LECTURE 4

1 Cardinality

My goal for us is to get the big picture about cardinality. In particular I want you to learn the meaning of the terms "finite", "denumerable", "countable" and "infinite". I want you to gain a deeper appreciation for the difference between real and rational numbers.

1.1 one-one correspondence and finite sets

Definition 1.1 (equivalent sets). *Two sets A and B are said to be* **equivalent** *iff there exists a one-one correspondence between them. In the case that there exists a bijection from A to B we say that $A \cong B$.*

We can easily show that $\cong$ forms an *equivalence relation* on the "class" of all sets. Notice we did not say "set of all sets". We should avoid the tiresome question: "does the set of all sets contain itself?".

Example 1.2 (finite sets). *Consider a set $A = \{1, \emptyset, dora\}$. This is equivalent to the set $\{1, 2, 3\}$. To prove this construct the mapping*

$\boxed{f(1) = 1,\ f(\emptyset) = 2,\ f(dora) = 3}$

$$\cancel{\Psi(1) = 1, \quad \Psi(\emptyset) = 2, \quad \Psi(3) = dora}$$

it is clear this is both one-one and onto $\{1, 2, 3\}$. You might object that these are not the "same" sets. I agree, but I didn't say they were the same, I said they were **equivalent** *or perhaps it is even better to say that the sets are in* **one-one correspondence**.

Now I repeat the same idea for an arbitrary finite set which has k things in it. Let $\mathbb{N}_k = \{1, 2, \ldots, k\}$. If a set A has k distinct objects in it then it is easy to prove it is equivalent to $\mathbb{N}_k = \{1, 2, \ldots, k\}$. Lable these k objects $A = \{a_1, a_2, \ldots a_k\}$ then there is an obvious bijection,

$$\Psi(a_j) = j \text{ for each } j \in \mathbb{N}_k$$

The mapping Ψ is one-one since for $a_j, a_l \in \mathbb{N}_k$ we find $\Psi(a_j) = \Psi(a_l)$ implies $j = l$ implies $a_j = a_l$.

I claim the mapping Ψ is also onto. Let $y \in \mathbb{N}$ then by definition of $\mathbb{N}_k$ we have $y = j$ for some $j \in \mathbb{N}$ with $1 \leq j \leq k$. Observe that $a_j \in A$ since $1 \leq j \leq k$, and $\Psi(a_j) = j$.

Given the last example, you can appreciate the following definition of **finite**.

Definition 1.3 (finite set, cardnality of finite set). *A set S is said to be* **finite** *iff it is empty $S = \emptyset$ or in one-one correspondence with $\mathbb{N}_k$ for some $k \in \mathbb{N}$. Moreover, if $S \cong \mathbb{N}_k$ we define the* **cardinality** *of A to be $\overline{\overline{A}} = k$. If $S = \emptyset$ then we define $\overline{\overline{A}} = 0$.*

To summarize, the cardality of a finite set is the number of elements it contains. The nice thing about finite sets is that you can just count them.

$\text{card}(A) = \overline{\overline{A}}$

$A \subseteq S$ is proper if $A \neq S$

1.2 one-one correspondence and infinite sets

Definition 1.4 (infinite sets). *A set S is infinite if it is not finite.*

Proposition 1.5. *A finite set is not equivalent to any of its proper subsets.*

A proper subset $A \subset B$ will be missing something since a "proper subset" A is a subset which is not the whole set B. It follows that B must have more elements and consequently $A \cong \mathbb{N}_a$ and $B \cong \mathbb{N}_b$ where $a < b$. The contrapositive[1] of the Proposition above is more interesting.

Proposition 1.6. *A set which is equivalent to one or more of its proper subsets is infinite.*

So if you were counting, there are two nice ways to show a set is infinite. First, you could assume it was finite and then work towards a contradiction. Second, you could find a bijection from the set to some proper subset of itself.

Example 1.7 ($\mathbb{N}$ is infinite). *Observe that the mapping $f : \mathbb{N} \to 2\mathbb{N}$ defined by $f(n) = 2n$ is a bijection. First, observe*

$$f(x) = f(y) \quad \Rightarrow \quad 2x = 2y \quad \Rightarrow \quad x = y$$

therefore f is injective. Next $2\mathbb{N} = \{2k \mid \exists k \in \mathbb{N}\}$. Let $y \in 2\mathbb{N}$ then there exists $k \in \mathbb{N}$ such that $y = 2k$. Observe that

$$f(k) = 2k = y$$

thus f is onto $2\mathbb{N}$. Therefore $\mathbb{N} \cong 2\mathbb{N}$ and since $2\mathbb{N}$ is a proper subset of $\mathbb{N}$ it follows that $\mathbb{N}$ is infinite.

1.3 countably infinite sets

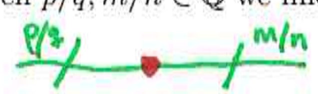
Aleph-not : $\aleph_0$

Definition 1.8 (denumerable). *Let S be a set, we say S is* **denumerable** *iff $S \cong \mathbb{N}$. The cardnality of $S \cong \mathbb{N}$ is said to be $\aleph_o$. We denote $\overline{\overline{S}} = \aleph_o$ iff $S \cong \mathbb{N}$.*

The following is a list of sets with cardnality $\aleph_o$,

$$\mathbb{N},\ 2\mathbb{N},\ 3\mathbb{N},\ \mathbb{Z},\ 2\mathbb{Z},\ \mathbb{N}\times\mathbb{N},\ \mathbb{N}^{123},\ \{x \in \mathbb{R} \mid \sin(x) = 0\},\ \left\{\frac{2}{n} \mid n \in \mathbb{N}\right\}$$

I don't find any of the examples above too surprising. These are all manifestly discrete sets. If you visualize them there is clearly gaps between adjacent values in the sets. In contrast, think about the rational numbers. Given any two rational numbers we can always find another in between them: given $p/q, m/n \in \mathbb{Q}$ we find



$$\frac{1}{2}\left(\frac{p}{q} + \frac{m}{n}\right) = \frac{1}{2}\left(\frac{pn + qm}{nq}\right) \in \mathbb{Q}$$

at the midpoint between p/q and m/n on the number line. It would seem there are more rational numbers then natural numbers. However, things are not always what they "seem". Cantor gave a

[1]in logic the contrapositive of P implies Q is that not Q implies not P. In symbols, $P \Rightarrow Q$ iff $\sim Q \Rightarrow \sim P$ where we denote the negation of P by $\sim P$. Here P is the statement " a finite set " whereas Q is the statement " set is not equivalent to any of its proper subsets". So, $\sim Q$ is that there exists a proper subset for which the set is equivalent and $\sim P$ is that the set is infinite.

not hard to show that f is invertible, so $\text{card}(\mathbb{N}) = \text{card}(\mathbb{Z})$. Therefore, by the definition, both $\mathbb{N}$ and $\mathbb{Z}$ are infinite sets.

Before we investigate another example, we propose another definition which will be helpful.

Definition 2.3. *We say that a set X is* countable *if* $\text{card}(X) \leq \text{card}(\mathbb{N})$. *When* $\text{card}(X) = \text{card}(\mathbb{N})$ *we say X is* countably infinite. *When* $\text{card}(X) < \text{card}(\mathbb{N})$ *we have that X is a finite set. If* $\text{card}(X) > \text{card}(\mathbb{N})$, *then X is* uncountable.

Notice that countable sets are exactly those which can be (in theory) listed off. If $\text{card}(X) = \text{card}(\mathbb{N})$, then there is an invertible function $f : \mathbb{N} \to X$. So for each $x \in X$ there is a unique $n \in \mathbb{N}$ such that $f(n) = x$ (n exists because f is onto, it is unique because f is one-to-one). Thus we can write $x = f(n) = x_n$. In other words, $X = \{x_0, x_1, x_2, \ldots\}$. Conversely, if we can list off a set $X = \{x_0, x_1, x_2, \ldots\}$, then we get a one-to-one function $f : X \to \mathbb{N}$ defined by $f(x_n) = n$, so that $\text{card}(X) \leq \text{card}(\mathbb{N})$ (with equality if X is infinite).

Now let's consider another mapping which may seem even more impossible. Recall that the rational numbers are defined as $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z} \text{ and } q \neq 0\}$. Is it possible that there is a one-to-one and onto function mapping between $\mathbb{N}$ and $\mathbb{Q}$? Since $\mathbb{N}$ is sparse on the number line (i.e., for any $n \in \mathbb{N}$, there are no natural numbers between n and $n+1$) and $\mathbb{Q}$ is dense (i.e., for any distinct $a, b \in \mathbb{Q}$, there exists an infinite number of rational numbers between a and b), it certainly seems improbable that such a mapping may exist. However, let us look at the figure below.

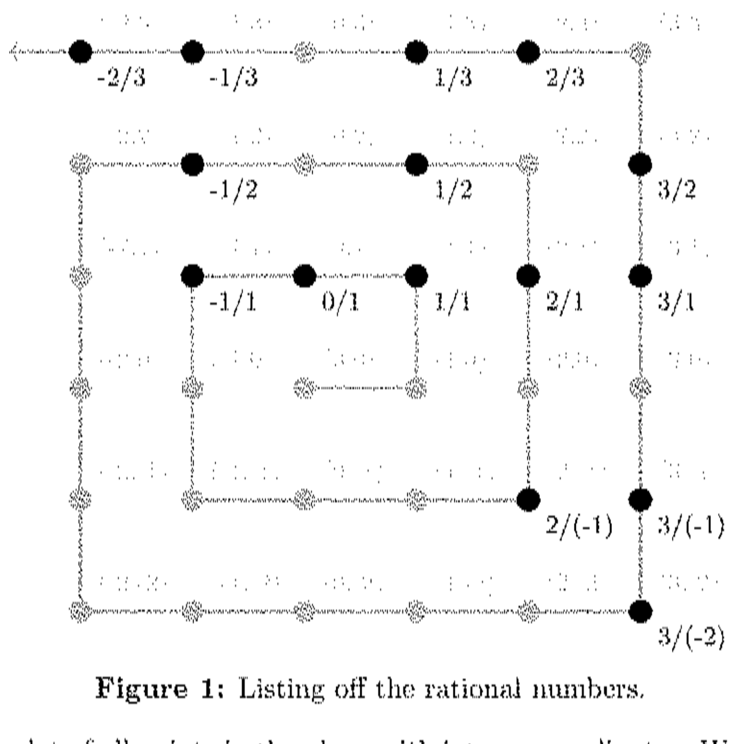


Figure 1: Listing off the rational numbers.

Here we have a plot of all points in the plane with integer coordinates. We start at the origin and spiral outward as shown above. Notice that the spiral hits a sequence of coordinates which can be likened to fractions: $(x, y) \to \frac{x}{y}$. To get the enumeration we desire, we need to make two additional rules. First, we skip over the x-axis since $x/0$ is not a rational number. Second, if we have already encountered a corresponding rational number, we skip over that redundant point.

bijection between $\mathbb{N}$ and postive rational numbers (see the Additional Reading folder, the explicit map is in my brother's paper on *Types of Infinity*, see pages 2-3.). Once you have that it's not hard to prove

$$\boxed{\overline{\overline{\mathbb{Q}}} = \aleph_o.}$$

Sometimes people say a denumerable set is being "countably infinite".

Definition 1.9 (countable). *A set S is said to be* **countable** *iff S is finite or denumerable. If a set S is not countable then it is said to be* **uncountable**.

Be warned that Pete Clark's articles posted in Additional Reading use *Countable* in place of *Countably Infinite*.

1.4 uncountably infinite sets

The title of this section is somewhat superfluous since every uncountable set is necessarily infinite. Uncountable sets are quite common.

Theorem 1.10. *The open interval $(0,1)$ is uncountable.*

The proof, basically it stems from the decimal expansion of the real numbers (see the Additional Reading folder, the explicit map is in my brother's paper on *Types of Infinity*, see Theorem 2.5.).

The result above assures us the following definition is worthwhile:

Definition 1.11 (continuum c). *We define the cardnality of the open interval $(0,1)$ to be c.*

The proof $(0,1)$ is uncountable is not too easy, but once you have the unit interval it's easy to get other subsets of $\mathbb{R}$.

Example 1.12. *Show $(0,1) \cong (5,8)$. To do this we want a one-one mapping that takes $(0,1)$ as its domain and $(5,8)$ as its range. A line segment will do quite nicely. Let $f(x) = mx + b$ and fit the points*

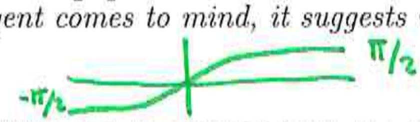
$$f(0) = 5 = b, \quad f(\overset{1}{5}) = \cancel{5}m + 5 = 8 \qquad f(0,1) \simeq (5,8)$$

Clearly $f(x) = \frac{3}{\cancel{5}}x + 5$ will provide a bijection of the open intervals. Its not hard to see this construction works just the same for any open interval (a,b). Thus the cardnality of any open interval is c.

There are bijections from the open interval to closed intervals and half-open half-closed intervals not too mention unions of such things. These mappings are not always as easy to find.

Example 1.13. *Show $(0,1) \cong \mathbb{R}$. First observe that $(0,1) \cong (-\frac{\pi}{2}, \frac{\pi}{2})$ thus by transitivity of $\cong$ is suffices to show that $(-\frac{\pi}{2}, \frac{\pi}{2}) \cong \mathbb{R}$. The graph of inverse tangent comes to mind, it suggests we use*

$$f(x) = \tan^{-1}(x)$$



This mapping has $dom(f) = \mathbb{R}$ and $range(f) = (-\frac{\pi}{2}, \frac{\pi}{2})$. This can be gleaned from the relation between a function and its inverse. The vertical asymptotes of tangent flip to become horizontal tangents of the inverse function. Notice that

$$f(a) = f(b) \;\Rightarrow\; \tan^{-1}(a) = \tan^{-1}(b) \;\Rightarrow\; a = b$$

by the graph and definition of inverse tangent. Also, if $y \in (-\frac{\pi}{2}, \frac{\pi}{2})$ then clearly $f(\tan(y)) = y$ hence f is onto.

If you can find me an explicit formula showing $[a, b)$ is equivalent to $[a, b]$ it would be worth some points.

1.5 Cantor's Theorem and transfinite arithmetic

Definition 1.14. *Let A and B be sets. Then*

(1.) $\overline{\overline{A}} = \overline{\overline{B}}$ *iff* $A \cong B$, *otherwise* $\overline{\overline{A}} \neq \overline{\overline{B}}$

(2.) $\overline{\overline{A}} \leq \overline{\overline{B}}$ *iff there exists an injection* $f : A \to B$

(3.) $\overline{\overline{A}} < \overline{\overline{B}}$ *iff* $\overline{\overline{A}} \leq \overline{\overline{B}}$ *and* $\overline{\overline{A}} \neq \overline{\overline{B}}$

$\overline{\overline{A}} \leq \overline{\overline{\mathcal{P}(A)}}$

$f(x) = \{x\} \in \mathcal{P}(A)$

Notice that the injection took A as its domain. The direction is important here, it is not assumed that $f(A) = B$ in part (2.). Thus, while we can form an inverse function from $range(f)$ to A that will not be a bijection from B to A since $range(f)$ may not equal B in general. Transfinite arithmetic enjoys many of the same rules as ordinary arithmetic, see the papers in Additional Reading for more if you're interested.

Theorem 1.15 (Cantor's Theorem). *For every set A, $\overline{\overline{A}} < \overline{\overline{\mathcal{P}(A)}}$.*

$\overline{\overline{\mathbb{N}}} < \overline{\overline{\mathcal{P}(\mathbb{N})}}$

It then follows that we have an unending string of infinities:

$$\aleph_o = \overline{\overline{\mathbb{N}}} < \underset{c}{\overline{\overline{\mathcal{P}(\mathbb{N})}}} < \overline{\overline{\mathcal{P}(\mathcal{P}(\mathbb{N}))}} < \overline{\overline{\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))}} < \cdots$$

An obvious question to ask is "where does the continuum c fit into this picture? It can be shown that $\aleph_o < c$. To see this, note $\aleph_o \leq c$ since $\mathbb{N} \subseteq \mathbb{R}$ we can restrict the identity function to an injection from $\mathbb{N}$ into $\mathbb{R}$ and since $\mathbb{R}$ is not equivalent to $\mathbb{N}$ we have that $\aleph_o < c$.

Theorem 1.16 (Cantor-Schröder-Bernstein Theorem). *If $\overline{\overline{A}} \leq \overline{\overline{B}}$ and $\overline{\overline{B}} \leq \overline{\overline{A}}$, then $\overline{\overline{A}} = \overline{\overline{B}}$.*

This is a non-trivial Theorem despite it's humble appearance. A proof written by my brother is posted in the Additional Reading folder. Its proof is also in one of Pete Clark's articles.

Application of Theorem: We can show $\overline{\overline{\mathcal{P}(\mathbb{N})}} \leq \overline{\overline{(0,1)}}$ and $\overline{\overline{\mathcal{P}(\mathbb{N})}} \geq \overline{\overline{(0,1)}}$. Thus $\overline{\overline{\mathcal{P}(\mathbb{N})}} = \overline{\overline{(0,1)}} = c$.

Note to Self: the phrase "we" means students in the sentence above. Turn this into a homework problem.

Definition 1.17 (trichotomy property of $\mathbb{N}$). *If $m, n \in \mathbb{N}$ then $m > n$, $m = n$, or $m < n$*

The following is called the **Comparability Theorem**:

Theorem 1.18. *If A and B are any two sets, then $\overline{\overline{A}} > \overline{\overline{B}}$, $\overline{\overline{A}} = \overline{\overline{B}}$, or $\overline{\overline{A}} < \overline{\overline{B}}$.*

It turns out that it is impossible to prove this Theorem in the Zermelo Fraenkel set theory unless we assume the Axiom of Choice is true.

Axiom of Choice: If $\mathcal{A}$ is a collection of non-empty sets, then there exists a function F (the **choice** function) from $\mathcal{A}$ to $\cup_{A \in \mathcal{A}} A$ such that for every $A \in \mathcal{A}$ we have $F(A) \in A$.

This axiom does lead to some unusual results. For example, the Banach-Tariski paradox which says that a ball can be cut into pieces and reassembled into two balls such that the total volume is doubled. (don't worry these "cuts" are not physically reasonable). Or the weird result that every subset of $\mathbb{R}$ can be reordered such that it has a smallest element.

Theorem 1.19. *If there exists a function from a set A onto a set B, then $\overline{\overline{B}} \leq \overline{\overline{A}}$.*

Notice surjectivity suggests that there is at least one thing in the domain to map to each element in the range B. It could be the case that more than one thing maps to each element in B, but certainly at least one thing in A maps to a given element in B. If the fibers in A are really "big" then inequality in the Theorem would become a strict $<$. ~~The proof of this Theorem given in the text involves choosing something in the fiber.~~

Remark 1.20. Confession: *we used the axiom of choice in Lecture 3 when we constructed S to create the injective function related an arbitrary function $f : A \to B$. In principle there were infinitely many fibers, we claimed that there existed a section that cut through the fibers such that each fiber was intersected just once. The choice function gives us the existence of such a section. Notice the non-constructive nature of that particular corner of the argument. We have no specific mechanism to select an element of the fiber. Now for particular examples the choice function can be explicitly constructed and in such a context we wouldn't really insist we were relying on the Axiom of Choice.*

Remark 1.21 (Continuum Hypothesis). *The* **Continuum Hypothesis** *states that c is the next transfinite number beyond $\aleph_o$. There is no other infinite set between the rationals and the reals. This was conjectured by Cantor, but only later did the work of Godel(1930's) and Cohen(1960's) elucidate the issue. Godel showed that the Continuum Hypothesis was* **undecidable** *but relatively consistent in Zermelo Frankael set-theory. Then later Paul Cohen showed that the Continuum Hypothesis was independent of the Axiom of Choice relative to Zermelo-Frankael set theory modulo the Axiom of Choice. The Continuum Hypothesis and the Axiom of Choice continue to be widely believed since they are important "big guns" for certain crucial steps in hard theorems.*

Well, I hope you don't let this Lecture influence your expectations of my expectations for other Lectures too much. I have taken a very laid-back attitude about proofs here. I will be more careful generally. This material is more about being "well-rounded" mathematically speaking.

Following these rules, we obtain a list $1, 0, -1, -2, 2, 1/2, -1/2$ etc., so the mapping $0 \mapsto 1$, $1 \mapsto 0$, $2 \mapsto -1$, etc. gives us a function from $\mathbb{N}$ to $\mathbb{Q}$. This function is one-to-one because we skip over any rational number we have already seen, and it is onto because every rational number can be expressed as x/y for some integers x and y (i.e., we will eventually see any element of $\mathbb{Q}$). Therefore, $\mathbb{N}$ and $\mathbb{Q}$ are both infinite and $\text{card}(\mathbb{N}) = \text{card}(\mathbb{Q})$. This means that $\mathbb{Q}$ is countable – although we suggest that you not try doing so. However, if you did, it is no more difficult than counting all the elements in $\mathbb{N}$. We might also note that this way of listing $\mathbb{Q}$, unlike the way we list $\mathbb{N}$, has nothing to do with the natural $<$ ordering of real numbers.

It is now time to name $\text{card}(\mathbb{N})$. We call it it Aleph null or $\aleph_0$ (Aleph is the first letter of the Hebrew alphabet). In fact, $\aleph_0$ is the smallest cardinality for infinite sets. If we allow $\mathbb{A}$ to denote that algebraic numbers (i.e., the set of all roots of polynomials with rational coefficients), we can state that $\text{card}(\mathbb{N}) = \text{card}(\mathbb{E}) = \text{card}(\mathbb{Z}) = \text{card}(\mathbb{Q}) = \text{card}(\mathbb{A}) = \aleph_0$. In other words, $\mathbb{N}$, $\mathbb{E}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{A}$ (as well as many other sets) are all infinite with the same cardinality of $\aleph_0$.

It would now be quite intuitive to believe that there is only one cardinality for all infinite sets. In order to investigate this further, let us define power sets. Given any set X, its power set, $\mathcal{P}(X)$ is the set of all of the subsets of X. For instance, let $X = \{a, b, c\}$. Then $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ where $\emptyset = \{\}$ is the empty set (i.e., the set with no elements). A few more examples would quickly verify that, if $\text{card}(X) = n$, then $\text{card}(\mathcal{P}(X)) = 2^n$. This leads immediately to Cantor's famous theorem.

Theorem 2.4. *Let X be any set and let $\mathcal{P}(X)$ denote the power set of X. Then* $\text{card}(X) < \text{card}(\mathcal{P}(X))$. *In other words, the power set of X is always larger than X itself.*[2]

Cantor's theorem tells us that for any set X: $\text{card}(X) < \text{card}(\mathcal{P}(X)) < \text{card}(\mathcal{P}(\mathcal{P}(X))) < \cdots$ and so, in particular, $\text{card}(\mathbb{N}) < \text{card}(\mathcal{P}(\mathbb{N})) < \text{card}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) < \cdots$. Since $\text{card}(\mathbb{N}) = \aleph_0$ is countable infinity, $\text{card}(\mathcal{P}(\mathbb{N}))$ must an uncountable infinity. This also establishes that there are infinitely many distinct infinite cardinalities and that no matter how big our set is, its power set is even larger. What is truly intriguing – and beyond the scope of this paper – is that some collections are too large to be sets! There is no such thing as the "set of all sets". Assuming the existence of such an object leads to a contradiction. We leave it to the interested reader to investigate this further [Halmos, 2011]. Wait! Did you see it? If $\aleph_0 = \text{card}(\mathbb{N}) < \text{card}(P(\mathbb{N}))$, then there must be something larger than $\aleph_0$. Let us now use Cantor's diagonalization argument to show that $\mathbb{R}$ is uncountable (i.e., $\text{card}(\mathbb{N}) < \text{card}(\mathbb{R})$).

Theorem 2.5. *The set of real numbers is uncountable.*

Proof: For sake of contradiction, suppose that $\mathbb{R}$ is countable. Therefore, every subset of $\mathbb{R}$ is countable and in particular, $I = [0, 1)$ is countable. This means we can list the elements of I say $I = \{x_1, x_2, x_3, \ldots\}$.

Next, every real number has a decimal expansion. In fact, it has a unique decimal expansion if we do not allow trailing 9's (for example, $12.3\bar{9} = 12.4$). Consider $x_j \in I$ so that $0 \le x_j < 1$. Expand x_j (without trailing 9's) and get $x_j = \underline{0.d_{j1}d_{j2}d_{j3}\cdots = d_{j1}10^{-1} + d_{j2}10^{-2} + d_{j3}10^{-3} + \cdots}$ where each digit $d_{ij} \in \{0, 1, \ldots, 9\}$. Now focus on the i^{th} decimal digit of the i^{th} number in our

[2] The proof of this theorem (which we omit) is surprisingly simple and uses an ingenious "self-referencing" trick.

list:

$$\begin{aligned} x_1 &= 0.d_{11}d_{12}\,d_{13}\,d_{14}\ldots \\ x_2 &= 0.\,d_{21}d_{22}d_{23}\,d_{24}\ldots \\ x_3 &= 0.\,d_{31}\,d_{32}d_{33}d_{34}\ldots \\ &\ \ \vdots \end{aligned}$$

Define y_i to be 1 if $y_i = 0$ and $y_i = d_{ii} - 1$ otherwise. Then $y = 0.y_1y_2y_3\ldots$ is a real number in $I = [0, 1)$. We chose y's digits so that it does not end in trailing 9's (this also keeps us from getting $0.\overline{9} = 1$).

Notice that $y \neq x_i$ for each $i = 1, 2, \ldots$ since y and x_i have differing i^{th} digits. Thus y is not on the list and so our list is incomplete (contradiction). ♦

Another way to establish that $\mathbb{R}$ is uncountable is to show $\mathrm{card}(\mathbb{R}) = \mathrm{card}(\mathcal{P}(\mathbb{N}))$.[3] This again shows that $\mathbb{R}$ is strictly larger than $\mathbb{N}$. We call the cardinality of the real numbers *continuum* and denote it by $\mathrm{card}(\mathbb{R}) = \mathrm{card}(\mathcal{P}(\mathbb{N})) = 2^{\aleph_0}$.

Again, recall that $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is the set of integers and since we can list them off: $0, -1, 1, -2, 2, -3, 3, \ldots$ we know that $\mathbb{Z}$ is countable. As we have seen, $\mathbb{Q}$ is also countable, as we already listed them off. In fact, from our enumeration of $\mathbb{Q}$ we may have already anticipated that $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(p, q) \mid p, q \in \mathbb{Z}\}$ is countable: $\mathrm{card}(\mathbb{Z}^2) = \mathrm{card}(\mathbb{N})$. To show this concretely, plot the elements of $\mathbb{Z}^2$ as grid points in the plane and then list them off by spiraling outward.

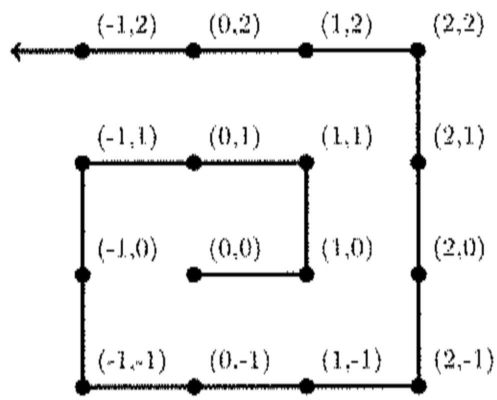


Figure 1: $\mathbb{Z}^2 = \{(0,0), (1,0), (1,1), (0,1), (-1,1), \ldots\}$ is countable.

Similarly, recalling that $\mathbb{N} = \{0, 1, 2, \ldots\}$, one can show that $f : \mathbb{N}^2 \to \mathbb{N}$ defined by $f(x, y) = \dfrac{1}{2}(x^2 + 2xy + y^2 + 3x + y)$ is an invertible function so that $\mathrm{card}(\mathbb{N}^2) = \mathrm{card}(\mathbb{N})$.

More generally, for non-empty sets X and Y where at least one is infinite, one can show that the cardinality of $X \times Y$ is the same as the maximum of the cardinalities of X and Y (this is

[3] Without getting into the details of such a proof, here is the idea: First, one can find an invertible function between $\mathbb{R}$ and the interval $I = [0, 2]$ so that $\mathbb{R}$ and I have the same cardinality. Next, each element of $b \in I$ can be represented in a binary expansion: $b = b_0.b_1b_2\cdots = b_0 2^0 + b_1 2^{-1} + b_2 2^{-2} + \cdots$ each binary digit b_i being either 0 or 1. Create a set $B = \{k \in \mathbb{N} \mid b_k = 1\}$. So each element of I is associated with a subset of $\mathbb{N}$. With a little effort one can show this association is one-to-one and onto.