CS 4510 Automata and Complexity February 26th 2024

Lecture 12: Countability

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

1 Introduction

Recall the main motivation of the class. We wish to understand the correspondence between infinite objects and their finite descriptions. Previously, we have studied the finite objects quite well. Let us now undertake a rigorous understanding of the infinite.

A quote often misattributed to Aristotle is that "*The whole is greater than any part*". Ancient Greek philosophy is often too vague to argue with. It certainly appears true. We may formalize this notion with sets.

Definition 1.1 (Aristotelian Property)**.** If $A \subsetneq B$ then $|A| \lneq |B|$

Despite this, Galileo discovered what he called a paradox. The squares of numbers could be put into correspondence with the numbers.

1	2	3	4	5	...	n	...
1	4	9	16	25	...	n^2	...

The squares are part of the numbers, yet by putting them in a 1-1 correspondence, it was apparent that there are as many squares as there are numbers. A strict part could be equal to the whole. Was this a counter-example to the Aristotelian property? The Aristotelian property is generalized from the intuition about *finite* sets. Galileo here, assumes that a "whole" could be an infinite set.[1] The Aristotelian property is not true for infinite sets. But can a set even be infinite?

Today, without hesitation, we may consider sets to contain infinitely many elements, but this was not always the case historically. Infinity used to be just a figure of speech, or perhaps a useful abstraction, not a real thing. It was understood that you could not discuss $\mathbb{N}$ as a set, only as the outcome of a iterative, never ending process. The natural numbers are constructed by induction.

- $0 \in \mathbb{N}$
- $\forall n \in \mathbb{N} \implies S(n) \in \mathbb{N}$

Because this process is ceaseless, it does not make sense to discuss $|\mathbb{N}|$, much like it doesn't make sense to discuss $f(x) = 1/x$ evaluated at $x = 0$. The sequence 0,1,2,... could be discussed, but not the set $\{0, 1, 2, ...\}$ The infinite could only be discussed in terms of limits, and never addressed directly. Georg Cantor disagreed. In the late 19th century, he undertook a serious attempt to formalize and understand the infinite, generalizing ideas from finite sets to infinite ones.

[1] Both Aristotle and Galileo did not know what a set was.

2 Generalizing our Intuition

We denote the cardinality of the set S as $|S|$. If S is finite then $|S|$ is just the size, the number of elements. 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 $A \subsetneq B \implies |A| \leq |B|$. We have observed for infinite sets that we do not have the Aristotelian property: $A \subsetneq B \not\Rightarrow |A| \lneq |B|$ when A, B are infinite.

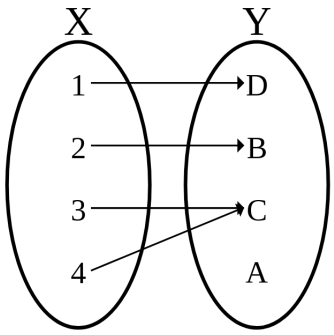
Definition 2.1. We say a set S is *countable* if $|S| \leq |\mathbb{N}|$. All finite sets are countable. We say a set is *countably infinite* if $|S| = |\mathbb{N}|$.

How can we show that a set has the same cardinality as natural numbers?

Definition 2.2 (Injection)**.** Recall $f : A \to B$ is one to one (injective) if $f(a) = f(b) \implies a = b$.

Definition 2.3 (Surjection)**.** 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.

Definition 2.4 (Bijection)**.** A function is said to be bijective if it is both injective and surjective.



See how both 3 and 4 map to the same element? That makes this function **not** injective. See how A is unmapped? That makes this function also **not** surjective. Bijections 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 intuitively have the same size.

Definition 2.5. 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.

To prove that a set is countably infinite, you need only to put it in correspondence with the naturals, like Galileo did.

3 Examples of Countably Infinite Sets

3.1 Those "other naturals"

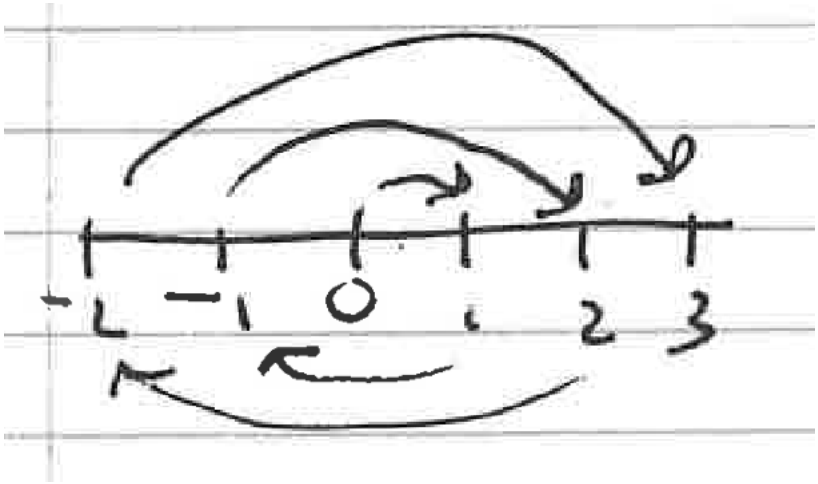
Outside of this class you may not consider zero to be a natural number. Lets prove it doesn't really matter, $|\mathbb{N}| = |\mathbb{N}_{\geq 1}|$. Recall that $\mathbb{N} = \{0, 1, 2, 3, ...\}$ and $\mathbb{N}_{\geq 1} = \{1, 2, 3, ...\}$. To prove these sets have the same cardinality, we give an obvious 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.

3.2 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 "half" of a countably infinite set is still countably infinite.

3.3 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. Since -1 never appears in this ordering, the map is not surjective. 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

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

You should convince yourself it is a bijection. Since every number appears atleast once in the ordering, it is surjective. Since each number appears no more than once, it is injective, so it must be bijective.

The integers feel like "twice as many" of the naturals so this can show that if you "double" a countably infinite set, it remains countably infinite. A countably infinite set also need not be well-ordered, it need not have a least element.

3.4 The Rationals

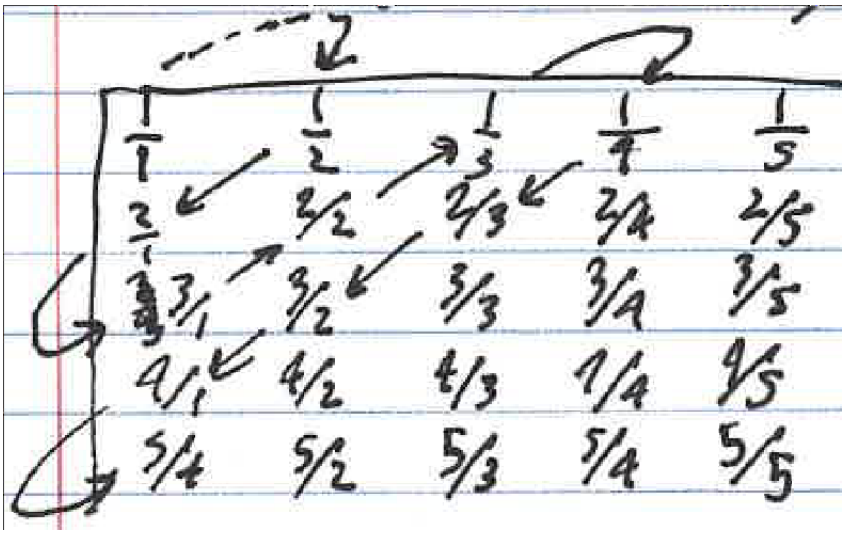
We define the rational numbers[2] as $\mathbb{Q} = \{ \frac{a}{b} \mid a, b \in \mathbb{N}; a, b \neq 0\}$. They do not contain repetitions, so $\frac{1}{1}, \frac{2}{2}$ are not distinct. Rational numbers have some very different properties than the previous examples. For example for the natural numbers,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

- $\exists x \in \mathbb{N}$ where $0 < x < 1$? no
- $\exists x \in \mathbb{Q}$ 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[3]. 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 representations of rationals into a table with columns and rows ordered by numerators and denominators. This table contains duplicates since 1/1 and 2/2 are the same rational. 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!

[2]The rationals can actually contain negatives and zero but suppose that we are only in consideration of the positive non-zero rationals

[3]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 it into numerator/denominator form.



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 since we define it to ignore duplicates.

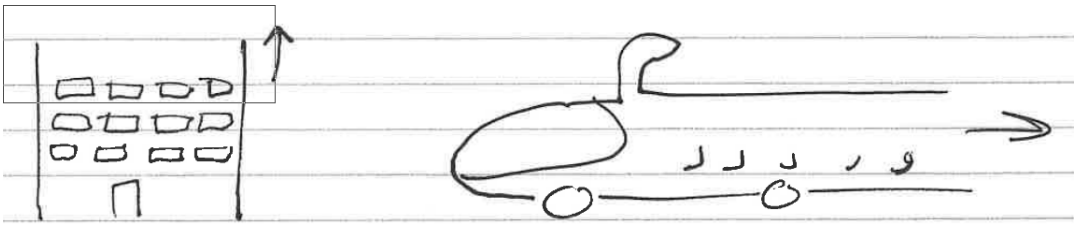
Here's another solution. Consider the function $f(a/b) = 2^a 3^b$. This function is bijective to some set $S = \{2^i 3^j \mid i, j \in \mathbb{N}_{\geq 1}\}$. Notice that $|\mathbb{Q}| = |S|$. Also notice that since $S \subseteq \mathbb{N}$ then $|S| \leq |\mathbb{N}|$. So by transitivity $|\mathbb{Q}| = |S| \leq |\mathbb{N}| \implies |\mathbb{Q}| \leq |\mathbb{N}|$. 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 just observed that since $|\mathbb{Q}| \leq |\mathbb{N}|$, we know $\mathbb{Q}$ is countable, as subsets of countable sets are countable. Observing that $\mathbb{Q}$ is infinite is enough to show it must be countably infinite.

3.5 Cartesian Products

The rationals are really just like, pairs of numbers. If we are tasked with finding a bijection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, 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, and so on.

4 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 a countably infinite number of new guests. Even though the hotel seemingly has no space, the new guests can still be accommodated. Tell each old guest to move from room n to room $2n$, 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 number of guests? I claim they can still be accommodated, and I leave it to you as an exercise to figure out how.

5 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 it would seem 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 infinites. We do not use ∞, as we need a way to distinguish between the kinds of infinite. We represent these as cardinals, $\aleph_0, \aleph_1$, and so on. These are not numbers, they are cardinals. Cantor's theorem tells us that there is no bijection between any set, and its power set[4].

Theorem 1 (Cantor)**.** If A is any set and $\mathcal{P}(A)$ is the set containing all subsets of A then

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

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

5.1 Diagonalization

Diagonalization is an extremely important proof technique. Perhaps one of the most important in history. We will prove Cantor's theorem several times to emphasize diagonalization. First we prove Cantor's theorem for the special case of the naturals.

Theorem 2.

$$|\mathbb{N}| \lneq |\mathcal{P}(\mathbb{N})|$$

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

Proof. Assume to the contrary that there does exist a bijection $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$. Then there exists a way to totally order the subsets of $\mathbb{N}$ like $S_0, S_1, S_2, ...$ where every possible subset of the naturals appear in this ordering exactly once. Consider the set D defined such that for all $i \in \mathbb{N}$

$$i \in D \iff i \notin S_i \tag{1}$$
$$i \notin D \iff i \in S_i \tag{2}$$

We go to the ith set in the ordering, see if it contains the ith number, and if it does, we define it not to be in D, and if it doesn't, we define D to include it. Notice that D is a set of numbers, so $D \subseteq \mathbb{N}$, or that $D \in \mathcal{P}(\mathbb{N})$. Then there exists a spot for it in line in our total ordering. There exists a number j such that $D = S_j$. Two sets are equal if they contain the same elements, so we know that

$$j \in D \iff j \in S_j$$

But by the definition of how we defined D, we know that

$$j \in D \iff j \notin S_j$$

Combining these, we see

$$j \in S_j \iff j \notin S_j$$

A contradiction. □

Let us remark on the proof. It is important that you understand that the proof is not circular. A circular proof is one which assumes its conclusion as a premise, so it demonstrates nothing. Nothing circular is going on here, but something else definitely is; self reference. The set D is defined against the ordering of subsets $S_0, S_1...$ and for a different ordering, there must be a different D. To further illustrate the mechanics of this proof technique, lets do it again. We will prove Cantor's theorem for the countably infinite case using diagonalization.

Theorem 3. Let A be any countably infinite set. Then

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

Proof. First we define the characterisitic sequence of a subset. Assume that A is countably infinite. Then its elements may be ordered like $a_0, a_1, ...$ If $S \subseteq A$, to S we associate the infinitely long binary sequence $\chi \in \Sigma^\infty$ such that

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

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 bits 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 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 $S_0, S_1, S_2, ...$ ordered in the same way. 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 $\chi_0, \chi_1, \chi_2, ...$ There exists a number j such that $D = \chi_j$ What is the jth bit of D? $D[j]$? 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

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

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 $f : A \to \mathcal{P}(A)$.

This is where the term diagonalization comes from. The element you are constructing is the negation of the diagonal of this implicit table. The diagonal entries are at coordinate (i, i) and the elements of D are defined considering if $i \in S_i$ or not. It is important that you understand that the diagonalization technique does have this nice visualization, but the technique goes far beyond this. When doing a proof by diagonalization, do not draw a table and define its elements. The table is completely implicit. This is important. See the first proof we did of diagonalization, in the proof by contradiction, the absurdity we derived was completely based on logic, and made no reference to a table. You will apply diagonalization to things which cannot be nicely visualized as a table. Let us now prove Cantor's theorem in the general case, so it may apply even when A is uncountable.

Theorem 4 (Cantor's Theorem)**.** If A is any set, then

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

Proof. Assume to the contrary that there is a bijection between A and $\mathcal{P}(A)$ Consider the subset of A such that the bijection f doesn't map x to a set containing x.

$$D = \{x \in A \mid x \notin f(x)\}$$

Since $D \subseteq A$, we know $D \in \mathcal{P}(A)$. Since f is a bijection, it is also surjective, so there must exist some j such that $D = f(j)$. Is $j \in D$? Two sets are equal if they have the same elements

$$j \in D \iff j \in f(j)$$

But by definition of D, we have that

$$j \in D \iff j \notin f(j)$$

contradiction.

□

For any set A, there always exists an injection $f : A \to \mathcal{P}(A)$, namely $f(x) = \{x\}$. We proved there cannot exist a bijection, but if there is always an injection, that means there is never a surjection. If every map from a set to its powerset is not surjective, so there is an element of the codomain always goes unmapped for every map. If cardinality is supposed to be an extension of the intuition about size, $\mathcal{P}(A)$ is "bigger" than A, even when A is infinite. There are atleast two infinities! In fact, we can remark that there are atleast a countably infinite number of infinities.

$$|\mathbb{N}| \lneq |\mathcal{P}(\mathbb{N})| \lneq |\mathcal{P}(\mathcal{P}(\mathbb{N}))| \lneq |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| \lneq ...$$

6 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?[5]. 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[6]. 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.

7 How to Prove Countability

7.1 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

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

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

7.2 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 $i = 0, 1, 2, 3, ...$ 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. Consider the map

$$f : A \times \mathbb{N} \to \bigcup_{i \in A} S_i$$

Such that $f((i, j))$ maps to the j'th element of S_i. Note that this map is surjective so $|A \times \mathbb{N}| \geq |\cup_{i \in A} S_i|$ and since $A \times \mathbb{N}$ is countable, so is our countable union.

7.3 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.

[5] 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

[6] 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 $0.999... = 0.333... + 0.333... + 0.333... = 3(0.333...) = 3\frac{1}{3} = 1$

- 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: $F([x_1, x_2, x_3, ..., x_k]) = 2^{x_1}3^{x_2}5^{x_3}...p_k^{x_k}$ 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

$$\Sigma^* = \bigcup_{i=0}^{\infty} \Sigma^i$$

This last point leads us to a powerful theorem called the **Typewriter principle**:

Theorem 5. If some set S has elements $a \in S$ where every element can be *uniquely* described by a string. Then S is countable.

Proof. If every element of S can uniquely be described by a string, then $f : S \to \Sigma^*$ is injective. The image $f(S)$ 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. Also take notes of the contrapositive. If a set is uncountable, its elements may not all be able to be uniquely described by strings.

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 $f : C \to S$
- 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 length 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, as it is a subset of a countable set.

8 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 $|U| \leq |S| \implies \aleph_1 \leq |S|$
- Find an injection $f : U \to S$
- Apply Cantor's theorem, show that it is the powerset $\mathcal{P}(A)$ of some 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. Common uncountable sets include $\mathcal{P}(\Sigma^*), \mathcal{P}(\mathbb{N}), \mathbb{R}, \mathbb{C}$, and others.

9 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 intuitionists and 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.*