Discrete Mathematics

Daniel Gonzalez Cedre

University of Notre Dame
Spring of 2023

Chapter 6

Cardinality

6.1 Functions

Definition 6.1 ***(Function).***
As a reminder, we say that $f : X \to Y$ is a function from X to Y *iff* both of the following hold:

I. $f \subseteq X \times Y$
II. $(\forall x \in X)(\exists! y \in Y)\big((x, y) \in f\big)$

⌟

Definition 6.2 ***(Composition).***
Given two functions $f : A \to B$ and $g : B \to C$, the *composition* of g with f is another function $g \circ f : A \to C$ given by $(g \circ f)(a) \coloneqq g\big(f(a)\big)$ for all $a \in A$.
⌟

Definition 6.3 ***(Injectivity).***
We say that a function $f : X \to Y$ is an *injection* $:\Leftrightarrow$ either of the following two statements holds:

I. $(\forall x_1 \in X)(\forall x_2 \in X)\big(x_1 \neq x_2 \;\Rightarrow\; f(x_1) \neq f(x_2)\big)$
II. $(\forall x_1 \in X)(\forall x_2 \in X)\big(f(x_1) = f(x_2) \;\Rightarrow\; x_1 = x_2\big)$

Notice that these two statements are equivalent since the leading quantifiers are identical and the unquantified implications are contrapositives of each other, and we know from the propositional logic that $(p \to q) \;\Leftrightarrow\; (\neg q \to \neg p)$.
It is common to denote injective functions using the notation $f : X \hookrightarrow Y$.
⌟

Definition 6.4 ***(Surjectivity).***
We say that a function $f : X \to Y$ is a *surjection* $:\Leftrightarrow (\forall y \in Y)(\exists x \in X)\big(f(x) = y\big)$.
It is common to denote injective functions using the notation $f : X \twoheadrightarrow Y$.
⌟

Definition 6.5 ***(Bijectivity).***
We say that a function $f : X \to Y$ is a *bijection* $:\Leftrightarrow f$ is both injective and surjective.
For bijections, it is common to combine the injective and surjective notations and denote them $f : X \hookrightarrow\!\!\!\!\rightarrow Y$.
⌟

Example 6.1.
Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(z) = z - 1$. This function is a bijection.
⌟

Proof. Let $x_1, x_2 \in \mathbb{Z}$ and suppose $f(x_1) = f(x_2)$. Then, we can observe

$$\begin{aligned} f(x_1) = f(x_2) &\;\Rightarrow\; x_1 - 1 = x_2 - 1 && \text{by definition} \\ &\;\Rightarrow\; \quad x_1 = x_2 && \text{by basic algebra} \end{aligned}$$

Therefore, f is an injection.
Now, let $y \in \mathbb{Z}$ and note $y + 1 \in \mathbb{Z}$. Since $f(y + 1) = (y + 1) - 1 = y$ by definition, we have that f is surjective.

Since f is both injective and surjective, f is a bijection by definition. Q.E.D.

6.1.1 Invertibility

Definition 6.6 ***(Identity).***
For every set A, we define its *identity function* $\mathrm{id}_A : A \to A$ by $\mathrm{id}_A(a) := (a)$ for all $a \in A$. ⌟

Definition 6.7 ***(Monomorphisms).***
We say that a function $f : A \to B$ is *monic* $:\Leftrightarrow (\exists g : B \to A)(g \circ f = \mathrm{id}_A)$. Such g are called *left-inverses* for f. ⌟

Definition 6.8 ***(Epimorphisms).***
We say that a function $f : A \to B$ is *epic* $:\Leftrightarrow (\exists g : B \to A)(f \circ g = \mathrm{id}_B)$. Such g are called *right-inverses* for f. ⌟

Definition 6.9 ***(Isomorphisms).***
We say that $f : A \to B$ is an *isomorphism* $:\Leftrightarrow (\exists g : B \to A)(g \circ f = \mathrm{id}_A \wedge f \circ g = \mathrm{id}_B)$. We can then say that g is an *inverse* (*a.k.a. two-sided inverse*) for f, and we then say that f is *invertible*. ⌟

Axiom ***(Axiom of Choice).***
Every surjection has a right-inverse. ⌟

Theorem 6.1.
Let $A \neq \varnothing$ and $B \neq \varnothing$ and consider $f : A \to B$. The following are true:

I. f is an injection $\Leftrightarrow$ f is a monomorphism.
II. f is a surjection $\Leftrightarrow$ f is an epimorphism.
III. f is a bijection $\Leftrightarrow$ f is an isomorphism.

⌟

6.2 Cardinality

Definition 6.10 ***(Cardinality).***
Let A and B be sets. The *cardinality* of a set, which we denote by $|A|$*, corresponds to our intuitive notion of its *size* relative to other sets. If we want to compare two sets, we assess their relative cardinalities by determining whether or not one set *fits inside* the other by seeing what kinds of functions it is possible to define between them.

We say that the *cardinality* of A is *no greater than* the *cardinality* of B $:\Leftrightarrow \exists f : A \to B$ such that f is an injection. In this case, we say that $|A| \leqslant |B|$.

We say that the *cardinality* of A is *no lesser than* the *cardinality* of B $:\Leftrightarrow \exists f : A \to B$ such that f is an surjection. In this case, we say that $|A| \geqslant |B|$.

Naturally, we say A and B have the *same cardinality* $:\Leftrightarrow \exists f : A \to B$ such that f is a bijection, denoted $|A| = |B|$. ⌟

Corollary 6.1.
For any nonempty sets $A \neq \varnothing$ and $B \neq \varnothing$, we have $|A| \leqslant |B| \;\Leftrightarrow\; |B| \geqslant |A|$. ⌟

Proof. Suppose $|A| \leqslant |B|$ for nonempty A and B. This means we have an injection $\varphi : A \to B$ by definition. Then, by Theorem 6.1, φ is monic, so we know that $\exists \psi : B \to A$ such that $\psi \circ \varphi = \mathrm{id}_A$. Since ψ has a right inverse, it must be epic by definition, so ψ is a surjection by Theorem 6.1.

Conversely, suppose $|B| \geqslant |A|$ for nonempty A and B. Then, there is a surjection $\psi : B \to A$. Since ψ is an epimorphism by Theorem 6.1, we have $\varphi : A \to B$ such that $\psi \circ \varphi = \mathrm{id}_A$. Since φ has a left inverse, it must be monic by definition, so φ is an injection by Theorem 6.1. Q.E.D.

Definition 6.11 ***(Finite Set).***
We say that a set A is *finite* $:\Leftrightarrow (\exists n \in \mathbb{N})(\exists f : A \to n)(f \text{ is a bijection})$. In this case, we will say that $|A| = n$. ⌟

Definition 6.12 ***(Countable Set).***
We say that a set A is *countable* $:\Leftrightarrow (\exists f : A \to \mathbb{N})(f \text{ is an injection})$. In this case, we say that $|A| \leqslant \aleph_0$. ⌟

*The *cardinality* of a set is not always guaranteed to exist without the Axiom of Choice.

Example 6.2.
Let's prove that $|\mathbb{N}| = |\mathbb{Z}|$. ⌟

Proof. Consider the function $f : \mathbb{Z} \to \mathbb{N}$ given by

$$f(z) = \begin{cases} 2z & \text{if } z \geqslant 0 \\ 2(-z) - 1 & \text{if } z < 0 \end{cases}$$

First, let's see that this is an injection. Let $x_1, x_2 \in \mathbb{Z}$ and suppose $f(x_1) = f(x_2)$. We now have two cases.

Case 1:
If $f(x_1)$ is even, then we know $f(x_1) = 2k$ for some $k \in \mathbb{N}$ by definition. Then, we have $f(x_2) = 2k$ as well, since $f(x_1) = f(x_2)$.

Now, we claim that $x_1 \geqslant 0$: if we assume $x < 0$ towards the contrary, then we would have $f(x_1) = 2(-x_1) - 1$, which is odd. We would then have

$$\begin{aligned} 2(-x_1) - 1 = 2k &\Rightarrow 2(-x_1) - 2k = 1 \\ &\Rightarrow 2(k - x_1) = 1 \\ &\Rightarrow k - x_1 = {}^1\!/_2 \end{aligned}$$

However, since k and x_1 are both integers (and $\mathbb{Z}$ is an ordered ring), $k - x_1$ must be an integer. ↯

By the same argument, we also have that $x_2 \geqslant 0$. Therefore, $2x_1 = f(x_1) = f(x_2) = 2x_2$, so $x_1 = x_2$.

Case 2:
This case is left as an exercise to the reader.

Thus, f is injective since $x_1 = x_2$ in both cases.

Now, let's show that f is a surjection. Suppose $y \in \mathbb{N}$ and again we have two cases.

Case 1:
If y is even, then $y = 2k$ for some $k \in \mathbb{N}$. But then, we can simply see $k \in \mathbb{Z}$ and $f(k) = 2k$ since $k \geqslant 0$.

Case 2:
If y is odd, then $y = 2k+1$ for some $k \in \mathbb{N}$. Then, $k \in \mathbb{Z}$ and $f(-k-1) = 2(k+1)-1 = 2k+2-1 = 2k+1$ because $k \geqslant 0 \ \Rightarrow \ -k \leqslant 0 \ \Rightarrow \ -k-1 < -k \leqslant 0$ and $-k-1 \in \mathbb{Z}$.

Therefore, since we found a preimage for y in both cases, f is surjective.

This means f is a bijection, so we can conclude that $|\mathbb{N}| = |\mathbb{Z}|$. Q.E.D.

Example 6.3.
Let's prove that $|\mathbb{N}| = |\mathbb{Q}|$. ⌟

Proof. TODO Q.E.D.

Theorem 6.2 ***(Cantor-Shröder-Bernstein).***
Given two sets A and B, if there exist injections $f : A \hookrightarrow B$ and $g : B \hookrightarrow A$, then there exists a bijection $h : A \hookrightarrow\!\!\!\!\rightarrow B$. ⌟

Definition 6.13 ***(Sequences).***
A *finite sequence* of length $n \in \mathbb{N}$ over a set X is a function $f : n \to X$. Here, the length of the sequence is given by its *domain* $n = \{0, 1, \ldots n-1\}$, and the individual elements in the sequence are taken from X.

An *infinite sequence* over a set X is a function $f : \mathbb{N} \to X$. Since the domain here is infinite, we have a place in the sequence for each natural number, so our sequence has infinite length.

Here, the inputs to the function act as indices for the entries in the sequence, and the entry itself is given by the output of the function at that index. So, the first entry is given by $f(0)$, the second by $f(1)$, *etc.*

Sequences are sometimes referred to as *strings*, evoking the similarity between list data structures in programming languages (*e.g.*, arrays in `C`, lists in `Python`) and finite sequences. When you access the third entry of a list in `Python`, you might use syntax like `L[2]`. Similarly, the third entry in a mathematical sequence is given by $f(2)$.

Since `String` data types in many languages are modeled using lists (*e.g.*, of `char` types), it is natural to associate strings with sequences.
⌟

Theorem 6.3 ***(Cantor's Diagonal Argument).***
Let $I \coloneqq \{f \mid f : \mathbb{N} \to \mathbb{N}\}$. Then $|\mathbb{N}| \ngeq |I|$.
⌟

Proof. TODO Q.E.D.

Theorem 6.4 ***(Cantor's Theorem).***
$|X| < \left|\mathcal{P}(X)\right|$ for every X.
⌟

Proof. Suppose, towards a contradiction, that $\varphi : X \twoheadrightarrow \mathcal{P}(X)$ is a surjection. TODO Q.E.D.