11-11-2018

Cardinality

The **cardinality** of a set is roughly the number of elements in a set. This poses few difficulties with finite sets, but infinite sets require some care.

I can tell that two sets have the same number of elements by trying to pair the elements up. Consider the sets

$$\{a, b, c, d\} \quad \text{and} \quad \{1, 2, 3, \text{Calvin}\}.$$

They have the same number of elements because I can pair the elements of the first set with the elements of the second:

$$\begin{array}{cccc} a & b & c & d \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & \text{Calvin} \end{array}$$

This kind of pairing is called a **bijection** or a **one-to-one correspondence**; it's easy to understand with finite sets, but I need to be more careful if I'm going to use the same idea with infinite sets. I'll begin by reviewing the some definitions and results about functions.

Definition. Let X and Y be sets and let $f : X \to Y$ be a function.

1. f is **injective** (or **one-to-one**) if $f(x) = f(y)$ implies $x = y$.

2. f is **surjective** (or **onto**) if for all $y \in Y$, there is an $x \in X$ such that $f(x) = y$.

3. f is **bijective** (or a **one-to-one correspondence**) if it is injective and surjective.

Definition. Let S and T be sets, and let $f : S \to T$ be a function from S to T. A function $g : T \to S$ is called the **inverse** of f if

$$g\left(f(s)\right) = s \quad \text{for all} \quad s \in S \quad \text{and} \quad f\left(g(t)\right) = t \quad \text{for all} \quad t \in T.$$

I proved the following result earlier.

Theorem. Let S and T be sets, and let $f : S \to T$ be a function. f is invertible if and only if f is bijective.
□

Example. Let

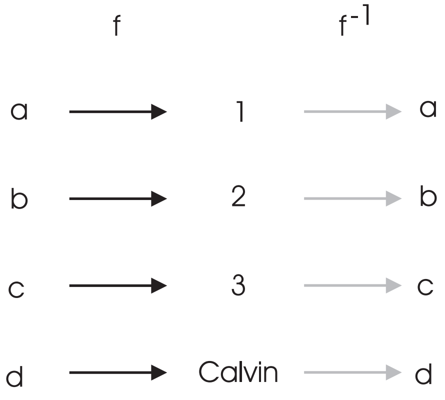
$$S = \{a, b, c, d\} \quad \text{and} \quad T = \{1, 2, 3, \text{Calvin}\}.$$

Define $f : S \to T$ by

$$f(a) = 1, \quad f(b) = 2, \quad f(c) = 3, \quad f(d) = \text{Calvin}.$$

Show that f is bijective.

I'll construct an inverse for f. The inverse should "undo" the effect of f:



As you can see, I need to define

$$f^{-1}(1) = a, \quad f^{-1}(2) = b, \quad f^{-1}(c) = 3, \quad f^{-1}(\text{Calvin}) = d.$$

I've constructed f^{-1} so that $f^{-1}(f(s)) = s$ for all $s \in S$. To be complete, I should check that it works the other way, too:

$$f\left(f^{-1}(1)\right) = f(a) = 1, \quad f\left(f^{-1}(2)\right) = f(b) = 2, \quad f\left(f^{-1}(3)\right) = f(c) = 3,$$

$$f\left(f^{-1}(\text{Calvin})\right) = f(d) = \text{Calvin}.$$

So f^{-1} really *is* the inverse of f, and f is a bijection. (For that matter, f^{-1} is a bijection as well, because the inverse of f^{-1} is f.)

Notice that this function is also a bijection from S to T:

$$h(a) = 3, \quad h(b) = \text{Calvin}, \quad h(c) = 2, \quad h(d) = 1.$$

If there is one bijection from a set to another set, there are many (unless both sets have a single element).

□

I introduced bijections in order to be able to define what it means for two sets to have the same number of elements. The number of elements in a set is called the **cardinality** of the set.

Definition. (a) Let S and T be sets. S and T have the **same cardinality** if there is a bijection f from S to T.

Notation: $|S| = |T|$ means that S and T have the same cardinality.

(b) A set S is **finite** if it is empty, or if there is a bijection $f : \{1, 2, 3, \ldots, n\} \to S$ for some integer $n \geq 1$. A set which is not finite is **infinite**.

(c) If S is a nonempty finite set and there is a bijection $f : \{1, 2, 3, \ldots, n\} \to S$ for some integer $n \geq 1$, I'll say that S has **cardinality** n or that S has n **elements**. In this case, I'll write $|S| = n$.

At this point, there is an apparently silly issue that needs to be resolved: Could a finite set be bijective with both $\{1, 2, 3\}$ and $\{1, 2, 3, 4\}$ (say)? Of course, everyday experience says that this is impossible. However, mathematicians always take the point of view that if something is *really* obvious, then it ought to be easy to justify.

Actually, this particular point isn't that simple to justify — try to prove it yourself! — but it's true, and I'll omit the proof.

Example. Prove that the set of natural numbers $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ has the same cardinality as the set $E = \{2, 4, 6, 8, \ldots\}$ of positive even integers.

Define $f : \mathbb{N} \to E$ by

$$f(n) = 2n.$$

This function has an inverse $f^{-1} : E \to \mathbb{N}$ given by

$$f^{-1}(m) = \frac{m}{2}.$$

Note that since $m \in E$, m is even, so m is divisible by 2 and $\dfrac{m}{2}$ is actually a positive integer.

Here's the proof that f and f^{-1} are inverses:

$$f\left(f^{-1}(m)\right) = f\left(\frac{m}{2}\right) = 2 \cdot \frac{m}{2} = m \quad \text{for} \quad m \in E,$$

$$f^{-1}\left(f(n)\right) = f^{-1}(2n) = \frac{2n}{2} = n \quad \text{for} \quad n \in \mathbb{N}.$$

This situation looks a little strange. E is *contained* in $\mathbb{N}$, but I've just shown that the two sets "have the same number of elements". The only reason this looks funny is that it contradicts your real world experience — which only deals with *finite* objects. In fact, it's *characteristic* of infinite sets that they have the same number of elements as some of their proper subsets. □

Informally, a set has the same cardinality as the natural numbers if the elements of an infinite set can be *listed*:

$$a_1, a_2, a_3, \ldots.$$

In fact, to define *listable* precisely, you'd end up saying "the set has the same cardinality as the natural numbers". But this is a good picture to keep in mind. I'll show that the real numbers, for instance, *can't* be arranged in a list in this way.

The next part of this discussion points out that the notion of cardinality behaves the way "the number of things in a set" ought to behave.

Proposition. Let S, T, and U be sets.

(a) The identity function $\mathrm{id} : S \to S$ given by $\mathrm{id}(s) = s$ is a bijection.

(b) The inverse of a bijection is a bijection.

(c) If $f : S \to T$ and $g : T \to U$ are bijections, then the **composite** $g \cdot f : S \to U$ is a bijection.

Proof. (a) The identity function has an inverse, namely itself. Therefore, the identity function is a bijection.

(b) If $f : S \to T$ is a bijection, then by definition it has an inverse $f^{-1} : T \to S$. To be inverses means that

$$f^{-1}\left(f(s)\right) = s \quad \text{for all} \quad s \in S \quad \text{and} \quad f\left(f^{-1}(t)\right) = t \quad \text{for all} \quad t \in T.$$

But these equation also say that f is the inverse of f^{-1}, so it follows that f^{-1} is a bijection.

(c) Suppose that $f : S \to T$ and $g : T \to U$ are bijections. Let $f^{-1} : T \to S$ and $g^{-1} : U \to T$ be their respective inverses. I'll prove that $f^{-1} \cdot g^{-1}$ is the inverse of $g \cdot f$.

$$\begin{array}{rcll} \left[\left(f^{-1} \cdot g^{-1}\right) \cdot (g \cdot f)\right](s) & = & f^{-1}\left(g^{-1}\left(g\left(f(s)\right)\right)\right) & \text{Definition of composite} \\ & = & f^{-1}\left(f(s)\right) & g^{-1}\left(g\left(\text{junk}\right)\right) = \text{junk} \\ & = & s & f^{-1}\left(f\left(\text{junk}\right)\right) = \text{junk} \end{array}$$

$$\begin{array}{rcll} \left[(g \cdot f) \cdot \left(f^{-1} \cdot g^{-1}\right)\right](u) & = & g\left(f\left(f^{-1}\left(g^{-1}(u)\right)\right)\right) & \text{Definition of composite} \\ & = & g\left(g^{-1}(u)\right) & f\left(f^{-1}\left(\text{junk}\right)\right) = \text{junk} \\ & = & u & g^{-1}\left(g\left(\text{junk}\right)\right) = \text{junk} \end{array}$$

This proves that $f^{-1} \cdot g^{-1}$ is the inverse of $g \cdot f$, so $g \cdot f$ is a bijection. □

Corollary. Let S, T, and U be sets.

(a) (Reflexivity) $|S| = |S|$.

(b) (Symmetry) If $|S| = |T|$, then $|T| = |S|$.

(c) (Transitivity) If $|S| = |T|$ and $|T| = |U|$, then $|S| = |U|$.

In other words, having the same cardinality is an equivalence relation.

Proof. (a) By the lemma, the identity function $\mathrm{id} : S \to S$ is a bijection, so $|S| = |S|$.

(b) If $|S| = |T|$, then there is a bijection $f : S \to T$. By the lemma, $f^{-1} : T \to S$ is a bijection. Therefore, $|T| = |S|$.

(c) If $|S| = |T|$ and $|T| = |U|$, then there are bijections $f : S \to T$ and $g : T \to U$. By the lemma, $g \cdot f : S \to U$ is a bijection, so $|S| = |U|$. □

%divider

Example. Prove that the interval $(0, 1)$ has the same cardinality as $\mathbb{R}$.

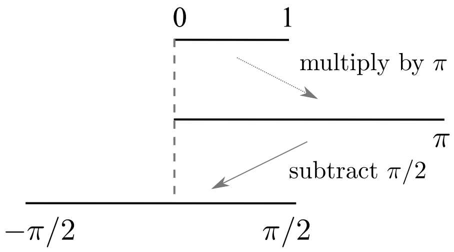
First, notice that the open interval $\left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$ has the same cardinality as the real line. To prove this, I have to construct a bijection $f : \left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right) \to \mathbb{R}$. It's easy: just define

$$f(x) = \tan x.$$

To show that f is bijective, I have to show that it has an inverse; the inverse is $f^{-1}(x) = \arctan x$.

Now I know that $\left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$ and $\mathbb{R}$ have the same cardinality. Next, I'll show that $(0, 1)$ and $\left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$ have the same cardinality.

The idea is to multiply by π to stretch $(0, 1)$ to $(0, \pi)$. Then I subtract $\dfrac{\pi}{2}$ to shift $(0, \pi)$ to $\left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$.



All together, I define $g : (0, 1) \to \left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$ by

$$g(x) = \pi x - \frac{\pi}{2}.$$

First, if $0 < x < 1$, then $0 < \pi x < \pi$, so $-\dfrac{\pi}{2} < \pi x - \dfrac{\pi}{2} < \dfrac{\pi}{2}$. This shows that g takes inputs in $(0, 1)$ and produces outputs in $\left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$.

To show that g is bijective, I have to produce an inverse. The standard "swap the x's and y's" procedure works; you get

$$g^{-1}(x) = \frac{x + \dfrac{\pi}{2}}{\pi}.$$

Here's the proof that g and g^{-1} are inverses:

$$g\left(g^{-1}(x)\right) = g\left(\frac{x + \dfrac{\pi}{2}}{\pi}\right) = \pi \cdot \frac{x + \dfrac{\pi}{2}}{\pi} - \frac{\pi}{2} = x + \frac{\pi}{2} - \frac{\pi}{2} = x,$$

$$g^{-1}\left(g(x)\right) = g^{-1}\left(\pi x - \frac{\pi}{2}\right) = \frac{\pi x - \dfrac{\pi}{2} + \dfrac{\pi}{2}}{\pi} = \frac{\pi x}{\pi} = x.$$

Therefore, g is a bijection, so $(0, 1)$ and $\left(-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right)$ have the same cardinality. By transitivity, $(0, 1)$ and $\mathbb{R}$ have the same cardinality. □

Example. Prove that $(0,1)$ has the same cardinality as $\mathbb{R}^+ = (0,\infty)$.

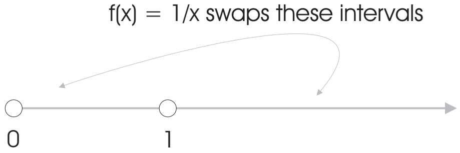
Define $f : (0,1) \to (1,\infty)$ by

$$f(x) = \frac{1}{x}.$$

Note that if

$$0 < x < 1, \quad \text{then} \quad \frac{1}{x} > 1.$$

Therefore, f *does* map $(0,1)$ to $(1,\infty)$.



I claim that $f^{-1}(x) = \dfrac{1}{x}$. If $x > 1$, then $0 < \dfrac{1}{x} < 1$, so f^{-1} maps $(1,\infty)$ to $(0,1)$. Moreover,

$$f\left(f^{-1}(x)\right) = f\left(\frac{1}{x}\right) = \frac{1}{\left(\dfrac{1}{x}\right)} = x,$$

$$f^{-1}\left(f(x)\right) = f^{-1}\left(\frac{1}{x}\right) = \frac{1}{\left(\dfrac{1}{x}\right)} = x.$$

Thus, f is a bijection.

Define $g : (1,\infty) \to (0,\infty)$ by

$$g(x) = x - 1.$$

If $x > 1$, then $x - 1 > 0$. Therefore, g *does* map $(1,\infty)$ to $(0,\infty)$.

I claim that $g^{-1}(x) = x + 1$. If $x > 0$, then $x + 1 > 1$, so g^{-1} maps $(0,\infty)$ to $(1,\infty)$. Moreover,

$$g\left(g^{-1}(x)\right) = g(x+1) = (x+1) - 1 = x,$$

$$g^{-1}\left(g(x)\right) = g^{-1}(x-1) = (x-1) + 1 = x.$$

Therefore, g is a bijection.

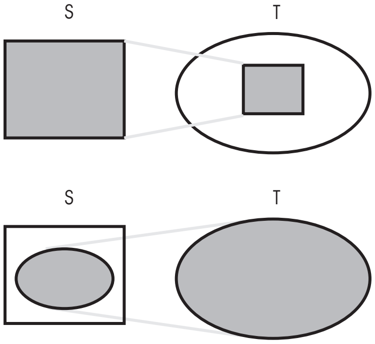
With the bijections f and g, I have $|(0,1)| = |(1,\infty)| = |(0,\infty)|$, so $(0,1)$ and $(0,\infty)$ have the same cardinality. $\square$

In many situations, it's difficult to show that two sets have the same cardinality by actually constructing a bijection between them. The theorem that follows gives an indirect way to show that two sets have the same cardinality.

Theorem. (Schröder-Bernstein) Let S and T be sets. Suppose there are injective functions $f : S \to T$ and $g : T \to S$. Then S and T have the same cardinality. $\square$

The proof of the Schröder-Bernstein theorem is a little tricky, so I won't do it here.

The Schröder-Bernstein theorem says that if S has the same cardinality as a subset of T, and T has the same cardinality as a subset of S, then S and T must have the same cardinality.



It is a powerful tool for showing that sets have the same cardinality. Here are some examples.

Example. Show that the open interval $(0,1)$ and the closed interval $[0,1]$ have the same cardinality.

The open interval $0 < x < 1$ is a *subset* of the closed interval $0 \le x \le 1$. In this situation, there is an "obvious" injective function $f : (0,1) \to [0,1]$, namely the function $f(x) = x$ for all $x \in (0,1)$. (f is called an **inclusion map**.) If $f(x_1) = f(x_2)$, then $x_1 = x_2$, so f is injective.

Next, I'll construct an injective function $g : [0,1] \to (0,1)$. The idea is to find a "copy" of $[0,1]$ in $(0,1)$, then do some scaling and translation to map $[0,1]$ onto the copy. I'll use the interval $[0.25, 0.75]$ as my target in $(0,1)$. The target has length 0.5, so I'll multiply by 0.5 to shrink $[0,1]$ to $[0,0.5]$. Next, I'll add 0.25 to shift $[0,0.5]$ to $[0.25,0.75]$. All together, I get

$$g(x) = 0.5x + 0.25 \quad \text{for} \quad 0 \le x \le 1.$$

First, if $0 \le x \le 1$, then $0 \le 0.5x \le 0.5$, so $0.25 \le 0.5x + 0.25 \le 0.75$. This proves that g is a function from $[0,1]$ to $[0.25,0.75]$.

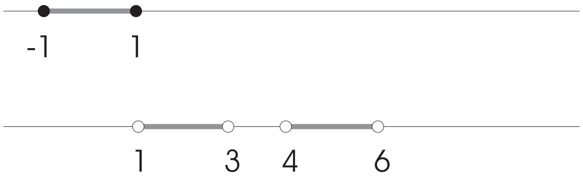
Next, I need to show that g is injective. Suppose that $g(a) = g(b)$, I must prove that $a = b$. Now $g(a) = g(b)$ means that

$$\begin{aligned} 0.5a + 0.25 &= 0.5b + 0.25 \\ 0.5a &= 0.5b \\ a &= b \end{aligned}$$

Therefore, g is injective. (In fact, g is bijective, and you could prove injectivity by constructing g^{-1} — though it would be overdoing it a bit.)

Now I have injective functions $(0,1) \to [0,1]$ and $[0,1] \to (0,1)$. By Schröder-Bernstein, $|(0,1)| = |[0,1]|$. □

Example. Prove that $[-1,1]$ has the same cardinality as $(1,3) \cup (4,6)$.



The two sets don't "look alike" — the first set is a single interval which is closed on both ends, while the second set consists of two open intervals. *When two sets don't look alike but you think they have the* *same cardinality, consider using the Schröder-Bernstein theorem.* I'll define injective functions going from each set into the other.

I'll describe in words how I'm getting the definitions of the functions. (Note that there are many functions you could use to do this!)

The first set is an interval of length 2, which (because of its endpoints) won't fit in either of the intervals that make up the second set. Since the second set's intervals *don't* have endpoints, if I just slide $[-1, 1]$ over, its endpoints will stick out of the ends of either $(1, 3)$ or $(4, 6)$. So the idea is to shrink $[-1, 1]$ first, then slide it inside either $(1, 3)$ or $(4, 6)$.

If I multiply $[-1, 1]$ by 0.5, I get $[-0.5, 0.5]$, an interval of length 1. This will surely fit inside $(1, 3)$ (say), and I can slide $[-0.5, 0.5]$ into $(1, 3)$ by adding 2. This takes $[-0.5, 0.5]$ to $[1.5, 2.5]$. I just have to do the two steps one after the other. So define $f : [-1, 1] \to (1, 3) \cup (4, 6)$ by

$$f(x) = 0.5x + 2.$$

First, I have to show that this makes sense — that is, that f really takes $[-1, 1]$ *into* $(1, 3) \cup (4, 6)$. Suppose $x \in [-1, 1]$. Then

$$\begin{gathered} -1 \le x \le 1 \\ -0.5 \le 0.5x \le 0.5 \\ -0.5 + 2 \le 0.5x + 2 \le 0.5 + 2 \\ 1.5 \le f(x) \le 2.5 \end{gathered}$$

Since $1.5 \le f(x) \le 2.5$, obviously $1 < f(x) < 3$, so f *does* map $[-1, 1]$ into $(1, 3) \cup (4, 6)$.

Next, I have to show that f is injective. Suppose $f(a) = f(b)$. Then

$$\begin{gathered} 0.5a + 2 = 0.5b + 2 \\ 0.5a = 0.5b \\ a = b \end{gathered}$$

Hence, f is injective.

Next, I have to define an injective function $g : (1, 3) \cup (4, 6) \to [-1, 1]$. Now $(1, 3) \cup (4, 6)$ occupies a total length of $6 - 1 = 5$, whereas the target interval $[-1, 1]$ has length 2. If I multiply by $\dfrac{1}{5} = 0.2$, I'll shrink $(1, 3) \cup (4, 6)$ to $(0.2, 0.6) \cup (0.8, 1.2)$, which has a total length of 1. Next, I can slide $(0.2, 0.6) \cup (0.8, 1.2)$ inside $[-1, 1]$ by subtracting 0.7, which should give $(-0.5, -0.1) \cup (0.1, 0.5)$.

Thus, define $g : (1, 3) \cup (4, 6) \to [-1, 1]$ by

$$g(x) = 0.2x - 0.7.$$

I need to check that g maps $(1, 3) \cup (4, 6)$ into $[-1, 1]$. Let $x \in (1, 3) \cup (4, 6)$. Then certainly x is between 1 and 6, i.e. $1 < x < 6$. (Of course, $1 < x < 6$ does *not* imply that $x \in (1, 3) \cup (4, 6)$. Do you see why?) So

$$\begin{gathered} 1 < x < 6 \\ 0.2 < 0.2x < 1.2 \\ 0.2 - 0.7 < 0.2x - 0.7 < 1.2 - 0.7 \\ -0.5 < g(x) < 0.5 \end{gathered}$$

Since $-0.5 < g(x) < 0.5$, obviously $-1 \le g(x) \le 1$, so g *does* map $(1, 3) \cup (4, 6)$ into $[-1, 1]$.

Next, I have to show that g is injective. Suppose $g(a) = g(b)$. Then

$$\begin{gathered} 0.2a - 0.7 = 0.2b - 0.7 \\ 0.2a = 0.2b \\ a = b \end{gathered}$$

Therefore, g is injective.

Hence, $[-1,1]$ and $(1,3) \cup (4,6)$ have the same cardinality, by the Schröder-Bernstein theorem. □

I've already noted that it's easy to find finite sets of different cardinalities: for example, a set with three elements does not have the same cardinality as a set with 42 elements. I've also given examples of infinite sets which have the same cardinality. It's an important fact that not all infinite sets have the same cardinality — there are different kinds of "infinity"! Here's some terminology which I'll used to describe the situation.

Definition. A set is **countably infinite** if it has the same cardinality as the natural numbers $\mathbb{N} = \{1,2,3,\ldots\}$. An infinite set which is not **countably infinite** is **uncountably infinite** or **uncountable**.

A set is **countable** if it is either finite or countably infinite.

I know that some infinite sets — the even integers, for instance — are countably infinite. I know of other infinite sets, such as the real numbers. Is the set of real numbers countably infinite? The answer is no; the proof is due to Georg Cantor (1845–1918), and is called the **diagonalization argument**.

Theorem. The open interval $(0,1)$ is uncountably infinite.

Proof. I'm going to be a little informal in this proof so that the main idea isn't lost in a lot of notation.

Suppose on the contrary that $(0,1)$ is countably infinite. Represent numbers in the interval as decimals $0.a_1a_2a_3\ldots$. (If a number ends in an infinite sequence of 9's, rewrite it as a finite decimal — so, for instance, $0.134999\ldots$ becomes 0.135.) Since $(0,1)$ is countably infinite by assumption, I can arrange the numbers in $(0,1)$ in a list:

```
. 3 6 8 9 7 3 4 8
. 5 0 4 1 8 5 6 3
. 0 2 4 7 3 5 9 6
. 2 1 7 6 1 4 0 7   . . .
. 4 4 2 0 5 9 3 1
. 7 9 6 9 3 2 1 5
. 7 1 8 1 8 0 4 2
. 1 3 5 4 6 7 6 3
         .
         .
         .
```

I emphasize that, by assumption, this list contains *all* of the numbers in the interval $(0,1)$.

Now go down the diagonal and make a number using the digits. In this case, I get the number $0.30465243\ldots$.

Take each of the digits in this number and *change it* to any other digit except 9. For example, you could add 1 to each digit from 0 to 7 and change 8 or 9 to 0. This would produce the number $0.41576354\ldots$.

(The reason you do not want to change digits to 9 is so that you don't wind up with a number that ends in an infinite sequence of 9's.)

The number $0.41576354\ldots$ differs from each of the numbers in my list. Specifically, the n^{th} digit of $0.41576354\ldots$ is different from the n^{th} digit in the n^{th} number on the list. This means that $0.41576354\ldots$ is not in my list — which is a contradiction, because I assumed that my list contained *all* of the numbers in the interval $(0,1)$.

Therefore, the interval $(0,1)$ must be uncountably infinite. □

Since the interval $(0,1)$ has the same cardinality as $\mathbb{R}$, it follows that $\mathbb{R}$ is uncountably infinite as well. Notice that $\mathbb{Z}$ (which is countably infinite) is a subset of $\mathbb{R}$. Are there any sets which are "between" $\mathbb{Z}$ and $\mathbb{R}$ in cardinality?

The **Continuum Hypothesis** states that there are *no* sets which are "between" $\mathbb{Z}$ and $\mathbb{R}$ in cardinality; it was first stated by Cantor, who was unable to construct a proof. Kurt Gödel [2] proved around 1940 that the Continuum Hypothesis was consistent relative to the standard axioms of set theory. Paul Cohen [1] proved in 1963 that the Continuum Hypothesis is *undecidable*: It is independent of the standard axioms for set theory.

In other words, the question of the existence of a subset of $\mathbb{R}$ which has cardinality different from either $\mathbb{Z}$ or $\mathbb{R}$ can't be settled without adding assumptions to standard mathematics — and you can assume either that such a set exists, or that it doesn't, without causing a contradiction.

Definition. Let S be a set. The **power set** $\mathcal{P}(S)$ of S is the set of all subsets of S.

For instance, suppose $S = \{a, b, c\}$. The power set of S is

$$\mathcal{P}(S) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Notice that the power set includes the empty set and the set S itself.

If you're constructing a subset of a set, there are two alternatives for each element: Either it is in the subset, or it is not. So if the set has n elements, the two alternatives for each element give 2^n possibilities in all. Therefore, if S is finite and $|S| = n$, then $|\mathcal{P}(S)| = 2^n$.

In this example, $|S| = 3$, and $|\mathcal{P}(S)| = 2^3 = 8$.

Theorem. If S is a set, then S and $\mathcal{P}(S)$ do not have the same cardinality.

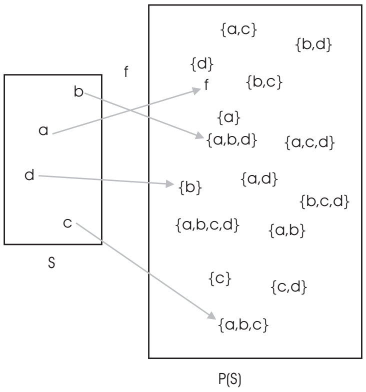
Proof. Suppose first that $S = \emptyset$. Now $\emptyset \subset \emptyset$, so $P(\emptyset) = \{\emptyset\}$. Hence, $|\emptyset| = 0$ while $|P(\emptyset)| = 1$, and the result is true in this case.

Now suppose that $S \neq \emptyset$. I'll prove the result by contradiction. Suppose that $|S| = |\mathcal{P}(S)|$. This means that there is a bijection $f : S \to \mathcal{P}(S)$.

Since f is a bijection, every element of the power set — that is, every subset of S — is paired up with an element of S. For example, there must be an element $s \in S$ for which $f(s) = \emptyset$.

Of course, $s \notin \emptyset$. So *s is an element which is paired up with a subset that doesn't contain it.* And in general, f takes an element of S to a subset of S, and that subset either contains the element or it doesn't.

Here's a particular example to help you get your bearings. In the picture below, the set is $S = \{a, b, c, d\}$ and the function f is depicted by the arrows.



In this example, f takes b and c to subsets that contain them; f takes a and d to subsets which don't contain them.

Continuing with the proof, let

$$T = \{s \in S \mid s \notin f(s)\}.$$

That is, T is the subset of elements of S which f takes to subsets which don't contain them. I know there is at least one such element, namely the element which f takes to the empty set.

Now f is bijective, and T is a subset of S, so there is an element $s_0 \in S$ such that $f(s_0) = T$. Question: Is $s_0 \in T$?

If $s_0 \in T$, then by definition of T, $s_0 \notin f(s_0) = T$. This is a contradiction.

If $s_0 \notin T$, then $s_0 \notin T = f(s_0)$, so s_0 satisfies the defining condition for T — which means $s_0 \in T$. This is a contradiction.

Since $s_0 \in T$ and $s_0 \notin T$ both lead to contradictions, I've actually contradicted my first assumption — that $|S| = |\mathcal{P}(S)|$. Therefore, $|S| \neq |\mathcal{P}(S)|$, as I wanted to prove. □

As an example, the power set of the natural numbers $\mathbb{N}$ has the same cardinality as $\mathbb{R}$.

I showed earlier that $\mathbb{N}$ is countably infinite, whereas $\mathbb{R}$ is uncountably infinite, so this confirms the theorem in this particular case.

Proposition. If X and Y are finite, then $|X \times Y| = |X|\,|Y|$.

Proof. Here's an informal proof. The elements of $X \times Y$ are ordered pairs (x, y) where $x \in X$ and $yinY$. Since there are $|X|$ choices for x and there are $|Y|$ choices for y, there are $|X|\,|Y|$ such ordered pairs.

More formally, suppose

$$X = \{x_1, x_2, \ldots x_m\} \quad \text{and} \quad Y = \{y_1, y_2, \ldots y_n\}.$$

Define a function $f : X \times Y \to \{1, 2, \ldots mn\}$ by

$$f(x_i, y_j) = (i - 1)n + j.$$

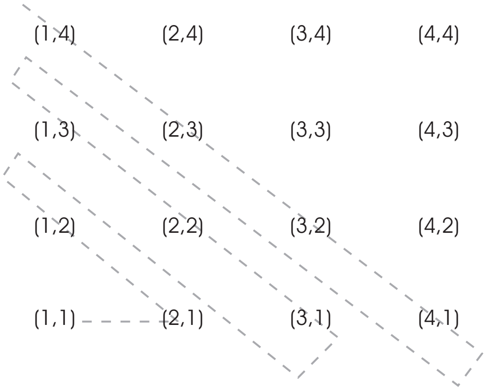
I'll let you verifty that it's injective and surjective, and hence, a bijection. □

For example, if S has 42 elements and T has 5 elements, then $S \times T$ has $42 \cdot 5 = 210$ elements.

Interesting things happen when S and T are infinite. For example, $\mathbb{N}$ is countably infinite; how big is $\mathbb{N} \times \mathbb{N}$?

Theorem. $\mathbb{N} \times \mathbb{N}$ is countably infinite.

Proof. $\mathbb{N} \times \mathbb{N}$ is the set of pairs (m, n), where m and n are natural numbers:



I'm going to list the pairs starting with $(1, 1)$ in the order shown by the grey line. This means I'm constructing a function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Here it is:

$$f(m, n) = \frac{(m + n - 2)(m + n - 1)}{2} + m.$$

Here is why this works. (m, n) is the m^{th} element on the diagonal line whose elements add up to $m+n$. Previous to that, the number of element I've gone through is

$$0 + 1 + 2 + \cdots + (m + n - 2) = \frac{(m + n - 2)(m + n - 1)}{2}.$$

That gives $\dfrac{(m + n - 2)(m + n - 1)}{2} + m$.

It's a little tricky to show f is injective, so I'll omit the proof here. There is an obvious way to make an injective function from $\mathbb{N}$ to $\mathbb{N} \times \mathbb{N}$:

$$g(n) = (1, n).$$

If $g(n_1) = g(n_2)$, then $(n_1, 1) = (n_2, 1)$, so $n_1 = n_2$, and hence g is injective. By the Schröder-Bernstein theorem, $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$ have the same cardinality. $\square$

[1] Paul J. Cohen, *Set Theory and the Continuum Hypothesis*, Reading, Massachusetts: The Benjamin-Cummings Publishing Company, Inc., 1966 [ISBN 0-8053-2327].

[2] Kurt Gödel, Consistency-proof for the generalized continuum hypothesis, *Proc. Nat. Acad. Sci. U.S.A.*, 25(1939), 220-204.