themselves into thinking that they understand a concept because they understood what they read in a textbook. This is a workbook. There is information given to you and there are even a few examples, but this work is made up of the exercises you need to be able to write proofs on your own.

These materials are meant to be used in class. For that reason, you will have to bring this work with you to every class. It's not recommended that you try to work ahead as this will damage the integrity of the in-class activities. Many students forget to actually read what is presented in this work, leaving themselves baffled as to how to proceed. Mathematics seems to workout best when we proceed slowly, so don't be in a rush to get to questions and write something

down. Working through this workbook doesn't end when class ends. It's important that you take time on your own to carefully rewrite proofs from class and do your best to find errors in your work.

Young mathematicians tend to be blindsided by their introductory proof writing class. I've had many students tell me they went into mathematics because they weren't creative and didn't like writing. Then after 12 years on elementary and high school mathematics they're hit out of nowhere with a writing course. You have every right to be surprised by this sudden demand for explanation, and you should be prepared to find learning to write proofs to be a frustrating and confusing process. My advice to you is to be patient, deliberate, and careful as you move forward in learning to write proofs. It's important to understand that you won't understand everything right away and that you'll often think you know what you're doing when you don't. Always try to keep in the back of your mind that no one makes as many mathematical mistakes as a mathematician. Why should a math student be any different? Learn from your mistake and persevere.

Dr. Justin Wright
Assistant Professor of Mathematics
Plymouth State University
jpwright1@plymouth.edu

Contents

Chapter 1

Logic and Statements Review

Recall that a **statement** is a sentence that is definitely true or definitely false. We can combine statements to make more complicated statements using the logical connectives "and," "or," and "not."

Goals:

- Combine statements using "and," "or," and "not."
- Write and parse conditional statements.
- Use truth tables to determine the truth value of complex statements.

Q1. Determine which of the following are statements. Recall that a statement is sentence that *is* true or false, not a sentence that could be true or false.

(a) The integer 5 is even.

(b) $x^2 = 4$

(c) $x^2 = -1$

(d) Dr. Justin Wright's cat has three legs.

(e) Brian called his dad.

Definition 1.1 Let P and Q be statements. The statement "P **and** Q" is true if and only if both P and Q are true. The statement "P **and** Q" is expressed symbolically as

$$P \wedge Q$$

and is known as a **conjunction**.

Definition 1.2 Let P and Q be statements. The statement "P **or** Q" is true if and only if P is true, Q is true, or both P and Q are true. The statement "P or Q" is expressed symbollically as

$$P \vee Q$$

and is known as a **disjunction**.

Remember that the word "or" is often used differently in mathematics than it is in common English. For instance, a police officer might say "Drop your weapon or I will shoot you" and you would understand that if you drop your gun you will not be shot. However, in mathematics the above statement would still be true if you drop your weapon AND the officer shoots you. A mathematician might say "Either drop your weapon or you will be shot, but not both."

Definition 1.3 Let P be a statement. The statement "It is not true that P," known as the **negation** of P and denoted $\sim P$, is true if and only if P is false.

Q2. Let P be the statement "n^2 is even" and Q be the statement "m is a multiple of 3." Express the following as ordinary English sentences.

(a) $P \wedge Q$

(b) $P \vee Q$

(c) $\sim P$

(d) $\sim Q$

(e) $\sim (P \wedge Q)$

(f) $\sim(P \vee Q)$

When dealing with a complicated statement, it can be handy to use a **truth table** to determine the truth value of the statement. The truth tables for the basic connectives are below.

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

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

P	$\sim P$
T	F
F	T

Q3. Make truth tables for the following statements. I've given you the start of the table for the first two to give you the idea.

(a) $\sim(P \wedge Q)$

P	Q	$(P \wedge Q)$	$\sim(P \wedge Q)$
T	T		
T	F		
F	T		
F	F		

(b) $(\sim P) \wedge (\sim Q)$

P	Q	$\sim P$	$\sim Q$	$(\sim P) \wedge (\sim Q)$
T	T			
T	F			
F	T			
F	F			

(c) $(\sim P) \vee (\sim Q)$

Q4. In the truth table above you looked at the statements "$\sim (P \wedge Q)$," "$(\sim P) \wedge (\sim Q)$," and "$(\sim P) \vee (\sim Q)$." Based on these truth tables, do you think there is a distribution rule for negation? That is, is "$\sim (P \wedge Q)$" the same as "$(\sim P) \wedge (\sim Q)$?"

Definition 1.4 If P and Q are statements the conditional statement "**If P, then Q**" is denoted $P \Rightarrow Q$ and has the truth table below.

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Q5. Suppose Dr. Wright were to tell you "If you come to every class, then you will get an A in the course." Find simple statements, P and Q, so that this statement is the same as "$P \Rightarrow Q$." Then determine what conditions are necessary for Dr. Wright to have lied to you.

Q6. Express each complex statement using statement variables and the logical connectives. Parse the statement as much as possible, and remember to say what your variables stand for.

(a) If I eat now, then I will not be hungry later.

(b) If f is not differentiable, then f is not continuous.

(c) Matrix M is invertible and matrix N is in row reduced form.

(d) If it snows today, then we will not have class and I will not learn anything.

This packet has been designed to help you review some of the content from your Introduction to Formal Mathematics class. In reality, we won't spend much time determining if things are

statements, converting to symbolic logic, or building truth tables. Most of our time will be spent proving conditional statements.

Chapter 2

Basic Set Theory

Sets are arguable the most basic building blocks of mathematics. It is not possible to discuss writing proofs nor to write proofs without know some basic set theory and notation.

Goals:

- Practice with set-builder notation.
- Practice finding cardinalities.

Q1. Write each of the following sets by listing their elements between braces.

(a) $\{3x + 2 : x \in \mathbb{Z}\}$

(b) $\{x \in \mathbb{Z} : -2 \leq x < 7\}$

(c) $\{x \in \mathbb{R} : x^2 + 5x = -6\}$

(d) $\{5a + 2b : a, b \in \mathbb{Z}\}$

Q2. Write each of the following sets in set-builder notation.

(a) $\{3, 4, 5, 6, 7, 8\}$

(b) $\{\ldots, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\}$

Q3. Describe (in your own words) what the cardinality of set is.

Q4. Determine the following cardinalities.

(a) $|\{2, 3, 4, 5\}|$

(b) $|\{2, 3, \{4, 5\}\}|$

(c) $|\emptyset|$

(d) $|\{\emptyset\}|$

(e) $|\{x \in \mathbb{Z} : x^2 - 3 \leq 0\}|$

Q5. (a) Suppose that A, B, and C are sets. What does the notation $A \subseteq B$ and $A \not\subseteq C$ mean? Be explicit.

(b) List all of the subsets of $A = \{2, 5, 7\}$.

The set of all of the subsets of A is called the **power set** of A and is denoted $\mathscr{P}(A)$. Symbolically, $\mathscr{P}(A) = \{X : X \subseteq A\}$.

Q6. Let $B = \{0, \{1\}\}$. Determine $\mathscr{P}(B)$.

We'll need to use set notation and the concepts listed here and in sections 1.1 and 1.3 of the text throughout the semester. If you ever find yourself unsure about set notation, don't hesitate to review these concepts and to ask questions.

Chapter 3

Axiomatic Systems

You have most likely heard of Euclid's axioms and you've maybe even heard of the Axiom of Choice. While there are a few famous axioms, most of the axioms of mathematics live in the dark corners and are ignored most of the time.

Goals:

- Describe some fundamental axioms.
- Use the Division Algorithm.

Mathematics is the most rigorous scientific field. However, even in mathematics, if you ask the question "But why?" enough times you arrive at a question without an answer. An axiom is the frustrated parent of the mathematical world's way of saying "Because I said so." In reality, **an axiom is just something we assume to be true without any proof that it is true.**

For our purposes, we will take some properties of sets to be axiomatic. Most of our axioms will seem so obviously true, that you may question why we're taking the time to point them out at all. However, almost all of *our* axioms are provable, just not with the mathematics available to us in this course. That is, a mathematician's choice of axioms is often dependent on how much work he or she is willing to do. See Section 1.10 of the text to learn about some of the impacts of the choice of axioms in mathematics.

3.1 Some Set Related Axioms

Axiom 3.1 If A is a set, then $A \subseteq A$.

We will assume that every set is a subset of itself. This axiom isn't required in general, and some very interesting things happen if you throw it out.

Q1. Consider the set $A = \{X : X \text{ is a set and } X \notin X\}$.

(a) By the definition of A, what would be implied if $A \notin A$?

(b) What would be implied if $A \in A$?

(c) What's wrong with these implications?

One of the set related axioms that we're using (but not explicitly stating) is that the questions above don't make sense because they would require that the set A be defined in terms of itself.

Axiom 3.2 If A is a set, then $\emptyset \subseteq A$.

There are actually quite a few axioms for sets that we'll be assuming without explicitly stating. Most of them are for strange situations that are beyond the scope of this course.

3.2 Arithmetic Properties of the Real Numbers and Their Subsets

A lot of time in this course will be spent dealing with real numbers. The good news is that you've been working with the real numbers for most of your life, so you're pretty familiar with them. The bad news is that we'll want be taking all of your knowledge as axiomatic. That is, we'll assume a few basic things to be true and then prove the rest later. Many of the axioms we assume can be proven, just not without a great knowledge of mathematics.

Axiom 3.3 (Closure under addition) For $X = \mathbb{Z}$, $\mathbb{R}$, or $\mathbb{Q}$, if $a \in X$ and $b \in X$, then $a + b \in X$.

Q2. Consider $X = \mathbb{Z}$ in the axiom. Can you think of a reasonable argument that the statement is true that doesn't rely on the statement?

Q3. We probably don't need to take the statement as an axiom when $X = \mathbb{Q}$. Let $x = {}^{a}\!/\!_{b}$ and $y = {}^{c}\!/\!_{d}$. Provide a reasonable explanation for the statement $x + y \in \mathbb{Q}$.

Q4. Your argument for Q3. probably made an assumption about multiplication. What assumption did you make?

We'll often need to reference closure in our proofs when we need to explain how we know that the quantities we're dealing with are in the sets in which we claim them to be. Axiom 3.4 below should be pretty familiar. We can assume it without reference in our proofs.

Axiom 3.4 (Common Arithmetic Properties) For $X = \mathbb{Z}$, $\mathbb{R}$, or $\mathbb{Q}$ and $a, b, c \in X$.

- $a(b + c) = ab + ac$ (*Distribution*)
- $a + b = b + a$ and $ab = ba$ (*Commutativity*)
- $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$ (*Associativity*)

Remark 3.2.1. If you go back through the few properties that we have for arithmetic, you'll find the division isn't mentioned anywhere. That's because *our sets are not closed under division.* In proof writing, it's best to avoid using division altogether.

Axiom 3.5 The Zero Product Law If a and b are real numbers and $ab = 0$, then $a = 0$ or $b = 0$.

Q5. The Zero Product Law is the fundamental tool in most of algebra. Use it to solve the equation $x^2 + 5x + 6 = 0$.

Q6. The Zero Product Law is also the tool we use to avoid division. Solve the equation $2x^2 = 4x$ using only the allowed arithmetic operations and the Zero Product Law. Do not use division.

Additionally, we will assume that the following rules for working with fractions are valid. They're easy enough to prove, but we'll just assume them for now.

Axiom 3.6 Given real numbers a, b, c, and d

- $\dfrac{a}{b} = \dfrac{ac}{bc}$ if $b \neq 0$ and $c \neq 0$

- $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ if $b \neq 0$ and $d \neq 0$
- $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ if $b \neq 0$ and $d \neq 0$.
- $\frac{a/b}{c/d} = \frac{ad}{bc}$ if $b \neq 0$, $c \neq 0$, and $d \neq 0$

This is all that we'll be assuming about the operations of the real numbers. Any other properties will have to be proven as we go.

3.3 General Properties of the Real Numbers and Their Subsets

Axiom 3.7 (Trichotomy of the Real Numbers) If x and y are real numbers, then $x = y$, $x < y$, or $x > y$.

The Trichotomy of the Reals is sometimes just called the ordering of the reals (which doesn't sound as cool or impressive). It's the property that allows us to plot real numbers on a number line in a meaningful way.

Axiom 3.8 (The Well-Ordering Principal) Any set of natural numbers contains a smallest element.

Q7. Consider the set $A = \left\{\frac{1}{n} : n \in \mathbb{R}, n > 0\right\}$.

(a) Is A a set of natural numbers?

(b) Does A have a smallest element?

(c) Can you say that the Well-Ordering Principal holds for sets other than the natural numbers?

Q8. A concept closely related to the Well-Ordering Principal is the Quotient-Remainder Theorem (which is also knowns as the Division Algorithm). To get things started, we need to go back to elementary school.

(a) Use long division to determine the remainder when 113 is divided by 8.

(b) Give integers p and r such that $113 = 8p + r$ where $0 \leq r < 8$.

Q9. Repeat the steps above when 258 is divided by 17.

The Quotient-Remainder Theorem sounds scary, but it really just says that you can do long division the way you have since grade school. It is stated below.

Axiom 3.9 (The Quotient-Remainder Theorem) Given any integers a and b with $b > 0$, there exist integers q and r such that $a = qb + r$ where $0 \leq r < b$.

The variable q is sometimes referred to as the quotient and r as the remainder. Hence the name of the theorem.

The most important thing to take from the Quotient-Remainder Theorem is the restriction on r. It says that if a is divided by b then the remainder will be less than b. This fact is surprisingly useful.

Q10. What are the possible remainders when dividing by 2? What about when dividing by 3?

Q11. We can talk about writing integers in terms of other integers using the Quotient-Remainder Theorem. For instance, we can write 7 in terms of 2 by writing $7 = 3(2) + 1$. In the notation of the theorem, we have $a = 7$, $b = 2$, $q = 3$, and $r = 1$.

(a) Let $n \in \mathbb{Z}$. Ignoring the fact that we don't know the value for q, what are the only ways that n can be written in terms of 2?

(b) Ignoring q again, what are the only ways to write an integer n in terms of 3?

For now, we'll take the Quotient-Remainder Theorem as an axiom. We will prove it later this semester when we're ready.

Chapter 4

Basic Existence Proofs

Many definitions in mathematics involve existence statements. In some sense the most fundamental piece of proof writing is showing that an element of a set satisfies some definition. Doing so requires what is called an existence proof.

Goals:

- Write existence proofs based on given definitions
- Disprove statements using existence proofs

4.1 Why you're here

You're in this course to learn to write mathematical proofs of statements. To make this a digestible task, you'll be writing proofs of statements that we already know to be true. You will often think to yourself "Isn't that obvious?" Maybe it is, but that doesn't mean you don't have to prove it. If a statement isn't an axiom then it needs to be proven. Once it has been proven it can be used in the future.

You need to master the art of proof writing before you move on to more advanced math courses. In upper level courses like Geometries, Abstract Algebra, and Analysis proofs will be the primary assessment tool. You will demonstrate your understanding of concepts and definitions by writing proofs about them. Of course, that requires that you already know how to write a proof when you get there. Proof writing is to advanced mathematics as algebra is to calculus. It will be assumed that you have a perfect working knowledge of it when you're called upon to use it.

4.2 Definitions

Definitions are the cornerstone of advanced mathematics. We work from axioms and definitions to build new ideas. As the semester progress, you'll learn to work with a lot of new and interesting definitions. Some will be somewhat familiar, while others will be very new. There are two important things to keep in mind about mathematical definitions. First, you only know a definition if you can restate it verbatim. Paraphrasing isn't good enough. Second, definitions change between textbooks and mathematical works. You should never accept your prior knowledge as good enough where a definition is concerned. Always do your best to find the authors version of the definition.

We will need the following definitions for this topic and throughout the remainder of the semester.

Definition 4.1 (Even) An integer n is **even** if there exists $k \in \mathbb{Z}$ such that $n = 2k$.

Definition 4.2 (Odd) An integer n is **odd** if there exists $k \in \mathbb{Z}$ such that $n = 2k + 1$.

Definition 4.3 (Divides) An integer a **divides** an integer b, denoted $a \mid b$, if and only if there exists $k \in \mathbb{Z}$ such that $ak = b$.

Note: The expression "$a \mid b$" is a mathematical statement, not a mathematical expression. That is, "$a \mid b$" is true or false. Do not confuse this notation with the expression "a/b" which is a rational number.

If $a, b \in \mathbb{Z}$ and $a \mid b$, then we will often say that b is a **multiple** of a. For instance, "$5 \mid 10$" and "10 is a multiple of 5" give us the same information. The terms "divides" and "multiple" can be used in similar situations, but "divides" tends to be more concise. For instance, consider

$$\{k \in \mathbb{N} : k \mid 12\} = \{k \in \mathbb{N} : 12 \text{ is a multiple of } k\} = \{1, 2, 3, 4, 6, 12\}.$$

Writing note: The word "divides" is an active verb, where as "is" is not. Most of us naturally prefer action verbs when reading. As a result, saying "$5 \mid 10$" instead of "10 is a multiple of 5" will make your writing more interesting to read.

4.3 Existence Proofs

Consider the statement P:"The integer 6 is even." Odds are that you're willing to accept this statement as being true without any argument. You've been exposed to even and odd integers for some time now. Still, this example will serve as great practice.

The statement P is an existence statement in disguise.

$$P \equiv Q : \text{"There exists an integer } k \text{ such that } 6 = 2k.$$

While statements P and Q say exactly the same thing, Q helps us understand what we need to do to demonstrate that P is true: we need to provide and integer k so that $2k = 6$. The integer 3 should work just fine.

Claim 4.1. The integer 6 is even.

Proof. Notice that $2(3) = 6$, so there exists an integer k such that $6 = 2k$. Thus 6 is even by definition. □

Q1. Directions: Prove the following existence statements. Please note that being asked to prove something means you're being asked to do more than provide the example for the existence statement. You need to use full sentences and reference appropriate definitions and axioms.

Claim 4.2. The integer 8 is even.

Claim 4.3. The integer 7 is odd.

Claim 4.4. The integer -5 is odd.

Claim 4.5. The integer 0 is even.

Claim 4.6. For some integer k, the integer $8k$ is even.

Claim 4.7. For some integer k, the integer $2k + 3$ is odd.

Claim 4.8. For some integers n and m, the integer $2n + 2m + 1$ is odd.

Claim 4.9. The integer 15 divides the integer 30.

Claim 4.10. For some integer k, $2|(4k + 6)$.

Hopefully you found the claims in this section relatively easy to prove. These basic existence proofs will often appear as a part of larger, more substantive proofs. Later in the semester we will discuss existence proofs that require more than knowledge or arithmetic.

4.4 Disproof

When not proving statements of the form $\exists\ x, P(x)$ we'll be proving statements of the form $\forall\ x, P(x)$.

Q2. If $\forall\ x, P(x)$ is false, then its negation is true. Give the negation of this statement.

Q3. If we want to show that a universally quantified statement is false, what method do you think we can employ?

Since we prove that a universal statement is false by proving that a related existence statement is true, and we prove existence statements by providing an example, we often call the example used to disprove a universal statement a *counter example*.

Q4. Directions: Disprove the following statements by providing a counter example.

Claim 4.11. If $x, y \in \mathbb{R}$ and $x < y$, then $x^2 < y^2$.

Claim 4.12. For $n \in \mathbb{Z}$, if $2|n$, then $4|n$.

Claim 4.13. For integers n and k, if $n = 2k$ then k is even.

Disproving statements isn't considered all that interesting by mathematicians. However, we often employ disproof techniques to find errors in proofs. For example, if Natal has written a proof containing the claim "Since $x \in \mathbb{R}$, $x^2 > 1$" we know Natal's proof is entirely wrong if we can provide a counterexample to this single statement.

Chapter 5

Direct Proof

Direct proof is the most often used, and in some sense most useful, proof writing method. Students new to writing proofs often attempt to employ more complicated proof techniques when a direct proof will suffice.

Goals:

- Write a direct proof based on given definitions
- Write a proof with subtle steps (rewriting proofs)
- Develop a proof by considering examples of the statement

Here we prove statements either of the form $P \Rightarrow Q$ or statements that can be written this way. Hopefully you will recall that statements of the form $P \Rightarrow Q$ can be thought of as universal statements: "For all x such that $P(x)$ is true, $Q(x)$ is true."

It's important to distinguish the universal statements we will prove in this chapter from the existential statements we proved in Chapter 4. Examples are never enough to prove universal statements and therefore we'll need to work a little harder here.

We will need the following definitions for this packet and throughout the remainder of the semester.

Definition 5.1 (Even) An integer n is **even** if $n = 2k$ for $k \in \mathbb{Z}$.

Definition 5.2 (Odd) An integer n is **odd** if $n = 2k + 1$ for $k \in \mathbb{Z}$.

Definition 5.3 (Divides) An integer a **divides** an integer b, denoted $a \mid b$, if and only if there exists $k \in \mathbb{Z}$ such that $ak = b$.

Note: The expression "$a \mid b$" is a mathematical statement, not a mathematical expression. That is, "$a \mid b$" is true or false. Do not confuse this notation with the expression "a/b" which is a rational number.

If $a, b \in \mathbb{Z}$ and $a \mid b$, then we will often say that b is a **multiple** of a. For instance, "$5 \mid 10$" and "10 is a multiple of 5" give us the same information. The terms "divides" and "multiple" can be used in similar situations, but "divides" tends to be more concise. For instance, consider

$$\{k \in \mathbb{N} : k \mid 12\} = \{k \in \mathbb{N} : 12 \text{ is a multiple of } k\} = \{1, 2, 3, 4, 6, 12\}.$$

Writing note: The word "divides" is an active verb, where as "is" is not. Most of us naturally prefer action verbs when reading. As a result, saying "$5 \mid 10$" instead of "10 is a multiple of 5" will

make your writing more interesting to read.

The goal of this workbook is generally not to tell you exactly how to do things. You're much better off trying to do things on your own and looking back at the examples provided in the textbook for more clarity later. That way you're critically thinking about the task at hand rather than trying to duplicate the process that somebody else used.

That being said, proofs of statements of the form $P \Rightarrow Q$ tend to have some similarities. They'll start off by saying something like "Let [P be true]" where P is replaced with the appropriate statement. These proofs usually end by arriving at the statement Q. It's up to the writer to connect the two ideas using whatever valid mathematical steps are necessary.

For right now, your goal is to be able to connect the P and Q statements. We'll focus more on clear writing as we move forward. You should still try your best to communicate your ideas as clearly and efficiently as possible.

It's important in proof writing to accept that a particular proof writer's style can have a drastic impact on the appearance of their proofs. Developing your own style will be helpful as it will add to sense of comfort and familiarity to your writing so that you won't spend as much time thinking about how to say things. Ultimately you'll need to be careful to make sure that your style conforms to the writing expectations within mathematics.

Directions: For each of the following claims answer the questions about the claim and then attempt to prove the claim.

Claim 5.1. If x is an even integer, then x^2 is even.

Q1. Determine statements P and Q so that the claim can be written in the form $P \Rightarrow Q$.

Q2. According to Definition 1, what does it mean for x to be even?

Q3. Square your new expression for x. Can you rewrite this expression so it has the form of an even integer?

Proof. Let $x \in \mathbb{Z}$ be even. □

Claim 5.2. Suppose a, b, and c are integers. If $a \mid b$ and $b \mid c$, then $a \mid (b + c)$.

Q5. According to Definition 3, what does it mean to say that $a \mid b$?

Q6. According to Definition 3, what does it mean to say that $b \mid c$?

Q7. What must we show to be able to conclude that $a \mid (b + c)$?

Proof. Let $a, b, c \in \mathbb{Z}$ such that

□

Claim 5.3. Suppose a is an integer. If $7|4a$, then $7|a$.

Q5. According to Definition 3, what does it mean to say that $7|4a$?

Q6. What do you need to show to be able to conclude that $7|a$?

Q7. Find an integer a such that $7|4a$. What do you notice about the numbers $4a$ and a?

Proof. Let $a \in \mathbb{Z}$ such that

□

Claim 5.4. If x is a real number and $0 < x < 4$, then $\dfrac{4}{x(4-x)} \geq 1$.

Q5. Here we have $\boxed{\text{P: } x \text{ is a real number and } 0 < x < 4}$, $\boxed{\text{Q: } \frac{4}{x(4-x)} \geq 1}$, and we want to show $P \Rightarrow Q$. It isn't clear how we should start this (there's no way into the maze). Begin with Q and manipulate the expression into a simple statement about x.

Proof. Let $x \in \mathbb{R}$ such that $0 < x < 4$.

□

Claim 5.5. Every odd integer is a difference of two squares. (Example: $7 = 4^2 - 3^2$)

Q5. It will be very beneficial for you to find more examples. Can you find the appropriate integers for 5, 9, and 11? That is, find integers a and b such that $5 = a^2 - b^2$ then do the same for 9 and 11.

Q6. What do you notice about the relationship between a and b?

Proof. Let

□

Chapter 6

More on Direct Proof: Treating Cases

Using cases to write proofs allows us to assume some information about the statement we are trying to prove. This added information is often a helpful tool in writing proofs.

Goals:

- Break the P statement in $P \Rightarrow Q$ into cases
- Write proofs using cases
- Write proofs about new definitions

Our focus is still on proving statements of the form $P \Rightarrow Q$. Very often, P doesn't give us much information to work with. For instance, consider the following two statements.

Statement 1: If n is an odd integer, then n^2 is an odd integer.

Statement 2: If n is an integer, then $n^2 + 7n + 6$ is even.

By now, you have probably figured out that to prove Statement 1, you would start out by saying "Suppose n is an odd integer. Then $n = 2k + 1$ for $k \in \mathbb{Z}$." However, in Statement 2, we only know that n is an integer, so it isn't clear where we might start our proof. We might consider the case when n is even and the case when n is odd separately, so we can make an assumption like we did for Statement 1. Since an integer must be either even or odd, proving the statement for these two cases will give the desired result.

To keep things light for today, we'll write proofs about the following definition to give us practice with cases.

Definition 6.1 (Parity) Two integers have the **same parity** if they are both even or they are both odd. Otherwise, they have **opposite parity**.

Q1. Prove that if n is an integer, then n and $n + 2$ have the same parity by considering the case when n is even and the case when n is odd separately.

Q2. Prove that if n is an integer, then n and n^2 have the same parity.

Q3. Prove that if n is an integer, then n and $n + 3$ have opposite parity.

Q4. Prove that if two integers have the same parity, then their sum is even.

Q5. Prove that if n is an integer, then $2 \mid (n^2 - n)$. (Note: You should prove this statement now with cases, but there is a much shorter proof possible that doesn't require a proof by cases. See if you can figure it out after you've finished this section.)

Q6. Prove that if $x \in \mathbb{R} - \{0, 1\}$, then either $x^2 < x$ or $x^2 > x$. (Recall: $x \in \mathbb{R} - \{0, 1\}$ if $x \in \mathbb{R}$ and $x \notin \{0, 1\}$.)

Q7. Prove that if n is an integer, then $3 \mid (n^3 - n)$.

Using proof by cases can be very tempting, even when it isn't necessary. Often times we'll initially write a proof by cases because the added assumption we get to make helps us see things more clearly. Consider the following claim.

Claim 6.1. If n is an integer, then $(2n+3)+(-1)^n(2n+1)$ is even.

Q8. Prove Claim 5.1 by using cases.

Q9. Prove Claim 5.1 by considering the parity of $2n+3$ and $(2n+1)$.

Chapter 7

Proof Reading with Examples

One aspect of writing proofs is learning to read and critique them. In later classes you will reading and trying to understand proofs of concepts with which you are not particularly familiar. Here, our goal is to learn to read proofs with an eye for critiquing them. This will help you to find problems with your own proofs.

Goals:

- Learn to read proofs using examples
- Read an interpret proofs written by others
- Find mistakes in proofs

7.1 Reading Proofs

Reading a mathematical proof is not like reading a passage in a novel or an article online. Reading a proof is an activity in which the reader must take an active role in the process. Fortunately, a well-written proof usually tells you exactly what you should be doing.

Directions: Consider the following claim whose proof is taken from the text. Answer the questions as you go.

Claim 7.1. If x is an even integer, then $x^2 - 6x + 5$ is odd.

Proof. Suppose x is an even integer.

Q1. Do as the first sentence tells you to do. Choose an even integer value to assign to the variable x. Write your choice here and confirm that the claim is true for your choice.

Then $x = 2a$ for some $a \in \mathbb{Z}$, by definition of an even integer.

Q2. If this sentence is true, then you should be able to choose the value of a for your choice of x. Write that value here.

So

$$\begin{aligned} x^2 - 6x + 5 &= (2a)^2 - 6(2a) + 5 \\ &= 4a^2 - 12a + 5 \\ &= 4a^2 - 12a + 4 + 1 \\ &= 2(2a^2 - 6a + 2) + 1. \end{aligned}$$

Therefore we have $x^2 - 6x + 5 = 2b + 1$, where $b = 2a^2 - 6a + 2 \in \mathbb{Z}$ by closure.

Q3. This is probably overkill, but double check that b is in fact an integer for your a value.

Consequently $x^2 - 6x + 5$ is odd, by definition of an odd number. □

In the above questions you checked the mathematics of a proof using examples. Of course, examples aren't enough to prove general statements, but they can be helpful guides. Reading along with a proof using examples not only helps us find potential mathematical errors, but it can also serve as a guide for clear proof *writing*.

Directions: Consider the following proof of the same claim. Once again, follow treat the statements made in the proof like instructions. Reflect on how elements of the proof are introduced. Did you have to make changes as you read?

Proof. Suppose x is an integer.

Let x be even.

Let a be an integer such that $2a = x$.

We know there is an a because x is even.

So $x^2 = (2a)^2 = 4a^2$. Let $a^2 = m$ so that $x^2 = 4m$ so x^2 is even.

Next, $-6x = -6(2a) = 2(-6a)$. Let $-6a = k$ so that $-6x = 2k$ so $-6x$ is even.

Finally an even plus an even is even plus and odd is odd. □

As you read your own proofs and the proofs of others this semester, keep in mind that you should always be able to follow along with them using examples. If you find that doing so is tedious with a particular proof, then there's a good chance the proof could use some rewriting.

7.2 Finding Errors in Proofs

The following proofs come from assignments of previous students. Each proof contains at least one error and most contain several. However, none of these proofs is totally wrong. They just need some adjusting. For each proof, find any errors that you can and suggest a correction.

Claim 7.2. If $n \in \mathbb{Z}$, then $n^2 + 7n + 6$ is even.

Proof. Suppose n is an odd integer. Thus, $n = 2k + 1, k \in \mathbb{Z}$. We substitute for n in $n^2 + 7n + 6$ to get:

$$(2k + 1)^2 + 7(2k + 1) + 6$$

$$4k^2 + 4k + 1 + 14k + 7 + 6$$

$$4k^2 + 18k + 14$$

$$2(2k^2 + 9k) + 14$$

We let $m = (2k^2+9k+7)$ to get $2m+14$. We know that m will be some integer, therefore, $n^2 + 7n + 6$ is even. □

Proof. Suppose n is an even integer. Thus,$n = 2k, k \in \mathbb{Z}$. We substitute for n in n^2+7n+6 to get:

$$(2k)^2 + 7(2k) + 6$$

$$4k^2 + 14k + 6$$

$$2(2k^2 + 7k) + 6$$

We let $m = (2k^2 + 7k + 3)$ to get $2m + 6$. We know that m is some integer, therefore, $n^2 + 7n + 6$ is even. □

Claim 7.3. If $n \in \mathbb{Z}$, then $5n^2 + 3n + 7$ is odd.

Proof. Suppose n is some integer.

Case 1: Assume n is an even integer. By definition of an even integer $n = 2k$ for some integer k. Then $5n^2 + 3n + 7 = 5(2k)^2 + 7 = 20k^2 + 6k + 6 + 1$. We can then factor out a 2 so $5n^2 + 3n + 7 = 2(10k^2 + 3k + 3) + 1$. Let $p = 10k^2 + 3k + 3$ so that $5n^2 + 3n + 7 = 2p + 1$. Which is the definition of an odd integer, thus $5n^2 + 3n + 7$ is odd.

Case 2: Assume n is an odd integer. By definition of an odd integer $n = 2k + 1$ for some integer k. Then $5n^2+3n+7$ is equal to $5(2k+1)^2+3(2k+1)+7 = 20k^2+16k+14+1$. We can factor out a 2 so $5n^2 + 3n + 7 = 2(10k^2 + 8k + 7) + 1$. Let $p = 10k^2 + 8k + 7$ so that $5n^2 + 3n + 7 = 10k^2 + 8k + 7$. Which is the definition of an odd integer thus, $5n^2 + 3n + 7$ is odd.

Case 3: Assume n is equal to zero. Then $5(0)^2 + 3(0) + 7 = 7$, by definition 7 is an odd integer. Thus, $5n^2 + 3n + 7$ is odd.

Since all three cases math up then for some integer n, $5n^2 + 3n + 7$ is odd. □

Claim 7.4. If $x \in \mathbb{R}$ and $x \notin \{-1, 0, 1\}$, then $x^3 < x$ or $x^3 > x$.

Proof. Suppose that $X \in \mathbb{R}$. We can say that $x(x+1)(x-1) > 0$ or $x(x+1)(x-1) < 0$ is true when $x \notin \{-1, 0, 1\}$. We can rewrite the inequality $x(x+1)(x-1) > 0$ to get $x(x^2-1) > 0$ which can be factor to $x^3 - x > 0$ and finally expressed as $x^3 > x$.

We can do the same to the inequality $x(x+1)(x-1) < 0$ to get $x(x^2-1) < 0$ which can be factored to $x^3 - x < 0$ and finally expressed as $x^3 < x$.

Therefore, if $X \in \mathbb{R}$ & $x \notin \{-1, 0, 1\}$, then $x^3 > x$ or $x^3 < x$. □

Claim 7.5. Suppose $a, b, c, d \in \mathbb{Z}$. If $a \,|\, b$ and $c \,|\, d$, then $ac \,|\, bd$.

Proof. Suppose $a, b, c, d \in \mathbb{Z}$ so that $a \,|\, b$ and $c \,|\, d$. For a to divide b, we need an integer k so that $ak = b$. For c to divide d, we need an integer ℓ so that $c\ell = d$. We can multiple each of these sides to give us $bd = akc\ell$ which can be rewritten as $bd = (ac)(k\ell)$. We can make $k\ell$ some integer m giving us $bd = (ac)(m)$. Showing that ac divides bd. Therefore, if $a \,|\, b$ and $c \,|\, d$, then $ac \,|\, bd$. □

Proof. By definition, a divides b if $ak = b$ for $k \in \mathbb{Z}$. That applies to c dividing d, so we have $c\ell = d$. Therefore, $bd = (ak)(c\ell)$ or $bd = (ac)(k\ell)$ which shows that ac is a multiple of bd. □

Claim 7.6. Suppose $x, y \in \mathbb{R}$. If $x < y$, then $x < \dfrac{x+y}{2} < y$.

Proof. Suppose $x, y \in \mathbb{R}$, then $x < \frac{x+y}{2}$ where $x = \frac{2x}{x} = \frac{x+x}{2}$. By substituting, $\frac{x+x}{2} < \frac{x+y}{2}$ is equivalent to $\frac{2x}{2} < \frac{x+y}{2}$ in which, $x < \frac{x+y}{2}$. If $\frac{x+y}{2} < y$ and $y = \frac{2y}{2} = \frac{y+y}{2}$, then $\frac{x+y}{2} < \frac{y+y}{2}$. After multiplying both sides by 2 we get $x + y < y + y$. Then, by subtracting y we can see that $x < y$. Therefore, $x < \frac{x+y}{2} < y$. □

Proof. Let $x, y \in \mathbb{R}$ and suppose $x < y$. Multiplying each side by 2, $x < y = 2x < 2y$ and subtracting an x and y from both sides we have $-x - y < -y - x$. Adding $2x$ to the left side, and $2y$ to the right side of the inequality, $2x - x - y < 2y - y - x$ which can be rewritten as $2x < x + y < 2y$. Dividing each expression by 2 we see that when $x < y$ then $x < \frac{x+y}{2} < y$. □

Chapter 8

Contrapositive and Proof by Contrapositive

Proof by contrapositive is a very powerful proof technique. Technically speaking, any statement that can be proven with a direct proof can be proven with a contrapositive proof and vice versa. However, it is almost always the case that one proof is significantly easier to write.

Goals:

- Negate statements in a useful manner
- Construct contrapositive statements
- Write proofs using contrapositive statements.

Before we start working on writing proofs by contrapositive, let's review negating statements. Consider the following statements.

P : The number 2 is even.
Q : $x < y$.
R : Set $A = \emptyset$.

Recall that negating these statements is essentially putting the phrase "It is not true that" in front of the statement.

$\sim P$: It is not true that 2 is even. $\equiv$ The number 2 is odd.
$\sim Q$: It is not true that $x < y$. $\equiv$ $x \geq y$.
$\sim R$: It is not true that $A = \emptyset$. $\equiv$ $|A| > 0$.

Notice that two forms of the above statements are given. The first is the direct negation, while the second is, in some sense, a more helpful version of the negation.

Q1. Negate the following simple statements and open sentences. Express the negation in a more natural way if possible. That is, don't simple write "It is not true that" in front of the original statement.

(a) The sum of a and b is odd.

(b) $a \nmid 2b$.

(c) $x \geq 1$.

It can be more complicated to negate a complicated statement or open sentence. Consider the statement below.

$$R: \text{ Integer } a \text{ is even and integer } b \text{ is odd.}$$
$$\sim R: \text{ It is not true that } a \text{ is even and } b \text{ is odd.}$$

Notice that the statement given for $\sim R$ does not tell us anything specific about a or b. Thus, it is the correct negation, but of no practical use. We can see that $R \equiv P \wedge Q$ if P : "Integer a is even" and Q : "Integer b is odd." Recall that by DeMorgan's Laws, $\sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q)$. Then we can express $\sim R$ as follows.

$$\sim R: \text{ Integer } a \text{ is odd } \textit{or} \text{ integer } b \text{ is even.}$$

Q2. Negate the following complicated statements using DeMorgan's Laws and the negation of a conditional statement.

(a) $2 \,|\, a$ or $2 \nmid b$.

(b) Integer 2 is a divisor of 10 and 20.

(c) $x < 1$ or $x \geq 2$.

(d) $-2 < x < 3$.

Now that we feel comfortable negating statements, let's recall what the contrapositive actually is. Fill in the following truth table.

P	Q	$P \Rightarrow Q$	$\sim Q$	$\sim P$	$\sim Q \Rightarrow \sim P$
T	T				
T	F				
F	T				
F	F				

Notice that the statements $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ are logically equivalent. That is, they produce they same truth values for any given P and Q. This means that if we are asked to prove a statement of the form $P \Rightarrow Q$, we can instead prove the statement $\sim Q \Rightarrow \sim P$. This probably doesn't seem like much of an improvement. Like integration by parts in Calculus 2, this seems to make things more difficult rather than less difficult. However, like integration by parts, contrapositive can be very handy in practice. Consider the following example.

$$P : n^2 \text{ is even}$$
$$Q : n \text{ is even}$$

If asked to prove this statement, we might start out with something like

"Suppose n^2 is even. Then $n^2 = 2a$ for $a \in \mathbb{Z}$."

Unfortunately, there's no clear way to turn this into a statement about n. (Give some thought as to why you can't just take the square root of each side of the equation.) On the other hand, the contrapositive is quite simple to prove.

Q3. (a) For the statements P and Q listed above, give the contrapositive of $P \Rightarrow Q$. Remember to restate the negations in a useful manner.

(b) Prove the contrapositive found in part (a) using a direct proof.

Before we really start writing proofs by contrapositive, we need to discuss two conventions that we'll use in this class. The first is used almost universally by mathematicians, and the second is just for the purposes of our class.

Let the reader know it's a contrapositive proof: Keep in mind that our proof reader is either someone who is skeptical of our claim or someone who doesn't fully understand our claim. If we decide to write a contrapositive proof rather than a direct proof, then our reader could quickly become very confused. For that reason, we always inform the reader at the start of the proof that we are writing a proof by contrapositive. The two most common ways to do this are as follows.

Claim 8.1. Suppose n is an integer. If n^2 is even, then n is even.

(i) *Proof.* (By Contrapositive) Suppose n is odd. Then ...

□

(ii) *Proof.* We proceed by contrapositive, so suppose n is odd. Then ...

□

Dr. Justin Wright prefers the first method be used by his students, and Dr. Emma Wright prefers the second.

Give the contrapositive: This convention is only for the purposes of this course, and shouldn't be used otherwise. Because you're new at this, it is a good idea to state the thing that you are trying to prove outright. This will prevent Dr. Wright from trying to decide if you're proving the wrong thing correctly or the right thing incorrectly if there's a problem. Our proof should appear as follows.

Proof. (By Contrapositive) [If n is odd, then n^2 is odd.] Suppose n is odd. Then ...

□

Q4. You're finally ready. Prove the following claims using a proof by contrapositive. Follow all conventions.

Claim 8.2. Suppose $x \in \mathbb{Z}$. If $x^2 - 6x + 5$ is even, then x is odd.

Claim 8.3. Suppose $x, y \in \mathbb{Z}$. If $5 \nmid xy$, then $5 \nmid x$ and $5 \nmid y$.

Claim 8.4. Suppose a and b are integers. If $a + b$ is even and ab is even, then a and b are both even.

With a new proof technique comes new definitions.

Definition 8.1 Given integers a and b and an $n \in \mathbb{N}$, we say that a and b are **congruent modulo n** if (and only if) $n|(a-b)$. We express this as $a \equiv b \pmod{n}$. If a and b are not congruent modulo n, we write this as $a \not\equiv b \pmod{n}$. Here, n is referred to as the **modulus**.

Q5. This new definition really isn't so bad. We can think of it as saying $a \equiv b \pmod{n}$ if a and b have the same remainder when divided by n. For instance, $8 \equiv 14 \pmod{3}$ because $8 = 3(2) + \boxed{2}$ and $14 = 3(4) + \boxed{2}$. Determine if the following statements are true or false.

(a) $7 \equiv 17 \pmod{5}$

(b) $24 \equiv 6 \pmod{6}$

(c) $-1 \equiv 4 \pmod 5$

(d) $8 \equiv -2 \pmod 4$

Q6. Prove the following claim using both direct proof and proof by contrapositive. Which proof is easier to write? Which is easier to understand?

Claim 8.5. Let a, b, and $c \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod n$ and $a \equiv c \pmod n$, then $c \equiv b \pmod n$.

Q7. There are no distinct rules about when to use a direct proof versus when to use proof by contrapositive. However, you may have developed some intuition about where you may want to start. List some ideas you have of how to decide between direct proof or proof by contrapositive.

Chapter 9

Proof by Contradiction

I've probably referred to all of our proof techniques as "powerful," but the method of contradiction really is amazingly powerful. Most often, we employ proof by contradiction when proving a claim for which there is no clear beginning for the proof. You'll see some examples soon.

Goals:

- Develop the logic behind proof by contradiction
- Find the contradiction in given proofs by contradiction
- Write proofs using contradiction

We're still working to prove statements of the form $P \Rightarrow Q$. The process of proof by contradiction begins with negating such a statement. You may recall from Intro to Formal Mathematics that

$$\sim (P \Rightarrow Q) \equiv P \wedge \sim Q.$$

Q1. Confirm that $\sim (P \Rightarrow Q) \equiv P \wedge \sim Q$ using the truth table below.

P	Q	$P \Rightarrow Q$	$\sim (P \Rightarrow Q)$	$\sim Q$	$P \wedge \sim Q$
T	T				
T	F				
F	T				
F	F				

Q2. Negate the following conditional statements using the form $P \wedge \sim Q$. Remember to negate Q in a *useful* way if possible.

(a) If $x > 1$, then $x^3 > x$.

(b) If $a \,|\, b$, then $a \,|\, bc$.

(c) If $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{n}$.

(d) If a is even, then a^2 is even and a^3 is even.

(e) If $x \,|\, yz$, then $x \,|\, y$ or $x \,|\, z$.

It is very possible that you've employed a contradiction argument before as it is common even outside of mathematics. The structure of the method is simple. We begin with a statement R that is true. The statement R itself may be quite complicated. It could be a conjunction, disjunction, conditional statement like $R \equiv (P \Rightarrow Q)$, or any combination thereof. To argue that R is true we begin by supposing that R is false. We then derive a series of statements using correct deductive reasoning. With any luck we manage to derive an *absurdity*, that is, a statement that is always false. Often times the absurdity will take the form $C \wedge \sim C$, but this is not always the case.

Q3. Complete the following truth table for $C \wedge \sim C$ to show that this statement is an absurdity.

C	$\sim C$	$(C \wedge \sim C)$
T		
F		

Q4. The general form of the argument in a proof by contradiction is $\sim R \Rightarrow (C \wedge \sim C)$. Fill in the truth table for this argument form to see that it is true precisely when R is true.

R	C	$(C \wedge \sim C)$	$\sim R \Rightarrow (C \wedge \sim C)$
T	T		
T	F		
F	T		
F	F		

Q5. We need one more step before we really get started. We'll use the following claims as lemmas today. That is, we'll use them while proving other statements. You can prove the following claims with either a direct proof or a proof by contrapositive.

Claim 9.1. Suppose $n \in \mathbb{Z}$. If n^3 is even, then n is even.

Claim 9.2. Suppose $a, b, c \in \mathbb{Z}$. If $a \,|\, (b + c)$ and $a \,|\, b$, then $a \,|\, c$.

Let's take a look at using contradiction to prove the following claim. The proof given below is adapted from the one given in your text.

Claim 9.3. If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.

Here, R is the conditional statement "If $a, b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$." Recall then that $\sim R$ will be "$a, b \in \mathbb{Z}$ and $a^2 - 4b - 3 = 0$." This is how our proof will begin.

Notice, that there is no given C. The statement of the claim gives no indication of what the contradicting piece will be. We are forced deduce things from our initial claim seemingly at random until we stumble across a contradiction.

Finally, like contrapositive, we want to tell our reader how we are proving the claim so that he or she is not confused by our proof. Usually, we begin proofs by contradiction with the phrase "Suppose for the sake of contradiction that..." or "By way of contradiction, suppose..." For the purposes of this class, when using contradiction we will also start by writing "(Contradiction)."

Proof. (Contradiction) Suppose for the sake of contradiction that $a, b \in \mathbb{Z}$ and $a^2 - 4b - 3 = 0$.

Then

$$\begin{aligned} a^2 &= 4b + 3 \\ &= 4b + 2 + 1 \\ &= 2(2b + 1) + 1. \end{aligned}$$

Since $2b + 1$ is an integer, we have that a^2 is odd by definition. Recall from a previous proof that if a^2 is odd then a is odd, so $a = 2c + 1$ for $c \in \mathbb{Z}$. By substitution, we have

$$\begin{aligned} a^2 - 4b - 3 &= 0, \\ (2c + 1)^2 - 4b - 3 &= 0, \\ 4c^2 + 4c + 1 - 4b - 3 &= 0, \\ 4c^2 + 4c - 4b - 2 &= 0, \\ 2(2c^2 + 2c - 2b - 1) &= 0, \\ 2c^2 + 2c - 2b &= 1, \\ 2(c^2 + c - b) &= 1. \end{aligned}$$

Since $(c^2 + c - b) \in \mathbb{Z}$, the last equality gives us that 1 is an even integer. Since we know 1 to be an odd integer, we have a contradiction. □

There are definitely a few things to point out about this process and this proof now that we've seen an example. First, notice that the contradiction didn't exactly take the form $C \wedge \sim C$, though we could have phrased it that way. Either way, we did arrive at a clearly false statement. Second, no planning went in to decide to use $\sim R$ to show that 1 is even. After several lines of manipulation it became clear that this contradiction was possible. Arguably the hardest part of proof by contradiction is recognizing your contradiction when you find it. Third, it is very likely that there are many other contradictions that can be derived from assuming $\sim R$. In general, there is no one way to write a contradiction proof. Finally, our proof ends with an explanation to our reader of why we have a contradiction. Unfortunately, this aspect is often left out of proofs by contradiction and it is the reader's responsibility to recognize the contradiction for what it is.

When we write proofs by hand, we have a few common symbols people employ to indicate the line their contradiction appears on. The most common that Dr. Wright has seen is the opposing arrows symbol ($\rightarrow\!\!\!\!\!\!\leftarrow$). Another popular symbols is the "blitzkrieg" or lightning symbol ($\lightning$). Neither symbol has any business in a formal proof and you won't find either one in standard LaTeX, so don't try typing them.

We'll need the following definition as we go forward.

Definition 9.1 (Rational) A number n is *rational*, denoted $n \in \mathbb{Q}$, if there exist integers a and b such that $n = a/b$. The number n is called *irrational* if no such integers exist.

Q6. The following proofs are written using contradiction, but no explanation is given as to what the contradiction is. Read the proof and find the contradiction.

(a) There is no greatest even integer.

Proof. Suppose for sake of contradiction that there is a greatest even integer N. Then for all $k \in \mathbb{Z}$, $n = 2k \leq N$. Let $M = N + 2$. □

(b) The sum of any rational number and any irrational number is irrational.

Proof. For the sake of contradiction, suppose there exists rational number x and irrational number y such that $(x + y)$ is rational. Then $x = {}^{a}\!/\!_{b}$ for $a, b \in \mathbb{Z}$ and $b \neq 0$ and $(x + y) = {}^{c}\!/\!_{d}$ for $c, d \in \mathbb{Z}$ and $d \neq 0$. Using substitution,

$$\begin{aligned} x + y &= \frac{c}{d}, \\ \frac{a}{b} + y &= \frac{c}{d}, \\ y &= \frac{c}{d} - \frac{a}{b}, \\ y &= \frac{cb - ad}{bd}. \end{aligned}$$

□

(c) The cube root of 2 is irrational.

Proof. Suppose for sake of contradiction that $\sqrt[3]{2}$ is rational. Then there exist integers a and $b \neq 0$ such that $\sqrt[3]{2} = (a/b)$ and we may assume that (a/b) is fully reduced. Using algebra, we see

$$\begin{aligned} 2 &= \frac{a^3}{b^3} \\ 2b^3 &= a^3. \end{aligned}$$

Since $b^3 \in \mathbb{Z}$, we have that a^3 is even which we have seen previously means that a is even. Then $a = 2c$ for $c \in \mathbb{Z}$ and using substitution again,

$$\begin{aligned} 2b^3 &= (2c)^3, \\ 2b^3 &= 8c^3, \\ b^3 &= 4c^3. \end{aligned}$$

□

Q7. It's time to write some contradiction proofs of your own. As you work on each of the following, carefully consider how you might prove the claim without contradiction.

Claim 9.4. Suppose $n \in \mathbb{Z}$. If n is odd, then n^2 is odd.

Claim 9.5. Suppose $a, b \in \mathbb{R}$. If a is rational and ab is irrational, then b is irrational.

Claim 9.6. For every $x \in [\pi/2, \pi]$, $\sin(x) - \cos(x) \geq 1$.

(Hint: If $x \in [\pi/2, \pi]$, then $\sin(x) - \cos(x) > 0$.)

Chapter 10

More on Proof: Biconditional and Existence Proofs

Believe it or not, we've actually covered all of the fundamental proof techniques. Any statement of the form "If P, then Q" can be proved using direct proof, contrapositive proof, or contradiction proof (assuming the statement can be proven at all). We will devote the remainder of the semester to writing proofs of particular kinds of statements. Often, we will still employ one of the methods mentioned above, but there are certain expectations and conventions for these types of proofs that we will follow.

Goals:

- Write Biconditional Proofs
- Prove Existence Theorems

10.1 Biconditional Proofs

Recall that a biconditional statement has the form $(P \Leftrightarrow Q)$, which is read as "P if and only if Q". This is really just short hand for $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. To prove a biconditional statement we must prove both $P \Rightarrow Q$ and its converse $Q \Rightarrow P$. In other words, we have to write two proofs in one. Generally speaking, the two pieces may require two different proof techniques. It is very common that $P \Rightarrow Q$ can be done via direct proof, but $Q \Rightarrow P$ requires proof by contrapositive or contradiction.

Directions: For each of the following claims, answer any questions and then prove the statements.

Claim 10.1. The integer n is even if and only if n^2 is even.

Q1. Determine the two conditional statements that comprise the conditional statement in the claim.

Q2. Prove the first conditional statement using any means you find appropriate.

Q3. Prove the second conditional statement using any means you find appropriate.

Q4. Combine the two proofs to prove the biconditional statement. Yes, I'm requiring that you write out everything again. Keep the following in mind: (1) the proofs of the two conditional statements must be in separate paragraphs, and (2) the second paragraph should begin with "Conversely," to indicate that you're proving the converse of the first statment. When we are writing biconditional proofs by hand, we often label the two directions with "($\Rightarrow$)" and "($\Leftarrow$)." This is usually considered inappropriate in formal proof writing, but it's a good idea while you try to get used to the technique.

Claim 10.2. Suppose $a, r \in \mathbb{Z}$, $n \in \mathbb{N}$, and $0 \leq r < n$. Then $a \equiv r (\text{mod } n)$ if and only if a has remainder r when divided by n.

Other than the fact that you have to write two proofs in one, there's really nothing new to you about writing biconditional proofs. Therefore, we'll move on to something that is new.

10.2 Equivalent Statements

If the statement "P if and only if Q" holds, then we often refer to P and Q as equivalent statements. This is because if we know that one is true then we can automatically assume that the other is also true. There are many very important theorems in math (especially in geometry and linear algebra) that are really just a list of equivalent statements. The example below gives such a list (this example is not from linear algebra).

Claim 10.3. The following statements are equivalent.

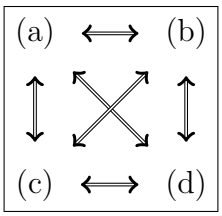
(a) The integer n is even.

(b) The integer n^2 is even.

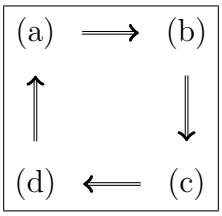
(c) The integer n^3 is even.

(d) The integer n^2 is divisible by 4.

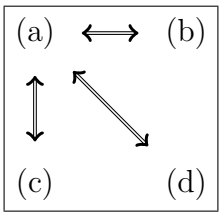
Again, by equivalent the claim means the biconditional statements $(a) \Leftrightarrow (b)$, $(a) \Leftrightarrow (c)$, $(b) \Leftrightarrow (c)$, and (c) $\Leftrightarrow$ (d) are all true. The diagram below shows the relationships between the statements.



In reality, this diagram is equivalent to the one below. If we wanted to prove the claim, it would be easiest to prove the relationships as described in the following diagram because it would require fewer proof directions.



Unfortunately, proving $(b) \Rightarrow (c)$ would be difficult, so we would have to prove this claim according to the following diagram. It requires six proof directions, but it's still the easiest way to go.



We won't actually write any equivalent statement proofs this semester. They only employ the methods we know, so ultimately they just take longer than the proofs we write otherwise. Still, you should be aware of them and prepared to see them in future courses.

10.3 Existence Proofs

Thus far we've mostly proved statements of the form $P \Rightarrow Q$. Even biconditional statements amount to proving this type of statement. We now revisit proving "existence" statements. Existence statements are statements that claim that some entity exists. They take the form

$$\exists\ x,\ P(x).$$

Recall that in the above notation, P is a statement whose truth value depends on the value of x. Proving existence statements is actually quite simple in concept. All we have to do is give

an example of the thing that's supposed to exist. Of course, our proof should also include an explanation of why our example fits the requirements of the claim.

Claim 10.4. There exists a smallest odd prime number.

Proof. The smallest odd prime number is 3. Notice that $3 = 2(1) + 1$ so 3 is odd. Also, the only natural numbers that divide 3 are 1 and 3. Finally, the odd prime numbers are a subset of the natural numbers so the Well-Ordering Principal guarantees the existence of a smallest element. Since the only natural numbers less than 3 are 1 and 2, 1 is not prime, and 2 is not odd, we know that 3 is the smallest odd prime number. □

The proof above is considered a **constructive** proof. This is because it proves that statement and constructs (or in this case provides) the smallest odd prime number. The proof below is **non-constructive**. It ensures that the smallest odd prime exists, but does not provide it.

Proof. Notice that all prime numbers are natural numbers, so the odd prime numbers are a subset of the natural numbers. As such, the Well-Ordering Principal guarantees the existence of a least element. □

It probably does not surprise you that constructive proofs are often preferred since they provide an example. However, both are acceptable in general.

Directions: Prove the following existence statements.

Claim 10.5. There exists a positive real number x for which $x^2 < \sqrt{x}$.

Claim 10.6. There exist distinct irrational numbers a and b such that ab is rational.

Chapter 11

Existence and Uniqueness

Many ideas in mathematics aren't particularly useful unless we happen to know that something is unique. For instance, the greatest common divisor of two numbers, the prime factorization of an integer, the absolute maximum of a function on a closed interval, and y-intercept of a function are all unique entities.

Goals:

- Prove Existence and Uniqueness Statements
- Use Bezout's Lemma to write proofs

We've already discussed how to prove an existence statement. Our goal now is to prove that the item that we have guaranteed to exist is also unique. In short-hand notation, we'll be proving statements of the form

$$\exists! x,\ P(x).$$

In the statement above, the "!" symbol is read as "unique."

To prove a uniqueness statement we use a process not unlike contradiction. That is, we assume that the item is not unique, and then prove this to be an absurdity. The following example demonstrates this.

Claim 11.1. If $x \in \mathbb{R}$, there exists unique $y \in \mathbb{R}$ such that $x + y = x$.

Proof. Notice that if we set $y = 0$, then $x + y = x + 0 = x$.

To prove uniqueness, assume that there exists $z \in \mathbb{R}$ such that $z \neq y$ and $x + z = x$. If $x + z = x$, we can subtract x from both sides of the equation to find that $z = 0$, so $z = y$.

Therefore, there exists unique $y \in \mathbb{R}$ such that $x + y = x$. □

Q1. Prove the following claims. Notice that they are both existence and uniqueness statements, and you'll need to prove both.

Claim 11.2. If $x \in \mathbb{R}$ and $x \neq 0$, there exists unique $y \in \mathbb{R}$ such that $xy = x$.

Claim 11.3. If $x \in \mathbb{R}$, there exists unique $y \in \mathbb{R}$ such that $x + y = 0$.

Claim 11.4. If $x \in \mathbb{R}$ and $x \neq 0$, there exists unique $y \in \mathbb{R}$ such that $xy = 1$.

Claim 11.5. If $a, b \in \mathbb{R}$ and $a < b$, then there exists unique $M \in \mathbb{R}$ such that

$$b - M = M - a = \frac{b-a}{2}.$$

(Hint: On the real line, $b - a$ is the distance between a and b.)

Existence and uniqueness proofs will be revisited later in this course and will play a major role in your upper level math course (especially Abstract Algebra and Analysis). However, our exposure to a relatively limited amount of mathematics at this point will prevent us from proving them too often.

We move on now to working with some ideas that should be familiar to you.

Definition 11.1 (Greatest Common Divisor) The *greatest common divisor* of two integers a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b.

Definition 11.2 (Prime) An integer n is *prime* if it has exactly two positive divisors, 1 and n.

Q2. Prove the following.

Claim 11.6. Suppose $a, p \in \mathbb{Z}$. If p is prime then $\gcd(a, p) = 1$ or $\gcd(a, p) = p$.

The next claim is very commonly used in basic number theory and ties together a variety of ideas in basic arithmetic. The text refers to the claim as Proposition 7.1, but the claim is so common that we will refer to it by the name Bezout's Lemma (pronounced BAY-Zoo). The text gives a proof of the claim.

Lemma 11.1 (Bezout's Lemma)**.** If $a, b \in \mathbb{N}$, then there exists $k, \ell \in \mathbb{Z}$ such that $gcd(a, b) = ka + \ell b$.

Q3. Use Bezout's Lemma to prove the following claim which is often referred to as Euclid's Lemma.

Claim 11.7 (Euclid's Lemma)**.** If $a \,|\, (bc)$ and $gcd(a, b) = 1$, then $a \,|\, c$.

Q4. Prove the following claim in two ways. First, prove the claim using Euclid's Lemma, then prove the claim using only Bezout's Lemma.

Claim 11.8. Suppose $a, b, p \in \mathbb{Z}$. If p is prime and $p \,|\, (ab)$, then $p \,|\, a$ or $p \,|\, b$.

Chapter 12

Proofs Involving Sets

Since most structures in mathematics are collections of objects, many of the proofs we write are related to sets. The proof techniques we use are the same ones we have seen before, but there are proof techniques associated with sets that work in general and are usually expected by an audience.

Goals:

- Prove that an object is an element of a set.
- Prove that a set is contained in another set.
- Prove that two sets are equal.

12.1 Proving $a \in A$

In linear algebra you must show that vectors are contained in vector spaces. In abstract algebra you must show that elements are contained in groups. In real analysis you must show that functions are contained in functional spaces. All of these structures are sets, so the proof boils down to showing that the object in question is in the set in question.

Notice, if a set is finite then there should be no issue with showing that a given element is contained in the set. Infinite sets, on the other hand, are usually defined using set builder notation, that is $A = \{x : P(x)\}$. Recall that $P(x)$ is an open sentence, and if $P(x)$ is true then $x \in A$. Otherwise $x \notin A$.

Q1. Given a set $A = \{x : P(x)\}$, what do you think you need to show to ensure that $a \in A$?

Q2. Prove that $18 \in \{x \in \mathbb{Z} : 2 \,|\, x \text{ and } 3 \,|\, x\}$.

Q3. Prove that $(2, 3) \in \big\{(x, y) : \exists\ k \in \mathbb{R} \text{ where } x^k = y\big\}$.

12.2 Proving $A \subseteq B$

Q4. If A and B are two non-empty sets, what does it mean to say $A \subseteq B$?

Q5. What steps do you think are necessary to show that $A \subseteq B$? Remember, if A and B are infinite sets then it is not possible to check if every element of A is contained in B.

Q6. Prove that $\{x \in \mathbb{Z} : 8 | x\} \subseteq \{x \in \mathbb{Z} : 4 | x\}$.

Q7. Prove that $\{x \in \mathbb{Z} : 12 | x\} \subseteq \{x \in \mathbb{Z} : 3 | x\}$.

Q8. Suppose A and B are non-empty sets. Prove $A \cap B \subseteq B$.

12.3 Proving $A = B$

Recall that two sets, A and B, are equal if they contain the same elements. Of course, this means that all the elements of A are contained in B and all the elements of B are contained in A. More succinctly,

$$A = B \Leftrightarrow (A \subseteq B \wedge B \subseteq A).$$

As such, we show two sets are equal by showing that each set contains the other. This is not the only way to show that two sets are equal, but it is the most expected method.

Q9. Prove that $\{2k + 1 : k \in \mathbb{Z}\} = \{2k + 3 : k \in \mathbb{Z}\}$.

Q10. Prove that $\{x \in \mathbb{Z} : 15 \,|\, x\} = \{x \in \mathbb{Z} : 3 \,|\, x\} \cap \{x \in \mathbb{Z} : 5 \,|\, x\}$.

Q11. Prove that $\left\{y = \sqrt{1 - x^2} : 0 \leq x \leq 1\right\} = [0, 1]$.

Sometimes this proof technique is a little clumsy, especially if we do not have specific details about the sets with which we are dealing. This happens especially when we have to prove general properties of sets. In these instances, we use the definitions for basic set structures.

Q12. Justify each step of the following proof of one of DeMorgan's Laws. Fill in the definitions below the statement of the law to help you.

DeMorgan's Law: If A and B are subsets of a universal set $\mathcal{U}$, then $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

$A \cap B =$
$A \cup B =$
$A - B =$
$\overline{A} =$

Proof. Suppose A and B are subsets of a universal set $\mathcal{U}$. Then

$$\begin{aligned}
\overline{A \cup B} &= \mathcal{U} - (A \cup B) \\
&= \{x : (x \in \mathcal{U}) \wedge (x \notin A \cup B)\} \\
&= \{x : (x \in \mathcal{U}) \wedge \sim (x \in A \cup B)\} \\
&= \{x : (x \in \mathcal{U}) \wedge \sim ((x \in A) \vee (x \in B))\} \\
&= \{x : (x \in \mathcal{U}) \wedge (\sim (x \in A) \wedge \sim (x \in B)\} \\
&= \{x : (x \in \mathcal{U}) \wedge ((x \notin A) \wedge (x \notin B))\} \\
&= \{x : (x \in \mathcal{U}) \wedge (x \in \mathcal{U}) \wedge (x \notin A) \wedge (x \notin B)\} \\
&= \{x : (x \in \mathcal{U} \wedge (x \notin A) \wedge (x \in \mathcal{U}) \wedge (x \notin B)\} \\
&= \{x : ((x \in \mathcal{U} \wedge (x \notin A)) \wedge ((x \in \mathcal{U}) \wedge (x \notin B)\} \\
&= \{x : (x \in \mathcal{U}) \wedge (x \notin A)\} \cap \{x : (x \in \mathcal{U} \wedge (x \notin B)\} \\
&= (\mathcal{U} - A) \cap (\mathcal{U} - B) \\
&= \overline{A} \cap \overline{B}.
\end{aligned}$$

□

Chapter 13

Proving That Statements Are False (Disproof)

So far we've only been concerned with proving that true statements are true. You've been handed a statement that you've been told is true and asked to prove the statement. Even knowing that the statement is true, you may still have found it difficult to develop an appropriate proof. Reality is more complicated. Mathematicians spend most of their time making conjectures and trying to prove them. However, not being able to develop a proof isn't the same as a conjecture being false. Here we'll discuss common methods to prove that statements are false.

Goals:

- Determine what is necessary to prove that a universal statement is false.
- Determine what is necessary to prove that a conditional statement is false.
- Determine what is necessary to prove that an existence statement is false.

13.1 Basic Disproof

Q1. Consider the statement P: "It rains every day." We know that this statement is false, but how can we demonstrate that this statement is false?

Q2. Write the statement $\sim P$ in English. Try to do better than "It does not rain every day."

Q3. By demonstrating that P is false, have you said anything about $\sim P$?

Q4. Now consider the statement Q : There exist $x, y \in \mathbb{R}^+$ such that $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$. Hopefully you recognize that this statement is false. What would you have to do to show that this statement is false?

Q5. Would your argument in the above question say anything about $\sim Q$?

Q6. What do you think is the fundamental structure of an argument to show that a statement is false? Hint: Are you proving that anything is true by proving that a statement is false?

13.2 Disproving Universal Statements

Recall that a universal statement has the generic form $\forall x, P(x)$. They are arguably the simplest type of statement to prove false.

Q7. Suppose Q is the following statement: $\forall x, P(x)$. Based on your work in the first section, how do you think you can disprove Q.

Q8. In symbolic logic, what does the statement $\sim Q$ look like?

Q9. Consider the statement "For all positive real numbers a and b, $a + b < 2\sqrt{ab}$." What statement would you prove to show that this statement is false?

Q10. What type of proof would be required in the above question? What is the format for such a proof?

The examples used to disprove universal statements are called **counterexamples**. You should keep in mind that it is the responsibility of the proof writer, and not the proof reader, to explain why a given counterexample is in fact a counterexample. Often times textbooks will expect the reader to determine why something is a counterexample for the students benefit, but this is unacceptable in most work.

13.3 Disproving Conditional Statements

Q11. When is the conditional statement $P \Rightarrow Q$ false?

Q12. Based on your work in the first section, how can you show that $P \Rightarrow Q$ is false?

Q13. What do you need to do to disprove the statement "If $x, y \in \mathbb{R}$, then $\dfrac{x}{x+y} = \dfrac{1}{1+y}$." Keep in mind that you could rephrase this statement as
"For all $x, y \in \mathbb{R}$, $\dfrac{x}{x+y} = \dfrac{1}{1+y}$."

13.4 Disproving Existence Statements

Recall that an existence statement has the form "$\exists x,\ P(x)$."

Q14. Disproving an existence statement requires some real work. Why do you think this is the case?

Q15. What would you have to do to prove that "There exist distinct prime numbers a and b such that $a + b > ab$" is a false statement? Prove this statement is false.

Chapter 14

Basic Induction

Proof by induction is a technique that allows us to prove a variety of statements that have one thing in common: the "objects" the statement refers to are in correspondance with the natural numbers. Often times we use induction to prove statements about the natural numbers, but the method applies in a surprising variety of situations.

Unlike many of our proof techniques, a proof by induction does follow a certain form to which we must adhere. This form is necessary for both the validity of the method, and for others to be able to understand our proofs.

Goals:

- Follow along with the steps of an induction proof
- Write a basic induction proof

Q1. Follow along with the induction proof below and answer the questions as you go.

Claim 14.1. For all $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

(a) This claim establishes a lot. If we let $P(n)$ be the statement "$1+2+3\cdots+n = \frac{n(n+1)}{2}$," then our claim becomes $\forall\ n \in \mathbb{N}, P(n)$. What is the statement $P(1)$? What about $P(2)$? Are these statements true?

(b) By checking that $P(1)$ is true above, you actually did the first step of the induction proof. This step is known as the "Basis" step. Checking that $P(2)$ is true is not part of the basis step, but it never hurts to check a few values.

(c) The next step of induction is the "induction step." The goal here is to show that $P(n) \Rightarrow P(n+1)$. That is, we will show that "If $P(n)$ is true, then $P(n+1)$ is true." What do you think is the purpose of the induction step, keeping in mind that we've already established that $P(1)$ is true?

(d) We almost always use a direct proof to show that $P(n) \Rightarrow P(n+1)$. That is, we will suppose that $P(n)$ is true and use it to show that $P(n+1)$ is true. What is the statement $P(n)$? What is the statement $P(n+1)$?

(e) The proof below shows that $P(n) \Rightarrow P(n+1)$. Follow along with the proof and justify each step.

Proof. Suppose $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$. Then

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

Therefore, if $1+2+\cdots+n = \frac{n(n+1)}{2}$ then $1+2+\cdots+n+(n+1) = \frac{(n+1)((n+1)+1)}{2}$. □

(f) Together, the basis step and the induction step make up a proof by induction.

Q2. The following is a proof of the same claim. The proof correctly follows the format of a proof by induction, but contains a severe flaw. See if you can find the mistake.

Claim 14.2. For all $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

Proof. We proceed by mathematical induction.
Basis Step: Notice that when $n = 1$ the statement becomes $1 = \frac{1(1+1)}{2}$, which is obviously true.

Induction Step: Suppose $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$. Then

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

Since the last statement if obviously true, if $1+2+\cdots+n = \frac{n(n+1)}{2}$ then $1+2+\cdots+n+1 = \frac{(n+1)(n+2)}{2}$. □

Q3. Prove the following claim using mathematical induction.

Claim 14.3. If $n \in \mathbb{N}$, then $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Proof. We proceed by mathematical induction.
Basis Step:

Induction Step:

□

Chapter 15

General Induction

Since induction proofs have a standard form, proving a claim about the natural numbers that involves an equality is usually pretty straightforward. Usually the only real challenge is the algebraic manipulations that are required during the induction step.

Induction may seem more complicated if the statement is about an inequality, but the same techniques still apply. Often times students just struggle to make the necessary observations while writing the proof. Keep in mind that proof writing always has a goal and you can do anything necessary to reach that goal as long as it is mathematically valid.

Goals:

- Justify the steps of an induction proof involving an inequality
- Write an induction proof that contains an inequality
- Write an induction proof about an object other than a natural number

Q1. Follow along with the induction proof below and answer the questions as you go.

Claim 15.1. For all $n \in \mathbb{N}$, $3^n \leq 3^{n+1} - 3^{n-1} - 2$.

(a) If $P(n)$ is the statement "$3^n \leq 3^{n+1} - 3^{n-1} - 2$," what is the statement $P(1)$? What about $P(2)$? Are these statements true or false?

(b) The induction step for this proof follows below. Justify each line of the proof.

Proof. Suppose $3^k \leq 3^{k+1} - 3^{k-1} - 2$ for $k \geq 1$. Notice

$$\begin{aligned} 3^{k+1} &= 3 \cdot 3^k \\ &\leq 3(3^{k+1} - 3^{k-1} - 2) \\ &\leq 3^{k+2} - 3^k - 6 \\ &\leq 3^{(k+1)+1} - 3^{(k+1)-1} - 6 + 4 \\ &\leq 3^{(k+1)+1} - 3^{(k+1)-1} - 2. \end{aligned}$$

Thus, if $3^k \leq 3^{k+1} - 3^{k-1} - 2$ then $3^{k+1} \leq 3^{(k+1)+1} - 3^{(k+1)-1} - 2$. □

(c) The inequality symbol "$\leq$" is used throughout the above proof. Could it be replaced by an equality symbol ($=$) or a strict inequality symbol ($<$) at any line? Why do you think the proof writer chose to use the symbol "$\leq$" throughout?

Q2. Prove the following claim.

Claim 15.2. If $n \in \mathbb{N}$, then

$$\frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

Q3. Prove the following claim using induction.

Claim 15.3. Suppose A_1, A_2, ..., A_n are sets in some universal set U and $n \geq 2$ is a natural number. Then

$$\overline{A_1 \cup A_2 \cup \cdots A_{n-1} \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{n-1}} \cap \overline{A_n}.$$

Chapter 16

Strong Induction

Goals:

- Compare strong induction to induction
- Write a proof by strong induction
- Determine when strong induction is necessary or appropriate.

Strong induction is a proof technique based on induction, but with a small variation. Recall that in the induction step of an induction proof we assume the statement $P(n)$ is true (usually for some $n \geq 1$) and use this to prove that $P(n+1)$ is true. In strong induction, we instead use $P(k)$ to prove $P(n+1)$ where k is some natural number less that $n+1$. If we use our stairs analogy from class, this would be like skipping stairs a few at a time rather than going up one step at a time.

We have to adjust the base step when using strong induction. For example, suppose we will use $P(n)$ to prove $P(n+3)$ in a strong induction proof. This would be like going up our staircase 3 steps at a time. Remember, our goal isn't getting to the top of the staircase necessarily, but rather showing that you can get on every stair (that is, $P(n)$ is true $\forall n \in \mathbb{N}$). Since our proof technique requires that we skip 3 stairs at a time, we have to ensure that we can get onto the first 3 steps. Then, if we can get onto each of the first three stairs and go up three at a time, we can get onto any stair that we wish.

There are essentially two situations in which strong induction is appropriate. The first is when $P(n)$ alone isn't enough to ensure that $P(n+1)$ is true. This happens when our statements require several previous cases as you'll see below. The other situation, which appears on page 159, is when $P(n)$ may imply $P(n+1)$, but we can't come up with a proof to ensure that it is true. You should take a look at the example, but bare in mind that it is a ridiculous application of strong induction. A much simpler direct proof is possible.

Q1. The following claim has the perfect setup for strong induction.

Claim 16.1. For the following recursively defined sequence, a_n is odd for all $n \in \mathbb{N}$. Here $a_1 = 1$, $a_2 = 3$, and $a_n = a_{n-2} + 2a_{n-1}$ for $n \geq 3$.

(a) Find the first 5 items in this sequence.

(b) Here, for $n \geq 3$, the statement $P(n)$ is "$a_n = a_{n-2} + 2a_{n-1}$ is odd." Since this statement refers explicitely to the $n-2$ and $n-1$ terms of our sequence, we need to consider these items in our basis step. Determine what the statements $P(1)$ and $P(2)$ are, and determine if they're true.

(c) The remainder of the proof is very similar to the induction step in any induction proof. Many of the justifications are left out of the proof. As you read the argument, explain why each step is true.

Proof. Suppose a_n is odd for $n \geq 3$. Then consider

$$\begin{aligned} a_{n+1} &= a_{n-1} + 2a_n \\ &= (2k+1) + 2(2m+1) \\ &= 2k + 1 + 4m + 2 \\ &= 2(k + 2m + 1) + 1. \end{aligned}$$

Therefore a_{n+1} is odd. □

Q2. Prove the following claim.

Claim 16.2. Let a sequence be defined by $T_1 = T_2 = T_3 = 1$, and $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ for $n \geq 4$. Then $T_n < 2^n$ for all $n \in \mathbb{N}$.

Chapter 17

Relations and Functions

We'll now a make a major change in the focus of the course. Up to this point, our focus has been on learning techniques to write proofs. Along the way we've had to learn a few new concepts to have something new to write proofs about. The remainder of our time will be devoted to learning to concepts and we'll write proofs about them along the way.

Goals:

- Discuss and define relations
- Write common relations using set-builder notation
- Explore functions as relations

17.1 Relations

Every major concept in mathematics can be described entirely using sets. This isn't exactly exciting news for many first-year mathematics students. However, it is an important property to observe if we're going to view some concepts in a light that will allow us to write proofs about them.

Q1. Let's pretend that you're teaching an elementary school class and you need to teach the students how to properly use the less than symbol "$<$." To keep things simple, we'll focus entirely on the integers in the set $A = \{1, 2, 3, 4, 5\}$. The students need to see some examples, so write down every possible correct use of the "$<$" symbol for this set.

Q2. Repeat the same process for the "$=$" symbol and the set A in question 1.

In the examples above, there's nothing particularly special about the "$<$" and "$=$" symbols. That is, the symbols themselves don't really have any meaning. It's the elements that we put the symbols between that really matter. We could choose to represent this same information with the sets

$$R_< = \{(1,2),(1,3),(1,4),(1,5),(2,3),(2,4),(2,5),(3,4),(3,5),(4,5)\},$$
$$R_= = \{(1,1),(2,2),(3,3),(4,4),(5,5)\}.$$

This probably doesn't seem particularly beneficial to you. However, it does completely encode the important information about "less than" and "equal to" for the set A, without ever having to define what "less than" or "equal to" actually mean. This can be pretty handy for a more complicated idea.

The concepts of "less than" and "equal to" are *relations*. Simply put, relations describe relationships between things. Since this is math class, the "things" are the elements of some sets. There are an infinite number of possible relations and many of them are very different. As a result, the defintion of a relation may seem a little strange.

Definition 17.1 (Relation) A *relation* R between a set A and a set B is a subset $R \subseteq A \times B$. We abbreviate the statement "$(x,y) \in R$" as xRy which is read aloud as "x is related to y". If $(x,y) \notin R$ we write $x \not R y$. Often, $A = B$.

Notice that a relation on a set A is a subset of the Cartesian product $A \times B$. That means that the elements of a relation are ordered pairs. Each ordered pair tells you that those two elements are related. The notation above may seem strange, but it's really no different than writing "$x < y$" or "$x = y$." Keep in mind that we're not saying that the symbol "$<$" is a set, we're saying that the relationship it describes is a set. Also, if the set A or B changes, then the elements that are related by "$<$" change as well. This is why a relation is a subset of $A \times B$ and not defined on its own terms.

Q3. Going by the definition above, do you think the order of the items in each ordered pair matters? Why?

Q4. Let $A = \{2,3\}$.

(a) What is $A \times A$? List all of its elements.

(b) What is $\mathscr{P}(A \times A)$? List all of its elements.

(c) Notice that $\mathscr{P}(A \times A)$ contains every possible subset of $A \times A$. That means that you have now listed every possible relation for the set A. Which of the relations are familiar to you and what common symbol do they represent?

Q5. Let $B = \{-2, -1, 0\}$. Express the relation "$\geq$" on B as a set of ordered pairs.

So far, we've only discussed relations on finite sets. Of course, "$<$," "$=$," and "$\geq$" can all be thought of on the infinite sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, etc. We can't possibly list all of the necessary ordered pairs for infinite sets, so we have to use set-builder notation instead.

Q6. The set $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : (x - y) \in \mathbb{N}\}$ describes a common relation. Determine what relation it is.

Q7. Describe the divides relation "$|$" on $\mathbb{Z}$ using set-builder notation. (Remember that you can't use the divides symbol nor the word "divides" to define the relation.)

Q8. Congruence modulo 7 is a relation on $\mathbb{Z}$. Describe the relation using set builder notation. In this example xRy if and only if $x \equiv y \pmod 7$.

We could probably spend several weeks discussing relations. Since we don't have many weeks left, this probably isn't the best use of our time. Be assured, you'll spend a lot of time discussing relations in your Geometries, Abstract Algebra, Calculus 3, and Linear Algebra classes. We'll move on to discussing the most common example of a relation: a function.

17.2 Functions

When Dr. Wright asks his students to define functions in classes, he invariably gets slightly different versions of the following three answers.

1. Like $f(x)$ is x^2 or like $\sin(x)$ or something.

2. It passes the vertical line test.

3. A rule that takes input and gives output.

None of these answers are wrong, but none of them are particularly good either. The first response is an example at best. Many functions cannot be described using $f(x)$ (or with any algebraic formula for that matter). The second answer shows a little more recognition, but there are lots of functions for which the idea of a vertical line test doesn't even make sense. Ask your classmates in Calculus 3 about them some time. The third answer is starting to get somewhere, but it's not strict enough to pin down what it really means. (As a future teacher, you should be terrified of definitions like #3. Trying to explain a bad definition to a student who doesn't understand the concepts is like trying to shave a cat. It's messy, it hurts, and in the end you won't like each other very much.) In reality, a function is a special type of relation.

Definition 17.2 (Function) Suppose A and B are sets. A *function* f from A to B, denoted $f : A \to B$, is a relation $f \subseteq A \times B$ from A to B with the property that for each $a \in A$, f contains exactly one ordered pair of the form (a, b). We abbreviate $(a, b) \in f$ by $f(a) = b$.

Q9. How is the definition of a function different from the definition of a relation?

Q10. Does the definition indicate that every element $a \in A$ must be related to something by the function $f : A \to B$?

Q11. Does the definition indicate that every element $b \in B$ must be related to something by the function $f : A \to B$?

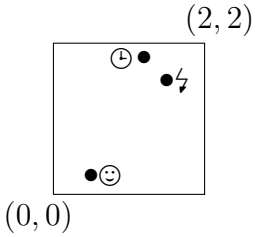
Q12. Consider the Birthmonth Function, m. The two sets for our Birthmonth Function will be the individuals in our class and the month of their birth. For your group, write down the set A of people in your group and the set B of months of your birth.

(a) Is $m : A \to B$ a function for your group? Is it the same for the other groups in the class?

(b) Is $m : B \to A$ a function for your group? Is it the same for the other groups in the class?

Q13. Consider the Birthmonth Function, $m : A \to B$, again where A is an unknown group of people and B is their birth months. What are the elements in B? That is, what are the *possible* outputs of the function? Is it the same as all the actual outputs?

Q14. One of Dr. Wright's favorite functions for examples is the archery function $a : Q \to T$. For the archery function, we have 3 labelled arrows that will be shot at a square target. When the arrows hit the target, their coordinates on the target are recorded. In the example that follows, the arrows are represented by labelled dots.



(a) What are the possible "inputs" for the function? That is, what elements are in the set Q?

(b) What are the possible "outputs" for the function? That is, what elements are in the set T?

(c) Is every element in T hit by an arrow?

In the two previous examples of functions, the things that could get "hit" by the function and what actually got hit were not the same. This is one of the issues that sometimes comes up

when discussing the range of a function. In higher levels of math, we clarify these issues with the following definitions.

Definition 17.3 (Domain, Codomain, & Range) For a function $f : A \to B$, we call the set A the **domain** of f. We call the set B the **codomain** of f. We call the set $R_f = \{b \in B : \exists\ a \in A \text{ for which } f(a) = b\}$ the **range** of f.

In the above definition, the domain is the set of all "inputs" of the function. Technically speaking, a function must be defined for all elements of its domain or it's not a function. The codomain is the collection of all possible "outputs." In our archery example the codomain was all coordinates on the target. In the birthday example the codomain is all of the calendar months. These are the things that could get hit by the function, but are not necessarily hit by the function. Finally, the range is the collection of "outputs," that is, the things that are actually hit by the function.

Q15. Let $A = \{1, 5, 7, 9, -2, 10\}$ and $B = \{\Delta, \Psi, \Omega, \xi, \Sigma, \Pi, \Lambda, \Gamma\}$ and let $f : A \to B$ be defined by

$$f = \{(1, \Omega), (5, \Psi), (7, \Omega), (9, \xi), (-2, \xi), (10, \Delta)\}.$$

List the domain, codomain, and range of f.

Q16. Consider the more traditional function $f(x) = \sin(x)$. Give the implied domain, codomain, and range of f.

Q17. Consider the ceiling function $f(x) = \lceil x \rceil$. Recall that this function tells you to round up to the next integer so that $f(1) = 1$, $f(1.1) = 2$, $f(1.5) = 2$, etc. Determine the domain, codomain, and range of f. Is there more than one possible codomain? Is there more than one possible range?

Chapter 18

Injections and Surjections and Bijections...Oh My!

While functions can have any number of various properties, none are more important than injectivity, surjectivity, and bijectivity. More commonly you know of injective as "one-to-one" and surjective as "onto."

Goals:

- Define injection, surjection, and bijection
- Prove that functions have these properties

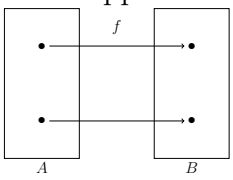
You've undoubtedly heard the terms "one-to-one" and "onto" at some point in your mathematics education, but to be fair you probably don't have a strong grasp on these concepts. Part of this is because the functions that you normally see that are defined on the real numbers make these concepts more complicated than they need to be. Let's start with injectivity.

18.1 Injections

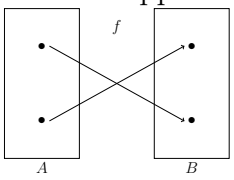
Definition 18.1 Let $f : A \to B$. For $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$ implies that $a_1 = a_2$, then we say that f is *injective* or *one-to-one*.

What this definition says is that a function is injective if any output that gets hit only gets hit by one input. So

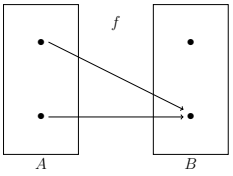
This happens:



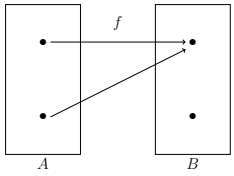
Or this happens:



Not this:



Nor this:



A function might be one-to-one as opposed to two-to-one. The common function $f(x) = x^2$ is two-to-one because each output of the function gets hit by two inputs. For instance 4 gets hit by 2 and -2, 9 gets hit by 3 and -3, etc. By definition, if something is one-to-(a number bigger than one) then it's not a function. We call such things *maps*.

Q1. Is the Birthmonth function injective for your group? Why or why not?

Q2. Is the archery function injective? Explain your answer.

The definition given above for injection is the most common because it's the simplest to understand (that's debatable). The next definition requires that you recall what the range of f, denoted R_f, is.

Q3. For $f : A \to B$, what is R_f? Give the name of R_f and its description in set-builder notation.

Definition 18.2 The function $f : A \to B$ is *injective* if for all $b \in R_f$ there exists a unique $a \in A$ such that $f(a) = b$.

The benefit of this new definition is that it tells us that to prove a function is injective, we need to write a uniqueness proof.

Q4. How do you prove something is unique?

Q5. Read the following injection claim and proof and justify the steps.

Claim 18.1. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = -2x + 1$ is injective.

Proof. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = -2x + 1$ and for sake of contradictions suppose there exists distinct real numbers a and b such that $f(a) = f(b)$. Then

$$\begin{aligned} -2a + 1 &= -2b + 1 \\ -2a &= -2b \\ a &= b. \end{aligned}$$

This is a contradiction, so $f(a) \neq f(b)$ when $a \neq b$. Therefore f is injective. □

Q6. Prove that $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^3$ is injective.

Q7. Prove that $h : \mathbb{R}^+ \to \mathbb{R}$ given by $h(t) = \sqrt{t}$ is injective.

Q8. Prove that $s : \mathbb{R} \to \mathbb{R}$ given by $s(t) = \sin(t)$ is not injective.

18.2 Surjections

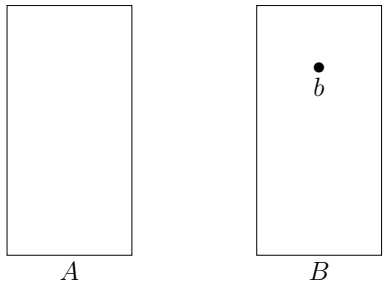
The idea of a surjection (or onto function) is actually really simple. Dr. Wright is convinced that the only reason anyone ever struggles with it is because they weren't taught the difference between a range and a codomain. Two equivalent definitions for surjective follow. The first one tells us what surjective really means, but the second tells us how to prove a function is surjective.

Definition 18.3 Let $f : A \to B$. Then f is *surjective* or *onto* if $R_f = B$.

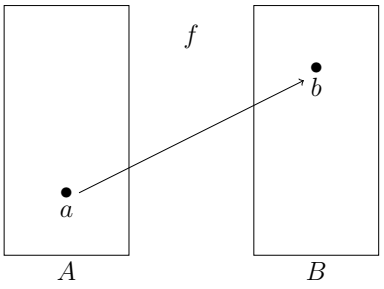
Definition 18.4 Let $f : A \to B$. Then f is *surjective* or *onto* if for all $b \in B$, there exists $a \in A$ such that $f(a) = b$.

In pictures,

If we have this,...



then we have this.



From these definition, we can tell that proving that a function is surjective means writing an existence proof.

Q9. Read the following proof that $f(x) = \sqrt[3]{x}$ is surjective and answer the questions that follow.

Proof. Suppose $f(x) = \sqrt[3]{x}$ and suppose $b \in \mathbb{R}$. Let $a = b^3$. Then $f(a) = f(b^3) = \sqrt[3]{b^3} = b$. Thus, for all $b \in \mathbb{R}$, there exists $a \in \mathbb{R}$ such that $f(a) = b$. □

(a) Does the proof tell us where letting $a = b^3$ came from? Should the proof tell us how to find the appropriate a?

(b) Remember that one way to think about a surjection is $R_f = B$. The proof has shown that $B \subseteq R_f$. Why doesn't it need to show that $R_f = B$?

Q10. Prove that $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = 5x + 7$ is surjective.

Q11. Prove that $g : \mathbb{R} - \{0\} \to \mathbb{N}$ given by $g(x) = \lceil x^2 \rceil$ is surjective.

Q12. Another way to say that function is surjective is to say is "maps A onto B." For a function f with domain D, is it true that f maps D onto R_f? Why or why not?

18.3 Bijectivity

The best thing about bijections is that they're really nothing new.

Definition 18.5 For $f : A \to B$, f is a *bijection* if it is both injective and surjective.

Q1. For each of the following, determine if the function is an injection, surjection, or bijection for the given sets. Prove your conclusion either with an appropriate proof or counterexample.

(a) When $f : \mathbb{R} \to \mathbb{R}$ is given by $f(x) = e^x$.

(b) When $f : D \subseteq \mathbb{R} \to \mathbb{R}$ is given by $f(x) = \tan(x)$.

(c) When $f : \mathbb{Z} \to \{0, 1, \ldots, 9\}$ is given by $f(x) = 2x \pmod{10}$. (Remember to interpret this as a function. Substitute a value for x then find the remainder mod 10 to evaluate. For example, $f(7) = 2(7) \pmod{10} = 14 \pmod{10} = 4$ so $f(7) = 4$.)

(d) When $f : \mathbb{Z} \to \{0, 1, 2\}$ is given by $f(x) = 2x \pmod{3}$.

Chapter 19

Inverses, Images, and Preimages

Every student that has gone through Calculus I has encountered inverse functions extensively. In some instances you were able to explicitly solve (algebraically) for an expression that gave an inverse function. In other instances inverses were more intangible. Recall that there is no formal definition for the natural log function nor the inverse trig functions other than the fact that they are inverses. With our newfound mastery of functions we can explore these concepts in more detail.

Goals:

- Define inverses, images, and preimages of functions
- Determine what kind of functions have inverses
- Find inverses, images, and preimages for various functions.

19.1 Inverses

Q1. Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = -2x + 1$. Find the inverse of f, f^{-1}, using the techniques you learned in algebra.

Often times in advanced mathematics there is no algebraic description for our function. Certainly this means that there is no way to solve for the inverse of the function. In this situation we need a definition for an inverse that doesn't rely on an equation or a graph. Recall that a function is a relation before reading the next definition.

Definition 19.1 (Inverse) Suppose $f : A \to B$ is a function. Then the *inverse* of f, denoted f^{-1}, is the set

$$f^{-1} = \{(y, x) : (x, y) \in f\}.$$

The above definition says some pretty important things. First, we can always construct the inverse of a function simply by flipping the ordered pairs that are elements of the function. This

may seem odd, but in reality this is precisely how we get the graph of functions like $y = \ln(x)$ and $y = \arctan(x)$. Second, there's no reason to think that the inverse of a function is itself a function.

Q2. Let $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d\}$, $C = \{K, L, M\}$, and $D = \{\phi, \psi, \theta\}$ and consider the following functions

$$\begin{aligned} f &: A \to B & f &= \{(1, a), (2, a), (3, c), (4, b), (5, d)\} \\ g &: C \to B & g &= \{(K, a), (L, d), (M, c)\} \\ h &: D \to C & h &= \{(\phi, M), (\psi, K), (\theta, L)\} \\ j &: B \to A & j &= \{(a, 2), (c, 1), (b, 3), (d, 5)\}. \end{aligned}$$

(a) Which of the functions is injective? Which is surjective? Bijective?

(b) For which of the above functions is the inverse also a function? Make sure you consider domains and codomains as you answer.

(c) What properties do you think a function f must have to ensure that f^{-1} is a function? Be careful, it may not be the same as what you were taught in algebra.

19.2 Images and Preimages

There's a surprising amount of disagreement about the appropriate definitions for some terms in mathematics. For the most part it doesn't matter, but individual authors tend to have their own preferences. This is definitely true with the definition of an image. The author of our textbook and Dr. Wright disagree on this definition in a subtle way. For the purposes of this course, we'll go with Dr. Wright's definition. However, in practice, you'll always need to double check these definitions when they come up. In most textbooks above the sophomore level, there is a preliminary chapter devoted to establishing the definitions of these common terms.

Definition 19.2 (Dr. Wright's Image) Let $f : A \to B$. If $x_0 \in A$ then we call $y_0 = f(x_0)$ the *image* of x_0 under f. If $X \subseteq A$, we also call $f(X) = \{f(x) : x \in X\} \subseteq B$ the *image* of X under f.

Definition 19.3 (Book's Image) If $f : A \to B$ and $X \subseteq A$, then the *image* of X is the set $f(X) = \{f(x) : x \in X\} \subseteq B$.

The only real difference here is that Dr. Wright likes to be able to refer to the output of a particular input as an image. There is almost no disagreement about the next definition.

Definition 19.4 (Preimage) Let $f : A \to B$. If $Y \subseteq B$, the *preimage* of Y is the set $f^{-1}(Y) = \{x \in A : f(x) \in Y\} \subset A$. If the invertibility of f is unknown and $y_0 \in B$, then the *preimage* of y_0 is the set $f^{-1}(y_0) = \{x \in A : f(x) = y_0\}$.

Q3. Let $f : \{\bigcirc, \Delta, \square, \heartsuit, \lightning, \odot, \leftmoon, \checkmark\} \to \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be given by

$$f = \{(\bigcirc, 0), (\Delta, 2), (\square, 2), (\heartsuit, 2), (\lightning, 5), (\odot, 9), (\leftmoon, 0), (\checkmark, 8)\}.$$

(a) Determine each of the following.

(i) $f(\{\bigcirc, \square, \heartsuit, \odot\})$

(ii) $f(\{\bigcirc, \heartsuit, \lightning\})$

(iii) $f(\{\checkmark, \odot\})$

(iv) $f^{-1}(\{1\})$

(v) $f^{-1}(\{0, 2, 9\})$

(vi) $f^{-1}(\{2, 5, 8\})$

(b) Is f a bijection? Explain.

(c) Is f^{-1} a function? Explain.

Chapter 20

To Infinity and Beyond: Countability and Cardinality

It is now time to put our newfound knowledge of functions to some good use. Somewhat surprisingly, we will be using that knowledge to "count" the number of elements in sets.

Goals:

- Define countability for sets
- Compare cardinalities of different sets

Before beginning, your textbook really does a great job of exploring cardinality and countability in chapter 13. You should absolutely read the chapter. We'll be taking a slightly different approach here just so you feel like you are getting more out of class than an exploration of the textbook. The two together should make a great resource.

20.1 Countability

We begin by exploring what it means to be able to count the number of elements in a set. Of course, if the set is finite then we shouldn't have any trouble (as long as the set isn't too complicated). What if the set is infinite? We realize that this means we will never finish counting the elements in the set, but that doesn't mean we couldn't make progress if we tried.

Let's start by considering the integers. In the table below, elements of the integers appear on in the second row. We'll count using the natural numbers just like you have for your entire life.

Counter	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
Integers	0	1	-1	2	-2	3	-3	4	-4	5	-5	$\cdots$

Table 20.1: Counting the Integers

Q1. Using this counting method, what will your counter be when you get to the integer -11?

Q2. Is there an integer you couldn't eventually get to by listing the integers in this way?

In some sense, saying that we can count a set means that we can order its elements in a way that will allow us to reach all elements eventually.

Q3. Provide a method for counting both the even integers and the odd integers below.

If we're going to talk about counting infinite sets, we should have an example of an infinite set that is not countable. That is, no matter how long we count there will always be numbers in the list that we can't reach. The set $\{x \in \mathbb{R} : 0 < x < 1\}$ is such a set. You know this set more commonly as the open unit interval $(0, 1)$. The proof that this set is uncountable is surprisingly only about 150 years old, which is pretty young in mathematics. You'll write a formal proof later, but for now let's just explore the idea.

The argument proceeds by contradiction, so it starts off by assuming that we have an ordering for the numbers in the unit interval that let's us count them. Suppose the table below is the start of such a list.

Counter	Real Number
1	$0.567458720384\ldots$
2	$0.103910000000\ldots$
3	$0.9001928491001\ldots$
4	$0.000000010000001\ldots$
5	$0.25999987453321\ldots$
6	$0.888888888888888\ldots$
7	$0.121212121212121212\ldots$
$\vdots$	$\vdots$

When we build our table we use the decimal forms of the numbers and we list an infinite number of zeros at the end of numbers with a finite amount of decimal places. To form our contradiction, we construct a number that is not in the list.

Q4. The number we construct must be between 0 and 1, so it will start with "0.". We construct the number one decimal place at a time. To form the first digit after the decimal, go to the first digit after the decimal of the first number. If that digit is a 0 write a 1. If that digit is anything other than 0, write a 0. Proceed by going to the second digit of the second number to get the next digit. Construct the number for the list above.

Q5. Could you construct such a number for any list of the reals in the unit interval? Explain. What does that tell you about our ability to build a list of the numbers in the unit interval?

Having played around with the idea of countability, let's see a formal definition.

Definition 20.1 (Countable) The set A is *countable* if $|A|$ is finite or if there exists a bijection, $f : \mathbb{N} \to A$.

Looking at Table 20.1, we see that we have defined a bijection from the naturals to the integers. Notice that we don't need to provide a formula (an $f(x)$ if you will) to describe the bijection.

Q6. It should come as no surprise that the positive even integers are also countable. Provide the necessary bijection.

Q7. Provide a bijection that shows that the positive multiples of 10 are countable.

20.2 Cardinality

The idea of countability brings with it a very important question: "So what?" If a set is infinite and countable, is that really any different from being infinite and uncountable? The blunt answer is no, both sets are still infinite. However, that doesn't mean we can't gain some interesting insights about infinity if we start comparing the cardinalities of infinite sets.

We were able to define a bijection between $\mathbb{N}$ and $\mathbb{Z}$. In some sense, that means for each natural number there is exactly one integer. We were also able to find a bijection from $\mathbb{N}$ to the even integers. Putting the two ideas together suggests that there are as many even integers as there are integers. There is no bijection between $\mathbb{N}$ and $(0, 1)$, therefore they can't have the same number of elements.

Definition 20.2 (Same Cardinality) Two sets A and B have the *same cardinality*, denoted $|A| = |B|$, if there exists a bijection between A and B.

Q8. Find a bijection from $(0, 1)$ to $(0, 100)$ to prove that $|(0, 1)| = |(0, 100)|$. (Don't try too hard. The simplest type of function possible should do it.)

Q9. Let $a, b, c, d \in \mathbb{R}$. Find a bijection from the interval (a, b) to the interval (c, d) to show that any bounded interval of real numbers has the same cardinality.

Q10. Find a bijection from $(0, 1)$ to $(-\infty, \infty)$ to show that $|(0, 1)| = |\mathbb{R}|$. (Hint: You'll need to come up with a function that is capable of mapping a bounded interval to $(-\infty, \infty)$ and make adjustments from there.)

Q11. Find a bijection from $\mathbb{N}$ to a proper subset of $(0, 1)$. (Let fractions be your guide.) Can you now conclude that there are more elements in $(0, 1)$ than there are in $\mathbb{N}$?

Of course, there are times when finding a bijection isn't quite so simple. In this case, we have to accept the fact that we may not be able to provide a formula for our bijections. That doesn't mean we can't describe it.

Q12. It can be shown that the rational numbers, $\mathbb{Q}$, are countable. The book provides the full argument, but here we'll just show that the positive rationals are countable. (The arguments are nearly identical.)

The trick is finding a way to list the rationals to show that they are countable. Such a list is given below, but the 2D array doesn't really prove anything. Can you come up with the necessary ordering of the rationals to show that they are countable? Note, you can't just go across a row or down a column because you would never get to the numbers in the neighboring rows or columns.

$$\begin{array}{cccccccc}
\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \frac{6}{1} & \cdots \\
\frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \frac{6}{2} & \cdots \\
\frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \frac{6}{3} & \cdots \\
\frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \frac{6}{4} & \cdots \\
\frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} & \frac{5}{5} & \frac{6}{5} & \cdots \\
\frac{1}{6} & \frac{2}{6} & \frac{3}{6} & \frac{4}{6} & \frac{5}{6} & \frac{6}{6} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

Providing bijections between sets to prove they are somehow the same is one of the cornerstone methods of mathematics. It's vital in analysis to go between sequences; in algebra to go between groups, rings, and fields; in Linear Algebra to go between vector spaces; it's the fundamental concept behind all of manifold theory; and its subtly hidden throughout Calculus 3, Differential Equations, and Discrete Dynamics. You will see it again.

20.3 Hilbert's Hotel

David Hilbert is one of the most influential mathematicians of recent times. He is one of several individuals responsible for our modern, rigorously proof based approaches to mathematics. Further, he posed 23 problems during his life that largely influenced the world of mathematical research during the 20^{th} century. The following thought experiment is named in honor of him.

The Grand Hilbert Hotel is a historic landmark of immense size. It features a countably infinite number of rooms (with all the amenities) numbered according to the natural numbers. During the 42^{nd} Fancy Cat Festival, the hotel was proud to boast that it had filled all of its rooms. However, as we all know, the Fancy Cat Festival draws quite a crowd. The day before the festival was to begin, a countably infinite number of guests showed up looking for rooms. Despite being fully booked, the Grand Hilbert staff found a way to free up an infinite number of rooms by simply having guests move to other rooms. Can you suggest a room changing scheme that can accommodate everyone? (Remember to avoid the elevator during the switching. It's likely to be busy for some time.)

Chapter 21

Which is bigger: $\mathbb{R}$ or $\mathbb{R}^2$? They're the same?! Never mind then.

21.1 Comparing Infinite Cardinalities

We have worked out that $|\mathbb{N}| \neq |(0,1)|$. This means we definitely have two different types of infinity, but how do they compare? Recall that we showed $|\mathbb{N}| \neq |(0,1)|$ by showing that it's impossible to list the unit interval in an ordered way. What this means is that we cannot provide a surjective function from $\mathbb{N}$ to $(0,1)$.

Q1. Provide a surjective function $f : (0,1) \to \mathbb{N}$. Is your function injective? Do you think it's possible to find an injective function?

With this last example in mind, we define what it means to compare sets with infinite cardinalities.

Definition 21.1 Suppose A and B are infinite sets. We say $|A| < |B|$ if there are injective functions from A to B, but no surjective functions from A to B. We say $|A| > |B|$ if there are surjective functions from A to B, but no injective functions.

In general, proving that there are no surjections between infinite sets is quite difficult. For instance, it seems like it should be easy to prove that $|\mathbb{R}^2| > |\mathbb{R}|$, but in reality $|\mathbb{R}| = |\mathbb{R}^n|$ for all $n \in \mathbb{N}$ (see the questions about zipper functions in the homework). When we start dealing with infinities, we just can't trust our intuition anymore. Let's explore one of the simpler examples.

Claim 21.1. If A is any set, then $|A| < |\mathscr{P}(A)|$.

Let's work out a proof for Claim 1.

Proof. Let A be a set.

Q2. The claim doesn't require that A be finite or infinite, so we should consider both cases. Prove that if A is finite, then $|A| < |\mathscr{P}(A)|$.

Q3. When A is infinite, things get a little more complicated because $\mathscr{P}(A)$ is infinite as well. Recall that our goal is to show that there are injective functions from A to $\mathscr{P}(A)$, but no surjective functions from A to $\mathscr{P}(A)$. Provide an injective function from A to $\mathscr{P}(A)$. If you construct a sensible function, it should be clear it's injective without a proof.

Q4. We now need to show that there are no surjections from A to $\mathscr{P}(A)$.

For sake of contradiction, suppose $f : A \to \mathscr{P}(A)$ is a surjection. Notice, if $x \in A$ then $f(x) \in \mathscr{P}(A)$.

Q5. Why is the above statement true?

Q6. If $f(x) \in \mathscr{P}(A)$, then what else must be true about $f(x)$? (Think about what a power set is.)

Since f sends elements of A to subsets of A, for $x \in A$ we can say either $x \in f(x)$ or $x \notin f(x)$. With this in mind, we construct the set

$$B = \{x \in A : x \notin f(x)\} \subseteq A.$$

Since $B \subseteq A$, it must be true that $B \in \mathscr{P}(A)$. Since f is assumed to be a surjection, there exists $a \in A$ such that $f(a) = B$.

Q7. Suppose $a \in B$. What can you say about a?

Q8. Suppose $a \notin B$. What can be said about a?

□

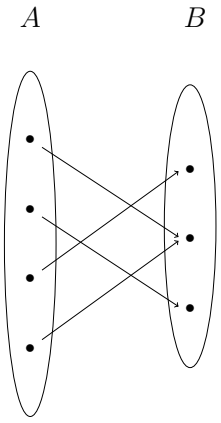
21.2 The Pigeonhole Principle

Finally, we explore a relatively simple concept that can be used to write some interesting proofs. Colloquially, the Pigeonhole Principle says that if you have more pigeons than you do pigeonholes and each pigeon goes to a hole, then at least one hole contains more than one pigeon. Or, if you have more holes than pigeons, at least one hole contains no pigeons. The principle is stated more formally below.

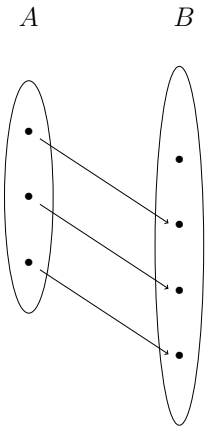
The Pigeonhole Principle: Suppose A and B are sets and $f : A \to B$ is any function.

(1) If $|A| > |B|$ then f is not injective.

(2) If $|A| < |B|$ then f is not surjective.



$|A| > |B|$



$|A| < |B|$

This property shouldn't seem particularly surprising. Humans have a relatively strong inherent sense of numbers, and even children just learning to count have some rudimentary understanding of this concept. Let's define a new type of set to play with the Pigeonhole Principle.

Definition 21.2 ($\mathbb{Z}_p$) Suppose p is a prime number. We define $\mathbb{Z}_p$ to be the set $\{0, 1, \ldots, p\}$.

Notice that $\mathbb{Z}_p$ contains all of the possible remainders when dividing by p.

Q2. Let p be any prime and prove that any function from $\mathbb{Z}_p$ to $\mathbb{N}$ is not surjective.

Below is an interesting use of the Pigeonhole Principle.

Claim 21.2. If A is any set of 9 numbers with values between 1 and 50 (with repeats allowed), then there are two subsets of A, X and Y with $X \neq Y$ for which the sum of the elements of X is the same as the sum of the elements of Y.

As an example, let $A = \{1, 3, 7, 11, 12, 17, 23, 31, 42\}$. We could have $X = \{11, 12\}$ and $Y = \{23\}$ or $X = \{12, 23\}$ and $Y = \{1, 3, 31\}$.

Proof. Let A be a set of 9 numbers with values between 1 and 50.

Q3. What is the largest possible value for the sum of the elements of A? What about the smallest? Remember that repeats are allowed.

Q4. How large is the power set of A? (You'll actually need to know the value.)

Define the function $f : \mathscr{P}(A) \to \{9, 10, \ldots, 450\}$ as the sum of the elements in the set. (So $f(\{1, 2, 3\}) = 6$. Notice that f's inputs are sets and not individual numbers).

Q5. What does the Pigeonhole Principle tell you about f? What can you conclude?

□

Bibliography