Lecture 12

Images and surjections; Cantor's Theorem

12.1 A retrospective

Last week, we studied Peano's axioms. They were *axioms* (starting assumptions, or statements we just declare to be true at the beginning of our logical universe), and their intent was to ensure that a thing called "the set of all natural numbers" exists.

Remark 12.1.1. Let me remind you: You *know* what natural numbers are. You know it in your heart. So don't let Peano's axioms take away from your intuitions.

In one way, Peano's axioms are very abstract. They don't tell you *what* a natural number is. They just characterize the set of all natural numbers. This is actually a common thing to do in modern mathematics. If there is a family of things you want to understand (like natural numbers) it turns out to be easier to characterize the entire collection of those things, rather than to characterize what it means to be one of those things.

For, once you construct the set/collection of the things you want, then all you need to do is declare that a thing you want is an element of that set.

In some sense, Peano's axioms represent one of the first instances of "categorification" in this sense. You don't need to know what that term means. Most modern mathematicians don't.

Remark 12.1.2. Earlier in this course, I kept emphasizing that an alien might not know what you mean by "next."

And in fact, Peano's axioms choose to *axiomatize* next. Peano doesn't define what next is. Peano just *assumes*, or declares, that there exists some function t, and that this function dictates what nextness is.

This is again a common math strategy. There is a structure, and you don't know how to talk about it. So you try to identify the properties of that structure (like there is only one non-next thing, or like "next" is an injective function). If there is only one such structure with those properties, well then, by golly, you've characterized the structure you want to describe!

12.2 Notation for functions

Before we go on, now I'd like to introduce some new terms and new notation. Again, I am introducing terms and notation *after* the ideas they represent have already come up. This is so that you know that the terms and notations are secondary; the underlying concepts are what matter.

Notation 12.2.1. Let X and Y be sets. We will write

$$f : X \to Y$$

to mean that f is a function from X to Y.

Remark 12.2.2. Note that the notation contains a colon :; this is to indicate that what came before it (f) is a function, and what comes after it (X) is the domain of that function.

Then, what comes after the arrow (Y) tells you that Y is the codomain.

Warning 12.2.3. Note also the arrow $\to$. It is not $\hookrightarrow$, or $\mapsto$, or $\twoheadrightarrow$, or $\implies$. It is a very specific kind of arrow: $\to$. Please use this no-frills, no-tail arrow when talking about functions from X to Y. The other arrows I drew in this paragraph have very different kinds of meanings.

Example 12.2.4. Many lazy mathematicians, including myself, will write

$$\text{Fix } f : X \to Y$$

to mean "fix a function f with domain X and codomain Y." You can see that this notation saves a lot of space.

Example 12.2.5. You may see someone write

$$\text{Define } f : \mathbb{R} \to \mathbb{R} \text{ by } f(x) = x^2.$$

This means "Let f be a function from the set of real numbers to the set of real numbers, and which sends any real number x to its square."

Example 12.2.6. You may see someone write

$$\text{Define } f : \mathbb{N} \to \mathbb{N} \text{ by } f(x) = x^2.$$

This means "Let f be a function from the set of natural numbers to the set of natural numbers, and which sends any natural number x to its square."

Note that this function is a *different* function from the previous example, because it has a different domain (and codomain)!

Notation 12.2.7 ($\mapsto$)**.** We will use the arrow $x \mapsto f(x)$ to denote that a function f sends an element x to the element $f(x)$.

Example 12.2.8. For example, let $f : \mathbb{R} \to \mathbb{R}$ be the function $f(x) = x^2$. Then $3 \mapsto 9$ and $4 \mapsto 16$.

Example 12.2.9. If you see someone write

$$f : \mathbb{R} \to \mathbb{R}, \qquad x \mapsto x^2 - 3$$

this means "Let f be a function from $\mathbb{R}$ to $\mathbb{R}$ which takes any real number x to the real number $x^2 - 3$."

12.3 Images and surjections

I also want you to know two new terms.

Definition 12.3.1. Let f be a function from X to Y. Then the *image of f* is the set

$$\{y \in Y \mid \text{For some } x \in X,\ f(x) = y\}.$$

In other words, the image of f is the set of all elements in Y that are hit by f.

Example 12.3.2. Let $f : \mathbb{R} \to \mathbb{R}$ be the function $x \mapsto x^2$. Then the image of f is the set of all non-negative real numbers. (That is, the set of all real numbers greater than or equal to zero.)

Example 12.3.3. Let $f : \mathbb{N} \to \mathbb{N}$ be the function $x \mapsto 2x$. then the image of f is the set of all even natural numbers.

Remark 12.3.4. Note that the image of f is always a subset of the codomain.

Notation 12.3.5. Let $f : X \to Y$. We will often write the image of f as

$$\text{image}(f).$$

Remark 12.3.6. Historically, mathematicians struggled a lot with whether the idea of "codomain" and "image" should be separate. For example, it was incredibly common for mathematicians to treat the image as the codomain. (After all, who cares about the elements that we *don't* hit?)

Now-a-days, I think we have settled on *always* remembering the codomain, and thinking of the image as a subset of the codomain.

One reason is that we often want to compose functions. For example, suppose we have a function $f : X \to Y$ and a function $g : Y \to Z$. Then we know what it means to define $g \circ f$. (We declare an element x to go to the element $g(f(x))$.)

Notice that defining this composition suddenly becomes a lot messier if we forget Y and only remember the image of f; you'd have to then always have the caveat that "we can also treat g as a function from the image of f, rather than a function from all of Y." We avoid all that by having the notion of codomain once and for all.

Finally, we have talked about whether or not functions "hit every element of the codomain." For example, this is one of the requirements for a function to be a bijection. It turns out we hav a word for this, too.

Definition 12.3.7. Let $f : X \to Y$. We say that f is a *surjection* if $\text{image}(f) = Y$.

Example 12.3.8. A function is a bijection exactly when it is both an injection and a surjection.

Example 12.3.9. Let $\mathbb{R}_{\geq 0}$ be the set of all non-negative numbers. Consider the three functions

1. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$.
2. $f : \mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$.
3. $f : \mathbb{R}_{\geq 0} \to \mathbb{R}, x \mapsto x^2$.
4. $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$.

The first is neither a surjection nor an injection.

The second and third are injections but not surjections.

The last is a bijection.

12.4 Our next theorem

What is a theorem?

A *theorem* is a true statement that is both important, and difficult to prove. Note that both these criteria are subjective. Who is to say what statement is important? Who's to say whether something is difficult to prove?

It would not be so inaccurate to say that the point of much of mathematics is to verify theorems. Who doesn't want to know that important facts are true? For example, the *fundamental theorem of calculus* is a theorem you probably saw in calculus class. This is the theorem that allows you to compute integrals as antiderivatives.[1]

So, without further ado:

Theorem 12.4.1 (Cantor's Theorem)**.** Let X be a set. Then the power set of X does not admit a bijection from X.

You probably don't have any intuition for this. However, you saw that in some examples, this statement seems true—indeed, in Exercise 4.3.8, you saw that there were more subsets of X than there were elements of X. Regardless, we certainly haven't seen why this ought to be true for *any* set, especially because we don't really have much intuition for infinite sets at this point.

[1] If you think that integrals and antiderivatives are the same thing without explanation, your calculus professor did not tell you why the fundamental theorem of calculus is so fundamental. The point is that the integral is defined as an area, while antiderivative is defined without using any notion of area. The fact that area can be computed using the process of finding antiderivatives is a completely non-obvious fact, and incredibly important. This is why the fundamental theorem of calculus is called a theorem.

Well, I'm about to show you that it is true for any set. And this demonstration is called a *proof.*

Proof, written in a very "chatty" way. For sake of argument, let's first assume that there *is* a bijection from X to the power set of X. I'm going to convince you that this assumption is going to blow up the logical universe—more specifically, I'm going to show you that this assumption will lead to a conclusion that we know must be false.

Think about it: If an assumption leads you to a false conclusion, the assumption itself must be false.

In other words, there could not be any bijection from X to its power set.

Okay; everything up to this point was a description of our strategy. Let's carry it out.

Let's give the bijection a name because we'll want to be lazy/efficient. Let's call it f. So, for every element x of X, f assigns some subset of X. Let's call this subset $f(x)$. So far, this is just notation. We have done no reasoning, and we have made no logical progress.

Here is our first act of creativity: We're going to consider a very special subset of X, defined using the data of f. Specifically, let's consider a set whose only elements are those x for which $x \notin f(x)$.

Well, f is a bijection, so it hits every element of the power set. In other words, this "very special subset of X" is equal to $f(w)$ for some element w of X.

Now, I will convince you that w cannot be in $f(w)$, and it also must be in $f(w)$. Does that sound crazy? Good. This is the "false conclusion" that I referred to when describing our strategy.

Beginning of convincing you. So, why is that w cannot be in $f(w)$? Because if w were to be in $f(w)$, that would contradict the definition of our very special subset—$f(w)$ is the subset whose only elements are those that are not contained in their label.

On the other hand, if w is not in $f(w)$, then by definition of our very special subset, w must be in $f(w)$!

Oh boy, your head might hurt. Make sure to think this through. **End of convincing you.**

To summarize: I began with the assumption that a bijection exists. This assumption led to a known false fact. Therefore the assumption itself must be false—that is, no bijection can exist from X to its power set. $\square$

12.5 What just happened?

There was a lot that just happened. Let me tell you what you are supposed to take away from this.

- First, we actually just proved a useful fact, so you should know this fact from now on: A set X never admits a bijection to its power set.
- Second, this useful fact has a name, so you should know the name: Cantor's Theorem. (In fact, there's another statement known sometimes as Cantor's Theorem; we'll get to that in a future class.)
- Third, we made use of a new idea: That if you begin with an assumption, and you lead to a false conclusion, then the assumption itself must have be wrong. This is called *proof by contradiction.*
- Finally, we also saw that we had to juggle many complicated ideas in our head at once. The notion of element, and the notion of this "very special set" $f(w)$, for example. You will probably have to read over the proof many times to feel like you get it. *This is normal.* Very, very few mathematicians can read over a proof and understand it the first time around. You will need to spend the time to read, *conceptualize*, and try to understand what is going on.

12.6 Another example of proof by contradiction: Why $\frac{1}{0}$ is undefined.

To recap: To prove a statement by contradiction, you do the following: Start off by assuming that the statement is false. Then, show that this assumption leads to a conclusion known to be false.

Why is this a "proof" that the original statement must be true? If the logical universe is to be consistent, it must be that the assumption is wrong—in a logically consistent universe, we cannot derive false statements from true ones.

Proof by contradiction is an incredibly powerful tool for proving things. Here, let's use it to see *why* the fraction $1/0$ must be undefined.

Hiro's claim. There is no system of arithmetic where (i) the rules of fraction arithmetic hold true, and (ii) $1/0$ is some real number.

Proof, but not in a chatty style. Suppose there exists such a system. Recall that the rules of arithmetic for fractions guarantee that

$$b \times \frac{a}{b} = a.$$

Setting $b = 0$, this means

$$0 \times \frac{1}{0} = 1. \tag{12.6.0.1}$$

However, another rule of arithmetic tells us that $(0 \times \text{anything}) = 0$. Using this equality on the lefthand side of (12.6.0.1), we conclude

$$0 = 1.$$

This is obviously false. □

So our initial assumption that "a system of arithmetic satisfying both (i) and (ii) exists" must be false. Now, you choose: Do you want to live in a universe where (i) the rules of fraction arithmetic as you know them are true, or in a universe where (ii) 1/0 is defined as some real number? You'd probably prefer (i). And to preserve (i), our only recourse is to live in a universe where $\frac{1}{0}$ cannot be defined using any real number. This is why we tell all our students that $\frac{1}{0}$ is undefined—because it *cannot* be defined if we want to operate in a math world where the rules of fractions are followed.[2]

Remark 12.6.1. If you replace 1 by any other non-zero real number a, you can write a similar proof showing that $a/0$ must be undefined for the rules of fractions to hold true. Try it out.

Exercise 12.6.2. Show that there is no system of arithmetic where (i) the rules of fraction arithmetic hold true, and (ii) 0/0 is some real number.

Hint: You will need to use more rules of fraction arithmetic than we used in the previous proof. One rule is that "anything divided by itself is 1," and another is $(a/b) + (c/b) = (a + c)/b$.

[2]You may take an abstract algebra class in the future. The underlying fact we are invoking in the proof of Hiro's claim is: In a ring with more than one element, the additive identity does not admit a multiplicative inverse. And what I called "rules of fraction arithmetic" are the defining properties of rings, additive identity, and multiplicative inverse.

12.7 How do you write a proof (by contradiction?)

We will, inevitably, talk more about how to write a "proof" in general. Because it would be unhelpful to discuss what the word "proof" means before we get our brain juices flowing, let me just talk about writing style here.

But here, let me just say that there are different ingredients to writing anything.

(a.) Do you want to be *friendly* to the reader and include some details, or some extra instructions? For example, note that in the above proof, I didn't write "We will prove this statement by contradiction." This explicit tip might be very helpful! But an experience mathematician might not need this instruction because they can figure out that this is meant to be a proof by contradiction.

    Note that, sometimes, trying to be friendly can mean you become very chatty, and that you start drawing so many trees that the reader cannot see the forest. On the other hand, when you think that the reader is new to the subject, being friendly can be very helpful!

(b.) Do you want to be *efficient* and exclude some of the gnarly details, and only write enough so that whatever can be "read between the lines" is easy enough for the reader to figure out?

    Reading "efficiently written" proofs is very difficult; but it can also be the most fun. Trying to figure out how one sentence implies the next is a fun mental challenge, so every sentence is a puzzle. Writing "efficiently" also titrates the logic into its most important pieces, so in the end, it can help to give the reader a more intuitive of pictures of which steps were the most salient steps of your proof.

    If you like, efficient proofs read a little more like power point slides than like drawn-out essays.

(c.) But the most important part of the proof is that every step is *logically sound*. In other words, do all of your conclusions follow logically from previous knowledge or from your assumptions? For many students taking this class, even before questions of efficiency or friendliness, the biggest challenge will be coming up with a logically sound reason for certain conclusions. This is why we will practice, and this is why we will get feedback on our drafts.

The above commentary was about how to write proofs in general.

For now, let me just say that—to be friendly—it would be nice for you to write any of the following:

1. "We will prove the statement by contradiction," or "we proceed by contradiction."
2. "For the sake of contradiction, assume otherwise."
3. "Assume otherwise," or "assume not," or "suppose not."

These will all let the reader know that you are about to execute a proof by contradiction.

12.8 Exercises

Exercise 12.8.1. Which of the following does the notation $f : X \to Y$ imply?

(a) f is a function.

(b) f is a bijection.

(c) The domain of f is Y.

(d) The domain of f is X.

(e) The codomain of f is Y.

(f) f is a surjection.

(g) The image of f is Y.

Exercise 12.8.2. Which of the following is true?

(a) The image of a function is always equal to the codomain.

(b) The image of a function is always a subset of the codomain.

(c) The image of a function can be empty.

(d) If a function is a surjection, then its image is the codomain of the function.

(e) If the image of a function is the codomain, then the function is a surjection.