CREATING AND WRITING PROOFS

ADAM VAN TUYL

1. Introduction

One of the main goals of this course, besides learning the mathematical content, is to learn how to create and write a proof. Up to this point in your mathematical career, you have been learning how to do calculations or learning techniques to solve various types of problems. For example, in calculus, you learn how to differentiate a function like $f(x) = x^{34} + 78x^2 + 1$.

Unfortunately, this exposure to mathematics may have given you a skewed perspective on what mathematicians do. We do *not* sit around and integrate functions all day. Instead, we prove assertions, and to do so, we must write proofs. The purpose of this course is to help you make this transition from learning techniques to learning how to create and write proofs, and in doing so, you will better understand what a working mathematician does.

Creating and writing proofs is an acquired skill, and takes lots and lots of practice. Do not get discouraged at the beginning, because it will take some time to get used to this format. As well, creating proofs is a time involved process. Do not be surprised if this course takes up a large amount of your time – it should! Please bare this in mind as you approach your homework. It is not unreasonable to expect some questions to take hours to solve.

This short note will give you some pointers on what a proof is and how to write a proof.

2. Fundamentals

Mathematics can be broken down into *definitions* and *theorems*.

Definitions describe the objects we choose to study. They should be natural and simple enough so that no reasonable person will disagree with them. For example:

Definition. *A positive integer $p > 1$ is a prime if the only positive integers that divide p are 1 and itself.*

Theorems, on the other hand, are logical consequences that we deduce about those objects described in the definitions. For example

Theorem. *There exist an infinite number of primes.*

Note that sometimes we use the word **Proposition** instead of Theorem, but they mean the same thing. As well, a **Lemma** is also another term used to describe a logical consequence, but is usually reserved for results that are needed to prove a much more complicated Theorem. Think of a Lemma as a "little theorem". A **Corollary** is also a logical consequence that follows from a more general theorem. For example, a corollary of the above theorem would be

Corollary. *There exist one million primes.*

The process by which theorems are deduced from definitions is called a *proof.* A proof is a logical explanation of a theorem. For example,

Theorem. *If m is an odd integer, then m^2 is an odd integer.*

Proof. Let m be an odd integer. Since m is odd, there exists an integer k such that $m = 2k + 1$. Then

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

Since $m^2 = 2(2k^2 + 2k) + 1$, m^2 is an odd integer. □

A proof always starts with the word *Proof*, and at the end of the proof, we usually put a box □ to denote the end of the proof. When writing a proof, we always use the proper rules of English grammar (more on this at the end).

3. Finding proofs

Of course, before we can even discuss writing proofs, by which we mean writing up your logical explanation, we need to first describe how to determine the proof in the first place. This, however, is no easy task since there is no general strategy for finding a proof for a theorem (if there was, mathematicians would be out of a job!).

Luckily, there are some general strategies for specific types of problems, that I will describe below.

3.1. Induction.

This is a proof strategy that will be familiar to most, so we will not spend too much time on it. Basically, mathematical induction is used to prove statements like:

Theorem. *For all positive integers n, it is true that n has property P.*

For example:

Theorem. *For every positive integer n,*

$$1 + 2 + \cdots + n = n(n + 1)/2.$$

Formally, mathematical induction is based upon the following axiom:

Principle of Induction. *Given a logical statement $P(n)$ that depends upon a positive integer n, if we can show that*

1. *Base Case: $P(1)$ is true, and*
2. *Induction step: If $P(k)$ is true, then $P(k + 1)$ is true;*

Then $P(n)$ is true for all positive integers n.

We will now prove the above theorem using induction.

Proof. We use mathematical induction. To prove the base case, we must show that the statement $1 + 2 + \cdots + n = n(n + 1)/2$ is true if $n = 1$. This is simple to see since $1 = 1(1 + 1)/2$.

We now must show that if the statement $1+2+\cdots+n = n(n+1)/2$ is true for some integer n, then the statement also holds true for $n+1$, that is, $1+2+\cdots+n+n+1 = (n+1)(n+2)/2$. Assuming that $1+2+\cdots+n = n(n+1)/2$ is true, we then have

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

We then have shown that $1+2+\cdots+n+n+1 = (n+1)(n+2)/2$, and so by the Principle of Induction, the statement is true for all positive integers n. □

3.2. **If-Then Proofs.** A great majority of mathematical theorems have the *if-then form.*

Theorem. *If (conditions A) are true, then (conditions B) follows.*

For example

Theorem. *If m is an even integer, then m^2 is divisible by* 4.

The *if* part of the proof are the given assumptions. This should be the first part of your proof. We usually expand out what is written using the definitions of the given terms.

The *then* part of the proof is what we want to show follows from our assumptions. It will appear at the end of the proof as our conclusion.

To prove a *if-then* proof, you need to show how the given assumptions and logical deductions lead to the conclusion. You should try working "forwards and backwards". Work forwards by thinking about what the assumptions imply, and work backwards by thinking about what sort of conditions will imply the conclusion.

We will prove the above theorem as an example:

Proof. Let m be an even integer. Since m is even, there exists an integer k such that $m = 2k$. If $m = 2k$, then $m^2 = (2k)^2 = 4k^2$. Since $m^2 = 4k^2$, the integer m^2 is divisible by 4. □

3.3. **Contrapositive.** The contrapositive is a variation of the *if-then* proof. Recall that the statement

If A is true, then B follows.

is logically equivalent to the contrapositive statement

If B is not true, then A does not follow.

So, to prove the first statement, it is enough to the prove the second. For example,

Theorem. *If m is a natural number such that m^2 is odd, then m is odd.*

Proof. We shall prove the contrapositive statement: "If m is not odd, then m^2 is not odd." If m is not odd, then m is even. If m is even, then we showed earlier that m^2 is even. Since m^2 is even, m^2 is not odd. □

3.4. **If and Only If.** The "if and only if" (or sometimes, biconditional) is another variation of the *if-then* structure. We sometimes are sloppy, and write iff for "if and only if". An iff statement has the following form:

A is true iff B is true.

An iff statement is really two *if-then* statements:

If A is true, then B follows.

and

If B is true, then A follows.

So, to prove an iff statement, two statements must be proved. For example:

Theorem. *Let m be an integer. The integer m is even if and only if $m+1$ is odd.*

Proof. $\Rightarrow$ We will first show that if m is even, then $m+1$ is odd. If m is even, then there exists an integer k such that $m = 2k$. If $m = 2k$, then $m+1 = 2k+1$. Thus, $m+1$ is odd.

$\Leftarrow$ We now show that if $m+1$ is odd, then m is even. Since $m+1$ is odd, there exists an integer l such that $m+1 = 2l+1$. If $m+1 = 2l+1$, then $m = 2l$. Thus, m is even. □

The arrows $\Rightarrow$ and $\Leftarrow$ are used to denote what "direction" of the iff statement we are proving.

3.5. **Equivalence of sets.** In many proofs, one needs to show that two sets, say A and B, are equal. To do this, one first shows that $A \subseteq B$, and then one shows that $B \subseteq A$. To show that $A \subseteq B$, take an arbitrary element $x \in A$, and argue why x is also an element of B. The following theorem and its proof is an example of how to prove two sets are equal.

Theorem. *For any sets A and B, prove that*

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

Proof. $\subseteq$ Let $x \in (A-B) \cup (B-A)$. Then $x \in (A-B)$ or $x \in (B-A)$. If $x \in (A-B)$, then $x \in A$, but $x \notin B$. So $x \in (A \cup B)$. Since $x \notin B$, we have $x \notin (A \cap B)$. So, $x \in (A \cup B) - (A \cap B)$. On the other hand, if $x \in (B-A)$, then $x \in B$, but $x \notin A$. Since $x \in B$, we have $x \in (A \cup B)$. Because $x \notin A$, the element $x \notin (A \cap B)$. So $x \in (A \cup B) - (A \cap B)$

Since x was an arbitrary element, we have $(A-B) \cup (B-A) \subseteq (A \cup B) - (A \cap B)$.

$\supseteq$ Let $x \in (A \cup B) - (A \cap B)$. Then $x \in (A \cup B)$ so $x \in A$ or $x \in B$. On the other hand, $x \notin (A \cap B)$. Thus, if $x \in A$, $x \notin B$, or if $x \in B$, then $x \notin A$. In the first case $x \in (A-B) \subseteq (A-B) \cup (B-A)$, and in the second, $x \in (B-A) \subseteq (A-B) \cup (B-A)$. Since x was an arbitrary element, we have $(A \cup B) - (A \cap B) \subseteq (A-B) \cup (B-A)$. □

The containment symbols $\subseteq$ and $\supseteq$ are used to denote which containment "direction" we are proving.

3.6. **Other types of proofs.** The list given above is far from complete. For example, there is an entire class of proofs commonly refereed to as $\delta - \epsilon$ proofs which are used in Real Analysis. Keep your eyes open for patterns, but do not think that all proof strategies fall nicely into one of these categories. In fact, the opposite is true.

4. Writing your proof

A well written proof is a joy to read. However, it is difficult to write a nice polished proof. Like any writing assignment, a written proof usually goes through many drafts before it is finished. To do assignments that comprise of proofs, I suggest the following procedure:

(1) On scrap paper, sketch out the logical steps of the proof. Do not worry about grammar and English rules at this stage. Make sure that each step is a valid step.
(2) Look over your proof, and look for gaps in your proof. For example, you should think about your peers in your class. If you had to explain your proof to them, would they be able to understand? In fact, it is always a good idea to talk to your classmates.
(3) Write a rough draft of your proof (on scrap), but this time use all the proper rules of grammar. Edit you draft just as you would for an English assignment.
(4) On your homework assignment, write out the final version of your proof.

As you can see, writing proofs is a highly non-trivial process. Make sure that you leave enough time to write up your proofs. You might want to spread some of the steps over several days.

Here are some specific suggestions to help improve your mathematical writing.

(1) Use the present, first person plural active voice.
Bad: It will now be shown that...
Good: We show...

(2) Choose the right technical term. For example, not all formulas are equations.

(3) Do not start a sentence with a symbol.
Bad: $x^n - a$ has n distinct roots.
Good: The polynomial $x^n - a$ has n distinct roots.

(4) Respect the equal sign.
Bad: $x^2 = 4 = |x| = 2$
Good: If $x^2 = 4$, then $|x| = 2$.

(5) If you use "if", then use "then".
Bad: If x is positive, $x > 0$.
Good: If x is positive, then $x > 0$

(6) Do not omit "that".
Bad: Assume x is positive.
Good: Assume that x is positive

(7) Identify the type of variables.
Bad: For all $x, y, |x + y| \leq |x| + |y|$.
Good: For all real numbers x, y we have $|x + y| \leq |x| + |y|$.

(8) Use "that" and "which" correctly.
Bad: The least integer which is greater than $\sqrt{27}$.
Good: The least integer that is greater than $\sqrt{27}$.

(9) A variable used as an appositive need not be set off by commas.
Bad: Consider the group, G, that...
Good: Consider the group G that...

(10) Do not use symbols such as $\exists, \forall, \leq$ in text; replace them by words. (They can be used in formulas).

Bad: Let S be the set of numbers < 1.
Good: Let S be the set of numbers less than 1.

(11) Use complete sentences and proper paragraph structure.