Cantor's Diagonal Argument

Recall that...

- A set S is finite iff there is a bijection between S and $\{1, 2, \ldots, n\}$ for some positive integer n, and infinite otherwise. (I.e., if it makes sense to count its elements.)
- Two sets have the same cardinality iff there is a bijection between them. ("Bijection", remember, means "function that is one-to-one and onto".)

A set S is called countably infinite if there is a bijection between S and $\mathbb{N}$. That is, you can label the elements of S 1, 2, ... so that each positive integer is used exactly once as a label.

Why "countably infinite"? Such a set is countable because you can count it (via the labeling just mentioned). Unlike a finite set, you never stop counting. But at least the elements can be put in correspondence with $\mathbb{N}$.

On the other hand, **not all infinite sets are countably infinite. In fact, there are infinitely many sizes of infinite sets.**

Georg Cantor proved this astonishing fact in 1895 by showing that the the set of real numbers is not countable. That is, it is impossible to construct a bijection between $\mathbb{N}$ and $\mathbb{R}$. In fact, it's impossible to construct a bijection between $\mathbb{N}$ and the interval $[0, 1]$ (whose cardinality is the same as that of $\mathbb{R}$).

Here's Cantor's proof.

Suppose that $f : \mathbb{N} \to [0, 1]$ is any function. Make a table of values of f, where the 1st row contains the decimal expansion of $f(1)$, the 2nd row contains the decimal expansion of $f(2)$, ... the nth row contains the decimal expansion of $f(n)$, ... Perhaps $f(1) = \pi/10$, $f(2) = 37/99$, $f(3) = 1/7$, $f(4) = \sqrt{2}/2$, $f(5) = 3/8$, so that the table starts out like this.

n	$f(n)$												
1	0	.	3	1	4	1	5	9	2	6	5	3	...
2	0	.	3	7	3	7	3	7	3	7	3	7	...
3	0	.	1	4	2	8	5	7	1	4	2	8	...
4	0	.	7	0	7	1	0	6	7	8	1	1	...
5	0	.	3	7	5	0	0	0	0	0	0	0	...
⋮	⋮												

Of course, only part of the table can be shown on a piece of paper — it goes on forever down and to the right.

Can f possibly be onto? That is, can every number in $[0, 1]$ appear somewhere in the table?

In fact, the answer is no — there are lots and lots of numbers that can't possibly appear! For example, let's highlight the digits in the main diagonal of the table.

n	$f(n)$												
1	0	.	**3**	1	4	1	5	9	2	6	5	3	...
2	0	.	3	**7**	3	7	3	7	3	7	3	7	...
3	0	.	1	4	**2**	8	5	7	1	4	2	8	...
4	0	.	7	0	7	**1**	0	6	7	8	1	1	...
5	0	.	3	7	5	0	**0**	0	0	0	0	0	...
⋮	⋮												

The highlighed digits are $0.37210\ldots$. Suppose that we add 1 to each of these digits, to get the number

$$0.48321\ldots.$$

Now, this number can't be in the table. Why not? Because

- it differs from $f(1)$ in its first digit;
- it differs from $f(2)$ in its second digit;
- ...
- it differs from $f(n)$ in its nth digit;
- ...

So it can't equal $f(n)$ for any n — that is, it can't appear in the table.

This looks like a trick, but in fact there are lots of numbers that are not in the table. For example, we could subtract 1 from each of the highlighted digits (changing 0's to 9's), getting 0.26109 — by the same argument, this number isn't in the table. Or we could subtract 3 from the odd-numbered digits and add 4 to the even-numbered digits. Or we could even highlight a different set of digits:

n	$f(n)$												
1	0	.	3	**1**	4	1	5	9	2	6	5	3	...
2	0	.	**3**	7	3	7	3	7	3	7	3	7	...
3	0	.	1	4	2	**8**	5	7	1	4	2	8	...
4	0	.	7	0	**7**	1	0	6	7	8	1	1	...
5	0	.	3	7	5	0	**0**	0	0	0	0	0	...
⋮	⋮												

As long as we highlight at least one digit in each row and at most one digit in each column, we can change each the digits to get another number not in the table. Here, if we add 1 to all the highlighted digits, we end up with $0.42981\ldots$ — there's a real number that does not equal $f(n)$ for any positive integer n.

What is the point of all this? Precisely that the function f can't possibly be onto — there will always be (infinitely many!) missing values. Therefore, there does not exist a bijection between $\mathbb{N}$ and $[0, 1]$.

If S is a set, then the power set $\mathcal{P}(S)$ is defined as the set of all subsets of S. For example, if $S = \{1, 3, 4\}$, then

$$\mathcal{P}(S) = \Big\{\ \{\},\ \{1\},\ \{3\},\ \{4\},\ \{1,3\},\ \{1,4\},\ \{3,4\},\ \{1,3,4\}\ \Big\}.$$

When S is finite, it's not hard to see that $|\mathcal{P}(S)| = 2^{|S|}$: (because to choose a subset R of S, you need to decide whether each element of S does or does not belong to R). In the above example, $|S| = 3$ and $|\mathcal{P}(S)| = 8 = 2^3$.

What about infinite sets? Using a version of Cantor's argument, it is possible to prove the following theorem:

Theorem 1. *For every set S, $|S| < |\mathcal{P}(S)|$.*

Proof. Let $f : S \to \mathcal{P}(S)$ be any function and define

$$X = \{s \in S \mid s \notin f(s)\}.$$

For example, if $S = \{1, 2, 3, 4\}$, then perhaps $f(1) = \{1, 3\}$, $f(2) = \{1, 3, 4\}$, $f(3) = \{\}$ and $f(4) = \{2, 4\}$. In this case X does not contain 1 (because $1 \in f(1)$), X does contain 2 (because $2 \notin f(2)$), X does contain 2 (because $3 \notin f(3)$), and X does not contain 2 (because $4 \in f(4)$), so $X = \{2, 3\}$.

Now, is it possible that $X = f(s)$ for some $s \in S$? If so, then either s belongs to X or it doesn't. But by the very definition of X, if s belongs to X then it doesn't belong to X, and if it doesn't then it does. This situation is impossible — so X cannot equal $f(s)$ for any s. But, just as in the original diagonal argument, this proves that f cannot be onto. □

For example, the set $\mathcal{P}(\mathbb{N})$ — whose elements are sets of positive integers — has more elements than $\mathbb{N}$ itself; that is, it is not countably infinite.

As a consequence of this result, the sequence of infinite sets

$$\mathbb{N}, \quad \mathcal{P}(\mathbb{N}), \quad \mathcal{P}(\mathcal{P}(\mathbb{N})), \quad \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))), \quad \ldots$$

must keep increasing in cardinality. That is, there are infinitely many different sizes of infinity!