A Primer in Infinite Sets

Dominik Scheder

Abstract

When do two sets have the same size? When is one smaller than the other? This question seems trivial when considering *finite* sets. For infinite sets, however, it leads to a beautiful theory, of which this essay sketches the basics.

1 An Inifnite Set We All Know

We all know the set of natural numbers, $1, 2, 3, \ldots$. It is infinite, so we cannot write it down in its entirety. Instead, we invented a neat symbol for it: $\mathbb{N}$. Sometimes, it is convenient to include the number 0 in it, in which case we write $\mathbb{N}_0$. That is, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Clearly, $\mathbb{N}_0$ is larger than $\mathbb{N}$, since it has more element. In set-theoretic notation, $\mathbb{N} \subsetneq \mathbb{N}_0$, i.e., the former is a proper subset of the latter. Somewhat surprisingly for the set-theoretic novice, these two sets have the same size, for a certain meaning of "size". Note that we can pair the elements of $\mathbb{N}_0$ with those of $\mathbb{N}$ such that none goes unmatched:

$\mathbf{N}_0$	0	1	2	3	...
$\mathbf{N}$	1	2	3	4	...

Formally, we just defined a function $f : \mathbb{N}_0 \to \mathbb{N}$, $x \mapsto x + 1$. This function is bijective: for every element $y \in \mathbb{N}$, there is exactly one element $x \in \mathbb{N}_0$ such that $f(x) = y$. In this sense, $\mathbb{N}$ and $\mathbb{N}_0$ are actually of the same size!

Definition 1. *Two sets A, B are said to have the same* cardinality *if there exists a bijection $f : A \to B$. In this case we write $A \cong B$ as a shorthand.*

Note that we use the fancy word "cardinality" instead of "size", probably since "size" carries too many everyday connotations. We just proved that $\mathbb{N} \cong \mathbb{N}_0$. If you imagine $\mathbb{N}$ and $\mathbb{N}_0$ before your eyes, you must admit that they kind of "look the same", with $\mathbb{N}_0$ just being shifted to the left. In contrast, the set $\mathbb{Z}$ of integers, $\ldots, -2, -1, 0, 1, 2, \ldots$ looks very different—it is "infinite on both sides", whereas $\mathbb{N}$ and $\mathbb{N}_0$ are only "infinite on the right". Still, being a bit creative, we can pair up $\mathbb{N}_0$ with the integers $\mathbb{Z}$:

$\mathbf{N}_0$	0	1	2	3	4	5	6	...
$\mathbf{Z}$	0	−1	1	−2	2	−3	3	...

Again, this defines a bijection $g : \mathbf{N}_0 \to \mathbf{Z}$ by

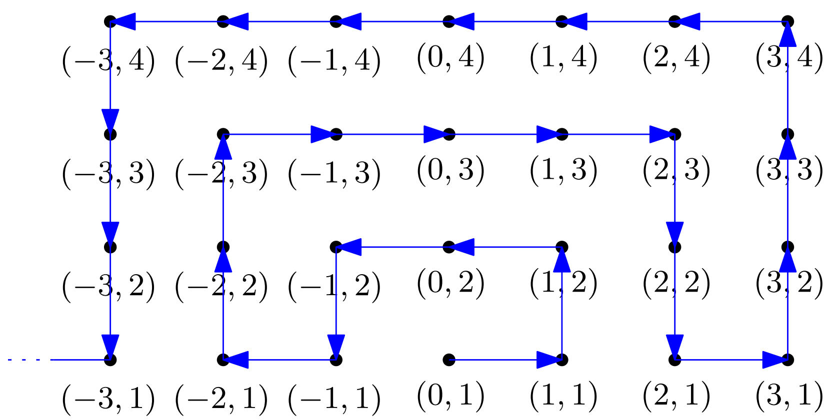
$$g(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even },\\ \\ -\frac{x+1}{2} & \text{if } x \text{ is odd }. \end{cases}$$

Note that g is not as "nice" as f, since we have to "fold" $\mathbb{Z}$ to make it look like $\mathbb{N}_0$. We have just proved that $\mathbb{N}_0 \cong Z$.

Proposition 2. *$\cong$ is an equivalence relation in the following sense: $A \cong A$ for every set A; $A \cong B$ implies $B \cong A$; and $A \cong B, B \cong C$ imply $A \cong C$.*

2 The Rational Numbers

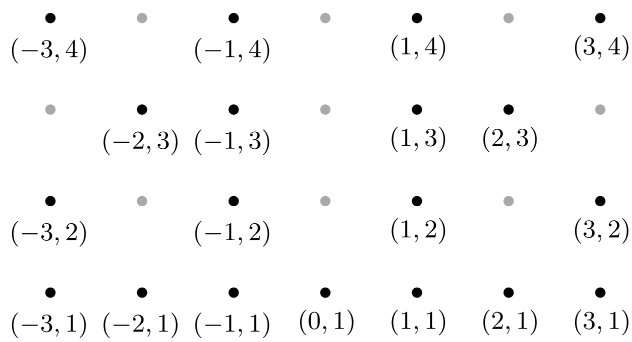
By now we know that$\mathbb{N} \cong \mathbb{N}_0 \cong \mathbb{Z}$. But surely $\mathbb{Q}$, the set of rational numbers, looks very different! For example, in $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}$, one number neatly follows the other, all in a row, whereas $\mathbb{Q}$ is *dense*, meaning that between any two rational numbers you find another one (and in fact infinitely many)! Surprisingly, it turns out that $\mathbb{N}$ and $\mathbb{Q}$ have the same cardinality! As a first step, consider the set $\mathbb{Z} \times \mathbb{N}$. This is the set of all pairs (a, b) with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. We can imagine $\mathbb{Z} \times \mathbb{N}$ as a grid that is infinite to the left, right, and top, but not the bottom. The figure below depicts a path that starts at $(0, 1)$ and visits all elements in $\mathbb{Z} \times \mathbb{N}$.



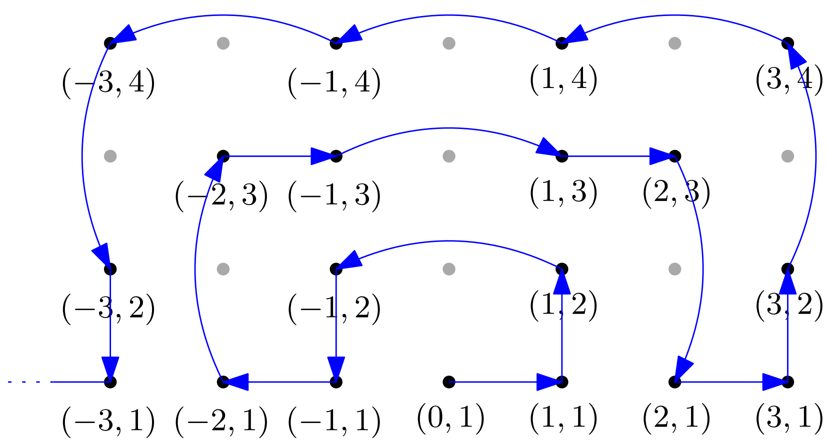
This path actually defines a bijection $f : \mathbb{N}$ to $\mathbb{Z} \times \mathbb{N}$: $f(i)$ is the i^{th} point on the path, for example $f(5) = (-1, 2)$.

Proposition 3. $\mathbb{N} \cong \mathbb{Z} \times \mathbb{N}$.

Nice, but what does this have to do with the rational numbers $\mathbb{Q}$? Well, a rational number is a fraction $\frac{a}{b}$ with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. So $\mathbb{Q}$ and $\mathbb{Z} \times \mathbb{N}$ are the same thing? Note quite: $\frac{1}{2}$ and $\frac{2}{4}$ are the same rational number, but $(1, 2)$ and $(2, 4)$ are two different elements of $\mathbb{Z} \times \mathbb{N}$. Sticking to the picture above, let us delete all points (a, b) for which $\gcd(a, b) > 1$, i.e., for which the fraction a/b is not reduced:



We can now draw the same path, simply jumping over deleted points:



We see that the path visits every rational number exactly once. This defines a bijection $h : \mathbb{N} \to \mathbb{Q}$ via $h(i)$ being $\frac{a}{b}$, where (a, b) is the i^{th} point on the path. For example, $h(5) = -1$, $h(10) = \frac{2}{3}$. I don't know of any "nice" way to write down this function, but clearly h is a function, and a bijection on top of that! To summarize what we have discovered so far:

Theorem 4. *The sets* $\mathbb{N}, \mathbb{N}_0, \mathbb{Z} \times \mathbb{N}, \mathbb{Q}$ *all have the same cardinality.*

Exercise 2.1. Prove that $\mathbb{N} \cong \mathbb{N} \times \mathbb{N}$. Rather than re-working the path construction above, try to build upon previous results, like $\mathbb{Z} \times \mathbb{N} \cong \mathbb{N}$.

Exercise 2.2. Prove that $\mathbb{N} \times \mathbb{N} \times \mathbb{N} \cong \mathbb{N}$, and in fact $\mathbb{N}^k \cong \mathbb{N}$. Recall that $\mathbb{N}^k$ is the set of all k-tuples $(a_1, \ldots, a_k)$ where $a_1, \ldots, a_k \in \mathbb{N}$.

For a set A, let A^* denote the set of all finite tuples $(a_1, \ldots, a_k)$ over A, where k is arbitrary but finite. That is, $A^* = \{\epsilon\} \cup A \cup A^2 \cup A^3 \cup A^4 \cup \ldots$. Here, ϵ denotes the empty sequence.

Exercise 2.3. Show that $\{0,1\}^* \cong \mathbb{N}$. Recall that $\{0,1\}^*$ is the set of all finite bit sequences.

Exercise 2.4. Show that $\mathbb{N}^* \cong \mathbb{N}$.

So far, we have encountered several infinite sets which turn out to have the same cardinality as the set of natural numbers. Perhaps *all* infinite sets have the same size? The answer is no, as we will see in the next section.

3 Uncountable Sets

An infinite set A having the same cardinality as $\mathbb{N}$ is called *countable* or *countably infinite*. An infinite set A for which there is no bijection $\mathbb{N} \to A$ is called uncountable. Consider the set $\{0,1\}^{\mathbb{N}}$ of infinite bit sequences $(a_1, a_2, \ldots)$.

Theorem 5. *The set* $\{0,1\}^{\mathbb{N}}$ *is uncountable.*

Proof. Let $f : \mathbb{N} \to \{0,1\}^{\mathbb{N}}$ be a function. To prove the theorem, we have to show that f is not a bijection. In fact, we will show that f is not surjective, that is, there is some sequence $\mathbf{a} = (a_1, a_2, \ldots) \in \{0,1\}^{\mathbb{N}}$ such that $\mathbf{a}$ is not in the image of f, meaning $f(i) \neq \mathbf{a}$ for all $i \in \mathbb{N}$.

We can draw f as an infinite table, where the i^{th} row is $f(i)$. The following picture gives an example how the left-upper part of this table could look.

i	$f(i)$						
1	1	0	1	0	0	1	...
2	0	1	1	0	1	1	...
3	1	0	0	1	0	1	...
4	1	1	0	1	1	0	...
5	0	1	1	1	1	1	...
6	1	0	0	0	0	0	...
$\vdots$							

From this table, we will construct a new sequence. First, look at the diagonal on this table.

i	$f(i)$						
1	1	0	1	0	0	1	...
2	0	1	1	0	1	1	...
3	1	0	0	1	0	1	...
4	1	1	0	1	1	0	...
5	0	1	1	1	1	1	...
6	1	0	0	0	0	0	...
$\vdots$							

This itself is an infinite sequence $(d_1, d_2, \dots)$, in this case $(1, 1, 0, 1, 1, 0, \dots)$. Now define the sequence $\mathbf{a} := (1 - d_1, 1 - d_2, 1 - d_3, \dots)$. In other words: if the i^{th} entry to the i^{th} row of the table is 0, then a_i is 1, otherwise it is 0. Is there any row in the table that is equal to $\mathbf{a}$? Clearly not: suppose, for the sake of contradiction, that the i^{th} row of the table equals $\mathbf{a}$. Then the i^{th} entry of this row is d_i, by definition of d_i. But $a_i = 1 - d_i$, so they are not equal. In other words, the sequence $\mathbf{a}$ does not appear as a row in this table; $\mathbf{a}$ is not in the image of f; $f(i) \neq \mathbf{a}$ for all $i \in \mathbb{N}$. In short, f is not surjective.

Let us summarize what we have done: for any given function $f : \mathbb{N} \to \{0, 1\}^{\mathbb{N}}$, we have constructed a sequence $\mathbf{a} \in \{0, 1\}^{\mathbb{N}}$ that is not in the image of f, showing that f is not surjective, let alone bijective. $\square$

The above proof is also called Cantor's diagonalization argument, because it was first discovered by Georg Cantor, and focusing on the diagonal plays a crucial role.

4 The Real Numbers

We all know (or think we know) the set of real number $\mathbb{R}$. What is its cardinality, compared to the sets we have seen above—$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \{0,1\}^{\mathbb{N}}$? We first show that $\mathbb{R}$ actually contains as many numbers as the open unit interval $(0,1)$.

Proposition 6. *$\mathbb{R} \cong (0,1)$.*

Proof. Consider the function $f : \mathbb{R} \to (0,1)$, $x \mapsto \frac{e^x}{e^x+1}$. Elementary calculus shows that this is a bijection. □

Exercise 4.1. Show that $(0,1) \cong [0,1) \cong (0,1] \cong [0,1]$.

Next, we want to show that $\mathbb{R}$ and $\{0,1\}^{\mathbb{N}}$ have the same cardinality. By the previous proposition and exercise, it suffices to show that $[0,1) \cong \{0,1\}^{\mathbb{N}}$. Let us construct a function $f : [0,1) \to \{0,1\}^{\mathbb{N}}$. We know that every real number $0 \le x < 1$ can be uniquely represented in binary, with possibly infinitely many digits. For example, $1/3 = 0.010101\ldots$ and $1/4 = 0.01$. In case the representation is finite, as for $1/4$, we can always pad it with infinitely many 0's: $1/4 = 0.01000\ldots$. This defines f:

$$f : [0,1) \to \{0,1\}^{\mathbb{N}},\ x \mapsto (a_1, a_2, a_3, \ldots)\ ,$$

where $0.a_1a_2a_3\ldots$ is the unique representation of x in binary.

Is f a bijection? Seems like. But no, it isn't. Clearly, it is injective, since two real numbers $0 \le x < y < 1$ will have two different binary representations. However, f is not surjective, as strings like $(0,1,1,1,1,1,\ldots)$ are not in its image. In fact, every $x \in [0,1)$ has a unique binary representation $x = 0.a_1a_2a_3\ldots$ where this infinite *does not have an infinite tail of* 1*'s.*

Exercise 4.2. Modify the above function f to make it a bijection $[0,1) \to \{0,1\}^{\mathbb{N}}$.

Recall that for a set A, its power set, denoted by 2^A, is the set of all subsets of A. For example, $2^{\{3,4\}} = \{\emptyset, \{3\}, \{4\}, \{3,4\}\}$. It is easy to see that $\{0,1\}^{\mathbb{N}} \cong 2^{\mathbb{N}}$ and thus $2^{\mathbb{N}} \cong \mathbb{R}$.

Exercise 4.3. Prove that $\mathbb{R} \not\cong 2^{\mathbb{R}}$.

5 The Schröder-Bernstein Theorem

It was easy enough to define an injective function $f : [0,1) \to \{0,1\}^{\mathbb{N}}$. Making this function bijective (Exercise 4.2) turned out to be a bit inconvenient. Let's take another way. Can we find an injective function $g : \{0,1\}^{\mathbb{N}} \to [0,1)$? Of course we are tempted to define g by converting a string $(a_1, a_2, \dots)$ into the number it defines, via

$$(a_1, a_2, a_3, \dots) \mapsto \sum_{i=1}^{\infty} a_i 2^{-i} \ .$$

This is, in a way, the "inverse" of f; it maps $(0,1,0,1,0,1,\dots)$ to $1/3$, $(0,1,0,0,\dots)$ to $1/4$ and so on. However, it is not injective, since $(0,0,1,1,1,\dots)$ also gets mapped to $1/4$. The trouble is again caused by strings with an infinite tail of 1's. Here is a simple workaround: take the sequence $(a_1, a_2, \dots)$ and stretch with, filling the gaps with 0's: $(0, a_1, 0, a_2, 0, a_3, \dots)$. Even if $\mathbf{a}$ had an infinite tail of 1's, the new sequence won't, and we can safely convert it into a real number. Formally, we define

$$g : \{0,1\}^{\mathbb{N}} \to [0,1), \ (a_1, a_2, a_3, \dots) \mapsto \sum_{i=1}^{\infty} a_i 4^{-i} \ .$$

Replacing base 2 by base 4 creates "enough space" to make sure no two values of g collide, making g injective. Let us summarize our results:

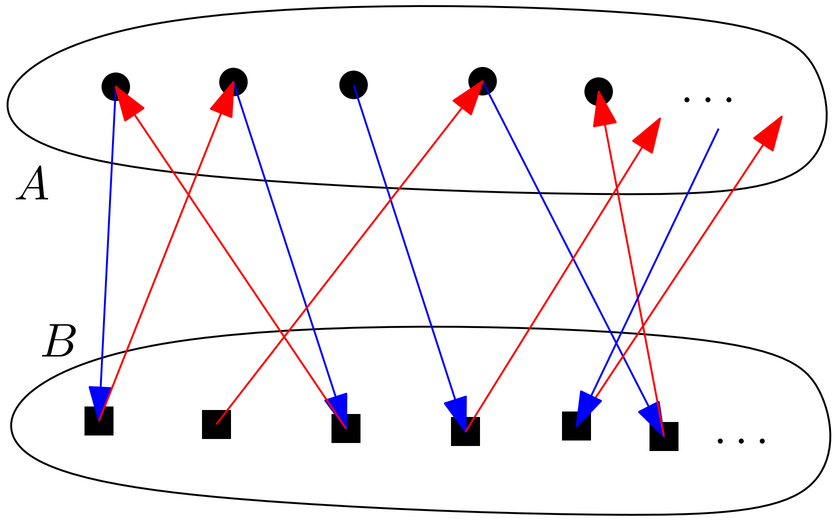
Proposition 7. *The functions $f : [0,1) \to \{0,1\}^{\mathbb{N}}$ and $g : \{0,1\}^{\mathbb{N}} \to [0,1)$ are injections.*

Definition 8. *Let A, B be sets. If there exists an injection $f : A \to B$, we say the cardinality of A is* at most *the cardinality of B and write $A \leq B$ and $B \geq A$.*

We have just showed that $[0,1) \leq \{0,1\}^{\mathbb{N}}$ and $[0,1) \geq \{0,1\}^{\mathbb{N}}$. Surely this implies that their cardinality is equal. Well, not so fast! Don't be fooled by our suggestive notation "$\leq$". For $A \leq B$ and $B \leq A$, it seems obvious that $A \cong B$. But $A \cong B$ means that there is a *bijection* between A and B, and we are only given injections in both directions. Can we always merge those two injections into one bijection? The answer turns out to be yes, but it is not that obvious.

Theorem 9 (Schröder-Bernstein Theorem)**.** *Let A, B be set. If $A \leq B$ and $B \leq A$, then $A \cong B$.*

Proof. What do we have to do? We are given injective functions $f : A \to B$ and $g : B \to A$ and have to construct a bijection $h : A \to B$. To simplify things, we assume that A and B are disjoint, i.e., $A \cap B = \emptyset$. Think about why we can assume this! Let us draw a picture illustrating A, B, f, and g.



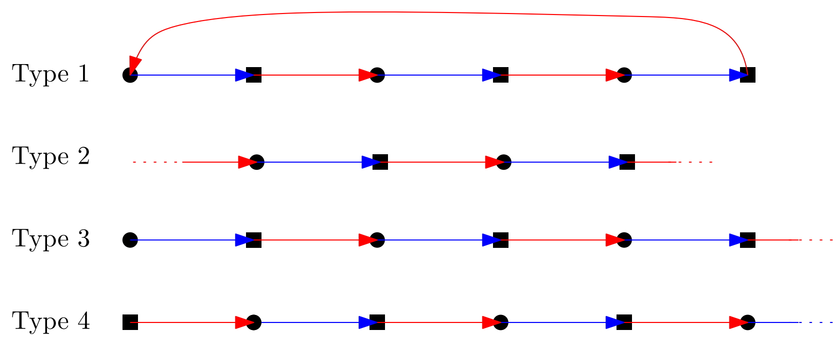
Blue arrows represent f and red arrows represent g. By following the blue and red arrows, we see that $A \cup B$ becomes a collection of "paths". A minute of thought shows that there are four types of "paths":

1. finite paths, which are actually cycles, with the same number of elements in A as in B;

2. bi-infinite paths, extending infinitely in both directions, i.e., looking like $\mathbb{Z}$;

3. infinite paths starting with an element $a \in A$ that has no incoming arrow;

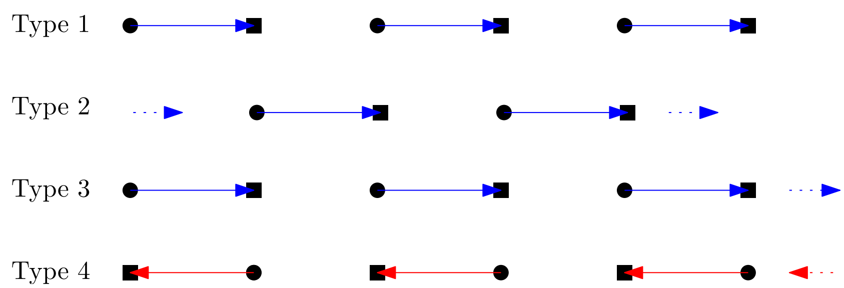
4. infinite paths starting with an element $b \in B$ that has no incoming arrow.



Let A' be the set of all elements $a \in A$ contained in a path of type 1, 2, or 3. Similarly define B' to be the set of all elements $b \in B$ contained in a path of type 1, 2, or 3. Let $A'' := A \setminus A'$ and $B'' := B \setminus B''$. These are the elements contained in a path of type 4. Observe that f defines a bijection $A' \to B'$ and g defines a bijection $B'' \to A''$. In particular it is surjective, meaning that for every $a \in A''$ there is a unique $b \in B''$ such that $g(b) = a$. Thus, we can define $h : A \to B$ via

$$h : A \to B, \ a \mapsto \begin{cases} f(a) & \text{if } a \in A' \ , \\ g^{-1}(a) & \text{else} \quad . \end{cases}$$

In the picture above, the function h would look like this:



Note that we use the red arrows for Type-4-elements but reverse them, i.e., we use g^{-1}. $\square$

If you think the Schröder-Bernstein Theorem is obvious and wonder why we give such a long proof, try to prove, as formally as you can, the following obvious-sounding theorem:

Theorem 10 (Trichotomy Theorem in Set Theory)**.** *Let A, B be sets. Then there exists an injective function $f : A \to B$ or an injective function $g : B \to A$, or both.*

This is called the Trichotomy Theorem because it states that there are only three possibilities: either $A < B$ (meaning $A \leq B$ but not $A \cong B$) or $B < A$ or $A \cong B$.

Indeed, the Trichotomy Theorem is more difficult to prove than the Schröder-Bernstein Theorem, and its proof uses the Axiom of Choice, a set-theoretic axiom which sounds obvious but has counter-intuitive consequences and is considered problematic by some set theorists.