Maggie Johnson
CS109

Methods of Proof

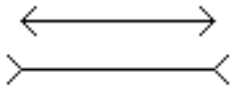
Key topics:

* Why is Proof Important?
* What Are We Trying to Prove?
* The Art of Proving Things
* Direct Proof
* Indirect Proof: Contradiction
* Quantifiers I: Construction
* Quantifiers II: Counterexample and Choose
* Some Famous Conjectures

Why is Proof Important?

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

1) observation cannot prove because our eyes can deceive us:



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; but, in most cases, 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 the 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 you to think in very precise terms which is a necessity in the field. It also teaches you a lot of different problem-solving techniques and strengthens your 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.

What *Are* We Trying to Prove?

Statements that we have to prove often have the form of the **implication** or **conditional**: *if* A, *then* B. To prove that such a statement is true, we have to analyze the meaning of the A statement

and the B statement. A is called the **hypothesis**, and B is called the **conclusion**. As shown in a previous lecture, the truth table for implication is:

A	B	A->B
T	T	T
T	F	F
F	T	T
F	F	T

In propositional logic, we are not concerned with the *meaning* of A and B. We analyze all the possible combinations of true and false (for A and B) to determine whether or not a compound proposition is true or false. Now, however, we are concerned with meaning, so only one of the true/false combinations in the truth table will fit a particular A statement and B statement (with a resulting value for the implication). In a proof, we want to prove the truth of the implication. One way of doing this is to assume the hypothesis is true, and we then proceed to show, using definitions and axioms from a particular frame of reference, that the conclusion is true. If B is true, then the implication is true (note that this method of proof "implies" causation of B by A, but as you will see, A does not have to be true). Or, we can just show A is false (then the implication is always true), or we can show B is true without any information about A (if B is true, the implication is always true). There are lots of ways to do it, but the most common technique is using the A information to get to the B conclusion; when both are true, the implication is true.

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

So the first lesson is you must be prepared to give a substantial reason for **every** step of your proof. These substantial reasons are based on a particular *frame of reference*. The frame of reference of the above example is simple 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 classes 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 $n = 2k$ for some integer k, you can prove lots of things by substituting these definitions:

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

This statement is an implication and as stated earlier, one way to proceed is to prove that the conclusion is true. To do this, we can use the information given in the hypothesis. Therefore, we know that n is an even number so we can substitute the definition of an even number for n:

n is even: $n = 2k$ for some integer k

$(-1)^n = (-1)^{2k}$	substitution
$((-1)^2)^k$	property of exponents
$(1)^k$	$(-1)^2 = 1$
$(1)^k = 1$	by the laws of exponents

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

Now that you have a general feeling for proof, we need to look more closely at the thought process and the different techniques that can be used to do proofs.

Direct Proof

Direct proof is a technique where we prove an implication by showing that the conclusion B must be true when the hypothesis A is true. Therefore, the proof consists of attempting to find a link between the statements we know are true in the hypothesis, and what we are trying to prove in the conclusion. This technique uses a thought process called forward-backward, because we may begin by working backward from B or by working forward from A. We used this technique in the above example with even numbers. In that example, the link was very obvious, but this is not often the case.

Step 1: Recognize the A and B parts of the statement to be proven and determine the frame of reference. This will be the first step of all our proof techniques.

> If the right triangle XYZ with sides of length x & y, and hypotenuse of length z, has an area of $(z^2)/4$, then the triangle XYZ is isosceles.
>
> A: right triangle XYZ with sides of length x & y, and hypotenuse of length z, has an area of $(z^2)/4$.
>
> B: XYZ is isosceles.

The frame of reference is the information we need about the particular area of the implication. In this example, we need information about geometry, triangles and probably some basic algebra.

Step 2: Formulate the abstraction question:

Assume A is true and use this information to reach the conclusion that B is true. We can work forward from A or backward from B. We usually begin working backward by formulating the *abstraction question*: "How or when can I conclude that B is true?". This question must be phrased in a general way concerning the problem at hand. A good abstraction question for the example above is "How can I show that *any* triangle is isosceles?". Notice this is not in terms of triangle XYZ.

Step 3: Answer the abstraction question:

a) Show that two of the triangle's sides have equal length.
b) Show that x = y. (B1)

Now we have a new statement B1 (Show x=y) with the property that if you can prove B1 is true, then B is true. So, now we focus on proving B1 is true.

Step 4: Continue doing Steps 2 (formulate a new abstraction question based on B1) and (answer the abstraction question) until you find that you cannot answer the abstraction question posed, or you reach statement A.

How can I show that two real numbers are equal?

a) Show that their difference = 0.
b) Show that x - y = 0. (B2)

How can I show that x - y = 0?

We are going in circles now (show that x=y); we have posed a question that we cannot answer so this is a clue to start the forward process.

Step 5: Using the last abstraction answer (B2), use the information in A to come up with a statement A1 which is true because A is true. The goal is to find a way to match the final B abstraction answer.

A1: $xy / 2 = (z^2) / 4$	(area of a right triangle = 1/2 base * height)
A2: $x^2 + y^2 = z^2$	(Pythagorean theorem)
A3: $xy/2 = (x^2 + y^2) / 4$	(substitute: we need x and y not z)
A4: $x^2 - 2xy + y^2 = 0$	(rewrite A3 to look like B2; multiply both sides by 4 and subtract 2xy from both sides.)
A5: $(x - y)^2 = 0$	(factor)
A6/B2 : $x - y = 0$	(square root of each side)
B1: $x = y$	add y to both sides

Therefore, If the right triangle XYZ with sides of length x & y, and hypotenuse of length z, has an area of $(z^2)/4$, then the triangle XYZ is isosceles.

Notice that the forward process consists of rewriting statements in different forms until we finally reach the final abstraction answer. This requires detailed knowledge of the frame of reference, insight and some trial and error.

Forward-backward is a fundamental technique used in many of the proof methods we will study. We have used it here to do direct proof. Note that we seldom would include all the details we went through (as above) to complete the proof. In fact, the forward-backward process may be intuitive for you. One more example:

Prove: If x and y are nonnegative real numbers that satisfy x+y = 0,
then x = 0 and y = 0.

Statement	Reason
x >= 0	given
x = -y	subtraction on given statement
-y <= 0	y >= 0 so therefore -y must be <= 0
x <= 0	substitution
x = 0	definition of a real number equaling 0: x <= 0 and x >= 0
0 + y = 0	substitution
y = 0	identity law

Therefore, If x and y are nonnegative real numbers that satisfy x+y = 0,
then x = 0 and y = 0.

Notice that the abstraction question was: How can I show that a real number is 0? We use a definition from the frame of reference (arithmetic) to answer this question: if x <= 0 and x >= 0 then x = 0.

Indirect Proof: Contradiction

An indirect proof is one where we take a roundabout route from hypothesis to conclusion: a statement is shown to be true by showing that its negation is false. Recall that the only case where the implication "if A, then B" is false is when B is false. In a proof by contradiction, you rule out this possibility by assuming B is false and then finding a contradiction.

To do a proof by contradiction of an implication, the first step (as usual) is to find the A and B parts. Then, you write a new proof statement where B is false. You then assume A is true and use the forward-backward technique with the new B conclusion. You keep going until you reach a statement that cannot be true.

Prove: If n is an integer and n^2 is even, then n is even.

New statement: If n is an integer and n^2 is even, then n is odd.

Statement	Reason
n = 2k + 1 for some integer k	definition of an odd number
$n^2 = (2k + 1)^2$	square both sides
$n^2 = 4k^2 + 4k + 1$	algebra
$n^2 = 2 (2k^2 + 2k) + 1$	algebra
$2k^2 + 2k$ is an integer	k is an integer
$n^2 = 2k + 1$	substitution
n^2 is odd	definition of odd number - contradiction

Since we have arrived at a contradiction (n^2 is odd when "n^2 is even" is a given), we have proven: if n is an integer and n^2 is even, then n is even.

Note the form of a formal proof (whether direct or indirect) as illustrated above. The statement to be proven is given (and in the case of proof by contradiction, the "new" statement is also given); then a statement and reason chart is given *with all detailed steps included*. Finally, a concluding statement is given summarizing why the statement is true. **Always include all three of these steps in your proofs on problem sets to avoid losing points.**

There are some classic little problems using contradiction. Here is a famous one:

* Suppose there are only two types of people living on an island: knights and knaves. Knights always tell the truth and knaves always lie:

A says: B is a knight.
B says: A and I are of opposite types.

What are A and B? To find out who's who, we have four possibilities: A & B are both knights; A is a knight and B is a knave; A is a knave and B is a knight; A and B are both knaves. We'll start by assuming that A is a knight and see if we come up with a contradiction.

If A is a knight, he always tells the truth so B is also a knight. That means B also always tells the truth, but B says something contradictory. So, A cannot be a knight.

If A is a knave, then he is lying so B is also a knave. B also lies by saying they are of opposite types. Therefore, A and B must both be knaves.

(From Smullyan: What is the Name of this Book?). By finding contradictions, we were able to find the solution. This example is also important as an illustration of a **proof by cases**. A proof by cases is where we must analyze more than one possibility to prove a particular statement.

Quantifiers 1: Construction

The next two topics concern implications that have an additional twist: the terms "for all" or "there exists" which are called **quantifiers** because they refer to some quantity or number of elements for which a property is true. These types of implications are very common. We will discuss **existential** implications first. They have the form:

> There is an object with a certain property such that something is true.

The first step in proving these statements is recognizing the object, property, and the something that is true. Then you proceed by using the **construction** method. The basic idea is to just construct the object, which makes the statement true. In addition, you must show that the object has the "certain property" and the "something is true". But, we only need one object to prove the statement true.

Sometimes you construct the object by trial and error, or you might develop an algorithm to produce the desired object.

> Prove: There exists an integer n that can be written in two ways as a sum of two prime numbers.
>
> object: integer n
> property: none really except that n is an integer
> something is true: n can be written two ways as a sum of two prime numbers.
>
> By trial and error, n = 10: 5 + 5 = 10 and 7 + 3 = 10. Therefore, there exists an integer n that can be written in two ways as a sum of two prime numbers.

Quantifiers II: Counterexample and Choose

Implications with the words "for all" are **universal** implications. They have the form:

> For all x in S, if A(x) then B(x).

The first step in proving such an implication is to get it into this form. Then, we can proceed a couple different ways. One is to find a **counterexample** thereby proving the statement is false (it doesn't work for all).

> Prove: All primes are odd.
>
> New statement: For all integers k, if k is prime, then k is odd.
>
> 2 is a prime number and is not odd. Thus, by counterexample all primes are not odd.

Another method is called the **choose** method, which is based on the following idea: To show that every element in a set satisfies a particular property, suppose an element x is a particular but arbitrarily chosen element of the set, and show that x satisfies that property. The point of having x be arbitrarily chosen (or generic) is to make the proof general, i.e., you are making no special assumptions about x that are not also true of all the other elements of S. So, whatever you prove about x, you can prove about any other element in the set. *You must be careful to keep the objects generic.*

> Prove: The sum of any two even numbers is also even.

New statement: For all integers m and n, if m and n are even, then m+n is even.

Suppose m and n are particular but arbitrarily chosen even integers, we must show that m+n is also even. To do so, we use the definition of an even integer (m = 2r for some integer r and n = 2s for some integer s; note that we use different letters because we don't want to set up a special case).

Statement	Reason
m+n = 2r + 2s	substitution
m+n = 2(r + s)	factor out the two
r+s is an integer k	r is an integer and s is an integer and the sum of any two integers is an integer.
m + n = 2(k)	substitution
m + n is even	definition of an even number.

Therefore, the sum of any two even numbers is also even.

Some Famous Conjectures

There are many conjectures that have never been proven or disproved, some of which seem so simple that one might think they are easy to prove. Some famous ones:

1) Goldbach's Conjecture: If n is an even integer > 2, then n can be represented as the sum of two primes.

Note that 4 = 2+2, 6 = 3+3, 8 = 5+3, 10 = 5+5, 12 = 7+5, etc. No one has proven this but computer calculations show this is true for all integers up to 100,000,000.

2) Euler's conjecture that $a^4 + b^4 + c^4 = d^4$ has no integer solution. This was accepted as true for 200 years until it was proven wrong by one counterexample:

$95800^4 + 217519^4 + 414560^4 = 422481^4$

(It was also proven wrong formally by Elkies at Harvard)

3) Fermat's Last Theorem: It is impossible to find positive integers x, y, z such that $x^n + y^n = z^n$ for n >= 3 (there are solutions for n = 2 e.g., $3^2 + 4^2 = 5^2$)

Fermat wrote this theorem in the margin of a book he was reading about 350 years ago. He wrote beside it: "I have discovered a truly remarkable proof of this theorem which this margin is too small to contain." This was one of the most famous open questions in mathematics until recently when it was proven by Andrew Wiles of Princeton.

There will always be open conjectures in mathematics. Recall that Gödel's Undecidability Theorem states that it is not always possible to find a proof for every true statement in a mathematical system. Thus, we may never be able to establish whether certain conjectures are actually true.

More Proofs

The best way to sharpen your skills at doing proofs is to just try and do them. The following problems can be used for additional practice.

1) You are visiting the island described above where only knaves and knights live. You meet two natives Fred and Barney. Fred says: Barney is a knave. Barney says: Fred is a knave. Are either Fred or Barney a knave?

There is one knave. Fred and Barney cannot both be knights because then both would be knaves (knights only tell the truth). This is a contradiction. Fred and Barney cannot both be knaves either because then both would be telling the truth which is impossible for knaves. The only possible answer is that one is a knight and one is a knave - one is telling the truth and one is lying.

2) Give a direct proof of the following: if a, b and c are integers and b is divisible by a and c is divisible by a, then (b-c) is divisible by a.

Statement	*Reason*
*b = a * r for some integer r*	*definition of divisibility*
*c = a * s for some integer s*	*definition of divisibility*
b - c = ar - as	*substitution*
b - c = a(r - s)	*distributive law*
r - s is an integer	*r and s are both integers & so is their difference*
b-c is divisible by a	*definition of divisibility*

Therefore, if a, b and c are integers and b is divisible by a and c is divisible by a, then (b-c) is divisible by a.

3) Find the error in the following proof: If a and b are even integers, then a * b is also an even integer.

Statement	Reason
a = 2 * c for some integer c	definition of even
b = 2 * c for some integer c	definition of even
a * b = 2c * 2c	substitution
$2c * 2c = 2(2c^2)$	multiplication
2 * c * c is an integer	product of integers is an integer
a* b = 2 * an integer	substitution
a* b is even	definition of even

Using the same symbol c for the representation of a and b severely limits the generality of this proof. By saying that a = 2c and b = 2c, the proof specifies that a = b and, therefore, we are only proving the statement for the case where a = b. A correct "choose method" proof must deduce the conclusion for all integers a and b, so we need a different symbol for b's representation.

4) Give a proof by contradiction of the following statement: if a, b, & c are integers and if bc is not divisible by a, then b is not divisible by a.

negation of conclusion: if bc is not divisible by a, then b IS divisible by a.

*b = a * k for some integer k*	*definition of divisibility*
*bc = (a * k)c*	*multiply both sides by c*
*bc = a * (kc)*	*associative law*
kc is an integer	*product of integers is an integer*
bc is divisible by a	*definition of divisibility (contradiction)*

Since we have arrived at a contradiction (bc is divisible by a when "bc is not divisible by a" is a given), we have proven: if a, b, & c are integers and if bc is not divisible by a, then b is not divisible by a.

5) Give a proof by construction of the following: There exists three consecutive odd prime integers a, b, and c.

By trial and error: 3, 5 and 7. Therefore, there exists three consecutive odd prime integers a, b, and c.

6) Give a proof using the Choose method: For all integers m and n, if n - m is even, then $n^3 - m^3$ is even.

Suppose m and n are any particular but arbitrarily chosen integers such that n - m is even. (The whole idea of this proof is to transform $n^3 - m^3$ to some format that uses n - m since the only fact we have is that n - m is even).

$n^3 - m^3 = (n - m)(n^2 + nm + m^2)$	*factoring & multiplication*
n - m is even	*given*
$(n^2 + nm + m^2)$ is an integer	*products and sums of integers are integers*
$(n - m)(n^2 + nm + m^2)$ is even	*product of an even integer and an integer is even (see below)*
$n^3 - m^3$ is even	*substitution*

"helper proof": The product of an even integer and an integer is even.

*m = 2 * k*	*m is even*

*x = m * n*	*given*
*x = (2k) * n*	*substitution*
x = 2(kn)	*associative*
kn is an integer	*k and n are integers and so is their product*
x is even	*definition of even*

Therefore we have proven: For all integers m and n, if n - m is even, then $n^3 - m^3$ *is even.*

Bibliography

G. Pólya, *How to Solve It*, Garden City, NY: Doubleday, 1957.

G. Pólya, *Mathematical Discovery,* New York: Wiley, 1962.

R. Smullyan, *What is the Name of This Book - The Riddle of Dracula and Other Logical Puzzles*, Englewood Cliffs, NJ: Prentice Hall, 1978.

D. Solow, *How to Read and Do Proofs*, New York: Wiley, 1982.

Historical Notes

Doing proofs was an integral part of deductive reasoning as introduced by Aristotle. He defined many of the rules of inference defined in the propositional logic handout. Euclid (*Elements of Geometry*) used many of Aristotle's techniques to prove geometric properties around 300 BC. Probably the first, and one of the most famous proofs by contradiction is Euclid's proof of the irrationality of sqrt(2). Proofs were also an essential component of symbolic logic (Leibniz, Boole and DeMorgan).

If you are interested in how Wiles proved Fermat's Last Theorem, I have a brief description of the proof; send me some email or stop by during office hours. The following is a report received just after the proof was announced:

Subject: Take That, Fermat!

Here is a recent report on Wiles' proof.
-=-
News Item (June 23)-Mathematicians worldwide were excited and pleased today by the announcement that Princeton University professor Andrew Wiles had finally proved Fermat's Last Theorem, a 356-year-old problem said to be the most famous in the field.

Yes, admittedly, there was rioting and vandalism last week during the celebration. A few bookstores had windows smashed and shelves stripped, and vacant lots glowed with burning piles of old dissertations. But overall we can feel relief that it was nothing- nothing- compared to the outbreak of exuberant thuggery that occurred in 1984 after Louis deBranges finally proved the Bieberbach Conjecture.

"Math hooligans are the worst," said a Chicago Police Department spokesman. "But the city learned from the Bieberbach riots. We were ready for them this time."

When word hit Wednesday that Fermat's Last Theorem had fallen, a massive show of force from law enforcement at universities all around the country headed off a repeat of the festive looting sprees that have become the traditional accompaniment to triumphant breakthroughs in higher mathematics.

Mounted police throughout Hyde Park kept crowds of delirious wizards at the University of Chicago from tipping cars over on the midway as they first did in 1976 when Wolfgang Haken and Kenneth Appel cracked the long-vexing Four-Color Problem. Incidents of textbook-throwing and citizens being pulled from their cars and humiliated with difficult story problems last week were described by the university's math department chairman Bob Zimmer as "isolated."

Zimmer said, "Most of the celebrations were orderly and peaceful, But there will always be a few-usually graduate students-who use any excuse to cause trouble and steal. These are not true fans of Andrew Wiles."

Wiles himself pleaded for calm even as he offered up the long elusive proof that there is no solution to the equation $x^n + y^n = z^n$ when n is a whole number greater than two, as Pierre de Fermat first proposed in the 17th Century. "Party hard but party safe," he said, echoing the phrase he had repeated often in interviews with scholarly journals as he came closer and closer to completing his proof.

Some authorities tried to blame the disorder on the provocative taunting of Japanese mathematician Yoichi Miyaoka. Miyaoka thought he had proved Fermat's Last Theorem in 1988, but his claims did not bear up under scrutiny of professional referees, leading some to suspect that the fix was in. And ever since, as Wiles chipped away steadily at the Fermat problem, Miyaoka scoffed that there would be no reason to board up windows near universities any time soon; that God wanted Miyaoka to prove it.

In a peculiar sidelight, Miyaoka recently took the trouble to secure a U.S. trademark on the equation "$x^n + y^n = z^n$" as well as on the now-ubiquitous expression, "Take that, Fermat!" Ironically, in defeat, he stands to make a good deal of money on cap and T-shirt sales.

This was no walk-in-the-park proof for Wiles. He was dogged, in the early going, by sniping publicity that claimed he was seen puttering late one night doing set theory in a New Jersey library when he either should have been sleeping, critics said, or focusing on arithmetic algebraic geometry for the proving work ahead.

"Set theory is my hobby, it helps me relax," was his angry explanation. The next night, he channeled his fury and came up with five critical steps in his proof. Not a record, but close.

There was talk that he thought he could do it all by himself, especially when he candidly referred to University of California mathematician Kenneth Ribet as part of his "supporting cast," when most people in the field knew that without Ribet's 1986 proof definitively linking the Taniyama Conjecture to Fermat's Last Theorem, Wiles would be just another frustrated guy in a tweed jacket teaching calculus to freshmen.

His travails made the ultimate victory that much more explosive for math buffs. When the news arrived, many were already wired from caffeine consumed at daily colloquial teas, and they took to the streets en masse shouting, "Obvious! Yessss! It was obvious!"

The law cannot hope to stop such enthusiasm, only to control it. Still, one has to wonder what the connection is between wanton pillaging and a mathematical proof, no matter how long-awaited and subtle.

The Victory Over Fermat rally, held on a cloudless day in front of a crowd of 30,000 (police estimate: 150,000) was pleasantly peaceful. Signs unfurled in the audience proclaimed Wiles the greatest mathematician of all time, though partisans of Euclid, Descartes, Newton and C.F. Gauss and others argued the point vehemently.

A warmup act, The Supertheorists, delighted the crowd with a ragged song, "It Was Never Less Than Probable, My Friend," which included such gloating, barbed verses as- "I had my proof all ready/But then I did a choke-a/Made liberal assumptions/Hi! I'm Yoichi Miyaoka."

In the speeches from the stage, there was talk of a dynasty, specifically that next year Wiles will crack the great unproved Riemann Hypothesis ("Rie-peat! Rie-peat!" the crowd cried), and after that the Prime-Pair Problem, the Goldbach Conjecture ("Minimum Goldbach," said one T-shirt) and so on.

They couldn't just let him enjoy his proof. Not even for one day. Math people. Go figure 'em.

-=-

Note: if you are interested in other famous unsolved problems, check out:

R.K. Guy, *Unsolved Problems in Number Theory*, New York: Springer-Verlag, 1980.