CS 70 Discrete Mathematics and Probability Theory
Summer 2019 Course Notes **Note 10**

# 1 Infinity and Countability

In this note we'll discuss the question of when two sets have the same *cardinality* (size). This is a simple issue for finite sets, but for infinite sets it becomes quite tricky. We'll see how to formulate the question precisely, and then see several quite surprising consequences. To set the scene, we begin with the simple case of finite sets.

## 1.1 Bijections and Cardinality

When we think of the "size" of finite sets, we normally think about the number of elements in them. For example, we think of the "size" of $\{1,2,3\}$ as three because that's how many elements it has. In the finite case, it is easy to determine if two sets have the same size: we simply count the number of elements in each and see if we get the same result.

Unfortunately, this will not generalize well to infinite sets. Suppose, for example, I wish to compare the set of natural numbers $\mathbb{N}$ with the set of positive integer $\mathbb{Z}^+$. These both have an infinite number of elements — but how do we know if one infinity is the same as the other? In this case, $\mathbb{N}$ contains zero whereas $\mathbb{Z}^+$ does not — does this mean that their infinities are different? As a more extreme example, how does this definition compare $\mathbb{N}$ with $\mathbb{R}$?

What this suggests is that we need a different way of comparing sizes of sets, one which will generalize better to the infinite case. For this, we will use bijections, as introduced in Note 6.5. In particular, we will say that two sets $A$ and $B$ have the same cardinality (denoted $|A| = |B|$) if there exists a bijection $b : A \to B$.

Let us first verify that this definition makes sense in terms of finite sets. Suppose our sets $A$ and $B$ have the same size; that is, suppose they both have the same number of elements, $n$. We can give each of these sets an order, and give a bijection $b$ which maps the $i$th element of $A$ to the $i$th element of $B$. Thus, if two finite sets were the same size under our original, intuitive definition, they will also be the same size under this bijection definition.

On the flip side, consider what happens if $A$ and $B$ have different numbers of elements. If the number of elements in $A$ is smaller, any function from $A$ to $B$ can hit at most $|A|$ of the elements in $B$, so there cannot exist an onto map from $A$ to $B$ (and thus cannot exist a bijection). If $A$ is instead bigger, the pigeonhole principle tells us that any map from $A$ to $B$ must map two elements of $A$ to the same point. Thus, in this case, no function from $A$ to $B$ can be one-to-one, and hence there still cannot be a bijection.

What this all tells us is that the bijection definition of size is at least reasonable insofar as that it matches with our intuitive definition of size for finite sets. As we will see in the remainder of this note, though, the bijection definition generalizes much more easily to the infinite case, allowing us to uncover surprising and beautiful structures therein.

# 2 Countability

The natural numbers $\mathbb{N}$ is one of the most widely used infinite sets. Thus, it will be natural for us to compare other sets to $\mathbb{N}$ and see which are the same size, which are bigger, and which are smaller.[1] In this first section, we explore *countable* sets, which are sets that are the same size as $\mathbb{N}$ or smaller.

## 2.1 A First Example

We first return to a question we asked at the beginning of the note: are $\mathbb{N}$ and $\mathbb{Z}^+$ the same size, or is one bigger than the other? With our new bijection definition, we can very quickly see that they are in fact the same size, as we have the following mapping from $\mathbb{N}$ to $\mathbb{Z}^+$:

$$\begin{array}{lcccccccc}
\mathbb{N} & 0 & 1 & 2 & 3 & 4 & 5 & \dots & \\
f\downarrow & \searrow & \searrow & \searrow & \searrow & \searrow & \searrow & & \\
\mathbb{Z}^+ & & 1 & 2 & 3 & 4 & 5 & 6 & \dots
\end{array}$$

Why is this mapping a bijection? Clearly, the function $f : \mathbb{N} \to \mathbb{Z}^+$ is onto because every positive integer is hit. And it is also one-to-one because no two natural numbers have the same image. (The image of $n$ is $f(n) = n+1$, so if $f(n) = f(m)$ then we must have $n = m$.) Since we have shown a bijection between $\mathbb{N}$ and $\mathbb{Z}^+$, this tells us that there are as many natural numbers as there are positive integers! (Very) informally, we have proved that "$\infty + 1 = \infty$."

## 2.2 More Examples

We next consider the set of *even* natural numbers $2\mathbb{N} = \{0,2,4,6,...\}$? In the previous example the difference was just one element. But in this example, there seem to be twice as many natural numbers as there are even natural numbers. Surely, the cardinality of $\mathbb{N}$ must be larger than that of $2\mathbb{N}$ since $\mathbb{N}$ contains all of the odd natural numbers as well? Though it might seem to be a more difficult task, let us attempt to find a bijection between the two sets using the following mapping:

$$\begin{array}{lccccccc}
\mathbb{N} & 0 & 1 & 2 & 3 & 4 & 5 & \dots \\
f\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
2\mathbb{N} & 0 & 2 & 4 & 6 & 8 & 10 & \dots
\end{array}$$

The mapping in this example is also a bijection. We could as before prove that it is both one-to-one and onto, but it is much easier to simply notice that it has an inverse mapping $f^{-1}(n) = \frac{n}{2}$, implying that it must be a bijection. Since we have found a bijection between these two sets, this tells us that in fact $\mathbb{N}$ and $2\mathbb{N}$ have the same cardinality!

As a final example in this section, suppose we want to compare $\mathbb{N}$ to $\mathbb{Z}$. At first glace, it may seem like $\mathbb{Z}$ should be bigger, as it contains infinitely many negative numbers, which $\mathbb{N}$ does not have. But upon

[1] It in fact turns out that there are no infinite sets smaller than $\mathbb{N}$, though we will not prove that fact in this class.

closer thought, we notice that almost exactly the same statement could be made about $\mathbb{N}$ and $2\mathbb{N}$, as only the former contains the (infinitely many) odd numbers! And indeed, as before, we will be able to define a bijection between $\mathbb{N}$ and $\mathbb{Z}$ as follows:

$$\begin{array}{cccccccc}
\mathbb{N} & 0 & 1 & 2 & 3 & 4 & 5 & \dots \\
f\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\
\mathbb{Z} & 0 & 1 & \text{-1} & 2 & \text{-2} & 3 & \dots
\end{array}$$

Written in function notation, this mapping is

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

As before, we could prove that this function is one-to-one and onto, but it is simpler to notice that

$$f^{-1}(y) = \begin{cases} 2y-1 & y > 0 \\ -2y & y \leq 0 \end{cases}$$

is the inverse of this mapping, thus implying that $f$ is a bijection. Since we have a bijection between $\mathbb{N}$ and $\mathbb{Z}$, we can conclude that they do in fact have the same cardinality.

## 2.3 Enumeration

Something you may have noticed in the last example was that the explicit formula for the bijection from $\mathbb{N}$ to $\mathbb{Z}$ was a tad convoluted, making it a bit difficult to come up with and somewhat difficult to understand at first glance. This will be the case for many sets we'd like to study, so it would behoove us to derive a cleaner way of proving that a bijection exists.

This method will be what is known as *enumeration*. Formally, in order to prove that a set $S$ is countable, we need to describe a way to list its elements in some order such that any arbitrary element will appear at a finite position. In the case of $\mathbb{Z}$, our enumeration would be

$$0, 1, -1, 2, -2, 3, -3, 4, -4, ...$$

To understand why this works, note that by enumerating a set $S$, we are implicitly defining a bijection from $\mathbb{N}$ to $S$ — simply map $n \in \mathbb{N}$ to the $n$th element of our enumeration! Thus, giving an enumeration is equally powerful to giving an explicit bijection, with the advantage of (often) being easier to understand and write out.

However, when enumerating, we do need to be careful to ensure we meet the criterion that any element appears at a finite position. As an example of how this can fail, consider the following "enumeration" of $\mathbb{Z}$:

$$0, 1, 2, 3, ..., -1, -2, -3, ...$$

While this might seem valid at first glance, what happens if we ask for the position number of $-1$? There are an infinite number of positive integers before it, so its "position" would be $\infty$, which isn't allowed! If we used this "enumeration" to try and define a bijection from $\mathbb{N}$ to $\mathbb{Z}$, nothing would ever be mapped to $-1$.

## 2.4 Example Enumerations

To see this new tool in action, let's consider the set of finite-length bit strings, denoted $\{0,1\}^*$. To give an enumeration of this set, we consider such bit strings in *lexiographical order*; that is, we list shorter strings before longer strings, and if two strings have the same length, we put them in alphabetical order. Concretely, we have the following enumeration of $\{0,1\}^*$:

$$\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots$$

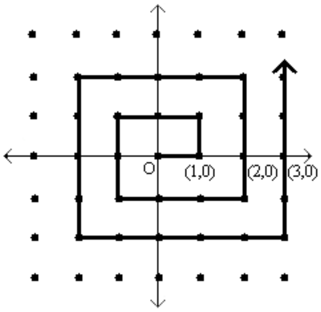
where $\varepsilon$ represents the empty string.

---

*Sanity check!* Convince yourself that every finite bit string has a finite position in the above enumeration.

---

Our next example really shows how much easier enumeration can make our lives over explicitly giving a bijection. For this, we wish to show that $\mathbb{Z} \times \mathbb{Z}$ (that is, the set of *pairs* of integers) is the same size as $\mathbb{N}$. We describe our enumeration of $\mathbb{Z} \times \mathbb{Z}$ by picture:



In words, we start our enumeration at $(0,0)$ and steadily move outwards in a spiral pattern. Thus, $(0,0)$ appears at position 0 in the enumeration, $(1,1)$ appears at position 2, $(-1,0)$ appears at position 5, and so forth. From the picture, we can intuitively see that this enumeration will eventually hit every point in $\mathbb{Z} \times \mathbb{Z}$.

---

*Sanity check!* Try writing out the bijection from $\mathbb{N}$ to $\mathbb{Z} \times \mathbb{Z}$ given by the above enumeration. Can you see how much more difficult it is than just drawing this picture?

---

## 2.5 Injections, Surjections, and Cardinality

While enumeration is certainly helpful in simplifying the representation of a bijection, there are still cases where it isn't enough. For example, suppose we wished to compare the set of rationals $\mathbb{Q}$ to $\mathbb{N}$. We could attempt to give an enumeration like the one for $\mathbb{Z} \times \mathbb{Z}$ (where the pair $(a,b)$ represents the number $\frac{a}{b}$), but this won't give us exactly what we want — rational numbers will appear multiple times (for example, $\frac{1}{2}$ would be represented by both $(1,2)$ and $(2,4)$), and the points on the x-axis don't correspond to rational numbers at all, as we would be dividing by zero!

However, something we notice amidst these problems is that the idea of making rational numbers correspond to pairs of integers is reasonable. In fact, we can create a one-to-one mapping from $\mathbb{Q}$ to $\mathbb{Z} \times \mathbb{Z}$: if a rational number $q$ can be represented in lowest terms as $\frac{a}{b}$, we map it to the pair $(a,b)$. Thus, for example, .25 would be mapped to $\frac{1}{4}$ and 1.3333... would be mapped to $\frac{4}{3}$.

This by itself does not allow us to conclude that $|\mathbb{Q}| = |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$, as it is not a bijection. However, when combined with the following theorem, we can actually get somewhere.

**Theorem 10.1** (Cantor-Schröder-Bernstein Theorem)**.** *Let $A$ and $B$ be sets. If there exist one-to-one mappings $f : A \to B$ and $g : B \to A$, then there exists a bijection $b : A \to B$.*

While the proof of this theorem is beyond our scope, its applications are not. In particular, this theorem allows us to define a reasonable sense of order on the cardinalities of sets: we have that $|A| \leq |B|$ if there exists an injection from $A$ to $B$. In order for this to make sense, we need to ensure that if $|A| \leq |B|$ and $|B| \leq |A|$, $|A| = |B|$ — but this is exactly what Theorem 10.1 says!

Applying this back to our original problem, we know that $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N}|$. But notice that since $\mathbb{N} \subseteq \mathbb{Q}$, we immediately have an injection from $\mathbb{N}$ to $\mathbb{Q}$: simply map the natural number $n$ to the rational number $n$. Thus, we also have that $|\mathbb{N}| \leq |\mathbb{Q}|$, so in fact $|\mathbb{Q}| = |\mathbb{N}|$.

As a final note in this section, we point out that there exists a one-to-one function from $A$ to $B$ if and only if there is an onto function from $B$ to $A$. Thus, similar to how we said that $|A| \leq |B|$ if there is an injection from $A$ to $B$, we can also say that $|B| \geq |A|$ if there exists a surjection from $B$ to $A$. Depending on the problem at hand, it may be much easier to find and/or describe a surjection than an injection.

---

*Exercise.* Given a one-to-one function $f : A \to B$, construct an onto function $g : B \to A$.
Given an onto function $g : B \to A$, construct a one-to-one function $f : A \to B$.

---

# 3 Uncountability

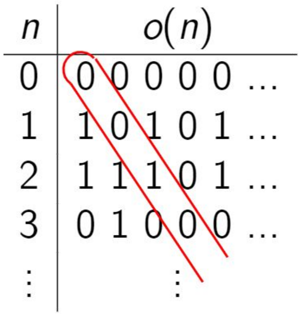
Up to this point, all of the sets we've seen have been countable; that is, they've been the same size as $\mathbb{N}$ or smaller. A natural question that might arise at this point is "are all sets countable?" As it turns out, the answer to this question is no! In order to prove this (potentially surprising) fact, we use a method known as *Cantor's Diagonalization*, named after its creator Georg Cantor.

## 3.1 A First Diagonalization

As a first trial run of the diagonalization technique, we will prove that the set of infinite length bit strings, denoted $\{0,1\}^\infty$ is uncountable; that is, there exists no surjection from $\mathbb{N}$ to $\{0,1\}^\infty$. Note here that $\{0,1\}^\infty$ is different from the set $\{0,1\}^*$ we considered earlier in the note in that each element in $\{0,1\}^\infty$ has infinitely (rather than finitely) many digits in it. This will make the difference between countability and uncountability.

**Theorem 10.2.** $\{0,1\}^\infty$ *is not countable. That is, there does not exist an onto function $o : \mathbb{N} \to \{0,1\}^\infty$.*

*Proof.* Suppose for the sake of contradiction that there exists an onto function $o : \mathbb{N} \to \{0,1\}^\infty$. We can write out the evaluations of this function in table form, as below:



| $n$ | $o(n)$ |
|---|---|
| 0 | 0 0 0 0 0 ... |
| 1 | 1 0 1 0 1 ... |
| 2 | 1 1 1 0 1 ... |
| 3 | 0 1 0 0 0 ... |
| ⋮ | ⋮ |

In particular, we will consider the diagonal of this evaluation table, highlighted in red. Consider what happens if we take each element of the diagonal and flip it; that is, we create an (infinite-length) bit string $s$ such that the $i$th bit of $s$ is the opposite of the $i$th bit of the diagonal. I claim that $s \neq o(n)$ for any $n \in \mathbb{N}$. Indeed, we know that $s \neq o(0)$, as the zeroth bit of $s$ was defined to be the opposite of that of $o(0)$. Similarly, we know that $s$ and $o(1)$ have different first bits, so $s \neq o(1)$. We can repeat this argument for all natural numbers $n$, meaning that $s \neq o(n)$ for any $n \in \mathbb{N}$.

But now this means that $o$ is not actually onto — there exists an infinite-length bit string with no preimage in $\mathbb{N}$. Hence, we have reached a contradiction, and so can conclude that $\{0,1\}^\infty$ is, in fact, uncountable. □

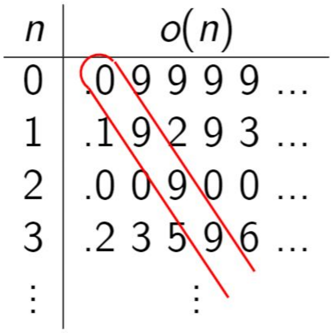
It is worthwhile to take a step back at this point and realize what we just did. We just showed that no function, no matter how cleverly crafted, can ever map $\mathbb{N}$ onto $\{0,1\}^\infty$. It would not have been enough to simply find some examples of functions from $\mathbb{N}$ to $\{0,1\}^\infty$ which are not onto — that would simply show that those particular examples don't exist, but it would still be possible for there to be some very clever way of making it work that we just hadn't thought of yet. The key behind Cantor's diagonalization is that it works *no matter what function* we try to use.

## 3.2 A Fixable "Proof"

In this section and the next, we give examples of common mistakes that occur when trying to use diagonalization. In this section, we give a "proof" that the real numbers are uncountable, then describe how to fix the errors in it.

**Theorem 10.3.** *Let* $[0,1] = \{x \in \mathbb{R} | 0 \leq x \leq 1\}$. *Then* $[0,1]$ *is uncountable.*

*Proof Attempt.* Suppose for contradiction that there exists an onto function $o : \mathbb{N} \to [0,1]$. I claim that every number in $[0,1]$ can be represented as $0.d_1d_2d_3d_4...$, where $d_i$ is the $i$th digit in the decimal expansion of my number.[2] Thus, we can list out the evaluations of $o$ in table format:



| $n$ | $o(n)$ |
|---|---|
| 0 | .0 9 9 9 9 ... |
| 1 | .1 9 2 9 3 ... |
| 2 | .0 0 9 0 0 ... |
| 3 | .2 3 5 9 6 ... |
| ⋮ | ⋮ |

[2] This is clear for any number smaller than 1. To see that it is also true for 1, note that 0.99999... = 1.

As before, we look at the diagonal and change each element of it to something else. In this case, we take the $i$th digit on the diagonal and add 1 to it (modulo 10). Thus, for the example given in the picture, we would construct the number $0.1000...$. This number cannot be the same as any in my table, as it disagrees with $o(n)$ on at least the $n$th digit. Hence, $o$ is not in fact onto, and we have reached the desired contradiction. □

It should seem at first like this is a valid proof — after all, it follows almost exactly the same format as the original, correct proof that $\{0,1\}^\infty$ is uncountable. The error here arises from a subtle peculiarity of the real numbers: the decimal expansion of a number is not always unique.

As a concrete example of this, consider the real numbers 0.1000... and 0.09999.... These are in fact two different decimal expansions of the same real number![3] This is true even though the former has a first digit of 1 while the latter has a first digit of 0. Thus, just knowing that the number we construct differs from $o(n)$ on the $n$th bit is not sufficient to conclude that they are different numbers — indeed, in our example, we see that the number we constructed turned out to be 0.1000..., which is exactly the same as $o(0) = 0.09999...$.

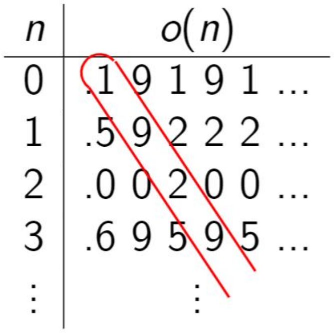
Fortunately, this problem is easy enough to fix. In our diagonalization step, instead of adding 1 mod 10 to our diagonal elements, we can instead add 2 mod 10. This allows us to avoid the above problem, and makes our proof correct. Thus, $[0,1]$ is larger than $\mathbb{N}$, and since $[0,1] \subseteq \mathbb{R}$, we must also have that $|\mathbb{R}| > |\mathbb{N}|$.

## 3.3 An Unfixable "Proof"

Finally, we give yet another example of a diagonalization proof gone awry, though this time there will not be a way for us to fix the proof, as the claim we are trying to prove is wrong.

**Claim 10.1.** *The rational numbers between 0 and 1 ($\mathbb{Q} \cap [0,1]$) are uncountable.*

*"Proof"*. Suppose for contradiction that there exists an onto map $o : \mathbb{N} \to \mathbb{Q} \cap [0,1]$. As with our proof for the real interval $[0,1]$, we can represent each element of $\mathbb{Q} \cap [0,1]$ as its decimal expansion $0.d_1d_2d_3d_4...$ and list the function values of $o$ in tabular form:



| $n$ | $o(n)$ |
|---|---|
| 0 | .1 9 1 9 1 ... |
| 1 | .5 9 2 2 2 ... |
| 2 | .0 0 2 0 0 ... |
| 3 | .6 9 5 9 5 ... |
| ⋮ | ⋮ |

Again mirroring the (correct) proof for the real interval $[0,1]$, we take each element of the diagonal and add two to it modulo 10. This ensures that the number we construct will be different from $o(n)$ for all $n$, and hence is not mapped to by $o$. This contradicts $o$ being onto, so we can conclude that $\mathbb{Q} \cap [0,1]$ is uncountable. □

[3] You likely saw in elementary or middle school the proof that $1 = 0.9999...$; this is exactly the same deal.

But wait — earlier, we proved that the entirety of $\mathbb{Q}$ is countable. So there must have either been an error in that proof or an error in this one!

Indeed, the error lies in our most recent proof. This time the issue is not that the number we construct is the same as one of the $o(n)$s, as the adding 2 to each digit made sure that would not happen. Instead, we notice that the modified diagonal is not guaranteed to be a rational number. Indeed, in the example picture, we would end up construction $0.3141... = \frac{\pi}{10}$, which is certainly not rational! Thus, it doesn't matter that $o$ doesn't map any natural number to this construct, as we were never trying to map to it in the first place.

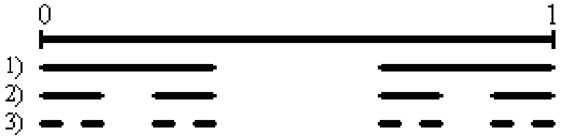
The moral of these two stories is that in a proof by diagonalization, you need to be careful that whatever you construct by modifying the diagonal (1) is actually different from each $o(n)$ and (2) is actually in the set you are attempting to prove is uncountable. Being sloppy with either of those two steps can lead to you "proving" false statements!

# 4 Optional Additional Reading

The material in the remainder of this note is optional reading, and will not be in scope for the class. We do still recommend you read it, as it is interesting and can help you get a better grasp on the other material in this note, but none of it will be explicitly tested for.

## 4.1 The Cantor Set [OPTIONAL]

The Cantor set is a remarkable set construction involving the real numbers in the interval $[0,1]$. The set is defined by repeatedly removing the middle thirds of line segments infinitely many times, starting with the original interval. For example, the first iteration would involve the removal of the (open) interval $(\frac{1}{3},\frac{2}{3})$, leaving $[0,\frac{1}{3}]\cup[\frac{2}{3},1]$. We then proceed to remove the middle third of each of these two remaining intervals, and so on. The first three iterations are illustrated below:



The Cantor set contains all points that have *not* been removed: $C=\{x : x \text{ not removed}\}$. How much of the original unit interval is left after this process is repeated infinitely? Well, we start with an interval of length 1, and after the first iteration we remove $\frac{1}{3}$ of it, leaving us with $\frac{2}{3}$. For the second iteration, we keep $\frac{2}{3}\times\frac{2}{3}$ of the original interval. As we repeat these iterations infinitely often, we are left with:

$$1 \longrightarrow \tfrac{2}{3} \longrightarrow \tfrac{2}{3}\times\tfrac{2}{3} \longrightarrow \tfrac{2}{3}\times\tfrac{2}{3}\times\tfrac{2}{3} \longrightarrow \cdots \longrightarrow \lim_{n\to\infty}(\tfrac{2}{3})^n = 0$$

According to the calculations, we have removed everything from the original interval! Does this mean that the Cantor set is empty? No, it doesn't. What it means is that the *measure* of the Cantor set is zero; the Cantor set consists of isolated points and does not contain any non-trivial intervals. In fact, not only is the Cantor set non-empty, it is uncountable![4]

[4] It's actually easy to see that $C$ contains at least countably many points, namely the endpoints of the intervals in the construction—i.e., numbers such as $\frac{1}{3}$, $\frac{2}{3}$, $\frac{1}{9}$, $\frac{1}{27}$ etc. It's less obvious that $C$ also contains various other points, such as $\frac{1}{4}$ and $\frac{3}{10}$. (Why?)

To see why, let us first make a few observations about ternary strings. In ternary notation, all strings consist of digits (called "trits") from the set $\{0,1,2\}$. All real numbers in the interval $[0,1]$ can be written in ternary notation. (E.g., $\frac{1}{3}$ can be written as 0.1, or equivalently as $0.0222\ldots$, and $\frac{2}{3}$ can be written as 0.2 or as $0.1222\ldots$.) Thus, in the first iteration, the middle third removed contains all ternary numbers of the form 0.1xxxxx. The ternary numbers left after the first removal can all be expressed either in the form 0.0xxxxx... or 0.2xxxxx... (We have to be a little careful here with the endpoints of the intervals; but we can handle them by writing $\frac{1}{3}$ as $0.02222\ldots$ and $\frac{2}{3}$ as 0.2.) The second iteration removes ternary numbers of the form 0.01xxxxx and 0.21xxxxx (i.e., any number with 1 in the second position). The third iteration removes 1's in the third position, and so on. Therefore, what remains is all ternary numbers with only 0's and 2's. Thus we have shown that

$$C = \{x \in [0,1] : x \text{ has a ternary representation consisting only of 0's and 2's}\}.$$

Finally, using this characterization, we can set up an *onto* map $f$ from $C$ to $[0,1]$. Since we already know that $[0,1]$ is uncountable, this implies that $C$ is uncountable also. The map $f$ is defined as follows: for $x \in C$, $f(x)$ is defined as the binary decimal obtained by dividing each digit of the ternary representation of $x$ by 2. Thus, for example, if $x = 0.0220$ (in ternary), then $f(x)$ is the binary decimal 0.0110. But the set of all binary decimals $0.\text{xxxxx}\ldots$ is in 1-1 correspondence with the real interval $[0,1]$, and the map $f$ is onto because every binary decimal is the image of some ternary string under $f$ (obtained by doubling every binary digit).[5] This completes the proof that $C$ is uncountable.

## 4.2 Power Sets and Higher Orders of Infinity [OPTIONAL]

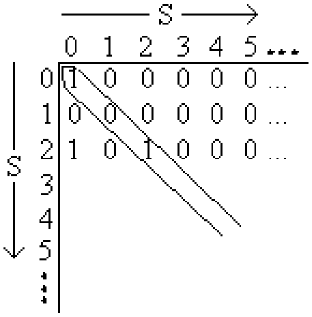
Let $S$ be any set. Then the *power set* of $S$, denoted by $\mathscr{P}(S)$, is the set of all subsets of $S$. More formally, it is defined as: $\mathscr{P}(S) = \{T : T \subseteq S\}$. For example, if $S = \{1,2,3\}$, then $\mathscr{P}(S) = \{\{\},\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$.

What is the cardinality of $\mathscr{P}(S)$? If $|S| = k$ is finite, then $|\mathscr{P}(S)| = 2^k$. To see this, let us think of each subset of $S$ corresponding to a $k$ bit string, where a 1 in the $i$th position indicates that the $i$th element of $S$ is in the subset, and a 0 indicates that it is not. In the example above, the subset $\{1,3\}$ corresponds to the string 101. Now the number of binary strings of length $k$ is $2^k$, since there are two choices for each bit position. Thus $|\mathscr{P}(S)| = 2^k$. So for finite sets $S$, the cardinality of the power set of $S$ is exponentially larger than the cardinality of $S$. What about infinite (countable) sets? We claim that there is no bijection from $S$ to $\mathscr{P}(S)$, so $\mathscr{P}(S)$ is not countable. Thus for example the set of all subsets of natural numbers is not countable, even though the set of natural numbers itself is countable.

**Theorem:** $|\mathscr{P}(\mathbb{N})| > |\mathbb{N}|$.

**Proof:** Suppose towards a contradiction that there is a bijection $f : \mathbb{N} \to \mathscr{P}(\mathbb{N})$. Recall that we can represent a subset by a binary string, with one bit for each element of $\mathbb{N}$. (So, since $\mathbb{N}$ is infinite, the string will be infinitely long. Contrast the case of $\{0,1\}^*$ discussed earlier, which consists of all binary strings of *finite* length.) Consider the following diagonalization picture in which the function $f$ maps natural numbers $x$ to binary strings which correspond to subsets of $\mathbb{N}$:

[5] Note that $f$ is *not* injective; for example, the ternary strings $0.20222\ldots$ and 0.22 map to binary strings $0.10111\ldots$ and 0.11 respectively, which denote the same real number. Thus $f$ is not a bijection. However, the current proof shows that the cardinality of $C$ is at least that of $[0,1]$, while it is obvious that the cardinality of $C$ is at most that of $[0,1]$ since $C \subset [0,1]$. Hence $C$ has the same cardinality as $[0,1]$ (and as $\mathbb{R}$).



|  | 0 | 1 | 2 | 3 | 4 | 5 ... |
|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 ... |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 ... |
| 2 | 1 | 0 | 1 | 0 | 0 | 0 ... |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| ⋮ |  |  |  |  |  |  |

In this example, we have assigned the following mapping: 0 → {0}, 1 → {}, 2 → {0,2}, ... (i.e., the $n$th row describes the $n^{th}$ subset as follows: if there is a 1 in the $k^{th}$ column, then $k$ is in this subset, else it is not.) Using a similar diagonalization argument to the earlier one, flip each bit along the diagonal: 1 → 0, 0 → 1, and let $b$ denote the resulting binary string. First, we must show that the new element is a subset of $\mathbb{N}$. Clearly it is, since $b$ is an infinite binary string which corresponds to a subset of $\mathbb{N}$. Now suppose $b$ were the $n^{th}$ binary string. This cannot be the case though, since the $n^{th}$ bit of $b$ differs from the $n^{th}$ bit of the diagonal (the bits are flipped). So it's not on our list, but it should be, since we assumed that the list enumerated all possible subsets of $\mathbb{N}$. Thus we have a contradiction, implying that $\mathscr{P}(\mathbb{N})$ is uncountable.

Thus we have seen that the cardinality of $\mathscr{P}(\mathbb{N})$ (the power set of the natural numbers) is strictly larger than the cardinality of $\mathbb{N}$ itself. The cardinality of $\mathbb{N}$ is denoted $\aleph_0$ (pronounced "aleph null"), while that of $\mathscr{P}(\mathbb{N})$ is denoted $2^{\aleph_0}$. It turns out that in fact $\mathscr{P}(\mathbb{N})$ has the same cardinality as $\mathbb{R}$ (the real numbers), and indeed as the real numbers in $[0,1]$. This cardinality is known as $\mathbf{c}$, the "cardinality of the continuum." So we know that $2^{\aleph_0} = \mathbf{c} > \aleph_0$. Even larger infinite cardinalities (or "orders of infinity"), denoted $\aleph_1, \aleph_2, \ldots$, can be defined using the machinery of set theory; these obey (to the uninitiated somewhat bizarre) rules of arithmetic. Several fundamental questions in modern mathematics concern these objects. For example, the famous "continuum hypothesis" asserts that $\mathbf{c} = \aleph_1$ (which is equivalent to saying that there are no sets with cardinality between that of the natural numbers and that of the real numbers).