1 *Formalizing Cardinality*

Given any two sets A and B, we define what it means to compare the cardinality of A to the cardinality of B as follows.[1]

$$|A| \leqslant |B| \;:\Leftrightarrow\; \exists f : A \to B \text{ such that } f \text{ is injective.}$$
$$|A| \geqslant |B| \;:\Leftrightarrow\; \exists f : A \to B \text{ such that } f \text{ is surjective.}$$
$$|A| = |B| \;:\Leftrightarrow\; \exists f : A \to B \text{ such that } f \text{ is bijective.}$$

[1] Recall *"injective"* and *"surjective"* are synonymous with *"one-to-one"* and *"onto"* respectively.

The idea that $|A| < |B|$ means $|A| \leqslant |B|$ and $|A| \neq |B|$ simultaneously, along with the analogous idea for $|A| > |B|$, implies the following results.

$$|A| < |B| \;\Leftrightarrow\; \forall f : A \to B, f \text{ is not surjective.}$$
$$|A| > |B| \;\Leftrightarrow\; \forall f : A \to B, f \text{ is not injective.}$$

Using functions to formalize our notion of *"the size of a set"* has the potential to drastically complicate things. Thankfully, several theorems simplify the situation.

Axiom: The Trichotomy of Cardinality.
For any two sets A and B, either $|A| \leqslant |B|$ or $|A| \geqslant |B|$.

This is equivalent to the Axiom of Choice. lmao

Theorem 1: Cantor-Schröder-Bernstein.
For any sets A and B for which there exist functions $f : A \to B$ and $g : B \to A$, if f and g are both *injective,* then there exists $h : A \to B$ such that h is a bijection.

A note for math majors: This theorem has a surjective analogue, but its proof requires the use of the Axiom of Choice.

Corollary 1.
For any sets A and B such that $|A| \leqslant |B|$ and $|B| \leqslant |A|$, we have $|A| = |B|$.

Theorem 2.
For any sets A and B for which there exist functions $f : A \to B$ and $g : B \to A$, if f and g are both injective, then there exists $h : A \to B$ such that h is a bijection.

Corollary 2.
For any sets A and B, we have $|A| \leqslant |B| \wedge |B| \leqslant |A| \Rightarrow |A| = |B|$.

Theorem 3.
For any two sets A and B, the following equivalences hold.[2]

$$|A| < |B| \;\Leftrightarrow\; |B| > |A|$$
$$|A| \leqslant |B| \;\Leftrightarrow\; |B| \geqslant |A|$$
$$|A| = |B| \;\Leftrightarrow\; |B| = |A|$$

[2] A note for math majors: This theorem Let A and B be sets. If $\varphi : A \to B$ is injective, then φ *always* has a surjective left-inverse. However, if $\psi : B \to A$ is surjective, then ψ only has an injective right-inverse if we assume the Axiom of Choice.
Thus, without the Axiom of Choice, we don't have the right-to-left directions of these equivalences for *all* sets, and the theorem fails.

2 Results from Lecture

Exercise 1. Show that $|\mathbb{N}| = |\mathbb{N}_+|$.

Proof. Consider the function $f : \mathbb{N} \to \mathbb{N}_+$ given by $f(x) := x + 1$ for all $x \in \mathbb{N}_+$. We will prove that f is a bijection.

Injectivity:
Let $x, y \in \mathbb{N}$ and suppose $f(x) = f(y)$. We then have $x + 1 = y + 1$, so that $x = y$.

Surjectivity:
Let $y \in \mathbb{N}_+$ and notice that $y - 1 \geqslant 0$ since $y \geqslant 1$. Then, $f(y - 1) = (y - 1) + 1 = y$.

Therefore, f is a bijection, and we can conclude $|\mathbb{N}| = |\mathbb{N}_+|$. QED

Exercise 2. Show that, for every $k \in \mathbb{N}$, we have $|\mathbb{N}| = |\mathbb{N} - \{0, 1, \ldots, k\}|$.

Proof. We follow the same idea as the previous exercise. Let $k \in \mathbb{N}$ and consider the function $f : \mathbb{N} \to \mathbb{N} - \{0, 1, \ldots, k\}$ given by $f(x) := x + k$ for all $x \in \mathbb{N}$.

Injectivity:
Let $x, y \in \mathbb{N}$ and suppose $f(x) = f(y)$. We then have $x + k = y + k$, so that $x = y$.

Surjectivity:
Let $y \in \mathbb{N} - \{0, 1, \ldots k\}$, which means $y \in \mathbb{N}$ and $y \notin \{0, 1, \ldots, k\}$ by definition. This implies $y \geqslant k + 1$, so that $y - k \geqslant 0$. We can the observe $f(y - k) = (y - k) + k = y$.

Therefore, f is a bijection, and we can conclude $|\mathbb{N}| = |\mathbb{N} - \{0, 1, \ldots, k\}|$. QED

Exercise 3. Let $\mathbb{N}_e = \{n \in \mathbb{N} \mid \exists k \in \mathbb{Z}, n = 2k\}$. Show that $|\mathbb{N}| = |\mathbb{N}_e|$.

Proof. Consider the function $f : \mathbb{N} \to \mathbb{N}_e$ given by $f(x) := 2x$ for all $x \in \mathbb{N}$.

Injectivity:
Let $x, y \in \mathbb{N}$ and suppose $f(x) = f(y)$, so that $2x = 2y$ by definition. Then $x = y$ clearly.

Surjectivity:
Let $y \in \mathbb{N}_e$. By definition, there then exists $k \in \mathbb{Z}$ such that $y = 2k$. Since $y \geqslant 0$, we know $2k \geqslant 0$, so that $k \geqslant 0$, implying $y \in \mathbb{N}$. We then see $f(k) = 2k = y$ of course.

Therefore, f is a bijection, and we can conclude that $|\mathbb{N}| = |\mathbb{N}_e|$. QED

Exercise 4. Show that $|\mathbb{N}| = |\mathbb{Z}|$.

For this proof, see the in-class notes from Week 5 (the *23rd of September, 2025*).

Exercise 5. Show that $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$.

Proof. We proceed by constructing two injections in opposite directions.

First, consider the function $\varphi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ given by $\varphi(n) := (n, 0)$ for all $n \in \mathbb{N}$. To prove that φ is injective, take $n, m \in \mathbb{N}$ and suppose $\varphi(n) = \varphi(m)$. Then, by definition, we know $(n, 0) = (m, 0)$, so that $n = m$. Thus, φ is an injection.[3]

[3] We say $(a, b) = (x, y)$ when $a = x$ and $b = y$.

Second, consider the function $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by $\psi(x, y) := 2^x 3^y$. To prove that ψ is injective, let $(a, b), (x, y) \in \mathbb{N} \times \mathbb{N}$ and assume $\psi(a, b) = \psi(x, y)$. We then have $2^a 3^b = 2^x 3^y$ by the definition of ψ.[4] Dividing both sides by $2^x 3^y$ yields $2^{a-x} 3^{b-y} = 1$. Since the exponential function with any base is always non-negative, and since $a, b, x, y \in \mathbb{N}$, we know $2^{a-x} \in \mathbb{N}_+$ and $3^{b-y} \in \mathbb{N}_+$. This implies that $2^{a-x} = 1 = 3^{b-y}$, from which $a - x = 0$ and $b - y = 0$ readily follows. We can immediately deduce $a = x$ and $b = y$, so that $(a, b) = (x, y)$ as desired.

Now, we have an injection $\varphi : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ and another injection $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. By the *Cantor-Schröder-Bernstein Theorem,* there exists a function $\rho : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ such that ρ is a bijection, letting us conclude $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. QED

[4] If we recall the precise statement of the *Fundamental Theorem of Arithmetic,* then we could finish this branch of the proof off right here by arguing that, if any of a, b, x, y are nonzero, then $2^a 3^b \geqslant 2$ and $2^x 3^y \geqslant 2$, so that $a = x$ and $b = y$ by the *uniqueness* of their prime factorizations. This would be a much *"tighter"* argument with less *"leaps of logic"* than the one presented.

3 Countability

We say, by definition, that a set X is *countable* when $|X| \leqslant |\mathbb{N}|$, meaning that X can be *injected* into $\mathbb{N}$. A countable set that is also infinite is called *countably infinite.* In the previous section, we showed that most of the infinite sets we commonly deal with are actually countable. Additionally, every finite set is (obviously) countable.[5] All of those proofs relied on defining some functions and proving they were injective, surjective, or bijective. There are, however, more *"sophisticated"* techniques.

[5] As a simple exercise, think about how you might prove this.

Theorem 4: Dedekind Infinite Means Infinite.
For any set X, we have that X is infinite if and only if $\exists Y \subsetneq X$ such that $|Y| = |X|$.

The earliest known definition of what it means for a set to be *infinite* that did not rely on the natural numbers was due to Richard Dedekind; he characterized infinite sets as those that contain an equinumerous proper subset. This theorem establishes that this notion of infinity is exactly the usual one (as long as we assume something along the lines of the Axiom of Countable Choice).

Lemma 1.
If X is infinite, then $|\mathbb{N}| \leqslant |X|$.

Lemma 2.
If A is an infinite set and B is a set, then $|A \cup B| = \max(|A|, |B|)$.

Theorem 5: Countable Unions of Countable Sets are Countable.
Let $\mathcal{A} := \{A_i \mid i \in \mathbb{N}\}$, where $|A_i| \leqslant |\mathbb{N}|$ for all $i \in \mathbb{N}$. The following then holds.

$$\left| \bigcup_{i \in \mathbb{N}} A_i \right| \leqslant |\mathbb{N}|$$

Further, if $\exists i \in \mathbb{N}$ such that A_i is infinite, then $\left| \bigcup_{i \in \mathbb{N}} A_i \right| = |\mathbb{N}|$.

Note that the notation $\bigcup_{i \in \mathbb{N}} A_i$ is a more precise way of writing $\bigcup_{i=0}^{\infty} A_i$, which is perhaps more familiar. The same convention applies more generally: $\sum_{i \in \mathbb{N}} a_i$ is a more precise way of writing $\sum_{i=0}^{\infty} a_i$.

3.1 Finite Strings

We represent a binary string of length $k \in \mathbb{N}$ as a function whose domain is $\{0, 1, \ldots, k\}$ and whose codomain is $\{0, 1\}$. For example, the string `"010110"` is encoded by the function $f : \{0, 1, 2, 3, 4, 5\} \to \{0, 1\}$ defined below.

$$\begin{aligned} f(0) &:= 0 & \quad f(3) &:= 1 \\ f(1) &:= 1 & \quad f(4) &:= 1 \\ f(2) &:= 0 & \quad f(5) &:= 0 \end{aligned}$$

We can then define the *length* of a string s, denoted $\texttt{len}(s)$, to be the domain of s.

Exercise 6. Let $\mathfrak{B} = \{f \mid \exists k \in \mathbb{N}, f : \{0, ..., k-1\} \to \{0,1\}\}$ be the set of all finite-length binary strings. Show that $\mathfrak{B}$ is countably infinite.[6]

Proof. First, let's show that $\mathfrak{B}$ is infinite. Towards a contradiction, suppose $\mathfrak{B}$ is finite. Consider $\mathfrak{D} := \{\texttt{len}(\mathfrak{b}) \mid \mathfrak{b} \in \mathfrak{B}\}$. Since $\mathfrak{B}$ is finite, we know $\mathfrak{D}$ is also finite.[7] Combining this with the fact that $\mathfrak{D} \subseteq \mathbb{N}$, we know there is a maximal element $\mathfrak{d}_{\max} \in \mathfrak{D}$ corresponding with the length of (at least) one string $\mathfrak{b}_{\max} \in \mathfrak{B}$.[8] What we know now is that, for any string $\mathfrak{b} \in \mathfrak{B}$, we have $\texttt{len}(\mathfrak{b}_{\max}) \geqslant \texttt{len}(\mathfrak{b})$.

Now, consider the string $\mathfrak{c}$ defined by appending exactly one `"0"` to $\mathfrak{b}_{\max}$. We can see that $\texttt{len}(\mathfrak{c}) = \texttt{len}(\mathfrak{b}_{\max}) + 1 > \texttt{len}(\mathfrak{b}_{\max})$, but this also implies that $\mathfrak{c} \in \mathfrak{B}$ since $\texttt{len}(\mathfrak{b}_{\max}) + 1 \in \mathbb{N}$. ↯ Therefore, $\mathfrak{B}$ is *infinite.*

We will now show that $\mathfrak{B}$ is countable. For each natural number $n \in \mathbb{N}$, define $\mathfrak{B}_n = \{b \in \mathfrak{B} \mid \texttt{len}(b) = n\}$. Given an arbitrary string $s \in \mathfrak{B}$, we know that $\texttt{len}(s) = k$ for some $k \in \mathbb{N}$ by definition, so $s \in \mathfrak{B}_k$. This shows $\mathfrak{B} \subseteq \bigcup_{n=0}^{\infty} \mathfrak{B}_n$. Similarly, if $s \in \bigcup_{n=0}^{\infty} \mathfrak{B}_n$, then $s \in \mathfrak{B}_k$ for some $k \in \mathbb{N}$, meaning $\texttt{len}(s) = k$, so that $s \in \mathfrak{B}$ by definition. We therefore know that $\mathfrak{B} = \bigcup_{n=0}^{\infty} \mathfrak{B}_n$.

We should now pause to notice something. Given some $k \in \mathbb{N}$, we know that there are exactly 2^k binary strings of length k,[9] so that $|\mathfrak{B}_k| = 2^k$. From this analysis, we deduce that $\mathfrak{B}_k$ is countable for every $k \in \mathbb{N}$. We can now apply the theorem that the countable union of countable sets is countable to conclude that $\mathfrak{B}$ is *countable.*

Therefore, since $\mathfrak{B}$ is both countable and infinite, we conclude $|\mathfrak{B}| = |\mathbb{N}|$. **QED**

[6] This is equivalent to saying $|\mathfrak{B}| = |\mathbb{N}|$ given our previous theorems.

[7] $\mathfrak{B}$ being finite actually means that there exists $n \in \mathbb{N}$ such that $\mathfrak{B}$ is in bijection with the set $\{0, ..., n-1\}$. The obvious function $\lambda : \mathfrak{B} \to \mathfrak{D}$ defined by $\lambda(\mathfrak{b}) := \texttt{len}(\mathfrak{b})$ for each $\mathfrak{b} \in \mathfrak{B}$ is clearly a surjection, so $|\mathfrak{B}| \geqslant |\mathfrak{D}|$, proving $\mathfrak{D}$ is also finite.

[8] Since there are only finitely many strings to pick from (by assumption), we can pick $\mathfrak{b}_{\max}$ without any concerns regarding the Axiom of Choice.

[9] There are many ways to see that this is true, but one elegant way relies on the theorem that $|\mathbb{P}(X)| = 2^k$ for any set X where $|X| = k \in \mathbb{N}$. To illustrate the idea, let $k := 5$ and define $X := \{0, 1, 2, 3, 4, 5\}$. Now, consider a subset $Y := \{1, 2, 4\} \subseteq X$. We can associate Y with the binary string `"011010"` whose i^{th} character is `"1"` if and only if $i \in Y$. This association induces a bijection between $\mathbb{P}(\{0, ..., k-1\})$ and $\mathfrak{B}_k$.

3.2 Infinite Strings

In a similar way to how we represented finite-length strings as functions with finite domains, we will say that infinite-length binary strings are functions whose domain is $\mathbb{N}$ and whose codomain is $\{0, 1\}$. For example, the infinite-length binary string `"010101..."` whose characters are `"0"` at the odd indices and `"1"` at the even indices is represented by the following function.

$$f : \mathbb{N} \to \{0,1\} \text{ given by } f(n) := \begin{cases} 0 \text{ if } n = 2k \text{ for some } k \in \mathbb{Z} \\ 1 \text{ if } n = 2k+1 \text{ for some } k \in \mathbb{Z} \end{cases}$$

Remarkably, despite the panoply of sets we've just proven are equinumerous with $\mathbb{N}$, there are *strictly more* binary strings of infinite length than there are natural numbers!

Theorem 6: Cantor's Diagonal Argument.
The set $\mathfrak{B}_\infty := \{f \mid f : \mathbb{N} \to \{0, 1\}\}$ of infinite-length binary strings is *uncountable,* which means precisely that $|\mathbb{N}| < |\mathfrak{B}_\infty|$.

Proof. Towards a contradiction, suppose $|\mathbb{N}| \geqslant |\mathfrak{B}_\infty|$. Then, by definition, there exists a function $\varphi : \mathbb{N} \to \mathfrak{B}_\infty$ such that φ is a surjection. Notice that the i^{th} string that φ enumerates is $\varphi(i)$, and the j^{th} character in that string is $\varphi(i)(j)$.

Consider the infinite-length binary string $\delta : \mathbb{N} \to \{0, 1\}$ defined as follows below.

$$\delta(n) := \begin{cases} 0 \text{ if } \varphi(n)(n) = 1 \\ 1 \text{ if } \varphi(n)(n) = 0 \end{cases} \qquad \text{for each } n \in \mathbb{N}$$

Since δ is a binary string of infinite length, we know $\delta \in \mathfrak{B}_\infty$ by definition. Because φ is surjective, this implies there exists some $i \in \mathbb{N}$ such that $\varphi(i) = \delta$. This means the string $\varphi(k)$ and δ must agree on their characters at each index; formally, this is equivalent to saying $(\forall j \in \mathbb{N})(\varphi(i)(j) = \delta(j))$. However, the following two equivalences follow directly from the definition of δ.

$$\varphi(i)(i) = 1 \;\Leftrightarrow\; \delta(i) = 0 \;\Leftrightarrow\; \delta(i) \neq 1 \;\Leftrightarrow\; \delta(i) \neq \varphi(i)(i)$$
$$\varphi(i)(i) = 0 \;\Leftrightarrow\; \delta(i) = 1 \;\Leftrightarrow\; \delta(i) \neq 0 \;\Leftrightarrow\; \delta(i) \neq \varphi(i)(i)$$

This means $\varphi(i) \neq \delta$, directly contradicting the fact that $\varphi(i) = \delta$. ↯

Therefore, $|\mathbb{N}| < |\mathfrak{B}_\infty|$, and we conclude that $\mathfrak{B}_\infty$ is uncountable. QED