

Cantor's Theorem

For a set S , define its *power set* (denoted $\mathcal{P}(S)$) to be the set whose members are the subsets of S . For example, if S is the two-element set $\{1, 2\}$, then $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Thus $\mathcal{P}(S)$ is always a set of sets.

If S is a finite set with n elements, then $\mathcal{P}(S)$ contains 2^n elements. (This is because to form a subset of S , we can go through the n elements, deciding for each whether to put it into the subset or leave it out—two choices. There are 2^n ways of making the n choices.) This holds even for $n = 0$; the power set of \emptyset is the one-element set $\{\emptyset\}$.

It is always true that $n < 2^n$, and therefore a finite set is always strictly smaller than its power set. Something analogous holds for all sets:

Cantor's Theorem (1873). A set never has the same cardinality as its power set. In fact, for any set S , there is no function from S onto its power set.

Proof: Consider any set S and any function f from S to $\mathcal{P}(S)$. We want to show that f is not onto $\mathcal{P}(S)$. For that purpose, it suffices to find some subset A of S that is *not* in the range of f .

Here it is:

$$A = \{x \in S \mid x \notin f(x)\}.$$

The definition of A makes sense; whenever x is in S , then $f(x)$ will be a subset of S , and it might or might not contain x itself.

At least $A \subseteq S$. It remains to verify that A is not in the range of f . That is, we need to be sure that for each x_0 in S , we have $A \neq f(x_0)$. We have by the construction of A ,

$$x_0 \in A \iff x_0 \notin f(x_0).$$

But this tells us that the two sets A and $f(x_0)$ differ in at least one way: one of the two contains x_0 and the other does not! \neg

Example: \mathcal{N} and $\mathcal{P}(\mathcal{N})$ do not have the same cardinality, so $\mathcal{P}(\mathcal{N})$ is uncountable. The above proof of Cantor's theorem, when we take S to be \mathcal{N} , is closely related to the proof on page 18 that the reals are uncountable.

For any non-empty set S , it is easy to find a function from $\mathcal{P}(S)$ onto S . (How?) So in a sense, we can "cover" S by $\mathcal{P}(S)$. Cantor's theorem tells us that we cannot, in this sense, cover $\mathcal{P}(S)$ by S . So there is a sense in which $\mathcal{P}(S)$ is larger than S , even when S is infinite.

We can iterate the power-set operation: $S, \mathcal{P}(S), \mathcal{P}(\mathcal{P}(S)), \dots$, obtaining larger and larger sets. There is no largest set.

H. B. Enderton