In these notes, which will serve as a record of what we covered in weeks 3-4, we discuss various indirect methods of proof. While direct proof is often preferred it is sometimes either not possible or not aesthetically pleasing. In these cases one may resort to *proof by contradiction* or *proof by mathematical induction*. Proof by contradiction is especially indicated for nonexistence statements, in which case it is essentially direct proof of the corresponding universal statement. Contradiction is also often used for proving implications, in which case it is often just direct proof of the contrapositive. Induction is most naturally used to prove statements for all natural numbers.

# 1 Proof by Contradiction

In writing a proof by contradiction, you begin by imagining a situation where the claimed result fails, and show that this is in fact contradictory. For example:

**Example 1.** *There is no largest real number.*

*Proof.* Assume for the sake of contradiction that there was a largest real number, say $n$ (i.e. assume there exists $n$ such that $n \geq x$ for all $x$). We know $1 > 0$ so $n + 1 > n$ by the order axioms. But this contradicts the initial assumption that $n \geq n + 1$. □

(Note that this is a theorem for any ordered field, with the same proof.) This simple example shows the general form of a contradiction argument.

- First we clue the reader in to the fact that the proof is operating by contradiction, "Assume for the sake of contradiction..." is standard.
- We assume the negation of the statement to be proved.
- We do work to obtain a contradiction. It's not necessarily obvious what the contradiction will be in advance. The most satisfying proofs are when the contradiction shows "why" the assumption can't happen.

The process of writing a proof by contradiction involves some suspension of disbelief. In order to be effective you need to reason as if the assumption you believe must be false is in fact true. In the real world of course, you may end up discovering new territories where your desired theorem fails. For example, much of the early work in non-Euclidean geometry was done by people who didn't believe such a thing was possible. They patiently went about proving theorems with the full expectation that eventually they would reach a contradiction, whereas we now know no such contradiction can arise[1]. Another example:

**Example 2.** *For any integers $a, b$ the product $ab$ is even if and only if $a$ is even or $b$ is even.*

[1] More precisely, non-Euclidean geometry is contradictory if and only if ordinary Euclidean geometry is.

*Proof.* If $a$ is even or $b$ is even then clearly the product is too (lemma from last week). Conversely assume for the sake of contradiction that $ab$ is even but neither $a$ nor $b$ is. Say $a = 2k + 1$, $b = 2j + 1$. Then $ab = (2k + 1)(2j + 1) = 2(2kj + k + j) + 1$ is not even, contradicting the assumption. □

Examining this proof, it is clear that what we proved directly was the contrapositive of the hard implication. We stated

$$ab \text{ even} \implies a \text{ even or } b \text{ even}$$

but instead proved the equivalent statement

$$a \text{ odd and } b \text{ odd} \implies ab \text{ odd}$$

. Indeed this is commonly the case when proving implications by contradiction and can be phrased explicitly as such: "We prove the contrapositive:. . . ". This is especially common in proving if and only if situations, where one of the directions will be proved in contrapositive form, so both arguments seem to go "the same way". For example one might commonly show $P \iff Q$ by proving

$$P \implies Q \text{ and } Q \implies P$$

but it's equally common to show

$$P \implies Q \text{ and } \neg P \implies \neg Q$$

, and indeed all 4 combinations of direction are often used without comment.

## Exercise 1

Prove that for any integers $a, b$ if 3 divides $ab$ then 3 divides $a$ or 3 divides $b$. You may need to divide into cases.

Similarly nonexistence proofs by contradiction are usually proving the equivalent universal statement directly, and so we could have introduced the first example by writing "We prove the equivalent statement that for any real number $n$ there is another number $m$ such that $m > n$. . . ". Nonetheless contradiction is both a useful pattern of thought and a common means to write proofs. Here is a classical example, sometimes credited to Hippasus:

**Theorem 1.** *The real number $\sqrt{2}$ cannot be written as a fraction.*

*Proof.* Assume for the sake of contradiction that $\sqrt{2} = \frac{a}{b}$. Further assume that the fraction $\frac{a}{b}$ is in lowest terms, in particular that $a$ and $b$ are not both even. Then we have:

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

$$2b^2 = a^2$$

so $a^2$ is even and thus (by the previous example) $a$ is even, say $a = 2k$. Then

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

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

so by the same argument we see $b$ is even. But this contradicts the assumption that $\frac{a}{b}$ was in lowest terms. □

This fact allegedly angered the Pythagoreans, who ascribed great mystical significance to whole number ratios, and may or may not have taken Hippasus on a very long boat trip shortly after his proof. So it goes.

We see here a great advantage of proof by contradiction: you get some starting assumptions for free. Instead of heading out into the wilderness attempting to prove $P$ directly, you can simply *assume* $\neg P$ and use that to prove all sorts of stuff that would otherwise be inaccessible. For this reason it's embarrassingly common to by reflex assume the contrary of a statement, *proceed to directly prove said statement*, and then conclude by saying your direct proof contradicts the original assumption.

For future use we introduce some terminology.

**Definition 1.** A real number is *rational* if it can be written as a fraction (necessarily non-unique). The set of all rational numbers is denoted $\mathbb{Q}$. A real number that is not rational is *irrational*.

So Hippasus' theorem is usually stated "$\sqrt{2}$ is irrational."

The next example is perhaps the worst correct proof everyone should know.

**Theorem 2.** *$\sqrt[3]{2}$ is irrational.*

*Proof.* Assume to the contrary that $\sqrt[3]{2} = \frac{a}{b}$. Then we have

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

$$2b^3 = a^3$$

$$b^3 + b^3 = a^3$$

Contradicting Fermat's Last Theorem. □

Of course one can adapt Hippasus' proof as well.

Some more easy examples:

**Theorem 3.** *The complex numbers $\mathbb{C}$ (a field) cannot be given the structure of an ordered field.*

*Proof.* Recall that complex numbers are expressions $a + bi$, $a, b \in \mathbb{R}$ where $i^2 = -1$. Assume for the sake of contradiction that there is a relation $<$ giving $\mathbb{C}$ the structure of an ordered field. We proved previously that in an ordered field $x^2 \geq 0$ for all $x$. On the other hand we have $i^2 = -1 < 0$ a contradiction. □

**Example 3.** *If for two integers $a, b$ 4 divides $a^2 - 3b^2$ then at least one of $a, b$ is even.*

*Proof.* Assume for the sake of contradiction that $a, b$ are odd but 4 divides $a^2 - 3b^2$. We write $a = 2j + 1$, $b = 2k + 1$. Then

$$a^2 - 3b^2 = 4j^2 + 4j + 1 - 12k^2 - 12k - 3 = 4(j^2 + j - 3k^2 - 3k - 1) + 2$$

which is not divisible by 4 (division algorithm: we wrote it as $4l + 2$ and $0 < 2 < 4$). □

## Exercise 2

1. Prove there is no right triangle with all 3 sides of odd length.
2. Prove there is no right triangle with the two short sides of odd length.

Contradiction can be used to prove many amusing things. An interesting feature of such arguments is they are often purely nonconstructive. That is to say even when they prove that a specific object exists, they may give no information as to how to build it. (This is why some mathematicians, especially in the early 20th century, reject proof by contradiction. This approach is called *constructivism*.) Consider the game of *Chomp*[2].

Chomp is played by two players starting with a rectangle of delicious chocolate. The upper left square of the chocolate, though still delicious, is poisoned and the two players wish to avoid eating it. The game proceeds in turns. On a players turn he or she must choose one square of the chocolate and eats that square as well as all the squares below and to the right of it (including any squares directly below or to the right). The player who eats the poisoned square loses.

One obviously wants to develop a strategy for avoiding being poisoned. The first rather trivial result is

**Theorem 4.** *One of the two players has a winning strategy. That is if they play perfectly they can win every time no matter what choices the other player makes.*

The proof of this theorem is an easy exercise in mathematical induction, so we leave it to the next section.

The question now is which player has the winning strategy. Does it depend on board size?

**Theorem 5.** *Unless the starting board is $1 \times 1$ (i.e. only the poisoned piece, in which case the second player P2 has the winning strategy of watching the first poison himself) the first player P1 has a winning strategy.*

[2]Neither this nor Cutcake are my invention. I first learned them from one of Ian Stewart's recreational math articles, though it's not his game either. See the Wikipedia page for better references.

*Proof.* Assume for the sake of contradiction that the board size is $> 1 \times 1$ and the P2 has a winning strategy. In this case if the first player P1 eats the bottom right piece there is at least one move that P2 can respond with that places P1 into a losing position (as long as P2 continues to play perfectly). But notice that whichever piece P2 chooses the eaten portion of the board is simply a rectangle, and P1 could have chosen to eat that piece originally, thus placing P2 in the exact same losing position (P1 would be able to "steal" P2's strategy). This contradicts the assumption that P2 had a winning strategy. □

After following the proof you may now sit down to a game of Chomp confident that if you move first you can force a win, but with no idea how to do so in practice.

## Exercise 3

Using the same type of "strategy stealing" argument as we did for Chomp, show that the second player in tic-tac-toe cannot have a winning strategy.

As a final example of proof by contradiction we prove a significant theorem about the number $e$ from calculus is, which is defined by the infinite sum:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots$$

where $n! = n(n-1)(n-2)\dots 3 \cdot 2 \cdot 1$ (read $n$ *factorial*).

**Theorem 6.** *$e$ is irrational.*

*Proof.* Assuming for nefarious purposes that $e = \frac{a}{b}$, with $a, b$ integers, we define

$$k = b!(e - 1 - \frac{1}{1!} - \frac{1}{2!} - \dots - \frac{1}{b!})$$

We prove two things about $k$:

**$k$ is a positive integer** Indeed, $k$ is positive since $b!$ is positive and the sum $1 + \frac{1}{1!} + \frac{1}{2!} + \dots + \frac{1}{b!})$ is less than $e$, since it is only the first $b+1$ terms of the sum of positive numbers defining $e$. Moreover $k$ is an integer since $b!$ divides the denominator every term inside the parenthesis.

**$k$ is less than $\frac{1}{b+1}$** Recall the formula

$$\frac{1}{x-1} = \frac{1}{x} + \frac{1}{x^2} + \frac{1}{x^3} + \dots$$

(True for $x > 1$. To convince yourself of this, ignoring convergence issues, simply multiply both sides by $x - 1$.) Now we have

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

but this is term-wise less than or equal to the sum

$$\frac{1}{(b+1)} + \frac{1}{(b+1)^2} + \frac{1}{(b+1)^3} + \dots$$

which equals $\frac{1}{b}$ by the formula.

These two conclusions are contradictory so we conclude that $e$ cannot be rational. □

# 2 Proof by Mathematical Induction

Induction is a technique for proving families of statements parameterized by the natural numbers. If you recall, we never actually gave a definition (or axiom set) for the natural numbers, so it's hardly surprising that we can't prove much about them. We rectify this by asserting that the natural numbers are exactly those numbers that you can arrive at by starting at 0 and repeatedly adding 1 (we call $n+1$ the *successor* of $n$). Unfortunately the word "repeatedly" seems to give a certain circularity (or at least informality) to this definition. The corresponding formal statement is:

**Axiom 1** (Principle of Induction)**.** *Let $\phi(n)$ be any statement[3] about natural numbers. Suppose:*

1. *$\phi(0)$ is true.*
2. *For all $k \in \mathbb{N}$ $\phi(k) \implies \phi(k+1)$.*

*Then we can conclude $\phi(n)$ is true for all $n \in \mathbb{N}$.*

For a compact axiom set for $\mathbb{N}$, we need only use these three axioms involving $S$, the successor function $a \mapsto a+1$ (we don't write it as "+1" since the axioms don't require or define addition or the constant 1).

1. There a natural number "0".
2. $S(a) = S(b) \implies a = b$ for all $a, b$.
3. $S(a) \neq 0$ for all $a$.
4. The induction principle.

These are known as the *Peano axioms*, and the resulting theory is known as *Peano arithmetic*.

We can easily use the axiom to prove things.

[3] We don't require anything about the statement being given by a formula, etc.. Any arbitrary subset $S \subset \mathbb{N}$ determines a perfectly good $\phi$ (where $\phi(n) \iff n \in S$)

**Example 4.** *For all natural numbers $n > 0$:*

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

*Proof.* We proceed by induction on $n$.

**Base case** Clearly the sum "1" is equal to $\frac{1\cdot(1+1)}{2}$.

**Inductive step** Assume now that the result is true for $n = k$. We wish to show it holds for $n = k + 1$ as well. Indeed

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

by assumption, and

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

as desired.

By induction we conclude the result holds for all $n$. □

**Remark 1.** *This is an ancient result, but commonly associated to Gauss, who was allegedly asked as a schoolchild to sum the numbers from 1 to 100. Gauss infuriated the schoolteacher by immediately writing the answer on his slate.*

## Exercise 4

Eccles pg. 56, 20

## Exercise 5

Eccles pg. 56, 21

Oftentimes one wants to use a stronger inductive assumption, and assume $\phi(n)$ is true for all $n \leq k$ in order to deduce $\phi(k+1)$. This is known as *strong induction*. Strong induction is actually no stronger than the ordinary version:

**Proposition 1** (Strong Induction)**.** *Let $\phi(n)$ be any statement about natural numbers. Suppose:*

1. *$\phi(0)$ is true.*
2. *For all $n \in \mathbb{N}$ ($\phi(k)$ for all $k \leq n$) $\Longrightarrow \phi(n+1)$.*

*Then we can conclude $\phi(n)$ is true for all $n \in \mathbb{N}$.*

*Proof.* Assume $\phi$ satisfies the hypothesis of the proposition. Then define $\phi'(n)$ to be

$$\forall k \leq n, \phi(n)$$

By assumption $\phi'(0)$ is true (since $\phi'(0)$ is equivalent to $\phi(0)$), and $\phi'(n) \implies \phi'(n+1)$. By (regular!) induction we conclude that $\phi'(n)$ holds for all $n$, but since $\phi'(n) \implies \phi(n)$ we observe that $\phi(n)$ is also true for all $n$, as desired. □

We recall that strong induction was already used in the previous notes to show that we can write arbitrary sums without parentheses (a priori the associativity axiom only tells us this for sums of 3 terms). The reader is invited to revisit that proof.

We now prove Theorem 4, that one of the players in Chomp has a winning strategy. To this end we define a valid Chomp position to be *winning* if the player moving from that position can force a win by playing perfectly (i.e. that player has a winning strategy from that position). Similarly we define a position as *losing* if the player moving from that position is guaranteed to lose provided her opponent plays perfectly (the second player to move as a winning strategy). The form of the Theorem we prove is that every valid Chomp position is either winning or losing.

*Proof.* We use (strong) induction on the number of squares on the board. Clearly if there is only one square (the poisoned one) that is a losing position. Assume then that we have a position $P$ of $k+1$ squares, and we know that every position of $k$ or fewer squares is either winning or losing. In particular every position that can result by moving from $P$ is winning or losing. If it is possible to move from $P$ directly to a losing position then that move is the first part of a winning strategy, so $P$ is winning. Otherwise every possible move results in a winning position for the next player, so $P$ is losing. Hence $P$ is either winning or losing and by induction we conclude every position is winning or losing. □

Families of mathematical objects are often defined using induction. For example, consider the sequence of numbers $F_n, n > 0$ defined by:

$$\begin{aligned} F_1 &= 1 \\ F_2 &= 1 \\ F_n &= F_{n-2} + F_{n-1} \end{aligned}$$

This is of course the *Fibonacci sequence* $1, 1, 2, 3, 5, 8, 13 \ldots$. (Such formulae are also called *recursive* definitions, or *recurrences* for short.) Remarkably one can find a "closed form" expression for $F_n$. (This is known as "solving the recurrence".)

**Proposition 2** (Binet Formula)**.** *Write*

$$\phi = \frac{1+\sqrt{5}}{2}, \psi = \frac{1-\sqrt{5}}{2}$$

*($\phi$ is the so-called* Golden Ratio*). Then we have:*

$$F_n = \frac{\phi^n - \psi^n}{\phi - \psi}$$

*for all $n$.*

*Proof.* We use induction on $n$. Observe that both $\phi, \psi$ satisfy the equation $x + 1 = x^2$. Also note that $\phi - \psi = \sqrt{5}$. We then have

$$\frac{\phi - \psi}{\phi - \psi} = 1 = F_1$$

$$\frac{\phi^2 - \psi^2}{\phi - \psi} = \frac{(\phi + 1) - (\psi + 1)}{\phi - \psi} = 1 = F_2$$

, which together will form the base of our induction. Assume then that the Binet formula holds for all $n \leq k$. We wish to deduce it for $n = k + 1$. Well

$$F_{k+1} = \frac{\phi^{k-1} - \psi^{k-1}}{\phi - \psi} + \frac{\phi^k - \psi^k}{\phi - \psi}$$

by assumption, so doing algebra:

$$\begin{aligned} F_{k+1} &= \frac{\phi^{k-1} + \phi^k - (\psi^{k-1} + \psi^k)}{\phi - \psi} \\ &= \frac{\phi^{k-1}(1 + \phi) - \psi^{k-1}(1 + \psi)}{\phi - \psi} \\ &= \frac{\phi^{k+1} - \psi^{k+1}}{\phi - \psi} \end{aligned}$$

as desired. Hence the Binet formula holds for all $n$ by induction. □

**Remark 2.** *In class Mark commented that this formula gives little insight into the nature of the sequence $F_n$. I suppose this depends on what type of insights one is desirous of, however one immediately can see the fact mentioned by Andreas that*

$$\lim_{n \to \infty} \frac{F_{n+1}}{F_n} = \lim_{n \to \infty} \frac{\phi^{n+1} - \psi^{n+1}}{\phi^n - \psi^n} = \phi$$

*(since $|\phi| > 1$ and $|\psi| < 1$).*

Here's an exercise everyone should do involving strong induction:

## Exercise 6

Show that every natural number $> 1$ is divisible by a prime (that is, for all $n \in \mathbb{N}, n > 1$ there is some prime $p$ such that $p$ divides $n$).

To do this, of course, we need to recall what a prime number is

**Definition 2.** A natural number $p > 1$ is *prime* if the only natural numbers dividing it are 1 and $p$.

The standard result that everyone should know is

**Theorem 7** (Attributed to Euclid)**.** *There are infinitely may prime numbers.*

*Proof.* For the sake of contradiction assume that there are only finitely many prime numbers, say $p_1, p_2, \ldots, p_n$. Consider the number

$$q = p_1 p_2 \ldots p_n + 1$$

By construction none of the primes on the list divide $q$ (division algorithm: the remainder is 1). On the other hand the Exercise shows that *some* prime must divide $q$. Contradiction. □

There is a third form of induction that is commonly used, based on the following theorem.

**Theorem 8** (Well Ordering Principle)**.** *Any nonempty subset of the natural numbers* $\mathbb{N}$ *has a smallest element.*

*Proof.* We will prove the statements $\phi(n)$: "Every subset of $\mathbb{N}$ containing $n$ has a least element" by strong induction on $n$. Clearly any subset containing 0 has a least element, namely 0 (the smallest natural number). Furthermore let $S$ be a subset containing $k+1$ and assume the claim holds for all $n \leq k$. Then either $k+1$ is the smallest element of $S$ or there is some smaller element, say $j \in S$ with $j \leq k$. But then the induction hypothesis applies so $S$ has a smallest element in that case too. □

The reader will observe that this conclusion fails for rational or real numbers. The set of all positive real numbers, for example, has no smallest element.

For writing proofs a common use of the Well Ordering Principle is *proof by minimal counterexample*. This is a proof by contradiction wherein one notes that if counterexamples exist then there must be a smallest one, and works for a contradiction from there. An example from folklore:

**"Theorem" 1.** *Every natural number is interesting.*

*Proof.* Assume not. Then there are some uninteresting numbers and so by Well Ordering there must be a smallest one. But being the smallest uninteresting number is a very interesting property. □

It is often stated that the Well Ordering Principle is strictly equivalent (in Peano arithmetic) to the other forms of induction, and you can find many proofs online or in textbooks. *This is false.* One needs to be in a setting slightly stronger than Peano arithmetic for this theorem to hold, in particular you need to somehow arrive at the following fact

**Fact 1** (Predecessor Theorem)**.** *Every natural number other than 0 is the successor of some other natural number.*

**Theorem 9.** *The Well Ordering Principle plus the Predecessor Theorem imply the Induction Principle.*

*Proof.* We start with the hypothesis of the Induction Principle: a family of statements $\phi(n)$ such that

- $\phi(0)$ is true.
- $\phi(k) \implies \phi(k+1)$ (so $\neg\phi(k+1) \implies \neg\phi(k)$).

Assume that the Well Ordering Principle holds but somehow $\phi(n)$ is not true for some $n$. Then there is a smallest $n$ ("minimal counterexample") such that $\phi(n)$ is not true. Since this is not 0 by assumption we can write the minimal counterexample as $k+1$ and so by the second point of the assumptions $k$ is also a counterexample, contradicting minimality. □

The upshot is that in practical settings any inductive proof can be phrased as a proof by minimal counterexample, which is often my favorite way to think about them. Moreover inductive type arguments can often be constructed for any well ordered set, not just the naturals (more on this later).

Finally we worked a fun combinatorial example. Define the *Catalan numbers* $C_n$ inductively as follows:

$$C_1 = 1$$
$$C_n = \sum_{i=1}^{n-1} C_i C_{n-i}$$

. So the first few are $1, 1, 2 = 1+1, 5 = 2+1+2, 14 = 5+2+2+5, \ldots$.

Write $P_n$ for the number of inequivalent ways to fully parenthesise a sum of $n$ things. For example with 4 things $a, b, c, d$:

- $((a+b)+c)+d$
- $(a+(b+c))+d$
- $(a+b)+(c+d)$
- $a+((b+c)+d)$
- $a+(b+(c+d))$

so $P_4 = 5$. We want to show in general that $P_n = C_n$.

To do this we use induction on $n$. Certainly there is only one way to parenthesise a sum of 1 thing so $P_1 = C_1$. Assume then that $P_n = C_n$ for $n \leq k$. We wish to show that $P_{k+1} = C_{k+1}$. Observe that in any fully parenthesised sum of $k+1$ elements there is exactly one addition that is performed last, corresponding to a single "+" sign that is not contained in parentheses. On the left and right of this are nonempty sums $S_1, S_2$ where the total number of elements is still $k+1$ (say $S_1$ has $i$ elements so $S_2$ has $k+1-i$). By assumption there

are $C_i$ and $C_{n-i}$ ways to parenthesise $S_1$ and $S_2$, so $C_i C_{k+1-i}$ total ways to parenthesise a sum of $k+1$ elements given that particular choice of final "+" sign. There are $k$ such choices so the total number of parenthesisztions is

$$\sum_{i=1}^{k} C_i C_{k+1-i} = C_{k+1}$$

as desired.