This is a handout discussing basic results on cardinality, most of which I don't have time to prove or discuss in class. It covers a bit more than Chapter 2.5 of the textbook. Most of the material here is taken from Munkres's *Topology*, Sections 1.6 and 1.7.

Please send any questions/comments/corrections to hhao@berkeley.edu.

1 Finite Sets

Definition 1.1. If $n \in \mathbf{N}$, then we denote $[n]$ to be the subset $\{1, 2, \ldots, n\}$ of $\mathbf{N}$. If $n = 0$, then $[0]$ is defined to be the empty set.

Of course, we have a very good mental picture of what it means for a set to be finite: it means that we can count the elements in that set, starting at 1 and ending at some positive integer n. This is imprecise (because we have not formalized what it means to "count"), but it can easily be made precise: to "count" is to give a bijection between our set and the set of integers from 1 through n. Therefore:

Definition 1.2. A set S is *finite* if there is a bijection $f : S \to [n]$ for some $n \in \mathbf{N} \cup \{0\}$. If $n = 0$, then S has *cardinality* 0, and if $n \geq 1$, S has *cardinality* n. We often write $|S| = n$ or $\#S = n$ to denote this.

When a set is finite, the words "cardinality" and "size" are often interchanged.

Example 1.1. The set $S = \{a, b, c\}$ has cardinality 3, because there is a bijection $f : S \to [n]$: f sends a to 1, b to 2, and c to 3.

Example 1.2. Suppose A is finite and there is a bijection $f : A \to B$. Then B is also finite.

From the above, it is not immediately clear that the cardinality of a finite set is uniquely determined (and we cannot yet say "*the* cardinality of a finite set," as "the" implies uniqueness). That is, suppose S is a finite set with cardinality n, so that there is a bijection between S and $[n]$. This does not yet preclude the possibility that there is a bijection between S and $[m]$ for some $m \neq n$, which would imply S has size n and size m at the same time. Even though this is intuitively impossible, it must be proved and is not something we can take for granted. Unfortunately, the proof is somewhat annoying and requires the use of the "well-ordering property" of the natural numbers $\mathbf{N}$ (which is a property equivalent to the induction axiom). Therefore we only state the technical lemmas, and do not prove them.

First, an exercise involving the special case of the empty set:

Exercise 1.1. The only finite set with cardinality 0 is the empty set. In particular, the cardinality of the empty set is uniquely determined (the empty set has cardinality 0 and does not have cardinality n for any $n \geq 1$).

Proposition 1.1. Let n be a positive integer, A be a nonempty set, and a an element of A. Let $n \geq 0$ be an integer. Then there is a bijection $f : A \to [n+1]$ if and only if there is a bijection $g : A - \{a\} \to [n]$.

Proposition 1.2. Let A be a nonempty set, and assume there is a bijection $f : A \to [n]$ for some $n \in \mathbf{N}$. Let B be a proper subset of A. Then there is no bijection $g : B \to [n]$, and if B is nonempty, there does exist a bijection $h : B \to [m]$ for some $1 \leq m < n$.

Proposition 1.1 can be thought of some sort of "induction tool" for finite cardinalities. It is used to prove Proposition 1.2, which leads to a number of useful consequences. For instance, if A is finite and B is a subset of A, then B is finite.

Corollary 1.1. If A is a finite set, then there is no bijection of A with a proper subset of itself.

Proof. The empty set has no proper subsets, so the corollary is vacuously true in that case. So now assume A is nonempty with B a proper subset of A. Suppose for contradiction that there is a bijection $f : A \to B$, with inverse bijection $f^{-1} : B \to A$. Since A is finite, there is a bijection $g : A \to [n]$ for some $n \in \mathbf{N}$, in which case $g \circ f^{-1}$ is a bijection from B to $[n]$. This contradicts Proposition 1.2. □

Exercise 1.2. Prove that $\mathbf{N}$ is not finite (this "obvious" fact cannot be immediately deduced from the definitions!).

And here is the promised fact:

Corollary 1.2. Let A be a finite set. Then A has a uniquely determined cardinality. In particular, it makes sense to say *the* cardinality of a finite set A.

Proof. From Exercise 1.1, we may assume that A is nonempty. So suppose for contradiction that A is nonempty, and there are distinct positive integers m, n such that A has cardinality m and A has cardinality n. Without loss of generality, $m < n$, so $m+1 \leq n$ and $m+1 \in [n]-[m]$. Then by definition, there are bijections $f : A \to [n]$ and $g : A \to [m]$, so the composition $f \circ g^{-1} : [m] \to [n]$ is also a bijection. Since $[m]$ is a subset of $[n]$ (the latter contains $m+1$ but the former does not), this contradicts Corollary 1.1. □

In particular, if B is a proper subset of a finite set A, then the (uniquely determined) cardinality of B is strictly less than the cardinality of A, by the last part of Proposition 1.2.

Corollary 1.3. Let A and B be finite sets of the same cardinality, and let $f : A \to B$ be a function. Then the following are equivalent:

(1) f is injective.

(2) f is surjective.

(3) f is bijective.

Proof. The case where A and B both have cardinality 0 (so are empty, by Exercise 1.1) is left to the reader. So suppose A and B have a common cardinality $n \geq 1$.

(3) implies (1) and (2) by definition. We now show (1) implies (3). Let $f : A \to B$ be an injective function. We need to show that f is also surjective. Suppose for contradiction that it is not, so $f(A)$ is a *proper* subset of B. Then we induce a *bijection* $f' : A \to f(A)$. Then given a bijection $g : A \to [n]$, we see that $g \circ (f')^{-1} : f(A) \to [n]$ is a bijection between a proper subset of B with $[n]$. This contradicts Proposition 1.2. Hence (1) implies (3).

To show (2) implies (3), we use a result from HW2 that a surjective function $f : A \to B$ is right-invertible, i.e. there exists $h : B \to A$ such that $f \circ h = \mathrm{id}_B$. Then h is left-invertible, so injective (again see HW2), hence bijective by what we just showed. So $f = f \circ h \circ h^{-1} = \mathrm{id}_B \circ h^{-1} = h^{-1}$, so f is the inverse bijection to h. Hence (2) implies (3). □

There are a host of other results one could prove about finite sets using the above propositions. As many of them require the well-ordering axiom of the integers or a similar inductive proof, we won't provide the proofs, but rather just one more convenient fact and corollary:

Proposition 1.3. If A is a nonempty set, then the following are equivalent:

(1) A is finite.

(2) There exists $n \in \mathbf{N}$ such that there is a surjection $f : [n] \to A$.

(3) There exists $m \in \mathbf{N}$ such that there is an injection $g : A \to [m]$.

Corollary 1.4. If $A_1, \ldots, A_n$ are finite sets, then $\bigcup_{i=1}^n A_i$ is finite. Moreover, $\prod_{i=1}^n A_i = A_1 \times A_2 \times \ldots \times A_n$ is also finite, with cardinality $\prod_{i=1}^n |A_i|$.

Proof. We first show the statement about unions when $n = 2$. If A_1 or A_2 is empty, then the union $A_1 \cup A_2$ is either A_2 or A_1, so the result is trivial. Otherwise, neither A_1 nor A_2 are empty, so choose bijections $f : [m] \to A_1$ and $g : [n] \to A_2$ for some positive integers m, n. Define $h : [m + n] \to A_1 \cup A_2$ as follows:

$$h(i) = \begin{cases} f(i) & 1 \leq i \leq m \\ g(i - m) & m + 1 \leq i \leq m + n \end{cases}.$$

Then h is surjective (why?), so by Proposition 1.3, $A_1 \cup A_2$ is finite.

This argument shows that $A_1 \cup A_2$ is finite. Running the same argument shows that $A_1 \cup A_2 \cup A_3 = (A_1 \cup A_2) \cup A_3$ is finite (the union of the two finite sets $A_1 \cup A_2$ and A_3), and so on. So by repeating the same proof (this is an intuitive form of an induction argument), we conclude that $\bigcup_{i=1}^{n} A_i$ is finite. In particular, any finite union of finite sets is finite, since the indexing set I over which the union is taken has a bijection with some $[n]$.

Next, we prove the statement about the Cartesian product, again starting in the case $n = 2$. Again we may assume A_1 and A_2 are nonempty. Then given $a_1 \in A_1$, there is a bijection between $\{a_1\} \times A_2$ and A_2, given by $(a_1, a_2) \mapsto a_2$. Hence $\{a_1\} \times A_2$ is finite for any $a_1 \in A_1$. Now,

$$A_1 \times A_2 = \bigcup_{a_i \in A_1} \{a_1\} \times A_2,$$

and the right-hand side is a finite union (with finite indexing set A_1) of finite sets. By what we proved above, $A_1 \times A_2$ is finite. Then the same induction argument as before shows that $\prod_{i=1}^{n} A_i$ is finite for any $n \in \mathbf{N}$.

The last statement about cardinality is left as an exercise. $\square$

2 Infinite Sets

Definition 2.1. A set that is not finite is called *infinite*.

Definition 2.2. If A is an infinite set, and if there is a bijection $f : A \to \mathbf{N}$, then A is called *countably infinite*. A *countable* set is any finite or countably infinite set. Otherwise, A is *uncountably infinite* or *uncountable*.

The intuition for a countably infinite set is that the bijection from A to $\mathbf{N}$ allows us to "place the elements of A in order and count them."

As an example, $\mathbf{N}$ is countable. What is less obvious is that the following sets are countable, because they both seem to differ from $\mathbf{N}$ by "infinitely many elements":

Example 2.1. The set S of even integers is countable. This is because the map $f : \mathbf{N} \to S$, $f(n) = 2n$ is a bijection.

Example 2.2. The set $\mathbf{Z}$ of all integers is countable. We define a function $f : \mathbf{Z} \to \mathbf{N}$ as follows:

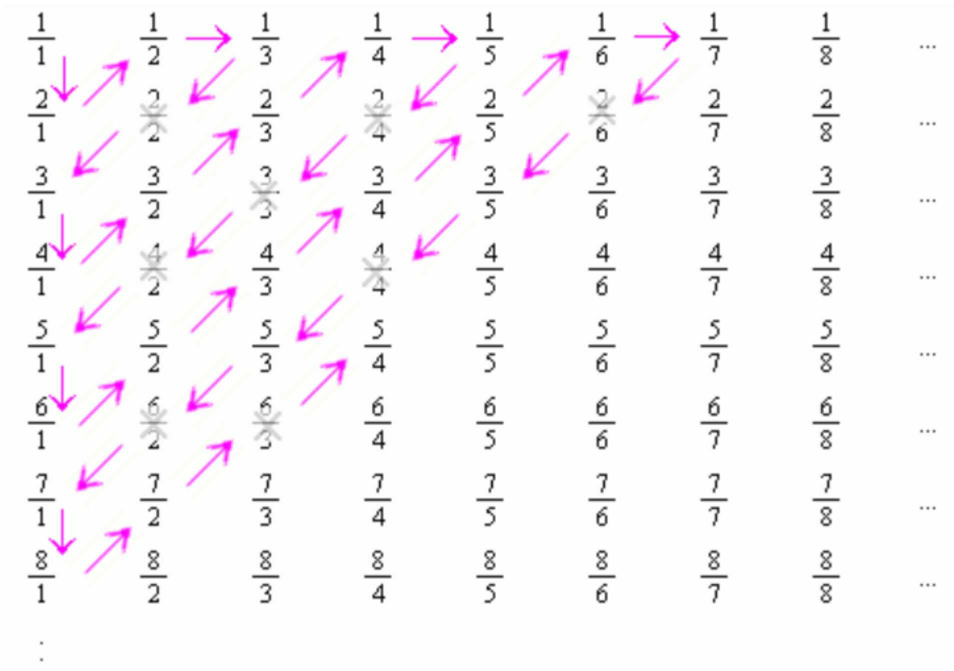
$$f(0) = 0, f(1) = 1, f(-1) = 2, f(2) = 3, f(-2) = 4, \ldots.$$

One can express this function in closed form as

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

We leave it to the reader to check that f is bijective.

Perhaps even more surprising is that **Q** is countable. Here is a "proof without words:"



Unfortunately, this picture, while very helpful for intuition, does not give a precise proof. We will give such a proof below after some preliminary facts. Again, these will be stated without proof, since the proofs are quite tedious and involve notions about well-ordering and recursion that we have not yet discussed.

Lemma 2.1. An infinite subset of **N** is countably infinite.

Proposition 2.1. If A is a nonempty set, then the following are equivalent:

(1) A is countable (possibly finite).

(2) There exists a surjection $f : \mathbf{N} \to A$.

(3) There exists an injection $g : A \to \mathbf{N}$.

Compare this result with Proposition 1.3.

All the hard work is pushed into this proposition, and so we are free to derive many useful consequences:

Corollary 2.1. A subset of a countable set is countable.

The intuition is that countable sets are "small", so a subset of a small set is still small.

Proof. If B is a subset of countable A, then by Proposition 2.1, there is an injection $g : A \to \mathbf{N}$. Then the restriction $g|_B : B \to \mathbf{N}$ is injective, so B is countable. $\square$

Corollary 2.2. The set $\mathbf{N} \times \mathbf{N}$ is countable.

Proof. By Proposition 2.1, we just need to give an injection $f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$. Consider the map given by $f(a, b) = 2^a 3^b$. One can use the fundamental theorem of arithmetic to prove that this is injective, but this is not necessary. Indeed, assume $2^a 3^b = 2^c 3^d$. Then if $a \neq c$, then WLOG $a > c$, so $2^{a-c} 3^b = 3^d$. The left-hand side is even (as $a - c > 0$), but the right-hand side is odd, which is absurd. Therefore $a = c$, and we have $2^a 3^b = 2^a 3^d \Rightarrow 3^b = 3^d$. Then if $b \neq d$, then WLOG $b > d$, so $3^{b-d} = 1$. The left-hand side is divisible by 3 (as $b - d > 0$), but the right-hand side is not, contradiction. Therefore $b = d$, so $(a, c) = (b, d)$, which shows that f is injective. $\square$

As promised, we can now prove that $\mathbf{Q}$ is countable.

Example 2.3. The set of rationals $\mathbf{Q}$ is countable. One method of proof is given by the image on the previous page. The idea is to define a bijection from $\mathbf{N}$ to $\mathbf{Q}$ by "counting via diagonals," but this idea takes a bit of work to make rigorous. The main roadblock is that we need to "recursively" define our function (i.e. $f(n + 1)$ is defined in terms of $f(n)$), and making this precise is quite painful. But armed with our current machinery, we can give a much better proof. Indeed, since $\mathbf{N} \times \mathbf{N}$ is countable, and there is a bijection $f : \mathbf{N} \to \mathbf{Z}$, we can give a bijection $\mathbf{N} \times \mathbf{N} \to \mathbf{Z} \times \mathbf{Z}$ by $(a, b) \mapsto (f(a), f(b))$. Therefore $\mathbf{Z} \times \mathbf{Z}$ is countable. Then there is a surjection $g : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Q}$ given by

$$g(a, b) = \begin{cases} \frac{a}{b} & b \neq 0 \\ 0 & b = 0 \end{cases}.$$

By Proposition 2.1, there is a surjection $h : \mathbf{N} \to \mathbf{Z}$. Then the composition $g \circ h : \mathbf{N} \to \mathbf{Q}$ is a surjection, so $\mathbf{Q}$ is countable.

The intuition for this argument is that "rationals are represented by some ordered pair of integers". Since the set of such ordered pairs is countable, then $\mathbf{Q}$ should be as well.

These next two propositions allow us to create new countable sets from known ones.

Proposition 2.2. Let I be a countable index set, and let $\{A_i\}_{i \in I}$ be a countable collection of sets indexed by the $i \in I$. Suppose all the A_i are countable. Then $\bigcup_{i \in I} A_i$ is countable (a countable union of countable sets is countable).

The intuition should be that the proof goes along the same lines as the above proof that $\mathbf{Q}$ is countable (after unraveling said proof to see what is really going on). Indeed, one could express $\mathbf{Q}$ as a countable union of subsets Q_n, where Q_n is the set of rationals that can be expressed as a fraction of integers with numerator n.

Proof. Each A_i is countable, so for each i, choose a surjection $f_i : \mathbf{N} \to A_i$. Similarly, the index set I is countable, so choose a surjection $g : \mathbf{N} \to I$. Then define $h : \mathbf{N} \times \mathbf{N} \to \bigcup_{i \in I} A_i$ by $h(a, b) = f_{g(a)}(b)$. That is, given an ordered pair (a, b), choose the element in $A_{g(a)}$ that is the image of $f_{g(a)}(b)$. The function h is surjective, because every element x in the union is an element of A_i for some $i \in I$, so if $b \in \mathbf{N}$ is such that $f_i(b) = x$ and $a \in \mathbf{N}$ is such that $g(a) = i$, then $h(a, b) = x$. We conclude that $\bigcup_{i \in I} A_i$ is countable in the same manner as in Example 2.3. □

Proposition 2.3. Let $A_1, \ldots, A_n$ be finitely many countable sets. Then the product $\prod_{i=1}^{n} A_i$ is countable (a finite product of countable sets is countable).

Proof. By the same inductive argument as in Corollary 1.4, it suffices to prove the proposition in the case $n = 2$. If either A_1 or A_2 is empty, then so is the product, so the proposition is trivially true. So suppose A_1 and A_2 are nonempty. Pick surjections $f : \mathbf{N} \to A_1$ and $g : \mathbf{N} \to A_2$. Then $h : \mathbf{N} \times \mathbf{N} \to A_1 \times A_2$, $h(a, b) = (f(a), g(b))$ is surjective, so we conclude that $A_1 \times A_2$ is countable in the same manner as in Example 2.3.

Again, note how similar this is to the proof that $\mathbf{Q}$ is countable! □

Now, we have given many examples of countable sets. We have $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{Z} \times \mathbf{Z}$, $\mathbf{Q} \times \mathbf{Q}$, any subset thereof, etc. On the other hand, we have not given an example of any uncountable set. We will do that now:

Theorem 2.1. The set $\mathbf{R}$ of real numbers is uncountable.

One proof uses a famous argument known as *Cantor's diagonal argument*, which you will replicate on HW2. On the other hand, the proof uses properties of the decimal expansions of real numbers, which are actually not elementary to develop from the basic axioms of $\mathbf{R}$. So we will be taking a lot of background on faith here, which means our proof is not developed from "first principles." There are "better" proofs of this theorem without using the decimal expansion of real numbers, but as for guiding intuition, Cantor's proof is still the best.

Proof. We will assume without proof that every real number has a *unique* decimal expansion, with the caveat that we never allow decimal expansions ending in an infinite string of consecutive 9's (as $0.999\ldots = 1.00\ldots$). Such a decimal expansion can be made infinite by padding a string of trailing zeros, if necessary.

We actually prove that the subset $[0, 1)$ is uncountable. Suppose for contradiction that it were. Then there is a surjection $f : \mathbf{N} \to [0, 1)$. Given $n \in \mathbf{N}$, let a_n be the nth digit (after the decimal point) of the unique decimal expansion of $f(n)$. Let b_n be an integer in $[0, 9]$ that does not equal a_n or 9. Then consider the real number r with decimal expansion

$$0.b_1 b_2 b_3 b_4 \ldots,$$

which by construction of the b_n's, does not end in an infinite string of consecutive 9's. This is some real number in $[0, 1)$, but $r \neq f(n)$ for any n. Indeed, by construction, the decimal expansion of r differs from the decimal expansion of $f(n)$ in the nth digit, and because such a decimal expansion is *unique*, we have $r \neq f(n)$. But this contradicts the surjectivity of f, because we constructed r not in the image of f.

To complete the proof, we use the fact that $[0, 1)$ is uncountable to show that $\mathbf{R}$ is uncountable.

Lemma 2.2. If B is a subset of a set A and B is uncountable, then A is uncountable.

Similarly to before, the intuition is that uncountable sets are "large", so a superset of a large set is still large.

Proof. Suppose for contradiction that A is countable. Then there is an injection $f : A \to \mathbf{N}$. But there is an injection $g : B \to A$ given by inclusion of B into A (i.e. $g(b) = b$, where the first b is considered as an element of B, and the second as an element of A), so $g \circ f : B \to \mathbf{N}$ is an injection. This contradicts the assumption that B is uncountable. □

Now apply this lemma to the subset $[0, 1) \subseteq \mathbf{R}$. □

Let's demonstrate how the diagonal element works intuitively and see where its name comes from. Suppose for contradiction that $[0, 1)$ was countable. Then we can order its elements according to some surjection $f : \mathbf{N} \to A$:

$$f(1) = 0.\mathbf{2}56283057\ldots$$
$$f(2) = 0.1\mathbf{7}9456238\ldots$$
$$f(3) = 0.65\mathbf{0}486171\ldots$$
$$f(4) = 0.210\mathbf{6}08969\ldots$$
$$f(5) = 0.1111\mathbf{7}1823\ldots$$

Then if we construct a decimal in $[0, 1)$ whose nth digit after the decimal point always differs from the bolded nth digit of $f(n)$, such as $r = 0.32123\ldots$, then r can never be written down in the list of $f(n)$'s, so our "counting/ordering procedure" never gets to r.

Corollary 2.3. The set of complex numbers $\mathbf{C}$ is uncountable.

Proof. $\mathbf{C}$ contains $\mathbf{R}$ as a subset, so apply Lemma 2.2 and Theorem 2.1. □

Corollary 2.4. The set $\mathbf{R} - \mathbf{Q}$ of irrational numbers is uncountable.

Proof. Otherwise $\mathbf{R} = \mathbf{Q} \cup (\mathbf{R} - \mathbf{Q})$ would be countable by Proposition 2.2. □

The diagonal argument can produce more examples of uncountable sets. As examples:

Example 2.4. In Proposition 2.3, we showed that a *finite* product of countable sets is countable. On the other hand, an infinite product of countable sets is usually not countable, even if all the sets in question are finite (but have cardinality greater than 1). As an example, if X is the two-element set $\{0,1\}$, then the infinite product

$$\prod_{n=1}^{\infty}\{0.1\} = \{0,1\} \times \{0,1\} \times \{0,1\} \times \dots$$

is uncountable. The proof is left as an exercise (mimic the diagonal argument again).

Example 2.5. Suppose S is a countably infinite set (e.g. $S = \mathbf{Z}$). Then $\mathcal{P}(S)$, the power set of S, is uncountable. It suffices to prove that there is no surjection $S \to \mathcal{P}(S)$. Indeed, if $\mathcal{P}(S)$ were then countable, with a bijection $f : \mathcal{P}(S) \to \mathbf{N}$, then given some bijection $g : S \to \mathbf{N}$, $f^{-1} \circ g$ would be a bijection $S \to \mathcal{P}(S)$, a contradiction.

The proof that there is no surjection $S \to \mathcal{P}(S)$ is on HW2—it uses yet another variant of Cantor's diagonal argument.

3 Comparing Cardinalities

So far, we have split sets into three different types: the finite sets, the countably infinite sets, and the uncountably infinite sets. Our intuition tells us that the finite sets are the "smallest", followed by the countably infinite sets, and then the uncountably infinite sets are the "largest." We now make this precise by extending the idea of cardinality to infinite sets.

Definition 3.1. Let A and B be sets, possibly infinite. We say that *the cardinality of A is less than or equal to the cardinality of B*, written $|A| \leq |B|$, if there exists an injection from A to B. In this case, we can also write $|B| \geq |A|$ (this notation will be justified in Proposition 3.1).

We say that *the cardinality of A equals the cardinality of B*, written $|A| = |B|$, if there is a bijection from A to B. It may be the case that the cardinality of A is less than or equal to that of B, but not equal to the cardinality of B, in which case we write $|A| < |B|$.

There are many things to say about the above definition. First, we note that when A and B are finite, the definition agrees with our results from Section 1. In particular, if A and B are nonempty finite sets, with A having cardinality m and B having cardinality n, then $m \leq n$ if and only if $|A| \leq |B|$ in the sense of the above Definition 3.1: if $m \leq n$, then if we compose bijections $A \to [m]$ and $[n] \to B$ with an injection $[m] \to [n]$ in the right order, then we get an injection $A \to B$. Conversely, suppose $m > n$. Then supposing for contradiction that there is an injection $A \to B$, then there is an injection $f : [m] \to [n]$.

Then f restricts to a bijection $[m] \to \text{Im}(f)$, and by Proposition 1.2, then there is a bijection $\text{Im}(f) \to [n]$ if $\text{Im}(f) = [n]$ (in which case f is bijective), or a bijection $\text{Im}(f) \to [k]$ for some $1 \leq k < n$. In either case, there is a bijection of $\text{Im}(f)$ with a set $[k]$ for some $k \leq n < m$, hence a bijection of $[m]$ with its proper subset $[k]$. This contradicts, say, Corollary 1.1, so we must have $m \leq n$.

More importantly, we have not defined what $|A|$ is for infinite sets A. An initial idea is to just use the special symbol ∞, but we have already seen that we have to distinguish countably infinite and uncountable sets: they do not have the same cardinality. So if A is countably infinite but B is uncountably, we cannot represent $|A|$ and $|B|$ by the same symbol ∞.

It turns out that there is a system of "arithmetic," called *cardinal arithmetic*, that allows us to differentiate and manipulate (e.g. add/multiply) these different "sizes of infinity" in a rigorous way. For example, the *cardinal number* $\aleph_0$ is defined to be the cardinality of a countable set. One can define a "next-smallest cardinal," $\aleph_1$, which we would like to say is the cardinality of $\mathbf{R}$; that is, that $\mathbf{R}$ is the "smallest non-countably infinite set." This statement is the famous *continuum hypothesis* of set theory, which is in fact *unprovable*(!!!) under the usual *ZFC axioms* of set theory. Showing that the continuum hypothesis was unprovable won Paul Cohen a Fields Medal in 1966.

We do not discuss cardinal arithmetic any further; those interested should take an advanced course on set theory. We will only prove some basic results on comparing cardinalities.

Example 3.1. If B is a subset of A, then $|B| \leq |A|$.

Example 3.2. All countably infinite sets have the same cardinality, as they are all in bijection with each other (via a bijection with $\mathbf{N}$).

Example 3.3. We have $|\mathbf{Q}| < |\mathbf{R}|$ as there is an obvious injection $\mathbf{Q} \to \mathbf{R}$, and we have the strict inequality because $\mathbf{R}$ is not countable.

Example 3.4. If A, B, and C are sets with $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$. Hence the "cardinality comparison operator" $\leq$ is *transitive*.

Proposition 3.1. Suppose there is a surjection from B to A. Then $|A| \leq |B|$.

Proof. On HW2, it is proved that the existence of a surjection $g : B \to A$ implies the existence of an injection $A \to B$. $\square$

This solidifies the following intuition: the existence of an injection $A \to B$ means that A is "smaller than B", and conversely the existence of a surjection $A \to B$ means that A is "larger than B".

Let us now make precise our intuition that the countably infinite sets are the "smallest infinite sets."

Proposition 3.2. Let A be an infinite set. Then there exists a countably infinite subset B of A. In particular, $|\mathbf{N}| = |B| \leq |A|$.

Proof. The proof requires a "recursive definition" of a function. Since we do not want to bother ourselves with all the tedious details of making this precise, we will sweep them under the rug, and content ourselves with a plausible but not-entirely-rigorous proof. In the course of the proof, I also need to invoke the axiom of choice, but this will also be swept under the rug without comment (unfortunately, the axiom of choice cannot be avoided: see here).

Since A is infinite, it is not empty by definition. So pick some $a_1 \in A$. We define a function $f : \mathbf{N} \to A$, first by setting $f(1) = a_1$. Next, consider the subset $A - \{a_1\}$ of A. This must be nonempty, because otherwise there is a surjection $[1] \to A$ given by $1 \mapsto a_1$, contradicting the infinite-ness of A (recall Proposition 1.3). Therefore there is some $a_2 \in A - \{a_1\}$. Set $f(2) = a_2$.

We continue in this fashion. Given $n \geq 3$, suppose we have picked $a_1, \ldots, a_{n-1}$ such that for any $1 \leq k \leq n-1$, a_k was picked to be in the nonempty set $A - \{a_1, a_2, \ldots, a_{k-1}\}$, and we have set $f(k) = a_k$. Then $A - \{a_1, \ldots, a_{n-1}\}$ is nonempty, as otherwise there is a surjection $[n-1] \to A$ given by $m \mapsto a_m$. So pick some $a_n \in A - \{a_1, \ldots, a_{n-1}\}$, and set $f(n) = a_n$. This "inductively/recursively" defines $f(n)$ for all $n \in \mathbf{N}$.

We claim that f is injective. Suppose m and n are distinct positive integers, so WLOG $m < n$ and $m \leq n - 1$. Then by construction, $a_n = f(n)$ is in $A - \{a_1, \ldots, a_{n-1}\}$. In particular, since $a_m \in \{a_1, \ldots, a_{n-1}\}$, we have $a_n \neq a_m = f(m)$, so f is an injection $\mathbf{N} \to A$. Since f induces a bijection from $\mathbf{N}$ to $\mathrm{Im}(f) \subseteq A$, we have produced the desired countably infinite subset $\mathrm{Im}(f)$ of A. □

Example 3.5. As another example, let S be any set, and $\mathcal{P}(S)$ its power set. Then because we know from Example 2.5 that there is no bijection $S \to \mathcal{P}(\mathcal{S})$, we have $|S| \neq |\mathcal{P}(\mathcal{S})|$. But you will prove on HW2 that $|S| \leq \mathcal{P}(S)$, so we in fact have $|S| < \mathcal{P}(S)$.

We end by stating two facts which seem intuitively obvious, but actually tricky to prove. First, from our intuition with inequalities of real numbers, we know that given two real numbers x and y, then either $x \leq y$ or $y \leq x$. On the other hand, it is not so clear that given two sets A and B, then either $|A| \leq |B|$ or $|B| \leq |A|$ (this would upgrade the "cardinality comparison operator" $\leq$ from a *partial order* to a *total order*, a concept that we will discuss later in the class). Proving this would require the construction of an injection from A to B, or one from B to A, and it is not obvious that one in either direction exists, especially when A and B are both uncountably infinite. Fortunately, the statement is true:

Proposition 3.3. If A and B are sets, then either $|A| \leq |B|$ or $|B| \leq |A|$.

The proof requires a variant of the axiom of choice known as *Zorn's Lemma* (which is *very* useful in algebraic applications, as you might learn in a future math course).

Finally, we also know that if x and y are real numbers, and if we have both $x \leq y$ and $y \leq x$, then $x = y$. Again, this is not so clear with cardinalities. Even if we assume that $|A| \leq |B|$ and $|B| \leq |A|$, or in other words, that we have injections $f : A \to B$ and $g : B \to A$, it is not clear how to build a bijection $h : A \to B$ to conclude that $|A| = |B|$. Certainly our injections need not be inverse bijections, or even bijections at all: consider the case when $A = B = \mathbf{Z}$, $f(x) = 2x$, and $g(x) = 3x$. Fortunately, there is the amazing theorem:

Theorem 3.1 (Schroeder-Bernstein)**.** If A and B are sets with $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

The proof is outlined in Exercise 2.5.41 of our textbook.

As a sample application, we prove that $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ has the same cardinality as $\mathbf{R}$ (something we were not able to do before).

Proposition 3.4. We have $|\mathbf{R}^2| = |\mathbf{R}|$.

Proof. By Theorem 3.1, it suffices to find injections $\mathbf{R}^2 \to \mathbf{R}$ and $\mathbf{R} \to \mathbf{R}^2$. The latter is easy: take $f : \mathbf{R} \to \mathbf{R}^2$, $f(r) = (r, 0)$. For the former, we first note that the function

$$g : (0,1) \to \mathbf{R}, g(x) = \frac{2x-1}{2x(1-x)}$$

is a bijection (exercise: check this).[1] Therefore there is a bijection from $(0,1)^2$ to $\mathbf{R}^2$, which means that we can construct an injection $\mathbf{R}^2 \to \mathbf{R}$ by constructing an injection $(0,1)^2 \to (0,1)$, and then composing various bijections with this injection.

We repeat the setup and assumptions of Theorem 2.1, where every real number in $(0,1)$ has a unique decimal expansion that does not end in an infinite string of consecutive 9's. Then we define a function $h : (0,1)^2 \to (0,1)$ as follows:

$$h(0.a_1a_2a_3\ldots, 0.b_1b_2b_3\ldots) = 0.a_1b_1a_2b_2a_3b_3\ldots.$$

Because neither $0.a_1a_2a_3\ldots$ nor $0.b_1b_2b_3\ldots$ end in an infinite string of consecutive 9's, $0.a_1b_1a_2b_2a_3b_3\ldots$ does not either. Using the *uniqueness* of the decimal expansion, one can check that h is injective (exercise: check this too). So h induces an injection $\mathbf{R}^2 \to \mathbf{R}$, and we have proved that $|\mathbf{R}^2| = |\mathbf{R}|$ via application of the Schroeder-Bernstein theorem. □

[1] One can also show that there is a bijection betwen $(0,1)$ and $\mathbf{R}$ via the Schroeder-Bernstein theorem, but this is surely overkill.