

Number Theory & Proving "Real" Theorems

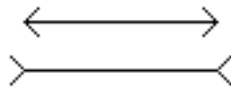
We have just spent weeks learning about first-order logic and how to do both formal and informal proofs in FOL. For the most part, the proofs we have done pertained to formal logic, e.g., we proved things about P, Q, R, etc. We occasionally did a proof where we were interested in the actual meaning of the premises and the conclusion.

Now, we turn our attention to mathematical proofs. Our goal is to use the foundations that we have laid in formal logic to help us derive solid proofs of meaningful statements. We will begin by doing "semi-formal" proofs in this context where we provide detailed statement and reason charts. We call such proofs semi-formal because they will not be as rigorous (and capable of mechanical checking) as the ones we did in Fitch. But our semi-formal proofs will leave out no steps. As we proceed, we will begin to work on the skills required to do informal proofs. It takes practice learning what is appropriate to leave out in an informal mathematical proof.

Why is Proof Important?

Most students are introduced to the concept of mathematical proof in high-school geometry. There, students learn that you have to do a proof about geometric properties because:

1) Observation cannot prove because our eyes can deceive us. For example, these horizontal lines are the same length):



2) Measurement cannot prove because the certainty of the conclusion we arrive at is dependent on the precision of the measuring instrument and care of the measurer.

3) Experiment cannot prove because the conclusions are only probable ones: It is probable that the dice are loaded if 10 successive 7's are thrown; it is even more probable if 20 successive 7's are thrown (*but* it's not certain).

This last example is especially relevant in computer science. Thus far, you have validated the correctness of the programs that you write by testing, i.e., by experimentation. In most cases however, it is impossible to test all relevant inputs. So, you do enough testing to convince yourself that the boundary cases and several cases in between are covered. This is good enough for school assignments, but if you are designing the software for collision avoidance in a new aircraft, you will want to do a lot more than just test isolated inputs; you will want to use proof techniques to *verify* correctness, as well as *validate* it.

In addition, proof is important to science and engineering students because it teaches us to think in very precise terms, which is a necessity in our field. It also teaches a particular approach to problem-solving and it strengthens algorithmic skills. Donald Knuth in [The Art of Computer](#)

Programming compared constructing a program from a set of specifications to writing a mathematical proof based on a set of definitions and known truths.

The Art of Proving Things

The reason we do proofs is to convince a skeptical audience that a given statement is absolutely true. Imagine a listener challenging every statement that you make with "Why is that so?" If you can counter with every possible challenge, your proof is valid. As a very simple example, imagine having to prove to someone unfamiliar with math that if $5x+3 = 33$ then $x = 6$. Your proof might go like this:

$5x + 3 = 33$	given
$5x + 3 - 3 = 33 - 3$	we can subtract = quantities from both sides of an equation
$5x = 30$	subtraction
$x = 6$	division by 5 on both sides

Of course, a proof for someone who is familiar with math would be much shorter since we could leave out the obvious steps (probably all of them). An important point then, is know your audience. What can you leave out based on their knowledge and experience? The reasons that must be included for the proof to "flow" and to suit the needs of your audience come from a particular *frame of reference*. The frame of reference of the above example is arithmetic. Every frame of reference has basic definitions that you can accept as true and use in your proof. Definitions are very important in proofs; they will frequently provide you with the starting point of a proof. Most of the proofs we will do in the next couple lectures will use number theory as the frame of reference.

As an example of how definitions can help in proofs: if you know that the definition of an even number n is that $n = 2k$ for some integer k , you can prove lots of things by substituting this definition:

Prove: If n is an even integer, then $(-1)^n = 1$

The first thing to recognize is that there is an implicit universal quantification here. We are using n as a variable, and we want to prove that the statement is true for all even integers. Using FOL, we might write the sentence to be proved as

$$\forall n ((\text{Integer}(n) \wedge \text{Even}(n)) \rightarrow (-1)^n = 1)$$

Realizing that this quantification is intended lets us see that we are doing a general conditional proof, and being veterans of Fitch, we know exactly what to do. We will pick a name c to stand for an arbitrarily chosen even integer. Then we will show that it must be the case that $(-1)^c = 1$.

Proof: Let c be the name of an arbitrarily chosen even integer.

$$\begin{array}{ll}
 c = 2k \text{ for some integer } k & \text{definition of even} \\
 (-1)^c = (-1)^{2k} & \text{substitution} \\
 = ((-1)^2)^k & \text{property of exponents} \\
 = (1)^k & (-1)^2 = 1 \\
 = (1)^k = 1 & \text{by the laws of exponents}
 \end{array}$$

Since $(-1)^c = 1$ for the arbitrary even integer c , we have shown by general conditional proof that for any even integer n , $(-1)^n = 1$.

Knowing the definitions of the frame of reference, and being able to use them effectively is crucial in doing proofs:

"Such then is the whole art of convincing. It is contained in two principles: to define all notations used, and to prove everything by replacing mentally the defined terms with their definitions."

Blaise Pascal

A Review of Proof Strategies

- Convince yourself that the conclusion is indeed valid by studying the premises and understanding their meaning:
 - Make sure you understand all the terms used in the premises and conclusion - get your definitions ready.
 - We typically prove general conclusions about a set of objects. One way to understand what is to be proven is by proving the conclusion for a particular element of the set. Convince yourself that the conclusion is true for this element (and if you find that it is not, you have just disproven the conclusion). This will also give you insight into how to do the general proof.
 - Try giving an informal proof of the conclusion - explain it to a friend.

If you have convinced yourself that the conclusion is valid, there are various ways to proceed:

1. If the process you went through in understanding the premises and conclusion (working through an example or defining an informal proof) gave you all the details you need, write up a formal (or informal depending on the requirements) proof following the same sequence of steps. In writing an informal proof, you may leave out obvious steps if you know your audience can fill in those gaps.

2. If you are convinced of the conclusion's validity but are having trouble formalizing it, try working backwards from the conclusion, rather than forward from the premises. But always be careful that any intermediate goals you define are consequences of the available information. Think carefully about each step, whether working forwards or backwards.
3. Another approach is to use proof by contradiction. Assume the negation of what you want to prove, and see if you arrive at a contradiction.

If you are not convinced that the conclusion is valid, try to find a counterexample. You may go back and forth between trying to do a proof and trying for a counterexample a few times before you arrive at an answer!

When finished, check your work: Remember that each line in a proof (whether formal or informal) is either a premise, intermediate goal or final goal. Any goal, intermediate or final, must be justified. Make certain that the justifications are valid and lead step-by-step to the conclusion.

If you are writing a formal proof, the justifications must be explicitly stated. If you are writing an informal proof, certain obvious justifications can be left out assuming that your audience can still follow the proof.

If any line in your proof is not a premise, intermediate goal or final goal (or perhaps a clarifying remark), it probably does not belong in your proof.

A well-written proof flows. The reader should feel as though they are being taken on a ride that takes them directly and inevitably to the desired conclusion without any distractions or irrelevant details.

Original handout by Maggie Johnson; modified by Robert Plummer