MATH 350: LECTURE 11

1. Review

Recall that we say sets A and B have the "same size", denoted $A \approx B$, iff there exists a one-to-one correspondence between elements of A and B. We saw that $\mathbb{Z}_{pos} \approx \mathbb{Z}_{pos} + 10$, $\mathbb{Z}_{pos} \approx 2\mathbb{Z}_{pos}$, $\mathbb{Z}_{pos} \approx \mathbb{Z}$, and $\mathbb{Z}_{pos} \approx \mathbb{Q}_{pos}$.

If $\mathbb{Z}_{pos} \approx A$, we say A is **countable**. We did not say *if and only if* here, since A is also countable if it is finite. Shreya wondered if we could modify our definition of "countable" to say that A is countable iff A is the same size as $\mathbb{Z}_{pos}$ *or smaller*. We'll come back to this!

2. Size of $\mathbb{R}$

So far, all the sets we've looked at have been countable. But we left off last time with a question from Jason: Is $\mathbb{R}$ countable?

Remark. Recall that for a set to be countable, we don't need *every* correspondence between the set and $\mathbb{Z}_{pos}$ to be a one-to-one correspondence. We just need to be able to find *some* one-to-one correspondence.

Theorem 2.1 (Cantor, "1876"ish)**.** *The open interval* $(0, 1)$ *is uncountable.*

Proof. What if $(0, 1)$ were countable? This means we can come up with a list of all the numbers in $(0, 1)$ such that we can pick any number in the interval and that number will be the m^{th} item on the list for some integer m. Say:

$$\begin{aligned} 1 &\leftrightarrow 0.53472\ldots \\ 2 &\leftrightarrow 0.86245\ldots \\ 3 &\leftrightarrow 0.2 \\ 4 &\leftrightarrow 0.9999832\ldots \\ &\vdots \end{aligned}$$

Cantor came up with a way of creating $\alpha \in (0, 1)$ that's nowhere on this list. The first digit of $x_1 = 0.\mathbf{5}3472\ldots$ is 5; we'll set the first digit of α to be something other than 5—say, 4. Similarly, the second digit of $x_2 = 0.8\mathbf{6}245\ldots$ is a 6, and we choose the second digit of α to be different from this, say 7. The third digit of x_3 is 0, and we pick the third digit of α to be different from this, say, 3. In general, choose the n^{th} digit of α to be different from the

Date: October 17, 2024.
Template by Leo Goldmakher.

n^{th} digit of the n^{th} number x_n on the list. Going through this process, we might construct a number $\alpha = 0.4732\ldots$. Note that $\alpha \neq x_n$ for all n because α and x_n disagree at the n^{th} digit (at the very least—probably in other digits, too). Therefore α is nowhere on the list. $\square$

You might object and say, well, our list is infinitely long, so maybe α occurs after infinitely many numbers on the list. One objection to this objection is: what does it mean to go *after* infinitely many other numbers? How do we get there? But also, recall that our definition of countability is the requirement that we can reach any number in our set after a *finite* amount of time, and we will never arrive at our constructed α after any finite number of steps. Thus our putative enumeration of $(0, 1)$ doesn't work.

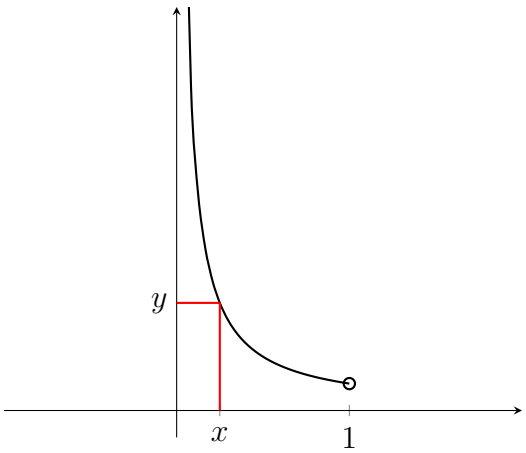
We've proved that $(0, 1) \not\approx \mathbb{Z}$, but in fact this tells us more. Observe

$$\underbrace{\{1/2, 1/3, 1/4, 1/5, \cdots\}}_{\approx \mathbb{Z}_{pos}} \subsetneq (0, 1) \implies \mathbb{Z}_{pos} \precneqq (0, 1)$$

That is, $\mathbb{Z}_{pos}$ is *strictly smaller* than $(0, 1)$; there's a copy of $\mathbb{Z}_{pos}$ sitting inside $(0, 1)$. What does this tell us about the size of $\mathbb{R}$? Before we tackle this, note the following facts:

- $[0, 1] \approx (0, 1)$. Intuitively, we don't expect adding a couple of points to change the size of the interval, but you'll prove this on the HW!
- $(1, 2) \approx (0, 1)$. The mapping $n \mapsto n+1$ is a one-to-one correspondence from $(0, 1) \to (1, 2)$
- $(0, 2) \approx (0, 1)$. The mapping $n \mapsto 2n$ is a one-to-one correspondence from $(0, 1) \to (0, 2)$

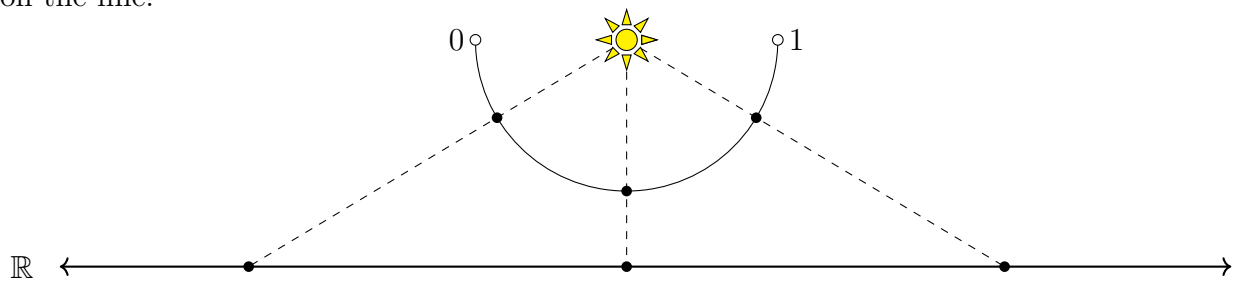
Most people thought $\mathbb{R} \approx (0, 1)$, but it was not as clear how to come up with a one-to-one correspondence. So how do we know this? Noam observed that the graph of $y = 1/x$ produces a one-to-one correspondence between $(1, \infty)$ and $(0, 1)$:



An illustration of the $1-1$ *correspondence* $(0, 1) \approx (1, \infty)$*, e.g.* x *corresponds to* y

Of course this doesn't quite answer the question about comparing $\mathbb{R}$ to $(0, 1)$, but it seems plausible that $(1, \infty) \approx \mathbb{R}$. How can we compare $\mathbb{R}$ to $(0, 1)$ directly? Here's a nice visualization (meta-analytic, but can be made rigorous!) of a one-to-one correspondence between $(0, 1)$ and $\mathbb{R}$. Imagine you bend the interval $(0, 1)$ into an arc above the real number line and

place a light source in the center. Each point on the interval will cast a shadow at a unique point on the line, and each point on the line will be the shadow of a unique point on the arc. This gives us a one-to-one correspondence between the points in the interval and the points on the line!



The openness of the interval is crucial here, since the endpoints would not cast shadows on the line. In a sense, we can think of the openness of this interval as corresponding to the infiniteness of $\mathbb{R}$.

Question. *(asked by Armie) Are $\mathbb{Z}$ and $\mathbb{R}$ the only two sizes that infinities come in, i.e., can we have infinite sets that are bigger, smaller, or in between?*

You'll prove on your HW that an infinite set cannot be strictly smaller than $\mathbb{Z}$. By contrast, given *any* set, it turns out we can construct a strictly larger set! Here's one way to see this:

Theorem 2.2 (Cantor)**.** *$\mathcal{P}(A)$ is strictly larger than A, for any set A.*

Thus, for example, $\mathbb{R} \precneqq \mathcal{P}(\mathbb{R}) \precneqq \mathcal{P}\Big(\mathcal{P}(\mathbb{R})\Big) \precneqq \cdots$. We will prove Cantor's theorem in a lecture or two (it's also in the book).

We've now answered Armie's question except for infinities strictly between $\mathbb{Z}$ and $\mathbb{R}$. Cantor conjectured the following:

Conjecture 2.3 (Continuum Hypothesis)**.** *There does not exist any set B s.t. $\mathbb{Z}_{pos} \precneqq B \precneqq \mathbb{R}$.*

The status of this conjecture is highly unusual. Kurt Gödel proved that the Continuum Hypothesis cannot be disproved using the (Zermelo-Fraenkel) axioms of set theory, which certainly lends credence to the conjecture. Paul Cohen shocked the mathematical world by proving that CH also cannot be *proved* using axioms of set theory. In other words, CH is independent of the axioms of set theory—even though it's phrased purely in the language of set theory! This is one example of a famous result due to Gödel: in any "nice" axiomatic system, it's possible to construct a statement in the language of that system that can neither be proved nor disproved within the system.

3. Injections, Surjections, and Bijections

Most of what we've done so far has been meta-analytic. Lets now make the notion of "one-to-one correspondence" more rigorous. Consider a function $f : A \to B$. By definition of a

function, this sets up a correspondence between *all* elements of A and *some* elements of B. How might this fail to be a one-to-one correspondence? There are precisely two ways:

(i) Two things in A might map to the same thing in B.

(ii) There might be something in B to which *no* element of A gets mapped.

Thomasina proposed a way to adapt our function to avoid both of these: for every $b \in B$, we stipulate the existence of precisely one $a \in A$ such that $f(a) = b$. There's an issue with this definition, however—it uses the word "one" as an adjective, which is something we have never rigorously defined how to do! (We know what the noun 1 means, but don't have an interpretation of it as a counting number.) Fortunately, as Thomasina pointed out, there's a way to restate the definition without using one at all:

Definition. A function $f : A \to B$ is a **bijection** iff $\forall b \in B\ \exists! a \in A$ s.t. $f(a) = b$.

Definition. We say $A \approx B$ if and only if there exists a bijection $f : A \to B$.

Observe that our notion of a bijection is secretly a two part definition. Indeed, to verify that f is a bijection, we need to prove two independent assertions:

(i) if $f(a) = f(a')$ then $a = a'$, and

(ii) $\forall b \in B\ \exists a \in A$ s.t. $f(a) = b$.

Any function $f : A \to B$ satisfying (i) is called injective (or an injection). Any function $f : A \to B$ satisfying (ii) is called surjective (or a surjection). Note that these two properties each fix the corresponding potential issue (i) and (ii) above.