Cardinality

Benjamin Cosman, Patrick Lin and Mahesh Viswanathan

Fall 2020

TAKE-AWAYS

- The cardinality of a finite set A (denoted $|A|$) is the number of elements in set A.
- The cardinality of the Cartesian product of finite sets is the product of the cardinalities of the individual sets, i.e., $|A_1 \times A_2 \times \cdots \times A_k| = n_1 n_2 \cdots n_k$, where $|A_i| = n_i$ for $i \in \{1, 2, \ldots k\}$.
- For finite sets A, B, if there is a surjective function $f : A \to B$ then $|B| \leq |A|$, and if there is a bijective function $f : A \to B$ then $|A| = |B|$.
- For any finite set A, $|\mathcal{P}(A)| = 2^{|A|}$.
- *Cantor's Definition:* For infinite sets A, B, we say $|B| \leq |A|$ if there is a surjective (onto) function $f : A \to B$, and we say $|A| = |B|$ if there is a bijective function $f : A \to B$.
- The following properties hold for Cantor's definition. For any set A, $|A| = |A|$. If $B \subseteq A$ then $|B| \leq |A|$. Finally, for infinite sets A, B, C, if $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$, and if $|A| \leq |B|$ and $|B| \leq |C|$ then $|A| \leq |C|$.
- *Cantor-Schröder-Bernstein Theorem:* For any infinite sets A and B, if $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.
- For infinite sets A and B, if there is an injective function $f : A \to B$ then there is a surjective function $g : B \to A$. Thus, if there is an injective function $f : A \to B$ then $|A| \leq |B|$.
- A set S is *countable* if either S is finite or $|S| = |\mathbb{N}|$.
- The sets $\mathbb{E}$ $(= \{2n \mid n \in \mathbb{N}\})$, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{N} \times \mathbb{N}$ are all countable.
- $\mathcal{P}(\mathbb{N})$ is not countable.

Finite Sets

THE CARDINALITY of a set A is the number of elements in set A, and it is denoted by $|A|$. Thus, $|\{0,1\}| = 2$ since $\{0,1\}$ has two elements 0 and 1. On the other hand, since $\emptyset$ has *no elements*, $|\emptyset| = 0$. Notice that $|\{\mathbb{N},\mathbb{Z}\}| = 2$; eventhough each element of $\{\mathbb{N},\mathbb{Z}\}$ is set with infinitely many members, $\{\mathbb{N},\mathbb{Z}\}$ has only 2 elements, namely $\mathbb{N}$ and $\mathbb{Z}$. Finally, as

$$\{0,1\} \times \{0,1\} \times \{0,1\} = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),\\ (1,0,0),(1,0,1),(1,1,0),(1,1,1)\},$$

$|\{0,1\} \times \{0,1\} \times \{0,1\}| = 8$.

The example in the previous paragraph about the cardinality of $\{0,1\} \times \{0,1\} \times \{0,1\}$ can be generalized — the cardinality of the Cartesian product of sets is the product of the cardinalities of the individual sets. Let us prove this observation.

Proposition 1. *For any finite sets $A_1, A_2, \ldots A_k$, $|A_1 \times A_2 \times \cdots \times A_k| = n_1 n_2 \cdots n_k$, where $|A_i| = n_i$ for $i \in \{1,2,\ldots k\}$.*

Proof. Let $A_1, A_2, \ldots A_k$ be arbitrary finite sets such that $|A_i| = n_i$ for $i \in \{1,2,\ldots k\}$. Elements of the set $A_1 \times A_2 \times \cdots \times A_k$ are tuples/sequences of the form $(a_1, a_2, \ldots a_k)$, where a_i is an element of set A_i. Since each a_i can be any element of A_i, we have n_1 choices for a_1, n_2 choices for a_2, and so on. Thus the total number of possible tuples in $A_1 \times A_2 \times \cdots \times A_k$ (which is its cardinality) is $n_1 n_2 \cdots n_k$. □

While we can compare the size of two sets by counting the elements in each set, we can also do it by the presence of certain types of functions between the sets. If there is a surjective function $f : A \to B$ then we can conclude that the $|B| \leq |A|$. This is an important observation that we prove next.

Proposition 2. *If there is a surjective funtion $f : A \to B$ then $|B| \leq |A|$. If there is a bijective function $f : A \to B$ then $|A| = |B|$.*

Proof. Let A and B be arbitrary finite sets, and let $f : A \to B$ be any function (not necessarily surjective or bijective). Since every element in A is mapped to some element in the $\mathsf{rng}(f)$, we can conclude that $|A| \geq |\mathsf{rng}(f)|$. That is,

$$|A| \geq |\{f(a) \mid a \in A\}| = |\mathsf{rng}(f)|.$$

Further since $\mathsf{rng}(f) \subseteq B$, we have the $|\mathsf{rng}(f)| \leq |B|$. Putting these observations together we get

$$|A| \geq |\mathsf{rng}(f)| \leq |B|.$$

These observations we have made so far are true for *any* function f.

When f is surjective or onto, by definition, the $\mathsf{rng}(f) = \mathsf{codom}(f) = B$. Thus in this case

$$|A| \geq |\mathsf{rng}(f)| = B.$$

If f is injective or 1-to-1, then since every element in A is mapped to a different element. Thus, when f is injective, we have $|A| = |\mathsf{rng}(f)|$. Therefore,

$$|A| = |\mathsf{rng}(f)| \leq B.$$

Therefore, if f is a bijective function, then since f is both injective and surjective,

$$|A| = |\mathsf{rng}(f)| = |B|.$$

□

Proposition 2 is very useful since it allows one to compute the size of one set based on another set whose size is easy to compute. Let us apply this to determine the cardinality of power sets.

Proposition 3. *For any finite set A, $|\mathcal{P}(A)| = 2^{|A|}$.*

Proof. Consider an arbitrary finite set A. Let $A = \{a_1, a_2, \ldots a_n\}$, i.e., $|A| = n$. Our proof will have the following structure. First we will show that the $|\mathcal{P}(A)| = |\{0,1\}^n|$ [1]. We will show this by demonstrating a bijection between $\mathcal{P}(A)$ and $\{0,1\}^n$, and using Proposition 2. Next, observe that by Proposition 1, $|\{0,1\}^n| = 2^n$. Putting these together proves our proposition.

Let us now prove that $|\mathcal{P}(A)| = |\{0,1\}^n|$ by defining a bijection $\chi : \mathcal{P}(A) \to \{0,1\}^n$; χ is sometimes called the *characteristic function*. The function χ is defined as follows: for $S \subseteq A$, $\chi(S) = (b_1, b_2, \ldots b_n) \in \{0,1\}^n$ where, for any i

$$b_i = \begin{cases} 1 & \text{if } a_i \in S \\ 0 & \text{if } a_i \notin S \end{cases}$$

Let us look at an example to understand the function χ. Suppose $A = \{1,2,3,4,5\}$ and $S = \{2,4,5\}$. Then $\chi(S) = (0,1,0,1,1)$. On the other hand, $\chi(\emptyset) = (0,0,0,0,0)$ while $\chi(A) = (1,1,1,1,1)$.

We will now prove that χ is bijective. Consider arbitrary subsets S, T of A such that $S \neq T$. Since $S \neq T$, there must be some element (say) a_i that belongs to exactly one out of S and T. Without loss of generality, assume that $a_i \in S$ and $a_i \notin T$ [2]. Suppose $\chi(S) = (b_1, b_2, \ldots b_n)$ and $\chi(T) = (c_1, c_2, \ldots c_n)$. Observe that $b_i = 1$ but $c_i = 0$. Thus, $\chi(S) \neq \chi(T)$. This proves that χ is injective. To prove that χ is surjective, consider an arbitrary tuple

[1] $\{0,1\}^n$ denotes the n-fold Cartesian product of $\{0,1\}$ with itself, i.e., $\{0,1\}^n = \overbrace{\{0,1\} \times \{0,1\} \times \cdots \times \{0,1\}}^{n}$.

[2] There are two possibilties to consider — either $a_i \in S$ and $a_i \notin T$ or $a_i \in T$ and $a_i \notin S$. The proof in each of these two cases is the same. To avoid repeating this proof twice, we say "without loss of generality" to say that "we will prove the case when $a_i \in S$ and $a_i \notin T$, and the other case is the same so we skip its proof". Sometimes "without loss of generality" is abbreviated as "WLOG".

$\mathsf{v} = (b_1, b_2, \ldots b_n) \in \{0,1\}^n$. We will show that $\mathsf{v} \in \mathsf{rng}(\chi)$. Define $\mathsf{set}(\mathsf{v}) = \{a_i \mid b_i = 1\}$. Observe that $\chi(\mathsf{set}(\mathsf{v})) = \mathsf{v}$, proving that χ is surjective.

To summarize our argument, since χ is bijective, by Proposition 2, $|\mathcal{P}(A)| = |\{0,1\}^n|$. Further by Proposition 1, $|\{0,1\}^n| = 2^n$. Therefore, since $|A| = n$, we have $|A| = |\{0,1\}^n| = 2^n = 2^{|A|}$, establishing the proposition. □

Infinite Sets

What is the cardinality of infinite sized sets? It is difficult to take it to be "the number of elements in the set" because that would require us to count to infinity (and beyond?). But what does it mean to count to such numbers? Should we take the cardinality of all such sets to be just ∞? Does that mean that all such sets have the same "size" (whatever that means)? Georg Canter's remarkable realization was that Proposition 2 can serve as the basis for comparing the size of (even) infinite sets and uses it to *define* the cardinality of infinite sets.

Definition 4 (Cantor)**.** For infinite sets A, B, we say $|B| \leq |A|$ if there is a surjective (onto) function $f : A \to B$. We say $|A| = |B|$ if there is a bijective function $f : A \to B$.

Notice that for infinite sets, this is a *definition*. It cannot be proved like we did for finite sets, since there is no independent notion of size for infinite sets. This simple definition is one of the most important discoveries in mathematics and has some counterintuitive consequences that are best understood by looking at examples. We begin by making a series of observations that demostrate that Definition 4 is *sound*, i.e., it has all the properties one would expect if it aims to capture the size of sets. After that, we look at examples that highlight its subtle aspects.

Properties of Cantor's Definition

We begin by making some simple observations that confirm that this definition behaves naturally. For example, clearly we expect, for any set A, $|A| = |A|$; observe that this statement requires a proof now because we need to show the existence of a bijective function from A to A. Another natural property we expect is that if $B \subseteq A$ then $|B| \leq |A|$. These do indeed hold.

Proposition 5. *For arbitrary infinite sets A, B, $|A| = |A|$ and if $B \subseteq A$ then $|B| \leq |A|$.*

Proof. Let A and B be arbitrary infinite sets.

To show $|A| = |A|$, we need to find a bijective function $f : A \to A$. Take f to be the identity function, i.e., for every $a \in A$, $f(a) = a$. We need to prove that f is bijective. Clearly, if $f(a) = f(b)$ for any $a, b \in A$ then since $f(a) = a$ and $f(b) = b$, we have $a = b$. Thus f is injective. And we know that f is surjective because for any $a \in A$, $f(a) = a$; thus $\mathsf{rng}(f) = \mathsf{codom}(f) = A$.

Now assume (for a direct proof) that $B \subseteq A$. Since B is an infinite set $B \neq \emptyset$ and let b_0 be a particular element of B. To show that $|B| \leq |A|$, by Cantor's definition, we need to show that there is a surjective function $g : A \to B$. Let us define g as follows.

$$g(a) = \begin{cases} a & \text{if } a \in B \\ b_0 & \text{if } a \notin B \end{cases}$$

We will show that g is surjective. Observe that for any $b \in B$, $g(b) = b$. Thus, $\mathsf{rng}(g) = \mathsf{codom}(g) = B$. □

Next, we would expect that if a set B has size no more than A, and set C has size no more than B, then C must have size no more than A. Similarly, one would expect that if $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$.

Proposition 6. *Let A, B, and C be arbitrary infinite sets.*

1. *If $|B| \leq |A|$ and $|C| \leq |B|$ then then $|C| \leq |A|$.*
2. *If $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$.*

Proof. Let A, B, and C be arbitrary infinite sets. Let us prove each of these statement using a direct proof.

1. Suppose $|B| \leq |A|$ and $|C| \leq |B|$. By Definition 4, there are surjective functions $f : A \to B$ and $g : B \to C$. We need to show that $|C| \leq |A|$, that is, there is a surjective function from A to C. Consider the function $g \circ f : A \to C$. We will claim that $g \circ f$ is surjective [3]. Let c be an arbitrary element of C. Since g is surjective, there is a $b \in B$ such that $g(b) = c$. Similarly, since f is surjective, there is a $a \in A$ such that $f(a) = b$. Then observe that $g \circ f(a) = g(f(a)) = g(b) = c$. Thus, $g \circ f$ is surjective.

   [3] We proved this in Homework 3, Problem 4(a), but we repeat it here for completeness.

2. Assume $|A| = |B|$ and $|B| = |C|$. By Definition 4, there are bijective functions $f : A \to B$ and $g : B \to C$. We need to prove that there is a bijective function from A to C. Consider the function $g \circ f : A \to C$. We will show that $g \circ f$ is bijective. From the previous part, we already know that $g \circ f$ is surjective. So all that is left is to prove that $g \circ f$ is injective. Let $a_1, a_2 \in A$ be arbitrary

elements such that $g \circ f(a_1) = g \circ f(a_2)$. Observe that we have $g \circ f(a_1) = g(f(a_1)) = g(f(a_2)) = g \circ f(a_2)$. Observe that since g is injective, $f(a_1) = f(a_2)$. Next, since f is injective, we have $a_1 = a_2$. This proves that $g \circ f$ is injective. Since $g \circ f$ is both injective and surjective, it is bijective, thus showing that $|A| = |C|$.

□

Finally, one would expect that if $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$. This is an important result in set theory called the *Cantor-Schröder-Bernstein* theorem.

Theorem 7 (Cantor-Schröder-Bernstein)**.** *For any infinite sets A, and B, if $|A| \leq |B|$ and $|B| \leq |A|$ then $|A| = |B|$.*

The fact that it is "named theorem" suggests both its importance and its difficulty in proving. But why is it so difficult to prove? Isn't it obvious? To realize its subtlety, it helps to re-read this statement using Cantor's definition about cardinality. The theorem is stating that if there is a *surjective* function $f : B \to A$, and a *surjective* function $g : A \to B$ then there is a *bijective* function $h : A \to B$. The proof of this result is beyond the scope of these lectures.

Examples

Let us look at some examples. Let us look at the set $\mathbb{N}$ and the set of even natural numbers

$$\mathbb{E} = \{2n \mid n \in \mathbb{N}\}.$$

Clearly, since $\mathbb{E} \subseteq \mathbb{N}$ (from Proposition 5) $|\mathbb{E}| \leq |\mathbb{N}|$. In addition, $\mathbb{E}$ is *proper* subset of $\mathbb{N}$ — there are infinitely many numbers, namely the odd numbers, that belong to $\mathbb{N}$ but not to $\mathbb{E}$. This suggests that $\mathbb{E}$ should be set of smaller size. However, it turns out it has the same size as $\mathbb{N}$.

Proposition 8. $|\mathbb{E}| = |\{2n \mid n \in \mathbb{N}\}| = |\mathbb{N}|$.

Proof. To prove that $\mathbb{E}$ and $\mathbb{N}$ have the same cardinality, we need to show that there is a bijective function between the two sets. Consider the function $\mathsf{dbl} : \mathbb{N} \to \mathbb{E}$ where $\mathsf{dbl}(n) = 2n$. We will prove that this function is bijective.

Injective: Let us prove that dbl is injective. That requires us to show that if $\mathsf{dbl}(m) = \mathsf{dbl}(n)$ then $m = n$. Let us prove this by a direct proof. Consider arbitrary m and n such that $\mathsf{dbl}(m) = \mathsf{dbl}(n)$. This means that $2m = 2n$. Dividing both sides by 2, we can conclude that $m = n$. Therefore dbl is injective.

Surjective: Next, let us prove that dbl is surjective. That is, every even number is in $\mathsf{rng}(\mathsf{dbl})$. Let m be an arbitrary even number. That means there is a natural number k such that $m = 2k$. That means $\mathsf{dbl}(k) = m$.

□

Another surprising observation, like Proposition 8, is that $\mathbb{Z}$ and $\mathbb{N}$ have the same cardinality, despite the fact that $\mathbb{Z}$ has infinitely many elements that are not in $\mathbb{N}$.

Proposition 9. $|\mathbb{Z}| = |\mathbb{N}|$.

Proof. Once again to prove this proposition, we need to show that there is a bijective function between the two sets. Consider the function $\mathsf{sgn} : \mathbb{Z} \to \mathbb{N}$ that maps non-negative integers to even natural numbers and negative numbers to odd natural numbers as shown below.

$$\begin{aligned} 0 &\mapsto 0 \\ -1 &\mapsto 1 \\ 1 &\mapsto 2 \\ -2 &\mapsto 3 \\ 2 &\mapsto 4 \\ &\vdots \end{aligned}$$

sgn can be defined precisely as

$$\mathsf{sgn}(k) = \begin{cases} 2k & \text{if } k \geq 0 \\ 2(-k) - 1 & \text{if } k < 0 \end{cases}$$

The proof that sgn is bijective is as follows.

Injective: Let i, j be arbitrary integers such that $\mathsf{sgn}(i) = \mathsf{sgn}(j)$. Since non-negative integers are mapped to even numbers and negative integers to odd, it must be the case that either both i, j are non-negative or both are negative. Let us consider these two cases in order. Suppose i, j are both non-negative. Then $\mathsf{sgn}(i) = 2i = 2j = \mathsf{sgn}(j)$ which means that $i = j$. On the other hand, if i, j are both negative, then $\mathsf{sgn}(i) = 2(-i) - 1 = 2(-j) - 1 = \mathsf{sgn}(j)$. Again, simplifying the equation $2(-i) - 1 = 2(-j) - 1$, we get $i = j$.

Surjective: Consider an arbitrary $n \in \mathbb{N}$. We consider two cases. If n is even then $n = 2k$ for some k. We have $\mathsf{sgn}(k) = 2k = n$. If n is odd then, by definition, there is a k such that $n = 2k + 1$. Take $u = -(k + 1)$. Observe that $\mathsf{sgn}(u) = 2(-u) - 1 = 2(k + 1) - 1 = 2k + 1 = n$.

□

All infinite subsets of $\mathbb{N}$ can be shown to have the same cardinality as $\mathbb{N}$, as per Cantor's definition. Thus, $\mathbb{N}$ is the "smallest" infinite set. This leads to the definition of *countable* sets.

Definition 10 (Countable)**.** A set S is *countable* if it is either finite or $|S| = |\mathbb{N}|$.

Based on Propositions 5, 8 and 9, we can conclude that $\mathbb{E}$, $\mathbb{N}$, and $\mathbb{Z}$ are countable.

Let us consider the set $\mathbb{N} \times \mathbb{N}$. On the face of it $\mathbb{N} \times \mathbb{N}$ seems like a much larger set than $\mathbb{N}$. But it turns out that it has the same cardinality. To prove this, it is useful to make one observation about the connection between injective functions and cardinality.

Proposition 11. *Let A and B be arbitrary sets such that $A \neq \emptyset$. If there is an injective function $f : A \to B$ then there is a surjective function $g : B \to A$.*

Proof. Let A, B be arbitrary sets with $A \neq \emptyset$. Since A is non-empty, let a_0 be some element of A. Let $f : A \to B$ be an injective function. Define the function $g : B \to A$ as follows.

$$g(b) = \begin{cases} a & \text{if } f(a) = b \\ a_0 & \text{if } b \notin \mathsf{rng}(f) \end{cases}$$

Observe that g, by definition, is surjective. □

An immediate consequence of Proposition 11 is that the presence of an injective function $f : A \to B$ means that $|A| \leq |B|$.

Corollary 12. *For infinite sets A and B, if there is an injective function $f : A \to B$ then $|A| \leq |B|$.*

Proof. Let $f : A \to B$ be an injective function. By Proposition 11, there is a surjective function $g : B \to A$. Then by Definition 4, $|A| \leq |B|$. □

We are now ready to establish the countability of $\mathbb{N} \times \mathbb{N}$.

Proposition 13. *The set $\mathbb{N} \times \mathbb{N}$ is countable, i.e., $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.*

Proof. We will use Corollary 12 and Theorem 7 to prove this result. That is, we will show that there are injective functions $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ and $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, thereby establishing that $|\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$ and $|\mathbb{N} \times \mathbb{N}| \leq |\mathbb{N}|$ and therefore $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$.

Take $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be defined as $f(n) = (n, 0)$. It is easy to see that f is injective since $f(n) = (n, 0) = (m, 0) = f(m)$ means that $n = m$.

Consider $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ to be $g((m,n)) = 2^m 3^n$. Again injectiveness of g can be seen as follows. Suppose $g((m_1,n_1)) = 2^{m_1}3^{n_1} = 2^{m_2}3^{n_2} = g((m_2,n_2))$. Then by uniqueness of prime factorization, it means that $m_1 = m_2$ and $n_1 = n_2$. Thus, $(m_1,n_1) = (m_2,n_2)$. □

Diagonalization

ARE THERE INFINITE SETS THAT ARE NOT COUNTABLE? Even though all the infinite sets we have seen so far are countable, there are sets whose cardinality is larger than $\mathbb{N}$. Cantor showed that $\mathcal{P}(\mathbb{N})$ is not countable. He used a very clever proof technique called *diagonalization*, which we will see in this section.

Theorem 14 (Cantor)**.** *$\mathcal{P}(N)$ is not countable.*

Proof Sketch. Before presenting the proof, let us look at an outline of how we will show that the power set of the natural numbers is not countable. Observe that we need to prove that $|\mathbb{N}| \neq |\mathcal{P}(\mathbb{N})|$. By Cantor's definition, this requires us to prove that

there is no bijective function from $\mathbb{N}$ to $\mathcal{P}(\mathbb{N})$.

We will instead show something stronger. We will prove that there is not surjective function from $\mathbb{N}$ to $\mathcal{P}(\mathbb{N})$. In other words, we will prove

if $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ then f is not surjective.

So what we are showing is in fact, $|\mathcal{P}(\mathbb{N})| \not\leq |\mathbb{N}|$.

Let us consider an arbitrary function $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$. It is useful to sketch out the ideas for this proof by looking at an example f. So consider (say) f defined as follows.

$$\begin{aligned}
f(0) &= \{1,4\} \\
f(1) &= \{0,2,3,4\} \\
f(2) &= \emptyset \\
f(3) &= \{5,6,7\} \\
f(4) &= \mathbb{N} \\
f(5) &= \mathbb{E} \\
f(6) &= \{1,3,5,7\} \\
f(7) &= \{0,2,4\} \\
&\vdots
\end{aligned}$$

Recall (from the proof of Proposition 3) there is a 1-to-1 onto correspondence between the subsets of a universe, and 0/1 sequences of length equal to the cardinality of the universe. Thus, every subset S of $\mathbb{N}$ can mapped to an infinite sequence of 0s and 1s that

indicates those numbers that belong to S. For example, the set $\{1, 4\}$ corresponds to an infinite sequence of 0s and 1s that has 1s at position 1 and 4, and 0s everywhere else, i.e., the sequence $0, 1, 0, 0, 1, 0, 0, 0, \cdots$.

Therefore, the function f can be represented by an infinite table or matrix, where the row corresponding to 0 is the sequence of 0s and 1s that encodes $f(0)$, The row corresponding to 1 is sequence corresponding to $f(1)$, and so on. For the example f shown above, this matrix will look as follows.

	0	1	2	3	4	5	6	7	$\cdots$
0	0	1	0	0	1	0	0	0	$\cdots$
1	1	0	1	1	1	0	0	0	$\cdots$
2	0	0	0	0	0	0	0	0	$\cdots$
3	0	0	0	0	0	1	1	1	$\cdots$
4	1	1	1	1	1	1	1	1	$\cdots$
5	1	0	1	0	1	0	1	0	$\cdots$
6	0	1	0	1	0	1	0	1	$\cdots$
7	1	0	1	0	1	0	0	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

To prove that the function f is not surjective, we will find a set $K_f \subseteq \mathbb{N}$ that is not in $\mathsf{rng}(f)$. This set will be constructed from the principal diagonal of this infinite matrix by flipping each bit along the diagonal. In the example above, this corresponds to flipping each of the red entries in the matrix to get the sequence $1, 1, 1, 1, 0, 1, 1, 1, \cdots$ which corresponds to the set $K_f = \{0, 1, 2, 3, 5, 6, 7, \cdots\}$ that contains $0, 1, 2, 3, 5, 6$, and 7, but not 4.

For the constructed set K_f to be in the range of f, we need the corresponding binary sequence to match some row of this infinite matrix. But that is impossible! For example, constructed sequence is not the same as the first row because it differs in the first position, it is not the second row because they differ in the second position, it is not the third row because they differ in the third position, and so on. In general, the constructed sequence differs from the ith row in the ith position. Thus, $K_f \notin \mathsf{rng}(f)$, and f is not surjective. To conclude, this means that there is no bijective function from $\mathbb{N}$ to $\mathcal{P}(\mathbb{N})$, and so $\mathcal{P}(\mathbb{N})$ is not countable. □

Proof of Theorem 14. We will prove that there is no surjective function from $\mathbb{N}$ to $\mathcal{P}(\mathbb{N})$ using the ideas just outlined. Let $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ be an arbitrary function. We will prove that f is not surjective. Consider the subset $K_f \in \mathcal{P}(\mathbb{N})$ defined as follows.

$$K_f = \{i \in \mathbb{N} \mid i \notin f(i)\}$$

We claim that $K_f \notin \mathsf{rng}(f)$, and thereby establishing that f is not

surjective. To show that $K_f \notin \mathsf{rng}(f)$, we will prove that $K_f \neq f(n)$ for any n. Observe that by definition of K_f, $n \in K_f$ if and only if $n \notin f(n)$. Thus, $n \in (K_f \setminus f(n)) \cup (f(n) \setminus K_f)$ or $K_f \neq f(n)$. □