An Alternative Formulation and Proof of Cantor's Theorem

Ray Chen

University of Toronto

August 2, 2024

Introduction

- Cantor's Theorem, one of the most important theorems in set theory, has many different equivalent formulations
- Generally, the Theorem can be summarized by its most notable implication: "There is no largest cardinal number."
- The main formulation and proof method taught in undergraduate set theory and analysis courses relies on proving that the power set (the set of all subsets) of any set is strictly larger than the original set, finite or infinite
- In this presentation, I shall demonstrate an alternative formulation and proof of Cantor's Theorem utilizing the set 2^X

What is 2^X, anyway?

- Some math textbooks consider 2^X to be *exactly equivalent* to the power set $\mathcal{P}(X)$, and refer to both as "the power set"
- However, this is not *literally* true
- Generally, for two sets A, B we define:

$$B^A := \{f \mid f : A \to B\}$$

  or "B^A is the set of all functions $A \to B$"
- 2 is simply the natural number 2, which in the standard set theoretic definition, is the set $\{0, 1\}$
- So in summary, 2^X is expressed as "The set of all functions from the set X to the set $\{0, 1\}$"
- We can say $|2^X| = 2^{|X|}$ (this is the definition of the cardinal $2^{|X|}$ when X is infinite; try proving it for finite sets!)
- Furthermore, $|2^X| = |\mathcal{P}(X)|$ (another exercise)

An application of set powers: Linear Algebra

- If you've done linear algebra before, then you've seen set power notation used in $\mathbb{R}^n$, or the set of all n-dimensional vectors
- For example, we can precisely define any vector $(x, y) \in \mathbb{R}^2$ as such:

$$(x, y) = [f : 2 \to \mathbb{R}] \in \mathbb{R}^2 \mid f(0) = x, f(1) = y$$

Motivation

- But why even go through the effort of this alternative proof?
- Through this formulation of the theorem, we get a more *precise* value for the cardinality of power sets, one that works for both finite and infinite sets
- I personally find $2^{|X|}$ to be a "purer" expression than $|\mathcal{P}(X)|$, though this is just an opinion; the former is a representation of a number (infinite cardinal or not) while the latter is the size of another set
- Additionally, this proof aligns much closer with the informal diagonalization argument; imagining diagonalization with sets is much harder in my opinion than imagining it with digits

The Proof (Introduction)

We want to prove the statement "There is no largest cardinal number." We shall show that for any set and its associated cardinality, there is a set with a strictly larger cardinality.

Let X be any set. We want to show that there exists a set Y such that $|X| < |Y|$. We pick $Y = 2^X$.

We shall show:

- $|X| \leq |2^X|$ (there's an injection from X to 2^X)
- $|X| \geq |2^X|$ is impossible (there's no surjection from X to 2^X)

(Note that technically, only the latter is strictly required to prove the theorem, as $\neg(|X| \geq |2^X|) \implies |X| < |2^X|$, but this is actually surprisingly difficult to prove for infinite cardinals, and requires the Axiom of Choice, so our chosen route gives us a "simpler" proof.)

The Proof (Part 1: $|X| \leq |2^X|$)

We are trying to find an injective function $f : X \to 2^X$. In other words, we want a function that maps each element of X to another function $s : X \to \{0, 1\}$ (call this inner function a "sequence"), and we want each mapped sequence to be distinct from any other.

For any $x \in X$, define $f(x) = s_x : X \to \{0, 1\}$ such that for any $y \in X$,

$$s_x(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{otherwise} \end{cases}$$

In other words, map each element x to its "indicator" sequence that only gives the value 1 if x is passed.

Suppose for some $x_1, x_2 \in X$ that $x_1 \neq x_2$. Then $f(x_1) = s_{x_1}$ and $f(x_2) = s_{x_2}$. $s_{x_1}(x_1) = 1$ by definition. However, since $x_1 \neq x_2$, $s_{x_2}(x_1) = 0$. Thus, since they differ in at least one value, $s_{x_1} \neq s_{x_2}$, meaning $f(x_1) \neq f(x_2)$. Thus, the function f is an injection, and $|X| \leq |2^X|$.

The Proof (Part 2: $\neg(|X| \geq |2^X|)$)

Now we show that there can be no surjection between X and 2^X. Let $f : X \to 2^X$ be arbitrary. To show non-surjectivity, we must show that the image $f[X]$ is not equivalent to the codomain 2^X by demonstrating the existence of a sequence $s \in 2^X$ such that $s \notin f[X]$.

For any $x \in X$, define $s : X \to \{0, 1\}$ as:

$$s(x) = \begin{cases} 1 & \text{if } [f(x)](x) = 0 \\ 0 & \text{if } [f(x)](x) = 1 \end{cases}$$

Since s is a function $X \to \{0, 1\}$, it is in 2^X by definition.

For any $x \in X$, either $[f(x)](x) = 0$ or $[f(x)](x) = 1$.

If the former is true, then by definition $s(x) = 1$ and $s \neq f(x)$ since they differ by a value. On the other hand, if the latter is true, then likewise $s(x) = 0$ so again, $s \neq f(x)$.

Thus, there is no $x \in X$ where $f(x) = s$, meaning $s \notin f[X]$. From there we know that our arbitrary f is not surjective, so $\neg(|X| \geq |2^X|)$.

The Proof (Conclusion)

From Part 1, we know that there is an injection from X to 2^X ($|X| \leq |2^X|$).

From Part 2, we know that there is no surjection from X to 2^X, meaning there is no bijection ($\neg(|X| \geq |2^X|) \implies |X| \neq |2^X|$).

It follows that the cardinality of X is strictly smaller than the cardinality of 2^X ($|X| < |2^X|$).

We conclude that there is no largest cardinal number, as for any cardinal κ, we know the cardinal 2^κ is larger. $\square$

Remarks

- This proof was adapted from a problem set given in the course MAT246: Concepts in Abstract Mathematics taught by Tona Wiederhold at the University of Toronto
- If you're familiar with a proof of the power set version of Cantor's Theorem, you'll notice similarities in structure, though the differences in definition of 2^X and $\mathcal{P}(X)$ still lead to largely distinct proofs
- Exercise: try illustrating this proof as a diagonalization argument, specifically proving there's no bijection between the natural numbers and infinite strings of ones and zeroes (e.g. 10101010..., 10010110..., 11111111... etc.)