

MAT 137Y – An Introduction to Proofs

One of the challenges that most students encounter in this course is the ability (or lack thereof) to write proofs. This is because most high schools tend to focus on the computational aspect of mathematics. However, university mathematics also deal with analysis and theory; we formulate mathematical questions and use logic to provide rigorous solutions or ideas.

It is likely that this is your first encounter with theorems and proofs, and as such, we recommend that you read this material carefully. You should pay particular attention to the actual theorems and proofs that are illustrated in this handout. Sometimes you may have to read a proof more than once to understand it, which is normal. More importantly, articulating proofs is a skill that you will need to master if you are to be successful in this course. You will often be asked to demonstrate these skills in your problem sets.

We will assume that everyone is familiar with the different sets of numbers: the real numbers \mathbb{R} , the rationals \mathbb{Q} , the irrationals, the natural numbers \mathbb{N} , and the integers \mathbb{Z} . These are defined in Section 1.2 of Salas, Hille, and Etgen. We will also assume you have some familiarity with the mathematical notation that you have learned in high school. For example,

$$\mathbb{Q} = \{x \in \mathbb{R} \mid x = \frac{p}{q}, p, q \in \mathbb{Z}; q \neq 0\},$$

which says: the rationals is the set of all real numbers x such that x can be written in the form p/q , where p and q are integers, and q is not zero. The irrationals are defined as

$$\overline{\mathbb{Q}} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\},$$

that is, the set of all real numbers x such that x is not rational. One question which should spring to mind is: how do we know there are any irrational numbers at all? Later we will prove that $\sqrt{2}$ is one such number that is irrational.

We will now focus on the basics of mathematical statements, theorems, and proofs. If you have not done so already, please read Section 1.8 of the textbook. In a nutshell, consider the statement

If it rains, then the baseball game is cancelled.

The statement consists of a hypothesis (“It rains”) and the conclusion (“The baseball game is cancelled”). Whether the statement is true depends on the truth of the hypothesis and conclusion. The only case where the statement is false is when the hypothesis is true and the conclusion is false; in other words, the statement is false if it rains and the baseball game is not cancelled.

To simplify things a bit, we often use the notation $A \Rightarrow B$ to denote “If A , then B .” The *converse* of the statement $A \Rightarrow B$ is defined to be the statement $B \Rightarrow A$. A statement and its’ converse are not necessarily equivalent. For example, if the baseball game is cancelled, it does not mean that it is raining. If a statement and its’ converse are equivalent, we use the notation “ $A \Leftrightarrow B$ ” to denote “ A if and only if B ” (“ $A \Rightarrow B$ ” and “ $B \Rightarrow A$ ”). Finally, the *contrapositive* of the statement $A \Rightarrow B$ is the statement “not $B \Rightarrow$ not A .” A statement and its’ contrapositive are both equivalent. For example, if we look at the baseball example, if the game is held, then it cannot have rained.

To illustrate the use of mathematical statements, let’s start by looking at the set of integers \mathbb{Z} . Everyone knows what it means for an integer to be even or odd, but let’s define the terms rigorously.

Definition An integer n is *even* if there exists an integer k such that $n = 2k$. Similarly, an integer n is *odd* if $n = 2k + 1$ for some integer k .

With this definition, we now have a criterion which tells us whether a certain integer is even or odd. For

example, 36 is even since $36 = 2 \cdot 18$, and 18 is an integer. $55 = 2 \cdot 27 + 1$, so 55 is odd. Also, any integer that is not even must be odd, and vice versa. We all believe that every natural number is either even or odd. How do we know this? Well, 1 is odd, 2 is even, 3 is odd, and in general: if n is even, $n + 1$ is odd, and if n is odd, then $n + 1$ is even. This is the kind of thinking behind the principle of mathematical induction, which is discussed in Section 1.8 of the text.

Now consider the following statement, which we will label as a proposition.

Proposition 1. For every integer n , if n is even, then n^2 is even.

What we usually do is try a few test cases. For example, if $n = 4$ then $n^2 = 16$ and $n = -12$ gives $n = 144$, so it appears that the statement is true. However, this is not a valid proof; even though it works for a few cases does not mean it works for all even numbers. A proof requires showing the statement is true *for all* even n .

How do we go about this? We're given the assumption that n is an even integer and we need to show that n^2 must also be even. What we would like to do is to fill in the intermediate steps that link the hypothesis to the conclusion. This method of proof is often known as a "direct proof."

Since n is even, then by the definition we stated earlier, we know that $n = 2k$ for some integer k . What can we say about n^2 ?

$$n^2 = (2k)^2 = 4k^2 = 2 \cdot (2k^2).$$

Since $2k^2$ is an integer, this shows that n^2 is two times some integer (namely $2k^2$), so by the definition of even numbers, n^2 must be even. This completes the proof.

Now that we've proven this statement, it naturally begs the question: Is the converse true?

Proposition 2. For every integer n , if n^2 is even, then n is even.

Well, yes, but how do we prove it? Suppose we try to prove our new proposition using a direct proof. Given that n^2 is even, then for some integer k ,

$$n^2 = 2k, \text{ so } n = \pm\sqrt{2k}.$$

This doesn't show whether n is even or not, and at this point we're stuck. Perhaps there is a different way to prove this.

Instead, we will perform a *proof by contradiction*. To do this, we assume that the hypothesis is true and the conclusion is false, and arrive at a contradiction.

So returning to our proof, suppose n^2 is even, but n is **not** even. Then it follows that n must be odd. So what does that say about n^2 ? By the definition of odd integers, $n = 2k + 1$ for some integer k . Similar to our proof to Proposition 1, we get

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(k^2 + 2k) + 1,$$

so n^2 must be odd by definition, since $k^2 + 2k$ is an integer. But this contradicts the assumption that n^2 is even. So the assumption that n is odd must be false; therefore, n must be even.

We can now summarize our results into a theorem.

Theorem 1. For all integers n , n is even if and only if n^2 is even.

Proof. Suppose n is even. Then $n = 2k$ for some integer k . But $n^2 = 4k^2 = 2(2k^2)$, so n^2 must also be even. Conversely, suppose n^2 is even. By contradiction, assume n is odd. Then $n = 2m + 1$ for some integer m .

But $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$, so n^2 is odd, a contradiction. So n is even, and this concludes the proof. ■

Before we go on, it is important to note that the statements

$$“A \Rightarrow B” \text{ and } “\text{not } A \Rightarrow \text{not } B”$$

are NOT equivalent.

With this one theorem, and our definitions of the different sets of real numbers, we are actually quite prepared to demonstrate one of most beautiful proofs in mathematics.

Theorem 2. $\sqrt{2}$ is irrational.

Proof. Suppose $\sqrt{2}$ is rational. (This means we are proving this by contradiction.) Then by definition of the rationals, there exist non-zero integers p and q such that $\frac{p}{q} = \sqrt{2}$, where p and q do not have common divisors (in other words, p/q is in lowest terms). Squaring both sides, we have

$$\frac{p}{q} = \sqrt{2} \implies \left(\frac{p}{q}\right)^2 = 2 \implies \frac{p^2}{q^2} = 2 \implies p^2 = 2q^2.$$

Since q^2 is an integer, we have that $2q^2$ must be even. But $p^2 = 2q^2$, so it follows that p^2 is even. Since p^2 is even, then by Theorem 1, p must also be even. Therefore,

$$p = 2k,$$

where k is some integer. Squaring both sides, we get

$$p^2 = 4k^2 = 2q^2 \implies q^2 = 2k^2.$$

Since $2k^2$ must be even, then q^2 must also be even. Again, by Theorem 1, it follows that q must be even. Therefore, p and q are both even. But this contradicts the fact that p and q have no common divisor and p/q is in lowest terms. Hence, $\sqrt{2}$ must be irrational. ■

As an aside, what we have shown is that there is no rational number whose square is 2. How do we know that there even exists a real number whose square is 2? This is something we take for granted, for example, the length of a diagonal of a square of side length 1 is equal to $\sqrt{2}$. But this assumes that lengths of lines and real numbers are the same thing, which seems clear but in fact is a profound insight. To prove that $\sqrt{2}$ exists we need a few definitions and theorems, including a special fact about the real numbers called the “Least Upper Bound axiom”, which we will cover later in the course.

Strong Induction

Now we switch our attention to the properties of the natural numbers, which leads us to mathematical induction. We assume that you have read Section 1.8 of the text, which covers induction. The textbook uses the set of natural numbers to describe the axiom of induction, however we will define induction in a way that helps us to do proofs.

Principle of Mathematical Induction. We define P as some statement and $P(n)$ means that the statement P is true for some value n , where $n \in \mathbb{N}$. Suppose the following conditions hold:

- $P(1)$ is true. (Base case)
- $P(k)$ is true implies $P(k+1)$ is true.

Then the statement P is true for all $n \in \mathbb{N}$.

A proof by induction requires showing that the base case is true, then assuming the statement holds for $n = k$ (the induction hypothesis), and then showing the statement is true for $n = k + 1$. As you will have seen plenty of examples in the textbook and in class, there is no need to provide any further examples.

However, there is one form of induction called *strong induction* that is not mentioned in the textbook. This is also known as *complete induction*.

Strong Induction. We define $P(n)$ as before. Suppose the following conditions hold:

- $P(1)$ is true. (Base case)
- $P(n)$ is true for all $n = 1, 2, \dots, k$ implies $P(k+1)$ is true.

Then the statement P is true for all $n \in \mathbb{N}$.

The difference between regular and strong induction is in the induction hypothesis; whereas in regular induction we “assume the statement is true for $n = k$ ”, in complete induction we “assume that the statement is true **for all n up to k** .”

Here is a simple example of strong induction involving the Fibonacci Sequence.

Example. The Fibonacci Sequence $\{F_n\}$ is defined as follows: $F_1 = 1$, $F_2 = 1$, and $F_{n+2} = F_n + F_{n+1}$ for all integers $n \geq 1$. The first few Fibonacci numbers are $F_1 = 1$, $F_2 = 1$, $F_3 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, and so on. Prove that $F_n \leq 2^n$ for all positive integers n .

Solution. We prove this using strong induction. Because the sequence is defined recursively and each Fibonacci number is computed by looking at the previous two Fibonacci numbers, we need two base cases. Since $F_1 = 1 \leq 2^1$ and $F_2 = 1 \leq 2^2$, it follows the base cases are true. Now suppose $F_n \leq 2^n$ for all $n = 1, 2, 3, \dots, k$. Then

$$\begin{aligned} F_{k+1} &= F_k + F_{k-1} && \text{(by definition of the Fibonacci sequence)} \\ &\leq 2^k + 2^{k-1} && \text{(by the induction hypothesis)} \\ &\leq 2^k + 2 \cdot 2^{k-1} = 2^k + 2^k = 2 \cdot 2^k = 2^{k+1}, \end{aligned}$$

so $F_{k+1} \leq 2^{k+1}$, and thus the statement is true for all n . ■

Notice how strong induction is required to complete the proof. Not only did we assume that $F_k \leq 2^k$ (the case where $n = k$), we also assumed that $F_{k-1} \leq 2^{k-1}$, which is the case $n = k - 1$.

Exercise. Let $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. Show that $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$ and prove using strong induction that $F_n = (\alpha^n - \beta^n)/\sqrt{5}$. (This is left up to you. The result is important; by using strong induction we are able to find a non-recursive formula for the Fibonacci numbers.)

There are a few comments that need to be made. Sometimes, the base case need not start at $n = 1$. This usually depends on the question. Also, if you are using strong induction, you may have several base cases. Here is an example that illustrates these two points.

Example. A restaurant sells chicken nuggets in small packs of 4 nuggets and large packs of 5 nuggets. Show that for any integer $n \geq 12$ it is possible to buy exactly n nuggets in any combination of small and large packs.

Solution. We prove this using complete induction. It is easy to show that we can buy 12, 13, 14, or 15 nuggets using the right combination of packs:

$$12 = 4(3) + 5(0), \quad 13 = 4(2) + 5(1), \quad 14 = 4(1) + 5(2), \quad 15 = 4(0) + 5(3),$$

so for instance, to buy 14 nuggets we buy one 4-pack and two 5-packs. Therefore, these base cases ($n = 12, 13, 14, 15$) are all true.

Now suppose we can buy n nuggets in combinations of 4-packs and 5-packs for all $n = 12, 13, \dots, k$, where $k \geq 15$. (This is, of course, the induction hypothesis.) We need to show that we can buy $k + 1$ nuggets in combinations of 4-packs and 5-packs. By the induction hypothesis, we can buy $k - 3$ in combinations of 4-packs and 5-packs. Buying an additional 4-pack gives us our required $k + 1$ nuggets.

Therefore, we can buy any number of nuggets over 12 in combinations of 4-packs and 5-packs, and we are done. ■

Notice that because of the question the base case starts at $n = 12$, so it is imperative that our proof does not start at, say, $n = 1$. Furthermore, there are four elements in the base case. This is because the proof requires $k - 3$ nuggets to exist. Therefore, if we had only used the base case $n = 12$, it would be insufficient to prove that we could buy 13, 14, or 15 nuggets.