Topics: Cardinality of power sets

Theorem (Cantor) For any set $A$, $|A| < |P(A)|$.

Proof: If $A = \emptyset$, then $P(A) = \{\emptyset\}$, and
$$|A| = 0 < 1 = |P(A)|$$

So we can assume for the rest of the proof that $A \neq \emptyset$.

We need to show there is an injection $f: A \to P(A)$ and that $f$ is a bijection $g: A \to P(A)$.

Let $f: A \to P(A)$ be given by $f(a) = \{a\} \subseteq A$.

This is injective since for all $a, b \in A$, $\{a\} \neq \{b\} \iff a = b$.

Now assume for a contradiction that there is a bijection $g: A \to P(A)$.

Note that for all $a \in A$, $g(a) \subseteq A$, so it makes sense to ask whether $a$ is an element of $g(a)$ and we can define
$$B = \{a \in A : a \notin g(a)\} \subseteq A$$

Since $g$ is surjective, $B \subseteq \text{im}(g)$, i.e., $\exists a \in A$ such that $g(a) = B$. By definition of $B$, we see that
$$a \in B \iff g(a) \supseteq a$$
$$a \notin B \iff a \in g(a)$$

In either case we have a contradiction.

So, $\exists$ a bijection $g: A \to P(A)$.  

Remark: The proof is similar to the well-known "berber paradox".

There is a village where the barber cuts the hair of every person who does not cut their own hair. Who cuts the barber's hair?
A consequence of the above theorem is that we can build bigger and bigger sets:

\[ |\mathbb{N}| < |\mathbb{R}| < |\mathcal{P}(\mathbb{R})| < (\mathcal{P}(\mathcal{P}(\mathbb{R})))| < \cdots \]

Cantor’s theorem leads to a famous paradox in math: Let \( U \) be the set of all sets. Since \( \mathcal{P}(U) \) is a collection of sets, \( \mathcal{P}(U) \subseteq U \Rightarrow |\mathcal{P}(U)| \leq |U| \). But by Cantor’s theorem, \( |U| < |\mathcal{P}(U)| \).

Hence, there is no such thing as a set of all sets!

**Question:** Where does \( \mathcal{P}(\mathbb{N}) \) fit in (*) above?

Thus \( |\mathcal{P}(\mathbb{N})| = \aleph_0 \) (so \( |\mathcal{P}(\mathbb{N})| < |\mathbb{R}| \)).

We prove this via a series of lemmas.

First, we use the fact that any \( x \in [0, 1] \) has a binary expansion:

\[
\begin{align*}
x &= \left[0.a_0a_1a_2\ldots\right]_2 \\
&= \sum_{n=1}^{\infty} \frac{a_n}{2^n}
\end{align*}
\]

where \( a_n \in \{0, 1\} \) for all \( n \in \mathbb{N} \). If there is more than one representation (e.g., \( [0.111\ldots]_2 = [0.010101\ldots]_2 \)), we take the terminating expansion.

**Lemmas**

**Lemma 1:** Define a function

\[ f: [0, 1] \to \mathcal{P}(\mathbb{N}) \]

by \( f(x) = \{ n \in \mathbb{N} : a_n = 1 \} \) in the binary expansion \( x = [0.a_0a_1a_2\ldots]_2 \) \( x \subseteq \mathbb{N} \).

The \( f \) is injective, hence \( c \leq |\mathcal{P}(\mathbb{N})| \).

**Proof:** Take \( x, y \in [0, 1] \) such that \( f(x) = f(y) \).

Write \( x = [0.a_0a_1a_2\ldots] \) and \( y = [0.b_0b_1b_2\cdots] \).

Since \( f(x) = f(y) \), we have that...
\[ \forall n \in \mathbb{N} : a_n = 1^3 = 5 \neq n \in \mathbb{N} : b_n = 13 \]

Thus, \( a_n = 1 \Rightarrow b_n = 1 \). Then since \( a_n, b_n \in \{0, 1\} \forall n \in \mathbb{N} \), we also have that \( \forall n \in \mathbb{N}, \ a_n = 0 \Rightarrow b_n = 0 \).

Putting these together, \( a_n = b_n \ \forall n \in \mathbb{N} \), hence \( x = y \). This shows that \( f \) is injective, and thus 
\[ |\{C, \{1\}\}| = |\mathcal{P}(\mathbb{N})| \]

Now recall that the Cantor set \( C \) can be described as the set of \( x \in [0, 1] \) whose ternary expansion
\[ x = [0, a_1, a_2, \ldots]_3 = \sum_{n=1}^{\infty} \frac{a_n}{3^n} \]

has an \( \in \{0, 2\} \ \forall n \in \mathbb{N} \), and this expression is unique.

Lemma 2 Define the function
\[ g : \mathcal{P}(\mathbb{N}) \to C \]
by \( g(A) = \sum_{n=1}^{\infty} \frac{a_n}{3^n} \) where \( a_n = \begin{cases} 0 & \text{if } n \notin A \, \text{and} \\ 2 & \text{if } n \in A. \end{cases} \)

Then, \( g \) is bijective.

Proof: Injectivity: Take \( A, B \in \mathcal{P}(\mathbb{N}) \) such that \( g(A) = g(B) \). Then \( a_n = b_n \) \( \forall n \in \mathbb{N} \).

By uniqueness of the ternary expansion of elements of \( C \),
\[ \sum_{n=1}^{\infty} \frac{a_n}{3^n} = \sum_{n=1}^{\infty} \frac{b_n}{3^n} \Rightarrow a_n = b_n \ \forall n \in \mathbb{N}. \]

Thus, by definition of \( g \), we have
\[ n \in A \iff a_n = 2 \iff b_n = 2 \iff n \in B. \]
So \( A = B \) and \( g \) is injective.
Surjectivity: Take any $x \in C$. Write
\[ x = \sum_{n=1}^{\infty} \frac{a_n}{3^n} \]
with $a_n \in \{0, 2, 3\}$ for all $n \in \mathbb{N}$. Now define
\[ A = \{ n \in \mathbb{N} : a_n = 2 \} \subset \mathbb{N} \]
Then $A \in \mathcal{P}(\mathbb{N})$ and
\[ g(A) = \sum_{n=1}^{\infty} \frac{a_n}{3^n} = x. \]
So $g$ is surjective.

We conclude that $g$ is bijective. \qed

**Proof:** Recall we want to prove that
\[ \left| \mathcal{P}(\mathbb{N}) \right| = \left| [0, 1] \right|. \]

By Lemma 1
\[ \left| [0, 1] \right| \leq \left| \mathcal{P}(\mathbb{N}) \right|. \]

By Lemma 2 and since $C \subseteq [0, 1]$, we have
\[ \left| \mathcal{P}(\mathbb{N}) \right| = \left| C \right| \leq \left| [0, 1] \right|. \]

By Cantor–Schröder–Bernstein,
\[ \left| \mathcal{P}(\mathbb{N}) \right| = \left| C \right| = \left| [0, 1] \right|. \] \qed
Aside: The Continuum Hypthesis.

Question: We saw that $\mathbb{N} \leq \mathbb{R}$. Is there anything in between? More precisely, does there exist a set $A$ such that $\aleph_0 < \mathcal{P}(A) < \mathbb{R}$?

Stage answer:

Van (Gödel - Cohen): It is impossible to answer this question in our current axiomatic framework (ZFC).

More precisely, the continuum hypothesis cannot be proven or disproven in our current axiomatic system.

Continuum hypothesis: For any set $A$, if $\aleph_0 \leq |A| < \mathbb{R}$ then either $|A| = \aleph_0$ or $|A| = \mathbb{R}$.

Rud Gödel - Cohen: give a formal proof that it is impossible to give a formal proof of something. This is strange...

A result of their theorem is that we can add the CH to our axioms if we like, it's more a matter of whether or not we believe it.