REAL ANALYSIS: LECTURE 12

OCTOBER 19TH, 2023

1. Preliminaries

We've seen that

$$\mathbb{Z}_{\text{pos}} \approx \mathbb{Z} \approx \mathbb{Q}_{\text{pos}} \approx \mathbb{Q}.$$

Actually we're slightly cheating here: we've only shown that each is the same size as $\mathbb{Z}_{\text{pos}}$, but it turns out that $\approx$ is *transitive* (ie if $A \approx B$ and $B \approx C$ then $A \approx C$). Cool, let's get a little terminology going:

Definition (Countable)**.** If $A \approx \mathbb{Z}_{\text{pos}}$ or A is finite, we say A is *countable*. Otherwise, we say A is *uncountable*.

Remark. This word "countable" sorta makes intuitive sense. If $A \approx \mathbb{Z}_{\text{pos}}$ there's a way to pair up the elements $1, 2, 3, \ldots$. In other words, there exists an algorithm such that, if you give me some $x \in A$, that algorithm will "count" elements of A and get to x in a finite amount of steps. Note that the algorithm *doesn't depend on your choice of* x!

Remark. You might think that any two uncountable sets have the same size, but this is not the case! When two sets are uncountable, all we know is that neither has the same size as $\mathbb{Z}_{\text{pos}}$. (We'll see concrete examples of uncountable sets of different sizes below.)

Let's meet our first example of an uncountable set:

Theorem 1 (Cantor)**.** $[0, 1]$ *is uncountable.*

(This proof is slightly informal, but it can be made completely rigorous.)

Proof. Suppose $[0, 1]$ were countable, i.e. there exists a bijection $f : \mathbb{Z}_{\text{pos}} \hookrightarrow\!\!\!\!\rightarrow [0, 1]$. So maybe for example we have something like

$$\begin{aligned} 1 &\mapsto .5298771 \\ 2 &\mapsto .125 \\ 3 &\mapsto .44451208 \\ 4 &\mapsto .92716 \\ &\vdots \end{aligned}$$

We claim $\exists \alpha \in [0, 1]$ s.t. α isn't anywhere in the list; in other words, f isn't a bijection! Here's how we construct α. We begin with

$$\alpha = 0.1\ldots$$

Whatever α is, it's definitely not the first number, since the first number starts with $.5$. Ok. Let's keep going:

$$\alpha = 0.17\ldots$$

Whatever α is, it still can't be the first number on our list, but it also can't be the second number, since it disagrees in the second place with $.125$. Keep going! Construct an α for which the nth digit of α is different from the nth digit of the nth number of the putative bijection above. This new α *must* be different than every number on the list, but it's surely in $[0, 1]$, meaning that f is *not* a bijection. (In other words, f will *never* count all the way up to α.) This contradiction implies that $[0, 1]$ is *uncountable*. $\square$

Notes on a lecture by Leo Goldmakher; written by Justin Cheigh.

Remark. This proof is called *Cantor's diagonal argument*. It's rare for a proof to have a name, but this idea turns out to be useful in many other disciplines.

OK, so $[0,1]$ and $\mathbb{Z}_{\text{pos}}$ aren't the same size. Which one is bigger? Forrest observed

$$\left\{\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots\right\} \subseteq [0,1],$$

and it seems pretty clear (and is true) that

$$\left\{\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots\right\} \approx \mathbb{Z}_{\text{pos}}.$$

So, a copy of $\mathbb{Z}_{\text{pos}}$ lives in $[0,1]$, but we proved there's no bijection between $[0,1]$ and $\mathbb{Z}_{\text{pos}}$, which together imply (intuitively) that $[0,1]$ is strictly bigger.

Edith asked an important question: what goes wrong with trying to apply the "diagonalization" argument to the rationals? Here's one way to think about what's happening: if a set is countable, then there exists an algorithm that will get you to any element in a finite number of steps. **Note, crucially, that it's a single algorithm—it doesn't depend on which element you're trying to get to!** Our algorithm for counting the rationals—sweeping back and forth along diagonals, skipping any repeats—would arrive at any given rational after a finite number of steps. By contrast, Cantor's diagonal argument demonstrates that *any* algorithm that attempts to accomplish this for the unit interval is doomed to failure—given any counting algorithm, there exist numbers in the interval that the algorithm will never get to.

Ali observed that this argument isn't really about the specific interval $[0,1]$. For example, what about $[0,.5]$? It's also uncountable! In fact, it has the same size as $[0,1]$:

$$\begin{aligned} [0,1] &\hookrightarrow\!\!\!\!\!\rightarrow [0,0.5] \\ x &\mapsto x/2. \end{aligned}$$

What about $(0,1)$? It's plausible that it's uncountable, and moreover, that

$$[0,1] \approx (0,1);$$

after all, these intervals only differ by two points. How can we show this?

Edith proposed the following strategy. By a similar logic to $[0,0.5] \approx [0,1]$, you can probably buy that

$$[0.25, 0.75] \approx [0,1].$$

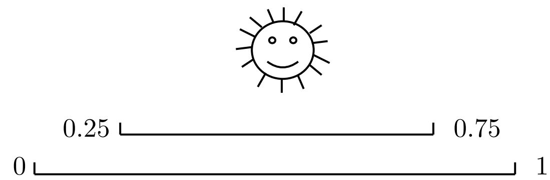
Further, $[0.25,0.75] \hookrightarrow (0,1)$, simply by mapping $x \mapsto x$. So, $(0,1)$ is *at least as large as* $[0.25,0.75] \approx [0,1]$. On the other hand, $(0,1) \hookrightarrow [0,1]$, so $[0,1]$ is *at least as large as* $(0,1)$. Since each of $[0,1]$ and $(0,1)$ are at least as large as the other, we expect them to have the same size. But is this expectation actually justified?

Theorem 2 (Cantor-Schröder-Bernstein)**.** *If $A \hookrightarrow B$ and $B \hookrightarrow A$, then $A \approx B$.*

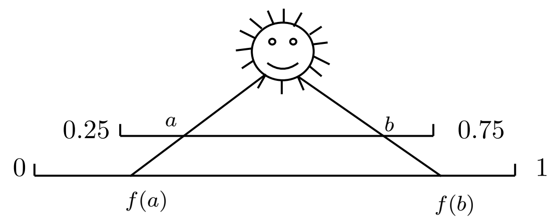
Remark. One way to think about this is that if we can find an injection $g : A \hookrightarrow B$, and a surjection $h : A \twoheadrightarrow B$, then there must exist a bijection $f : A \hookrightarrow\!\!\!\!\!\rightarrow B$. But this really isn't obvious: g and h might have nothing to do with one another, so out of the two of them, how do you construct a single function f that is simultaneously an injection and a surjection? This is what makes the proof quite tricky, despite the strong intuitive argument (suggested by Edith). A proof of this theorem will be posted to the course website.

This theorem is a good "hammer", i.e. it is very useful in proving two things have the same size. Cool, now what about $\mathbb{R}$? How does the size of $\mathbb{R}$ relate to the size of $(0,1)$ or $[0,1]$? Emily, coining a new term, calls $\mathbb{R}$ "countably" uncountable. Each $[0,1]$ interval is uncountable, and we can kinda "tile" $\mathbb{R}$ with a countable number of $[0,1]$ intervals ($[0,1] \cup [1,2] \cup [3,4] \cdots = \mathbb{R}$). Here's another way to see this.

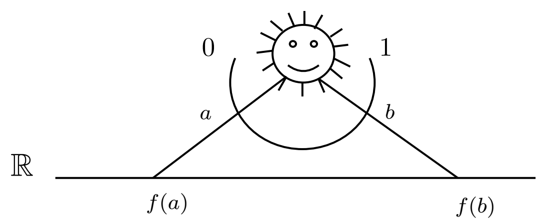
Let's look at a visual way to see $[0.25, 0.75] \approx [0,1]$.



Here, we just drew a "sun" over the interval $[0.25, 0.75]$ and $[0, 1]$. Now we can project sunbeams through the $[0.25, 0, 75]$ interval onto the $[0, 1]$ interval. The bijection we define is to map the points of $[0.25, 0.75]$ to wherever their shadow is in $[0, 1]$. Here's a picture:



For example, here the bijection f would send $a \in [0.25, 0.75]$ to $f(a) \in [0, 1]$, and same with $b \mapsto f(b)$. Ok, now let's do something analogous with $(0, 1)$ and $\mathbb{R}$. Here we can't just write the entire $\mathbb{R}$ and do the same trick, but Miles pointed out we can bend $(0, 1)$ to get a very similar picture:



Hopefully, this visualization convinces you that $\mathbb{R} \approx (0, 1)$.

We've seen that $\mathbb{Q}$ is countable while $[0, 1]$ is not, and that $[0, 1]$ is a "strictly larger" infinite set. Here's a different approach that shows that $\mathbb{Q}$ is minuscule compared to $[0, 1]$ from a geometric perspective:

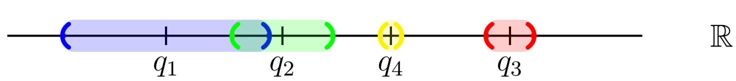
Claim. The total length of $\mathbb{Q}$ is 0, while the total length of $[0, 1]$ is 1.

Proof. Although we're only going to present an intuitive argument, it can be made rigorous (take measure theory to see how!). The length of $[0, 1]$ is clear, but what could it mean to measure the length of $\mathbb{Q}$?

$\mathbb{Q}$ is countable, so we can express it in the form

$$\mathbb{Q} = \{q_1, q_2, q_3, \dots\}.$$

Take q_1 and "cover" it with an interval $[q_1 - 1/4, q_1 + 1/4]$; note that this interval has length $\frac{1}{2}$. Next, cover q_2 with an interval $[q_2 - 1/8, q_2 + 1/8]$, which has length $\frac{1}{4}$. In general, cover q_k with an interval $\left[q_k - \frac{1}{2^{k+1}}, q_k + \frac{1}{2^{k+1}}\right]$, which has length $\frac{1}{2^k}$. Here's a picture of the situation:



Thus, we've "covered" the entirety of $\mathbb{Q}$ with intervals, the total length of which is

$$\leq \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots = 1.$$

(We have $\leq$ rather than $=$ because some of the intervals might be overlapping, as in the illustration.) In other words, we can cover the *entirety* of $\mathbb{Q}$ by intervals of total length ≤ 1. So we'll say the length of $\mathbb{Q}$ is at most 1.

Of course, there was nothing special about the number 1 above; we could have just as easily covered all of $\mathbb{Q}$ by intervals of total length at most 0.1, simply by replacing 1 everywhere in the argument above by 0.1 (which is what we did in class). More generally, we see that the length of $\mathbb{Q}$ can be made smaller than any positive number. There's only one non-negative real number that's smaller than every positive number: 0. We conclude that the length of $\mathbb{Q}$ must be 0, as claimed. $\square$

So far, all the infinite sets we've seen are either the same size as $\mathbb{Z}_{\text{pos}}$ or as $[0, 1]$. Are there larger ones? Yes! In fact, the following result shows that no matter which set we start with, there's always a strictly larger one:

Theorem 3 (Cantor)**.** $A \not\approx \mathcal{P}(A)$.

Observe that $A \hookrightarrow \mathcal{P}(A)$ (for example, via the map $x \mapsto \{x\}$). Thus, it suffices to show

$$\nexists f : A \twoheadrightarrow \mathcal{P}(A).$$

Before proving this, let's build up some intuition with a couple examples. Given $A := \{1, 2, 3\}$, we define a function $A \to \mathcal{P}(A)$.

(i) Consider $g(1) = \{1\}, g(2) = \{1, 2\}, g(3) = \{1, 2, 3\}$. This is not a surjection, since for example $\{2, 3\}$ is not an output.

(ii) Consider h defined by $1 \mapsto \emptyset, 2 \mapsto \{3\}, 3 \mapsto \{1, 2\}$. Notice $\{1, 3\}$ isn't an output, so h is not a surjection.

In these examples we showed that the maps weren't surjective by coming up with an example of a set that wasn't outputted. How does one construct such a set for an arbitrary function? Cantor came up with an ingenious one: given a function $f : A \to \mathcal{P}(A)$, consider the set

$$B := \{x \in A : x \notin f(x)\}.$$

In words: B consists of all the things in A that aren't elements of their own image. Thus in example (i) above we'd have $B = \emptyset$, while in example (ii) we'd have $B = \{1, 2, 3\}$. In both of these examples, B isn't in the image of the function, and that's not an accident:

Proof. Given $f : A \to \mathcal{P}(A)$, set

$$B := \{x \in A \ : \ x \notin f(x)\}.$$

Clearly, $B \in \mathcal{P}(A)$. If f were a surjection, there would exist some $a \in A$ such that $f(a) = B$. But now observe that

$$a \in B \quad \iff \quad a \notin f(a) \quad \iff \quad a \notin B.$$

This is a contradiction, and it follows that f cannot be a surjection. $\square$