Countable sets & Cantor's diagonal argument

April 6th, 2021

Countable sets – 1

Notation

In what follows, we set $\aleph_0 := |\mathbb{N}|$ (pronounced *aleph nought*).

Definition

A set E is countable if either E is finite or $|E| = \aleph_0$.

Countable sets – 2

Proposition

1. $|\mathbb{N} \setminus \{0\}| = \aleph_0$
2. $|\{n \in \mathbb{N} \ : \ n \equiv 0 \mod 2\}| = \aleph_0$
3. $|\mathbb{N} \times \mathbb{N}| = \aleph_0$

Countable sets – 2

Proposition

1. $|\mathbb{N} \setminus \{0\}| = \aleph_0$
2. $|\{n \in \mathbb{N} \; : \; n \equiv 0 \mod 2\}| = \aleph_0$
3. $|\mathbb{N} \times \mathbb{N}| = \aleph_0$

Proof.

1. The function $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ defined by $f(n) = n + 1$ is bijective with inverse $f^{-1} : \mathbb{N} \setminus \{0\} \to \mathbb{N}$ defined by $f^{-1}(n) = n - 1$.
2. The function $f : \mathbb{N} \to \{n \in \mathbb{N} \; : \; n \equiv 0 \mod 2\}$ defined by $f(n) = 2n$ is bijective.
3. Define $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by $f(a, b) = 2^a 3^b$.
   Then f is injective by uniqueness of the prime decomposition. Thus $|\mathbb{N} \times \mathbb{N}| \leq \aleph_0$.
   Besides $\{0\} \times \mathbb{N} \subset \mathbb{N} \times \mathbb{N}$, thus $\aleph_0 = |\{0\} \times \mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$.
   Hence $|\mathbb{N} \times \mathbb{N}| = \aleph_0$ by Cantor–Schröder–Bernstein theorem. ∎

Countable sets – 3

Proposition

If $S \subset \mathbb{N}$ is infinite then $|S| = \aleph_0$.

Countable sets – 3

Proposition

If $S \subset \mathbb{N}$ is infinite then $|S| = \aleph_0$.

Proof. Let's define the function $f : \mathbb{N} \to S$ by induction as follows.
Set $f(0) = \min S$ *(which is well-defined by the well-ordering principle since $S \neq \varnothing$ as it is infinite)*.
And then, assuming that $f(n)$ is already defined, we set $f(n+1) = \min\{k \in S : k > f(n)\}$ *(which is well-defined by the well-ordering principle: the involved set is non-empty since otherwise S would be finite)*.
It is easy to check that f is injective (note that $\forall n \in \mathbb{N},\ f(n+1) > f(n)$), therefore $\aleph_0 \leq |S|$.

But since $S \subset \mathbb{N}$, we also have $|S| \leq \aleph_0$.

Thus, by Cantor–Schröder–Bernstein theorem, $|S| = \aleph_0$. ∎

Countable sets – 4

Proposition

A set E is countable if and only if $|E| \leq \aleph_0$ (i.e. there exists an injection $f : E \to \mathbb{N}$), otherwise stated E is countable if and only if there exists a bijection between E and a subset of $\mathbb{N}$.

Countable sets – 4

Proposition

A set E is countable if and only if $|E| \leq \aleph_0$ (i.e. there exists an injection $f : E \to \mathbb{N}$), otherwise stated E is countable if and only if there exists a bijection between E and a subset of $\mathbb{N}$.

Proof.

$\Rightarrow$ Assume that E is countable.

- Either E is finite and then there exists $n \in \mathbb{N}$ and a bijection $g : \{k \in \mathbb{N} : k < n\} \to E$.
  We define $f : E \to \mathbb{N}$ by $f(x) = g^{-1}(x)$ *(which is well-defined since* $\{k \in \mathbb{N} : k < n\} \subset \mathbb{N}$*)*.
  And f is an injection since g^{-1} is.
- Or $|E| = \aleph_0$, i.e. there exists a bijection $f : E \to \mathbb{N}$.

$\Leftarrow$ Assume there exists an injection $f : E \to \mathbb{N}$.
Assume that E is infinite. Then $|E| = |f(E)| = \aleph_0$.
Thus either E is finite or $|E| = \aleph_0$. In both cases E is countable. ∎

Countable sets – 5

Theorem

A countable union of countable sets is countable,
i.e. if I is countable and if for every $i \in I$, E_i is countable then $\bigcup_{i \in I} E_i$ is countable.

Countable sets – 5

Theorem

A countable union of countable sets is countable,
i.e. if I is countable and if for every $i \in I$, E_i is countable then $\bigcup_{i\in I} E_i$ is countable.

Proof.
WLOG we may now assume that $I \subset \mathbb{N}$.
Let $i \in I$. Since E_i is countable, there exists an injection $f_i : E_i \to \mathbb{N}$[1].
We define $\varphi : \bigcup_{i\in I} E_i \to \mathbb{N}\times\mathbb{N}$ by $\varphi(x) = (n, f_n(x))$ where $n = \min\{i \in I \ : \ x \in E_i\}$ *(which exists by the well-ordering principle)*.
It is not difficult to check that φ is injective.
Therefore $\bigcup_{i\in I} E_i$ is countable. ∎

[1] We use the axiom of countable choice here.

Countable sets – 6

Theorem

If E is an infinite set then there exists $T \subset E$ such that $|T| = \aleph_0$, i.e. $\aleph_0$ is the least infinite cardinal.

Countable sets – 6

Theorem

If E is an infinite set then there exists $T \subset E$ such that $|T| = \aleph_0$, i.e. $\aleph_0$ is the least infinite cardinal.

Proof.
For $n \in \mathbb{N}$, set $E_n = \{S \in \mathcal{P}(E) \ : \ |S| = n\}$.
Since E is infinite, it contains a subset of cardinal n, therefore $E_n \neq \varnothing$.
So for every $n \in \mathbb{N}$, we can pick[2] $S_n \in E_n$.
Then $T := \bigcup_{n\in\mathbb{N}} S_n$ is countable as a countable union of countable sets.
Besides, $\forall n \in \mathbb{N}$, $S_n \subset T$ and $|S_n| = n$.
Therefore T is infinite since for every $n \in \mathbb{N}$ it contains a subset of cardinal n.
Thus $|T| = \aleph_0$ as an infinite countable set. ∎

[2] We use the axiom of countable choice here.

Countable sets – 7

Theorem

$|\mathbb{Z}| = \aleph_0$

Countable sets – 7

Theorem

$|\mathbb{Z}| = \aleph_0$

Proof 1. Since $\mathbb{N} \subset \mathbb{Z}$, we have $|\mathbb{N}| \leq |\mathbb{Z}|$.

Define $f : \mathbb{Z} \to \mathbb{N}$ by $f(n) = \begin{cases} 2^n & \text{if } n \geq 0 \\ 3^{-n} & \text{if } n < 0 \end{cases}$.

Then f is injective by uniqueness of the prime factorization. Therefore $|\mathbb{Z}| \leq |\mathbb{N}|$.

Hence $|\mathbb{Z}| = |\mathbb{N}|$ by Cantor–Schröder–Bernstein theorem. ■

Proof 2.

Define $f : \mathbb{Z} \to \mathbb{N}$ by $f(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -(2n+1) & \text{if } n < 0 \end{cases}$.

Then f is bijective with inverse $f^{-1}(m) = \begin{cases} k & \text{if } \exists k \in \mathbb{N},\ m = 2k \\ -k-1 & \text{if } \exists k \in \mathbb{N},\ m = 2k+1 \end{cases}$.

Therefore $|\mathbb{Z}| = |\mathbb{N}|$. ■

Countable sets – 8

Theorem

$|\mathbb{Q}| = \aleph_0$

Countable sets – 8

Theorem

$|\mathbb{Q}| = \aleph_0$

Proof 1. Note that $\mathbb{N} \subset \mathbb{Q}$, therefore $\aleph_0 \leq |\mathbb{Q}|$.
Define $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ by $f\left(\frac{a}{b}\right) = (a, b)$ where $\frac{a}{b}$ is in lowest form.
Then f is injective and thus $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}|$. Since $|\mathbb{Z}| = |\mathbb{N}|$, we get $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$.
We conclude using Cantor–Schröder–Bernstein theorem. ■

Proof 2. Note that $\mathbb{N} \subset \mathbb{Q}$, therefore $\aleph_0 \leq |\mathbb{Q}|$.
Moreover $f : \mathbb{Z} \times \mathbb{N} \setminus \{0\} \to \mathbb{Q}$ defined by $f(a, b) = \frac{a}{b}$ is surjective. Thus $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N} \setminus \{0\}|$.
Since $|\mathbb{Z}| = |\mathbb{N}|$ and $|\mathbb{N} \setminus \{0\}| = |\mathbb{N}|$, we get $|\mathbb{Z} \times \mathbb{N} \setminus \{0\}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$.
We conclude using Cantor–Schröder–Bernstein theorem. ■

Proof 3. Note that $\mathbb{N} \subset \mathbb{Q}$, therefore $\aleph_0 \leq |\mathbb{Q}|$.
Since $\mathbb{Q} = \bigcup_{(a,b) \in \mathbb{Z} \times \mathbb{N} \setminus \{0\}} \left\{ \frac{a}{b} \right\}$, $\mathbb{Q}$ is countable as a countable union of countable sets. So $|\mathbb{Q}| \leq \aleph_0$.
We conclude using Cantor–Schröder–Bernstein theorem. ■

Cantor's diagonal argument – 1

Theorem: $\mathbb{R}$ is not countable (Cantor 1874, the proof below dates back to 1891)

$\aleph_0 < |\mathbb{R}|$

Cantor's diagonal argument – 1

Theorem: $\mathbb{R}$ is not countable (Cantor 1874, the proof below dates back to 1891)

$\aleph_0 < |\mathbb{R}|$

$$\begin{array}{rcl} f(0) & = & \color{red}{a_{00}} \,.\, a_{01}\ a_{02}\ a_{03}\ a_{04}\ a_{05}\ \dots \\ f(1) & = & a_{10} \,.\, \color{red}{a_{11}}\ a_{12}\ a_{13}\ a_{14}\ a_{15}\ \dots \\ f(2) & = & a_{20} \,.\, a_{21}\ \color{red}{a_{22}}\ a_{23}\ a_{24}\ a_{25}\ \dots \\ f(3) & = & a_{30} \,.\, a_{31}\ a_{32}\ \color{red}{a_{33}}\ a_{34}\ a_{35}\ \dots \\ f(4) & = & a_{40} \,.\, a_{41}\ a_{42}\ a_{43}\ \color{red}{a_{44}}\ a_{45}\ \dots \\ \vdots & & \qquad\qquad\quad \vdots \end{array}$$

Cantor's diagonal argument – 1

Theorem: $\mathbb{R}$ is not countable (Cantor 1874, the proof below dates back to 1891)

$\aleph_0 < |\mathbb{R}|$

Proof. We are going to prove that there is no surjection $\mathbb{N} \to \mathbb{R}$ (and hence no such bijection).

Let $f : \mathbb{N} \to \mathbb{R}$ be a function. Given $n \in \mathbb{N}$, we know that $f(n)$ has a unique proper decimal expansion $f(n) = \sum_{k=0}^{+\infty} a_{nk} 10^{-k}$ where $a_{n0} \in \mathbb{Z}$ and $a_{nk} \in \{0, 1, \dots, 9\}$ for $k \geq 1$, i.e.

$$\begin{array}{l} f(0) = \color{red}{a_{00}} \,.\, a_{01}\ a_{02}\ a_{03}\ a_{04}\ a_{05}\ \dots \\ f(1) = a_{10} \,.\, \color{red}{a_{11}}\ a_{12}\ a_{13}\ a_{14}\ a_{15}\ \dots \\ f(2) = a_{20} \,.\, a_{21}\ \color{red}{a_{22}}\ a_{23}\ a_{24}\ a_{25}\ \dots \\ f(3) = a_{30} \,.\, a_{31}\ a_{32}\ \color{red}{a_{33}}\ a_{34}\ a_{35}\ \dots \\ f(4) = a_{40} \,.\, a_{41}\ a_{42}\ a_{43}\ \color{red}{a_{44}}\ a_{45}\ \dots \\ \quad\vdots \qquad\qquad\qquad\quad \vdots \end{array}$$

Given $k \in \mathbb{N}$, we set $b_k = \begin{cases} 1 & \text{if } a_{kk} = 0 \\ 0 & \text{otherwise} \end{cases}$.

Then $b = \sum_{k=0}^{+\infty} b_k 10^{-k}$ is a real number written with its unique proper decimal expansion.

Note that for every $n \in \mathbb{N}$, $b \neq f(n)$ since $b_n \neq a_{nn}$ (we use the uniqueness of the proper decimal expansion).

Therefore $b \notin \operatorname{Im}(f)$ and f is not surjective. ∎

Cantor's diagonal argument – 2

Cantor's theorem

Given a set E, $|E| < |\mathcal{P}(E)|$.

Cantor's diagonal argument – 2

Cantor's theorem

Given a set E, $|E| < |\mathcal{P}(E)|$.

Proof. *We are going to use Cantor's diagonal argument again.*
First, note that $g : E \to \mathcal{P}(E)$ defined by $g(x) = \{x\}$ is injective, therefore $|E| \leq |\mathcal{P}(E)|$.

We are going to prove that there is no surjection $E \to \mathcal{P}(E)$ *(and hence no such bijection)*.
Let $f : E \to \mathcal{P}(E)$ be a function. Define $S = \{x \in E : x \notin f(x)\}$.
Let $x \in E$.

- If $x \in f(x)$ then $x \notin S$.
- Otherwise, if $x \notin f(x)$ then $x \in S$.

Therefore $f(x) \neq S$ since one contains x but not the other one.
Thus $S \notin \operatorname{Im}(f)$ and f is not surjective. ■

Cantor's diagonal argument – 2

Cantor's theorem

Given a set E, $|E| < |\mathcal{P}(E)|$.

Proof. *We are going to use Cantor's diagonal argument again.*
First, note that $g : E \to \mathcal{P}(E)$ defined by $g(x) = \{x\}$ is injective, therefore $|E| \leq |\mathcal{P}(E)|$.

We are going to prove that there is no surjection $E \to \mathcal{P}(E)$ *(and hence no such bijection)*.
Let $f : E \to \mathcal{P}(E)$ be a function. Define $S = \{x \in E : x \notin f(x)\}$.
Let $x \in E$.

- If $x \in f(x)$ then $x \notin S$.
- Otherwise, if $x \notin f(x)$ then $x \in S$.

Therefore $f(x) \neq S$ since one contains x but not the other one.
Thus $S \notin \mathrm{Im}(f)$ and f is not surjective. ∎

Remark

There is no greatest cardinal.

$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

We already know that $|\mathbb{N}| < |\mathbb{R}|$ and that $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$. Actually $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Theorem

$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

We already know that $|\mathbb{N}| < |\mathbb{R}|$ and that $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$. Actually $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

Theorem

$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

Proof.
Define $f : \mathcal{P}(\mathbb{N}) \to \mathbb{R}$ by $f(S) = \sum_{n \in S} 10^{-n}$.
Then f is injective by uniqueness of the proper decimal expansion. Thus $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$.

Define $g : \mathbb{R} \to \mathcal{P}(\mathbb{Q})$ by $g(x) = \{q \in \mathbb{Q} : q < x\}$.
Then g is injective. Indeed, let $x, y \in \mathbb{R}$ be such that $x < y$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, there exists $q \in \mathbb{Q}$ such that $x < q < y$. So $q \notin g(x)$ but $q \in g(y)$. Therefore $g(x) \neq g(y)$.
Hence $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$ *(prove the last equality using that* $|\mathbb{Q}| = |\mathbb{N}|$*)*.

We conclude thanks to Cantor–Schröder–Bernstein theorem. ∎

There is no set of all sets

Theorem

There is no set containing all sets.

There is no set of all sets

Theorem

There is no set containing all sets.

Proof. Assume that such a set V exists.
Then the powerset $\mathcal{P}(V)$ exists too and $\mathcal{P}(V) \subset V$ by definition of V.
Therefore $|\mathcal{P}(V)| \leq |V|$, but $|V| < |\mathcal{P}(V)|$ by Cantor's theorem. Hence a contradiction. ∎

There is no set of all sets

Theorem

There is no set containing all sets.

Proof. Assume that such a set V exists.
Then the powerset $\mathcal{P}(V)$ exists too and $\mathcal{P}(V) \subset V$ by definition of V.
Therefore $|\mathcal{P}(V)| \leq |V|$, but $|V| < |\mathcal{P}(V)|$ by Cantor's theorem. Hence a contradiction. ∎

We may similarly prove that there is no set containing all finite sets, or even all singletons.

Theorem

There is no set containing all singletons.

There is no set of all sets

Theorem

There is no set containing all sets.

Proof. Assume that such a set V exists.
Then the powerset $\mathcal{P}(V)$ exists too and $\mathcal{P}(V) \subset V$ by definition of V.
Therefore $|\mathcal{P}(V)| \leq |V|$, but $|V| < |\mathcal{P}(V)|$ by Cantor's theorem. Hence a contradiction. ■

We may similarly prove that there is no set containing all finite sets, or even all singletons.

Theorem

There is no set containing all singletons.

Proof. Assume that the set S of all singletons exists.
Define $f : \mathcal{P}(S) \to S$ by $f(x) = \{x\}$ (which is well-defined).
Since f is one-to-one, we get that $|\mathcal{P}(S)| \leq |S|$.
Which contradicts $|S| < |\mathcal{P}(S)|$ (Cantor's theorem). ■