Lecture 6: Methods of proof

A good proof is like a well-written software program. The pieces that you need to put together may not be evident right from the beginning, and takes practice and experience. We will try to build an arsenal of proof methods that appear time and time again.

Here is a list of some simple proof methods. We already discussed the first two types in the previous lecture.

Direct proofs

Direct proofs of conditional statements (i.e., propositions of the form $p \implies q$) are constructed as follows: assume that p is true, and show using a sequence of rules of inference that q is true.

For example, suppose we want to prove the following statement:

> Let a, b be positive integers. If $n = ab$ then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

A direct proof would proceed as follows. The above statement is an implication of the form $p \implies q$, where:

- p: $n = ab$
- q: $(a \leq \sqrt{n}) \vee (b \leq \sqrt{n})$

Assume that the hypothesis p is true, i.e., $n = ab$. There are exactly two cases: we have either $a \geq b$ or $a < b$.

If $a < b$, then $a^2 < ab$ by multiplying both sides by a. Therefore, $a^2 < n$, or $a < \sqrt{n}$. Therefore, the consequence q is true.

If $a \geq b$, then $a^2 \geq ab$ by multiplying both sides by a. Therefore, $a^2 \geq n$, or $a \geq \sqrt{n}$. This implies that $1/a \leq 1/\sqrt{n}$; equivalently, $b = n/a \leq \sqrt{n}$. Therefore, the consequent q is true.

In either case, q is true, and therefore the implication is true.

Proofs by contraposition

In contrast, a proof by contraposition of a conditional statement is an *indirect* method of proof: assume that q is false (i.e., $\neg q$ is true), and conclude that p is false, (i.e.,)$\neg p$ is true). We have seen before that $p \implies q$ is logically equivalent to $\neg q \implies \neg p$. Therefore, this is equivalent to proving that $p \implies q$ is true.

Again, let us try and prove the statement:

> Let a, b be positive integers. If $n = ab$ then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

An indirect proof would proceed as follows. Let p and q be the same as above. Assume that the consequent q is false, i.e., $\neg q$ is true. By De Morgan's Laws, we have:

$$(a > \sqrt{n}) \wedge (b > \sqrt{n})$$

Therefore, $ab > \sqrt{n} \cdot \sqrt{n}$, or $ab > n$. In particular, $ab \neq n$, and hence p is false. This proves that the implication $\neg q \implies \neg p$ is true, or equivalently, $p \implies q$ is true.

Vacuous proofs

A vacuous proof of a conditional statement is constructed by observing that $p \implies q$ is true whenever p is false.

For example:

Let x *be a real number. If* $x^2 + 1 < 0$*, then x = 3.14159.*

A "proof" of this implication would proceed as follows. Observe that the antecedent (p) in the implication is the proposition $x^2 + 1 < 0$, which is false for all real numbers. Therefore, the above implication is *vacuously true*. Done!

Vacuous proofs are not frequently encountered in pure math, but often arise in logical thinking. Also, when we will study *mathematical induction* later in the course, we will see that vacuous proofs are frequently used to establish proofs of base cases.

Trivial proofs

A trivial proof of a conditional statement is constructed by observing that $p \implies q$ is true whenever q is true, regardless of the truth value of p.

For example:

Let x *be a real number. If* $x > 0$*, then* $x^2 + 1 > 0$*.*

A proof of this implication would be as follows. For any real number x,

$$x^2 + 1 > x^2 \geq 0.$$

Therefore, $x^2 + 1 \geq 0$ and the implication is *trivially* true.

Note that we never used the hypothesis that $x > 0$ in our proof. Still, the stated theorem is true.

Proof by counterexample

Counterexamples are important mathematical constructs. While it is often very difficult to *prove* a mathematical statement, a single counterexample can be used to *disprove* its validity. All we need to show is that the statement is false in at least one situation. For example, suppose we wish to *disprove* the following claim:

If n is prime, then n is odd.

Clearly, $n = 2$ is a counterexample. Therefore, the theorem is false.

Often, finding a counterexample can be challenging. For example,

For every nonnegative integer n, the number $n^2 + n + 41$ is a prime.

Let $P(n)$ be the predicate "$n^2 + n + 41$ is prime". Then, $P(n)$ indeed appears to be true for $n = 0, 1, 2, \ldots$. In fact it is true all the way up to $P(39)$. However, $P(40)$ is false since $40^2+40+1 = 41 \cdot 41$ which is not a prime number. Therefore, the theorem is false.

Proof of biconditionals

Suppose we wish to prove a *biconditional* statement, i.e., any statement of the form "p if and only if q". Recall that $p \iff q$ is logically equivalent to

$(p \implies q) \wedge (q \implies p)$.

Therefore, an if-and-only-if (or an *iff* for short) can be established by proving the forward implications $(p \implies q)$ and the reverse implication $(q \implies p)$ separately, using any of the techniques for proving implications that we discussed earlier.

This reasoning can be extended to any chain of if-and-only-if statements. Suppose we need to proof that "A iff B iff C". Then, we can arrive at this proof by individually showing that $A \implies B$, $B \implies C$, and $C \implies A$.

We round off our discussion with a list of several additional proof techniques.

Proof by construction

In contrast, proofs by construction are used to prove propositions of the form:

$\exists x, P(x)$.

To prove such as statement, we only need to demonstrate that the predicate $P(x)$ is true for *one* element in the domain of discourse; if we can do that, then we are done.

For example, suppose we need to prove the theorem:

There exist positive integers a, b, c, n such that $a^n + b^n = c^n$.

Consider $n = 1$ and $a = 1, b = 2, c = 3$. For this choice of numbers, clearly $a^n + b^n = c^n$ and hence the theorem is true *by construction*.

Equations of the form $a^n + b^n = c^n$ are examples of *Diophantine equations*. In fact, it is known that for any integer $n > 2$, there exist *no* combination of integers a, b, c that satisfy the above equation – this is the celebrated *Fermat's Last Theorem*, a famous problem in mathematics that remained unsolved for over 350 years.

Some rules of thumb

That was rather a long list of proof techniques.

Some rules of thumb could be of help:

- For proving an "if-then-", consider using direct proofs, proofs by contraposition, or contradiction.

- For proving an “A if and only if B”, think of proving both “A implies B” and “B implies A”.
- For proving “There exists - such that -”, think of a constructive proof.
- For disproving a statement, consider showing a counterexample.
- Use rules of inference wherever you can.

Of course, these are not guaranteed to work, and some techniques might be easier to use in certain cases than others. As always, there is only way to get better at constructing proofs: practice!