Proposition. If $S$ is a finite set, $A \subseteq S$ is a subset, then $A$ is finite with $|A| \leq |S|$. If in addition $|A| = |S|$, then $A = S$.

Proof. Since $S$ is finite, there is a bijection $f: S \to [m]$ for some $m \geq 0$. The map $f$ induces a bijective correspondence between $A$ and the image $f(A) \subseteq S$. So without loss of generality, we can assume $S = [m]$, and $A \subseteq [m]$.

Prove this by induction on $m$. If $m = 0$, $S = [0] = \emptyset$, so $A = \emptyset$. In general, if $A \subseteq [m]$, let $B = A \cap [m-1]$. Thus, by induction $B$ is finite with $|B| \leq m - 1$. If $m \not\in A$, then $A = B$, whence $|A| = |B|$, while if $m \in A$, then $A = B \cup \{m\}$ and $A \cap \{m\} = \emptyset$, so $|A| = |B| + 1$. In either case, $|A| \leq m$, and we can have equality only if $|B| = m - 1$ and $m \in A$.

□

Corollary. If $S$ is a set, and $A \subseteq S$ is a subset such that $A$ is infinite, then $S$ is also infinite.

Corollary. If $S$ is a finite set, and $A \subsetneq S$ is a proper subset, then there does not exist a bijection between $A$ and $S$.

Turning this around, this says that if $S$ is a set which can be put into a bijective correspondence with a some proper subset $A$, then $S$ must be infinite.

A set is countably infinite if there is a bijection $f: A \to \mathbb{N}$; if infinite and but no such bijection, it is not countably infinite.

Example: $\mathbb{Z}$.

There are non-countably infinite sets. The easiest examples are power sets of any infinite set.

Here’s a simpler example, which gives an example of a non-countably infinite set, namely the power set of $\mathbb{N}$.

Proposition. Let $S$ be any set, and let $T = \mathcal{P}S$ be the power set of $S$. Then there does not exist a bijection between $S$ and $T$.

Proof. Suppose there is a bijection $f: S \to T$; we will derive a contradiction. The bijection associates to each element $x \in S$ a subset $f(x) = A_x \subseteq S$. We define a new subset $B \subseteq S$, by

$$B = \{ x \in S \mid x \not\in A_x \}.$$

Since $B \in T$ and $f$ is a bijection, there exists $y \in S$ such that $A_y = B$. But now consider the question of whether $y$ is in this set. If $y \in B$, then by definition $y \not\in A_y$, which is impossible since $A_y = B$. But if $y \not\in B$, then by definition $y \in A_y$, which is again impossible since $A_y = B$. We have found a contradiction, so no bijection $f$ exists. □
Applied to finite sets, this gives a proof that \( n < 2^n \) for all \( n \in \mathbb{N} \cup \{0\} \).

Applied to \( S = \mathbb{N} \), this says that \( T = \mathcal{P}\mathbb{N} \) is not countable!

Remark: this actually proves that there is no surjection \( S \to \mathcal{P}S \) for any set \( S \).

**Theorem** (Cantor).  \( \mathbb{R} \) is not countably infinite.

**Proof of Cantor’s theorem.** Suppose given a bijection \( f : \mathbb{N} \to \mathbb{R} \). Define a number \( x \in \mathbb{R} \) as follows. It will have a decimal expansion of the form

\[
0.a_1a_2a_3\ldots
\]

where each \( a_i \in \{0, 1, \ldots, 9\} \). We define it by picking \( a_n \) to be different than the \( n \)th digit after the decimal point of \( f(n) \). To be explicit:

- If \( f(n) = \pm m.b_1b_2b_3\ldots \), with \( m \in \mathbb{N} \cup \{0\} \) and \( b_i \in \{0, 1, \ldots, 9\} \), set

\[
a_i := \begin{cases} 
1 & \text{if } b_i \in \{0, 2, \ldots, 9\}, \\
2 & \text{if } b_i = 1.
\end{cases}
\]

Then for all \( n \in \mathbb{N} \), \( f(n) \neq x \). Thus \( x \) is not in the image of \( f \), contradicting the hypothesis that \( f \) is a bijection. \( \square \)

Remark: you need to be a little careful with decimal expansions, because some numbers have two decimal expansions, e.g., 0.1234999… is the same as 0.1235000…. I made sure that \( x \) would never be such a number, so the issue won’t be a problem.

**More examples of countable infinite.** \( \mathbb{Z} \times \mathbb{Z}, \mathbb{N} \times \mathbb{N} \) are countably infinite.

For instance, \( f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \) by \( f(a,b) = 2^{a-1}(2b-1) \).

\( \mathbb{Q} \). This is countably infinite.

A countable union of countable sets is countable.

An **algebraic number** is an \( a \in \mathbb{R} \) which is the root of some polynomial \( f(x) = \sum c_i x^i \) with rational coefficients. E.g., \( \sqrt{2} \) is algebraic. The set \( A \) of algebraic numbers is countably infinite. As a consequence, we learn that there must exist non-algebraic numbers: \( \pi \) and \( e \) are examples, but they are difficult to prove.

The set of all functions \( F(\mathbb{N}, S) = \{ f : \mathbb{N} \to S \} \) is not countably infinite as long as \( S \) has at least two different elements. This is another example of the Cantor argument.

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, IL

E-mail address: rezk@math.uiuc.edu