Lecture 10: Countability & Beyond Infinity

built on 2021/02/03 at 21:04:48

Consider the following statements carefully: We're only talking about integers here.

- A is the set of all numbers (including both squares and nonsquares)
- B is the set of all squares.
- *Is A larger than B?*

Our intuition suggests that $|A| > |B|$. After all, A contains everything B has and some more. But then:

Thought 1: Let's see, how many squares there are? As many as the corresponding number of square roots (of the squares): every square number is x^2 so $\sqrt{x^2} = x$.

```
Commentary: For every square, there is a (unique) corresponding positive integer.
```

Thought 2: How many square roots are there? As many as all the numbers: every number is the square root of some square (for each y, there is y^2)

```
Commentary: Every number is the square root of a square.
```

Our intuition indeed fails to reason about infinite quantities. Even, Guass (Carl Friedrich Gauss) had said:

> *Infinity is nothing more than a figure of speech which helps us talk about limits. The notion of a completed infinity doesn't belong in mathematics.*

But as we look more at limits of computation, we need to be able to reason about infinity.

Today we're going to study some of Cantor's work. Georg Cantor (1845–1918) has made many contributions to the study of cardinality and infinities, among them:

- How to systematically compare the size of (infinite) sets, showing, among others, that $\mathbb{N}$ has the same "size" as $\{k^2 \mid k \in \mathbb{N}\}$.
- There are many levels of infinity.
- There are infinitely many infinities.
- The diagonalization argument.

Reaction to Cantor's idea at the time was mixed: Some thought he was crazy. Some saw genius in his work.

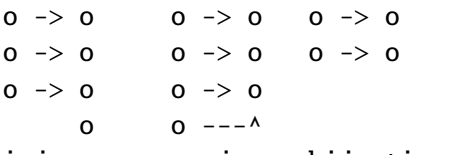
1 Cardinality: Cantor's Definition

Cantor's work is often seen as the origin of set theory. Before Cantor, the distinction was made only between finite sets, which were already intuitively easy to understand, and "the infinite," which was utterly confusing and reserved mainly for philosophical discussion. We begin our journey by looking at the notion of the relative size of two sets.

1.1 Reminder: The Three Worlds of Functions

You have seen this in Discrete Math. A quick reminder:

- *injective* (aka. 1-to-1). A function $f : A \to B$ is *injective* if for all $a \neq a'$, $f(a) \neq f(a')$.
- *surjective* (aka. onto). A function $f : A \to B$ is *surjective* if for all $b \in B$, there exists an $a \in A$ s.t. $f(a) = b$.
- *bijective* (aka. 1-to-1 onto, or 1-to-1 correspondence). A function f is *bijective* if it is injective and surjective.



Immediate from these definitions are the following facts:

- If there is an **injective** function $f : A \to B$, then $|A| \leqslant |B|$.
- If there is a **surjective** function $f : A \to B$, then $|A| \geqslant |B|$.
- If there is a **bijective** function $f : A \to B$, then $|A| = |B|$.

Definition 1.1 (Cantor's View of Size) *Let A and B be sets. Say A and B have the same* cardinality *(size), denoted by $|A| = |B|$, if there exists a bijection between them.*

Using this definition, we're ready to revisit our initial example:

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots\}$$
$$B = \{0, 1, \quad 4, \quad 9, \dots\}$$

Indeed, there is a bijection between $\mathbb{N}$ and B. We can show that $f : \mathbb{N} \to B$, where $f(x) = x^2$, is a bijection. The strange thing is that $B \subsetneq \mathbb{N}$ but $|\mathbb{N}| = |B|$.

1.2 Properties

We can then prove the following facts:

- $|A| \leqslant |B|$ if and only if $|B| \geqslant |A|$ (easy proof).
- $|A| \leqslant |B|$ and $|B| \leqslant |C|$ implies $|A| \leqslant |C|$ (easy proof).
- $|A| = |B|$ if and only if $|A| \leqslant |B|$ and $|B| \leqslant |A|$.

Therefore:

- To show $|A| \leqslant |B|$, give an injective function or otherwise show that $|B| \geqslant |A|$ by giving a surjective function.
- Don't forget we have transitivity
- To show $|A| = |B|$, suffices to show $|A| \leqslant |B|$ and $|B| \leqslant |A|$ — or give a bijection directly.

1.3 More Mind Benders: Hilbert's Hotel

Suppose we have a fully occupied hotel that has infinitely many rooms. Surprisingly:

- We can accommodate an extra guest: $|\mathbb{N} \cup \{\text{a new guest}\}| = |\mathbb{N}|$. The same argument allows us to show that $|N \backslash \{0\}| = |\mathbb{N}|$.
- We can accommodate twice as many guests:

  $$|\mathbb{N}| = \{\text{Bus1\_Cust1}, \text{Bus1\_Cust2}, \text{Bus1\_Cust3}, \dots\} =: A$$
  $$|\mathbb{N}| = \{\text{Bus2\_Cust1}, \text{Bus2\_Cust2}, \text{Bus2\_Cust3}, \dots\} =: B$$

  It can be shown that $|A \cup B| = |\mathbb{N}|$.
- We can accommodate infinitely many "buses":

  $$|\mathbb{N}| = \{\text{Bus}\mathbf{k}\text{\_Cust1}, \text{Bus}\mathbf{k}\text{\_Cust2}, \text{Bus}\mathbf{k}\text{\_Cust3}, \dots\} =: A_k$$

  It can be shown $|\bigcup_{i \in \mathbb{N}} A_i| = |\mathbb{N}|$. Ultimately, we know that $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Factoid: Pigeonhole doesn't apply here.

2 Countable and Countably Infinite

If S is an infinite set but we can list off the elements as $s_0, s_1, \ldots$ uniquely in a well-defined way, then $|S| = |\mathbb{N}|$. The "uniquely in a well-defined way" is code for if you are required to, you can write a precise bijection for it. This means (and you can verify later) that all the following have the same "size" as $\mathbb{N}$:

$$\begin{aligned}
\mathbb{N} &= \{0, 1, 2, \ldots, \} \\
\textsc{Even} &= \{0, 2, 4, 6, 8, \ldots\} \\
\mathbb{Z} &= \{0, -1, +1, -2, +2, -3, +3, \ldots\} \\
\textsc{Prime} &= \{2, 3, 5, 7, 11, 13, 17, \ldots\}
\end{aligned}$$

Definitions: Any set S is said to be *countably infinite* if $|S| = |\mathbb{N}|$. So then, a set is *countable* if it is either finite or countably infinite.

Hence:

- $\mathbb{N}$ is for sure countable (more precisely, countably infinite)
- What about $\mathbb{Z}$? It is countably infinite.
- What about $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$? By "dovetailing," we can enumerate $\mathbb{N}^2$. So $|\mathbb{N}^2| = |\mathbb{N}|$.
- The same is true for $\mathbb{Z}^2$: $|\mathbb{Z}^2| = |\mathbb{Z}| = |\mathbb{N}|$.
- What about the rationals $\mathbb{Q}$? Apparently, $\mathbb{Q}$ is also countably infinite. First, we observe that $|\mathbb{Z} \times \mathbb{Z}| \geqslant |\mathbb{Q}|$. Why? Consider the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Q}$, where

$$f(x, y) = \begin{cases} x/y & \text{if } y \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

  This function is surjective. It is easy to show (you do it) that $|\mathbb{Q}| \geqslant |\mathbb{N}|$, hence concluding that $|\mathbb{Q}| = |\mathbb{N}|$.

What about the set of all binary strings $\{0,1\}^*$? This turns out to be countable too. First, we do the empty string. Then strings of length 1 (in numerical order), then length 2 (in numerical order), etc. etc.

$$\begin{aligned}
\{0,1\}^* = \{&\varepsilon, \\
&0, 1 \\
&00, 01, 10, 11 \\
&000, 001, 010, 011, 100, 101, 110, 111 \\
&\vdots \\
\}&
\end{aligned}$$

Hence, $|\{0,1\}^*| = |\mathbb{N}|$.

3 The Diagonalization Argument

If A and B are infinite sets, do they always have the same size, i.e., $|A| = |B|$? Apparently not. Consider $\mathbb{R}$. We'll show, using Cantor's diagonalization argument, that $\mathbb{R}$ is strictly bigger than $\mathbb{N}$.

As a warm-up, we'll consider $\{0,1\}^{\mathbb{N}}$. This is different from $\{0,1\}^*$. Each element of the set $\{0,1\}^{\mathbb{N}}$ is a binary string of infinite length. On the other hand, each element of $\{0,1\}^*$ is a binary string of a finite length.

We'll now get to the proof.

Theorem 3.1 *$\{0,1\}^{\mathbb{N}}$ is **not** countable.*

Let's start with a sketch of proof ideas. Our proof will be by contradiction, so suppose on the contrary that we can make a list of all infinite binary strings. Hence, we'll have a list such as the following (binary strings only given for illustration purposes; who knows what they actually are):

$$\begin{aligned}
s_0 &= \underline{0}\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ \ldots \\
s_1 &= 1\ \underline{0}\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ \ldots \\
s_2 &= 0\ 1\ \underline{0}\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ \ldots \\
s_3 &= 1\ 0\ 0\ \underline{1}\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ \ldots \\
s_4 &= 1\ 0\ 0\ 0\ \underline{1}\ 0\ 0\ 0\ 1\ 0\ 0\ \ldots \\
&\vdots
\end{aligned}$$

Consider the following string formed by reading off the diagonal of this table—and its bitwise negation.

$$d = 0\ 0\ 0\ 1\ 1\ \ldots \implies \sim d = 1\ 1\ 1\ 0\ 0\ \ldots$$

This string $\sim d$ can't be any s_k because it differs from every one of them. And we have a contradiction!

Formal Proof: We can write it more formally as follows:
Proof: Suppose for a contradiction that $\{0,1\}^{\mathbb{N}}$ is countable, so $|\mathbb{N}| \geqslant |\{0,1\}^{\mathbb{N}}|$. This means, there exists a surjective function $f : \mathbb{N} \to \{0,1\}^{\mathbb{N}}$. Define the following string $d \in \{0,1\}^{\mathbb{N}}$ so that for $i = 0, 1, 2, \ldots,$

$$d[i] = 1 - f(i)[i]$$

that is, $d[i]$ is taking the i-th bit of the string given by $f(i)$ and negating it. We'll show that d differs from $f(k)$ for every $k \in \mathbb{N}$. In particular, they disagree on the k-th position, i.e., $d[k] \neq f(k)[k]$. Hence, f can't possibly be a surjective function from $\mathbb{N} \to \{0,1\}^{\mathbb{N}}$, a contradiction! ■

The same idea gives the following theorem:

Theorem 3.2 *For any nonempty set A (possibly infinite),* $|A| < |2^A|$.

Proof: Why don't you try it? ■

This means that $\{0,1\}^N$ is uncountable. Moreover, there is a whole family of larger and larger "infinities" $|\mathbb{N}| < |2^{\mathbb{N}}| < |2^{2^{\mathbb{N}}}| \ldots$.

Coming back to the reals.. The reals itself $\mathbb{R}$ is uncountable: we can show that $|[0,1)| = \mathbb{R}$ (see your hwk). We can also show that $|[0,1)| = \{0,1\}^{\mathbb{N}}$. How? Well, $f : [0,1) \to \{0,1\}^{\mathbb{N}}$ maps the input real number to its binary expansion[1]

4 Some Fun Facts

- We have shown $\{0,1\}^*$ is countable. The same idea can be used to show that Σ^* is countable for any finite Σ. Therefore, the set of all possible computer programs is countable.
- This also means the set of all polynomial in x whose coefficients are integers is countable. Pick Σ to be $\{0, 1, \ldots, 9, x, +, -, *, \hat{}\}$.
- Finally, many numbers are computable—in the sense that there is a computer program that computes it. But then, $|\mathbb{R}| > \Sigma^*$, so there are real numbers that can't be computed by any program.

[1] Technically, it's not surjective because 0.1 and $0.011111111\ldots$ are both $1/2$. But this technical glitch can be fixed. We won't bother with it here.