Lecture 5: Introduction to proofs

Instructor note: this lecture was cancelled due to the weather, so we will discuss the material of this lecture in Lectures 6 and 7.

Introduction to proofs

The above discussion gives us a framework to construct logically sound arguments. Recall that a proof is a *valid* argument, i.e., a sequence of correctly applied rules of inference that start with a bunch of premises and arrive at a conclusion.

Of course, the key in any proof is to figure out the *precise* sequence of steps needed to arrive at the conclusion. There is no magic recipe for this, unfortunately (other than try out all possible truth assignments and rules of inference, which is more or less what a truth table does.)

However, there are certain common *strategies* that mathematical proofs often use. We will see a few of them today and in future lectures. The goal is to put together (and become familiar with) a toolbox of proof techniques that can be used to prove a variety of theorems; in fact, much of the rest of the course will involve doing precisely this. Let us start with the simplest and most standard techniques.

Direct proofs

A *direct* proof of a conditional statement $p \implies q$ follows by assuming that p is true, and constructing a series of deductions to show that q must also be true.

For example, suppose we have the following "theorem":

> If $x > 2$ and $y > 7$, then $2x + y > 11$.

A direct proof of this theorem would look like this. Suppose we assume that for some generic x and y:

1. $x > 2$
2. $y > 7$

are both true. Then, we can infer from the first premise that

3. $2x > 4$

is true. Adding the inequalities (2) and (3) term by term, we get that

4. $2x + y > 11$

is true. Therefore, the given theorem is true.

Similarly, if we want to prove the statement:

> If a given integer n is odd, then n^2 is odd.

A direct proof would be as follows. Assume that the premise is true, i.e., n is an odd integer. Recall that n is odd if and only if it can be written as $n = 2k + 1$ for some integer k. Therefore,

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Therefore, n^2 can also be written as one greater than twice some integer. Thus, n^2 is also odd.

Proof by contraposition

An *indirect* proof, or a proof by *contraposition*, of a conditional statement $p \implies q$ consists of proving the contrapositive of the desired conditional, i.e, instead of proving $p \implies q$, we prove $\neg q \implies \neg p$. (Recall that an implication is logically equivalent to its contrapositive.)

For example, suppose we have the following theorem:

If $x + y > 9$, then $x > 2$ or $y > 7$.

In symbols, we need to prove that:

$x + y > 9 \implies (x > 2) \vee (y > 7)$.

which is of the form $p \implies q$. Suppose *q* is false, i,e,

$\neg((x > 2) \vee (y > 7))$.

is true. By De Morgan's Law, we can simplify this expression as:

$(x \leq 2) \wedge (y \leq 7)$

is also true.

By applying the rule of *Simplification* to this expression, we obtain that

$x \leq 2$

$y \leq 7$

are both true. Adding these inequalities term by term, we get:

$x + y \leq 9$

which is nothing but $\neg p$.

Proof by contradiction

A proof by contradiction is a type of indirect proof that is somewhat more general than a proof by contraposition. Proofs by contradiction are structured as follows. To prove that a statement A is true, you assume, to the contrary, that A is false (i.e., $\neg A$ is true). Then, as in a direct proof, you apply a series of logical deductions until you arrive at a statement that you *know* cannot be true (i.e., a contradiction.) Therefore, the original assumption that A is false is incorrect, and A itself has true.

Proofs by contradiction are an example of the Latin phrase:

Reductio ad absurdum

or "reduction to absurdity". One shows that a statement is true by showing that its opposite leads to a false or absurd result.

Here is a simple example. Let us prove the following theorem:

There exists no smallest positive rational number.

Suppose, to the contrary, that there exists a positive rational number *r* that is smaller than all other rational numbers. By definition, $r = m/n$ for some integers m and n. Consider the number $r/2$. It is certainly rational (since $r/2 = m/2n$, which is a itself ratio of integers) and smaller than r since halving a positive number reduces its value. However, this is a *contradiction*, since we have assumed that r is smaller than *all* other rational numbers. Therefore, the theorem is true.

Here is another example. Suppose there are two categories of people, *knights* and *knaves*. Knights always tell the truth, while knaves always tell a lie. We meet two people, Jack and Jill, but we don't know which category they belong to. They make the following claims:

Jack: "Jill is a knight!"

Jill: "We are of opposite types!"

We deduce their categories as follows. In fact, we will first prove the following "theorem":

Jack is a knave.

Suppose, to the contrary, that Jack is a knight. Since knights tell the truth, Jill is also a knight. Therefore, Jill's statement is also true and Jack is of the opposite type as Jill, i.e., he is a knave. However, this is a *contradiction* since we have assumed Jack is a knight. Therefore, the theorem is true.

Since Jack is a knave, and Jack claims that Jill is a knight, it logically follows that:

Jill is also a knave.

One last example (since proofs by contradiction are important!). This is a very common example given in several textbooks. Let us prove the following theorem:

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

Suppose, to the contrary, that $\sqrt{2}$ is rational. By assumption, we can write $\sqrt{2} = n/d$ in *lowest terms*, i.e., n and d have no common factors. We square both sides and multiply cross terms to get:

$$n^2 = 2d^2$$

Since the right hand side is a multiple of 2, the quantity n^2 is even (and consequently, by the discussion of the last lecture, n is also even.) Writing $n = 2q$ and canceling a factor 2, we get:

$$2q^2 = d^2.$$

This shows that d^2 is *also* a multiple of 2.

In other words, both d and n are even. But this is a *contradiction* since by our assumption above, n and d cannot have any common factors. Therefore, the theorem is true.

A note on writing good proofs

As mentioned earlier: writing out a proof is similar in spirit to writing out a large and complex block of code.

Similar to writing good code, a good proof must not only be logically correct and precise, but also be clearly written. All variables must be clearly defined; all assumptions must be either stated or justified; and all rules must be correctly applied.

A well-written proof is more likely to be correct and logical bugs will be easier to fix. On the other hand, a poorly written proof (even if correct) loses a lot of its value.

Here are some tips for writing good proofs:

- Identify your proof technique in the beginning. It is much easier to identify the flow of a proof if you (and the reader/grader) knows what technique is being used. Begin with something like "We will prove this statement by contraposition. . . ".
- Keep the flow linear, i.e., one statement should lead in to the next and so on.
- Avoid using arcane mathematical notation or jargon. Use ordinary language and short sentences. However, be precise (too little text may be equally bad).
- If a proof is long, break it down into smaller, digestible pieces.
- Revise and simplify your proof once you are done.
- Revise again! Check for common pitfalls, counterexamples, and possible missing cases.
- Conclude. Bring the discussion back to where it started and explain why the original statement is true. Many proofs end with the letters "Q.E.D.", which is an abbreviation of *quod erat demonstrandum*, a Latin phrase that means "which is what we set out to show". If you don't like Latin, a small square box will suffice as well.