Discrete Mathematics

Daniel Gonzalez Cedre

University of Notre Dame
Spring of 2023

Chapter 3

Zermelo-Fraenkel Set Theory

"No one shall expel us from the paradise that Cantor has created."

—David Hilbert

3.1 The Language of Set Theory

In order to use our first-order logic as a language with which to talk about math, we need to specify: what is our universe of discourse Ω, and what are our fundamental predicate symbols? The analogy drawn in class between the structure of the study of mathematics and the abstract structure of a modern computer should hopefully communicate how natural and common the notion is of having one *type* of object that implements other, more complicated objects. However, this decision actually goes back to the beginning of this 20^{th} century revolution in mathematics. The initial solution people came up with to the fundamental logical and foundational problems they had discovered has to use a *ramified*—or *typed*—ontology, where different objects had different *types* in a hierarchy and there were rules governing how objects could be manipulated based on their *type*. The problem with this approach is that it becomes very syntactically-cumbersome for humans (the primary practitioners of mathematics) to deal with directly, so it was quickly abandoned for an *untyped* approach.

Note. The converse is true about the *λ-calculus*, which is perhaps the most famous mathematical model of computation after the Turing machine. Although the untyped λ-calculus is more expressive (*i.e.*, stronger) than any of the typed λ-calculi (and is thus more interesting to study for mathematicians), the modern functional programming languages we have today (*e.g.*, Haskell, the LISP dialects, F#) are actually implementations of typed λ-calculi because computers have no issues dealing with the syntactic complications of a typed theory.

Our universe of discourse will consist of *those objects that we can prove exist* using the rules of inference and the *axioms of set theory* (which we will develop in this chapter). The axioms of set theory will be sentences in the *language of Zermelo-Fraenkel set theory* that describe *what exactly sets are* and *how they work*. The language of set theory will have two predicate symbols, defined below.

Definition 3.1 (Equality)**.**

We define the binary predicate $=$ to mean that its left argument is *identically the same* as its right argument. So, if x and y are sets, then we say $x = y$ when we mean that the names x and y both refer to the same underlying object. As a result, we will take the following three axioms for this predicate:

$$\forall x(x = x) \qquad \forall x\forall y\big((x = y) \Leftrightarrow (y = x)\big) \qquad \forall x\forall y\forall z\big((x = y \wedge y = x) \Rightarrow (x = z)\big)$$

Definition 3.2 (Elementhood)**.**

We define the binary predicate $\in$ to mean that its left argument is contained in its right argument as an element. So, if x and y are sets, then the phrase $x \in y$ conveys that x is an element of y.

Definition 3.3 (Language of Set Theory)**.**

The *language of Zermelo-Fraenkel set theory* consists of the first-order logic along with

I. a universe of discourse consisting of those things that provably exist from the axioms (Section 3.2),

II. the binary predicates for equality ($=$, Definition 3.1) and elementhood ($\in$, Definition 3.2).

3.2 Axioms of Set Theory

Axiom 0 (Existence)**.**

$$\exists x(x = x)$$

This axiom asserts that our universe of discourse is non-empty. Assuming this axiom lets us know for sure that when we make claims about sets, those claims are actually in reference to objects that provably exist (because we can use this axiom as an assumption in any proof).

Axiom 1 (Extensionality)**.**

$$\forall x \forall y\big((x = y) \Leftrightarrow \forall z(z \in x \Leftrightarrow z \in y)\big)$$

This axiom states that sets are equal *iff* they have the same elements, capturing what we mean by two sets being (or not being) equal. This establishes a fundamental relationship between $=$ and $\in$.

Definition 3.4 ($\in$-Augmented Quantification)**.**

When we want to talk about all of the elements of a set A that satisfy a given *wff* $\varphi(\cdot)$, we say

$$(\forall x \in A)\big(\varphi(x)\big) \;:\Leftrightarrow\; \forall x\big(x \in A \Rightarrow \varphi(x)\big).$$

Similarly, if we want to say that there is an element in A with the property $\varphi(\cdot)$, we say

$$(\exists x \in A)\big(\varphi(x)\big) \;:\Leftrightarrow\; \exists x\big(x \in A \wedge \varphi(x)\big).$$

The parentheses around $(\forall x \in A)$ and $(\exists x \in A)$ can be added or dropped for clarity based on context.

Theorem 3.1 (First-Order Set Notation)**.**

Let φ be a wff with at most one free variable and let A be a set. Then, the following statements hold.

$$(\forall a \in A)\big(\varphi(a)\big) \Leftrightarrow \left(\bigwedge_{a \in A} \varphi(a)\right) \qquad (\exists a \in A)\big(\varphi(a)\big) \Leftrightarrow \left(\bigvee_{a \in A} \varphi(a)\right)$$

Proof.

This proof is left as an exercise to the reader.

Q.E.D.

Definition 3.5 (Set-Builder Notation)**.**

The notation $\{x_1, \ldots x_n\}$, where each $x_1, \ldots x_n$ is a term, describes the set containing each of the x_i's, and *only* the x_i's, as elements. So, we say $\{x_1, \ldots x_n\}$ denotes the set X satisfying $\forall a\Big(a \in X \Leftrightarrow \bigvee_{i=1}^{n}(a = x_i)\Big)$. Another way of saying this is that $X \coloneqq \{x_1, \ldots x_n\}$ is the set that satisfies

$$\left(\bigwedge_{i=1}^{n} x_i \in X\right) \wedge \forall a\Big(a \in X \Rightarrow \big(\exists x \in X(a = x)\big)\Big).$$

Definition 3.6 (Set-Comprehension Notation)**.**

If φ is a *wff* with at most one free variable, then when we write down $\big\{a \;\big|\; \varphi(a)\big\}$, we mean the set consisting of all possible a satisfying the formula φ when the every occurrence of the free variable in φ is replaced by a. Similarly, if we have an already-existing set A, we can define the set of all elements of A that satisfy φ with the notation $\big\{a \in A \;\big|\; \varphi(a)\big\}$. These notations are read "the set of all a (in A) such that $\varphi(a)$". More precisely,

$$\exists x\Big(x = \big\{a \;\big|\; \varphi(a)\big\}\Big) \Leftrightarrow \exists x \forall a\big(a \in x \Leftrightarrow \varphi(a)\big),$$
$$\exists x\Big(x = \big\{a \in A \;\big|\; \varphi(a)\big\}\Big) \Leftrightarrow \exists x \forall a\Big(a \in x \Leftrightarrow \big(a \in A \wedge \varphi(a)\big)\Big).$$

Note. These sets may not always exist! Remember that we can only speak about the objects that *provably* exist, so when use this notation, we must be sure (with proof) that it is actually a set!

Axiom 2 (Pairing)**.**

$$\forall x \forall y \exists z \big(z = \{x, y\}\big)$$

This axiom allows us to take two existing sets and construct a set containing the pair of them.

Axiom 3 (Union)**.**

$$\forall x \exists A \Big(A = \big\{z \mid (\exists y \in x)(z \in y)\big\}\Big)$$

The notation we use for this set A, which we call the *union of* x, is $\cup x \coloneqq \big\{z \mid (\exists y \in x)(z \in y)\big\}$.

Theorem 3.2 (Union of Two Sets)**.**

For any sets x and y, we have $\exists A\Big(A = \big\{z \mid (z \in x) \vee (z \in y)\big\}\Big)$. Such an A is denoted $x \cup y$.

Proof.

Let x and y be sets. By Axiom 2, we know $A \coloneqq \{x, y\}$ exists. By Axiom 3, we know $\cup A$ exists. Recall that $\cup A = \big\{a \mid (\exists z \in A) a \in z\big\}$. Now, let b be an arbitrary set and observe

$$\begin{aligned}
b \in \cup A &\Leftrightarrow (\exists z \in A)(b \in z) && \text{by definition of } \cup A \\
&\Leftrightarrow (b \in x) \vee (b \in y) && \text{since } A = \{x, y\} \\
&\Leftrightarrow b \in \big\{a \mid (a \in x) \vee (a \in y)\big\} && \text{by definition.}
\end{aligned}$$

Therefore, we have that $\cup A = \big\{a \mid (a \in x) \vee (a \in y)\big\}$, so $x \cup y \coloneqq \big\{a \mid (a \in x) \vee (a \in y)\big\}$ exists.

Q.E.D.

Axiom 4 (Separation)**.**

$$\text{If } \varphi \text{ is a } \textit{wff} \text{ with at most one free variable, then } \forall x \exists y \Big(y = \big\{a \in x \mid \varphi(a)\big\}\Big)$$

This axiom tells us that, if we start with an already-existing set x, then we can collect all of its elements that satisfy φ and put them in a set by themselves.

Theorem 3.3 (Intersection of Two Sets)**.**

For any sets x and y, we have $\exists A\Big(A = \big\{a \mid (a \in x) \wedge (a \in y)\big\}\Big)$. Such an A is denoted $x \cap y$.

Proof.

Let x and y be sets. Recall that $x \cup y$ exists by Theorem 3.2. Then, by Axiom 4, we know that $A \coloneqq \big\{a \in x \cup y \mid (a \in x) \wedge (a \in y)\big\}$ exists. Now, let b be an arbitrary set and observe

$$\begin{aligned}
b \in A &\Leftrightarrow b \in \big\{a \in x \cup y \mid (a \in x) \wedge (a \in y)\big\} && \text{by the definition of } A \\
&\Leftrightarrow (b \in x \cup y) \wedge \big((b \in x) \wedge (b \in y)\big) && \text{by definition} \\
&\Leftrightarrow \big((b \in x) \vee (b \in y)\big) \wedge \big((b \in x) \wedge (b \in y)\big) && \text{by definition of } x \cup y \\
&\Leftrightarrow \Big(\big((b \in x) \vee (b \in y)\big) \wedge (b \in x)\Big) \wedge (b \in y) && \text{by Associativity} \\
&\Leftrightarrow \Big(\big((b \in x) \wedge (b \in x)\big) \wedge \big((b \in y) \wedge (b \in x)\big)\Big) \wedge (b \in y) && \text{by Distributivity} \\
&\Leftrightarrow \Big((b \in x) \wedge \big((b \in y) \wedge (b \in x)\big)\Big) \wedge (b \in y) && \text{by Idempotency} \\
&\Leftrightarrow \Big((b \in x) \wedge \big((b \in x) \wedge (b \in y)\big)\Big) \wedge (b \in y) && \text{by Commutativity} \\
&\Leftrightarrow \Big(\big((b \in x) \wedge (b \in x)\big) \wedge (b \in y)\Big) \wedge (b \in y) && \text{by Associativity} \\
&\Leftrightarrow \big((b \in x) \wedge (b \in y)\big) \wedge (b \in y) && \text{by Idempotency} \\
&\Leftrightarrow (b \in x) \wedge \big((b \in y) \wedge (b \in y)\big) && \text{by Associativity} \\
&\Leftrightarrow (b \in x) \wedge (b \in y) && \text{by Idempotency} \\
&\Leftrightarrow b \in \big\{a \mid (a \in x) \wedge (a \in y)\big\} && \text{by definition.}
\end{aligned}$$

Therefore, we have that $A = \big\{a \mid (a \in x) \wedge (a \in y)\big\}$, showing that $x \cap y = \big\{a \mid (a \in x) \wedge (a \in y)\big\}$ exists.

Q.E.D.

Theorem 3.4 (Difference of Two Sets)**.**

For any sets x and y, we have $\exists A\Big(A = \big\{a \mid (a \in x) \wedge (a \notin y)\big\}\Big)$. Such an A is denoted $x \setminus y$.

Proof.

Let x and y be sets. Consider $A \coloneqq \{a \in x \mid a \notin y\}$, which we know exists by Axiom 4. Now, let b be an arbitrary set and observe

$$\begin{aligned} b \in A &\Leftrightarrow b \in \{a \in x \mid a \notin y\} && \text{by the definition of } A \\ &\Leftrightarrow (b \in x) \wedge (b \notin y) && \text{by definition} \\ &\Leftrightarrow b \in \big\{a \mid (a \in x) \wedge (a \notin y)\big\} && \text{by definition.} \end{aligned}$$

Therefore, $A = \big\{a \mid (a \in x) \wedge (a \notin y)\big\}$ by Axiom 1, showing that $x \setminus y = \big\{a \mid (a \in x) \wedge (a \notin y)\big\}$ exists.

Q.E.D.

Definition 3.7 (Subsets)**.**

We say that x is a *subset* of y when every element of x is also an element of y. Formally, we define

$$x \subseteq y \;:\Leftrightarrow\; \forall a(a \in x \Rightarrow a \in y).$$

If $x \subseteq y$ but $x \neq y$, then we say that x is a *proper subset* of y and we write $x \subsetneq y$ (you may also encounter the alternative notations $x \subset y$ and $x \subsetneqq y$).

Axiom 5 (Power Set)**.**

$$\forall x \exists y\big(y = \{s \mid s \subseteq x\}\big).$$

This axiom tells us that, whenever we have a set x that exists, we are allowed to collect *all* of its subsets into one set, called the *power set* of x. We use the notation $\mathcal{P}(x)$.

Definition 3.8 (Empty Set)**.**

We say that a set A is *empty* $:\Leftrightarrow \forall x(x \notin A)$. Since there can only be one empty set by Axiom 1, we refer to this set as *the* empty set and use the special symbol $\varnothing$.

Axiom 6 (Regularity)**.**

$$\forall x\big((x \neq \varnothing) \Rightarrow (\exists y \in x)(x \cap y = \varnothing)\big).$$

This axiom establishes the *regularity* (*a.k.a. well-foundedness*) of the $\in$ predicate. Literally, this axiom simply says that every non-empty set has an element disjoint with it. However, this seemingly strange axiom has far-reaching consequences, not least of which is that it lets us prove that sets do not contain themselves.

Theorem 3.5 ($\in$ Well-foundedness)**.**

For any set x, we have $x \notin x$.

Proof.

Let x be an arbitrary set. Towards a contradiction, assume $x \in x$. Let $y \coloneqq \{a \in x \mid a = x\} = \{x\}$, which we know exists by Axiom 4. Since $x \in y$, we know $y \neq \varnothing$. Thus, Axiom 6 lets us know there is a $z \in y$ such that $y \cap z = \varnothing$. Since $y = \{x\}$ and $z \in y$, this implies $z = x$, yielding $y \cap x = \varnothing$. However, we already knew that $x \in y$ and $x \in x$, so we know by definition that $x \in \{a \mid a \in y \wedge a \in x\} = y \cap x$, and therefore $y \cap x \neq \varnothing$. ↯

Therefore, we must have that $x \notin x$. Since x was arbitrary, we can conclude $\forall x(x \notin x)$, as desired.

Q.E.D.

Definition 3.9 (Kuratowski Ordered Pairs)**.**

We define the *ordered pair* with left coordinate a and right coordinate b by $(a, b) \coloneqq \big\{\{a\}, \{a, b\}\big\}$. It is left as a simple exercise to the reader to prove that (a, b) always exists.

Definition 3.10 (Cartesian Product)**.**

We define the *Cartesian product* of two sets A and B, which is the set of all possible ordered pairs with left coordinate coming from A and right coordinate coming from B, by $A \times B \coloneqq \big\{(a, b) \mid a \in A \wedge b \in b\big\}$.

Theorem 3.6 (Existence of Cartesian Products)**.**
For any sets X and Y, the Cartesian product $X \times Y$ exists.

Proof.
details to be filled in

Q.E.D.

Theorem 3.7 (Existence of $\varnothing$)**.**
$\exists x(x = \varnothing)$.

Proof.
We know, by Axiom 0, that there exists a set x. Now, consider $E \coloneqq \{y \in x \mid y \neq y\}$, which we know exists by Axiom 4. We can clearly see that E is empty, because if $x \in E$ then we would immediately run into the contradiction $x \neq x$.

Therefore, $E = \varnothing$, so the empty set exists.

Q.E.D.

Definition 3.11 (Successor Functional)**.**
Given an arbitrary set x, we define the *successor* of x to be the set $x \cup \{x\}$, for which we introduce the notation $\mathcal{S}(x) \coloneqq x \cup \{x\}$. It should be clear that the successor of any set always exists.

Note. The successor $\mathcal{S}(x)$ of a set x is a set consisting of all of the elements of x as well as x itself.

Definition 3.12 (von Neumann Ordinals)**.**
The *natural numbers*, also known as the *finite ordinal numbers*, are defined recursively as follows:

$$\begin{aligned} 0 &\coloneqq \varnothing && \text{is a natural number} \\ n+1 &\coloneqq S(n) = n \cup \{n\} = \{0, 1, 2, \dots n\} && \text{if } n \text{ is a natural number} \end{aligned}$$

We say that a natural number n is a *successor number* $:\Leftrightarrow$ there exists a natural number m such that $n = \mathcal{S}(m)$. Every natural number except for 0 is a successor number, so when we define properties or operations on the natural numbers, we will usually take a recursive approach that explicitly defines what happens at 0 and then specifies what happens when you've encountered a successor number.

If n is a successor natural number, then we define the *predecessor* of n to be $n - 1 \coloneqq m$, where m is a natural number such that $\mathcal{S}(m) = n$.

Definition 3.13 (Arithmetic on the Natural Numbers)**.**
Given a natural number n, its *sum* with another natural number m is recursively given by

$$\begin{aligned} n + 0 &\coloneqq n \\ n + \mathcal{S}(m) &\coloneqq \mathcal{S}(n + m) && \text{if } m \text{ is a successor number} \end{aligned}$$

Similarly, we define the *product* of two natural numbers n and m recursively by

$$\begin{aligned} n \cdot 0 &\coloneqq 0 \\ n \cdot \mathcal{S}(m) &\coloneqq (n + m) + n && \text{if } m \text{ is a successor number} \end{aligned}$$

Finally, we can recursively define the *exponentiation* of one natural number n by another as

$$\begin{aligned} n^0 &\coloneqq 1 \\ n^{\mathcal{S}(m)} &\coloneqq n^m \cdot m && \text{if } m \text{ is a successor number} \end{aligned}$$

Definition 3.14 (Order on the Natural Numbers)**.**
Given two natural numbers n and m, say that n is *less than or equal to* $m :\Leftrightarrow n \subseteq m$. The syntax we use to express this relationship is $n \leqslant m$.

If $n \leqslant m$ and $n \neq m$, then we say $n < m$, which means n is *strictly less than* m.

Definition 3.15 (Iterated Sums & Products)**.**

If n and $x_0, \dots x_{n-1}$ are natural numbers, then we define the *iterated sum* of the x_i recursively by

$$\sum_{i=0}^{0} x_i = x_0$$
$$\sum_{i=0}^{k+1} x_i = \left(\sum_{i=0}^{k} x_i \right) + \big(x_{k+1}\big) \qquad \text{if } 0 < k+1 \leqslant n.$$

Similarly, we define the *iterated product* of the x_i recursively as

$$\prod_{i=0}^{0} x_i = x_0$$
$$\prod_{i=0}^{k+1} x_i = \left(\prod_{i=0}^{k} x_i \right) \cdot \big(x_{k+1}\big) \qquad \text{if } 0 < k+1 \leqslant n.$$

Axiom 7 (Infinity)**.**

$$\exists N \left(N = \left\{ n \;\middle|\; n = \varnothing \vee \exists (m \in N) \big(n = \mathcal{S}(m)\big) \right\} \right)$$

We call this set the *set of natural numbers* and use the symbol $\mathbb{N}$ to denote it.

Theorem 3.8 ($\mathbb{N}$ is an Ordered Semigroup)**.**