NOTES ON CARDINALITY

In these notes we discuss how to measure the size of sets. For finite sets this is easy since we can just count the number of elements. However, the issue is more delicate for infinite sets. How do we measure the "size" of an infinite set? Do all infinite sets have the same "size"? Does any of this matter?

We call the size of a set its *cardinality* and denote the cardinality of a set A by $|A|$. We use what are called *cardinal numbers* to describe these cardinalities. The simplest cardinal numbers to deal with are the natural numbers (including 0), which give the cardinalities of finite sets.

Now, let us think about what it should mean for two sets to have the same size, starting with the simple case of finite sets. Clearly, two finite sets should have the same cardinality if and only if they have the same number of elements. Instead of sitting down and counting the number of elements of two finite sets to determine if they have the same size, here is something else we can do: take an element of the first set and pair it with one from the second set, then place those elements aside and pair off two more elements, then two more, etc. Clearly if the finite sets have the same size, we should be able to pair up all elements from each in this way, with nothing left over in either set. The thing to notice is that this pairing up can actually be described by a function! Saying that each element from each set only gets paired up exactly once means that we have an injective function between the two sets (the function sends an element of the first set to the element from the second set that we pair it up with), while saying that nothing is left over means it is surjective. Thus, we conclude that two finite sets have the same size if and only if there is a bijection (i.e. a bijective function) between them.

Since it would be impossible to try and count the number of elements in an infinite set, we need another way of determining cardinality. Luckily the method given above via functions works perfectly well. Intuitively, we should agree that two infinite sets have the same size if and only if we can pair up elements from each in a way so that each element from each gets paired up exactly once and so that there is nothing in either set that does not get paired up. Hence, we make the following definition:

Definition 1. Two sets A and B are said to be *equinumerous* if there exists a bijection between A and B.

The notion of two sets being equinumerous is exactly what we should think of as saying they have the same size. Perhaps the simplest infinite set we can think of is the set of natural numbers $\mathbb{N}$. We have a special term to use for sets which are equinumerous to $\mathbb{N}$:

Definition 2. A set is said to be *denumerable* if it is equinumerous to $\mathbb{N}$. A set is *countable* if it is finite or denumerable; otherwise it is *uncountable*. The cardinality of a countable set is denoted by the cardinal number $\aleph_0$, pronounced "aleph-not".

As a word of caution, note that some authors use the word "countable" to mean "denumerable"; i.e. they would not say that a finite set is countable. We will use the definition given above and will sometimes say "countably infinite" to mean "denumerable".

Now that we have our first infinite cardinal number, $\aleph_0$, we can start figuring out the cardinalities of other sets we know and love. First we consider the set of integers $\mathbb{Z}$. At first glance, since $\mathbb{N}$ is a proper subset of $\mathbb{Z}$, proper meaning that it is a subset of $\mathbb{Z}$ but not equal to $\mathbb{Z}$, you might think that the "size" of $\mathbb{Z}$ should be greater than the "size" of $\mathbb{N}$. However, according to our definition of equinumerous, this is simply not true due to the following:

Proposition 1. *The set of integers $\mathbb{Z}$ is countably infinite.*

To see this, list the integers as

$$0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots$$

We can definite a bijection from $\mathbb{N}$ to $\mathbb{Z}$ by sending 1 to 0, 2 to 1, 3 to -1, and so on, sending the remaining natural numbers to the remaining integers in the list above consecutively. Thus even though $\mathbb{N}$ is a proper subset of $\mathbb{Z}$, both of these sets have the same cardinalities! This is where we start to see interesting facts about cardinalities that we do not see for finite sets. In fact, any countably infinite set is equinumerous with any of its infinite subsets.

Next we consider the rational numbers $\mathbb{Q}$. A bijection between $\mathbb{N}$ and $\mathbb{Q}$ is harder to describe here, but it still exists:

Proposition 2. *The set of rational numbers $\mathbb{Q}$ is countably infinite.*

Before describing such a bijection, we look more closely at what it means for a set to be denumerable. A bijection $f : \mathbb{N} \to S$ between $\mathbb{N}$ and a denumerable set S gives us a way to list the elements of S as

$$f(1), f(2), f(3), \ldots$$

Every element of S will be in this list exactly once if f is a bijection. The thing to notice is that given such a list of all elements of S, we can easily construct a bijection from $\mathbb{N}$ to S by sending 1 to the first term in the list, 2 to the second, and so on just as we did for the integers above. So, if you can find a way to list all elements of an infinite set like this, then that set is countably infinite.

Using this, we can show that $\mathbb{Q}$ is countable as follows: make a table like so

	0	1	-1	2	-2	...
1						
2						
3						
⋮						

Now, in each spot write the rational number given by the integer at the top divided by the natural number on the left. You will then have a table containing all rational numbers. Now we list them like so: start drawing a line at the upper left with $0/1$, then move down one spot to $0/2$, then diagonally up to the right one spot to $1/1$, then right one spot to $-1/1$, then diagonally down to the left two spots to $0/3$, then down one spot to $0/4$, and continue on in this zig-zag pattern. Now list the rational numbers as they appear as you follow the zig-zag pattern from the beginning, omitting any duplicates you come across (for example, $1/2$ would also appear as $2/4$, $3/6$, and so on; only list each rational once). This list then gives you a bijection between $\mathbb{N}$ and $\mathbb{Q}$!

You may be starting to wonder if there are any infinite sets which are not denumerable; i.e. are there any infinite cardinal numbers besides $\aleph_0$? The answer is a resounding yes!

We start with an important lemma. The following argument is known as "Cantor's diagonal argument".

Lemma 1. *There is no surjection from* $\mathbb{N}$ *to the interval* $(0, 1)$.

Proof. Let $f : \mathbb{N} \to (0, 1)$ be any function. We will show that f cannot be surjective. List the numbers in the image of f, using their decimal expansions, as follows:

$$\begin{aligned} f(1) &= 0.a_{11}a_{12}a_{13}\dots \\ f(2) &= 0.a_{21}a_{22}a_{23}\dots \\ f(3) &= 0.a_{31}a_{32}a_{33}\dots \\ &\vdots \end{aligned}$$

Consider the "diagonal" consisting of $a_{11}, a_{22}, a_{33}, \dots$. Define the real number

$$y = 0.y_1y_2y_3\dots$$

by setting

$$y_i = \begin{cases} 2 \text{ if } a_{ii} = 3 \\ 3 \text{ if } a_{ii} \neq 3. \end{cases}$$

Then y is in $(0, 1)$ but is not in the image of f! Indeed, y cannot equal $f(n)$ for any n since it differs from $f(n)$ in the nth decimal place by construction. Hence f is not surjective. $\square$

The lemma in particular implies that $(0, 1)$ is uncountable since if there is no surjection from $\mathbb{N}$ to $(0, 1)$, there is certainly no bijection from $\mathbb{N}$ to $(0, 1)$.

Theorem 1. *The set of real numbers* $\mathbb{R}$ *is uncountable.*

Proof. Let $g : \mathbb{R} \to (0, 1)$ be the function defined by

$$g(x) = \begin{cases} 1/(1 + |x|) & \text{if } x \neq 0, \\ 1/2 & \text{if } x = 0. \end{cases}$$

Then g is surjective (which I leave to you to check). If $\mathbb{R}$ was countable, there would exist a bijection $f : \mathbb{N} \to \mathbb{R}$. But then $g \circ f : \mathbb{N} \to (0, 1)$ would be surjective since it is the composition of surjections. By the lemma such a surjection does not exist, so we conclude that $\mathbb{R}$ is uncountable. $\square$

The cardinality of the set of real numbers is usually denoted by c. This result tells us that even though both $\mathbb{R}$ and $\mathbb{N}$ are infinite, the set of real numbers is in some sense "larger" than the set of natural numbers; we denote this by writing $\aleph_0 < c$. To sum up some of the cardinalities we have computed, we now know that:

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0 \text{ and } |(0,1)| = |\mathbb{R}| = c.$$

Actually we haven't yet shown that $(0,1)$ and $\mathbb{R}$ equinumerous, but we will skip this for now. I invite you to try and show it on your own.

There is a whole area of mathematics dealing with cardinal numbers and their arithmetic, i.e. what it means to add cardinal numbers, multiply cardinal numbers, etc. As we will see below, $\aleph_0$ and c are only the stepping stones into this vast area.

A natural question to ask is whether there exists a set whose cardinality is "between" $\aleph_0$ and c; that is, does there exist an uncountable proper subset of $\mathbb{R}$ that is not equinumerous with $\mathbb{R}$? The suggestion that this is not the case is known as the *continuum hypothesis*. A remarkable result in logic and set theory from the 20th century shows that the continuum hypothesis is *undecidable*, meaning that whether or not it is true or false depends on the axioms for set theory one is using. This is way beyond the scope of this course, but suggests that set theory can indeed become quite complicated and deserves serious study in its own right.

Since we already have at least two different "sizes" of infinity, we can ask how many more there are. Is there such a thing as a largest cardinal number? The answer is no:

Theorem 2. *For any set A, there does not exist a surjection from A to 2^A, the power set of A.*

Proof. Let f be any function from A to 2^A. We will show that f cannot be surjective. If $a \in A$, then $f(a) \in 2^A$ is a subset of A; in particular we can ask whether or not a itself is in this subset. Define the set B by

$$B = \{a \in A \mid a \notin f(a)\}.$$

Then B is a subset of A, but we claim that it is not in the image of f. To see this, by way of contradiction suppose that there exists $b \in A$ so that $f(b) = B$. There are two cases to consider:

- Case 1: If $b \in f(b)$, then $b \in B$ since $f(b) = B$. But by the defining property of B, $b \notin f(b)$, a contradiction.
- Case 2: If $b \notin f(b)$, then $b \in B$ by the defining property of B. Since $B = f(b)$, $b \in f(b)$, a contradiction.

Hence since both possibilities lead to contradictions, we conclude that there does not exist $b \in A$ so that $f(b) = B$ and hence that f is not surjective. $\square$

Since there is always an injection from a set to its power set (which you will show in the exercises), we know that the cardinality of a set is always less than or equal to the cardinality of its power set (in fact, you can take this kind of statement as the definition of what it means for one cardinal number to be less than another). The above result implies that these two cardinalities cannot be equal since there can be no bijection from a set to its power set if there is no surjection; we can state this as a corollary:

Corollary 1. *For any set A, $|A| < |2^A|$.*

So if A is a set, we have an unending list of increasing cardinal numbers

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

showing that there is no largest cardinal number.

The cardinality of the power set of a set A is commonly denoted by $2^{|A|}$ Notice that if F is a finite set, $2^{|F|}$ is exactly the size of the power set of F, as mentioned in the notes on set theory. In those notes, the proof of this fact suggested that you look first at the number of functions from F to $\{0, 1\}$. In fact, in the exercises below you will show that if A is any set, its power set is equinumerous with the set of functions from A to $\{0, 1\}$. It turns out that the power set of $\mathbb{N}$ does in fact have the same cardinality as $\mathbb{R}$, so we can write $2^{\aleph_0} = c$.

Exercises

1. Let A be a set. Construct an injection (don't forget to show that what you construct is in fact an injection) from A into 2^A.

2. Let A be a countably infinite set. Prove that $A \times A$ is countable. Hint: zig-zag!

3. Let A be any set. Show that 2^A is equinumerous with the set of functions from A to $\{0, 1\}$. (This latter set is commonly denoted by $\{0, 1\}^A$; indeed, in general the set of functions from a set B to a set C is commonly denoted by C^B)

4. Show that the relation of being equinumerous is an equivalence relation on the set of all sets. (Actually, there is no such thing as the set of all sets; instead, the collection of all sets forms what is called a *class*. This again is way beyond the scope of this course, so we will ignore this minor detail!)