13. To Infinity and Beyond

Cardinality

Terence Sim

Some infinities are bigger than other infinities.

John Michael Green
1977 —
The Fault in Our Stars

Reading

Section 7.4 of Epp.

13.1. Introduction

In today's lesson, you will learn:

1. What counting is
2. How to count to infinity
3. How to compare sizes without counting
4. How some infinities are more infinite than others

Quiz

1. $\infty + 1 =?$
2. $\infty + 10^{10} =?$
3. $\infty + \infty =?$
4. $\infty - \infty =?$
5. $\infty \times \infty =?$

Infinite hotel videos

http://youtu.be/faQBrAQ8714

https://www.youtube.com/watch?v=Uj3_KqkI9Zo

What is counting?

Definition 13.2.1

Let $\mathbb{Z}_n = \{1, 2, 3, \ldots, n\}$ denote the set of positive integers from 1 to n, inclusive.

Counting is the assignment of consecutive elements in $\mathbb{Z}_n$ to the objects being counted.

This assignment is a *bijection*, i.e. every object is assigned exactly one integer. Furthermore, the order of assignment does not matter.

Definition 13.2.2 (Finite)

A set S is said to be finite if, and only if,

(i) S is the empty set; or

(ii) There exists a bijection from S to $\mathbb{Z}_n$ for some $n \in \mathbb{Z}^+$

A set S is said to be infinite if it is not finite.

Definition 13.2.3 (Cardinality)

The cardinality of a finite set S, denoted $|S|$, equals

(i) 0, if $S = \varnothing$; or

(ii) n, if $f : S \to \mathbb{Z}_n$ is a bijection.

We will deal with the cardinality of infinite sets later.

Definition 13.2.4

A set A has the same cardinality as another set B iff there is a bijection from A to B.

We write $|A| = |B|$.

Theorem 7.4.1 (Epp): Cardinality Relation

The cardinality relation is an equivalence relation.
For all sets A, B, C:

1. (Reflexive) $|A| = |A|$.
2. (Symmetric) $|A| = |B| \;\Rightarrow\; |B| = |A|$.
3. (Transitive) $(|A| = |B|) \wedge (|B| = |C|) \;\Rightarrow\; |A| = |C|$.

Proof.

1. (Reflexive) The identity function $\mathcal{I}_A$ provides a bijection from A to A.
2. (Symmetric) Let $|A| = |B|$. This means there exists a bijection, $f : A \to B$. Then by Proposition 7.2.4, $f^{-1} : B \to A$ is a bijection.
3. (Transitive) Let $f : A \to B$ and $g : B \to C$ be bijections. Then $g \circ f : A \to C$ is also a bijection.[1]

[1] Try to prove this!

Example 1: Finite set

Let $A = \{a, b, c\}$. What is $|A|$?

It is easy to construct a bijection $f : A \to \mathbb{Z}_3$. Here's one, shown as a table:

x	f(x)
b	1
a	2
c	3

There are a total of $3! = 6$ possible bijections. Any one is sufficient to show that $|A| = 3$.

Example 2: Even integers

Define $2\mathbb{Z}$ to be the set of even integers. Prove that $2\mathbb{Z}$ has the same cardinality as $\mathbb{Z}$.

Proof.

By definition, we need to show that there exists a bijection from $2\mathbb{Z}$ to $\mathbb{Z}$. Since any bijection will do, we simply construct one, i.e. this is a proof by construction.

Define $f : 2\mathbb{Z} \to \mathbb{Z}$ by $f(n) = n/2$. We need to show that f is bijective.

1. (Injective) $\forall m, n \in 2\mathbb{Z},\ f(m) = f(n)$
   $\Rightarrow m/2 = n/2 \ \Rightarrow m = n$.
2. (Surjective) $\forall n \in \mathbb{Z}$, clearly, $2n \in 2\mathbb{Z}$ and $f(2n) = n$.

Thus $|2\mathbb{Z}| = |\mathbb{Z}|$. QED.

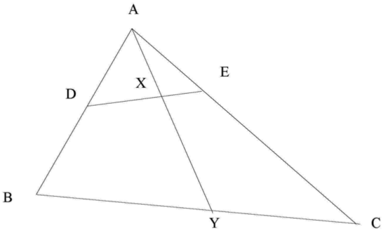
Note that $2\mathbb{Z} \subseteq \mathbb{Z}$ and $2\mathbb{Z} \neq \mathbb{Z}$. Yet $|2\mathbb{Z}| = |\mathbb{Z}|$. This is a strange result!

For a finite set A, any proper subset B of A will have $|B| < |A|$. But this is not true for infinite sets.

Some mathematicians have proposed to use this as the definition of an infinite set. That is, a set A is infinite iff there exists a set B such that $B \subseteq A \wedge B \neq A \wedge |B| = |A|$.

Example 3: Line segments

In the figure below, which line segment, DE or BC, has more points?



Answer: They have the same cardinality! Every point on DE can be paired up with a point on BC, e.g. the points X and Y. This pairing of points is a bijection.

13.3. Infinity

Definition 13.3.1 (Cardinal numbers)

Define $\aleph_0 = |\mathbb{Z}^+|$.

$\aleph$, pronounced "aleph", is the first letter of the Hebrew alphabet. This is the first cardinal number. Others will be defined later.

Definition 13.3.2 (Countably infinite)

A set S is said to be countably infinite (or, S has the cardinality of integers) iff $|S| = |\mathbb{Z}^+| = \aleph_0$.

Definition 13.3.3 (Countable)

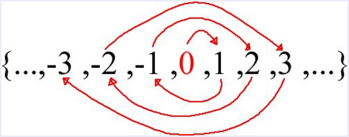
A set S is said to be countable iff it is finite or countably infinite.

A set is said to be uncountable if it is not countable.

Example 4: $\mathbb{Z}$ is countably infinite

Intuitively, $\mathbb{Z}$ contains twice as many numbers as $\mathbb{Z}^+$, so we expect $|\mathbb{Z}| = 2|\mathbb{Z}^+|$. But this is not true. Their cardinalities are equal!

This is how to count them:



That is, define $f : \mathbb{Z}^+ \to \mathbb{Z}$ by:

$$f(n) = \begin{cases} n/2, & \text{if } n \text{ is even} \\ -(n-1)/2, & \text{if } n \text{ is odd} \end{cases}$$

It is straightforward to show that f is a bijection. So, $|\mathbb{Z}| = |\mathbb{Z}^+|$.

Example 5: What about $\mathbb{Z}^+ \times \mathbb{Z}^+$?

What if an infinite number of buses, each carrying an infinite number of guests, arrive at the Infinite Hotel? Is there room for all of them?

	1	2	3	4	
1	(1,1)	(1,2)	(1,3)	(1,4)	$\cdots$
2	(2,1)	(2,2)	(2,3)	(2,4)	$\cdots$
3	(3,1)	(3,2)	(3,3)	(3,4)	$\cdots$
4	(4,1)	(4,2)	(4,3)	(4,4)	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

	1	2	3	4	
1	(1,1)	(1,2)	(1,3)	(1,4)	⋯
2	(2,1)	(2,2)	(2,3)	(2,4)	⋯
3	(3,1)	(3,2)	(3,3)	(3,4)	⋯
4	(4,1)	(4,2)	(4,3)	(4,4)	⋯
⋮	⋮	⋮	⋮	⋮	

Define $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ by:

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

Note that on each diagonal, $m + n$ is constant.

The formula exploits the fact that (m, n) is the m^{th} element on the diagonal where $m + n$ is constant.

Proving that f is bijective is tricky, but can be done. You try it!

As this example shows, finding bijections can be tricky. Proving them can be even trickier. It's time to have some theorems to make life easier.

Proposition 13.3.4 (Listing)

A set A is countably infinite iff its elements can be arranged, without duplication and without omission, in an infinite list $a_1, a_2, a_3, \ldots$.

Proof sketch

Clearly, such as listing is a bijection from $\mathbb{Z}^+$ to A.

Theorem 13.3.5 (Cartesian product)

If sets A and B are both countably infinite, then so is $A \times B$.

Proof sketch

By Proposition 13.3.4, the elements of A and B can be listed, respectively, as: $a_1, a_2, a_3, \ldots$ and $b_1, b_2, b_3, \ldots$.

Then $A \times B$ can be arranged in table form, similar to that in $\mathbb{Z}^+ \times \mathbb{Z}^+$ (slide 18). We can then use the same diagonal counting technique to map each element (a_m, b_n) to some positive integer k. This establishes a bijection from $A \times B$ to $\mathbb{Z}^+$.

Corollary 13.3.6 (General Cartesian product)

Given $n \geq 2$ countably infinite sets $A_1, A_2, \ldots, A_n$, the Cartesian product $A_1 \times A_2 \times \ldots \times A_n$ is also countably infinite.

Proof sketch

This is a proof by induction. The base case was already proven in Theorem 13.3.5.

Theorem 13.3.7 (Unions)

The union of countably many countable sets is countable.

That is, if $A_1, A_2, \ldots$ are all countable sets, then so is

$$A = \bigcup_{i=i}^{\infty} A_i$$

Proof sketch

By Proposition 13.3.4, the elements in each set A_i may be enumerated as $a_{i1}, a_{i2}, a_{i3}, \ldots$. Each element in the union A must come from some A_i, by the definition of union.

...

cont'd

We can therefore enumerate (without duplication or omission) the elements of A in a table:

$$\begin{array}{cccc} a_{11} & a_{12} & a_{13} & \cdots \\ a_{21} & a_{22} & a_{23} & \cdots \\ a_{31} & a_{32} & a_{33} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

Now by the diagonal counting method on page 18, we have our bijection.

Theorem 7.4.3 (Epp): Subset

Any subset of a countable set is countable.

Proof sketch

Let A be a countable set, and $B \subseteq A$.

Case 1, B is finite: Then, B is countable, by definition.

Case 2, B is infinite:

1. This implies A is countably infinite. By Proposition 13.3.4, list the elements of A: $L = a_1, a_2, \ldots$
2. Enumerate the elements of B by sequentially searching list L and selecting only those elements a_k that belong to B.
3. You now have a list for B: $a_{k1}, a_{k2}, \ldots$. By Proposition 13.3.4, B is countably infinite, and hence countable.

Example 6: the set of prime numbers, $\mathbb{P}$

Note: $\mathbb{P} \subseteq \mathbb{Z}^+$

1. List the elements of $\mathbb{Z}^+$:
   $L = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$
2. Mark the elements in L which are prime:
   $L = 1, 2^*, 3^*, 4, 5^*, 6, 7^*, 8, 9, 10, \ldots$
3. Thus, a listing of $\mathbb{P}$ is $2, 3, 5, 7, \ldots$

By Proposition 13.3.4, $\mathbb{P}$ is countably infinite.

Corollary 7.4.4 (Epp)

The superset of an uncountable set is uncountable.

That is, if $B \subseteq A$ is uncountable, then so is A.

Proof.

This is the contra-positive form of Theorem 7.4.3 (Epp).

Example 7: Is $\mathbb{Q}$ countable?

- Compared to integers, rational numbers are "dense", in the sense that given any two distinct rational numbers p, q with $p < q$, there exists another rational number r that is between them: $p < r < q$.
- An example is $r = (p + q)/2$.
- This is not true of integers; there is no integer between 3 and 4, for example. But there are an infinite number of rationals between 3 and 4.
- Surely $|\mathbb{Q}| > |\mathbb{Z}|$?
- Let's find out in 3 steps.

Step 1: Positive rationals

Define $\mathbb{Q}^+ = \{\ (m, n) \mid m, n \in \mathbb{Z}^+\ \wedge\ m, n \text{ are coprime}\}$ to be the set of positive rational numbers.

- Note that usually, a rational number is written as $\frac{m}{n}$, but that is just a notational habit. Here we will use (m, n), for reasons that will become obvious.
- Also, note that our definition of $\mathbb{Q}^+$ requires m and n to be co-prime (i.e. their gcd is 1), meaning that each rational number is already "reduced to lowest terms". For example, the number 0.5 will not be $(2, 4)$ but $(1, 2)$. This ensures that every rational number has a unique representation.
- Clearly, $\mathbb{Q}^+ \subseteq \mathbb{Z}^+ \times \mathbb{Z}^+$.
- Therefore by Theorem 7.4.3 (Epp), $\mathbb{Q}^+$ is countable.

Step 2: Negative rationals

Define $\mathbb{Q}^- = \{\ (-m, n) \mid m, n \in \mathbb{Z}^+ \ \wedge\ m, n$ are coprime$\}$ to be the set of negative rational numbers.

It is easy to define a bijection, $f : \mathbb{Q}^- \to \mathbb{Q}^+$, by $f((-m, n)) = (m, n)$. And thus by Definition 13.2.4, $|\mathbb{Q}^-| = |\mathbb{Q}^+|$, so the set of negative rationals is also countably infinite.

Step 3: Putting it all together

Define the rational number zero by $(0,1)$.

Now define the set of rational numbers by:

$$\mathbb{Q} = \mathbb{Q}^{+} \ \cup \ \{(0,1)\} \ \cup \ \mathbb{Q}^{-}$$

Then, by Theorem 13.3.7, $\mathbb{Q}$ is also countable.

This proves that, contrary to intuition, rational numbers have the same cardinality as integers; that is, $|\mathbb{Q}| = |\mathbb{Z}|$.

13.4. Beyond Infinity

- Q: What's beyond ∞ ?
- A: Larger infinities.
- Q: How many more?
- A: Countably infinitely many!

Theorem 7.4.2 (Epp)

The set of real numbers between 0 and 1, excluding the endpoints:

$$(0,1) = \{ x \in \mathbb{R} \mid 0 < x < 1 \}$$

is uncountable.

To prove that a set is uncountable means proving that there is *no possibility of a bijection* from that set to $\mathbb{Z}^+$. Simply saying, "I can't find a bijection", is not enough, since it could mean I didn't look hard enough, or I'm not smart enough to find one.

The way to prove is by contradiction. Georg Cantor, who gave us set theory, also gave an ingenius proof that $(0,1)$ is uncountable. We now refer to it as Cantor's Diagonalization Argument.

Proof sketch

1. Suppose $(0,1)$ is countable.
2. Since it is not finite, it is countably infinite.
3. By Proposition 13.3.4, the elements of $(0,1)$ can be listed in a sequence.

$$
\begin{aligned}
x_1 =&\quad 0.a_{11}a_{12}a_{13}\dots a_{1n}\dots\\
x_2 =&\quad 0.a_{21}a_{22}a_{23}\dots a_{2n}\dots\\
x_3 =&\quad 0.a_{31}a_{32}a_{33}\dots a_{3n}\dots\\
\vdots =&\qquad\qquad\quad \vdots\\
x_n =&\quad 0.a_{n1}a_{n2}a_{n3}\dots a_{nn}\dots\\
\vdots =&\qquad\qquad\quad \vdots
\end{aligned}
$$

where each $a_{ij} \in \{0,1,\dots,9\}$ is a single digit.[2]

[2]Note that some numbers have two representations, e.g. $0.499\ldots = 0.500\ldots$. We agree to use only the latter representation.

Proof cont'd

4. Construct a number $d = 0.d_1 d_2 d_3 \ldots d_n \ldots$ such that

$$d_n = \begin{cases} 1, & \text{if } a_{nn} \neq 1; \\ 2, & \text{if } a_{nn} = 1. \end{cases}$$

5. Note that $\forall n \in \mathbb{Z}^+, d_n \neq a_{nn}$. Thus, $d \neq x_n$, $\forall n \in \mathbb{Z}^+$.
6. But clearly, $d \in (0, 1)$, resulting in a contradiction. QED.

In other words, we constructed a new number $d \in (0, 1)$ that differs from x_1 in the first digit, from x_2 in the second digit, from x_3 in the third digit, etc.

Clearly, this d is *not* in the list. Yet d is in the set, resulting in a contradiction.

Example 8: Illustrating Cantor's argument

0. 2 0 1 4 8 8 0 2 ...	d_1 is 1 because $a_{11} = 2 \neq 1$
0. 1 1 6 6 6 0 2 1 ...	d_2 is 2 because $a_{22} = 1$
0. 0 3 3 5 3 3 2 0 ...	d_3 is 1 because $a_{33} = 3 \neq 1$
0. 9 6 7 7 6 8 0 9 ...	d_4 is 1 because $a_{44} = 7 \neq 1$
0. 0 0 0 3 1 0 0 2 ...	d_5 is 2 because $a_{55} = 1$

Hence, $d = 0.\ 1\ 2\ 1\ 1\ 2\ \ldots$, which is not in the list. That is, the list is incomplete. This is true no matter how the elements in $(0, 1)$ are listed.

Proposition 13.4.1 ($\mathbb{R}$ is uncountable)

Proof.

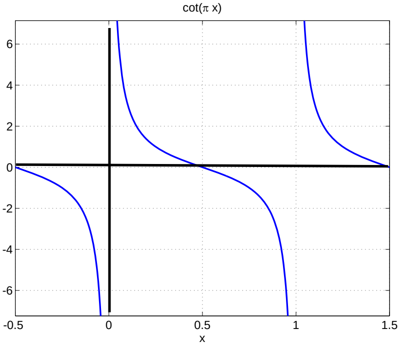
Since $(0, 1) \subseteq \mathbb{R}$ is uncountable, then by Corollary 7.4.4 (Epp), $\mathbb{R}$ is uncountable.

If $|A| = |\mathbb{R}|$, we say that A has the cardinality of the continuum, a phrase coined by Cantor.

Proposition 13.4.2 ($|(0,1)| = |\mathbb{R}|$)

Proof.

Define the bijection, $h : (0,1) \to \mathbb{R}$ by $h(x) = \cot(\pi x)$. By Definition 13.2.4, they have the same cardinality. QED.



Definition 13.4.3

Let A, B be sets.
If $|A| < |B|$, then there exists an injection $f : A \to B$, but no surjection $g : A \to B$.

Theorem 13.4.4 (Cardinality of Power set)

If A is any set, then $|A| < |\mathcal{P}(\mathcal{A})|$.

Proof.

1. Using Definition 13.4.3, we need to show that there exists an injection $f : A \to \mathcal{P}(A)$, but no surjection $g : A \to \mathcal{P}(A)$.
2. Define $f(x) = \{x\}$. This function maps $x \in A$ to the singleton set $\{x\} \in \mathcal{P}(A)$. To prove it is injective:
   (a) Suppose $f(x) = f(y)$.
   (b) Then, $\{x\} = \{y\}$.
   (c) By Definition 6.3.2 (Set Equality), $x = y$.
   QED.
3. We prove there is no surjection by contradiction.
   (a) Suppose there is a surjection $g : A \to \mathcal{P}(A)$.
   (b) This function maps $x \in A$ to $g(x) \in \mathcal{P}(A)$. That is, $g(x)$ is a subset of A.

...

Proof cont'd

3. Cont'd.
   (c) Define $B = \{x \in A \mid x \notin g(x)\}$.
   (d) Clearly, $B \subseteq A$, so that $B \in \mathcal{P}(A)$.
   (e) Since g is surjective, there exists $a \in A$ such that $g(a) = B$.
   (f) Question: $a \in B$ or $a \notin B$?

   Case 1: If $a \in B$, then the definition of B implies $a \notin g(a)$, and since $g(a) = B$ we get $a \notin B$. Contradiction.

   Case 2: If $a \notin B$, then the definition of B implies $a \in g(a)$, and since $g(a) = B$ we get $a \in B$. Again, contradiction.

   (g) Therefore there is no surjection $g : A \to \mathcal{P}(A)$.
4. Therefore, $|A| < |\mathcal{P}(A)|$. $\blacksquare$

Countably infinite number of infinities

Using Theorem 13.4.4, we can construct the following chain of infinite cardinalities.

$$\aleph_0 = |\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)| < |\mathcal{P}(\mathcal{P}(\mathbb{Z}^+))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{Z}^+)))| < \dots$$

The set $\mathbb{Z}^+$ is countable; all the others are uncountable.

Furthermore, it is clear that the set containing all the infinite sets produced in this manner has the cardinality of integers. That is, there are (at least) countably infinitely many infinities.

There *could* be even more infinities than these. That is, the set of infinite sets could well be uncountable. We just haven't found them yet!

Theorem 13.4.5

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{Z}^+)|$$

Proof.

We omit the long and complicated proof.

The Continuum Hypothesis

Cantor himself wondered if there exists a set A such that:

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

- In 1964, Paul Cohen proved that the Continuum Hypothesis is *undecidable*; it is independent of ZFC set theory.
- In other words, the existence of such a set A cannot be settled without adding new axioms to standard mathematics. You can assume either way without causing a contradiction!
- Assuming the Hypothesis is false (no such A), we can then define cardinal numbers as follows:

$$\aleph_1 = 2^{\aleph_0}, \aleph_2 = 2^{\aleph_1}, \aleph_3 = 2^{\aleph_2}, \ldots, \aleph_{k+1} = 2^{\aleph_k}, \ldots$$

This is called the Generalized Continuum Hypothesis.

Buzz Lightyear's last word

They even created a new dance for me:
`https://youtu.be/Jo0mZk4qxK8`