Proof Workshop

Contents

2 Week 2: Proof by Contradiction and Induction

2.1 Proofs By Contradiction

Suppose that we want to show that some given mathematical statement P is true. If we can show that $\neg P \Rightarrow 0$, then by looking at the truth tables, or using the fact that $\neg P \Rightarrow 0 = \neg(\neg P) \vee 0 = P$, we conclude that P must be true.

In other words, suppose that P is false. From this assumption, if we deduce a statement that contradicts some assumption we already made or some other known fact (perhaps a triviality, definition, axiom, or theorem), then our initial assumption of $\neg P$ must have been false, or in other words that P is true. This technique is called **proof by contradiction**.

In the case that, given a nice domain $\mathcal{D}$, P is the quantified statement $\forall x \in \mathcal{D} : (P_1(x) \Rightarrow P_2(x))$, then the method of proving by contradiction consists of verifying the implication

$$\neg(\forall x \in \mathcal{D} : P_1(x) \Rightarrow P_2(x)) \implies C,$$

for some contradiction C. Since

$$\begin{aligned} \neg(\forall x \in \mathcal{D} : P_1(x) \Rightarrow P_2(x)) &\iff \exists x \in \mathcal{D} : \neg(P_1(x) \Rightarrow P_2(x)) \\ &\iff \exists x \in \mathcal{D} : (P_1(x) \wedge \neg P_2(x)), \end{aligned}$$

the proof of such a P typically starts by assuming the existence of a counterexample of this P.

Let us summarize the above. When we prove by contradiction, we affirm a positive statement by refuting its denial. We often inform the reader that we are employing this strategy by stating something like *Suppose that P is false* or *Assume, to the contrary, that P is false.* Let's look at a few classic examples.

Example 2.1. Suppose we wish to show that there is no largest natural number. Assume the contrary, that there *is* a largest number $x \in \mathbb{N}$. By definition, there is no $n \in \mathbb{N}$ such that $n > x$. However, $x + 1 > x$, and $x + 1 \in \mathbb{N}$. This is a contradiction, so there is no largest natural number $\mathbb{N}$. ▫

For the next two proofs, we will assume the following fact and and some additional properties of primes. You will have the chance to prove many of these claims in this week's problem set.

Definition 2.2. A **prime number** is a natural number $p > 1$ such that if $a \in \mathbb{N}$ and $a \mid p$, then $a = 1$ or $a = p$. In other words, the only natural numbers dividing p are 1 and p.

Theorem 1 (Fundamental Theorem of Arithmetic (FTA))

Every positive integer $n > 1$ can be expressed as the product of primes; this representation is unique, apart from the order in which the factors occur.

Example 2.3 (Euclid)**.** *There are infinitely many primes.*

Proof. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$ be the primes in ascending order, and suppose there is a last prime, called p_n. Now consider the positive integer

$$P = p_1 p_2 \cdots p_n + 1.$$

Because $P > 1$, by FTA, P must be divisible by some prime p. Hence, p must equal one of $p_1, p_2, \ldots, p_n$. Combining the divisibility relation $p \mid p_1 p_2 \ldots p_n$ with $p \mid P$, we arrive at $p \mid P - p_1 p_2 \ldots p_n$; equivalently, $p \mid 1$. The only positive divisor of the integer 1 is 1 itself and, because $p > 1$, a contradiction arises. Hence, the number of primes is infinite. □

Example 2.4 (Pythagoras)**.** $\sqrt{2}$ is irrational.

Proof. Suppose, to the contrary, that $\sqrt{2}$ is a rational number, say $\sqrt{2} = a/b$, where a and b are coprime, i.e. $\gcd(a, b) = 1$. Squaring, we get $a^2 = 2b^2$, so that $b \mid a^2$. If $b > 1$, the FTA guarantees the existence of a prime p such that $p \mid b$. It then follows that $p \mid a^2$

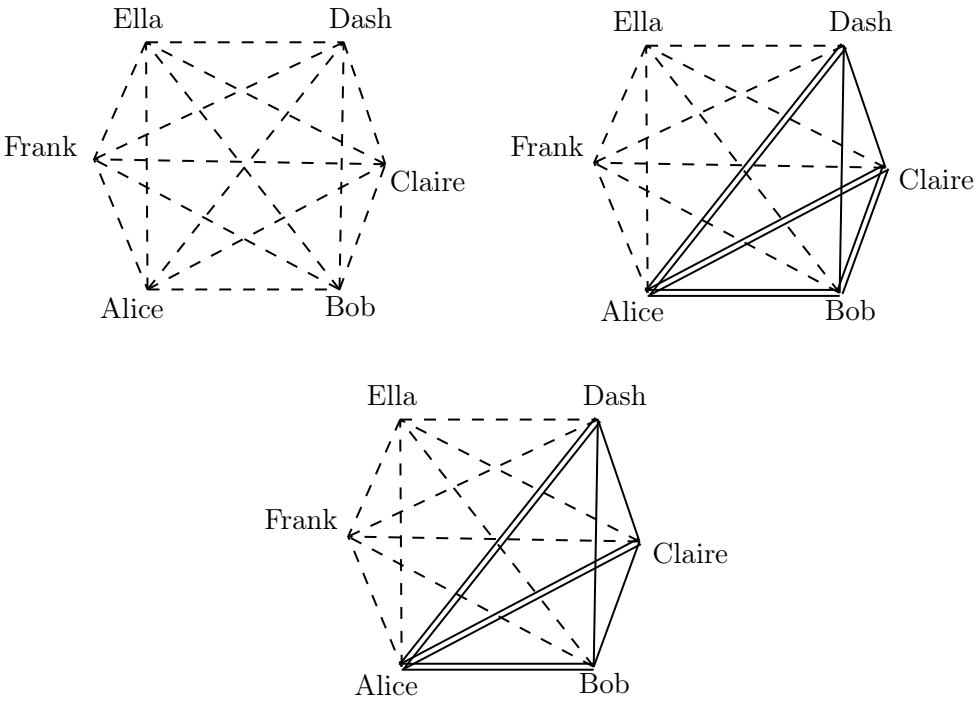
and that $p \mid a$;[1] hence $\gcd(a, b) \geqslant p$. We therefore arrive at a contradiction, unless $b = 1$. But if this happens, then $a^2 = 2$, which is merely circular. Our supposition that $\sqrt{2}$ is a rational number is untenable, and so $\sqrt{2}$ must be irrational. □

Example 2.5 (Ramsey's)**.** Prove that out of a party of six people, there exists a group of three mutual friends or a group of three mutual non-friends.

Proof. Suppose, for the sake of contradiction, that given any group of three people among the six, there are no more than two friendships or two non-friendships. Let the six people be Alice, Bob, Claire, Dash, Ella, and Frank. The possible relationships are shown with dashed lines (Figure 2.1). Start with Alice. Suppose that Alice is friends with at least three people, Bob, Claire, and Dash.

Let a friendship be denoted with a double line, and let a non-friendship be denoted with a single line. If any pair of Bob, Claire, or Dash are friends, then they form a group of 3 mutual friends with Alice, as shown in Figure 2.1.

If Bob, Claire, and Dash are all non-friends, then they form a group of 3 mutual non-friends. In fact, without loss of generality, this same contradiction arises with any combination of 4 people including Alice. Therefore, given any party of 6 people, there exists a group of 3 mutual friends or a group of 3 mutual non-friends. □



[1] We are using the fact that for a prime p, if $p \mid ab$, then $p \mid a$ or $p \mid b$. This is an "obvious" result that has no obvious proof. This result will be in the problem set for Week 3.

Remark 2.6. Often, people may give a proof of contradiction of $P \Rightarrow Q$ by assuming $\neg Q$ and proceed to give a proof of Q, deriving a contradiction, without ever meaningfully using the assumption $\neg Q$. *This is just a direct proof*, and will be shorter and easier to read if it is phrased as such.

2.2 Proof by Induction

2.2.1 The Principle of Mathematical Induction

The last basic proof technique is **mathematical induction**. It is designed for proving statements about the natural numbers.

Suppose we want to show some property P is true for all natural numbers 0,1,2,.... We can't check that all of these numbers individually satisfy the property since there are infinitely many of them. However, what we can show is that if n satisfies P, then $n+1$ also satisfies P. Then, if we show that 0 satisfies P, then it follows so does $0+1=1$, and so does $1+1=2$, and so on until all the natural numbers satisfy P.

Theorem 2 (Principle of Mathematical Induction)

Let P be a property pertaining to the natural numbers $\mathbb{N}$. Suppose that

1. $P(0)$ is true, and
2. for all $n \in \mathbb{N}$, if $P(n)$ is true, then $P(n+1)$ is also true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Therefore, to prove a statement of the form $\forall n \in \mathbb{N} : P(n)$:

1. Prove $P(0)$. This is called the *base case*.
2. Prove that $\forall n \in \mathbb{N} : P(n) \Rightarrow P(n+1)$. This is called the *induction step*, and the assumption that $P(n)$ is true is called the *induction hypothesis*.

We often signify we will use induction by saying "we will proceed by induction on n" or something similar. It helps to explicitly label "base case" or "induction step."

Example 2.7. Prove that for every natural number n,

$$\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \cdots + 2^n = 2^{n+1} - 1.$$

Proof. We proceed by induction on n.

Base case: We have $2^0 = 2^1 - 1 = 1$.

Induction Step: Suppose $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$. We will show $\sum_{i=0}^{n+1} 2^i = 2^{n+2} - 1$. Adding 2^{n+1} to $\sum_{i=0}^{n} 2^i$, we get

$$\sum_{i=1}^{n+1} 2^i = 2^{n+1} + 2^{n+1} - 1 = 2(2^{n+1}) - 1 = 2^{n+2} - 1. \qquad \square$$

We can also induct starting from any natural number n. More precisely, if we proved that $P(k)$ were true for some $k \in \mathbb{N}$ as a base case instead of $P(0)$, then we can conclude that $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geqslant k$. The following example illustrates how this works.

Example 2.8. For every natural number $n \geqslant 5$, $2^n > n^2$.

Proof. We proceed by induction on n.

Base Case: For $n = 5$, we have $2^n = 32 > 25 = n^2$.

Induction Step: Let $n \geqslant 5$ be arbitrary, and assume $2^n > n^2$. Then

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &> 2n^2 \\ &= n^2 + n^2 \\ &\geqslant n^2 + 5n \text{ since } n \geqslant 5 \\ &= n^2 + 2n + 3n \\ &> n^2 + 2n + 1 = (n+1)^2 \end{aligned}$$ $\square$

Example 2.9. For every real number $x > -1$ and every natural number n, $(1+x)^n > nx$.

Proof. Let $x > -1$ be arbitrary. We will show by induction that $(1+x)^n \geqslant 1 + nx$. It clearly follows that $(1+x)^n > nx$.

Base case: if $n = 0$, then $(1+x)^n = (1+x)^0 = 1 = 1 + nx$.

Induction step: suppose $(1+x)^n \geqslant 1 + nx$. Then

$$\begin{aligned} (1+x)^{n+1} &= (1+x)(1+x)^n \\ &\geqslant (1+x)(1+nx) \\ &= 1 + x + nx + nx^2 \\ &= 1 + (n+1)x \end{aligned}$$

since $nx^2 \geqslant 0$. $\square$

2.2.2 Strong Induction

Sometimes, it's not enough to prove that a natural number has a certain property only assuming the previous one does. We need something stronger, and need to assume *all* smaller natural numbers have this property. This is called *strong induction*.

Theorem 3 (Strong Induction)

Suppose P is a property pertaining to the natural numbers $\mathbb{N}$. Suppose that for all $n \in \mathbb{N}$,

1. if $P(k)$ is true for all natural numbers $k < n$, $P(n)$ is true.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Therefore, to prove a statement of the form $\forall n \in \mathbb{N} : P(n)$:

1. Prove that for all $n \in \mathbb{N}$, $(\forall k < n, P(k)) \implies P(n)$ is true. This means that we let n be a natural number, assume $P(k)$ is true for all $k < n$, and then prove $P(n)$.

Remark 2.10. Note that there is no "base case" described in the principle of strong induction. In reality, it is still there, just hidden. This is because for $n = 0$, there are no $k < n$, so the assumptions are vacuous and we must prove $P(0)$ independently.

The two forms of induction are actually equivalent; see https://en.wikipedia.org/wiki/Mathematical_induction#Complete_(strong)_induction for a quick discussion of this. Every proof by ordinary induction can be converted into one by strong induction, and vice versa, so you can't actually prove anything "stronger;" it is just easier.

The following example we give of strong induction is an important first step in the proof of FTA. You may wish to complete the proof yourself as an exercise.

Example 2.11. Every integer $n > 1$ is either prime or a product of primes.

Proof. We will show this by strong induction. Suppose $n > 1$ and suppose every integer $1 < k < n$ is either prime or a product of primes. If n is prime there is nothing to prove, so suppose n is not prime. By the definition of primeness, this means there are numbers $a, b < n$ such that $ab = n$. Note that since $a < n = ab$, it follows $b > 1$ and similarly $a > 1$. Then, by the inductive hypothesis, a and b are each either prime or a product of primes. Since $n = ab$, n is a product of primes. □

2.2.3 The Well-Ordering Principle

Induction implies a very important property of the natural numbers, known as the **well-ordering principle.** To start, a definition:

Definition 2.12. Let $S \subseteq \mathbb{N}$ be a subset of the natural numbers. A *minimal element* of S is an element $x \in S$ such that $x \leqslant y$ for all $y \in S$.

Theorem 4 (Well-Ordering Principle)

Every nonempty subset $S \subseteq \mathbb{N}$ has a minimal element.

Proof. We will prove the contrapositive. Suppose S has no minimal element. We will show that $S = \varnothing$ using a combination of contradiction and strong induction.

Let $P(n)$ be the statement that $n \notin S$. To show that $S = \varnothing$, it suffices to show that $P(n)$ is true for all $n \in \mathbb{N}$. Suppose $n \in \mathbb{N}$ and assume that $P(k)$ is true for all $k < n$, i.e. that $k \notin S$ for all $k < n$. We want to show that $n \notin S$.

Suppose by contradiction that $n \in S$. We claim that n is then a minimal element for S, which is impossible. If $y \in S$, then by the inductive hypothesis, $y \not< n$. Hence, $y \geqslant n$, proving that n is a minimal element. □

The well-ordering principle, combined with an additional assumption, implies the principle of mathematical induction—you may choose to prove this in the problem set.

Remark 2.13. The well-ordering principle is false for many familiar number systems. For example, the well-ordering principle is false for $\mathbb{Z}$; the subset $\mathbb{Z}$ is nonempty, but has no minimal element. It is also false for $\mathbb{R}$, for the same reason.

A more subtle example is the set $[0, 1]$, the set of real numbers $x \in \mathbb{R}$ with $0 \leqslant x \leqslant 1$. While $[0, 1]$ has a minimal element, namely 0, it is not well-ordered. The subset $(0, 1) \subseteq [0, 1]$, consisting of all the elements $0 < x < 1$, is nonempty and has no minimal element!

2.3 The Peano Axioms

So far, we have been taking as a given the definitions of the natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, the reals $\mathbb{R}$, and the various operations $+, \cdot, -, /$. But *why* do these rules work at all? What do we really mean when we say that $2 + 2 = 4$? How are addition, multiplication, and exponentiation defined?

The answer is actually quite hard. One problem is that, while we are working with the basic rules, we must not assume the things that we are already familiar with, but have not *proved*. We cannot assume that $a + b = b + a$, for example. We will begin by defining the natural numbers (for us, they include 0). From this, we may define addition. Repeated addition gives us multiplication. Then, repeated multiplication gives exponentiation.

What is addition? It is just the repeated process of *incrementing*, or counting forward. Incrementing seems to be the fundamental operation; we learn to count starting from 0, and then adding a number each to count up.

Thus, to define the natural numbers we start with two things: the zero number 0, and the increment operation. We will use $n{+}{+}$ to denote the *successor* of n (some denote it $\text{succ}(n)$ or $S(n)$).

Axioms 2.14 (The Peano Axioms)**.**

1. 0 is a natural number.
2. If n is a natural number, then $n{+}{+}$ is also a natural number.

3. 0 is not the successor of any natural number, i.e. we have $n{+}{+} \neq 0$ for every natural number n.

4. Different natural numbers must have different successors, i.e. if n, m are natural numbers and $n \neq m$, then $n{+}{+} \neq m{+}{+}$. Equivalently, if $n{+}{+} = m{+}{+}$ then we must have $n = m$.

5. (Principle of mathematical induction) Let $P(n)$ be any property depending on a natural number n. Suppose that $P(0)$ is true, and suppose that whenever $P(n)$ is true, $P(n{+}{+})$ is also true. Then $P(n)$ is true for every natural number n.

Axioms 1–5 are called the *Peano axioms* for the natural numbers. There is an additional axiom, more properly belonging to set theory:

Axiom 2.15 (Infinity)**.** There exists a set $\mathbb{N}$, whose elements are called natural numbers, as well as an object 0 in $\mathbb{N}$, and a function $++ : \mathbb{N} \to \mathbb{N}$ such that the Peano axioms hold.

Thus we take it as an axiom of sets that there is an object that satisfies the Peano axioms. Elements of the natural numbers are of the form $0{+}{+}, (0{+}{+}){+}{+}, ((0{+}{+}){+}{+}){+}{+}$, etc. As a matter of notation, we define 1 to be the number $0{+}{+}$, 2 to be $(0{+}{+}){+}{+}$, and so on.

Remark 2.16. If you are interested in learning more about the foundations of mathematics and formal proofs, we highly recommend the Natural Numbers Game, hosted at https://www.ma.imperial.ac.uk/~buzzard/xena/natural_number_game/. In a game-like environment you will prove many properties of the natural numbers and functions in Lean, a formal theorem proving system.

2.4 Thinking about Proofs

We now have a few basic proof techniques under our belts: direct proof, proof by contradiction, proof by counterexample, proof of the contrapositive, and proof by induction. We devote the remainder of today's time to practicing applying these to various statements and discussing how to think about proofs.

Example 2.17. Show that $x \in \mathbb{Z}$ is even if and only if x^2 is divisible by 4.

Proof. To prove the forward direction, let's assume that x is even, so $x = 2k$ for $k \in \mathbb{Z}$. Then $x^2 = (2k)^2 = 4k^2$, so 4 divides x^2.

That was easy; it was very straightforward to extract information about x^2 given information about x. It would be nice if we could prove the other direction in a similar manner.

Luckily, we can, by proving the contrapositive of the other direction; that is, that x odd $\implies$ x^2 not divisible by 4. We write $x = 2k + 1$ for $k \in \mathbb{Z}$. Then

$$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1.$$

This will clearly have a remainder of 1 when divided by 4, so this is not divisible by 4. This shows that x^2 being divisible by 4 implies that x is even, so we have shown the if-and-only-if statement. □

The moral here is that if proving one direction of an if-and-only-if statement is particularly simple, you may have an easier time proving the contrapositive of the other direction, as such a proof would likely be of a similar nature to the first direction.

Example 2.18. Can every $n \in \mathbb{N}$ be written as the sum of two squares, that is, $n = a^2 + b^2$ for $a, b \in \mathbb{Z}$? Prove or give a counterexample.

Let's first think of how we would prove that this statement is true. Given an arbitrary natural number n, we would need to exhibit two integers a and b, dependent on n. Since n is arbitrary, we have very little information to use to cook up an a and b, so this strategy is unlikely to work.

We could perhaps try induction, as this is a statement about all natural numbers. However, even if $n = a^2 + b^2$, then all we know is that $n + 1 = a^2 + b^2 + 1$, and there is no guarantee that any of $a^2 + b^2, a^2 + 1$, or $b^2 + 1$ are squares.

In general, it seems we do not have enough information about any random n to prove this statement. This suggests that it is not true for all n, and we may need to know some special properties about n to show it can be written as a sum of two squares. This tells us to move to finding a counterexample.

Starting simple, $1 = 1^2 + 0^2$ and $2 = 1^2 + 1^2$, so those don't work. However, we can only write 3 as 1+2 or 3+0, and neither 2 nor 3 are squares. This gives a counterexample.

We now open the floor to the types of proofs and problems you would like to practice thinking through.