Some Help on Reading Mathematics and Creating Proofs   rev. 1/21/03

Math 109 is an introduction to proofs and some mathematical concepts. Some written sources of advice are

- Comments on definitions (below).
- Pages xviii-xix of my text *Mathematical Methods in Artificial Intelligence* on reading mathematics (below)
- Why do we need proofs of obvious results (below)
- A possible taxonomy of proofs (below)
- Sections 0.3-0.4 of the Math 166 text: *Introduction to the Theory of Computation* by M. Sipser (excerpts below)
- Advice on discovering proofs from a book review by Silverman (below)
- Comments on negation (below)
- Proof by induction: (ps pdf) Appendix A of *Foundations of Applied Combinatorics* by E.A. Bender and S.G. Williamson. (There are many other sources.)
- *Mathematical Thinking: Problem Solving and Proofs* by J.P. D'Angelo and D.B. West

---

People are sometimes confused about what needs to be proved when "if" appears. Here are the three main cases:

- **"Theorem**: If A then B.**"**   means you must prove that whenever A is true, B is also true.
- **"Theorem**: A if and only if B.**"**   means you must prove that A and B are true and false at the same time. In other words, you must prove "If A then B" and "If not A then not B". Equivalently, you must prove "If A then B" and "If B then A".
- **"Theorem**: A only if B.**"**   means you must prove "If A then B", so there is no reason to use this form of a statement.

The importance of a comment attributed to E. Bishop (1985) cannot be overemphasized: "Do not ask whether a statement is true until you know what it means." Many students often attempt to prove something without understanding what they are trying to prove. Rather than leading to understanding, it usually reveals that the student doesn't understand the statement. To know what a statement means, you must understand all the concepts in the statement separately *and also* how the statement says they are related to one another.

This leads to an important question: **What is a definition?** Although the answer sounds obvious, people often miss the fact that "definition" is used in two different ways. An **extracted** definition is based on the common usages of a word. It may not say precisely what the word means; for example, the definition of when objects are called "chairs". As common usage shifts, extrracted definitions shift. A **stipulated** definition spells out precisely what a concept means in terms of other known concepts. This is usually the situation in games; for example, the definition of "touchdown" in football. Mathematical definitions are stipulated: They explain precisely in terms of previous concepts what a new concept means. Inevitably, there are some basic concepts that mathematicians don't define such as "point" and "line" in Euclidean geometry. This leads to another question: **Why be so precise?** Without such precision, it becomes unclear what has been proved and whether the proof is correct. Such uncertainty affects more than mathematics: Would you want to fly on an airplane whose design depended in part on mathematical computations based on numerical methods for solving differential equations to within a desired degree of accuracy that we think are correct? Would you like your doctor to rely on a CAT scan (which uses mathematically based image reconstruction techniques) if the techniques are based on flawed mathematics? As a scientist, would you be willing to reject a theory if sophisticated mathematical computations showed that it contradicted experimental results, but you weren't sure the mathematics was correct?

In doing mathematics, we deduce results from stipulated definitions and from other results that have been previously deduced from stipulated definitions. Hence it is **very important** to understand what a definition means. This understanding should be on two levels. The formal level, which is essential for deducing results, is the understanding of the statement so that you can decide when something fulfills the conditions in the

definition; for example, when a figure is an isosceles triangle or when a differential equation is exact. The informal level, which is not always present, is an understanding that let's you see what might be true. It may be in the notation or it may be a way of thinking about the concept. For example, a derivative is defined precisely in terms of a limit of ratios and is written dx/dt as if it were actually a ratio --- which it is not. This leads to an informal treatment of a derivative as if it were actually a ratio, which usually leads to correct results. However, it is not a proof of those results. Another example: checkmate in chess can be thought of as "the king can be captured on the next move". This is not quite correct since there would be no next move and since it includes the possibility of stalemate.

Reading Mathematics (from *Mathematical Methods in Artificial Intelligence*)

Many people learn mathematics the way I learned history in high school. The exams contained two columns and the goal was to match each date in column A with one of the persons, places, and events in column B. Being lazy, I learned the "whens" of history but never the "whys." I missed a whole world of ideas.

When mathematics is taught and learned by rote, students miss a world of ideas. Mathematics should be learned as an aid to thinking, not as a replacement for it. Learning mathematics is a skill that's seldom taught. If, like many students, you haven't mastered it, the following comments should be helpful.

The key is to work on understanding -- not on memorization. How can you do this?

Let's begin with definitions. Whenever you meet a new concept, develop an understanding of it by relating it to ideas you already know and by looking at what it means in specific cases. For instance, when learning what a polynomial is, look at specific polynomials; when learning what continuity is, see what it means for a specific function like x^2. *The importance of understanding the general through the specific cannot be overemphasized* -- even by using italics. The discussions and examples that immediately precede and follow definitions are often designed to foster understanding. If a definition refers to an earlier, unclear concept, stop! If you proceed, you may end up wandering aimlessly in a foggy landscape filled with shadowy concepts and mirages. Go back and improve your understanding of the earlier concepts so that they're practically solid objects that you can touch and manipulate. Finally, ask yourself why a definition has been introduced: What is the important or useful concept behind it? You may not be able to answer that question until you've read further in the text, but you can prepare your mind to recognize the answer when you see it.

What about theorems? The comments for definitions apply here, too: Look at specific examples, try to relate the theorem to other things you know, ask why it's important. Be sure you're clear on what the theorem *claims* and on what its words *mean*. In addition, attempt to see why the result seems reasonable before you read the proof. Reading and understanding the proof is the last step. If the proof is long, it may be helpful to make an outline of it. But don't mistake the ability to reproduce a proof for understanding. That's like expecting a photograph to understand a scene. There are better tests of understanding: Do you see where all of the assumptions are used? Can you think of a stronger conclusion than that in the theorem? If so, can you see why the stronger conclusion is not true, or at least why the proof is insufficient to establish the stronger conclusion? Examples play a key role in mathematics. In practically every mathematics text, they fall into three categories.

- The type that aren't in the text: They're the ones you create by following the preceding advice.

- The obvious ones that are labeled "example" in the text. They're usually illustrations of definitions, algorithms, or theorems. Sometimes they develop related ideas.

- The type that comes from homework problems: These examples are the s*olutions* to the problems you do yourself, not the problems themselves.

If you neglect any of these three types of examples, your mathematical text will be most useful to you as a doorstop.

Why do We Need Proofs?

It's clear why we need to prove mathematically something that's not obvious, like the Pythagorean Theorem, but why should we prove something that "common sense" tells us is obviously true.

First, if something cannot be proved, there may be something missing. For example, suppose we set up some equations that describe a physical system and it is obvious that the solution exists and is unique (e.g., equations of motion). It may happen that sometimes the equations have no solutions or have more than one solution. This may indicate that something is missing in our translation of a phyical problem into a mathematical one.

Second, if something is obvious to common sense, it might be wrong. For example, at one time common sense taught people that the only possible geometry was Euclidean. We know that is wrong. Here is another example.

- There is a team of three people in a room.
- The master of ceremonies (MC) places either a green sticker or a red sticker on each person's back. The colors are chosen randomly.
- People are allowed to see other people's stickers, but not their own. They may not communicate.
- Simultaneously each person must write one of three things on a sheet of paper without seeing what others write. The choices are:
  I guess my sticker is green.   I guess my sticker is red.   I have no guess.
- The MC collects the papers.
  If at least one person has made a correct guess and nobody has made an incorrect guess, the team wins.
  If there is an incorrect guess or no guesses, the team loses.
- The team knows the rules beforehand and can agree on a strategy.

What strategy should the team adopt? Clearly a guess only has a 50/50 chance of being right. Also, the more guesses there are greater the chance of a wrong guess being made. Therefore it is obvious that the team should select a spokesperson who guesses at random. We've just proved this by appealing to obvious facts and common sense. It is wrong. There is a strategy that lets the team win 3/4 of the time! You can find out about this in ***The Mathematical Intelligencer*** vol. 24 no. 4 (2002).

A Possible Taxonomy of Proof Types

Here is a possible way of describing the various types of proofs. Other people can have a different way. In each case, a theorem is given with at least part of the proof.

- ## Constructive
  - **Existence by Construction** Usually used to show that something exists. One constructs the thing whose existence is claimed. Existence can be proved without construction. See the discussion under [contradiction](#).
    Theorem: Between any two distinct rational numbers a and b there is another rational number c.
    Proof: We show that $c = (a+b)/2$ works. <u>Suppose $a < b$</u>. (The case $b < a$ is similar and is omitted.) We need to show that $a < (a+b)/2$ and that $(a+b)/2 < b$. We do just the first:
      $a < (a+b)/2$ is equivalent to $2a < a+b$,
      which is equivalent to $2a-a < b$,
      which is equivalent to $a < b$,
      which is true (see the underlined statement in the proof.)
  - **Description of All Cases** If there are only a finite number of possibilities
    Theorem: A claim in Boolean logic such as not(not(P)) is equivalent to P.
    Proof: Construct the truth table. In this example P is either **TRUE** or **FALSE**. If P is **TRUE**, not(P) is **FALSE** and so not(not(P)) is **TRUE**. The case P **FALSE** is done similarly.
- ## Non-Constructive

- _**Direct**_ One reasons directly from the hypotheses of the theorem and from known results.
  Theorem: The sum of the degrees of the nodes of a graph is even.
  Proof: Each end of an edge contributes 1 to the sum, so each edge contributes 2. A sum of twos is even.

- _**Indirect**_ In some way, the reasoning is not direct.

  - **Induction** This could have been placed under direct proofs. See a text for a discussion of induction. Theorems with a parameter n are candidates for such proofs. One sometimes has to find n buried in the statement of the theorem, as in this example:
    Theorem: The sum of the degrees of the nodes of a graph is even.
    Proof: We induct on n, the number of edges in the graph. It is obviously true for n=0 (graphs with no edges). Let G be any graph with n+1 edges and let e be an edge. Remove e to obtain a graph G'. By induction, the sum of the degrees of G' is even. Adding e to G' increases the sum by 2. Thus it is true for G.

  - **Contradiction** Assume the hypotheses of the theorem are true and that the conclusion of the theorem is false. Reason (usually directly) to obtain a contradiction. Theorems with a negative conclusion are good candidates for such proofs. Theorems that claim there is only one thing with some properties can be thought of as claiming there do not exist two things with the properties.
    Theorem: The square root of 2 is irrational.
    Proof: (Let s^2 mean the square of s.) Here the negative is in "irrational" = "not rational". Suppose the square root of 2 is rational, say r/s in lowest terms. Square and clear of fractions to obtain $2s$^2 = r^2. Conclude that r is even, say r = 2k. Substitute in and divide by 2: s^2 = 2r^2. Conclude that s is even. We have shown that both r and s are even, contradicting the assumption that r/s is the square root of 2 in lowest terms. This completes the proof.
        Next, we consider an existence result which we'll prove by contradiction.
    Theorem: If a and b are nonzero integers, there are integers x and y such that ax+by is a positive integer and divides both a and b.
    Proof: Let S = { ax+by | ax+by is positive and x and y are integers }. Let d be the smallest integer in S. We claim that d divides both a and b. (Here comes the proof by contradiction.) Suppose this is false. Then **either** d does <u>not</u> divide a **or** d does <u>not</u> divide b.
        Suppose d does <u>not</u> divide a. Then a = qd+r, where r>0 and q are the remainder and quotient when we divide a by d. Since d is in S, d = ax+by for some integers x and y. Then r = a-qd = a(1-qx) + b(qy). Since the things in parentheses are integers and r>0, it follows that r is in S. Since r is the remainder after division by d, r<d and this contradicts the definition of d.
        If d does <u>not</u> divide b, the same type of argument works. This completes the proof.

Excerpts from _Introduction to the Theory of Computability_ by M. Sipser

The following are a few tips for producing a proof.

- _**Be patient**_. Finding proofs takes time. If you don't see how to do it right away, don't worry. Researchers sometimes work for weeks or even years to find a single proof.
- _**Come back to it**_. Look over the statement you want to prove, think about it a bit, leave it, and then return a few minutes or hours later. Let the unconscious, intuitive part of your mind have a chance to work.
- _**Be neat**_. When you are building your intuition for the statement you are trying to prove, use simple, clear pictures and/or text. You are trying to develop your insight into the statement, and sloppiness gets in the way of insight. Furthermore, when you are writing a solution for another person to read, neatness will help that person understand it.
- _**Be concise**_. Brevity helps you express high-level ideas without getting lost in details. Good mathematical notation is useful for expressing ideas concisely. But be sure to include enough of your reasoning when writing up a proof so that the reader can <u>easily</u> understand what you are trying to say.

Advice by J. H. Silverman (Amer. Math. Monthly, 1999) in a book review

What, roughly, are some of the meta-mathematical tools (as opposed to mathematical techniques such as induction) that every mathematician keeps close at hand when tackling a mathematical problem? In no particular order, the following (non-definitive and non-disjoint) list comes to mind: [I've indicated those I think are most effective for textbook problems and those I think are least effective.--Ed B.]

- Do lots of examples, numerical or otherwise. [This gives you a feel for the problem. It's also a very good idea when you're reading mathematics.--Ed B.]
- Specialize the problem. Do special cases. [If you can do a special case, you may be able to build on that method to do the original problem.--Ed B.]
- Generalize the problem. Eliminate unnecessary hypotheses. This technique can be surprisingly effective, since with fewer hypotheses, there are fewer ways to proceed!
- Search for counterexamples to the original problem. [If it is true, you won't find any, but the difficulties you encounter may help you find a proof.--Ed B.]
- Find counterexamples when each of the hypotheses is relaxed. Thus the origin of the phrase "the exception proves the rule," using the original sense of the word "prove" meaning "test the limits of," not "verify the truth of." [This can give you clues as to how the hypotheses will play a role in the proof.--Ed B.]
- Formulate and prove analogous results to provide "evidence" for the validity of the original conjecture.

In addition, every mathematician must acquire various meta-mathematical skills, such as:

- Take a poorly or incompletely posed problem and formulate precise statements to be studied.
- "Fiddle" with a problem, try this-and-that-and-the-other, until eventually some of the ideas that didn't work suddenly fit together to give a solution.

The last item is, in some sense, the most important lesson for a student to absorb.

Comments on Negation

People are sometimes confused about what needs to be proved when "if" appears. Here are the three main cases:

- **"Theorem**: If A then B.**"**   means you must prove that whenever A is true, B is also true.
- **"Theorem**: A if and only if B.**"**   means you must prove that A and B are true and false at the same time. In other words, you must prove "If A then B" and "If not A then not B". Equivalently, you must prove "If A then B" and "If B then A".
- **"Theorem**: A only if B.**"**   means you must prove "If A then B", so there is no reason to use this form of a statement.

The following issues about negation often cause confusion

- the contrapositive,
- proof by contradiction,
- negating quantified ("for all ...", "for some ...") statements.

CONTRAPOSITIVE: Suppose we have a statement "If A, then B." The contrapositive is "If not B, then not A." A statement is true if and only if its contrapositive is true. This is the only "if...then" combination of A and B with negation for which this is the case.
Example: "If it rained, then the grass is wet." has the contrapositive "If the grass is dry, then it did not rain."
 Another combination: "If it did not rain, then the grass is dry." may be false because the grass could have been watered.
Example: "A if and only if B." means "(If A, then B) and (if B, then A)." Using the contrapositive, the latter is

equivalent to "(If A, then B) and (if not A, then not B)." Hence "A if and only if B" is sometimes proved by showing (i) if A is true, then B is true, and (ii) if A is false, then B is false.

PROOF BY CONTRADICTION: Suppose we want to prove a statement. To give a proof by contradiction, we show that, if the statement is not true, we can obtain an absurdity (i.e., a contradiction).

Example: "There are an infinite number of primes." Suppose false. Let $p1,..., pn$ be the primes. Let $m = p1$ x...x $pn + 1$. Let q be a prime dividing m. (Possibly $q = m$.) By assumption q is some pk. This is impossible since dividing m by pk gives a remainder of 1.

Example: The negation of "If A, then B." is "A is true and B is false." Thus, to give a proof by contradiction of "If A, then B," we assume that A is true and B is false and derive a contradiction.

NEGATING QUANTIFIED STATEMENTS: The phrases "for some X" and "there exists X" mean the same thing and are called <u>existential</u>. The phrases "for all X", "for every X", and "for each X" mean the same thing amd are called <u>universal</u>. We can move a "not" through an existential or a universal quantifier provided we switch from one type to the other, and we can repeat the process.

Example: The negation of "Every dog has its day." is "Some dog does not have its day."

Example: Continuity of $f(x)$ at $x = a$ is defined by

for every $e>0$ there is a $d>0$ such that for every x (if $|x-a|<d$, then $|f(x)-f(a)|<e$).

In words, for <u>every</u> positive e there is (at least one) positive d such that, whenever x is within d of a, $f(x)$ is within e of $f(a)$.

Let's negate it step by step [In the last line, ">=" means "greater than or equal to."]:

<u>not</u> $\Big($ for every $e>0$ there is a $d>0$ such that for every x (if $|x-a|<d$, then $|f(x)-f(a)|<e$)$\Big)$.

for some $e>0$ <u>not</u> $\Big($ there is a $d>0$ such that for every x (if $|x-a|<d$, then $|f(x)-f(a)|<e$)$\Big)$.

for some $e>0$ and every $d>0$ <u>not</u> $\Big($ for every x (if $|x-a|<d$, then $|f(x)-f(a)|<e$)$\Big)$.

for some $e>0$ and every $d>0$ there is an x such that <u>not</u> (if $|x-a|<d$, then $|f(x)-f(a)|<e$).

for some $e>0$ and every $d>0$ there is an x such that ($|x-a|<d$ and $|f(x)-f(a)|>=e$).

That completes the negation process. In words, to show that $f(x)$ is <u>not</u> continuous at a, we must find a positive e such that, for <u>every</u> positive d we can find an x such that x is within d of a and $f(x)$ is <u>not</u> within e of $f(a)$.