Morphology of Proof
An introduction to rigorous proof techniques

Craig Silverstein

Autumn, 1997

1 Methodology of Proof — an example

Deep down, all theorems are of the form **"If A then B,"** though they may be expressed in some other way, such as "All A are B" or "Let A be true. Then B is true." Thus every proof has assumptions — the **A** part — and conclusions — the **B** part. To prove a theorem, you must combine the **assumptions** you are given with **definitions** and other **theorems** to prove the conclusion. The hard part is figuring out what definitions and other theorems to use. Definitions and theorems let you convert statements to other statements; by stringing these definitions and theorems together you can convert the statements of **A** into the statements of **B**. This constitutes a proof. For instance:

Theorem 1 *Let x be a number greater than or equal to 4. Then $2^x \geq x^2$.*

This theorem converts the statement "a number x is greater than or equal to 4" to "for this number, $2^x \geq x^2$. We can use it in the proof of another theorem, like so:

Theorem 2 *Let x be the sum of four squares, $a^2 + b^2 + c^2 + d^2$, where a, b, c, and d are positive. Then $2^x \geq x^2$.*

If we can prove that x is of necessity greater than or equal to 4 (by noting, for instance, that a, b, c, and d are at least 1, and thus their sum is thus at least 4), then we can convert the assumption of our theorem from "x is the sum of four positive squares" to "x is at least 4." Then we can use the first proof to convert the statement "x is at least 4" to "$2^x \geq x^2$." This completes our proof.

Often, we use definitions to expand out mathematical shorthand before we can start applying proofs. For instance, if an assumption is that "x is prime," then you might need to convert this to "x has exactly two positive divisors" before continuing with your proof. **If you are at a loss for how to start a proof, convert all the terms in the assumptions to their definitions.**

Here is a theorem that can be proved with these techniques.

Theorem 3 *Let S be a finite subset of some infinite set U. Let T be the complement of S. Prove T is infinite.*

Intuitively, this is saying that if you have an infinite supply of something, and you take a finite amount of it away, you are left with an infinite amount. This explanation may seem obvious, but it is not a proof. To obtain a rigorous proof, we must get from the assumptions to the conclusion through theorems and definitions. We identify the assumptions: "S is a finite subset of an infinite set. It has a complement T." A good start is to expand the definitions in the assuption.

Definition: A set S is **finite** if there exists a number N such that the number of elements in S (denoted $|S|$) is less than N. If no such N exists, then S is **infinite**.

Note that you give me the set S before I try to figure out the number N. Thus, if *any* number N exists that is bigger than $|S|$, I will be sure to find it, since I know what S is. This ordering concern ("first we have S, then we find N") is important with statements such as "there exists" or "for all."

Definition: If S and T are both subsets of some set U, T is the **complement** of S (under U) if $S \cup T = U$ and $S \cap T$ is $\emptyset$.

So now we can use our definitions to convert our assumptions:

Original statement	**New statement**
S is finite	There is a number N such that $\|S\| < N$
U is infinite	There is no number M such that $\|U\| < M$
T is the complement of S	$S \cup T = U$ and $S \cap T$ is $\emptyset$

We're still stuck, so we have to apply one of the proof methods which will be discussed in the next sections. These let you use the conclusion — the **B** part — to help prove the theorem. What we need here is a common proof technique, proof by contradiction. We assume that the result is false, and show that as a result, the assumptions must be false as well. Since we know the assumptions are true, this means the theorem must also be true.

So we assume that the result is false, that is T is in fact finite. Then, applying a definition, there is a number P such that $|T| < P$. Since we know that $S \cup T = U$ and $S \cap T$ is $\emptyset$, we know $|S| + |T| = |U|$ (if you don't know this, then you can prove it on its own before you try to include it into this proof). But we know $|S| < M$ and $|T| < P$, so $|S| + |T| < M + P$, that is $|U| < M + P$. But we assumed there is no number such that $|U|$ is less than it, so our claim that the result is false is wrong. Thus the result is true, and the theorem is proved. We write it up in a more mathematical, terse form.

Proof: We know that $S \cup T = U$ and S and T are disjoint, so $|S| + |T| = |U|$. Since S is finite, $|S| < M$ for some M, and since U is infinite, $|U| > N$ for all N. So assume T is finite, that is, for some P, $|T| < P$. Then $|S| + |T| < M + P$, or, substituting, $|U| < M + P$. But this contradicts our claim that $|U| > N$ for all N.
♠

That spade is how I indicate the end of a proof. I am limited in what symbol I use by the fonts on my computer, but in general unlimited creativity is allowed here.

1.1 Summary — how to prove a theorem

1. Identify the assumptions and goals of the theorem.

2. Understand the implications of each of the assumptions made. Translate them into mathematical definitions if you can.

3. Either try to massage the definitions and theorems that you identified in (2) into the statement you are trying to prove, or, if that fails

4. Make an assumption about what you are trying to prove and show that it leads to a proof or a contradiction.

The last two items are the only two possible ways to convert your assumptions into proof. These and other possible techniques for proving theorems will be discussed in more detail in the next section.

2 Taxonomy — techniques useful in proving a theorem

1. Proving if and only if proofs in two directions
2. Structural induction
3. Contrapositive
4. Counterexample

2.1 Taxonomy of Proof — if and only if

While all proofs are of the form IF ... THEN, many have more complicated manifestations. The most basic proof has the form

if A then B or
A implies B or
$\mathbf{A} \rightarrow \mathbf{B}$

which was explored in the section 1. This means that whenever A is true, B is also true. A stronger connection between A and B is implied by the form

A if and only if B or
$\mathbf{A} \leftrightarrow \mathbf{B}$ or
A iff B

The term "if and only if" is really a code word for equivalence. To prove a theorem of this form, you must prove that A and B are equivalent; that is, not only is B true whenever A is true, but A is true whenever B is true. "If and only if" is meant to be interpreted as follows:

A if B means **if B then A**
A only if B means **if not B then not A**

It is a logical law that IF A THEN B is always equivalent to IF NOT B THEN NOT A (this is the basis to proof by contradiction), so A ONLY IF B is equivalent to IF A THEN B as well.

When proving an if and only if proof directly, you must make sure that the equivalence you are proving holds in all steps of the proof. This means that each step in the proof must use either a definition that is IF AND ONLY IF or a theorem that is IF AND ONLY IF. Using a less rigorous IF...THEN proof in one of your steps will invalidate your proof.

Making sure all the steps in your theorem obey this restriction is usually difficult and often impossible. The second, more common way then to prove an if and only if theorem is to physically **break an "if and only if" proof into two proofs**, the "forwards" and "backwards" proofs. To prove a theorem of the form "A if and only if B," you first prove "if A then B," then you prove "if B then A," and that completes the proof. Using this technique, you can use IF ... THEN proofs as well as IF AND ONLY IF proofs in your own proof.

Theorem 4 *Let x be a number. Let $\lfloor x \rfloor$ be the greatest integer less than x, and $\lceil x \rceil$ be the smallest integer greater than x. Prove that $\lfloor x \rfloor = \lceil x \rceil$ if and only if x is an integer.*

Proof:

$\rightarrow$ In this direction we assume $\lfloor x \rfloor = \lceil x \rceil$ and try to prove x is an integer. Note that $\lfloor x \rfloor \leq x \leq \lceil x \rceil$. Since $\lfloor x \rfloor = \lceil x \rceil$, then $x = \lfloor x \rfloor$ as well by the sandwich theorem. Since $\lfloor x \rfloor$ is an integer, x must be as well.

$\leftarrow$ Now we assume x is an integer and try to prove that $\lfloor x \rfloor = \lceil x \rceil$. If x is an integer, then $\lfloor x \rfloor = x$ and $\rfloor x \rfloor = x$ (by definition of both terms), so $\lfloor x \rfloor = \lceil x \rceil$ as well.

♠

2.2 Taxonomy of Proof — structural induction

"Straight" induction is an occasionally useful proof technique. It is used to prove there exists a relationship between some function of the integers and a given formula. Since there are an infinite number of integers, brute force won't work ("Well, the pattern holds for 1, and for 2, and for 3, and . . . "), so we use induction:

- Prove the pattern holds for at least one number
- Assume it holds for an arbitrary number N
- Prove that if it holds for N, it must hold for $N + 1$ as well.

Again, we can't escape the IF . . . THEN construction. Here's what I mean by pattern:

Theorem 5 *Prove that*

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

for all n.

If n is 1, the sum of the first n squares is 1, and the formula works out to $1 \times 2 \times 3/6 = 1$ as well. Since we want to prove this pattern of equality between sum and formula holds for all positive integers, not just the number 1, we use induction.

Proof: Assume the formula holds for some number n, that is

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \tag{1}$$

for this n. If we can prove that this implies

$$\sum_{i=1}^{n+1} i^2 = \frac{[n+1]([n+1]+1)(2[n+1]+1)}{6} \tag{2}$$

then we've proven the theorem ((1) is the same as (2), but with all the n's replaced by $n+1$'s). To get the left-hand side of (1) to match that of 2, we add $(n+1)^2$ to both sides of the equation. Adding $(n+1)^2$ to the right-hand side of (1) and multiplying it out gives

$\frac{1}{6}\left[2n^3+3n^2+n+6(n^2+2n+1)\right]$ which simplifies to $\frac{1}{6}\left(2n^3+9n^2+13n+6\right)$. If we expand the right-hand side of (2), we see it is $\frac{(n^2+3n+2)(2n+3)}{6}=\frac{1}{6}\left(2n^3+9n^2+13n+6\right)$. Hence the two sides match, the formula works, and we're done.

♠

There aren't many places where this is useful, however, for we rarely try to prove things about integers. However, forms of induction can be appropriate when trying to prove things about structures defined recursively (when you consider the integers as such a structure, where all numbers are defined by recursively adding one to itself, you get straight induction). For instance, a *string* in computer science is defined as a collection of characters, and proofs about strings often start with proving the case for single-character strings and then proving the rest by induction. This generalized induction is known as **structural induction**. It is useful when objects are built up from more primitive objects: if we can show the primitive objects have the desired property, and the act of building preserves that property, then we have shown that all objects must have the property. The inductive hypothesis (i.e., the assumption) is to assume that something is true for "simpler" forms of an object and then prove that it holds for "more complex" forms. "Complexity" is defined as a relative term: one object is more complex than another iff it includes that other object as a subpart. A classic use of structural induction is to prove that any legal expression has the same number of left parentheses and right parentheses:

Theorem 6 **E** *is a well-formed formula (wff) if it has one of the following forms:*

- *a number (constant) or letter (variable)*
- **E + F**, *where* **E** *and* **F** *are both wffs*
- **E * F**, *where* **E** *and* **F** *are both wffs, or*
- **(E)**, *where* **E** *is a wff.*

Prove all wffs have the same number of left and right parentheses.

In this example, wffs of type 1 are the primitive types, while the others make new wffs from simpler ones. We must take care not to forget a case.

Proof:

We let $E_($ be the number of left parentheses in a wff E and $E_)$ be the number of right parentheses in E. We now consider each case and its parentheses count:

case	number of ('s	number of)'s
1	0	0
2	$E_(+ F_($	$E_) + F_)$
3	$E_(+ F_($	$E_) + F_)$
4	$E_(+ 1$	$E_(+ 1$

In the last three cases, E and F are simpler than the complex forms they are part of [$E+F$, $E*F$, or (E)], and hence for these cases we can assume the inductive hypothesis for E and F: namely, that $E_(= E_)$ and $F_(= F_)$ for these simpler forms. Using this assumption, we see that $[E+F]_(= [E+F]_)$, $[E*F]_(= [E*F]_)$, and $[(E)]_(= [(E)]_)$. Finally, we see by inspection that in the base case (1) the parenthesis count matches, so they match in all cases.

♠

2.3 Taxonomy of proof — contrapositive

Contrapositive is a quite powerful method in proof: it allows you to attack a proof backwards. Instead of going from the assumptions and trying to derive the result, you start by assuming the result is false and show that this violates one of the assumptions. This makes use of the logical law of **contrapositive:**

if A then B
is equivalent to
if not B then not A

Since we are assuming that the result is not true and end up by contradicting our assumptions, this is also often called **proof by contradiction**. We used it back in section I for the very first proof; it is used quite a lot. It gives a lot of flexibility in IF AND ONLY IF proofs, because it allows us to interpret the "forward" and "backward" part of the proof in several different ways:

The two parts of an "if and only if" proof
Prove: A iff B.

- Prove A implies B. Then prove B implies A.
- Prove A implies B. Then prove not A implies not B.
- Prove B implies A. Then prove not B implies not A.

By applying the law of contrapositive, it is fairly easy to see that all three forms are in fact equivalent. This flexibility in proof methods is yet another reason to prefer the two-step approach to if and only if proofs to the monolithic approach.

2.4 Taxonomy of proof — counterexample

It may be significantly easier to disprove something than to prove it, for to prove a theorem false, often all you need to do is provide a counterexample. "Disproofs" can be as simple as this:

Theorem(?) 7 *All prime numbers are odd.*

Disproof: Two is prime, but two is even.
♠

Usually, however, counterexamples are not that easy to come by. Frequently, you are not asked to disprove something, but are given a statement and told either to prove or disprove it. A good general strategy in such cases is to **search for a proof, but use any weaknesses in your proof strategy to search for counterexamples**. Here is an example of this technique. The definition we need here is this: $a \bmod b$ is defined to be the unique integer r such that, for some q, $bq + r = a$, $bq \le a$, and $b(q+1) > a$. That is, $a \bmod b$ is the remainder when a is divided by b. Note that from the definition it follows that $0 \le a \bmod b < b$.

Theorem(?) 8 *Prove or disprove: There is no pair of numbers a and b such that $a \bmod b = b \bmod a$.*

When asked to do things with pairs of objects, it is often possible to simplify the relationship between the two numbers to help with the proof. In this case, we can assume $a < b$ without loss of generality, because if $a > b$, we can swap a and b and get the same equation — we are taking advantage of the problem's *symmetry*. We must be careful not to forget the third case, however, that $a = b$. This turns out to be the chink in our proof that leads to a counterexample, but for right now we try to prove the theorem, keeping our eyes out for counterexamples.

So first we assume $a < b$. Then $a \bmod b = a$ (from the definition above, with $q = 0$ and $r = a$). But $b \bmod a < a$, from our observation above that $x \bmod y$ is always less than y. Hence $a \bmod b \neq b \bmod a$ for any values of a or b. By switching around a and b, we get a similar proof for the case $b < a$.

But now we try to prove the theorem for the case $a = b$. And here we run into problems, because $a \bmod b = 0$ if $a = b$, and $b \bmod a = 0$ if $b = a$, so then $a \bmod b = b \bmod a$, disproving the theorem. Here's the proof:

Disproof: The theorem is false: if $a = b = 2$, for instance, then $2 \bmod 2 = 2 \bmod 2$.
♠

In the process of finding this counterexample, though, we found out something more than was asked for: we know exactly those conditions that make $a \bmod b = b \bmod a$. Thus we are able to prove a modified version of the theorem.

Theorem 9 *$a \bmod b = b \bmod a$ iff $a = b$.*

Since this is an if and only if proof, we have to do it in two directions. **As is often the case in if and only if proofs, one direction is much easier to do than the other**. We will do the easy direction first.

Proof:

$\rightarrow$ We assume $a = b$ and prove $a \bmod b = b \bmod a$. But this is clearly true, since $x \bmod x = 0$ for all x, and a and b are equal.

$\leftarrow$ Here we have to prove that if $a \bmod b = b \bmod a$, then $a = b$. Try to find a direct proof, and then give up and do the contrapositive: assume $a \neq b$, and prove that $a \bmod b \neq b \bmod a$. There are two possible cases: $a < b$, and $a > b$ (we've already assumed $a \neq b$).

- $a < b$ Then $a \bmod b = a$. But $b \bmod a$, as we noted, is strictly less than a, so it cannot be equal to a and hence can't be equal to $a \bmod b$.
- $a > b$ Then $b < a$, and the proof is the same as above with a replaced by b and b replaced by a.

♠