

Mathematical Proofs

John C. Mitchell & Maggie Johnson
Department of Computer Science
Stanford University

1. Why write proofs?

According to *Webster's Unabridged Dictionary*, the word *prove* comes from the Latin verb *probare* which means *to try* or *to test*. Two Webster's dictionary definitions are

- To try or to ascertain by an experiment, or by a test or standard....
- To evince, establish, or ascertain, as truth, reality, or fact, by argument ...

These two definitions reflect a distinction developed by philosophers, namely, the difference between analytic and synthetic statements. Putting it briefly, some statements are best confirmed by experiment and other statements are best confirmed by argument. If I were to tell you, while sitting in a room with no windows, that it is raining outside right now, then there is no amount of argument that would be as convincing as stepping outside to see for yourself. The statement "it is raining" is not an analytical statement about the relationship between concepts, but a synthetic proposition about the world that might or might not be true at any given time. In contrast, mathematical statements, such as $\forall x \forall y (x+y = y+x)$ are analytical statements that are better proved by argument than by experiment.

Analytic and synthetic statements

Aristotle and his followers for hundreds of years believed that objects fall at a speed proportional to their weight. This belief is a belief about the world around us. When Galileo wanted to prove that objects of different size fall at the same rate, for example, he conducted a series of careful experiments, timing pendulums and rolling balls of different size down an inclined plane. Many other basic laws of physics can also be confirmed by experiment. In terminology used by philosophers, a statement is synthetic if its truth or falsity depends upon the way the world is. Generally speaking, synthetic statements must be verified by direct observation of the world, or by deduction from statements that have been verified by direct observation.

To see how mathematical properties are different, we can think about Pythagoras' rule for right triangles: the square of the length of the hypotenuse is equal to the sum of the squares of the other two sides. If you want to convince a skeptical friend that this is true, you could try doing some experiments. If you draw four or five right triangles and measure their sides, you can build up some evidence for this rule. But since the rule is meant to apply to all of the infinitely many triangles we might draw, experiment is not the most convincing method. The accepted standard in mathematics is that statements must be proved by a form of argument that conforms to rigorous standards. In geometry, the Pythagorean Theorem is proved from accepted principles by a sequence of deductive steps that will convince anyone familiar with mathematics or logic that the theorem is true for all triangles. In terminology used by philosophers, a statement is analytic if its truth or falsity depends only on the meanings of the words used in the statement.

Generally speaking, analytic statements can be established by reasoning about the definitions of words and the relationships between the concepts involved. For example, a proof of the Pythagorean Theorem relies on the definitions of hypotenuse, right triangle, square of a number, and so on.

Logic and mathematical proof

A mathematical proof is an argument that begins with a set of postulates or assumptions and proceeds to a conclusion by agreed methods of argument. Logic is the field of inquiry concerned with identifying sound methods of argument and mathematical logic is a branch of logic that defines sound methods of argument rigorously and studies them.

Analytical methods in computer science

Computer science is the science and engineering discipline concerned with the design and production of computer hardware, the design and production of software that allows programmable hardware to perform useful functions, and the basic principles that underlie computer hardware, software, and their applications. Although computers are physical devices, computer software is often designed around concepts that come from or resemble mathematics. Therefore, reasoning about programs and the way they structure and manipulate data often involves analytical statements and mathematical reasoning.

A fundamental concept in computer science is abstraction and one of the most important skills of any successful computer scientist is the ability to move easily from one level of abstraction to another. For example, consider a computer program that uses numerical input to guide an airplane. At one level of abstraction, the computer is a set of silicon chips and wires, changing the charges on wires and parts of the chips as the program runs. The charges take time to propagate from one place to another, the wires have resistance and capacitance, and there can be magnetic effects or interference between one piece of hardware and another. At a higher level of abstraction, we can ignore the detailed physics of electronic impulses and think of the computer as an arrangement of logical gates, carrying values 0 and 1 from place to place. At another level of abstraction, we can think about the kinds of data explicitly mentioned in the program, such as integers, floating point numbers, and arrays, ignoring the fact that each of these is represented by a sequence of bits. At this level, the computer manipulates mathematical objects and the behavior of the program can be understood using mathematical principles associated with numbers and operations like addition, multiplication, trigonometric functions, and so on. In computer science, experimental methods are often used to try to understand the behavior of complex systems. Mathematical proofs, however, are important in designing and reasoning about data structures, algorithms, programs, and other computational concepts that can be defined abstractly in the same way as numbers and triangles.

2. The Gold Standard

Gold has been used in trade for thousands of years. From the Wikipedia: "Due to its rarity and durability, gold has long been used as a means of payment. The exact nature of the evolution of money varies significantly across time and place, though it is believed by historians that gold's high value for its utility, density, resistance to corrosion, uniformity, and easy divisibility made it useful both as a store of value and as a unit of account for stored value of other kinds..."

The interesting thing here is that it was gold itself that was valued. When you paid with a gold coin, you weren't providing a promise to deliver value; you were paying with the valuable thing.

3. Silver Certificates and Federal Reserve Notes

When paper money was introduced, it was often issued as a stand-in for precious metals, redeemable on demand. In the United States, silver certificates were issued from 1878 until 1968. One dollar silver certificates bore the obligation:

This certifies that there has been deposited in the Treasury of the United States of America One Silver Dollar payable to the bearer on demand.

As a result, every paper payment was backed by silver; anyone who didn't trust the U.S. paper money could go trade paper bills for silver. It might be helpful to think about proofs in a similar way. The most convincing proofs are formal proofs; these are the "precious metals" of mathematics. However, just as gold and silver are heavy and difficult to carry around, formal proofs can be long and complicated. Therefore, in common everyday mathematics, mathematicians and computer scientists use shorter English proofs instead. But just as the U.S. government backed its paper money with silver, every proof should be backed by a formal proof, or the ability in principle to construct a formal proof from the less formal English proof if needed. In practice, some authors find themselves in a hurry, or believe that they can more effectively convey useful information if they use some form of reasoning that is not very close to a formal proof. If you go on in computer science and prove things as part of your work, you may also find yourself drifting from the rigor of formal proof. This is not necessarily bad, as long as you reason correctly and your arguments are convincing and easily accepted by your audience. In fact, some mathematicians accept the following definition of proof:

A proof is an argument that convinces your audience.

Although the analogy is not very accurate, we might compare proof sketches and informal arguments to the Federal Reserve Notes that the U.S. government issued after silver certificates were discontinued in 1968. For those curious about the monetary system, U.S. paper money is now simply backed by U.S. law, which states that paper money is "legal tender for all debts public and private." In other words, if someone owes you an amount of money, and they present you with paper money, then by U.S. law they have paid their debt. In this class, we would like you to produce "semi-formal proofs", or silver certificates: arguments written in clear, understandable prose, using columns of formulas and their justifications as you choose, that you know you could convert to formal proofs if asked. This is a useful practice when you are learning to write mathematical proofs. Later, when you have more experience, you can issue your own "Federal Reserve Notes."

Standard of proof in this class

Here is how we would like to think about proofs:

- **Gold standard:** The true, undoubted proof of a statement is its formal proof. The proofs we did in Fitch were true formal proofs. As we saw in Fitch, the definition of a formal proof system is clear and unambiguous. We can mechanically check that a formal proof is written correctly, without using any creativity or ingenuity. Since the formal proof system we use has been proved sound, a correctly written formal proof demonstrates without a doubt that the conclusion follows from the assumptions.

- **Silver certificates:** A semi-formal proof should be a simplified way of conveying the same information as a formal proof. A skilled mathematician, logician or computer scientist should accept a semi-formal proof if that person can see how the argument could be converted to a formal proof, given enough time and energy. We think of semi-formal proofs as statement/reason chart proofs or *detailed* prose proofs.
- **Federal reserve notes:** In practice, many mathematical proofs do not contain all of the details that would be needed to construct a formal proof. Experienced mathematicians and computer scientists who do analytical work write informal proofs that are convincing to their audience. They have learned what steps can be left out so that the soundness of the argument and the flow of the proof are not affected.

In this class, please give formal proofs when the problem asks you to do so, and silver certificate proofs otherwise. In other words, even if you write your proof out in English, think about the problem carefully enough so that you are convinced that you could produce a formal proof if you needed to. As you gain more experience, this will become easier to do. Here are some things you can omit from proofs (unless you are asked to give a formal proof), assuming that an intelligent teaching assistant or grader is able to fill in the missing details (that's your audience):

1. Simple algebraic reasoning, of the sort you would do in a high-school algebra class. For example, you could simplify $3(x + 2x) + 4(x - 1)$ to $13x - 4$ in a single step without going through the calculation.
2. Simple tautologies and logical identities can be omitted, as long as the problem is not to prove a propositional tautology.
3. Anything previously proven on a problem set, in a handout or in the text, can simply be cited as a step in a proof.

4. Examples of Form

Formal Proof (Gold Standard)

Given: $(P \wedge R) \rightarrow Q$

P

Prove: $R \rightarrow Q$

1. $(P \wedge R) \rightarrow Q$							
2. P							
<table style="border-collapse: collapse;"> <tr> <td style="border-left: 1px solid black; padding-left: 10px;">3. R</td> <td></td> </tr> <tr> <td style="border-left: 1px solid black; padding-left: 10px;">4. $P \wedge R$</td> <td>\wedge Intro 2, 3</td> </tr> <tr> <td style="border-left: 1px solid black; padding-left: 10px;">5. Q</td> <td>\rightarrow Elim 1, 4</td> </tr> </table>	3. R		4. $P \wedge R$	\wedge Intro 2, 3	5. Q	\rightarrow Elim 1, 4	
3. R							
4. $P \wedge R$	\wedge Intro 2, 3						
5. Q	\rightarrow Elim 1, 4						
6. $R \rightarrow Q$	\rightarrow Intro, 3-5						

Therefore, $R \rightarrow Q$

Semi-Formal Proof (Silver Certificate)

Example: Statement/Reason Chart

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.

Example: Prose Form

Prove: The set of prime numbers is infinite.

Proof by Contradiction: Suppose not; i.e. suppose the set of prime numbers is finite. Then all prime numbers can be listed, say, in ascending order:

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \dots, p_n.$$

Consider the integer $N = (p_1 * p_2 * p_3 * \dots * p_n) + 1$. Then, $N > 1$. We will show elsewhere that any integer $n > 1$ is divisible by a prime, so N is divisible by some prime number p . But none of the primes $p_1 \dots p_n$ divides N , because dividing N by each of them produces a remainder of 1. So p must be some prime not in the list p_1, \dots, p_n , which contradicts the assumption that the list includes every prime. So the set of prime numbers is infinite.

Informal Proof (Federal Reserve Note) (from Rosen, *Discrete Mathematics and its Application*)

Prove: For every positive integer n , there is an integer divisible by more than n primes.

“Proof”: Let p_1, p_2, \dots, p_{n+1} be the first $n+1$ prime numbers. Then $p_1 * p_2 * \dots * p_{n+1}$ is divisible by more than n primes.

What’s missing from this proof?

Remember: Give formal proofs when the problem asks you to do so, and semi-formal proofs otherwise. In other words, even if you write your proof out in English, think about the problem carefully enough so that you are convinced that you could produce a formal proof if you needed to. Do not give informal proofs unless we specifically ask you to do so.

5. False methods of proof (humor)

Over the years, we've seen many humorous list of false proof methods. This list, lifted from <http://jwilson.coe.uga.edu/EMT668/EMAT6680.F99/Challen/proof/proof.html> might amuse you.

Be sure *not* to use any of these methods in CS103!

Proof by obviousness: "The proof is so clear that it need not be mentioned."

Proof by general agreement: "All in favor?..."

Proof by imagination: "Well, we'll pretend it's true..."

Proof by convenience: "It would be very nice if it were true, so..."

Proof by necessity: "It had better be true, or the entire structure of mathematics would crumble to the ground."

Proof by plausibility: "It sounds good, so it must be true."

Proof by intimidation: "Don't be stupid; of course it's true!"

Proof by lack of sufficient time: "Because of the time constraint, I'll leave the proof to you."

Proof by postponement: "The proof for this is long and arduous, so it is given to you in the appendix."

Proof by accident: "Hey, what have we here?!"

Proof by insignificance: "Who really cares anyway?"

Proof by mumbo-jumbo: $\forall \alpha \in \Phi \exists \beta \ni \alpha \delta \beta \asymp \delta \dots$

Proof by profanity: (example omitted)

Proof by definition: "We define it to be true."

Proof by tautology: "It's true because it's true."

Proof by plagiarism: "As we see on page 289,..."

Proof by lost reference: "I know I saw it somewhere...."

Proof by calculus: "This proof requires calculus, so we'll skip it."

Proof by lack of interest: "Does anyone really want to see this?"

Proof by logic: "If it is on the problem sheet, it must be true!"

Proof by majority rule: Only to be used if general agreement is impossible.

Proof by clever variable choice: "Let A be the number such that this proof works..."

Proof by tessellation: "This proof is the same as the last."

Proof by stubbornness: "I don't care what you say- it is true."

Proof by simplification: "This proof reduced to the statement $1 + 1 = 2$."

Proof by hasty generalization: "Well, it works for 17, so it works for all reals."

Proof by deception: "Now everyone turn their backs..."

Proof by supplication: "Oh please, let it be true."

Proof by poor analogy: "Well, it's just like..."

Proof by avoidance: Limit of proof by postponement as it approaches infinity

Proof by design: If it's not true in today's math, invent a new system in which it is.

Proof by authority: "Well, Don Knuth says it's true, so it must be!"

Proof by intuition: "I have this gut feeling."

Proof by Fermatation: Claim a remarkable proof will not fit in the space provided. Wait 356 years.