A Brief Introduction to Proofs

William J. Turner

October 22, 2010

1 Introduction

Proofs are perhaps the very heart of mathematics. Unlike the other sciences, mathematics adds a final step to the familiar scientific method. After experimenting, collecting data, creating a hypothesis, and checking that hypothesis through more experiments, mathematicians must prove their hypothesis is correct before it can be accepted as a true result. Similarly, mathematicians will only consider a piece of written mathematics a "paper" if it contains a proof. Otherwise it can be nothing more than an extended abstract at best.

At the same time, students find reading and writing proofs among the most difficult topics in mathematics. Writing proofs, in particular, takes years of practice. Textbooks usually offer very little guidance, although there are a few books on the topic, such as Solow [2005]. However, at over 250 pages, it is a bit long to expect students to read on their own during a busy semester.

I expect this short guide to proofs to serve as an introduction that students can reference throughout the semester. It will not replace longer reference guides such as Solow [2005], which students may still find useful.

2 Terminology

One reason students find reading mathematics so difficult is that mathematicians use a lot of terminology they have never seen before. For example, a *conjecture* is a statement that does not have a proof, while a *theorem* has a proof. For example, the famous Goldbach Conjecture does not have a proof. On the other hand, Fermat's Little Theorem has a proof.

Students will also run into other related terms. An *axiom* is a statement that is accepted as true without a formal proof. *Propositions*, *lemmas*, and *corollaries* are also all statements that also have proofs. Theorems may be considered to be very important propositions. Lemmas are minor propositions that lead toward a theorem, and corollaries are propositions that follow directly from a theorem. Their use is subjective, and deciding when to call a result a lemma or a corollary rather than a theorem or even a proposition is a matter of taste.

2.1 If: Implications, Hypotheses, and Conclusions

Mathematicians also use terms in a very precise way to which students are not accustomed. The most common example is the word "if," which denotes an *implication*: "If A, then B." Here, A represents an *hypothesis*, and B represents the *conclusion*. Alternatively, we can write the same implication as the statements "B if A" and "A implies B." Mathematicians will sometimes use the shorthand $A \Rightarrow B$. They may also say A is a *sufficient* condition on B or that B is a *necessary* consequence of A.

For example, consider the implication "If a student does not turn in an assignment, then he will fail." This does not mean a student is guaranteed to pass if he turns in an assignment. On the contrary, if he submits a poor assignment, he will likely also fail.

When proving the truth of an implication, you need only consider the case when the hypothesis is true. If the hypothesis is false, then the statement is vacuously true. In other words, to prove an implication is true, start by assuming the hypothesis is true and then show the conclusion is also true. Sometimes a statement will not have an hypothesis, but only a conclusion, in which case you must prove the conclusion is always true.

Students often use the word "if" in their every day language to indicate an equivalence that is more precisely represented by the phrase "if and only if." Consider the statement "A if and only if B" and its mathematical shorthand $A \iff B$. This contains the two implications $A \Rightarrow B$ and its *converse* $B \Rightarrow A$. In other words A is *necessary and sufficient* for B, and vice versa. For example, the statement "A student will fail if and only if he does not turn in an assignment" means both "A student will fail if he does not turn in an assignment" and "A student will only fail if he does not turn in an assignment." When proving an if and only if statement, you must be careful to prove both implications.

2.2 Inverse, Converse, and Contrapositive

Every implication $A \Rightarrow B$ has three related implications: its *inverse* $\neg A \Rightarrow \neg B$, its *converse* $B \Rightarrow A$, and its *contrapositive* $\neg B \Rightarrow \neg A$. Here, the shorthand $\neg A$ means "not A." Of these four statements, the original statement $A \Rightarrow B$ and its contrapositive $\neg B \Rightarrow \neg A$ are equivalent. To see this, consider the truth tables for the two statements as shown in Table 1. Notice the original statement $A \Rightarrow B$ is true whenever A is false or both A and B are true. In other words, it is only false when A is true and B is false. On the other hand, the contrapositive statement is false only when $\neg B$ is true and $\neg A$ is false, or when A is true and B is false. Similarly the inverse statement $\neg A \Rightarrow \neg B$ and the converse statement $B \Rightarrow A$ are contrapositives of each other and are thus equivalent, as is summarized in Table 2. However, notice the statement and its converse are not equivalent. In particular, notice the rows of the tables where either A or B is true and the other is false.

Table 1: Truth table for the statements $A \Rightarrow B$ and $\neg B \Rightarrow \neg A$

A	B	$\neg B$	$\neg A$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$
True	True	False	False	True	True
True	False	True	False	False	False
False	True	False	True	True	True
False	False	True	True	True	True

Table 2: Truth table for the statements $B \Rightarrow A$ and $\neg A \Rightarrow \neg B$

A	B	$\neg B$	$\neg A$	$B \Rightarrow A$	$\neg A \Rightarrow \neg B$
True	True	False	False	True	True
True	False	True	False	True	True
False	True	False	True	False	False
False	False	True	True	True	True

2.3 Definitions

Another confusing concept for students is using mathematical definitions. Students are used to remembering the gist of definitions and not their exact wording. However, students must begin to break this habit and memorize mathematical definitions. The exact wording of a definition is often very important in creating proofs. In fact, most definitions are worded in such a way as to make proofs more easy to construct.

2.4 Quantifiers

Many hypothesis and conclusions contain words or phrases, called *quantifiers* to describe the quantity of items in the domain in which we are dealing.

One type of quantifier is the *universal quantifier*, which says something applies to an entire class of things. Usually it is marked by the phrases "for each", "for all", "for every", or "for any", or by the shorthand $\forall$. For example, the notation $\forall x > 0$ means "for every x greater than zero." Universal quantifiers may appear in either hypotheses or conclusions. When dealing with them, you must show every object with the given property can be used, and not just a particular one. It may be helpful to think of them as if someone else gives you an object with the given property for you to use. For example, when you encounter $\forall n \in \mathbb{Z}$, consider your friend gives you an integer n to use, and you have no control over which integer you receive.

The other type of quantifier is the *existential quantifier*, which says something exists. It is usually denoted by the phrases "there is", "there are", or "there exists", and mathematicians use the shorthand $\exists$. For example, the notation $\exists x > 0$ means "there exists an x greater than zero," and the notation

$\exists n \in \mathbb{Z}$ means "there exists an integer n." Existential quantifiers typically only appear in conclusions, and when they do, you must prove that at least one object with the given property exists. This time you have control over the object and not your friend.

Sometimes existential quantifiers will be tied with a uniqueness property. Consider for example the phrase "there exists a unique integer," which can be denoted by the shorthands $\exists! n \in \mathbb{Z}$ and $\exists_1 n \in \mathbb{Z}$. Here you must prove not only that an integer n exists but that only one such integer exists.

You may also see *nested quantifiers* such as "for every real number x there exists a real number y such that $x = y^3$, or symbolically

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ s.t. } x = y^3. \tag{1}$$

The order of the quantifiers is very important. They must be taken left to right as in normal English. In this statement, we can think of y as depending upon x. When x changes, so may y. In other words, y is some function of x. (More properly, because in general there may exist more than one such y, the set of all possible y is a function of x.) We recognize this statement as being true. However, reordering the quantifiers changes the meaning. The statement

$$\exists y \in \mathbb{R}, \forall x \in \mathbb{R} \text{ s.t. } x = y^3 \tag{2}$$

means that there is at least one real number y such that its cube is *every* real number x. Here, x *cannot* depend upon y. You pick a y and the statement must be true for every x your friend gives you. For example, this means $y^3 = 1$ and also $y^3 = 0$, but this is clearly false because it would mean $0 = y^3 = 1$.

3 Proving a Statement

Once you understand the statement you want to prove, it is time to get to work. I recommend beginning by building an outline of your proof and filling in the details as you proceed. You might start only with the few things in your conclusion, or in the case of a statement of the form $A \iff B$, you may start with the two parts $A \Rightarrow B$ and $B \to A$. You may then add to the outline what you need to do to prove these parts, filling in more and more detail until you finish the proof.

You may also want to work both backwards and forwards. Start with your hypothesis and ask yourself what does this imply, but also look at your conclusion and ask what you need to prove to get to it. Slowly you may move both directions toward a common middle ground. As you do so, you may find your proof branching in many different directions. Do not ignore these, but rather try to keep them organized and proceed down the path that appears most likely.

You will probably encounter may dead-ends in the process, but do not despair. Every mathematician encounters these far more often than he or she would like. The key is to try to figure out what went wrong and to learn from them. You can then backtrack and try a different tactic. If you have other branches you have not explored, decide which is the best and follow it.

If you do not know whether a statement is true, as is always the case with true mathematical research, you may try proving it false. Often this means finding a *counter example*, as we did in equation (2). This is particularly useful in you need to prove a statement involving a universal quantifier. If the statement says something happens for every item in a set, you only need to prove it does not happen for a single item in the set to know the statement is false.

Trying to prove a statement false may also help you find a proof that it is true. If you are having trouble proving a statement is true, try to decide why you are having trouble and use that information to try to prove it false. Then, if you have trouble proving it false, try to use the reason you are running into difficulties to prove it true. As with dead-ends, the key is to try to glean as much information as you can, even when you are running into difficulties.

Once you have connected your branches and found a path, you can write up the proof as directions to get from the hypothesis to the conclusion. Think of a proof as a road map to get to a particular result. Do not just write it down in the order in which you discovered it. You may think of it as building a bridge over a river. You may build the bridge from both banks and eventually meeting in the middle, but in the end, the user only wants to got from one side to the other.

Write in complete sentences using all the normal rules of standard written English. The most common advice students receive, and often the only advice, is to "write in complete sentences!" I suggest you consult English style guides such as Hacker [2003], Hacker [2004], and Strunk and White [2000] as well as reference books on mathematical writing such as Krantz [1997], Higham [1998], and Knuth et al. [1989]. You might consult Turner [b] for a brief introduction to mathematical writing.

You can type proofs in any typesetting or word processing software. However, if you plan to do much mathematical writing, I suggest learning to use LaTeX, which is the standard tool to typeset papers in mathematics, physics, economics, and other disciplines. In this case, you might find Turner [a] for some basic LaTeX typesetting commands.

4 Proof Techniques

Most proofs employ one of several techniques. These proof techniques are very powerful and useful to know. More complicated proofs may even employ several of them. You should become very familiar with the most common proof techniques. Each of the following sections on a proof technique contains a proof employing that technique.

4.1 Direct Proofs

A direct proof establishes the conclusion by a logical combination of the hypothesis with axioms, definitions, and previously proved theorems.

Theorem 1. *The sum of two even integers is always even.*

Proof. Let x and y be any two even integers, so there exist integers a and b such that $x = 2a$ and $y = 2b$. Then, $x + y = 2a + 2b = 2(a + b)$, which is even. □

4.2 Constructive Proof

A constructive proof is a proof that demonstrates the existence of an object by creating or providing a method for creating such an object. Mathematicians tend to favor this proof technique over all others for existence theorems.

Theorem 2. *For every positive rational number x, there exists a rational number y such that $0 < y < x$.*

Proof. Let x be any positive rational number. Then there exist positive integers a and b such that $x = a/b$. Let $y = a/(2b)$. Thus, $y > 0$ is also rational and

$$y = \frac{a}{2b} < \frac{a}{b} = x. \quad \square$$

4.3 Proof by Contradiction

A very power proof technique is proof by contradiction, which is also known as *reduction ad absurdum*, or Latin for "reduction into the absurd." Here you show that if the conclusion were false, a logical contradiction would occur. You start by assuming the hypothesis is true and the conclusion is false, and you derive the contradiction.

Theorem 3. *The number of primes is infinite.*

Proof. Let us prove the theorem by contradiction. Assume the number of primes is finite: $p_1, p_2, p_3, \ldots, p_r$ for some integer r. Then, form the number

$$n = 1 + \prod_{k=1}^{r} p_k.$$

Note none of the primes $p_1, p_2, p_3, \ldots, p_r$ divide n, so any prime factor p of n is a prime distinct from $p_1, p_2, p_3, \ldots, p_r$. Because n is either a prime or has a prime factor p, this implies there is a prime distinct from $p_1, p_2, p_3, \ldots, p_r$. Thus we see for any finite r, the number of primes is not exactly r. Hence the number of primes is infinite. □

4.4 Proof by Transposition

In a proof by transposition, instead of directly proving a statement is true, you prove its contrapositive is true. As we saw in Section 2.2, these two statements are equivalent. The technique derives its name from the rule of inference that follow, namely the true of $A \Rightarrow B$ implies the truth of $\neg B \Rightarrow \neg A$, and conversely.

Notice this is similar to a proof by contradiction in that in both techniques you start by assuming the conclusion is false. However, in a proof by transposition, you prove the hypothesis must then be false rather than assuming it is

true as you do in a proof by contradiction. On the other hand, one can easily transform a proof by transposition into a proof by contradiction by just assuming the hypothesis is true at the beginning of the proof. Then, in proving the hypothesis is false, one derives a contradiction.

Theorem 4. *Suppose a and b are integers and $a \neq 0$. If a does not divide b, then the equation $ax^2 + bx + b - a = 0$ has not positive integer solution.*

Proof. Suppose $x > 0$ is an integer such that $ax^2 + bx + b - a = 0$. Then, the quadratic formula tells us

$$x = \frac{-b \pm \sqrt{b^2 - 4a(b-a)}}{2a} = \frac{-b \pm \sqrt{b^2 - 4ab + 4a^2}}{2a} = \frac{-b \pm (b - 2a)}{2a}.$$

Because $x > 0$, we must have

$$x = \frac{-b - (b - 2a)}{2a} = \frac{2a - 2b}{2a} = 1 - \frac{b}{a}.$$

Thus, $b = a(1 - x)$ and a divides b. □

4.5 Proof by Induction

You may find the induction technique useful for proving theorems involving an infinite number of cases based on some discrete method of categorizing them. In particular, induction proofs are useful for proving theorems about the positive integers of the form "For every integer $n \geq n_0$, $P(n)$," where $P(n)$ is some statement that depends upon n.

There are two types of induction, *weak* induction and *strong* induction, but both involve proving a *base case*, for example proving the statement $P(n_0)$, and then an *inductive step* in which you build up the proof for the other cases. In the inductive step, you assume the result holds for one or more cases and then prove it for a new cases. The difference between weak and strong induction comes in the form of this assumption, which is also called the *inductive hypothesis*

The inductive hypothesis often confuses students. They have learned it is bad to assume things. Instead they want a firm foundation on which to step to the next case. However, the magic of a proof by induction is that the base case initially gives us that firm foundation, and the inductive step means we keep it.

You can think of an inductive proof as climbing ladder. The base case lets you step onto the ladder, and the inductive step allows you to step to the next rung. In this allegory, the inductive hypothesis is just "assume you are standing on a rung," and the rest of the inductive step takes you to the next rung. The base case–stepping onto the ladder–grounds the assumption so that you can step to the second rung. Once there, the assumption is again true, so you can step to the third rung, and so on. It is here that the discreteness of the cases becomes important so that you can talk about the next case, just as you can think of the next rung of the ladder, or the next integer.

4.5.1 Weak Induction

In weak induction, the inductive hypothesis assumes the result is true for one case. For example, in the inductive step of a proof on the positive integers, you assume $P(n)$ is true for some n and prove $P(n+1)$ is also true. Alternatively, you may assume $P(n-1)$ is true and prove $P(n)$.

Theorem 5. *For any positive integer n,*

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

Proof. For the base case, take $n = 1$. Clearly, $1 = 2/2 = 1(1+1)/2$. For the inductive step, suppose the result (3) holds for some positive integer n. Then, by adding $n+1$ to both sides we obtain

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}. \quad \square \end{aligned} \tag{4}$$

Notice the final equation (4) in the proof is just the equation 3 of the theorem with n replaced by $n+1$. Thus, we have shown the result holds for $n+1$ if it holds for n. The base case tells us it holds for $n = 1$. Then the inductive step says it also holds for $n = 2$. Once it holds for $n = 2$, the inductive step says it also holds for $n = 3$. Once it holds for $n = 3$, the inductive step says it also holds for $n = 4$. Once it holds for $n = 4$, the inductive step says it also holds for $n = 5$. This chain of consequences continues for all positive integers, and thus we proved the theorem.

4.5.2 Strong Induction

Strong induction employs a stronger inductive hypothesis that assumes the result is true for multiple cases. For example, in the inductive step of a proof on the positive integers, you might assume assume $P(k)$ is true for all integers $1 \leq k \leq n$ and prove $P(n+1)$ is also true. Alternatively, you may assume $P(k)$ is true for all $1 \leq k \leq n-1$ and prove $P(n)$.

Theorem 6 (The Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 2$ can be factored into a product of primes*

$$n = p_1 p_2 \cdots p_r$$

in exactly one way.

This theorem actually contains two assertions: (1) the number n can be factored into a product of primes in some way, and (2) there is only one such way, aside from rearranging the factors. We will only prove the first assertion here.

Proof of the first assertion of the Fundamental Theorem of Arithmetic. For the base cases, consider $n = 2, 3, 4$. Certainly, $2 = 2$, $3 = 3$, and $4 = 2^2$, so each can be factored into primes. For the inductive step, let us suppose all positive integers $2 \leq k \leq n$ can be factored into primes. Then either $n+1$ is a prime number, in which case it is its own factorization into primes, or it is composite. If $n + 1$ is composite, it is the product $n+1 = n_1 n_2$ of two integers with $2 \leq n_1, n_2 \leq n$. By the inductive hypothesis, we know n_1 and n_2 can be factored into primes:

$$n_1 = p_1 p_2 \cdots p_r, \text{ and}$$
$$n_2 = q_1 q_2 \cdots q_s.$$

Thus,

$$n + 1 = n_1 n_2 = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s,$$

and $n + 1$ can be factored into a product of primes. □

References

Diana Hacker. *A Pocket Style Manual*. Bedford/St. Martin's, Boston, MA, 4th edition, 2003.

Diana Hacker. *Rules for Writers*. Bedford/St. Martin's, Boston, MA, 5th edition, 2004.

Nicholas J. Higham. *Handbook of Writing for the Mathematical Sciences*. Society for Industrial and Applied Mathematics, Philadelphia, PA, 2nd edition, 1998.

Donald E. Knuth, Tracy Larrabee, and Paul M. Roberts. *Mathematical Writing*. Mathematical Society of America, Washington, DC, 1989.

Steven G. Krantz. *A Primer of Mathematical Writing*. American Mathematical Society, Providence, RI, 1997.

Daniel Solow. *How to Read and Do Proofs*. John Wiley & Sons, Inc., New York, fourth edition, 2005. ISBN 0-471-68058-3.

White Strunk, Jr. and E. B. White. *The Elements of Style*. Allyn & Bacon, Needham Heights, MA, 4th edition, 2000.

William J. Turner. Basic LaTeX typesetting. a.

William J. Turner. A brief introduction to mathematical writing. b.