

Proof techniques in a nutshell

Author: Jonathan Cox
Revised January 24, 2012

1 Introduction

A *statement* is a declarative sentence that has a well-defined truth value. A *proof* of a statement is a careful argument, expressed in the language of mathematics, meant to convince the intended audience that the statement is true. An *argument* is a group of statements, one of which is called the *conclusion*, wherein all the other statements (called *premises*) are claimed to support the truth of the conclusion. Hence, the conclusion of a proof is the statement being proved.

Most statements of interest in mathematics involve *conditional implications*, which have logical form $p \rightarrow q$. (Here p and q represent simpler statements, called *component statements*.) In English this can be written in numerous ways, including the following.

“If p , then q .” “ q if p .” “ p implies q .” “ p only if q .”
“ p is sufficient for q .” “ q is necessary for p .”

Conditionals can be proved either directly or indirectly.

2 Direct Proof

Here is the truth table for $p \rightarrow q$.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Whenever p is false, the conditional is true already. If, on the other hand, p is true, then q must also be true in order for the conditional to be true. Thus one way to prove $p \rightarrow q$ is to *assume p is true and give an argument demonstrating that q must be true also*. This approach is called a *direct proof*. In applying this approach to a mathematical statement, p represents everything you’re assuming to be true (the hypothesis), and q represents everything you’re trying to prove (the conclusion). The first step is to recognize the hypothesis and conclusion in the statement. Then, you need to construct a sequence of statements, each a logical consequence of the previous, starting with p and ending with q . It isn’t always obvious how to reach q by going forward from p . Using the *forward-backward* method, which also involves working backward from q to statements that are closer to p , can be a big help. Daniel Solow’s book *How to Read and Do Proofs* gives an excellent development of the forward-backward method.

3 Disproving a conditional statement

A statement of the form “ r and s ” is true exactly when *both* r is true and s is true. The *negation* of a statement r is the statement “ r is false.” This is often abbreviated to “not r .” Disproving any statement consists of proving its negation. The negation of $p \rightarrow q$ is “ p and not q ,” as can be deduced from (the second row of) the truth table for $p \rightarrow q$. This points the way toward disproving an conditional. Show that both the hypothesis p can be true and the conclusion q can be false simultaneously. Once you’ve done this, you’ve demonstrated that the conditional is false.

4 Indirect Proof

An *indirect proof* is a proof of an conditional using any method other than direct proof. There are two important methods of this type, and both involve negation. The *contrapositive* of the conditional $p \rightarrow q$ is $(\text{not } q) \rightarrow (\text{not } p)$. It is easy to check that the contrapositive of an conditional is logically equivalent to the original conditional, *i.e.*, they have the same truth value for every combination of truth values of the component statements p and q .

One method of indirect proof is *proving the contrapositive*. This involves using direct proof to prove the contrapositive of the conditional. To do this, assume the original conclusion q is false and give an argument demonstrating that p must be false also. Successfully completing such an argument proves not only the contrapositive, but the original conditional as well, since it is logically equivalent to the contrapositive.

The other method of indirect proof is *proof by contradiction*. A *contradiction* is a statement that is false for every combination of truth values of its component statements. The most common form of contradiction is “ s and not s .” Let C denote a contradiction. Then the conditional $(\text{not } r) \rightarrow C$ is logically equivalent to r . To use proof by contradiction to show r is true, assume r is false and give an argument that concludes with a contradiction C . Successfully completing such an argument proves $(\text{not } r) \rightarrow C$, and thus proves r as well. To apply proof by contradiction to a conditional $p \rightarrow q$, just replace r above by $p \rightarrow q$, and begin by assuming the conditional is false as described in Section 3.

Providing a direct proof is preferable to providing an indirect proof. An indirect proof often obscures the logical connection between the hypothesis and the conclusion, and thus may give little insight into *why* the statement is true. Nonetheless, there are situations where an indirect proof is more feasible. For instance, consider indirect proof if 1) Direct proof isn’t getting anywhere, 2) The conclusion contains “not”, 3) The negation of the conclusion provides useful information, or 4) The original hypothesis is difficult to work with.

5 Proving Biconditionals

Another important type of statement in mathematics is a *biconditional* $p \longleftrightarrow q$, which is true exactly when p and q have the same truth value. In English this can be written in numerous ways, including the following.

“ p if and only if q .” “ p is equivalent to q .”
“ p is a necessary and sufficient condition for q .”

Two of the English representations above, those involving “and”, hint at the connection between biconditional and conditional. $p \iff q$ is logically equivalent to the statement “ $(p \rightarrow q)$ and $(q \rightarrow p)$.” Thus proving $p \iff q$ is a two-step task: First prove the conditional $p \rightarrow q$, and then prove its *converse* $q \rightarrow p$. It’s best to indicate the beginning of the second part of such a proof using the word “Conversely”.

6 Proof by cases

The statement “ p or q ” is true exactly when *at least one* of p or q is true. Conditionals of the form $(p \text{ or } q) \rightarrow r$ are common. To prove such a statement directly, you may assume “ p or q .” The problem is that you don’t know *which* of p or q is true. Thus, it is necessary to give *two* arguments, called *cases* in this situation. For the first case, assume p is true and argue from this that r is true. Then, for the second case, assume q is true and argue that r is true. After completing both cases, you have demonstrated that the truth of r follows from the hypothesis “ p or q .” Of course, an “or” statement could involve more than two component statements, and the approach above can easily be extended to cover this situation. A proof will require one case for each component in the “or” statement.

Often some of the cases in a proof by cases are almost identical. In this situation, after completing one of the cases, it’s sufficient to include a comment such as “The second case is similar and is therefore omitted.” Another way to accomplish this is to use the phrase “Without loss of generality”. When you assume one of the components of the “or” statement “without loss of generality”, you’re indicating that arguments for other cases are very similar and will not be included. Consider carefully whether the cases are really similar enough to use this type of argument!

7 Quantified statements

A *property* (also called a *predicate*, a *propositional function*, or an *open sentence* in various contexts) is a declarative sentence that contains one or more variables, with each variable representing a value in some set (its *domain*), that is **not** a statement, but that **becomes** a statement when specific elements are substituted for the variables. By itself, a property is not a statement: it might be true for some values of the variables and false for others. For simplicity, let’s consider a property $p(x)$ containing only one variable. We often want to consider *how many* values of x make $p(x)$ true. Actually there are typically only two such questions of mathematical interest:

- 1) Is $p(x)$ true for *at least one* value of x in the domain D ?
- 2) Is $p(x)$ true for *every* value of x in the domain D ?

We can answer Question 1 by determining the truth value of the statement “There exists $x \in D$ such that $p(x)$.” This is called an *existentially quantified statement* (e.q.s.). The

phrase “There exists” is called an *existential quantifier* and can also be expressed in English as “There is” or “For some” (among others).

We can answer Question 2 by determining the truth value of the statement “For all $x \in D$, $p(x)$.” This is called a *universally quantified statement* (u.q.s.). The phrase “For all” is called a *universal quantifier* and can also be expressed in English as “For every” or “For each” or “For arbitrary” or “For given” (among others).

Quantifiers can often be hidden. For example, the statements

“The polynomial $x^2 + 2x + 1$ has a real root.”

and “ $\sqrt{2}$ is rational.”

are both quantified statements. (Can you find the quantifiers?) For another such situation, consider that a property is often used to represent what is really meant to be a quantified statement. For example, the property

“If $x > 0$, then $x^3 > 0$.”

probably means “For all $x \in \mathbb{R}$, if $x > 0$, then $x^3 > 0$.” Both the quantifier and domain are left out and assumed to be clear from the context. The “probably” indicates that to leave quantifiers out risks ambiguity and confusion, but the practice is pretty common nonetheless.

The first steps in dealing with quantified statements are to recognize them and then to rewrite them in one of the standard forms above. Next you need to form an opinion about whether the statement is true or false. Then proceed by performing the appropriate task below.

To *prove* the e.q.s. “There exists $x \in D$ such that $p(x)$.”, find one *example* of an $x \in D$ such that $p(x)$ is true.

The negation of the e.q.s. above is “For all $x \in D$, not $p(x)$.” Thus it’s trickier to *disprove* an e.q.s., because you need to show that $p(x)$ is false for *every* $x \in D$. Two possible approaches are

1) Show the only values x for which $p(x)$ is true aren’t in D .

2) *Assume* there’s an x in D for which $p(x)$ is true, and show this implies a contradiction. However, since the negation of the e.q.s. is a u.q.s., it’s sometimes possible to simply follow the structure given next for proving a u.q.s., just with “not $p(x)$ ” in place of “ $p(x)$.”

To *prove* the u.q.s. “For all $x \in D$, $p(x)$.”, start by letting x represent any element of D , and then show $p(x)$ is true for that x . Such proofs begin, “Let $x \in D$.” or “Let x be a given element of D .” or “Let x be an arbitrary element of D .” The proof should end with an assertion like “Therefore $p(x)$.”

The negation of the u.q.s. above is “There exists $x \in D$ such that (not $p(x)$).” Thus *disproving* a u.q.s. can often be fairly easy. All you need to do is find one specific element c in D for which $p(c)$ is false. (Then it won’t be the case that $p(x)$ is true *for all* $x \in D$!) Such a c is called a *counterexample* to the u.q.s.

8 Proof by Induction

A nonempty subset $S \subset \mathbb{R}$ is *well-ordered* if every nonempty subset of S has a least element. The most basic well-ordered set is the set of natural numbers \mathbb{N} . More generally, any set of the form $\{n \in \mathbb{Z} \mid n \geq m\}$ for some fixed integer m is well-ordered. If the domain of a u.q.s. is a set of the form described, then another method called *induction* is available for proving the u.q.s. Actually there are two techniques that fall under the term induction. Each is based on a Principle of Mathematical Induction (PMI). We omit statements of the PMI's themselves.

Theorem 1 (PMI technique) *Let $A = \{n \in \mathbb{Z} \mid n \geq m\}$ for some $m \in \mathbb{Z}$, and let $p(n)$ be a property with domain A . If*

1. $p(m)$ is true and
2. The conditional $p(n) \rightarrow p(n + 1)$ is true for all $n \in A$,

then $p(n)$ is true for all $n \in A$.

Carrying out a proof by induction involves two steps: 1) Proving the base case and 2) the induction step. Before doing anything else it helps to precisely write out the property $p(n)$ for reference. It helps to think of $p(n)$ like a rule for a function, into which you can plug various values of n . The base case is the statement $p(m)$, where m is the least element of the set as described above. To get the base case, replace every n in $p(n)$ with the fixed integer m . Then prove the resulting statement. This is usually the easy part.

The induction step consists of proving the u.q.s. “For all $n \in A$, $p(n) \rightarrow p(n + 1)$.” As usual, start this by letting $n \in A$ be arbitrary. Then assume that $p(n)$ is true. (This assumption is called the induction hypothesis.) The goal is to use this assumption to argue that $p(n + 1)$ is true. It helps to write out the property $p(n + 1)$ explicitly by replacing every n in $p(n)$ with $n + 1$. This way you can see what you’re trying to prove. Then try to relate $p(n + 1)$ to the information in $p(n)$, which you’ll need to use somehow to deduce the truth of $p(n + 1)$.

Sometimes the PMI technique is not enough—we might need more than just $p(n)$ to get $p(n + 1)$. In a case like this, we can use the Strong PMI technique (also known as Generalized PMI or the Second PMI).

Theorem 2 (Strong PMI technique) *Let $A = \{n \in \mathbb{Z} \mid n \geq m\}$ for some $m \in \mathbb{Z}$, and let $p(n)$ be a property with domain A . If*

1. $p(m)$ is true and
2. The conditional $(p(m) \text{ and } p(m + 1) \text{ and } \dots \text{ and } p(n)) \rightarrow p(n + 1)$ is true for all $n \in A$,
then $p(n)$ is true for all $n \in A$.

Here, we get to assume $p(k)$ is true for all $k \leq n$.

9 Proofs involving sets

Suppose A and B are sets. The statement “ A is a subset of B ” means “For all $a \in A$, $a \in B$.” Thus, to show $A \subseteq B$, follow the usual procedure for proving a u.q.s.: Let a be an arbitrary element of A and then show $a \in B$.

Two sets are equal when they have exactly the same elements, *i.e.*, when each is a subset of the other. Thus, the standard method for showing that $A = B$ consists of two steps. You must show that both 1) $A \subseteq B$ and 2) $B \subseteq A$.

10 Proofs involving functions

To show that two functions f and g are equal, you must demonstrate that they have 1) the same domain A , 2) the same codomain B , and 3) the same value at every argument, *i.e.* $f(a) = g(a)$ for all $a \in A$. (In practice, the step showing the codomains are equal is often omitted, since the functions might be assumed to have some predetermined codomain from the context.)

To prove that a function $f : X \rightarrow Y$ is onto (surjective), let $y \in Y$ be arbitrary and show that there exists an $x \in X$ such that $f(x) = y$.

There are two standard ways to prove that a function $f : X \rightarrow Y$ is 1-1 (injective). The one that is usually easier consists of assuming that $x_1, x_2 \in X$ satisfying $f(x_1) = f(x_2)$ and then arguing that $x_1 = x_2$. The other method involves assuming $x_1, x_2 \in X$ such that $x_1 \neq x_2$ and arguing that $f(x_1) \neq f(x_2)$.

To prove that a function f is a 1-1 correspondence (bijection), show that it is both 1-1 and onto.

These are the most basic approaches to proving that a function has these special properties. But there are also higher level approaches that can be easier when they work. Denote identity function on a set X by I_X . (Thus $I_X(x) = x$ for all $x \in X$.) Then a function $f : X \rightarrow Y$ is

1. 1-1 if and only if there exists a function $g : Y \rightarrow X$ such that $g \circ f = I_X$,
2. onto if and only if there exists a function $h : Y \rightarrow X$ such that $f \circ h = I_Y$, and
3. a 1-1 correspondence if and only if there exists a function $g : Y \rightarrow X$ such that $g \circ f = I_X$ and $f \circ g = I_Y$.