Chapter 10: Cardinality

CS1231S Discrete Structures

Wong Tin Lok

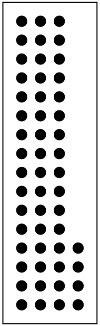
National University of Singapore

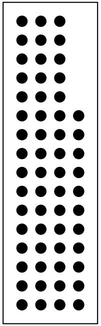
2021/22 Semester 1

> According to [Brouwer's] view and reading of history, classical logic was abstracted from the mathematics of finite sets and their subsets. [. . .] Forgetful of this limited origin, one afterwards mistook that logic for something above and prior to all mathematics, and finally applied it, without justification, to the mathematics of infinite sets. This is the Fall and original sin of set-theory, for which it is justly punished by the antinomies.
>
> Weyl 1946

The number of elements in a set

Late at night, Tin Lok walks in to the Hilbert Hotel to see whether there is a vacant room for him. Unfortunately, the hotel is already full. Nevertheless, the clerk is able to make a special arrangement for him. The clerk says, “Let me ask the guest in Room 1 to move to Room 2, the guest in Room 2 to move to Room 3, etc. Then you can check in to Room 1.” Fortunately, the Hilbert Hotel has infinitely many rooms!





Zoom poll

Recap

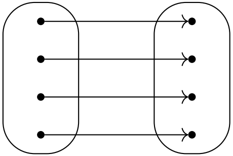
Late at night, Tin Lok walks in to the Hilbert Hotel to see whether there is a vacant room for him. Unfortunately, the hotel is already full. Nevertheless, the clerk is able to make a special arrangement for him. The clerk says, "Let me ask the guest in Room 1 to move to Room 2, the guest in Room 2 to move to Room 3, etc. Then you can check in to Room 1." Fortunately, the Hilbert Hotel has infinitely many rooms!

Definition 9.3.6 Let $f\colon A \to B$.

(1) f is *surjective* if $\forall y \in B \ \exists x \in A \ \ y = f(x)$.
(2) f is *injective* if $\forall x_1, x_2 \in A \ \ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.
(3) f is *bijective* if it is both surjective and injective, i.e., $\forall y \in B \ \exists! x \in A \ \ y = f(x)$.

Definition 9.3.14 Let $f\colon A \to B$. Then $g\colon B \to A$ is an *inverse* of f if

$$\forall x \in A \ \forall y \in B \ \big(y = f(x) \ \Leftrightarrow \ x = g(y) \big).$$



Theorem 9.3.19 A function is bijective if and only if it has an inverse.

Next

What surjections and injections tell us about cardinality

Injections and # elements

Defn 9.3.6(2). $f\colon A \to B$ is *injective* if $\forall x_1, x_2 \in A \ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

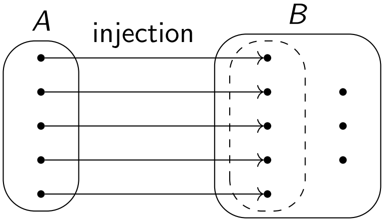
Theorem 10.1.1 (Pigeonhole Principle)

Let A and B be finite sets. If there is an injection $f\colon A \to B$, then $|A| \leqslant |B|$.

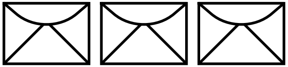
Contrapositive. Let $m, n \in \mathbb{Z}^+$ with $m > n$. If m letters are put into n pigeonholes, then there must be (at least) one pigeonhole with (at least) two letters.

Proof

1. Note that A is finite. Suppose $A = \{a_1, a_2, \ldots, a_m\}$, where $m = |A|$.
2. The injectivity of f tells us that, if $a_i \neq a_j$, then $f(a_i) \neq f(a_j)$.
3. So $f(a_1), f(a_2), \ldots, f(a_m)$ are m different elements of B.
4. This shows $|B| \geqslant m = |A|$. □



Injectivity means that no two arrows point to the same dot.



https://tex.stackexchange.com/a/128300

Surjections and # elements

Defn 9.3.6(1). $f: A \to B$ is *surjective* if $\forall y \in B \;\; \exists x \in A \;\; y = f(x)$.

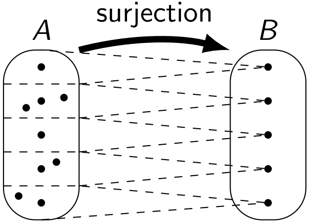
Theorem 10.1.2 (Dual Pigeonhole Principle)

Let A and B be finite sets. If there is a surjection $f: A \to B$, then $|A| \geqslant |B|$.

Contrapositive. Let $m, n \in \mathbb{Z}^+$ with $m < n$. If m letters are put into n pigeonholes, then there must be (at least) one pigeonhole with no letter.

Proof

1. Note that B is finite. Suppose $B = \{b_1, b_2, \ldots, b_n\}$, where $n = |B|$.
2. For each b_i, use the surjectivity of f to find $a_i \in A$ such that $f(a_i) = b_i$.
3. If $b_i \neq b_j$, then $f(a_i) \neq f(a_j)$, and so $a_i \neq a_j$ because f is a function.
4. So $a_1, a_2, \ldots, a_n$ are n different elements of A.
5. This shows $|A| \geqslant n = |B|$. $\square$



Surjectivity means that any dot on the right has an arrow pointing to it.

https://tex.stackexchange.com/a/128300

Checkpoint

Let A, B be finite sets.

Theorem 10.1.1 (Pigeonhole Principle)

If there is an injection $A \to B$, then $|A| \leqslant |B|$.

Theorem 10.1.2 (Dual Pigeonhole Principle)

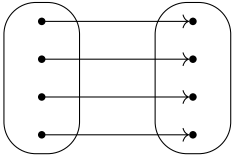
If there is a surjection $A \to B$, then $|A| \geqslant |B|$.

Theorem 10.1.3

There is a bijection $A \to B$ if and only if $|A| = |B|$.

Proof sketch

1. $(\Rightarrow)$ This follows from the two Pigeonhole Principles.
2. $(\Leftarrow)$ If $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$, then the function $f\colon A \to B$ satisfying $f(a_i) = b_i$ for all i is a bijection. $\square$



- The number of elements in *finite* sets can be compared using sur-/in-/bijections!
- Why not use them also for *infinite* sets?

Taking away some elements

Let A, B, C be sets.

Definition 10.2.1 (Cantor)

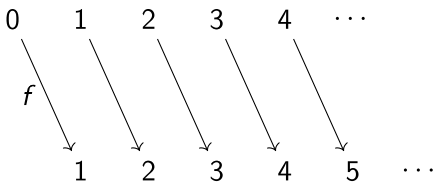
A is said to have the *same cardinality* as B if there is a bijection $A \to B$. In this case, we write $|A| = |B|$.

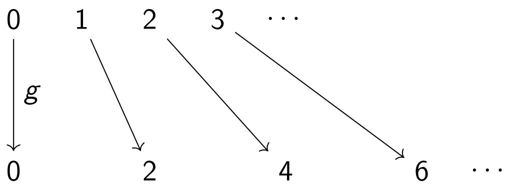
Note 10.2.2. We defined what $|A| = |B|$ means without defining what $|A|$ and $|B|$ mean.

Example 10.3.3

(1) $|\mathbb{Z}_{\geqslant 0}| = |\mathbb{Z}_{\geqslant 0} \setminus \{0\}|$ because the function $f\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0} \setminus \{0\}$ satisfying $f(x) = x + 1$ for all $x \in \mathbb{Z}_{\geqslant 0}$ is a bijection.

(2) $|\mathbb{Z}_{\geqslant 0}| = |\mathbb{Z}_{\geqslant 0} \setminus \{1, 3, 5, \dots\}|$ because the function $g\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0} \setminus \{1, 3, 5, \dots\}$ satisfying $g(x) = 2x$ for all $x \in \mathbb{Z}_{\geqslant 0}$ is a bijection.





Reflexivity

Let A, B, C be sets.

Definition 10.2.1 (Cantor)

A is said to have the *same cardinality* as B if there is a bijection $A \to B$. In this case, we write $|A| = |B|$.

Note 10.2.2. We defined what $|A| = |B|$ means without defining what $|A|$ and $|B|$ mean.

Proposition 10.2.3(1)

$|A| = |A|$.

Definition 7.2.5. $\mathrm{id}_A \colon A \to A$ that satisfies $\mathrm{id}_A(x) = x$ for all $x \in A$.

Proof

It suffices to show that id_A is a bijection $A \to A$.

1. id_A is injective because if $x_1, x_2 \in A$ such that $\mathrm{id}_A(x_1) = \mathrm{id}_A(x_2)$, then $x_1 = x_2$.
2. id_A is surjective because given any $x \in A$, we have $\mathrm{id}_A(x) = x$. $\square$

Definition 9.3.6. Let $f \colon A \to B$.

(1) f is *surjective* or *onto* if $\forall y \in B\ \exists x \in A\ (y = f(x))$.

(2) f is *injective* or *one-to-one* if $\forall x_1, x_2 \in A\ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$.

(3) f is *bijective* if it is surjective and injective.

Symmetry

Let A, B, C be sets.

Definition 10.2.1 (Cantor)

A is said to have the *same cardinality* as B if there is a bijection $A \to B$. In this case, we write $|A| = |B|$.

Theorem 9.3.19. A function is bijective if and only if it has an inverse.

Proposition 10.2.3(2)

If $|A| = |B|$, then $|B| = |A|$.

Definition 9.3.14. Let $f\colon A \to B$. Then $g\colon B \to A$ is an *inverse* of f if

$$\forall x \in A \ \forall y \in B \ \big(y = f(x) \ \Leftrightarrow \ x = g(y)\big).$$

Proof

1. Suppose $|A| = |B|$.
2. Use the definition of same-cardinality to find a bijection $f\colon A \to B$.
3. Then Theorem 9.3.19 gives us an inverse of f; call it g.
4. By the definition of inverses, for all $x \in A$ and all $y \in B$,
$$y = f(x) \quad \Leftrightarrow \quad x = g(y).$$
5. This tells us that f is an inverse of g in view the definition of inverses.
6. Thus g is a bijection $B \to A$ by Theorem 9.3.19.
7. This shows $|B| = |A|$. $\square$

Transitivity

Let A, B, C be sets.

Definition 10.2.1 (Cantor)

A is said to have the *same cardinality* as B if there is a bijection $A \to B$. In this case, we write $|A| = |B|$.

Theorem 9.3.19. A function is bijective if and only if it has an inverse.

Proposition 10.2.3(3)

If $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$.

Tutorial 7 Question 8. $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ for all bijections $f : A \to B$ and all bijections $g : B \to C$.

Proof

1. Suppose $|A| = |B|$ and $|B| = |C|$.
2. Use the definition of same-cardinality to find a bijection $f : A \to B$ and a bijection $g : B \to C$.
3. Then Tutorial 7 Question 8 tells us $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
4. In particular, this says $g \circ f$ has an inverse.
5. So $g \circ f$ is a bijection $A \to C$ by Theorem 9.3.19.
6. Hence $|A| = |C|$. $\square$

Checkpoint

Let A, B, C be sets.

Definition 10.2.1 (Cantor)

A is said to have the *same cardinality* as B if there is a bijection $A \to B$. In this case, we write $|A| = |B|$.

Proposition 10.2.3

(1) $|A| = |A|$. (reflexivity)

(2) If $|A| = |B|$, then $|B| = |A|$. (symmetry)

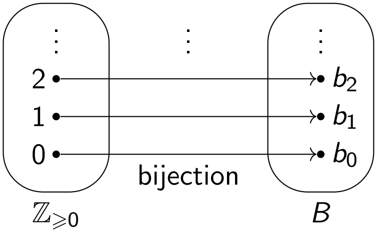
(3) If $|A| = |B|$ and $|B| = |C|$, then $|A| = |C|$. (transitivity)

No one shall be able to drive us from the paradise that Cantor created for us. David Hilbert

Next

sets that have the same cardinality as $\mathbb{Z}_{\geqslant 0}$

Countability



Definition 10.3.1 (Cantor)

A set is *countable* if it is finite or it has the same cardinality as $\mathbb{Z}_{\geqslant 0}$.

Note 10.3.2

Some authors allow only infinite sets to be countable.

Example 10.3.3

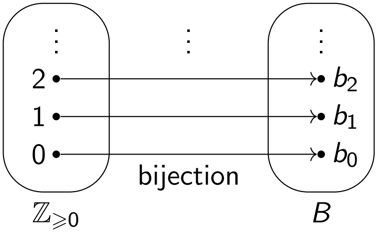
(1) $|\mathbb{Z}_{\geqslant 0}| = |\mathbb{Z}_{\geqslant 0} \setminus \{0\}|$ because the function $f\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0} \setminus \{0\}$ satisfying $f(x) = x + 1$ for all $x \in \mathbb{Z}_{\geqslant 0}$ is a bijection.

So $\mathbb{Z}_{\geqslant 0} \setminus \{0\} = \{1, 2, 3, \dots\}$ is countable.

(2) $|\mathbb{Z}_{\geqslant 0}| = |\mathbb{Z}_{\geqslant 0} \setminus \{1, 3, 5, \dots\}|$ because the function $g\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0} \setminus \{1, 3, 5, \dots\}$ satisfying $g(x) = 2x$ for all $x \in \mathbb{Z}_{\geqslant 0}$ is a bijection.

So $\mathbb{Z}_{\geqslant 0} \setminus \{1, 3, 5, \dots\} = \{0, 2, 4, \dots\}$ is countable.

Countability via sequences



Definition 10.3.1 (Cantor)

A set is *countable* if it is finite or it has the same cardinality as $\mathbb{Z}_{\geqslant 0}$.

Note 10.3.4

An infinite set B is countable if and only if
there is a sequence $b_0, b_1, b_2, \ldots \in B$ in which
every element of B appears exactly once.

Justification via Remark 9.1.1

function $f : \mathbb{Z}_{\geqslant 0} \to B$	sequence of elements of B
$f(0), f(1), f(2), \ldots$	$b_0, b_1, b_2, \ldots$
(surjectivity) $\forall b \in B \ \exists i \in \mathbb{Z}_{\geqslant 0} \ \ b = f(i)$	Every $b \in B$ appears at least once.
(injectivity) $\forall i, j \in \mathbb{Z}_{\geqslant 0} \ \ \big(f(i) = f(j) \Rightarrow i = j\big)$	Every $b \in B$ appears at most once.

Sequences with repetition

Note 10.3.4. An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \ldots \in B$ in which every element of B appears exactly once.

$b_1, b_2, \cancel{a_1}, b_3, \cancel{a_0}, b_1, b_2, b_0, \ldots$

$\rightsquigarrow b_1, b_2, b_3, \cancel{b_1}, \cancel{b_2}, b_0 \ldots$

$\rightsquigarrow b_1, b_2, b_3, b_0, \ldots$

Lemma 10.3.5

An infinite set B is countable if and only if

there is a sequence $c_0, c_1, c_2, \ldots$ in which every element of B appears.

Proof

1. ("Only if") This follows directly from Note 10.3.4.
2. ("If")
    - 2.1. Let $c_0, c_1, c_2, \ldots$ be a sequence in which every element of B appears.
    - 2.2. Remove those terms in the sequence that are not in B.
    - 2.3. If an element of B appears more than once, then remove all but the first appearance.
    - 2.4. The result is a sequence in which every element of B appears exactly once.
    - 2.5. So B is countable. $\square$

Exercise 10.4.4

> Note 10.3.4. An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \ldots \in B$ in which every element of B appears exactly once.

Which of the following sets is/are countable?

(1) $\mathbb{Z}$ ✓ Every element of $\mathbb{Z}$ appears exactly once in $0, 1, -1, 2, -2, 3, -3, \ldots$.

(2) $\mathbb{Q}$ ✓

(3) $\mathbb{R}$ ✗

(4) $\mathbb{C}$ ✗

(5) the set of all finite sets of integers ✓

(6) the set of all strings over $\{s, u\}$ ✓

(7) the set of all (infinite) sequences over $\{0, 1\}$ ✗

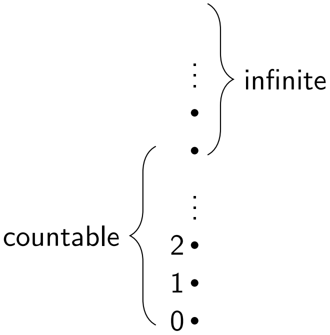
(8) the set of all functions $A \to B$ where A, B are finite sets of integers ✓

(9) the set of all computer programs ✓

> Proofs will appear in the notes, or in the tutorial.

Zoom poll

Countable cardinalities are the smallest cardinalities



Note 10.3.4. An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \ldots \in B$ in which every element of B appears exactly once.

Proposition 10.3.6

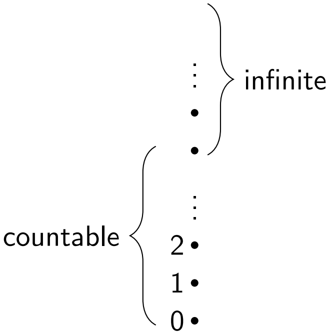
Any subset A of a countable set B is countable.

Proof

1. If A is finite, then A is countable by definition.
2. So suppose A is infinite.
   - 2.1. Then B is infinite too as $A \subseteq B$.
   - 2.2. Use the countability of B to find a sequence $b_0, b_1, b_2, \ldots$ in which every element of B appears exactly once.
   - 2.3. This is a sequence in which every element of A appears.
   - 2.4. So A is countable by Lemma 10.3.5. □

Countable infinity is the smallest infinity

Note 10.3.4. An infinite set B is countable if and only if there is a sequence $b_0, b_1, b_2, \ldots \in B$ in which every element of B appears exactly once.

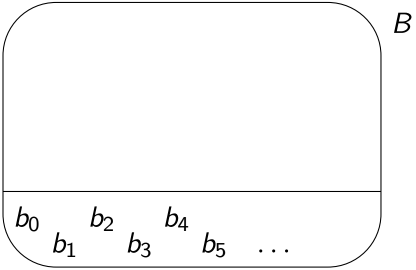


Proposition 10.3.7

Every infinite set B has a countable infinite subset.

Proof

1. Keep choosing elements $b_0, b_1, b_2, \ldots$ from B. When we choose b_n, where $n \in \mathbb{Z}_{\geqslant 0}$, we can always make sure $b_n \neq b_i$ for any $i < n$, because otherwise B is equal to the finite set $\{b_0, b_1, \ldots, b_{n-1}\}$, which is a contradiction.
2. The result is a countable infinite set $\{b_0, b_1, b_2, \ldots\} \subseteq B$. $\square$



Unions

Lemma 10.3.5. An infinite set B is countable if and only if there is a sequence $c_0, c_1, c_2, \ldots$ in which every element of B appears.

Proposition 10.4.1

Let A, B be countable infinite sets. Then $A \cup B$ is countable.

Proof

1. Apply Lemma 10.3.5 to find a sequence $a_0, a_1, a_2, \ldots$ in which every element of A appears.
2. Apply Lemma 10.3.5 to find a sequence $b_0, b_1, b_2, \ldots$ in which every element of B appears.
3. Then $a_0, b_0, a_1, b_1, a_2, b_2, \ldots$ is a sequence in which every element of $A \cup B$ appears.
4. So $A \cup B$ is countable by Lemma 10.3.5. $\square$

Products

Lemma 10.3.5. An infinite set B is countable if and only if there is a sequence $c_0, c_1, c_2, \ldots$ in which every element of B appears.

Theorem 10.4.2 (Cantor 1877)

$\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is countable.

Proof sketch

The figure on the right describes a sequence

$$(0,0), (1,0), (0,1),$$
$$(2,0), (1,1), (0,2),$$
$$(3,0), (2,1), (1,2), (0,3), \ldots$$

in which every element of $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ appears. So $\mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$ is countable by Lemma 10.3.5. $\square$

$$\begin{array}{cccccc}
\vdots & \vdots & \vdots & \vdots & \vdots & \iddots \\
(0,4) & (1,4) & (2,4) & (3,4) & (4,4) & \cdots \\
(0,3) & (1,3) & (2,3) & (3,3) & (4,3) & \cdots \\
(0,2) & (1,2) & (2,2) & (3,2) & (4,2) & \cdots \\
(0,1) & (1,1) & (2,1) & (3,1) & (4,1) & \cdots \\
(0,0) & (1,0) & (2,0) & (3,0) & (4,0) & \cdots
\end{array}$$

Power set

Lemma 10.3.5. An infinite set B is countable if and only if there is a sequence $c_0, c_1, c_2, \ldots$ in which every element of B appears.

Theorem 10.4.3 (Cantor 1891)

Let A be a countable infinite set. Then $\mathcal{P}(A)$ is not countable.

Definition 5.2.1
$\mathcal{P}(A)$ denotes the set of all subsets of A.

Plan of the proof

- Given any sequence of elements of $\mathcal{P}(A)$, we will produce an element of $\mathcal{P}(A)$ that does not appear in it.
- This will show that no sequence of elements of $\mathcal{P}(A)$ contains all the elements of $\mathcal{P}(A)$.
- Thus $\mathcal{P}(A)$ is uncountable by Lemma 10.3.5.

Power set

Lemma 10.3.5. An infinite set B is countable if and only if there is a sequence $c_0, c_1, c_2, \ldots$ in which every element of B appears.

Theorem 10.4.3 (Cantor 1891)

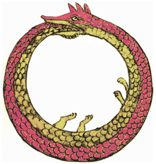
Let A be a countable infinite set. Then $\mathcal{P}(A)$ is not countable.

Definition 5.2.1
$\mathcal{P}(A)$ denotes the set of all subsets of A.

$$
\begin{array}{c|cccccc}
 & a_0 & a_1 & a_2 & a_3 & a_4 & \cdots \\
B_0 & \boxed{\notin} & \in & \notin & \notin & \notin & \cdots \\
B_1 & \in & \boxed{\notin} & \in & \notin & \in & \cdots \\
B_2 & \notin & \in & \boxed{\in} & \notin & \in & \cdots \\
B_3 & \notin & \notin & \in & \boxed{\notin} & \notin & \cdots \\
B_4 & \in & \notin & \in & \in & \boxed{\notin} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\
\hline
B & \in & \in & \notin & \in & \in & \cdots
\end{array}
$$

- Let $B_0, B_1, B_2, \ldots \in \mathcal{P}(A)$ in which every element of $\mathcal{P}(A)$ appears.
- $a_0, a_1, a_2, \ldots$ contains every element of A exactly once.
- $B \in \mathcal{P}(A)$ but B does not appear in $B_0, B_1, B_2, \ldots$.

Power set



https://commons.wikimedia.org/w/index.php?curid=54797

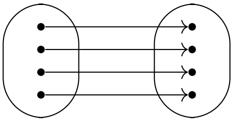
Theorem 10.4.3 (Cantor 1891)

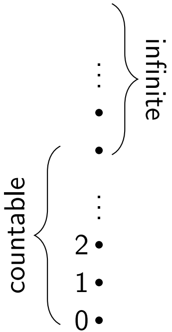
Let A be a countable infinite set. Then $\mathcal{P}(A)$ is not countable.

Proof (by contradiction)

1. Suppose $\mathcal{P}(A)$ is countable.
2. We know $\mathcal{P}(A)$ is infinite because A is infinite and $\{a\} \in \mathcal{P}(A)$ for every $a \in A$.
3. Use the countability of $\mathcal{P}(A)$ to find a sequence $B_0, B_1, B_2, \ldots \in \mathcal{P}(A)$ in which every element of $\mathcal{P}(A)$ appears exactly once.
4. Use the countability of A to find a sequence $a_0, a_1, a_2, \ldots \in A$ in which every element of A appears exactly once.
5. Define $B = \{a_i : a_i \notin B_i\}$.
6. Note that $B \subseteq A$ since $a_0, a_1, a_2, \ldots \in A$.
7.
   7.1. Let $i \in \mathbb{Z}_{\geqslant 0}$.
   7.2. If $a_i \notin B_i$, then $a_i \in B$ by the definition of B.
   7.3. if $a_i \in B_i$, then $a_i \notin B$ by the definition of B because no $j \neq i$ makes $a_j = a_i$ by the choice of $a_0, a_1, a_2, \ldots$.
   7.4. In either case, we know $B \neq B_i$.
8. This contradicts line 3 that every element of $\mathcal{P}(A)$ appears in $B_0, B_1, B_2, \ldots$. $\square$

Checkpoint





What we saw

- one way to compare the sizes of infinite sets
- the cardinality of $\mathbb{Z}_{\geqslant 0}$ is the smallest amongst those of infinite sets
- infinite sets can have different cardinalities

> No one shall be able to drive us from the paradise that Cantor created for us. David Hilbert

> Imagine set theory's having been invented by a satirist as a kind of parody on mathematics. Ludwig Wittgenstein

Questions

(1) When does one set have a smaller cardinality than another?

(2) What is the cardinality of an infinite set? Search for "cardinal numbers".

(3) Is there a subset of $\mathcal{P}(\mathbb{Z}_{\geqslant 0})$ that is not countable but not of the same cardinality as $\mathcal{P}(\mathbb{Z}_{\geqslant 0})$? Search for "continuum hypothesis".