CS 4510 Automata and Complexity February 27th 2023

Lecture 12: Countability

Lecturer: Abrahim Ladha *Scribe(s): Rishabh Singhal*

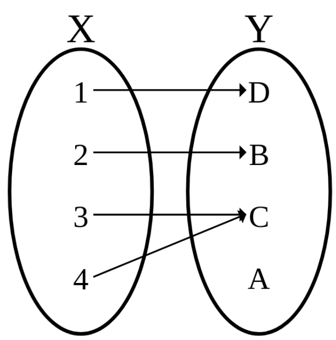
1 Introduction

Infinity used to be just a figure of speech, or perhaps a useful abstraction, not a real thing. In the late 19th and early 20th centuries, Georg Cantor undertook a serious attempt to formalize and understand the infinite, generalizing ideas from finite sets to infinite ones.

We denote the cardinality of the set S as $|S|$. If S is finite then $|S|$ is just the size. But what is the cardinality of the natural numbers $|\mathbb{N}|$? Certainly for all finite sets F, it is true that $|F| < |\mathbb{N}|$. When we talk about the cardinality of infinite sets, we want to preserve our intuition as much as possible. If A is a subset of B then $A \subseteq B \implies |A| \leq |B|$.

Definition: We say a set S is "countable" if $|S| \leq |\mathbb{N}|$. All finite sets are countable. We say a set is "countably infinite" if $|S| = |\mathbb{N}|$. How can we show that a set has the same cardinality as natural numbers?

- Recall $f : A \to B$ is one to one (injective) if $f(a) = f(b) \implies a = b$.
- Recall $f : A \to B$ is onto (surjective) if $\forall y\ \exists x$ such that $f(x) = y$. There do not exist any unmapped elements in the co-domain.



See how both 3,4 map to the same element? That makes this function **not** injective. See how A is unmapped? That makes this function also **not** surjective. We say a function is bijective if it is injective and surjective. Bijection gives us a natural "same size-ness" because if there is a bijection between two sets, the elements seem to pair up nicely, meaning they should have the same size.

Definition: We say a set S is countably infinite if $\exists\ f : \mathbb{N} \to S$ which is a bijection. Recall the inverse of a bijection is also a bijection so equivalently if $\exists\ g : S \to \mathbb{N}$ which is bijective.

2 Examples of Countably Infinite Sets

2.1 Those "other naturals"

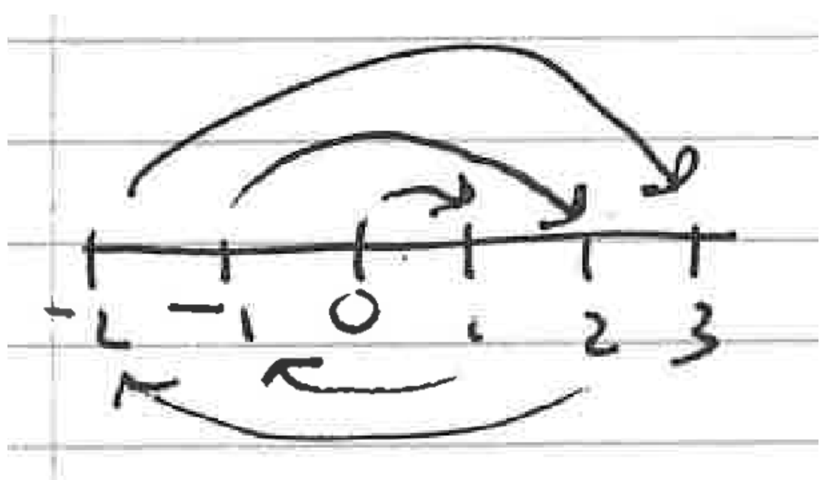
Outside of this class you may not consider zero to be a natural number. Lets prove it doesn't really matter, $|\mathbb{N}| = |\mathbb{N}_{\geq 1}|$. Recall that $\mathbb{N} = \{0, 1, 2, 3, ...\}$ and $\mathbb{N}_{\geq 1} = \{1, 2, 3, ...\}$. To prove these sets have the same cardinality, we give an obvious bijection. Namely $f : \mathbb{N} \to \mathbb{N}_{\geq 1}$ by $f(n) = n + 1$. The elements pair up obviously like $0 \to 1, 1 \to 2$ and so on, so our function is certainly bijective. This shows that if you add or remove a constant amount of elements from a countably infinite set, its still countably infinite.

2.2 The Evens

What is the cardinality of the even numbers? Define $2\mathbb{N} = \{0, 2, 4, 8, ...\}$. Our bijection is again obviously $f(n) = 2n$. This shows that an infinite subset of a countably infinite set is still countably infinite.

2.3 The Integers

Recall $\mathbb{Z} = \{-2, -1, 0, 1, 2, ...\}$. When you are asked to give a bijection, it is equivalent to showing that you can order the elements of a set in some way. Intuitively, if you can "count" them. A bad idea is to first order the elements like 0,1,2,... because then we will never reach the negative numbers. A better idea is to dovetail the negative and positive integers in the following way.



If you were to actually work out what this bijection would be like functionally, you would get

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

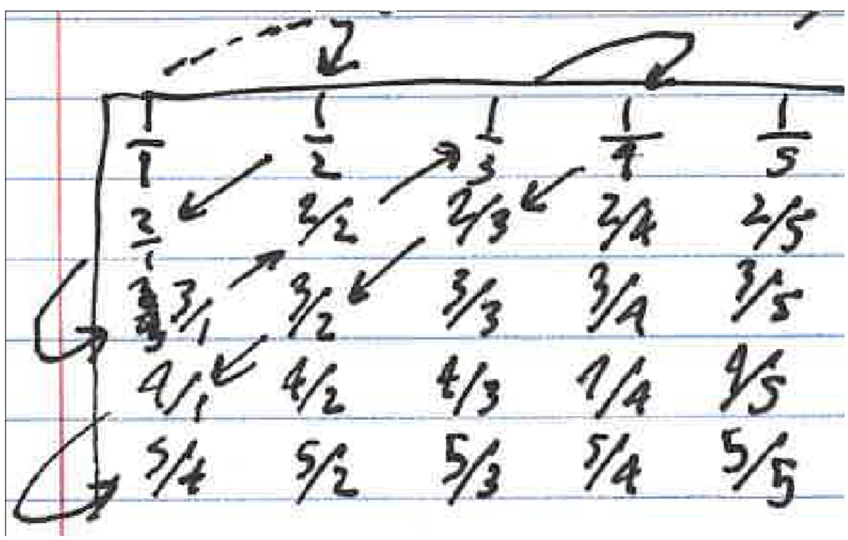
The integers feel like "twice as many" of the naturals so this can show that two countably infinite sets is countably infinite. A countability infinite also need not be well-ordered.

2.4 The Rationals

We define the rational numbers as $\mathbb{Q} = \{ \frac{a}{b} \mid a, b \in \mathbb{N}; a, b \neq 0\}$. They do not contain repetitions, so $\frac{1}{1}, \frac{2}{2}$ are not distinct. Rational numbers have some very different properties than the previous examples. For example for the natural numbers, there is only a finite number of naturals between any two naturals, but this isn't true for the rationals.

- $\mathbb{N}$: $\exists x$ where $0 < x < 1$? no
- $\mathbb{Q}$: $\exists x$ where $\frac{a}{b} < x < \frac{c}{d}$? yes

The naturals appear in discrete steps, but between any two rationals, there exists an infinite amount of rationals. Why? The average of any two rationals is a rational, so the midpoint between any two, you will find a rational[1]. Recursively applying this idea will give you an infinite amount between any two! The mathematically correct term for this is "dense". Could there be more rationals than naturals? It feels like there is a lot more of them. It turns out even despite this, the rationals are still only countably infinite, that $|\mathbb{N}| = |\mathbb{Q}|$. This bijection is a little less obvious. Put all the rationals into a table with columns and rows ordered by numerators and denominators. A bad idea would be to try to go left to right row by row. You would never reach the second row. The idea is then to compose the anti-diagonals ignoring duplicates!



This certainly is a bijection. Its surjective since every element is hit somewhere in this criss-crossing, since every element is on some anti-diagonal. Its injective as every element only can appear once in this ordering.

Here's another solution. Consider the function $f(a/b) = 2^a 3^b$. This function is bijective to some set $S = \{2^i 3^j \mid i, j \in \mathbb{N}_{\geq 1}\}$. Notice that $|\mathbb{Q}| = |S|$. Also notice that since $S \subseteq \mathbb{N}$ then $|S| \leq |\mathbb{N}|$. So by transitivity $|\mathbb{Q}| = |S| \leq |\mathbb{N}| \implies |\mathbb{Q}| \leq |\mathbb{N}|$. We also know that $|\mathbb{N}| \leq |\mathbb{Q}|$ by the injection $f(a) = \frac{a}{1}$ so combined we see that $|\mathbb{Q}| = |\mathbb{N}|$. We could have also

[1] If you wanted to work it out, the rational between $\frac{a}{b}, \frac{c}{d}$ is $\frac{a}{b} + (\frac{c}{d} - \frac{a}{b})/2$. You could simplify that with arithmetic to get some rational.

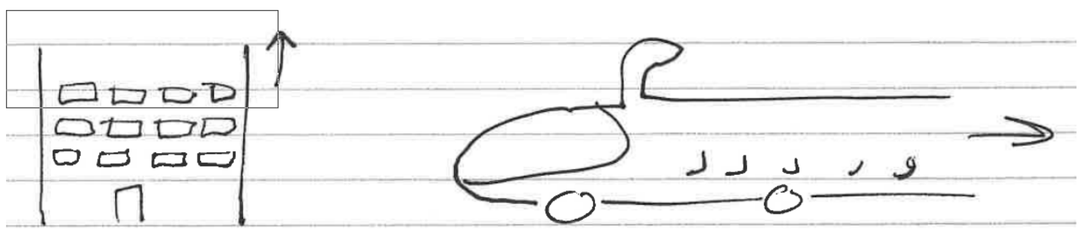
just observed that since $|\mathbb{Q}| \leq |\mathbb{N}|$, we know $\mathbb{Q}$ is countable. Observing that $\mathbb{Q}$ is infinite is enough to show it must be countably infinite.

2.5 Cartesian Products

The rationals are really just like, pairs of numbers. If we are tasked with finding a bijection for $\mathbb{N} \times \mathbb{N}$, we can immediately apply the same argument with the table and anti-diagonals. This is enough to prove that the cartesian product of two countable sets is countable. We can also immediately induct this argument to get that finitely many cartesian products of countable sets is countable. Notice that $\mathbb{N} \times \mathbb{N} \times \mathbb{N} = (\mathbb{N} \times \mathbb{N}) \times \mathbb{N}$. We know that $\mathbb{N} \times \mathbb{N}$ is countable. It remains countable if we perform one more cartesian product.

3 Hillbert's Hotel

Suppose we have an infinitely tall hotel of countably infinite rooms. Each room already has a guest, so the hotel is full.



- A single new guest arrives. Although every room already has a guest, the hotel staff aren't worried. They make each old guest move from room n into the next room, room $n + 1$. Now room zero is empty for the new guest.
- Suppose an infinitely long bus arrives with countably infinite new guests. Even though the hotel seemingly has no space, the new guests can still be accomodated. Tell each old guest to move from room n to $2n$, then each of the new guests to move into the now empty odd-numbered rooms.
- What if a countably infinite number of infinitely long busses arrive, each with countably infinite more guests? I claim they can still be accomodated, and I leave it to you as an exercise to figure out how.

4 Cantor's Theorem

It would seem that you can play with infinity in most ways and remain countably infinite. If we were to say that $|\mathbb{N}| = \infty$, then the vibes are that $\infty + 3, 3 \cdot \infty, \infty^3$ all equal to ∞. These are all polynomially related. Could it be the case that $2^\infty = \infty$? It turns out, no. Lets denote $|\mathbb{N}| = \aleph_0$ and $2^{\aleph_0} = \aleph_1$. We will show these are two very different infinities.

Cantor's theorem tells us that there is no bijection between any set, and its power set[2].

$$|A| < |\mathcal{P}(A)|$$

Note that its obviously true for finite sets. if $A = \{x, y\}$ then $\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$ and $|\mathcal{P}(A)| = 2^{|A|}$.

4.1 Diagonalization

We will prove Cantor's theorem for the countably infinite case. To do so, we present a new technique, called diagonalization. First we define the characterisitic sequence of a subset. If $S \subseteq \mathbb{N}$, to S we associate the infinitely long binary sequence $\chi \in \Sigma^\infty$ such that

$$X[i] = \begin{cases} 1 & i \in S \\ 0 & i \notin S \end{cases}$$

For example

- if $S = \{0, 3, 4\}$ then $\chi = 10011000000...$
- if $S = 2\mathbb{N}$ then $\chi = 10101010...$
- if $S = \mathbb{N}$ then $\chi = 11111...$
- if $S = \emptyset$ then $\chi = 00000...$

Notice immediately that to each subset, corresponds a unique characteristic sequence. There is a bijection between the set of infinitely long binary sequences, and the subsets of a countably infinite set. The infinite sequence of digits exactly characterizes which elements are and aren't in a subset. What is a subset if not just a selection of the elements? It is also important to remember that these sequences are infinitely long.

Let us proceed with the proof. Assume to the contrary that there exists some bijection $f : A \to \mathcal{P}(A)$ with A countably infinite. The elements of $\mathcal{P}(A)$ are exactly the subsets of A. So then there exists an ordering of the elements of $\mathcal{P}(A)$ like $S_0, S_1, S_2, ...$, where every element is in this ordering. Let $\chi_0, \chi_1, \chi_2, ...$ be the characteristic sequences of $S_0, S_1, S_2, ...$ defined in the same ordering. We define "the diagonal" D to be the infinite binary sequence with digits defined as

$$D[i] = 1 - \chi_i[i] = \overline{\chi_i[i]}$$

We take our ordering of characteristic sequences, find the ith one, find its ith digit, and then set the ith digit of D to be the exact opposite of that. D certainly is an infinite binary sequence, so it must be the characteristic sequence of some subset. Since f is bijective, D exists somewhere in our ordering. Suppose the subset corresponding to D is S_j in our order $S_0, S_1, S_2, ...$ Then D is the jth sequence in $\chi_0, \chi_1, \chi_2, ...$ so $D = \chi_j$.

What is $D[j]$? Well, since $D = \chi_j$ then $D[j] = \chi_j[j]$. But recall how we originally defined D, where $D[j] = 1 - \chi_j[j]$. Together, these imply that

$$\chi_j[j] = \overline{\chi_j[j]}$$

[2]Recall that a power set is the set of all subsets of a set

A digit cannot be zero and one simultaneously! Therefore, we see that we have reached a contradiction, and $|\mathcal{P}(A)|$ is not countable. Why is it called diagonalization? Well suppose you listed $\chi_0, \chi_1, ...$ into a table with each χ_i as a row:

χ_0	**0**	1	1	0	1	1	0	...
χ_1	0	**1**	0	0	0	0	0	...
χ_2	0	0	**0**	0	1	1	1	...
χ_3	0	0	1	**1**	0	0	1	...
χ_4	0	1	0	1	**1**	0	1	...
χ_5	0	0	1	1	1	**0**	0	...
...	...							

Then $D = 101001...$ is the opposite of the diagonal of the table. Since D is different than any row of the table, it exists no where in the table. For each row, it is defined to be different in atleast one place, namely the diagonal (i, i) but maybe more. Could it be χ_3? No because $\chi_3[3] = 1$ and $D[3] = 0$. Could it be χ_4? no, and so on. We assumed to the contrary that these sequences were countable and that we can order them, but no matter how we order them, we can always construct an element not in the ordering. So there can never exist a bijection $f : A \to \mathcal{P}(A)$. It is important to convince yourself that this argument is not circular, but self-referential.

5 Uncountability

We have now shown that $\mathcal{P}(A)$ is not countably infinite when A is countably infinite, it is something greater. We call these sets uncountable. Intuitively, a countably infinite set is one in which you can "count". It feels infinite in a discrete sense. At some element, you can choose a next one. Conversely, an uncountable set is literally "uncountable". Imagine a stream of water. What are the units? What is the "next" water?[3]. It feels infinite in a continuous sense.

By a similar diagonalization argument, you can prove the real interval $(0, 1]$ is uncountable, by diagonalizing over the decimal expansions beginning with zero[4]. Given that $(0, 1]$ is uncountable, you can prove that $\mathbb{R}_{\geq 0}$ is uncountable by the bijection $f(r) = 1/r - 1$. Essentially you can stretch the unit sized interval over the entire real positive line. We could have also performed the diagonalization proof directly on infinitely long binary strings Σ^∞ to show they are uncountable.

6 How to Prove Countability

6.1 Union of Two Countable Sets

Let A, B be countably infinite. Then there exists bijections $f : A \to \mathbb{N}$, $g : B \to \mathbb{N}$. We give a bijection for $A \cup B$ as

[3] If you recall that water is atoms then technically water is discrete and countable but the intuition is there even if the science isn't

[4] recall that $0.\overline{9} = 1$. There are a few proofs of this. One is that $1 - 0.999... = 0.0000...$ and another is to notice that $0.999... = 0.333... + 0.333... + 0.333... = 3(0.333...) = 3\frac{1}{3} = 1$

$$h(x) = \begin{cases} 2f(x) & \text{if } x \in A \\ 2g(x)+1 & \text{if } x \in B \end{cases}$$

We leave it to you as an exercise to show its bijective, reducing to the bijectivity of f, g.

6.2 Countable Union of Countable Sets

A countable union of countable sets is countable. Most unions you have ever seen have been countable. They index over $\mathbb{N}$ with $i = 1, 2, 3, ...$ but the index set of a union need not be countable in general. Consider

$$\bigcup_{x \in \mathbb{R}} \{x\} = \mathbb{R}$$

Here we index over $\mathbb{R}$, an uncountable set. Each element is a singleton containing just x, it is finite and therefore countable. But our union is over $\mathbb{R}$, uncountable. We have an uncountable union of countable sets, yet, it is uncountable.

Lets prove that a countable union of countable sets is countable. Let A be countable and each S_i be countable.

$$|\bigcup_{i \in A} S_i| \leq |A \times \mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$$

The first inequality holds by reordering the elements, and maximally assuming each S_i is not finite. The second inequality holds by assuming that A is not finite. The third inequality holds by what we previously proved. So a countable union of countable sets is countable. This proof is actually very rough and requires more rigor, but you get the idea.

6.3 Three solutions

Let's do a problem. Let $\mathbb{N}^*_{\geq 1}$ be the set of finite sequences of natural numbers greater than one. It may contain things like $[1, 11, 1]$ or $[23, 100, 18]$ and so on. We give three solutions to showing this set is countably infinite.

- Let $A_i =$ sequences which sum to i, for example A_3 would contain $[1, 1, 1], [3], [2, 1]$ and so on. Since each sequence sums to something, The A_i's partition $\mathbb{N}^*_{\geq 1}$

  $$\mathbb{N}^*_{\geq 1} = \bigcup_{i=1}^{\infty} A_i$$

  Notice that each A_i is finite, so countable. Then $\mathbb{N}^*_{\geq 1}$ is a countable union of countable sets, so its countable.

- consider the map: $F([x_1, x_2, x_3, ...]) = 2^{x_1} 3^{x_2} 5^{x_3} ...$ or more generally

  $$F([x_1, ..., x_k]) = \prod_{i=1}^{k} p_i^{x_i}$$

where p_i is the i'th prime. By the fundamental theorem of arithmetic, every number has a unique prime factorization, and this immediately gives us that our map is injective. Suppose two sequences exist a, b with $F(a) = F(b)$. Then they are divisible by exactly the same power of two, so then they share the same first element, x_1. Repeating this argument we see that $a = b$. Therefore, we have an injection $F : \mathbb{N}^*_{\geq 1} \to \mathbb{N}$ which implies that it is countable.

- There is a injection hiding in us all along. What is the difference between the two sequences $[1, 1]$ and $[2, 3, 4]$? Is it the length? Is it the number of elements? I put these on the board, you immediately know that the sequences are different. You didn't check the lengths or the elements, so how you did you know? The answer is that the two sequences are different because they look different! Define our injection $f(a) = $ "a". That is, it is the string casting function. Now its certainly true that "$[1, 1]$" $\neq$ "$[2, 3, 4]$". We observe that $f(\mathbb{N}^*_{\geq 1}) \subseteq \Sigma^*$ and subsets of countable sets are countable. Why is Σ^* countable? It is the countable union of countable sets. Recall $\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup ...$

This last point leads us to a powerful theorem called the **Typewriter principle**: If some set S has elements $a \in S$ where every element can be *uniquely* described by a string. Then S is countable. Lets prove it. If every element of S can uniquely be described by a string, then $f : S \to \Sigma^*$ is injective. The co-domain $f(S)$ is a set of strings, so $f(S) \subseteq \Sigma^*$ and f is certainly bijective to $f(S)$ so we see that S is bijective to a subset of a countable set, and is therefore, countable. This is not sufficient to show uncountability. Showing some elements of a set have some infinite encoding isn't enough, since you must also show that there does not exist a unique finite encoding. This turns out to be as hard as finding a bijection. Please only use it to show countability.

We now have an entire toolbox to show a set is countable. Let C be any countable set, and we want to show S is countable. We can do any of the following

- Give a bijection $f : C \to S$
- Give a bijection $f : S \to C$
- Give an injection $f : S \to C$
- Give a surjection $f : C \to C$
- Give an ordering of every element where no element appears twice
- Show that S is a subset of some countable set, since $S \subseteq C \implies |S| \leq |C| \implies |S| \leq \aleph_0$
- Show that S is representable as a countable union of countable sets
- Arrange the elements of S into a grid and compose the anti-diagonals, or some other pattern to implicitly give a bijection
- Show it is the closed under operations we know do not change the cardinality of the set, for example $S = (\{C \times C\} \cup \{0, 1\})^k$.

- Show that its elements can be uniquely represented as finite strings and apply the typewriter principle.

Common known countable sets include $\mathbb{N}, \mathbb{Z}, \Sigma^*, \mathbb{N}^*$, and so on. Every language is also countable.

7 How to prove Uncountability

Let U be some known uncountable set. We give several ways to show a set S is uncountable.

- Diagonalization
- Find a bijection $f : S \to U$
- Show that S contains some uncountable subset. Since if $U \subseteq S$ is uncountable then $|U| \leq |S| \implies \aleph_1 \leq |U|$
- Find an injection $f : S \to U$
- Apply Cantor's theorem, show that it is the powerset $\mathcal{P}(A)$ of some countably infinite A

We do have far fewer ways to show a set is uncountable than to show a set is countable. Which tool you use depends on ease of use.

8 Rejection

What are numbers? They were not there when we started all this. We logically construct the naturals by defining zero to exist, and the sucessor function $S(x) = x + 1$. By repeated application we can produce the numbers. It is well understood that they are the product of some infinite process. 0,1,2,... Ongoing. Forever. There are those who reject this idea. They do not object to the naturals, but the manipulation of an infinite process. They distinguish between the infinite process 0,1,2,... and calling this infinite process $\mathbb{N} = \{0, 1, 2, ...\}$, and then messing around with $\mathbb{N}$. These are the finists. But without what they object to, we are unable to construct the countable and uncountable. There is an even stronger group, known as the ultrafinists. I will leave you with a quote.
I have seen some ultrafinitists go so far as to challenge the existence of 2^{100} as a natural number, in the sense of there being a series of "points" of that length. There is the obvious "draw the line" objection, asking where in $2^1, 2^2, 2^3, ..., 2^{100}$ do we stop having "Platonistic reality"? Here this ... is totally innocent, in that it can be easily be replaced by 100 items (names) separated by commas. I raised just this objection with the (extreme) ultrafinitist Yessenin-Volpin during a lecture of his. He asked me to be more specific. I then proceeded to start with 2^1 and asked him whether this is "real" or something to that effect. He virtually immediately said yes. Then I asked about 2^2 , and he again said yes, but with a perceptible delay. Then 2^3 , and yes, but with more delay. This continued for a couple of more times, till it was obvious how he was handling this objection. Sure, he was prepared to always answer yes, but he was going to take 2^{100} times as long to answer yes to 2^{100} then he would to answering 2^1. There is no way that I could get very far with this.