Spamegg's Commentary on "Proof Methods: Chapters 1.7 - 1.9 (Session 2)"

https://github.com/spamegg1

August 8, 2021

Contents

1 Facts used

In addition to previous sections, we are using:

The Quotient-Remainder Theorem: For all pairs of integers $a, b > 0$ there exist unique integers q, r such that $a = bq + r$ and $0 \leq r < b$.

I will be mentioning sets, binary relations and Cartesian products, which will be covered in a later section in the course.

2 1.7 Proof by Cases

I get asked about the Theorem and its explanation here a lot. It's quite confusing.

There are many definitions here! It will seem like I am arguing some pointless edge cases, but it's good practice to do so and make sure, instead of assuming what is meant.

Definition 1. *Let's agree that given any two people, either they have met or not.*

When we are given vague definitions like this in English, it's a good exercise to try to formalize it, and think about possible edge cases.

This is actually defining a binary relation on a set.

Can these two people be the same person? It seems like Prof. Meyer's intention here is that these two people are different. So we will exclude a person "having met themselves."

What if person a met person b? Intuitively we would think that this means person b also met person a. (This is called "symmetry".)

So, in the language of sets and relations, if we have a set of people as an example, let's say $P = \{a, b, c\}$, and say, only a and b met, then *met* is a symmetric binary relation on the Cartesian product $P \times P$ minus the diagonal $\{(a, a), (b, b), (c, c)\}$ that would look like this:

	a	b	c
a		met(a,b)	¬ met(a,c)
b	met(b,a)		¬ met(b,c)
c	¬ met(c,a)	¬ met(c,b)	

Definition 2. *If every pair of people in a group has met, we'll call the group a club.*

I think that "pair of people" excludes someone being paired up with themselves. In our example $\{a, b\}$ is a club.

Definition 3. *If every pair of people in a group has not met, we'll call it a group of strangers.*

This definition is what solidifies it for me, that we should exclude a person meeting themselves from the relation. Otherwise a non-empty group could never be strangers, because there would always be a pair that has met (a person having met themselves).

In our example $\{a, c\}$ and $\{b, c\}$ are examples of strangers. Is it possible for a group to be neither a club nor strangers? Can you think of an example?

Indeed $\{a, b, c\}$ is neither a club nor strangers. It violates the club definition because the pair (a, c) has not met. It violates the strangers definition because the pair (a, b) has met.

Theorem 1. *Every collection of 6 people includes a club of 3 people or a group of 3 strangers.*

Prof. Meyer starts the proof with this:

The proof is by case analysis. Let x denote one of the six people. There are two cases:

1. Among 5 other people besides x, at least 3 have met x.

2. Among the 5 other people, at least 3 have not met x.

The first question I get from learners is: "why are these cases exhaustive, and how did Meyer come up with these particular cases? I would have done it completely

differently!" Let's keep reading:

Now, we have to be sure that at least one of these two cases must hold, but that's easy: we've split the 5 people into two groups, those who have shaken hands with x and those who have not, so one of the groups must have at least half the people.

This paragraph confuses a lot of learners. They go like: "What?"

Honestly I have no idea what Prof. Meyer is trying to say here. He seems to be defining ANOTHER binary relation "having shaken hands with". How is that related to the cases above? How is "one group having at least half the people" related to the cases being exhaustive? I don't get it. Neither do other learners. Let me know if you unambiguously understand this.

Let's define the cases in a better way. Like Meyer, let's fix one of the 6 people, call this person x. Now let's define:

Definition 4. *Define n to be the number of people, among the other 5, who have met x.*

OK, now let's think. What is the range of possible values for n? It should be: $0, 1, 2, 3, 4, 5$ right? So any case analysis should exhaustively cover these 6 possibilities.

Now let's think back to Prof. Meyer's cases: "at least 3 have met x" would translate to: $n \geq 3$. This covers the range $n = 3, 4, 5$.

"At least 3 have not met x"... how does this translate to n? Since we agreed that every pair of people has either met or not met, the number of people among the other 5 who have NOT met x would be $5 - n$. So this means $5 - n \geq 3$. Solving for n we get $2 \geq n$. This covers the range $n = 0, 1, 2$.

Together, these two cases cover the range of all possible values for n. I think it would have been much more natural to say in the second case: "at most 2 have met x" instead. It would have been a lot less confusing. However, expressing the second case in terms of "at least 3 people have not met x" makes writing that part of the proof a bit easier.

3 1.8 Proof by Contradiction

We face the dreaded definition of a rational number here again. Not explicitly defined, just defined in passing inside a paragraph: *Remember that a number is rational if it is equal to a ratio of integers.* That's it! No mention of anything else, such as, whether the denominator could be 0 or not, whether the integers involved are positive or negative, whether they have common divisors... Then we move on:

Theorem 2. *$\sqrt{2}$ is an irrational number.*

This is one of the most celebrated, beautiful proofs in all of mathematics. G. H. Hardy opens his book "A Mathematician's Apology" with it.

Prof. Meyer starts with the default boilerplate of a contradiction proof: *We use proof by contradiction. Suppose the claim is false, and* $\sqrt{2}$ *is rational.* ***Then we can write*** $\sqrt{2}$ ***as a fraction*** n/d ***in lowest terms.***

A fraction of what? And what does "lowest terms" mean? Some learners don't know this stuff. Also, I see a lot of learners misinterpret "Then we can write..." to mean "we can choose n and d." The definition of a rational number is actually an EXISTENTIAL statement, and we do not get to choose the numbers n and d (except up to a common divisor).

3.1 Rational number definition

Let's properly define what a rational number is.

Definition 5. *A real number* r *is called a* ***rational number*** *if there exist integers* n *and* d *such that* $d \neq 0$ *and* $r = \frac{n}{d}$.

In general, if one such pair of integers exists, there are infinitely many such pairs of integers (for example, $1/2 = 2/4 = -3/-6 = \cdots$*). So, without loss of generality we may assume that* n *and* d *are in "lowest terms": meaning* n *and* d *have no common divisors greater than 1.*

Moreover, without loss of generality, if $r > 0$ *we may assume both* n *and* d *are positive, and if* $r < 0$ *we may assume* $n < 0$ *and* $d > 0$.

Continuing with the proof: by this definition, there exist integers n and d such that:

$\sqrt{2} = n/d$ where n and d have no common divisors greater than 1, and $d \neq 0$.

Squaring both sides gives $2 = n^2/d^2$. Multiplying both sides by d^2 gives: $2d^2 = n^2$.

Then Prof. Meyer says: *This implies* n *is a multiple of 2* ***see Problems 1.10 and 1.11***. I see a lot of learners get stuck here. They either didn't do Problems 1.10 and 1.11 or they simply cannot make the jump in reasoning. Let's go do those Problems and come back.

3.2 Problem 1.10

The problem states:

Let n *be a nonnegative integer.*

(a) Explain why, if n^2 *is even - that is, a multiple of 2 - then* n *is even.*

(b) Explain why, if n^2 *is a multiple of 3, then* n *must be a multiple of 3.*

Proof. (of Part (a)) 1. Assume n^2 is a multiple of 2.

2. By definition of divisibility, there exists an integer k such that $n^2 = 2k$.

3. Argue by contradiction and assume n is not even.

4. By the Quotient-Remainder Theorem there exists integers q, r such that $n = 2q + r$ where $0 \leq r < 2$. Since n is not even, r cannot be 0. Therefore r must be 1.

5. So $n = 2q + 1$. Squaring both sides we get $n^2 = 4q^2 + 4q + 1$.

6. Combining (2) and (5) we see that $n^2 = 2k = 4q^2 + 4q + 1$.

7. Dividing by 2 we get $k = 2q^2 + 2q + \frac{1}{2}$.

8. Moving terms, we get $k - 2q^2 - 2q = \frac{1}{2}$ which is a contradiction, because the left-hand side is an integer, but the right-hand side is not an integer.

9. Therefore n must be even. □

Proof. (of Part (b)) 1. Assume n^2 is a multiple of 3.

2. By definition of divisibility, there exists an integer k such that $n^2 = 3k$.

3. Argue by contradiction and assume n is not a multiple of 3.

4. By the Quotient-Remainder Theorem there exists integers q, r such that $n = 3q + r$ where $0 \leq r < 3$. Since n is not a multiple of 3, r cannot be 0. Therefore r must be 1 or 2.

5. So $n = 3q + 1$ or $n = 3q + 2$. (Here we can do proof by cases, but we'll treat both cases together.)

6. Squaring both sides we get that either $n^2 = 9q^2 + 6q + 1$ or $n^2 = 9q^2 + 12q + 4$.

7. Combining (2) and (6) we see that either $3k = 9q^2 + 6q + 1$ or $3k = 9q^2 + 12q + 4$.

8. Dividing by 3 we get that either $k = 3q^2 + 2q + \frac{1}{3}$ or $k = 3q^2 + 4q + \frac{4}{3}$.

9. Moving terms, we get that either $k - 3q^2 - 2q = \frac{1}{3}$ or $k - 3q^2 - 4q = \frac{4}{3}$ which is a contradiction, because in both cases the left-hand side is an integer, but the right-hand side is not an integer.

10. Therefore n must be a multiple of 3. □

3.3 Problem 1.11

It asks: *Give an example of two distinct positive integers m, n such that n^2 is a multiple of m, but n is not a multiple of m. How about having m be less than n?*

Proof. Let $n = 6$ and $m = 4$. Then $n^2 = 36$ is a multiple of 4 but $n = 6$ is not a multiple of 4. And, on top of it, $m < n$ as requested. □

We should think about the reasons for this counterexample, instead of randomly guessing some numbers. We want n^2 to be a multiple of m but we don't want n to be a multiple of m. So we can let m be the square of a prime number, like $m = p^2$, and include this prime as a divisor of n, like $n = p \cdot q$ where q is some other prime.

This way n^2 will have p^2 as a divisor but n won't. To make sure $m < n$ we can choose $q > p$. The primes $p = 2$ and $q = 3$ satisfy these requirements perfectly.

3.4 Back to the proof of the Theorem

So by Problem 1.10 (a), we have that n is even.

By definition of divisibility, there exists an integer k such that $n = 2k$.

Squaring, we get $n^2 = 4k^2$. (This is where Prof. Meyer says "n^2 is a multiple of 4". Writing out equations makes it clearer I think.)

Substituting, we get $2d^2 = n^2 = 4k^2$.

Dividing by 2 we get $d^2 = 2k^2$. So d^2 is even, therefore by Problem 1.10 (a) again, d is even.

This means n and d are both divisible by 2, which contradicts the fact that they have no common divisors greater than 1.

Thus $\sqrt{2}$ must be irrational. **QED**

4 1.9 Good proofs in practice

This is the most important section in the whole book! You should re-read it multiple times, over and over. Prof. Meyer says:

Mathematicians generally agree that important mathematical results cannot be fully understood until their proofs are understood. That is why proofs are an important part of the curriculum.

Mathematics IS proofs. Doing proofs is what doing math is all about. The proofs are more important than the results themselves, no matter how impressive they may seem simply stated. This is why you should regard the Algorithms courses as math courses, not programming. The algorithms will already be given to you in pseudo-code. Anyone can implement them. But without understanding the proofs; in a job interview, when you are given a problem you've never seen before, how will you solve it, analyze its run time, and prove its correctness?

Conversely, proofs in the first weeks of a beginning course like 6.042 would be regarded as tediously long-winded by a professional mathematician.

Great! Be as tedious and long-winded as you can. This is the point where you do all the hard work, in order to solidify your logical, reasoning, argumentation skills; your meta-cognitive skills to detect hidden assumptions and definitions; your mathematical rigor and strictness; learning to write bullet-proof arguments with no gaps, flaws or openings, although they will be too long-winded and tedious at first.

This is the single, most important moment in your computer science journey. Because the math will get only more complicated as time goes on. Skipping over "unimportant

small details" NOW will hurt you far more in the future, when there are so many more layers of definitions, assumptions, details and edge cases, which will be harder to see or reason about. All the testing, debugging, and stepping in the world WILL NOT HELP YOU! Proofs are better than tests and debugging.

Take it from Prof. Meyer if you don't believe me:

The analogy between good proofs and good programs extends beyond structure. The same rigorous thinking needed for proofs is essential in the design of critical computer systems. When algorithms and protocols only "mostly work" due to reliance on hand-waving arguments, the results can range from problematic to catastrophic. An early example was the Therac 25, a machine that provided radiation therapy to cancer victims, but occasionally killed them with massive overdoses due to a software race condition. A more recent (August 2004) example involved a single faulty command to a computer system used by United and American Airlines that grounded the entire fleet of both companies—and all their passengers!

Let's summarize Prof. Meyer's tips:

State your game plan.

Keep a linear flow.

A proof is an essay, not a calculation. This is very important; however also keep in mind that explanations "in plain English" can be too vague, you should know the technical explanation behind it completely before you write it in a more "accessible" form.

Avoid excessive symbolism. True; however sometimes things are better explained and understood in formulas or equations; you'll have to make good judgment on this.

Revise and simplify.

Introduce notation thoughfully.

Structure long proofs.

Be wary of the "obvious". *But remember that what's obvious to you may not be—and typically is not—obvious to your reader.* Remember the meta-hierarchy I mentioned in an earlier commentary? Always keep in mind a reader who is weaker than yourself.

Finish.