ECS 20: Discrete Mathematics for Computer Science — Lecture 5 (3T)
UC Davis — Phillip Rogaway — January 18, 2022

Proofs

Today:

□ Example Proofs

0. Introduction

We have distinguished formal proofs—meaning proofs under a formalized proof system—from informal ones. Proofs in mathematics are rarely of the former variety. But that doesn't mean that other can't be rigorous. An argument is considered rigorous if the community of people evaluating it feel absolutely convinced of its correctness. This depends on the argument, of course, but it is also a notion situated in time and in a disciplinary culture.

Recall the advice I gave in lecture 1 for how to solve problems. The advice encompassed more than the construction of proofs, but everything said applies specifically to the enterprise of constructing proofs:

1. Reformulate to something equivalent
2. Generalize
3. Work out special cases. Small cases. Look for patterns.
4. Name things (e.g., introduce variables)
5. Create tailor-made definitions
6. Draw pictures
7. Think recursively
8. Adopt a playful attitude
9. Forget pattern-matching
10. But look for echoes
11. Know what you know (don't fool yourself, don't try to fool others)
12. Give serious attention to exposition. Never turn in a first draft. Critically read what you write.

The taxonomy of proofs in the zyBook follows that of Rosen. It is conventional maybe not terribly useful. The "types" of proofs considered are: direct proofs; establishing the contrapositive of what you want to show; proofs by contradiction; and proofs that work by enumerating cases.

I think I would have come up with very different categories. Maybe something like proofs in which you:

1. Follow your nose
2. Introduce the right extra thing
3. Draw the right picture
4. Find a good counterexample
5. Find a good representation
6. Break into good cases
7. Reduce to a known result

This is *not* an exhaustive list. Nor a precise one. But in trying to come up with example for today, the semantic categories above made some sense.

The way to get good at proving things is to see—and to devise—plenty of proofs.

The use of the word "devise" in the last sentence suggests an epistemological viewpoint that proofs are the result of invention, not discovery. I do indeed see things that way. But I might mention from the outset that this is not the only view. Consider the title of the popular text *Proofs from THE BOOK*, by Martin Aigner and Günter M. Ziegler, `https://bit.ly/3GKwS9k`. THE BOOK was Paul Erdös' way of speaking of proofs that are so beautiful and perfect that they are maintained by God. Proofs of that sort are discovered, many mathematicians feel in their bones; they were always out there, patient and perfect, waiting to be discovered by us dumb humans.

Maybe. What do I know.

Example 1: A direct proof — $\sqrt{2}$ is irrational

Zane did this in discussion. I'm going to start off by repeating it.

For the problem to make sense, we need a definition. A real number x is said to be *rational* if $x = m/n$ for some integers m and n with $n \neq 0$. A real number is *irrational* if it is not rational.

A definition like that last sentence is *not* superfluous. Defining a rational number does not somehow define an irrational one. In math, every word or phrase that is being given a technical meaning has to have a definition.

Now for our proof. Suppose for contradiction that $\sqrt{2}$ is rational, whence there exists integers m and n, the latter nonzero, such that $\sqrt{2} = m/n$. Squaring both sides gives $2 = m^2/n^2$, when $2n^2 = m^2$. That is to say, m is even.

I claim that if the square of some integer is even, then that number itself was even. This is what you would guess from doing some examples: the squares of $0, 2, 4, \ldots$ are are $0, 4, 16, \ldots$—all even. While the squares of $1, 3, 5, \ldots$ are $1, 9, 25, \ldots$—all odd. We need to *prove* our claim at some point; consider it a pending obligation. But for now let's just *assume* the claim and proceed.

OK, so we have that m is even. What does that mean? Another definition. An integer j is even if $j = 2i$ for some integer i. That's it. Could you write it as a formula of first-order logic?

Using our definition now, we can write m as $2k$ for some integer k. Doing so, we have that $2n^2 = (2k)^2 = 4k^2$, whence $n^2 = 2k^2$. This means that n^2 is also even and so, as before n is even.

At this point we know that both m and n are even—they are multiples of 2. If I am clever I can see that as a contradiction. How? When we wrote $\sqrt{2}$ as m/n we could have *assumed* that m and n had not common divisors. If they did have any common divisors, you could have "crossed them out." Had we had made that assumption we'd have our contradiction. So go back and make that assumption on m and n, and our proof is done.

Modulo the claim that we didn't prove.

I have intentionally presented this proof not quite in the manner that one would read the finished argument in a book, but in the manner that a mathematician would rediscover it. The discovery of proofs often follows a long and circuitous path that is not revealed if you look only at a refined final draft of a proof.

We could go back and prove our claim that the square of a number being even implies that that number was even. But let's instead move on, and use our first result, too.

Example 2: Clever cases — exponentiating irrational numbers

Let us show that there are irrational numbers a and b such that a^b is *rational.* It's an interesting claim. One somehow expects that, for most irrational numbers a and b, a^b should remain irrational. But we're just saying that *some* a and b work out.

Let's consider $a = b = \sqrt{2}$, the only number we've shown to be irrational. Well, if $a^b = \sqrt{2}^{\sqrt{2}}$ is rational then we are done: it's what we wanted to prove. On the other hand, if $a^b = \sqrt{2}^{\sqrt{2}}$ is irrational, then we have augmented our stock of irrational numbers by one more, $A = \sqrt{2}^{\sqrt{2}}$. What about raising *it* to $b = \sqrt{2}$? We'd get 2, which is about as rational as they come. Thus we know that either $a = b = \sqrt{2}$ works to satisfy the claim, or we know that $a = \sqrt{2}^{\sqrt{2}}$, $b = \sqrt{2}$ works to satisfy the claim. Either way, the claim holds.

Our proof had two simple cases. We won either way.

Something interesting about our proof is that it was mildly *nonconstructive.* We proved that there existed an (a, b) with a certain property even though we aren't sure just what (a, b) is. A nonconstructive proof establishes the existence of an object without explicitly identifying it. Some people don't like nonconstructive proofs (but I think they're great). In any case, our proof was only "slightly" non constructive because it actually identified two candidate (a, b) pairs and proved that at least one of them worked.

Example 3: Exhaustive case analysis — tic-tac-toe

That last case analysis had just two cases. Sometimes the difficulty is that there are too many damn cases! It even happens that, sometimes, computers are needed to assist in the case analysis.

Oftentimes, however, a little bit of cleverness can vastly reduce the amount of casework needed.

Let us show that, in playing tic-tac-toe, if the first player moves to a corner, then the second player must take the center. If he doesn't, the first player can force a win.

We can substantially reduce the number of cases to check by exploiting *symmetry.* Let's number the squares of the tic-tac-toe board from 1 to 9 as we go left-to-right, then top-to-bottom.

Let's say that the player who moves first is X.

To begin, if we check the claim for X initially moving to 1 that will be enough, because X moving to 3, 7, and 9 is exactly the same after clockwise rotations. Great. So X initially moved to 1. Now we will have four cases:

1. Player O moves to 2. By symmetry argument, this will also cover the case of O moving to 4.

   In this case have X move to 5. This forces O to move to 9, whence X can move to 7 and have a guaranteed win on its next move.

2. Player O moves to 3. By symmetry argument, this will also cover the case of O moving to 7.

   In this case have X move to 9. This forces O to move to 5, whence X can move to 7 and have a guaranteed win on its next move.

3. Player O moves to 6. By symmetry argument, this will also cover the case of O moving to 8.

   In this case have X move to 5. This forces O to move to 9, whence X can move to 3 and have a guaranteed win on its next move.

4. Player O moves to to 9.

   In this case have X move to 7. This forces O to move to 4, when X can move to 3 and have a guaranteed win on its next move.

That completes our proof.

I will warn that it is easy to write something like "by a symmetry argument" or "without loss of generality" when you don't actually understand what those thing mean—and when you might well be wrong. Make sure that any time you use such a phrase, you fully understand it, and can justify it.

I will mention that we proved the theorem above without explaining *anything* in the theory of two-person games. Routinely mathematicians stack up the definitions at the beginning, and then force you to use them. But it's not the way that any of it evolved—and it's probably not the way to pique your interest. Instead, there is interest in developing such a theory precisely because you have a problem in mind, and hit a point where not having good vocabulary or notions was getting in your way.

As an example, a student asked if we should now show that if player-O took 5 in response to 1, then player X can't force a win. Maybe by that point you'd like to have some rigorous notion for what it *means* to be able to force a win. And to have a notion general enough that we can ask question like: "should white win in chess, should black, or should it be a draw?" (It's definitely an interesting question to people who play chess. And we don't know the answer. I think chess players suspect it's a draw.)

Example 4: Add the right extra thing — Area of a triangle

Let us show that the area of a triangle all of whose angles are acute is $bh/2$ where b is the triangle's base and h is its height.

Actually, let's not do it. Because it's the first example in the Lockhart reading, which I have asked you to read this week.

Example 5: Algebra vs. pictures — Sum of the first n numbers

Let us give gave two different proofs that $1 + 2 + \cdots + n = n(n + 1)/2$. A first, algebraic proof. Then a second, pictorial

The algebraic proof is nice. It uses the following idea. For some fixed n, name the sum S and write its value twice, once in the "increasing" direction and once in the "decreasing" direction:

$$\begin{aligned} 1 + 2 \quad + \cdots + (n-1) + n &= S \quad \text{and} \\ n + (n-1) + \cdots + 2 \quad + 1 &= S \end{aligned}$$

Add up the left sides and add up the right sides to get

$$\underbrace{(n+1) + (n+1) + \cdots + (n+1) + (n+1)} n \text{ addends} \quad = \quad 2S$$

which is to say that

$$n(n+1) \quad = \quad 2S$$

so $S = n(n + 1)/2$. Done.

But not quite done. I suggest that, after you discover a formula like this, you try a bunch of values to see that it's working. So plus in $n = 1, 2, 3, 4$, say, and see that it really *is* the case that $1 + 2 + \cdots + n = n(n + 1)/2$ for these particular values.

No amount of trying values will work to prove that you got it right. But if you didn't get it right, you are likely to discover that right away, in my experience, by checking out if the equation is working out on small values.

Once you have *one* proof, does that mean that there is no point for another. *No!!!*. Mathematicians don't just prove things to learn if they are true. They prove things because it's *fun*. And

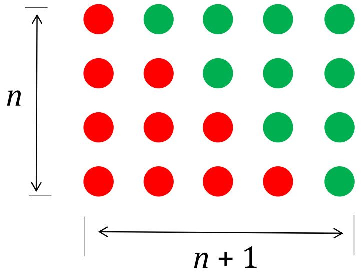

Figure 1: A visual proof that $1+2+\cdots+n = n(n+1)/2$.

because it can afford insight into *why* things are true. And because math is of art, and finding new proofs is creating new art. Once somehow has painted one image of a dying flower in a vase, does that mean that other artists should never try their hand at that concept, because dying-flower-in-a-vase is now "done"? I don't think so.

For a second proof, then, just look at the image of Figure 1. In it we count the $1+2+3+4$ red balls, which comprise half the balls in our 4×5 grid of balls. This is a *visual proof* that $1+2+3+\cdots+n = n(n+1)/2$. You don't need many words to explain it; the picture makes it clear!

Example 6: More pictures — Sum of the first n odd numbers

Pictorial proofs are so fun that I can't help but give another. In Figure 2 you'll see a lovely pictorial proof that $1+3+5+\cdots+(2n-1) = n^2$.

You could have discovered that result easily enough. In exploring the sum, you'd have made a table that would have made the general formula trivial to guess. The table would also have helped you get right how to index the last sum—whether it should be, say, $2n-1$ or $2n+1$. The latter comes out as the clear winner, ensuring that n is the number of addends and that n^2 is the value of the sum. Had you stopped at $2n+1$, it wouldn't have been so pretty.

Expression	Number of addends	Value
1	1	1
$1+3$	2	4
$1+3+5$	3	9
$1+3+5+7$	4	16
$1+3+5+\cdots+(2n-1)$	n	n^2

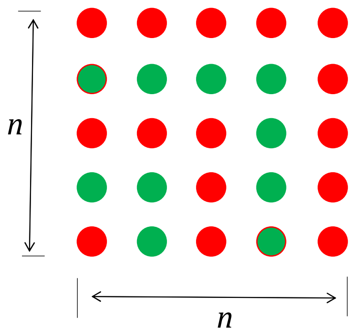

Figure 2: A visual proof that $1 + 3 + \cdots + (2n - 1) = n^2$.

Example 7: Translate to the familiar — 20 random cards

Here's the problem. Twenty random cards are placed in a row, all face down. 17 A *move* consists of turning a face-down card face-up and turning over the card, if any, immediately to its *right*. Show that no matter what the choice of cards to turn, this sequence of moves *must* terminate.

The problem appears in the film A Brilliant Young Mind (2014); you can find the clip at `https://bit.ly/3nCVdX7`. My own treatment uses a different convention, representing face-down cards with 0 and face-up cards as 1. In this way each moves *increase* the 20-bit binary number, and you start at start zero, so you can't have any of 2^{20} or more moves. Just a bit more natural, I think. But Nathan did just fine.

Example 8: Employ or invent — handshaking theorem

We investigated the phenomenon in which men claim to have had a higher number of opposite-gender sexual partners than women claim to have. Quoting from the "MIT book" (linked to from our course homepage):

> Who, on average, has more opposite-gender partners: men or women? ….
>
> In one of the largest [studies], researchers from the University of Chicago interviewed a random sample of 2500 people over several years … Their study, published in 1994, … found that men have on average 74% more opposite-gender partners than women.
>
> Other studies have found that the disparity is even larger. In particular, ABC News claimed that the average man has 20 partners over his lifetime, and the average woman has 6, for a percentage disparity of 233%. The ABC News study [claimed] a 2.5

So this time the thing we wanted to prove didn't even start with a problem statement. It started with nothing but some claimed statistics, in which *you* should conjecture a mathematical claim.

I asked student their reactions and many were incredulous. *Shouldn't the numbers be the same?*, some asked? Or just a general sense that it seemed fishy.

But then I drew a picture: one man, two women, then man slept with both women, the so the average number of parters men had is 2, the average number of parters women had is 1, so the averages needn't be the same after all.

But that counterexample depended on have the number of men different from the number of women. If they are equal, well, maybe *then* the two averages should be the same.

How could we represent what is going on? I think it is natural to drop each man as a dot on the left, and each woman as a dot on the right. And let's assume that there are the same number n of dots on the left and on the right. Then let's draw a line from a man to a woman if they've been partners. Here we are making an assumption: that our has-slept-with relation is *symmetric.* That a woman A has slept with a man B exactly when the man B has slept with the woman A. That *seems* like it should be right . . . but maybe not.

OK, so we have these n points (men) on the left, another n points (women) on the right, and an edge between a man and a woman if they've been sexual partners. Let's call the number of lines ε. How many partners has the the average man had? That would be ε/n. How many partners has the the average woman had? That would be ε/n. So the two numbers really *should* be the same.

It leaves open the question of how to explain the survey data. The math is right, so there must be some sense in which the mathematical model does not reflect the social reality.

Maybe men lie in such surveys, overstating how many women they've slept with. Maybe women lie in the surveys, understating how many women they've slept with. Maybe men and women look back on their lives differently, and the assumption that the has-slept-with relation is symmetric is at odds with how the world works, or how it is remembered. I myself don't know. But those who study human sexuality have something to explain.

One more point. When you study a subject subject like graph theory you get a bunch of definitions and results, and they might seem like they are plucked from nowhere. But what really happened is that you had situations like the ones above, and they motivated people to *invent* the thing of interest—what we would call, here, a *bipartite graph.* I suspect that math in general, and theorems in particular, are much more interesting to most people if we have in mind to pursue particular and interesting results. Definitions, just like proofs, better be either aesthetic or applicable, otherwise I wouldn't be interested in them, either.

Summary

1. Finding proofs is *not* mechanical; it is an art.
2. Mathematical discovery is more than proofs: guessing and discovering results is also key. Only in a class setting do proofs come as a "prepackaged" task for you.

3. Don't get so obsessed with rigor that you fail to develop and refine intuition. It is ok to guess and even to err.

4. Proofs evolve. They can be quite dialectical.

5. Intuition can be lost in a refined, succinct proof. Proofs are never "born" in such a manner.

6. You can't prove what doesn't make sense to you. Don't even try to prove something until you get to the point of the language and claim making sense.