A FIRST COURSE IN SET THEORY

ANTON BERNSHTEYN

Abstract. This is a set of lecture notes for a semester-long course in set theory. The presentation here is aimed at graduate (or advanced undergraduate) students in mathematics without prior knowledge of set theory or mathematical logic more broadly. Therefore, all necessary logic background is developed from scratch. The material covered in these notes can roughly be described as "set theory before forcing" and includes the axiomatic foundations of set theory, ordinals and cardinals, remarks on the role of the Axiom of Choice, basic properties of Gödel's constructible universe L, consistency of AC and CH, and a taste of descriptive set theory. The text includes a large number of exercises, as well as five problem sets. Please reach out to me via email if you are interested in getting access to the problem sets' solutions.

Contents

Department of Mathematics, University of California, Los Angeles, CA, USA
E-mail address: bernshteyn@math.ucla.edu.
This work is partially supported by the NSF CAREER grant DMS-2239187.

1. The first axioms

1.1. Introduction

The topic of this course is **set theory**, a field studying some of the simplest mathematical structures, namely *sets*. In contrast to many other areas that gradually grew and took shape through the efforts of many researchers, set theory was invented by a single person, namely Georg Cantor, in the 1870s.[i] After Cantor's initial discoveries, many subsequent developments followed, leading to an axiomatic formulation of set theory that we will be using in this course. Before jumping into this subject, it is worthwhile to ponder what makes set theory important and worth studying. To this end, we shall begin with a brief review of the main concepts of *naive set theory* (this is the name given to the informal version of set theory predating the modern axiomatic treatment).

A **set** is an abstract mathematical model for a collection of objects. As usual, we write $x \in A$ the indicate that an object x is an **element** (or a **member**) of a set A, or, equivalently, x **belongs** to A. We use curly braces $\{, \}$ to write down sets; for example,

$$\{a, b, c\} \tag{1.1}$$

is a set with the elements a, b, and c. To clarify, the only information contained in a set is which objects do and which ones don't belong to it, without any other relationship between the set's elements. For example, the following are different ways of writing the same set as in (1.1):

$$\{b, c, a\}, \quad \{a, a, b, c\}, \quad \{c, b, c, b, c, b, a\}.$$

This idea has a name: *the Principle of Extensionality*:

Principle of Extensionality: *Sets with the same elements are equal.*

The empty collection of elements (i.e., $\{\}$) is a perfectly valid set, called the **empty set** and denoted by $\varnothing$. (We are justified in calling it *the* empty set due to the Principle of Extensionality.) An important feature of set theory is that sets are allowed to be infinite. For example, we have the set

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\} \tag{1.2}$$

of all natural numbers. Notice that formula (1.2) is somewhat informal, since we cannot explicitly list all the elements of the (infinite) set $\mathbb{N}$. To avoid such informality, we use the notation $\{x : P(x)\}$ to denote the set of all x satisfying the property P. For example, we can write

$$\mathbb{N} = \{x : x \text{ is a natural number}\}.$$

One reason for set theory's utility is that it provides tools for manipulating collections of objects arising in any field of math. For example, we have the standard operations on sets:

- union: $A \cup B$,
- intersection: $A \cap B$,
- difference: $A \backslash B$, etc.

In a similar vein, a set A is a **subset** of a set B, in symbols $A \subseteq B$, if all elements of A belong to B. The reader can no doubt see why this terminology is very useful across mathematics.

That being said, if all set theory gave us was some convenient notation, it wouldn't be a very exciting field. What makes set theory really interesting is that sets can be viewed as a basic type of mathematical structure out of which all others can be built. The key observation here is that sets can have *other sets* as elements. This allows us to "nest" sets inside each other to encode more complicated structures.

Exercise 1.1. Explain why the sets $\varnothing$ and $\{\varnothing\}$ are different.

---

[i] The actual history is slightly less clean than that, as some of the early key ideas were suggested to Cantor by Dedekind in their correspondence. But certainly the main insight was Cantor's.

For example, consider the concept of an *ordered pair*. An **ordered pair** (a, b) is a structure with the property that $(a, b) = (x, y)$ if and only if $a = x$ and $b = y$. In other words, as the name suggests, an ordered pair (a, b) "remebers" not only the identity of the elements a, b but also their *ordering*. Note that the set $\{a, b\}$ does *not* have this property, as $\{a, b\} = \{b, a\}$. Nevertheless, perhaps surprisingly, it is possible to construct structures with the ordered pair property using only (unordered) sets as building blocks. There are several viable approaches, the most standard being the following one due to Kuratowski:

$$(a, b) \coloneqq \{\{a\}, \{a, b\}\}.$$

Note that if $a = b$, then $(a, b) = \{\{a\}, \{a, a\}\} = \{\{a\}\}$.

Proposition 1.1. *With the above definition, we have* $(a, b) = (x, y)$ *if and only if* $a = x$ *and* $b = y$.

PROOF. It is clear that if $a = x$ and $b = y$, then $(a, b) = (x, y)$. Now suppose that $(a, b) = (x, y)$. Consider first the case $a \neq b$. Then (a, b) contains a set with two distinct elements, namely $\{a, b\}$. As $(a, b) = (x, y) = \{\{x\}, \{x, y\}\}$ and $\{x\}$ has only one element, it follows that $\{a, b\} = \{x, y\}$. Thus, either $a = x$ and $b = y$ (as desired) or $a = y$ and $b = x$. The latter situation cannot occur, since $\{a\} \in (a, b)$ but $\{a\} \notin (b, a)$. The case $a = b$ is left as an exercise. ■

Having constructed ordered pairs, we can now define ordered triples, e.g., as follows:

$$(a, b, c) \coloneqq (a, (b, c)),$$

and then naturally extend this definition to ordered tuples of arbitrary finite length.

As another example, consider the notion of a *function*. Informally, a function $f \colon X \to Y$ assigns to each $x \in X$ a corresponding element $f(x) \in Y$ (the same element of Y may be assigned to different elements of X). To encode this assignment as a set, we collect all ordered pairs of the form $(x, f(x))$:

$$\{(x, y) : x \in X \text{ and } y = f(x)\}.$$

This set (often called the **graph** of f) contains exactly the same information as the function f itself, so we may as well say that it is *equal* to f. Thus, we are led to the following definition: A **function** from a set X to a set Y is a set f such that:

- every element of f is an ordered pair of the form (x, y) with $x \in X$ and $y \in Y$, and
- for each $x \in X$, there is exactly one $y \in Y$ such that $(x, y) \in f$.

A binary operation on a set X is just a function $X \times X \to X$, where $X \times X$ is the set of all ordered pairs (x, x') with x, $x' \in X$. At this point we clearly have enough building blocks to define all sorts of algebraic structures as sets with certain properties. For example, a group is an ordered pair $(G, \cdot)$, where $\cdot$ is a binary operation on the set G satisfying a list of axioms. The reader is invited to think of other examples of mathematical structures and ways they can be encoded by sets.

In addition to general classes of structures (e.g., functions or groups), we may also want to use sets to construct models for specific objects. Take, for instance, the natural numbers. How do we represent, say, the number 5 by a set? As with ordered pairs, there are different approaches to this task, the most common of which is due to von Neumann. Von Neumann's idea is to represent each natural number n by a set with n elements. For $n = 0$, this leaves us no choice but to define

$$0 \coloneqq \varnothing.$$

For $n = 1$, we need a set with one element. Thankfully, we already have one element lying around, namely 0, so we let

$$1 \coloneqq \{0\}.$$

Continuing in the same manner, we define

$$2 \coloneqq \{0, 1\}, \quad 3 \coloneqq \{0, 1, 2\}, \quad 4 \coloneqq \{0, 1, 2, 3\}, \quad \ldots,$$

and, more generally,

$$n + 1 := \{0, 1, 2, \ldots, n\} \quad \text{for all } n.$$

Notice that, according to this definition,

$$n + 1 = \{0, 1, 2, \ldots, n - 1\} \cup \{n\} = n \cup \{n\}.$$

The fact that the successor operator on $\mathbb{N}$ has such a simple set-theoretic description is one of the reasons this way of defining natural numbers is particularly convenient.

At this point, we come to a striking observation: Notice that the only elements we used to build the sets representing the natural numbers *were sets themselves* (we were able to start the construction with the empty set, thus avoiding the need to have any non-set elements to begin with). It turns out that, more generally, in order to build a model of the whole of mathematics, we never need to consider any objects other then sets (whose elements are sets, whose elements are sets, etc.). This can be formulated as the *atomless assumption*:

Atomless Assumption: *The only elements of sets are themselves sets.*

Of course, one can also study set theory with atoms (i.e., with objects that can be elements of sets but aren't sets themselves), but in this course we'll be focusing on the atomless case.

The above discussion is meant to convince you that, although the theory of atomless sets seems extremely simple, it is in fact rich enough to encompass all of mathematics. In fact, in the naive form sketched above, it is a little too powerful, as it leads to internal contradictions, or *paradoxes*. The most famous of these is *Russell's Paradox*. We begin by asking: Can a set be its own element, i.e., can we have $x \in x$? This certainly seems bizarre, so perhaps it's better to focus on only those sets x that satisfy $x \notin x$. Bertrand Russell observed that this lands us in difficulties:

Russell's Paradox: *Consider the set* $R := \{x : x \notin x\}$. *Is* R *an element of itself?*

A moment's thought shows that neither answer to the above question is consistent. Indeed, if $R \in R$, then, by the definition of R, we have $R \notin R$. On the other hand, if $R \notin R$, then, by the definition of R again, we must have $R \in R$.

Getting rid of problems such as Russell's paradox took a few decades of very hard work. The final solution was to give an explicit list of axioms for set formation that prohibits defining sets such as $\{x : P(x)\}$ unless certain specific conditions are fulfilled. According to these axioms, Russell's set R is not actually a set, and so no paradox occurs. Designing an axiom system that is flexible enough for all desirable applications of set theory yet sufficiently restrictive to avoid paradoxes is a tremendous challenge, and the resulting axiom system is by necessity somewhat complex and subtle. While there are several largely equivalent axiomatizations of set theory, by far the most well-known is the axiom system ZFC: *the Axioms of* Z*ermelo–*F*raenkel with the Axiom of* C*hoice*. In the first part of this course we will learn what these axioms are, how to use them, and what each of them tells us about the universe of sets as a whole.

1.2. The language of set theory

For the rest of this course, we will be working in a **universe of set theory**, i.e., a collection $\mathcal{U}$ of objects equipped with a binary relation $\in$. In other words, a universe of set theory is a *directed graph* whose vertices are the members of $\mathcal{U}$ and whose directed edges are given by the relation $\in$. The members of $\mathcal{U}$—i.e., the vertices of the digraph—are called **sets**, while $\in$ is called the **membership relation**. When x and y are sets such that $x \in y$, we say that x is an **element** or a **member** of y or that x **belongs** to y. At this point, you should forget everything you know about sets: although we use the name "set" for the members of $\mathcal{U}$, without any additional assumptions, *any* digraph is a valid universe of set theory.

Using the relation $\in$, we can define an array of other properties of sets. For example, we write $x \subseteq y$ and say that x is a **subset** of y, if all elements of x are also elements of y; in symbols

$$\forall z\,(z \in x \;\rightarrow\; z \in y). \tag{1.3}$$

Note that here the universal quantifier $\forall z$ ranges over all members of $\mathcal{U}$ (i.e., over all sets). Throughout the course, we will be working with various properties that can be expressed by formulas such as (1.3). Formally, we say that they can be expressed in the **language of set theory**. The language of set theory consists of the following symbols:

- the membership relation symbol $\in$,
- the equality symbol $=$,
- logical connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$,
- quantifiers $\forall$, $\exists$,
- parentheses (,), and
- variables x, y, A, B, ...

A **word** in the language of set theory is a finite string of symbols from the above list. A variable x **appears** in a word w if it is one of the symbols used in w at least once. Let w be a word and let x be a variable that appears in w. We say that x is **free** in w if w does not contain the words $\exists x$ and $\forall x$ as contiguous substrings; otherwise, x is **bound** in w. Thus, if we say that a variable x is *not* bound in w, this means that either x does not appear in w, or x is free in w. A **formula** is a word built according to the following rules:

- if x and y are variables, then $x = y$ and $x \in y$ are formulas;
- if φ is a formula, then $\neg(\varphi)$ is a formula;
- if φ and ψ are formulas such that no variable free in one of these formulas is bound in the other, then $(\varphi) \wedge (\psi)$, $(\varphi) \vee (\psi)$, and $(\varphi) \rightarrow (\psi)$ are formulas;
- if φ is a formula and x is a variable not bound in φ, then $\forall x\,(\varphi)$ and $\exists x\,(\varphi)$ are formulas.

Only words obtained through finitely many applications of the above rules are formulas.

Example 1.2. The formula $\forall z\,((z \in x) \rightarrow (z \in y))$ mentioned above has two free variables x and y and asserts that x is a subset of y.

Example 1.3. The formula $\forall y\,(\neg(y \in x))$ says that x has no elements (i.e., x is an empty set).

Exercise 1.2. Write down a formula whose meaning is "x has exactly one element."

Here we should make an important remark. Formulas, as defined above, *are not sets*, in the sense that they are not members of $\mathcal{U}$. You should keep in mind that so far, $\mathcal{U}$ is an arbitrary digraph, and there is no relationship whatsoever between its vertices and finite strings of symbols formed according to certain rules. That being said, we will later introduce axioms that will allow us to define notions such as "natural numbers" and "finite sequences" inside $\mathcal{U}$ (after all, our goal is to view $\mathcal{U}$ as a model of set theory that is rich enough to express all of mathematics). Nevertheless, the above definition of a formula refers to these notions in an "intuitive" sense, rather than to their set-theoretic counterparts. In other words, for the purposes of this course, it will be assumed that you comprehend the English language, are able to perform correct mathematical arguments, and are familiar with basic mathematical concepts such as "a finite string of symbols." The extent to which these assumptions can be removed is an interesting question (in mathematical logic and philosophy), but it falls outside the scope of this course.

When dealing with formulas, we often use some standard abbreviations and conventions. For instance, we write $x \neq y$ for $\neg(x = y)$ and $x \notin y$ for $\neg(x \in y)$. Also, $(\varphi) \leftrightarrow (\psi)$ is a shortcut for

$$((\varphi) \rightarrow (\psi)) \wedge ((\psi) \rightarrow (\varphi)).$$

When this does not impede understanding, we often omit some of the parentheses to aid readability. For instance, we may write

$$x = y \vee (x \in y \wedge x \in z) \qquad \text{to mean} \qquad (x = y) \vee ((x \in y) \wedge (x \in z)).$$

Another convenient convention is to write $\exists x \in y\,(\ldots)$ instead of $\exists x\,(x \in y \wedge (\ldots))$.

Exercise 1.3. Explain what the notation $\forall x \in y\,(\ldots)$ means.

If $\mathcal{U}$ is a universe of set theory, then, given any formula φ, we may replace some of the free variables in φ by members of $\mathcal{U}$, obtaining a **formula with parameters** from $\mathcal{U}$. For example, if a is a member of $\mathcal{U}$ and x is a variable, then $x \in a$ is a formula asserting that x is an element of a, where a is used as a parameter.

A formula φ (possibly with parameters from $\mathcal{U}$) can be interpreted by viewing $\in$ as a symbol representing the binary relation on $\mathcal{U}$ and allowing the variables to range over $\mathcal{U}$. If φ is such a formula without any remaining free variables not replaced by parameters, then it is called a **sentence**. Any sentence φ is naturally seen as either true or false in $\mathcal{U}$. If φ is true in $\mathcal{U}$, then we write $\mathcal{U} \models \varphi$.

Exercise 1.4. Give a careful definition of what it means for a sentence φ to be true in $\mathcal{U}$. You will have to start with the case when φ is of the form $a = b$ or $a \in b$ (where a and b are sets in $\mathcal{U}$ used as parameters) and then proceed inductively through the possible steps of the construction of φ.

1.3. The Axiom of Extensionality

Consider the universe of set theory $\mathcal{U}$ consisting of three distinct sets a, b, c such that the only instances of the membership relation are $a \in b$ and $a \in c$. Then $\mathcal{U} \models b \subseteq c$, since the only element of b, namely a, is also an element of c. Similarly, we have $\mathcal{U} \models c \subseteq b$. Nevertheless, $b \neq c$. This shows that $\mathcal{U}$ violates the first axiom of ZFC, called the **Axiom of Extensionality** (Ext for short):

Extensionality (Ext)

$$\forall x \forall y\,\big((x \subseteq y \wedge y \subseteq x) \to x = y\big).$$

Exercise 1.5. Check that the Axiom of Extensionality is equivalent to the following:

$$\forall x \forall y\,\big(\forall z\,(z \in x \;\leftrightarrow\; z \in y) \;\to\; x = y\big).$$

From now on, unless explicitly stated otherwise, we shall assume that $\mathcal{U} \models \mathsf{Ext}$.

1.4. Classes

A **class** is simply another name for a formula with one free variable (possibly with parameters). Given such a formula $\varphi(x)$ with a single free variable x, we write the corresponding class as

$$\mathcal{C} \,:=\, \{x \,:\, \varphi(x)\}.$$

That is, we think of $\mathcal{C}$ as the collection of all sets x satisfying $\varphi(x)$. *This is nothing but a mere verbal convenience.* Every statement about classes is really a statement about formulas, just phrased using different—and often more convenient—notation. For example, if $\mathcal{C}$ is a class given by a formula $\varphi(x)$, then we write $x \in \mathcal{C}$ to mean that $\varphi(x)$ holds. Here are some examples of classes:

Example 1.4. The class of all sets $\mathcal{U} = \{x \,:\, x = x\}$. Every set x satisfies $x \in \mathcal{U}$.

Example 1.5. The **empty class** $\varnothing := \{x \,:\, x \neq x\}$. There is no set x such that $x \in \varnothing$.

Example 1.6. The class of all one-element sets:

$$\{x \,:\, \exists y \forall z\,(z \in x \longleftrightarrow z = y)\}.$$

Exercise 1.6. Show that the class $\{x : \exists y \exists z\, (x = (y, z))\}$ of all ordered pairs in indeed a class, where the ordered pair (y, z) is defined as $(y, z) := \{\{y\}, \{y, z\}\}$. To this end, you will need to check that the property $x = (y, z)$ can be expressed by a formula in the language of set theory.

Exercise 1.7. Give further interesting examples of classes.

We use standard set-theoretic notation, such as $\cap$ and $\cup$, for classes in the obvious way. For instance, given two classes $\mathcal{C} = \{x : \varphi(x)\}$ and $\mathcal{D} = \{x : \psi(x)\}$, the class

$$\mathcal{C} \cap \mathcal{D} \;:=\; \{x : x \in \mathcal{C} \text{ and } x \in \mathcal{D}\}$$

corresponds to the formula $\varphi(x) \wedge \psi(x)$. In the same setting, we write $\mathcal{C} \subseteq \mathcal{D}$ if

$$\forall x\, (x \in \mathcal{C} \to x \in \mathcal{D}),$$

or, in terms of formulas, $\forall x\, (\varphi(x) \to \psi(x))$.

Exercise 1.8. Let $\mathcal{C}$ and $\mathcal{D}$ be classes. Define the classes $\mathcal{C} \cup \mathcal{D}$ and $\mathcal{C} \times \mathcal{D}$.

An important convention is that, given a pair of classes $\mathcal{C}$ and $\mathcal{D}$, we write

$$\mathcal{C} \;=\; \mathcal{D}$$

to mean $(\mathcal{C} \subseteq \mathcal{D}) \wedge (\mathcal{D} \subseteq \mathcal{C})$. This is a slight abuse of notation (because $\mathcal{C} = \mathcal{D}$ here doesn't mean that the underlying formulas are actually equal, just that they are equivalent), but it makes working with classes particularly convenient.

Every set a gives rise to the class $\mathcal{C}$ given by the formula $x \in a$ (here a is used as a parameter). By definition, the members of this class $\mathcal{C}$ are precisely the elements of a. In general, given a class $\mathcal{C}$, we say (with another small abuse of terminology) that $\mathcal{C}$ **is a set** if there is a set a in $\mathcal{U}$ such that

$$\forall x\, (x \in a \;\longleftrightarrow\; x \in \mathcal{C}). \tag{1.4}$$

Note that, if $\mathcal{U} \models \mathsf{Ext}$, then such a set a must be unique. We shall often use the same name for a class $\mathcal{C}$ and the set a satisfying (1.4) (for instance, we may write $\mathcal{C} = a$ in that case). If no such set a exists, we say that $\mathcal{C}$ is a **proper class**. Most axioms of ZFC assert that certain classes are sets.

Example 1.7 (Russell's paradox)**.** Consider the class $R := \{x : x \notin x\}$. Russell's paradox discussed in §1.1 can be seen as a proof that R is a proper class. Indeed, if R were a set, then we would either have $R \in R$ or $R \notin R$, and both of these assumptions lead to a contradiction.

1.5. A few more axioms

We are ready to add a few axioms to our list, all of which we will henceforth assume to be true in $\mathcal{U}$.

Empty Set (Empty)

The empty class $\varnothing$ is a set.

In symbols, the Empty Set Axiom can be written as

$$\exists x \forall y\, (y \in x \;\longleftrightarrow\; y \neq y),$$

or, more concisely, $\exists x \forall y\, (y \notin x)$. This is a common feature of the axioms of ZFC: they can all be expressed by sentences in the language of set theory (without parameters).

As usual, we denote the empty set (which exists by Empty) by the symbol $\varnothing$ (same as for the empty class). Note that the expression $x = \varnothing$ is really a shortcut for the following formula:

$$\forall y\, (y \notin x).$$

It is a bit less obvious that an expression such as $\varnothing \in x$ can be written as a formula as well. The idea is to change the phrase "the empty set is an element of x" to "there exists a set that is an element of x and is empty," i.e.,

$$\exists z \left(z \in x \wedge \forall y \left(y \notin z\right)\right).$$

This trick of getting rid of extra symbols by introducing additional quantifiers is quite common, so it is good to keep it in mind for later use.

Pairing (Pair)

For all sets a, b, the class $\{a, b\} := \{x : x = a \vee x = b\}$ is a set.

Note that the formula $x = a \vee x = b$ defining the class $\{a, b\}$ uses a and b as parameters. Again, the Pairing Axiom can be stated explicitly as a sentence in the language of set theory:

$$\forall a \forall b \, \exists x \forall y \left(y \in x \longleftrightarrow (y = a \vee y = b)\right).$$

Proposition 1.8. *For every set a, the class $\{a\} := \{x : x = a\}$ is a set*

PROOF. Note that $\{a\} = \{a, a\}$ and apply Pair. ■

Proposition 1.9. *For all sets a, b, the ordered pair $(a, b) := \{\{a\}, \{a, b\}\}$ is a set.*

PROOF. Use Pair three times. ■

Unfortunately, the Pairing Axiom does not suffice to prove the existence of a triple $\{a, b, c\}$ (or any set with more than two elements). To remedy this, we need another axiom:

Union (Union)

For every set a, the class $\bigcup a := \{x : \exists y \in a \, (x \in y)\}$ is a set.

The set $\bigcup a$ is called the **union** of a. It is the union of all members of a (keep in mind that the elements of a are themselves sets, so this makes sense!).

Proposition 1.10. *For all sets a, b, their union $a \cup b := \{x : x \in a \vee x \in b\}$ is a set.*

PROOF. Note that $a \cup b = \bigcup\{a, b\}$, which is a set by Pair and Union. ■

Proposition 1.11. *For all sets a, b, c, $\{a, b, c\}$ (defined in the obvious way) is also a set. Furthermore, for any finite list of sets $a_1, \ldots, a_k$, we can form a set $\{a_1, \ldots, a_k\}$.*

PROOF. Given sets a, b, c, we can write $\{a, b, c\} = \{a\} \cup \{b, c\}$, which is a set by Proposition 1.10. Similarly, if we are given a finite list $a_1, \ldots, a_k$ of sets, we can form the set $\{a_1, \ldots, a_k\}$ by applying the Union Axiom $k - 2$ times. ■

Here we should make an important remark. So far, we haven't described the interpretation of the concept "natural number" inside $\mathcal{U}$. As a result, the variable k in the "furthermore" part of Proposition 1.11 refers not to a set but to our "intuitive" understanding of what "finite" means. In other words, Proposition 1.11 really contains an infinite list of sentences in the language of set theory, asserting the existence of sets such as $\{a_1, a_2, a_3\}$, $\{a_1, a_2, a_3, a_4\}$, $\{a_1, a_2, a_3, a_4, a_5\}$, etc., each with its own proof (note that the length of the proof is proportional to the number of elements in the set we are trying to construct). A logician would say that Proposition 1.11 is not a theorem but a *theorem schema*: a "blueprint" explaining how to prove an infinite list of individual theorems.

The last axiom in this section is the **Poweset Axiom**:

Powerset (Pow)

For every set a, the class $\mathcal{P}(a) := \{x : x \subseteq a\}$ is a set, called the **powerset** of a.

1.6. The Axiom Schema of Comprehension

The above axioms (Empty, Pair, Union, and Pow) all describe specific operations on sets that produce sets as output. In this section we will expand our axiom list by giving a general condition that guarantees that a certain class is a set. The intuition is this:

If a class is "small," then it is a set.

One way to witness that a class is "small" is by including it inside a (larger) set:

Comprehension (Comp)

A subclass of a set is a set. I.e., if $\mathcal{C}$ is a class and x is a set such that $\mathcal{C} \subseteq x$, then $\mathcal{C}$ is a set.

Technically, Comp is a *axiom schema* rather than an individual axiom, in the sense that it includes an infinite list of sentences of a particular form, one for each class $\mathcal{C}$. Specifically, for every formula $\varphi(x, a_1, \ldots, a_k)$ with free variables x, a_1, ..., a_k and no parameters, the following is an axiom:

$$\forall a_1 \ldots \forall a_k \left(\exists x \forall y \left(\varphi(y, a_1, \ldots, a_k) \to y \in x\right) \longrightarrow \exists z \forall y \left(\varphi(y, a_1, \ldots, a_k) \leftrightarrow y \in z\right)\right). \tag{1.5}$$

Here we think of the class $\mathcal{C}$ in the statement of the Comprehension Schema as defined by the formula φ with parameters a_1, ..., a_k, i.e., $\mathcal{C} = \{y : \varphi(y, a_1, \ldots, a_k)\}$.

Even though we have not yet discussed some further important axioms, once we assume that $\mathcal{U} \models$ Ext + Empty + Pair + Union + Pow + Comp, there is already a great deal of mathematical machinery we can construct.

Proposition 1.12. *For any sets X, Y, their* product $X \times Y := \{(x, y) : x \in X, y \in Y\}$ *is a set.*

Proof. Since $X \times Y$ is a class (exercise!), we just need to find a set that includes $X \times Y$ as a subclass and then apply Comprehension. To this end, note that if

$$z = (x, y) = \{\{x\}, \{x, y\}\} \in X \times Y,$$

then every element of z is a subset of $X \cup Y$, and thus $z \subseteq \mathcal{P}(X \cup Y)$. It follows that

$$X \times Y \subseteq \mathcal{P}(\mathcal{P}(X \cup Y)),$$

and we are done by Union, Pow, and Comp. ■

Exercise 1.9. Prove that if X and Y are sets, then so are $X \cap Y$ and $X \setminus Y$.

Exercise 1.10. Show that for every nonempty set a, the class $\bigcap a := \{x : \forall y \in a\, (x \in y)\}$ is a set.

Exercise 1.11. Show that $\mathcal{U}$ is a proper class. Hint: Example 1.7.

1.7. Relations and functions

A (**binary**) **relation** is a set R or ordered pairs. If R is a relation, we often write $x\,R\,y$ to mean $(x, y) \in R$ and say that x is R-**related** to y. Given a relation R, we define the following classes:

- the **domain** of R: $\mathrm{dom}(R) := \{x : \exists y\, ((x, y) \in R)\}$,
- the **range** of R: $\mathrm{ran}(R) := \{y : \exists x\, ((x, y) \in R)\}$.

Proposition 1.13. *For a relation R,* $\mathrm{dom}(R)$ *and* $\mathrm{ran}(R)$ *are sets.*

Proof. Note that $\mathrm{dom}(R)$ and $\mathrm{ran}(R)$ are subclasses of $\bigcup\bigcup R$, so they are sets by Comp. ■

Given a set A, we let the **image** of A under R be the class

$$R[A] := \{y : \exists x \in A\, ((x, y) \in R)\}.$$

Exercise 1.12. Show that if R is a relation and A is a set, then $R[A]$ is also a set.

Exercise 1.13. Show that for a relation R, $\mathrm{ran}(R) = R[\mathrm{dom}(R)]$.

As discussed in §1.1, we shall encode functions in $\mathcal{U}$ as sets of ordered pairs—i.e., relations—with certain properties:

Definition 1.14 (Functions)**.** A **function** is a relation f such that for every set x in $\mathcal{U}$, there is at most one set y with $(x, y) \in f$, or, equivalently,

$$\forall x \forall y \forall z \left(((x, y) \in f \wedge (x, z) \in f) \longrightarrow y = z \right).$$

Exercise 1.14. Write out a formula in the language of set theory saying that $(a, b) \in c$.

Since a function f is a relation, the notation $\mathrm{dom}(f)$ and $\mathrm{ran}(f)$ makes sense for it. For each $x \in \mathrm{dom}(f)$, we let $f(x)$ be the unique element of $\mathrm{ran}(f)$ such that $(x, f(x)) \in f$.

Exercise 1.15. Write out (or at least convince yourself that you can write out) formulas in the language of set theory saying that $f(x) = y$, $f(x) \in y$, and $y \in f(x)$.

Exercise 1.16. For a function f and a set x, explain the difference between $f(x)$ and $f[x]$.

Given sets X, Y, we write $f\colon X \to Y$ and say that f is a function **from** X **to** Y if f is a function with $\mathrm{dom}(f) = X$ and $\mathrm{ran}(f) \subseteq Y$. The class of all functions from X to Y is denoted by ${}^{X}Y$.

Exercise 1.17. Prove that for sets X, Y, the class ${}^{X}Y$ is a set.

1.8. The Axiom of Infinity

As a reminder, we are currently assuming that

$$\mathcal{U} \models \mathsf{Ext} + \mathsf{Empty} + \mathsf{Pair} + \mathsf{Union} + \mathsf{Pow} + \mathsf{Comp}.$$

This is already a fairly rich system of axioms. Nevertheless, it is still insufficient. In particular, it does not imply the existence of any *infinite* sets (for example, the powerset of a finite set is still finite). This issue is remedied by the so-called **Axiom of Infinity**, or Inf for short. The aim of this axiom is to assert the existence of a specific infinite set, namely the set of all natural numbers. Recall that we represent natural numbers by sets in the following way:

$$0 := \varnothing, \quad 1 := \{0\}, \quad 2 := \{0, 1\}, \quad \ldots, \quad n + 1 := \{0, 1, \ldots, n\} = n \cup \{n\}, \quad \ldots. \tag{1.6}$$

Bearing this in mind, how do we describe the set

$$\{0,\ 1,\ 2,\ 3,\ \ldots\}?$$

The challenge here lies in the use of the "…" symbol, which is imprecise and cannot be invoked in the formal language of set theory. To eliminate it, we rely on the following observation: the set of all natural numbers is the *smallest set that contains* 0 *and is closed under the operation* $n \mapsto n + 1$.

Formally, we say that a set X is **inductive** if $\varnothing \in X$ and $\forall x\, (x \in X \to x \cup \{x\} \in X)$.

Exercise 1.18. Let $\mathcal{F}$ be a nonempty set all of whose elements are inductive. Show that the set $\bigcap \mathcal{F}$ is also inductive.

We now add the following axiom to our list:

Infinity (Inf)

There exists an inductive set.

Theorem 1.15. *There is a unique inductive set* ω *such that for every inductive set* X, $\omega \subseteq X$.

Proof. It follows from Ext that such a set ω, if it exists, must be unique. To prove existence, let ω be the following class:

$$\omega := \{x : \forall X\, (X \text{ is inductive} \longrightarrow x \in X)\}.$$

By Inf, there exists some inductive set X, and since $\omega \subseteq X$ by definition, we see that ω is a set by Comp. The very definition of ω insures that ω is contained in every inductive set. It remains to verify that ω is itself inductive, which is left as an exercise. ■

From now on, we shall use ω to denote the smallest inductive set whose existence and uniqueness are established in Theorem 1.15. The elements of ω are called **natural numbers**. Note that, mostly for historical reasons, set-theorists use ω instead of $\mathbb{N}$ to denote the set of all natural numbers. While this notation is somewhat unusual, it will be useful to us, as it emphasizes that ω is a member of the universe $\mathfrak{U}$—i.e., a certain vertex of the digraph we are working with—which is not the same thing as the collection $\mathbb{N}$ of all natural numbers understood in the "intuitive" sense. That being said, for each particular "usual" natural number, such as 5, there exists a well-defined corresponding element of ω. For example, letting $n + 1 := n \cup \{n\}$ for all $n \in \omega$, the "ordinary" natural number 5 corresponds to the following element of ω:

$$((((0 + 1) + 1) + 1) + 1) + 1, \tag{1.7}$$

where "0" is a different name for $\varnothing$. For convenience, we use "5" to denote the set (1.7) (and the same convention extends to all other "ordinary" natural numbers, such as 2024). However, it is important to keep in mind that we are not allowed to use what we know about "standard" natural numbers to deduce properties of the elements of ω; instead, we must rely on the axioms of set theory and the definition of ω given by Theorem 1.15.

Example 1.16. How do we prove that for all $n \in \omega$, either $\varnothing = n$ or $\varnothing \in n$? (This property must hold if (1.6) is indeed true.) The only thing we can use is the definition of ω, i.e., the fact that ω is the smallest inductive set. This necessitates a proof by induction. Let

$$P := \{n \in \omega \,:\, \varnothing = n \vee \varnothing \in n\}.$$

By definition, $P \subseteq \omega$, and hence, by Comp, P is a set. Now we observe that P is inductive:

> $\varnothing \in P$: This is true by the definition of P (and since $\varnothing \in \omega$).
>
> *If $n \in P$, then $n \cup \{n\} \in P$*: If $n \in P \subseteq \omega$, then, since ω is inductive, we have $n \cup \{n\} \in \omega$. As $n \in P$, we have $n = \varnothing$ or $\varnothing \in n$. In the first case, $n \cup \{n\} = \{\varnothing\}$ and $\varnothing \in \{\varnothing\}$, so $n \cup \{n\} = \{\varnothing\} \in P$. In the second case, $\varnothing \in n \subseteq n \cup \{n\}$, so $n \cup \{n\} \in P$ again.

Since P is inductive and ω is the smallest inductive set, we conclude that $\omega \subseteq P$. It follows that $P = \omega$ by Comp.

1.9. Class functions and the Axiom Schema of Replacement

A useful technique for defining new sets that we explored in §§1.6 and 1.7 was to start with a ground set X, apply the powerset operation a few times, and then pass to a subset using Comprehension. But what will happen if we use the Infinity Axiom to iterate the powerset operation an *unbounded* number of times?

To be specific, consider the following recursive construction of sets V_n for $n \in \omega$:

$$\begin{aligned}
V_0 &:= \varnothing, \\
V_1 &:= \mathcal{P}(V_0) = \{\varnothing\}, \\
V_2 &:= \mathcal{P}(V_1) = \{\varnothing, \{\varnothing\}\}, \\
V_3 &:= \mathcal{P}(V_2) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}, \\
&\cdots\cdots \\
V_{n+1} &:= \mathcal{P}(V_n), \\
&\cdots\cdots
\end{aligned}$$

Can we now form the set

$$V_\omega := \bigcup_{n\in\omega} V_n = \bigcup\{V_n : n \in \omega\}?$$

Thanks to the Union Axiom, for V_ω to be a set we just need to ensure that $U := \{V_n : n \in \omega\}$ is a set. The difficulty here is that U cannot be "captured" by applying the powerset operation to the empty set any bounded number of times (and the empty set seems to be the only place we can start). As a result, we have no larger set from which U can be carved out by Comprehension. This raises the question: What makes us think that U is a set at all? Remember our motto from §1.6:

If a class is "small," then it is a set.

Now, the elements of $U = \{V_n : n \in \omega\}$ are indexed by the natural numbers, which shows that U is "not larger than" ω (even though it is not a subset of ω!), and hence it ought to be a set. This intuition is captured by the **Axiom Schema of Replacement**. To state it precisely, we need some terminology and notation.

A **class function** Φ is a formula $\varphi(x, y)$ with two free variables (and possibly with parameters from $\mathcal{U}$) such that for all $x \in \mathcal{U}$, there is at most one $y \in \mathcal{U}$ such that $\varphi(x, y)$ holds; in symbols,

$$\forall x \forall y \forall z \left((\varphi(x, y) \wedge \varphi(x, z)) \longrightarrow y = z\right).$$

Given a class function Φ corresponding to a formula $\varphi(x, y)$, we define the following classes:

- the **domain** of Φ: $\mathrm{dom}(\Phi) := \{x : \exists y\, \varphi(x, y)\}$,
- the **range** of Φ: $\mathrm{ran}(\Phi) := \{y : \exists x\, \varphi(x, y)\}$.

(Compare this to the definitions in §1.7.) Unsurprisingly, for $x \in \mathrm{dom}(\Phi)$, we write $\Phi(x)$ to denote the unique $y \in \mathrm{ran}(\Phi)$ such that $\varphi(x, y)$. Given classes $\mathcal{C}$ and $\mathcal{D}$, the notation $\Phi \colon \mathcal{C} \to \mathcal{D}$ means that Φ is a class function with $\mathrm{dom}(\Phi) = \mathcal{C}$ and $\mathrm{ran}(\Phi) \subseteq \mathcal{D}$.

Here are some examples of class functions with domain equal to $\mathcal{U}$:

- the identity function $x \mapsto x$ given by the formula $x = y$,
- the function $x \mapsto \{x\}$ given by the formula $\forall z\,(z \in y \longleftrightarrow z = x)$,
- the function $x \mapsto \mathcal{P}(x)$ (exercise!),
- for any fixed set a, the function $x \mapsto x \cup a$, given by the formula $\forall z\,(z \in y \leftrightarrow (z \in x \vee z \in a))$ (note that here a is used as a parameter),
- for any fixed set a, the constant function $x \mapsto a$ (exercise!),
- the function $x \mapsto x \cup \{x\}$, which yields the successor operation on ω (exercise!).

Exercise 1.19. Give further interesting examples of class functions.

If $\mathcal{C}$ is a class and Φ is a class function, then the **image** of $\mathcal{C}$ under Φ is the class

$$\Phi[\mathcal{C}] := \{y : \exists x\,(x \in \mathcal{C} \wedge \Phi(x) = y)\}.$$

Replacement (Rep)

The image of a set under a class function is a set. I.e., if A is a set and Φ is a class function, then $\Phi[A]$ is a set.

Note that, like Comprehension, Replacement is an axiom schema that includes one axiom for every formula that defines a class function.

Exercise 1.20. Write out explicitly the sentences without parameters in the language of set theory that are contained in the Replacement Schema (by analogy with (1.5)).

Example 1.17. It is worth remarking that for specific class functions Φ, the Replacement Schema often follows from the other axioms. For example, by applying it to the powerset function $\mathcal{P}$, we see that for each set A, the following is also a set:

$$\mathcal{P}[A] \coloneqq \{\mathcal{P}(x) : x \in A\}.$$

However, to establish this fact we don't have to invoke Replacement: as $\mathcal{P}[A] \subseteq \mathcal{P}(\bigcup A)$, it is a set by Union, Pow, and Comp.

Let us now go back to the set $U \coloneqq \{V_n : n \in \omega\}$. By the Replacement Schema, to show it is a well-defined set, we only need to argue that the mapping $\omega \to \mathfrak{U} \colon n \mapsto V_n$ is a class function, i.e., there is a formula $\varphi(x, y)$ such that

$$\varphi(x, y) \iff x \in \omega \text{ and } y = V_x.$$

This is surprisingly tricky, because the definition of the set V_x is *recursive*, and the language of set theory does not have a "built-in" mechanism for talking about recursion. The following (rather ingenious) way to express recursive definitions using the language of set theory is called **Dedekind's formalization of recursion**. The idea is this: in order to confirm that $y = V_x$, we have to list all the sets $V_0, V_1, \ldots, V_x$ in order and then check that the resulting sequence satisfies the recursive definition. (We will encounter this idea in a more general context again later.) In other words, what we want to say is something along these lines: We have $y = V_x$ if and only if

$x \in \omega$ and there exist sets $W_0, W_1, \ldots, W_x$ such that:

- $W_0 = \varnothing$,
- $W_{i+1} = \mathcal{P}(W_i)$ *for all* $i < x$, *and*
- $W_i = y$.

This is still not quite a formula in the language of set theory, because of the "..." symbol. But this can be remedied by asking for the existence of a *single* set, namely the function

$$W : n + 1 \to \mathfrak{U} : i \mapsto W_i,$$

which, as a set, is equal to

$$W = \{(0, W_0), (1, W_1), \ldots, (x, W_x)\}.$$

(Recall that for $x \in \omega$, we have $x + 1 = \{0, 1, \ldots, x\}$.) Thus, we have $y = V_x$ if and only if

$x \in \omega$ and there exists a function W with $\mathrm{dom}(W) = x + 1$ such that:

- $W(0) = \varnothing$,
- *for each* $i < x$, $W(i + 1) = \mathcal{P}(W(i))$, *and*
- $W(x) = y$.

Exercise 1.21 (tedious but useful for building character)**.** Write this down as an actual formula. You may find it helpful to keep in mind that a class function can be defined by a formula with parameters. For example, you may use ω as a parameter in your formula. (That being said, the above definition can also be written as a formula without parameters.)

Exercise 1.22 (harder than it looks!)**.** Prove that this formula actually defines a class function whose domain is all of ω. (Hint: You will need to use the formal definition of ω as the smallest inductive set; see Example 1.16 for inspiration.)

The following corollary of the Replacement Schema provides another interpretation of the "small classes are sets" motto:

Proposition 1.18. *There is no injective class function from a proper class to a set.*

Proof. Suppose, toward a contradiction, that $\Phi\colon \mathcal{C} \to A$ is an injective class function from a proper class $\mathcal{C}$ to a set A. By Comp, $\operatorname{ran}(\Phi) \subseteq A$ is a set. Since Φ is injective, we can define a class function $\Psi\colon \operatorname{ran}(\Phi) \to \mathcal{C}$ by letting $\Psi(y)$ be the unique $x \in \mathcal{C}$ with $\Phi(x) = y$. Then $\Psi[A] = \mathcal{C}$ is a set by Replacement, which contradicts the assumption that $\mathcal{C}$ is a proper class. ■

Exercise 1.23. Show that there is no set-to-one class function from a proper class to a set. (A class function Φ is **set-to-one** if for all y, the class $\{x : \Phi(x) = y\}$ is a set.)

If f is a function in $\mathcal{U}$ (see §1.7), then f gives rise to the class function Φ given by

$$\Phi(x) = y \quad :\Longleftrightarrow \quad f(x) = y \quad \Longleftrightarrow \quad (x, y) \in f.$$

(The formula defining Φ uses f as a parameter.) In general, given a class function Φ, we say that Φ **is a set function** if there is a set f in $\mathcal{U}$ such that f is a function satisfying

$$\forall x\, \forall y\, (f(x) = y \longleftrightarrow \Phi(x) = y).$$

Exercise 1.24. Show that if Φ is a class function whose domain is a set, then Φ is a set function.

1.10. The axiom system ZF^-

All the axioms that we have introduced so far form an axiom system denoted by ZF^-:

$$\mathsf{ZF}^- \;=\; \mathsf{Ext} + \mathsf{Empty} + \mathsf{Pair} + \mathsf{Union} + \mathsf{Pow} + \mathsf{Comp} + \mathsf{Inf} + \mathsf{Rep}.$$

There are still two axioms missing for the complete system ZFC: the Axiom of Foundation, AF and the Axiom of Choice, AC.[ii] However, we will only introduce these axioms a little later, when their role in the foundations of set theory will become more apparent. For now, we will be working in the system ZF^-, which already is quite rich and sufficient for a good deal of interesting mathematics.

Some of the axioms of ZF^- are redundant, as the following exercises show:

Exercise 1.25. Deduce Comp from the rest of the axioms of ZF^-.

Exercise 1.26. Deduce Pair from the rest of the axioms of ZF^-.

[ii] There is missed opportunity here of simply denoting the system Z instead of ZF^-. Unfortunately, the "F" in "ZFC" stands for "Fraenkel," not "Foundation."

2. Problem set 1

The default axiom system for the following exercises is ZF^-.

Exercise 2.1. For each of the following properties, write down an explicit formula *without parameters* in the language of set theory asserting that a set x has this property:

(*a*) "x is an ordered pair,"

(*b*) "x is a function,"

(*c*) "x is a natural number."

Exercise 2.2. Let $R \subseteq A \times A$ be a relation on a set A. We say that R is:

- **reflexive** if $x\,R\,x$ for all $x \in A$,
- **symmetric** if for all x, $y \in A$, $x\,R\,y$ implies $y\,R\,x$,
- **transitive** if for all x, y, $z \in A$, if $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$.

A relation is called an **equivalence relation** if it is reflexive, symmetric, and transitive. If R is an equivalence relation on A, then, given $x \in A$, the R-**equivalence class** of x is the set

$$[x]_R \coloneqq \{y \in A \,:\, x\,R\,y\} \;=\; R[\{x\}].$$

The class $\{[x]_R \,:\, x \in A\}$ is called the **quotient of** A **by** R and denoted by A/R.

(*a*) Show that A/R is a set. Do you need to use Replacement?

A **partition** of a set A is a set F of pairwise disjoint sets such that $\bigcup F = A$.

(*b*) Show that if R is an equivalence relation on a set A, then A/R is a partition of A.

(*c*) Conversely, suppose that F is a partition of a set A. Show that there is a unique equivalence relation R on A such that $F = A/R$.

Exercise 2.3. Prove that the following classes are sets:

(*a*) $X \cap Y$ for all sets X, Y,

(*b*) $X \backslash Y$ for all sets X, Y,

(*c*) $\bigcap X \coloneqq \{a \,:\, \forall Y \in X\,(a \in Y)\}$ for every nonempty set X

(*d*) ${}^XY \coloneqq \{f \,:\, f \text{ is a function from } X \text{ to } Y\}$ for all sets X, Y.

Exercise 2.4. Prove that $\{f \,:\, f \text{ is a function}\}$ is a proper class.

Exercise 2.5 (this is Exercise 1.24 in the main text)**.** Recall that a class function Φ **is a set function** if there is a set $f \in \mathfrak{U}$ such that f is a function and

$$\forall x\,\forall y\,(y = f(x) \longleftrightarrow y = \Phi(x)).$$

Show that a class function Φ is a set function if and only if $\mathrm{dom}(\Phi)$ is a set.

Exercise 2.6 (this is Exercise 1.26 in the main text)**.** Show that the Pairing Axiom follows from the rest of the axioms of ZF^-.

3. Ordinals, transfinite recursion, and the Axiom of Foundation

In this section, we work in a universe $\mathcal{U}$ that satisfies the axiom system ZF^-.

3.1. Well-ordered classes and sets

Let $\mathcal{C}$ be a class and let $\prec$ be a **class relation** on $\mathcal{C}$, i.e., a formula $\varphi(x, y)$ with two free variables x, y (and possibly with parameters from $\mathcal{U}$) such that

$$\forall x \forall y\, (\varphi(x, y) \longrightarrow x \in \mathcal{C} \wedge y \in \mathcal{C}).$$

We shall write $x \prec y$ to indicate that $\varphi(x, y)$ holds.

Exercise 3.1. Let S be a set and let $\prec$ be a class relation on S. Show that $\prec$ is actually a **set relation**, that is, the class $\{(x, y) \in S \times S \,:\, x \prec y\}$ is a set.

We call $\prec$ a **strict partial order**(**ing**) on $\mathcal{C}$ if:

(P1) $\prec$ is **irreflexive**, i.e., $\forall x\, \neg(x \prec x)$; and

(P2) $\prec$ is **transitive**, i.e., $\forall x \forall y \forall z\, ((x \prec y \wedge y \prec z) \rightarrow x \prec z)$.

Exercise 3.2. Show that a strict partial order $\prec$ is **asymmetric**, i.e., $\forall x \forall y (x \prec y \rightarrow \neg(y \prec x))$.

When dealing with a strict partial order $\prec$, we adopt the usual convention of writing $x \preccurlyeq y$ to mean $x \prec y \vee x = y$ and use $y \succ x$ as an equivalent to $x \prec y$.

A strict partial order $\prec$ on a class $\mathcal{C}$ is called **linear**, or **total**, if

$$\forall x,\, y \in \mathcal{C}\, (x = y \vee x \prec y \vee y \prec x),$$

i.e., if every two members of $\mathcal{C}$ are **comparable**. A linear order $\prec$ on a class $\mathcal{C}$ is a **well-ordering** if it satisfies the following two extra conditions:

(W1) if $S \subseteq \mathcal{C}$ is a nonempty subset of $\mathcal{C}$, then S has a $\prec$-**least element**, i.e., $\exists x \in S\, \forall y \in S\, (x \preccurlyeq y)$;

(W2) for each member $x \in \mathcal{C}$, its **initial segment** $S_x(\mathcal{C}) := \{y \in \mathcal{C} \,:\, y \prec x\}$ is a set.

Notice that if $\prec$ is a linear order on a *set* S, then $\prec$ automatically satisfies (W2). In other words, (W2) is only relevant when $\mathcal{C}$ is a proper class.

Proposition 3.1. *Let $\prec$ be a well-ordering on a class $\mathcal{C}$. If $\mathcal{D} \subseteq \mathcal{C}$ is a nonempty subclass of $\mathcal{C}$, then $\mathcal{D}$ has a $\prec$-least element.*

Proof. This is an apparent strengthening of (W1), since $\mathcal{D}$ may be a proper class. Thankfully, we can use (W2) to reduce the situation to the set case. Indeed, $\mathcal{D}$ is nonempty, so let $x \in \mathcal{D}$ be an arbitrary member of $\mathcal{D}$. By (W2) and Comp, $S := \mathcal{D} \cap S_x(\mathcal{C})$ is a set. If S is empty, then x itself is a $\prec$-least element of $\mathcal{D}$. Otherwise, by (W1), the *set* S has a $\prec$-least element, which is then also a $\prec$-least element of $\mathcal{D}$. ∎

3.2. Ordinals

A set A is **transitive** if every element of A is also a subset of A, i.e., if

$$\forall x \forall y\, (x \in y \wedge y \in A \longrightarrow x \in A).$$

An **ordinal** is a set α such that:

(O1) α is transitive; and

(O2) α is well-ordered by the relation $\in$.

(To be more accurate, we should be saying that α is well-ordered by the *restriction* of $\in$ to α, i.e., by the relation ${\in}{\restriction}\alpha := \{(x, y) \in \alpha \times \alpha \,:\, x \in y\}$.) The class of all ordinals is denoted $\mathbf{Ord}$.

Exercise 3.3. Verify that $\mathbf{Ord}$ is indeed a class.

Exercise 3.4. Suppose that α is an ordinal. Show that every element of α is also an ordinal.

Exercise 3.5. Let $\alpha \in \mathbf{Ord}$. Show that $\alpha \notin \alpha$.

Let $\alpha \in \mathbf{Ord}$. The **successor** of α is the set $\alpha + 1 := \alpha \cup \{\alpha\}$.

Proposition 3.2. *Let $\alpha \in \mathbf{Ord}$. Then $\alpha + 1 \in \mathbf{Ord}$ as well.*

PROOF. We need to check that $\alpha + 1$ is transitive and well-ordered by $\in$.

To show the transitivity of $\alpha + 1$, take any $\beta \in \alpha + 1 = \alpha \cup \{\alpha\}$. Then either $\beta \in \alpha$, in which case $\beta \subseteq \alpha \subset \alpha + 1$ by the transitivity of α, or else, $\beta = \alpha \subset \alpha + 1$.

To prove that $\alpha + 1$ is well-ordered by $\in$, consider any nonempty subset $S \subseteq \alpha + 1$. If $S \cap \alpha \neq \varnothing$, then, since α is an ordinal, $S \cap \alpha$ has a $\in$-least element, which is also a $\in$-least element for S. Otherwise, i.e., if $S \cap \alpha = \varnothing$, then $S = \{\alpha\}$, so α is the $\in$-least (and unique) element of S. ■

Corollary 3.3. $\omega \subseteq \mathbf{Ord}$.

PROOF. Since $\varnothing$ is an ordinal, it follows from the above proposition that $\omega \cap \mathbf{Ord}$ is an inductive set, and thus $\omega \cap \mathbf{Ord} \supseteq \omega$. ■

Exercise 3.6. Prove that ω is an ordinal.

Theorem 3.4 (Well-ordering of ordinals)**.** *The class $\mathbf{Ord}$ is well-ordered by the membership relation $\in$ (or, more precisely, by the restriction $\in\restriction\mathbf{Ord}$).*

We split the proof of Theorem 3.4 into a few lemmas.

Lemma 3.5. *The restriction of the relation $\in$ to $\mathbf{Ord}$ is a strict partial order.*

PROOF. The membership relation on the ordinals is irreflexive due to Exercise 3.5. To prove transitivity, suppose that α, β, γ are ordinals such that $\alpha \in \beta \in \gamma$. Since γ is a transitive set, $\beta \subseteq \gamma$, and hence $\alpha \in \gamma$ as well, as desired. ■

Lemma 3.5 justifies using the following notational convention: Given ordinals α and β, we write $\alpha < \beta$ to mean $\alpha \in \beta$. Note the following key property of ordinals:

$$\alpha \;=\; \{\gamma \in \mathbf{Ord} \,:\, \gamma < \alpha\}.$$

Let $\mathcal{C}$ be a class equipped with a strict partial order $\prec$. We say that a subclass $\mathcal{D} \subseteq \mathcal{C}$ is **downward closed** if for all $x \in \mathcal{D}$ and $y \in \mathcal{C}$, if $y \prec x$, then $y \in \mathcal{D}$.

Lemma 3.6. *Let α be an ordinal and suppose that $D \subseteq \alpha$ is a downward closed subset. Then either $D = \alpha$ or $D \in \alpha$. In particular, D is an ordinal.*

PROOF. Suppose that $D \neq \alpha$ and let β be the least element of $\alpha \backslash D$. Since α is totally ordered, D is downward closed, and $\beta \notin D$, every element of D must be less than β. In other words, every element of D belongs to β, i.e., $D \subseteq \beta$. On the other hand, if $\gamma < \beta$—which is the same as $\gamma \in \beta$—then $\gamma \in \alpha$ (by the transitivity of α) but, by the choice of β, γ cannot belong to $\alpha \backslash D$. Thus, $\gamma \in D$ and hence $\beta \subseteq D$. This shows that $D = \beta \in \alpha$. ■

Lemma 3.7 (Trichotomy)**.** *Let α, $\beta \in \mathbf{Ord}$. Then $\alpha = \beta$, or $\alpha < \beta$, or $\beta < \alpha$.*

PROOF. Let $\gamma := \alpha \cap \beta$. Then γ is a downward closed subset of both α and β (exercise!), thus γ is an ordinal and one of the following four cases occurs:

Case 1: $\gamma = \alpha$ *and* $\gamma = \beta$. In this case $\alpha = \beta$.
Case 2: $\gamma = \alpha$ *and* $\gamma < \beta$. In this case $\alpha < \beta$.
Case 3: $\gamma < \alpha$ *and* $\gamma = \beta$. In this case $\beta < \alpha$.
Case 4: $\gamma < \alpha$ *and* $\gamma < \beta$. In this case $\gamma \in \alpha \cap \beta = \gamma$, which contradicts Exercise 3.5. ■

Proof *of Theorem 3.4.* We already know that the ordinals are totally ordered. It remains to check conditions (W1) and (W2).

(W1) Let $S \subseteq \mathbf{Ord}$ be a nonempty set of ordinals. Pick any $\alpha \in S$. If α is the least element of S, then we are done. Otherwise, $S \cap \alpha$ is a nonempty subset of α, hence $S \cap \alpha$ has a least element, which is then also a least element of S.

(W2) If $\alpha \in \mathbf{Ord}$, then $S_\alpha(\mathbf{Ord}) = \{\gamma \in \mathbf{Ord} : \gamma < \alpha\} = \alpha$ is a set. ∎

Corollary 3.8. **Ord** *is a proper class.*

Proof. If **Ord** were a set, it would itself be an ordinal. But then we would have $\mathbf{Ord} \in \mathbf{Ord}$, contradicting Exercise 3.5. ∎

Exercise 3.7 (important)**.** Show that a downward closed set of ordinals is itself an ordinal.

Exercise 3.8. Show that if $\alpha \in \mathbf{Ord}$, then there is no ordinal β with $\alpha < \beta < \alpha + 1$, i.e., $\alpha + 1$ is the least ordinal greater than α.

A ordinal α is a **successor** if $\alpha = \beta + 1$ for some $\beta \in \mathbf{Ord}$. An ordinal α is a **limit** if $\alpha \neq 0$ and α is not a successor.

Exercise 3.9. Show that every positive natural number is a successor.

Exercise 3.10. Show that ω is a limit.

Exercise 3.11. Show that $\alpha \in \mathbf{Ord}$ is a successor if and only if there exists a largest ordinal $\beta < \alpha$, in which case $\alpha = \beta + 1$.

Exercise 3.12. Show that a positive ordinal α is a limit if and only if $\alpha = \bigcup \alpha$ (i.e., $\alpha = \bigcup_{\gamma < \alpha} \gamma$).

3.3. Transfinite recursion

Let $\mathcal{E}$ be a class function ("$\mathcal{E}$" for "extension"). A (set) function f is $\mathcal{E}$-**inductive** if:

(I1) the domain of f is an ordinal $\alpha := \mathrm{dom}(f)$;

(I2) for all $\beta < \alpha$, we have $f(\beta) = \mathcal{E}(f \restriction \beta)$.

As a reminder, here $f \restriction \beta$ denotes the restriction of f to all the ordinals less than β.

Lemma 3.9. *Let α be an ordinal and let $\mathcal{E}$ be a class function. If $f, g \colon \alpha \to \mathfrak{U}$ are $\mathcal{E}$-inductive functions, then $f = g$.*

Proof. Suppose $f \neq g$ and let $\beta < \alpha$ be the least ordinal such that $f(\beta) \neq g(\beta)$. As $f(\gamma) = g(\gamma)$ for all $\gamma < \beta$, we have $f \restriction \beta = g \restriction \beta$. But then $f(\beta) = \mathcal{H}(f \restriction \beta) = \mathcal{H}(g \restriction \beta) = g(\beta)$; a contradiction. ∎

Theorem 3.10 (Transfinite recursion)**.** *Let $\alpha \in \mathbf{Ord}$ and let $\mathcal{E}$ be a class function such that every $\mathcal{E}$-inductive function $g \colon \gamma \to \mathfrak{U}$ whose domain is an ordinal $\gamma < \alpha$ belongs to* $\mathrm{dom}(\mathcal{E})$*. Then there is a unique $\mathcal{E}$-inductive function $f \colon \alpha \to \mathfrak{U}$.*

Technically, this is a theorem schema comprising one sentence for each class function $\mathcal{E}$.

Proof. Uniqueness follows from Lemma 3.9, so it remains to prove existence. Suppose, toward a contradiction, that there is no $\mathcal{E}$-inductive function $f \colon \alpha \to \mathfrak{U}$. We may, without loss of generality, assume that α is the least ordinal with this property; that is, for every $\gamma < \alpha$, there is a (unique) $\mathcal{E}$-inductive function $g_\gamma \colon \gamma \to \mathfrak{U}$. At this point, it is worth noting that the assignment $\alpha \to \mathfrak{U} \colon \gamma \mapsto g_\gamma$ is a class function (since the statement "x is an ordinal less than α and y is an $\mathcal{E}$-inductive function with domain x" can be expressed as a formula in the language of set theory).

Note that $\alpha > 0$, since the empty function $\varnothing \colon 0 \to \mathfrak{U}$ is $\mathcal{E}$-inductive (condition (I2) holds vacuously for this function). Hence, we have two cases to consider:

Case 1: $\alpha = \beta + 1$ *for some* $\beta \in \mathbf{Ord}$. Define $f \colon \alpha \to \mathcal{U}$ by

$$f(\gamma) := \begin{cases} g_\beta(\gamma) & \text{if } \gamma < \beta; \\ \mathcal{E}(g_\beta) & \text{if } \gamma = \beta. \end{cases}$$

Then f is an $\mathcal{E}$-inductive function with domain α (exercise!), contradicting the choice of α.

Case 2: α *is a limit ordinal.* Note that $\{g_\gamma : \gamma < \alpha\}$ is a set by Rep, and thus we can define

$$f := \bigcup \{g_\gamma : \gamma < \alpha\}.$$

Then f is again an $\mathcal{E}$-inductive function with domain α (exercise; you will need to invoke Exercise 3.12 for this), and we are done. ■

There is also a class version of this theorem:

Theorem 3.11 (Transfinite recursion, class version)**.** *Let $\mathcal{E}$ be a class function such that every $\mathcal{E}$-inductive function belongs to* $\mathrm{dom}(\mathcal{E})$*. Then there is a unique class function $\mathcal{F} \colon \mathbf{Ord} \to \mathcal{U}$ such that for all $\alpha \in \mathbf{Ord}$, the function $\mathcal{F} \restriction \alpha$ is $\mathcal{E}$-inductive.*

Proof. It follows from Theorem 3.10 that the following definition works: $\mathcal{F}(\alpha) = y$ if and only if $\alpha \in \mathbf{Ord}$ and there exists an $\mathcal{E}$-inductive function $f \colon (\alpha + 1) \to \mathcal{U}$ with $f(\alpha) = y$. ■

3.4. The von Neumann universe and the Axiom of Foundation

As a representative application of transfinite recursion, we can extend the construction from §1.9 to all ordinals by defining a class function $\mathbf{Ord} \to \mathcal{U} \colon \alpha \mapsto V_\alpha$ as follows:

$$V_\alpha := \bigcup \{\mathcal{P}(V_\gamma) : \gamma < \alpha\} = \bigcup_{\gamma < \alpha} \mathcal{P}(V_\gamma). \tag{3.1}$$

Formally, we apply Theorem 3.11 to the class function $\mathcal{E}$ given by

$$\mathcal{E}(f) := \bigcup \{\mathcal{P}(f(x)) : x \in \mathrm{dom}(f)\} \quad \text{for all functions } f.$$

It is immediate from (3.1) that $V_\gamma \subseteq V_\alpha$ when $\gamma \leqslant \alpha$. As a result, we have $V_{\beta+1} = \mathcal{P}(V_\beta)$ for all $\beta \in \mathbf{Ord}$. On the other hand, Exercise 3.12 implies that $V_\alpha = \bigcup_{\gamma<\alpha} V_\gamma$ when α is a limit ordinal. Thus, the sets V_α can be equivalently defined as follows:

$$V_\alpha := \begin{cases} \varnothing & \text{if } \alpha = 0, \\ \mathcal{P}(V_\beta) & \text{if } \alpha = \beta + 1, \\ \bigcup \{V_\gamma : \gamma < \alpha\} & \text{if } \alpha \text{ is a limit ordinal.} \end{cases} \tag{3.2}$$

(In practice, it is common to give recursive definitions that distinguish between successors and limits in this way.) The class $V := \bigcup \{V_\alpha : \alpha \in \mathbf{Ord}\}$ is called the **von Neumann universe** (named after John von Neumann). For $x \in V$, the least $\alpha \in \mathbf{Ord}$ such that $x \in V_\alpha$ is called the **rank** of x and is denoted by $\mathrm{rank}(x)$. Observe that $\mathrm{rank} \colon V \to \mathbf{Ord}$ is a class function.

Exercise 3.13. Let $x \in V$. Then the rank of x is a successor ordinal.

Exercise 3.14. Let $y \in x \in V$. Then $y \in V$ and $\mathrm{rank}(y) < \mathrm{rank}(x)$.

Exercise 3.15 (important)**.** If α is an ordinal, then $\mathrm{rank}(\alpha) = \alpha + 1$. Hence, $\mathbf{Ord} \cap V_\alpha = \alpha$. (Hint: Let α be the least ordinal such that $\mathrm{rank}(\alpha) \neq \alpha + 1$... Also, use (3.1), not (3.2).)

Proposition 3.12. *We have $x \in V$ if and only if $\forall y \in x \, (y \in V)$.*

Proof. The "only if" direction is given by Exercise 3.14. For the "if" direction, suppose that all elements of x are in V. By Replacement, $\{\mathrm{rank}(y) : y \in x\}$ is a set, so $\beta := \bigcup \{\mathrm{rank}(y) : y \in x\}$ is a downward closed set of ordinals, and hence it is itself an ordinal by Exercise 3.7. It remains to observe that for each $y \in x$, $y \in V_{\mathrm{rank}(y)} \subseteq V_\beta$, so $x \in \mathcal{P}(V_\beta) = V_{\beta+1}$, and therefore $\mathrm{rank}(x) \leqslant \beta + 1$. (In fact, $\mathrm{rank}(x) = \beta + 1$—exercise.) ■

The class V comprises sets that can be built staring from the empty set by repeatedly applying the powerset operation (where the number of repetitions is indexed by an arbitrary ordinal—so it may be very infinite). Our next axiom says that these are the only sets we care about:

Foundation (AF)

$\mathcal{U} = V$.

Note that AF can be stated as a sentence in the language of set theory, but a very complicated one: "for all x, there is an ordinal α such that $x \in V_\alpha$" relies on the definition of ordinals and the recursive definition of the sets V_α. However, it turns out that AF is equivalent to a much simpler sentence, which just says that every nonempty set is disjoint from at least one of its elements:

Theorem 3.13. *Assuming* ZF^-, *the Axiom of Foundation is equivalent to the following statement:*

$$\forall x \left(x \neq \varnothing \longrightarrow \exists y \left(y \in x \wedge x \cap y = \varnothing\right)\right). \tag{3.3}$$

PROOF. $\mathcal{U} = V \implies$ (3.3). Take $\varnothing \neq x \in V$. Consider the set $\{\mathrm{rank}(y) : y \in x\}$. (It is indeed a set by Rep.) This is a nonempty set of ordinals, so it has a least element, say α. Let y be an arbitrary element of x with $\mathrm{rank}(y) = \alpha$. We claim that $y \cap x = \varnothing$, as desired. Indeed, by the choice of α, every element of x has rank *at least* α. On the other hand, by Exercise 3.14, every element of y has rank *strictly less* than α. This means that x and y cannot have any elements in common.

(3.3) $\implies \mathcal{U} = V$. Assuming (3.3), we have to argue that every set x belongs to some V_α, $\alpha \in \mathbf{Ord}$. We first handle the case when x is a transitive set:

Lemma 3.14. *Assume* (3.3). *If x is a transitive set, then $x \in V$.*

Proof. Suppose, toward a contradiction, that $x \notin V$. By Proposition 3.12, not all elements of x are in V, i.e., the set $x' := x \backslash V$ is nonempty (it is a set by Comp). By (3.3), there is an element $y \in x'$ such that $y \cap x' = \varnothing$. Since $y \in x' \subseteq x$, we have $y \in x$, and thus, by the transitivity of x, $y \subseteq x$. As $y \cap x' = \varnothing$, we conclude that $y \subseteq x \backslash x' = x \cap V$. In other words, every element of y is in V. By Proposition 3.12 again, we see that $y \in V$. This is a contradiction as $y \in x' = x \backslash V$. ☒

To reduce to the transitive set case, we need one more lemma (which is useful in its own right):

Lemma 3.15 (Transitive closure). *For every set x, there is a transitive set y such that $x \subseteq y$.*

Proof. Define a function $\omega \to \mathcal{U} \colon n \mapsto y_n$ recursively as follows:

$$y_0 := x, \qquad y_{n+1} := \bigcup y_n.$$

This definition tacitly relies on the following result:

Exercise 3.16. Show that every nonzero $n \in \omega$ is a successor.

Let $y := \bigcup\{y_n : n \in \omega\}$. Of course, $x = y_0 \subseteq y$. Also, if $z \in y$, then $z \in y_n$ for some $n \in \omega$ and hence $z \subseteq \bigcup y_n = y_{n+1} \subseteq y$, as desired. ☒

It is not hard to see (exercise!) that the set y constructed in the above proof of Lemma 3.15 is the *smallest* transitive superset of x; that is, if $z \supseteq x$ is any transitive set, then $y \subseteq z$. This set y is called the **transitive closure** of x.

Now we can finish the proof of Theorem 3.13. Let x be any set and let y be its transitive closure. By Lemma 3.14, there is an ordinal α such that $y \subseteq V_\alpha$, and hence $x \subseteq V_\alpha$ as well. Then $x \in V_{\alpha+1}$, and we are done. ■

The axiom system $\mathsf{ZF}^- + \mathsf{AF}$ is denoted by ZF. For the remainder of this section, we will continue working in ZF^- rather than ZF, except when explicitly stated otherwise.

The Axiom of Foundation implies that no set can be its own element. Indeed, if $x \in x$, then $\{x\}$ is a nonempty set whose one element, i.e., x, satisfies $x \cap \{x\} \neq \varnothing$. (Another way to see this is by using Exercise 3.14.) More generally, we have the following:

Proposition 3.16 (ZF)**.** *There is no infinite sequence of sets such that $x_0 \ni x_1 \ni x_2 \ni \cdots$. More precisely, there is no function $x \colon \omega \to \mathcal{U}$ such that $x(n+1) \in x(n)$ for all $n \in \omega$.*

PROOF. Suppose for contradiction that such a function $x \colon \omega \to \mathcal{U}$ exists and consider the set $x[\omega] = \{x(n) \,:\, n \in \omega\}$. For any element $x(n) \in x[\omega]$, we have $x(n+1) \in x(n) \cap x[\omega]$, so $x[\omega]$ is a counterexample to (3.3). An alternative approach is to use Exercise 3.14 and observe that the set $\{\mathrm{rank}(x(n)) \,:\, n \in \omega\}$ has no least element. ∎

Exercise 3.17 (ZF). Let $\mathcal{C}$ be a class such that for all sets x, if every element of x is in $\mathcal{C}$, then x is in $\mathcal{C}$ as well. Show that $\mathcal{C} = \mathcal{U}$.

The following consequence of AF is occasionally useful:

Lemma 3.17 (ZF; subset choice)**.** *Let X be a set and let $\mathcal{R}$ be a class of ordered pairs such that for each $x \in X$, the class $\mathcal{R}_x := \{y \,:\, (x, y) \in \mathcal{R}\}$ is nonempty. Then there is a function $f \colon X \to \mathcal{U}$ such that for each $x \in X$, $f(x)$ is a nonempty subset of $\mathcal{R}_x$.*

PROOF. For each $x \in X$, let $\alpha(x)$ be the least ordinal in the (nonempty) class $\{\mathrm{rank}(y) \,:\, y \in \mathcal{R}_x\}$. Since each V_α is a *set*, the function f given by $f(x) := V_{\alpha(x)} \cap \mathcal{R}_x$ has the desired properties. ∎

3.5. Ordinals as isomorphism types of well-orderings

Theorem 3.18 (Well-ordered sets)**.** *Let $(A, \prec)$ be a well-ordered set. Then there exists a unique ordinal α that is order-isomorphic to $(A, \prec)$. Furthermore, the isomorphism $f \colon \alpha \to A$ is unique.*

The unique ordinal α that is order-isomorphic to a well-ordered set $(A, \prec)$ is called the **order-type**, or simply the **type**, of $(A, \prec)$, and is denoted by $\mathrm{type}(A, \prec)$ or just $\mathrm{type}(\prec)$.

PROOF. The uniqueness part is left as an exercise. We will establish the existence. Let $(A, \prec)$ be a well-ordered set. The idea is to define f recursively as follows:

$$f(\beta) \;:=\; \min(A \backslash f[\beta]) \qquad (\text{assuming } f[\beta] \neq A).$$

Recall that $f[\beta]$ here stands for the image of the set $\beta = \{\gamma \in \mathbf{Ord} \,:\, \gamma < \beta\}$ under f; that is,

$$f[\beta] \;=\; \{f(\gamma) \,:\, \gamma < \beta\}.$$

In other words, we let $f(\beta)$ be the $\prec$-least element of A that comes after all $f(\gamma)$'s with $\gamma < \beta$. If at some point we reach a stage where $f[\beta] = A$, then f yields a desired order-isomorphism between β and A. Otherwise, f will be defined on all ordinals, i.e., it will be an injective—in fact, strictly increasing—class function from $\mathbf{Ord}$ to A, which is impossible.

To make this argument rigorous, suppose, toward a contradiction, that $(A, \prec)$ is not isomorphic to any ordinal. Let $\mathcal{E}$ be the class function such that

$$\mathcal{E}(f) = y \quad :\Longleftrightarrow \quad \mathrm{ran}(f) \subsetneq A \text{ and } y = \min(A \backslash \mathrm{ran}(f)).$$

By definition, a function $f \colon \alpha \to \mathcal{U}$ is $\mathcal{E}$-inductive if for all $\beta < \alpha$, we have

$$f(\beta) \;=\; \mathcal{E}(f \restriction \beta) \;=\; \min(A \backslash \mathrm{ran}(f \restriction \beta)) \;=\; \min(A \backslash f[\beta]).$$

To apply transfinite recursion, we have to verify the assumptions of Theorem 3.11; that is, we need to show that every $\mathcal{E}$-inductive function belongs to $\mathrm{dom}(\mathcal{E})$.

Claim 3.19. *Let $f \colon \alpha \to \mathcal{U}$ be an $\mathcal{E}$-inductive function. Then:*

(*a*) $\mathrm{ran}(f) \subseteq A$,

(*b*) *f is injective,*

(c) *f is strictly increasing,*

(d) $\operatorname{ran}(f) \neq A$, *and*

(e) $f \in \operatorname{dom}(\mathcal{E})$.

Proof. (a) Since f is $\mathcal{E}$-inductive, we have $f(\beta) = \min(A \backslash f[\beta]) \in A$ for all $\beta < \alpha$.

(v) Let γ, $\beta < \alpha$ be distinct. Without loss of generality, we may assume that $\gamma < \beta$. Then $\gamma \in \beta$, and so $f(\gamma) \in f[\beta]$. On the other hand, $f(\beta) = \min(A \backslash f[\beta]) \notin f[\beta]$. Hence, $f(\gamma) \neq f(\beta)$.

(c) Suppose that $\gamma < \beta < \alpha$. Then $\gamma \subseteq \beta$, so $A \backslash f[\gamma] \supseteq A \backslash f[\beta]$, and hence

$$f(\gamma) \;=\; \min(A \backslash f[\gamma]) \;\leqslant\; \min(A \backslash f[\beta]) \;=\; f(\beta).$$

Since f is injective, $f(\gamma) \neq f(\beta)$, and so $f(\gamma) < f(\beta)$, as desired.

(d) If $\operatorname{ran}(f)$ were equal to A, then $f \colon \alpha \to A$ would be a strictly increasing bijection, i.e., an order-isomorphism. But we have assumed that $(A, \prec)$ is not isomorphic to any ordinal.

(e) The domain of $\mathcal{E}$ consists precisely of functions whose image is a strict subset of A, and we have $\operatorname{ran}(f) \subsetneq A$ by (a) and (d). ☒

Now we can apply Theorem 3.11 to conclude that there exists a class function $\mathcal{F} \colon \mathbf{Ord} \to \mathcal{U}$ such that for each ordinal α, the function $\mathcal{F} \restriction \alpha$ is $\mathcal{E}$-inductive. But then $\mathcal{F}$ is an injective (in fact, strictly increasing) class function from **Ord** to A, which is a contradiction. ■

Theorem 3.20 (Well-ordered classes)**.** *Let $(\mathcal{C}, \prec)$ be a well-ordered proper class. Then there is a unique order-isomorphism $\Phi \colon \mathbf{Ord} \to \mathcal{C}$ (i.e., a bijective strictly increasing class function).*

Exercise 3.18. Prove Theorem 3.20. Hint: You will have to use (W2).

4. Introduction to the Axiom of Choice

In this section, we continue working in a universe $\mathcal{U}$ that satisfies the axiom system ZF^-. (The results that additionally rely on the Axiom of Foundation will be explicitly marked as such.)

4.1. Choice functions

A **choice function** for a set X is a mapping $\mathsf{choice}\colon X \to \bigcup X$ such that $\mathsf{choice}(x) \in x$ for all $x \in X$. An obvious necessary requirement for X to have a choice function is that $\varnothing \notin X$.

Example 4.1. Suppose that $X = \{x\}$, where $x \neq \varnothing$. Then there is a choice function for X. Indeed, since $x \neq \varnothing$, there is an element $y \in x$. Using the Pairing Axiom a few times, we prove the existence of the ordered pair (x, y) (Proposition 1.9). Using Pair once more, we see that there exists the set $f := \{(x, y)\}$. It remains to observe that f is a choice function for X.

Example 4.2. Now let $X = \{x_1, x_2, x_3\}$, where x_1, x_2, x_3 are distinct and nonempty. We claim that X has a choice function. Indeed, let $y_1 \in x_1$, $y_2 \in x_2$, $y_3 \in x_3$ be arbitrary elements (which exist since the x_i's are nonempty). By Proposition 1.9, there are ordered pairs (x_1, y_1), (x_2, y_2), and (x_3, y_3). Then, using Pair and Union, we establish the existence of the set

$$f := \{(x_1, y_1), (x_2, y_2), (x_3, y_3)\},$$

which is a desired choice function for X. A similar argument would work for, say $X = \{x_1, x_2, \ldots, x_{100}\}$, except that Pair and Union will need to be applied more times.

The above examples can be generalized as follows:

Definition 4.3 (Finite and infinite sets)**.** A set X is **finite** if there is a bijection $n \to X$ for some $n \in \omega$. Otherwise, X is **infinite**.

Exercise 4.1 (surprisingly challenging)**.** Show that ω is infinite.

Proposition 4.4 (Finite choice: only assuming ZF^-)**.** *Let X be a finite set such that $\varnothing \notin X$. Then there is a choice function for X.*

Proof. We proceed by induction on the natural number n such that there is a bijection $n \to X$ (which is the only approach we *can* use since that's how ω is defined). That is, we argue that

$$\mathcal{C} := \big\{ n \in \omega \,:\, \forall X \,\big((\varnothing \notin X \wedge \exists \text{ a bijection } n \to X) \longrightarrow \exists \text{ a choice function for } X\big)\big\}.$$

is an inductive set. Clearly, $0 \in \mathcal{C}$ (as $\varnothing$ is a choice function for $\varnothing$). Now suppose that $n \in \mathcal{C}$ and consider any set X such that $\varnothing \notin X$ and there is a bijection $x\colon (n+1) \to X$, i.e.,

$$X = \{x(0), x(1), \ldots, x(n)\}.$$

Let $X' := \{x(i) : i < n\}$ (or, more concisely, $X' = x[n]$). Since $n \in \mathcal{C}$ by assumption and $x{\restriction}n$ is a bijection from n to X', the set X' has a choice function f'. As the set $x(n)$ is nonempty, there is an element $y \in x(n)$. Now we use Pair and Union to define

$$f := f' \cup \{(x(n), y)\}.$$

By construction, f is a choice function for X. This shows that $n + 1 \in \mathcal{C}$, as desired. ■

Exercise 4.2. Where does the above inductive argument break down if there is a bijection $\omega \to X$?

Even if X is infinite, it may be possible to construct a choice function for X using only the axioms of ZF. For example, suppose that $X = \mathcal{P}(\omega) \setminus \{\varnothing\}$, the set of all nonempty subsets of ω. Then X has a choice function, namely the mapping $f\colon X \to \omega$ given by

$$f(x) := \min x.$$

On the other hand, can you find a choice function for $X = \mathcal{P}(\mathcal{P}(\omega))\backslash\{\varnothing\}$ (or, what's essentially the same[iii], $X = \mathcal{P}(\mathbb{R})\backslash\{\varnothing\}$)? It turns out that this challenge requires the use of an additional axiom, namely the famous—or rather infamous—**Axiom of Choice**:

Choice (AC)

If X is a set such that $\varnothing \notin X$, then there is a choice function for X. In symbols,

$$\forall X \left(\varnothing \notin X \longrightarrow \exists f \left(f \text{ is a function} \wedge \operatorname{dom}(f) = X \wedge \forall x \in X (f(x) \in x)\right)\right).$$

The axiom system ZF + AC is denoted by ZFC. It is the generally accepted axiom system in mathematics (meaning that if someone claims to prove a theorem without specifying the axioms explicitly, they are most likely working in ZFC). We also write ZFC^- for ZF^- + AC (i.e., ZFC without the Axiom of Foundation). The odium traditionally directed at AC is an outcome of its "non-constructive" nature: in contrast to the axioms (Pair, Pow, Comp, etc.) that provide conditions under which some specific classes must be sets, AC asserts that a set with certain properties—namely, a choice function—exists without first describing it as a class. As a result, while we know that a choice function for, say, $\mathcal{P}(\mathcal{P}(\omega))\backslash\{\varnothing\}$ *exists*, we don't know *what it is* or how to compute it.

It is important to keep in mind that the existence of a choice function for a particular set X does not always depend on the Axiom of Choice (for example, see Proposition 4.4). More generally, despite its name, the Axiom of Choice does not need to be invoked every time a mathematician says something like "choose x so that..." (most of the time, this is just an application of the definition of a nonempty set).

4.2. Recursion and choice

The Axiom of Choice often makes recursive definitions easier, as it allows making arbitrary choices on each step of the construction. The next result is an instance of this phenomenon:

Proposition 4.5 (ZFC^-). *If X is an infinite set, then there is an injection $\omega \to X$.*

Proof. We wish to define a function $f\colon \omega \to X$ recursively by letting $f(n)$ be an arbitrary element of X distinct from $f(0)$, $f(1)$, ..., $f(n-1)$; such an element must exist because X is infinite. In other words, we wish to use a recursive definition of the following form:

$$f(n) := \text{an arbitrary element of } X\backslash f[n]. \tag{4.1}$$

(Recall that $f[n] = \{f(0), f(1), \ldots, f(n-1)\}$.) The issue is that (4.1) does not fit into the framework of Theorem 3.10 because its right-hand side is not of the form $\mathcal{E}(f{\restriction}n)$ for some class function $\mathcal{E}$. This is where the Axiom of Choice comes in handy: We fix a choice function $\mathsf{choice}\colon \mathcal{P}(X)\backslash\{\varnothing\} \to X$ for the family of all nonempty subsets of X and define $f\colon \omega \to X$ by

$$f(n) := \mathsf{choice}(X\backslash f[n]).$$

Formally, we apply Theorem 3.10 to $\alpha = \omega$ and the class function $\mathcal{E}$ given by

$$\mathcal{E}(g) = y \quad :\Longleftrightarrow \quad \operatorname{ran}(g) \subsetneq X \text{ and } y = \mathsf{choice}(X\backslash\operatorname{ran}(g)).$$

Note that the formula with two free variables g and y that defines the class function $\mathcal{E}$ uses both X and choice as parameters. (Writing this formula out in detail is a valuable exercise.)

We now check the assumptions of Theorem 3.10. By definition, if $n \in \omega$ and a function $g\colon n \to \mathcal{U}$ is $\mathcal{E}$-inductive, then $g(i) = \mathsf{choice}(X\backslash g[i])$ for all $i < n$. Therefore, if $j < i < n$, then $g(j) \in g[i]$ and $g(i) \in X\backslash g[i]$, and hence $g(j) \neq g(i)$, so $g\colon n \to X$ is injective. As X is infinite, g cannot be surjective. We conclude that $\operatorname{ran}(g) \subsetneq X$ and $g \in \operatorname{dom}(\mathcal{E})$. Thus, Theorem 3.10 can be applied to obtain an $\mathcal{E}$-inductive function $f\colon \omega \to X$, which is injective, as desired. ∎

[iii] In set theory, it is common to refer to the subsets of ω as "the reals."

We remark that Proposition 4.5 cannot be proved from ZF alone (assuming ZF is consistent, i.e., the axioms are not contradictory).

Exercise 4.3. Show, without using AC, that if A is an infinite set, then for every $n \in \omega$, there is an injection $n \to A$. (Hint: induction on n.)

Exercise 4.4. Assuming ZFC^-, show that AF is equivalent to the statement that there is no function $x \colon \omega \to \mathcal{U}$ with $x(n+1) \in x(n)$ for all $n \in \omega$. (One direction is given by Proposition 3.16.)

4.3. The Well-Ordering Theorem

By extending the construction in the proof of Proposition 4.5, we arrive at the following result, known as the **Well-Ordering Theorem**:

Theorem 4.6 (Zermelo)**.** *Assuming ZF^-, the following statements are equivalent:*

(1) *the Axiom of Choice,*
(2) *for every set A, there is a well-ordering $\prec$ on A,*
(3) *for every set A, there is an ordinal α and a bijection $\alpha \to A$.*

The fact that every set can be well-ordered is one of the less intuitive consequences of AC. For example, how would you well-order the set $\mathcal{P}(\omega)$ (or the real numbers)?

Proof. First we note the equivalence (ii) $\iff$ (3). Indeed, if $\prec$ is a well-ordering on A, then A is in a bijection with the ordinal $\mathrm{type}(A, \prec)$ by Theorem 3.18. Conversely, if $f \colon A \to \alpha \in \mathbf{Ord}$ is a bijection, then the relation $\prec$ on A given by

$$x \prec y \quad :\iff \quad f(x) < f(y)$$

is a well-ordering. The implication (ii) $\Longrightarrow$ (1) is also clear. Indeed, suppose (ii) holds and let X be a set with $\varnothing \notin X$. Fix any well-ordering $\prec$ on $\bigcup X$ and define $\mathsf{choice} \colon X \to \bigcup X$ by

$$\mathsf{choice}(x) := \min x.$$

Clearly, choice is a choice function for X.

It remains to establish the implication (1) $\Longrightarrow$ (3). Here the argument almost verbatim repeats the proof of Theorem 3.18, but instead of using a well-ordering to pick the least element of $A \setminus f[\beta]$ on each step, we use a choice function provided by AC (this is also very similar to the approach we employed in the proof of Proposition 4.5). Specifically, let A be a set and suppose for contradiction that there is no bijection between A and any ordinal. Fix a choice function $\mathsf{choice} \colon \mathcal{P}(A) \setminus \{\varnothing\} \to A$ for the family of all nonempty subsets of A. We will use Theorem 3.11 to define an injective class function $\mathcal{F} \colon \mathbf{Ord} \to A$ via the following recursive formula:

$$\mathcal{F}(\beta) := \mathsf{choice}(A \setminus \mathcal{F}[\beta]).$$

More precisely, let $\mathcal{E}$ be the class function given by

$$\mathcal{E}(g) = y \quad :\iff \quad \mathrm{ran}(g) \subsetneq A \text{ and } y = \mathsf{choice}(A \setminus \mathrm{ran}(g)).$$

By definition, a function $f \colon \alpha \to \mathcal{U}$ is $\mathcal{E}$-inductive if for all $\beta < \alpha$, we have $f(\beta) = \mathsf{choice}(A \setminus f[\beta])$. An argument analogous to the one in the proof of Proposition 4.5 shows that such f is an injective, but not surjective, function from α to A. Thus, we can apply Theorem 3.11 to obtain an injective class function $\mathcal{F} \colon \mathbf{Ord} \to A$, which is a contradiction. The details are left as an exercise. ■

5. Problem set 2

The default axiom system for the following exercises is ZF^-.

Exercise 5.1.

(*a*) Let $\alpha, \beta \in \mathbf{Ord}$ and let $f : \alpha \to \beta$ be a strictly increasing function. Show that $\gamma \leqslant f(\gamma)$ for all $\gamma < \alpha$ and deduce that $\alpha \leqslant \beta$.

(*b*) Show that if two ordinals α, β are order-isomorphic, then $\alpha = \beta$ and the only isomorphism from α to β is the identity map.

Exercise 5.2. Let X be a set of ordinals.

(*a*) Show that the class $X^{\uparrow} := \{\alpha \in \mathbf{Ord} : \forall \beta \in X\, (\beta \leqslant \alpha)\}$ is nonempty.

Since $X^{\uparrow}$ is a nonempty class of ordinals, $X^{\uparrow}$ has a least element. The least element of $X^{\uparrow}$ is called the **supremum** of X and is denoted by $\sup X$. To wit, the supremum of X is the least ordinal greater than or equal to every element of X.

(*b*) Show that $\bigcup X$ is an ordinal.

(*c*) Conclude that $\sup X = \bigcup X$.

Exercise 5.3 (part (*a*) is basically Exercise 3.12 in the main text)**.**

(*a*) Let α be a nonzero ordinal. Show that α is a limit if and only if $\alpha = \sup \alpha$.

(*b*) Let X be a nonempty set of ordinals. Show that if $\sup X \notin X$, then $\sup X$ is a limit.

Exercise 5.4. Let $\Phi : \mathbf{Ord} \to \mathbf{Ord}$ be a class function with the following properties:

- for all $\alpha, \beta \in \mathbf{Ord}$, if $\alpha \leqslant \beta$, then $\Phi(\alpha) \leqslant \Phi(\beta)$,
- if α is a limit ordinal, then $\Phi(\alpha) = \sup\{\Phi(\gamma) : \gamma < \alpha\}$.

Show that Φ has a **fixed point**, i.e., an ordinal α such that $\Phi(\alpha) = \alpha$.

Exercise 5.5 (part (*a*) is Exercise 1.23 in the main text)**.**

(*a*) Show that there is no set-to-one class function from a proper class to a set. (A class function Φ is **set-to-one** if for all y, the class $\{x : \Phi(x) = y\}$ is a set.)

(*b*) Assuming AF, show that a class $\mathcal{C}$ is proper if and only if there is a surjective class function from $\mathcal{C}$ to $\mathbf{Ord}$.

Exercise 5.6. Assuming ZF, prove that the Axiom of Choice is equivalent to the following statement:

For every set X and every proper class $\mathcal{C}$, there exists an injection $f : X \to \mathcal{C}$.

6. Cardinality

6.1. Comparing sizes of sets

In this section we continue working in the axiom system ZF^-, unless explicitly stated otherwise. Given sets A, B, we write $A \lesssim B$ to mean that there is an injection $A \to B$ and $A \approx B$ to mean that there is a bijection $A \to B$ (in which case we say that A and B are **equinumerous**). Intuitively, $A \approx B$ if A and B have "the same number" of elements, while $A \lesssim B$ if A has "not more" elements than B. The following properties of the relations $\lesssim$ and $\approx$ are immediate:

Exercise 6.1. Prove that for all sets A, B, C:

- $A \approx A$,
- $A \subseteq B$ implies $A \lesssim B$,
- $A \approx B$ implies $B \approx A$,
- $A \lesssim B \lesssim C$ implies $A \lesssim C$,
- $A \approx B \approx C$ implies $A \approx C$.

Note also that $A \lesssim B$ if and only if A is equinumerous with a subset of B.

Definition 6.1 (Finite, infinite, countable, uncountable)**.** Recall from Definition 4.3 that a set X is **finite** if $X \approx n$ for some $n \in \omega$, and otherwise X is **infinite**. A set X is called **countable** if $X \lesssim \omega$ (note that finite sets are countable); otherwise, X is **uncountable**.

Note that, although $X \approx X$ for every set X, an injective function $f\colon X \to X$ may fail to be bijective. For example, the map $f\colon \omega \to \omega$ given by $f(n) := n + 1$ is injective but not surjective.

Definition 6.2 (Dedekind-finite and Dedekind-infinite)**.** A set X is called **Dedekind-finite** if every injective function $X \to X$ is surjective, and **Dedekind-infinite** otherwise.

By Proposition 4.5, if AC holds, then a set is Dedekind-infinite if and only if it is infinite. In general, we have the following:

Exercise 6.2. Prove (without using AC) that the following statements are equivalent for any set X:

(1) X is Dedekind-infinite,

(2) $\omega \lesssim X$.

Next we establish an important property of the relations $\lesssim$ and $\approx$:

Theorem 6.3 (Cantor/Schröder–Bernstein)**.** *For any sets A, B,*

$$A \approx B \quad \Longleftrightarrow \quad A \lesssim B \text{ and } B \lesssim A.$$

Proof. The ($\Longrightarrow$) direction is an easy exercise. Now we need to prove that if $A \lesssim B$ and $B \lesssim A$, then $A \approx B$. To this end, suppose that $f\colon A \to B$ and $g\colon B \to A$ are injections. We recursively define sets A_n and B_n for all $n \in \omega$ as follows:

$$A_0 := A \setminus \operatorname{ran}(g), \quad B_n := f[A_n], \quad A_{n+1} := g[B_n], \qquad \text{and let } A' := \bigcup_{n\in\omega} A_n,\ B' := \bigcup_{n\in\omega} B_n.$$

Since $B_n = f[A_n]$ for all $n \in \omega$, $B' = f[A']$ and hence $f{\restriction}A'$ is a bijection from A' to B'. Consider the sets $A'' := A \setminus A'$ and $B'' := B \setminus B'$. It is a routine exercise to check that $g{\restriction}B''$ is a bijection from B'' to A''. Therefore, the following function $h\colon A \to B$ is a desired bijection between A and B:

$$h(a) := \begin{cases} f(a) & \text{if } a \in A', \\ g^{-1}(a) & \text{if } a \in A''. \end{cases}$$

We emphasize that this proof is performed in ZF^- (in particular, it does not require AC). ■

6.2. There is always a bigger set

Is there a "largest" set? The following classical result of Cantor says "no":

Theorem 6.4 (Cantor)**.** *For every set X, we have $X \lesssim \mathcal{P}(X)$ but $\mathcal{P}(X) \not\lesssim X$.*

Moreover, there is a class function Cantor *defined by a formula without parameters such that, given any set X and a function $f\colon X \to \mathcal{P}(X)$, we have*

$$\mathsf{Cantor}(X, f) \in \mathcal{P}(X) \backslash \operatorname{ran}(f)$$

(*in other words,* $\mathsf{Cantor}(X, f)$ *witnesses that f is not surjective*).

Proof. Clearly, $X \lesssim \mathcal{P}(X)$ via the function $x \mapsto \{x\}$. We shall now verify the "moreover" part of the statement, from which it follows that there is no surjective function $X \to \mathcal{P}(X)$ and thus, in particular, $X \not\approx \mathcal{P}(X)$. Since $X \lesssim \mathcal{P}(X)$, this implies that $\mathcal{P}(X) \not\lesssim X$ by the Cantor/Schröder–Bernstein Theorem 6.3 (see also Exercise 6.3).

Given a set X and a function $f\colon X \to \mathcal{P}(X)$, we define

$$\mathsf{Cantor}(X, f) := \{x \in X : x \notin f(x)\}.$$

Clearly, Cantor is a class function defined by a formula without parameters, and $\mathsf{Cantor}(X, f) \subseteq X$. It remains to show $\mathsf{Cantor}(X, f) \notin \operatorname{ran}(f)$. For brevity, let $A := \mathsf{Cantor}(X, f)$ and suppose, toward a contradiction, that $A = f(x)$ for some $x \in X$. Now we ask: *Is x an element of A?* (This is very reminiscent of Russell's paradox.) Consider the two cases:

- If $x \in A$, then, by the definition of A, we have $x \notin f(x) = A$, which is a contradiction.
- On the other hand, if $x \notin A$, then $x \notin f(x)$ (because $f(x) = A$), and hence, by the definition of A, $x \in A$, which is again a contradiction.

Since we arrive at a contradiction in both cases, it follows that no such x exists, i.e., $A \notin \operatorname{ran}(f)$. ∎

Exercise 6.3. Show that if $\varnothing \neq A \lesssim B$, then there is a surjective function $B \to A$.

Exercise 6.4 (ZFC^-)**.** Show that if there is a surjective function $B \to A$, then $A \lesssim B$. (It is an open problem whether this statement is equivalent to AC!)

Theorem 6.5 (Hartogs)**.** *For every set X, there is $\alpha \in \mathbf{Ord}$ such that $\alpha \not\lesssim X$.*

Proof. This result has an easy proof assuming AC. Indeed, if AC holds, then, by Theorem 4.6, $\mathcal{P}(X) \approx \alpha$ for some ordinal α, and $\alpha \not\lesssim X$ by Theorem 6.4. What's remarkable, however, is that Hartogs' theorem can also be proved without relying on AC. In particular, the set X may not be *equinumerous* with any ordinal, yet there still must exist an ordinal that doesn't inject into it.

For a choiceless proof of Hartogs' theorem, consider the following class:

$$S := \{\alpha \in \mathbf{Ord} : \alpha \lesssim X\}. \tag{6.1}$$

It suffices to show that S is a set, since then S cannot be equal to $\mathbf{Ord}$. To this end, we can use Theorem 3.18: Every injection $f\colon \alpha \to X$ gives rise to a well-ordering on $\operatorname{ran}(f) \subseteq X$ of type α; conversely, for any well-ordering $\prec$ on a subset $Y \subseteq X$, there is a bijection $\operatorname{type}(\prec) \to Y$, and hence $\operatorname{type}(\prec) \in S$. To summarize,

$$S = \{\operatorname{type}(\prec) : \prec \text{ is a well-ordering on a subset of } X\}.$$

Now, every well-ordering on a subset of X is itself a subset of $X \times X$; hence

$$W = \{\prec : \prec \text{ is a well-ordering on a subset of } X\} \subseteq \mathcal{P}(X \times X)$$

is a set by Comp. Therefore, $S = \{\operatorname{type}(\prec) : \prec \in W\}$ is also a set by Rep, and we are done. ∎

Exercise 6.5. Let X be a set and let S be given by (6.1). Show that this set S actually *is* the least ordinal such that there is no injection $S \to X$.

From Theorem 6.5, we can deduce another formulation of AC, which very clearly demonstrates its role in the structure of the universe of sets:

Theorem 6.6. *Assuming* ZF^-, *the following statements are equivalent:*

(1) *the Axiom of Choice;*

(2) *for each pair of sets* A, B, *we have* $A \lesssim B$ *or* $B \lesssim A$ (*or both*).

PROOF. (1) $\Longrightarrow$ (2). Assume AC and let A and B be sets. By Theorem 4.6, there exist ordinals α and β such that $A \approx \alpha$ and $B \approx \beta$. Without loss of generality, say $\alpha \leqslant \beta$. Then $A \approx \alpha \subseteq \beta \approx B$, and hence $A \lesssim B$.

(2) $\Longrightarrow$ (1). Assume (2). We will show that every set can be well-ordered. Indeed, take a set X. By Hartogs' theorem, there is an ordinal α such that $\alpha \not\lesssim X$. By (2), this means that $X \lesssim \alpha$, i.e., there is an injection $f \colon X \to \alpha$. Then the relation $\prec$ on X given by $x \prec y :\Longleftrightarrow f(x) < f(y)$ is a well-ordering, and we are done. ■

6.3. Cardinals

A set X is **well-orderable** if there exists a well-ordering on X. (By Theorem 4.6, AC is equivalent to the assertion that every set is well-orderable.) It follows from Theorem 3.18 that X is well-orderable if and only if X is equinumerous with some ordinal. Thus, we may define the **cardinality** $|X|$ of a well-orderable set X as follows:

$$|X| \;\coloneqq\; \min\{\alpha \in \mathbf{Ord} \;:\; X \approx \alpha\}.$$

By definition, $X \approx |X|$. It is important to keep in mind that the notation $|X|$ is only defined for well-orderable sets X. That being said, assuming AC, every set has a well-defined cardinality.

Note that every ordinal is, by definition, well-orderable, and hence it has a well-defined cardinality. An ordinal κ is called a **cardinal** if there is no bijection from κ to a strictly smaller ordinal. In other words, $\kappa \in \mathbf{Ord}$ is a cardinal if and only if $\kappa = |\kappa|$. The class of all cardinals is denoted **Card**.

Proposition 6.7. *If* $\kappa \in \mathbf{Card}$, $\gamma \in \mathbf{Ord}$, *and* $\kappa \lesssim \gamma$, *then* $\kappa \leqslant \gamma$.

PROOF. Suppose for contradiction that $\gamma < \kappa$. Then $\gamma \subset \kappa$ and thus $\gamma \lesssim \kappa$. By the Cantor/Schröder–Bernstein theorem, we must have $\kappa \approx \gamma$, which is impossible as $\gamma < \kappa$ and κ is a cardinal.

An alternative proof that avoids the Cantor/Schröder–Bernstein theorem proceeds as follows. Suppose $f \colon \kappa \to \gamma$ is an injection from a cardinal κ to an ordinal γ. The set $\mathrm{ran}(f) \subseteq \gamma$ is well-ordered by the usual ordering on the ordinals (i.e., the membership relation), so, by Theorem 3.18, there exists an order-isomorphism $h \colon \delta \to \mathrm{ran}(f)$ for some ordinal δ. Since h is a strictly increasing map from δ to γ, it follows that $\delta \leqslant \gamma$ (see Exercise 5.1). But the composition $h^{-1} \circ f \colon \kappa \to \delta$ is a bijection from κ to δ, which is only possible if $\delta \geqslant \kappa$ as κ is a cardinal. Therefore, $\gamma \geqslant \delta \geqslant \kappa$, as desired. ■

If X is a well-orderable set, then $|X|$ must be a cardinal. Thanks to Proposition 6.7, comparing sizes of well-orderable sets turns into comparing their cardinalities in the usual ordering on **Ord**:

Proposition 6.8. *If* A, B *are well-orderable sets, then*

- $A \approx B \iff |A| = |B|$,
- $A \lesssim B \iff |A| \leqslant |B|$.

PROOF. Immediate from Proposition 6.7. ■

The notion of cardinality, when it is available, makes many arguments musch easier. For example, here's a proof of the Cantor/Schröder–Bernstein theorem assuming AC:

PROOF *of Theorem 6.3 assuming* AC. Suppose $A \lesssim B$ and $B \lesssim A$. Assuming AC, this is equivalent to $|A| \leqslant |B|$ and $|B| \leqslant |A|$, which implies $|A| = |B|$, i.e., $A \approx B$, as desired. ■

Note that every ordinal α satisfies $|\alpha| \leqslant \alpha$. Also, if $\kappa \in \mathbf{Card}$, then

$$\kappa \;=\; \underbrace{\{\alpha \in \mathbf{Ord} \,:\, \alpha < \kappa\}}_{\text{this is true whenever } \kappa \in \mathbf{Ord}} \;=\; \{\alpha \in \mathbf{Ord} \,:\, |\alpha| < \kappa\}. \tag{6.2}$$

The next results give some examples of cardinals.

Theorem 6.9. *Every natural number is a cardinal.*

Proof. We need to show that if $n < m < \omega$, then $m \not\approx n$. To this end, it suffices to argue that $n + 1 \nleqslant n$, i.e., there is no injective function $(n + 1) \to n$. We proceed by induction on n.

First, we note that there is no injective function $1 \to 0$, as there is in fact no function $1 \to 0$ at all (it is impossible to have a function from a nonempty set to $\varnothing$).

Now suppose that $n + 1 \nleqslant n$ for some $n < \omega$. Our goal is to show that $n + 2 \nleqslant n + 1$ (where $n + 2$ means $(n+1)+1$, of course). Suppose, toward a contradiction, that $f\colon (n+2) \to (n+1)$ is an injection and consider two cases depending on whether n is in the set $f[n + 1] = \{f(0), f(1), \ldots, f(n)\}$.

Case 1: $n \notin f[n + 1]$. Then for all $i \leqslant n$, we have $f(i) < n$. That is, $f{\restriction}(n + 1)$ is an injection from $n + 1$ to n, which cannot exist by the inductive hypothesis.

Case 2: $n \in f[n + 1]$. This means that $f(i) = n$ for some $i \leqslant n$, and thus $j := f(n + 1) < n$. But then the following map $g\colon (n + 1) \to n$ is an injection:

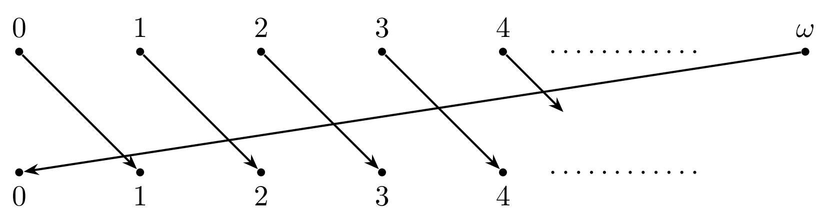
$$g(k) \;:=\; \begin{cases} j & \text{if } k = i, \\ f(k) & \text{if } k \neq i. \end{cases}$$

Thus, we arrive at a contradiction in both cases, completing the proof. ■

Corollary 6.10. *ω is a cardinal.*

Proof. Otherwise we would have $n + 1 \subset \omega \approx n$ for some $n < \omega$, contradicting Theorem 6.9. ■

On the other hand, $\omega + 1$ is not a cardinal, as we have $\omega + 1 \approx \omega$:



More generally, an infinite cardinal cannot be of the form $\beta + 1$ for any ordinal β:

Proposition 6.11. *Every infinite cardinal is a limit ordinal.*

Proof. We argue that an infinite successor ordinal is not a cardinal. If $\beta + 1$ is infinite, then $\beta \geqslant \omega$. We claim that then $\beta + 1 \approx \beta$. Indeed, the following map $f\colon (\beta + 1) \to \beta$ is a bijection:

$$f(\gamma) \;:=\; \begin{cases} \gamma + 1 & \text{if } \gamma < \omega, \\ \gamma & \text{if } \omega \leqslant \gamma < \beta, \\ 0 & \text{if } \gamma = \beta. \end{cases}$$

Therefore, $\beta + 1$ is not a cardinal. ■

Nevertheless, for each ordinal α there is a cardinal $\kappa > \alpha$. Indeed, by Hartogs' Theorem 6.5, there is an ordinal β such that $\beta \nleqslant \alpha$, which is equivalent to $|\beta| > \alpha$. It follows that $\mathbf{Card}$ is a proper class (exercise!). We emphasize that this argument does not use AC. For each cardinal κ, its **cardinal successor**, denoted by κ^+, is the least $\lambda \in \mathbf{Card}$ such that $\kappa < \lambda$.

Example 6.12. We have $0^+ = 1$, $1^+ = 2$, and, more generally, $n^+ = n + 1$ for all $n < \omega$. On the other hand, by Proposition 6.11, if κ is an infinite cardinal, then $\kappa^+ > \kappa + 1$.

Consider the class $\mathbf{Card} \setminus \omega$ of all infinite cardinals. It is a proper subclass of **Ord**, and as such it is well-ordered (by the usual ordering on the ordinals). By Theorem 3.20, there exists a unique order-isomorphism $\aleph \colon \mathbf{Ord} \to \mathbf{Card} \setminus \omega$ (read "aleph"), mapping each ordinal α to the corresponding infinite cardinal $\aleph_\alpha$. For instance, $\aleph_0 = \omega$ and $\aleph_1 = \omega^+$ is the least uncountable cardinal. In general, we have $\aleph_\alpha^+ = \aleph_{\alpha+1}$ for every ordinal α.

From (6.2), it follows that given $\kappa \in \mathbf{Card}$, we can define κ^+ explicitly as follows:

$$\kappa^+ \;=\; \{\alpha \in \mathbf{Ord} \,:\, |\alpha| \leqslant \kappa\}.$$

For instance, $\aleph_1$, i.e., the least uncountable cardinal, is the set of all countable ordinals. Even more explicitly, using the fact that ordinals are isomorphism types of well-orderings, we see that

$$\aleph_1 \;=\; \{\mathrm{type}(\prec) \,:\, \prec \text{ is a well-ordering on } \omega\}.$$

That is, there are precisely $\aleph_1$-many isomorphism types of well-orderings of the natural numbers.

We say that κ is a **successor cardinal** if $\kappa = \lambda^+$ for some cardinal $\lambda < \kappa$; if κ is positive and not a successor cardinal, then we call it a **limit cardinal**.

Example 6.13. ω is the least limit cardinal. The next smallest limit cardinal is $\aleph_\omega$. In general, $\aleph_\alpha$ for $\alpha > 0$ is a limit cardinal if and only if α is a limit ordinal (exercise!).

Recall that, assuming AC, every set has a well-defined cardinality. In particular, $|\mathcal{P}(\omega)|$ is an infinite cardinal, called the **cardinality of the continuum** and denoted by $\mathfrak{c}$. Then we have $\mathfrak{c} = \aleph_\alpha$ for some ordinal α. What is this α? We know that $\mathcal{P}(\omega)$ is uncountable—hence $\alpha > 0$—by Theorem 6.4. A famous conjecture of Cantor is that $\alpha = 1$:

Continuum Hypothesis (CH), formulation assuming AC

$$\mathfrak{c} \;=\; \aleph_1.$$

Although the above version of CH relies on AC to make $\mathfrak{c}$ well-defined, there is also a natural way to state it that makes sense even if $\mathcal{P}(\omega)$ is not well-orderable:

Continuum Hypothesis (CH), formulation without AC

If a set A satisfies $\omega \lesssim A \lesssim \mathcal{P}(\omega)$, then $\omega \approx A$ or $A \approx \mathcal{P}(\omega)$.

Famously, CH is an example of a natural mathematical statement that can be neither proved nor disproved using the axioms of ZFC alone (assuming ZFC is consistent, i.e., the axioms are not contradictory). The fact that CH cannot be *disproved* in ZFC was shown by Kurt Gödel in 1940, while Paul Cohen demonstrated in 1963 that CH cannot be *proved* either. Later in this course, we will prove Gödel's result (i.e., the consistency of CH); in fact, we will show that the following stronger assertion, called the **Generalized Continuum Hypothesis**, can't be refuted in ZFC (again, assuming ZFC itself is consistent):

Generalized Continuum Hypothesis (GCH)

Assuming AC: For every infinite cardinal κ, $|\mathcal{P}(\kappa)| = \kappa^+$.

Without AC: If X is an infinite set and $X \lesssim A \lesssim \mathcal{P}(X)$, then $X \approx A$ or $A \approx \mathcal{P}(X)$.

7. Ordinal arithmetic

7.1. Addition and multiplication of ordinals

In this section, a **linearly ordered set** is a pair $\boldsymbol{X} = (X, \prec_X)$ where $\prec_X$ is a strict linear ordering on X. In order to unclutter the notation, when there is no possibility of confusion, we will sometimes simply use the symbol $\prec$ to denote the linear ordering on $\boldsymbol{X}$ (just like we use the same symbol $<$ to denote the well-ordering on each ordinal α) and sometimes conflate $\boldsymbol{X}$ with its underlying set X.

For a pair of sets X, Y, we define their **disjoint union** as follows:

$$X \sqcup Y := (X \times \{0\}) \cup (Y \times \{1\}).$$

The idea of this definition is that $X \times \{0\}$ and $Y \times \{1\}$ are disjoint sets such that $X \approx X \times \{0\}$ and $Y \approx Y \times \{1\}$, so $X \sqcup Y$ is formed by taking the union of a "copy" of X and a "copy" of Y that are disjoint from each other.

Exercise 7.1. Let X, Y be sets and let $\iota_X : X \to X \sqcup Y$ and $\iota_Y : Y \to X \sqcup Y$ be the maps given by

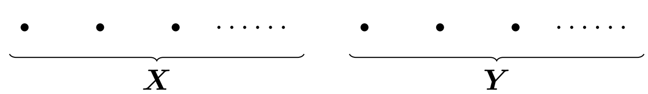
$$\iota_X(x) := (x, 0) \quad \text{and} \quad \iota_Y(y) := (y, 1) \quad \text{for all } x \in X,\ y \in Y.$$

Show that for every set Z and every pair of injections $f : X \to Z$ and $g : Y \to Z$, there exists a unique map $h : X \sqcup Y \to Z$ such that $f = h \circ \iota_X$ and $g = h \circ \iota_Y$.

Definition 7.1 (Addition of linear orders)**.** Let $\boldsymbol{X} = (X, \prec_X)$ and $\boldsymbol{Y} = (Y, \prec_Y)$ be linearly ordered sets. The **sum** of $\boldsymbol{X}$ and $\boldsymbol{Y}$ is the linear order $\boldsymbol{X} \boxplus \boldsymbol{Y} = (X \sqcup Y, \prec)$, where for all (a, i), $(b, j) \in X \sqcup Y$,

$$(a, i) \prec (b, j) \quad :\Longleftrightarrow \quad \begin{cases} i = 0 \text{ and } j = 1, & \text{or} \\ i = j = 0 \text{ and } a \prec_X b, & \text{or} \\ i = j = 1 \text{ and } a \prec_Y b. \end{cases}$$

Informally, $\boldsymbol{X} \boxplus \boldsymbol{Y}$ is obtained by taking a copy of $\boldsymbol{X}$ and placing a copy of $\boldsymbol{Y}$ following it:



(In the above illustration, the elements are ordered left-to-right.)

Exercise 7.2. Check that if $\boldsymbol{X}$ and $\boldsymbol{Y}$ are linearly ordered sets, then $\boldsymbol{X} \boxplus \boldsymbol{Y}$ is linearly ordered as well. Moreover, show that if $\boldsymbol{X}$ and $\boldsymbol{Y}$ are well-ordered, then so is $\boldsymbol{X} \boxplus \boldsymbol{Y}$.

Definition 7.2 (Addition of ordinals)**.** Let α, $\beta \in \mathbf{Ord}$. We view α and β as sets well-ordered by the usual ordering on the ordinals (i.e., the membership relation). By Exercise 7.2, $\alpha \boxplus \beta$ is also a well-ordered set, and we define the **sum** of α and β as its order-type:

$$\alpha + \beta := \operatorname{type}(\alpha \boxplus \beta).$$

Example 7.3. We have $2 + 2 = 4$. Indeed, the ordering on $2 \boxplus 2$ is

$$(0, 0) \prec (1, 0) \prec (0, 1) \prec (1, 1),$$

which is isomorphic to the standard ordering on the set 4:

$$0 < 1 < 2 < 3.$$

Proposition 7.4. *For all $\alpha \in \mathbf{Ord}$, the successor of α is the sum of α and 1 (i.e., our notation $\alpha + 1$ for the successor of α is consistent).*

Proof. The following map f is an order-isomorphism from the successor of α to $\alpha \sqcup 1$:

$$f(\gamma) := \begin{cases} (\gamma, 0) & \text{if } \gamma < \alpha, \\ (0, 1) & \text{if } \gamma = \alpha. \end{cases}$$ ■

Exercise 7.3. Verify the following facts about addition of ordinals:

- Addition of ordinals is associative.
- For all $\alpha \in \mathbf{Ord}$, $0 + \alpha = \alpha + 0 = \alpha$.

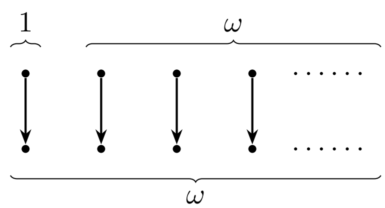
In general, addition of ordinals is not commutative. For example, we have

$$1 + \omega \;=\; \omega \;\neq\; \omega + 1.$$

To see that $1 + \omega = \omega$, we observe that the map f given by

$$f(n, i) \;:=\; n + i$$

is an order-isomorphism from $1 \boxplus \omega$ to ω; see the illustration below:



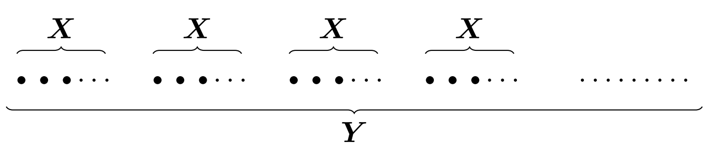
Exercise 7.4. Prove that $n + \omega = \omega$ for all $n < \omega$, but $\omega + \omega > \omega$.

Exercise 7.5. Show that for ordinals α, β, we have $\alpha \geqslant \beta$ if and only if there exists an ordinal γ such that $\alpha = \beta + \gamma$.

Definition 7.5 (Multiplication of linear orders)**.** Let $\boldsymbol{X} = (X, \prec)$ and $\boldsymbol{Y} = (Y, \prec)$ be linearly ordered sets. The **product** of $\boldsymbol{X}$ and $\boldsymbol{Y}$ is the linear order $\boldsymbol{X} \boxtimes \boldsymbol{Y} = (X \times Y, \prec)$, where

$$(x, y) \prec (x', y') \quad :\Longleftrightarrow \quad y \prec y' \text{ or } (y = y' \text{ and } x \prec x').$$

(Note that we compare the second coordinates first.) Informally, $\boldsymbol{X} \boxtimes \boldsymbol{Y}$ is obtained by taking a copy of $\boldsymbol{Y}$ and replacing each element in it by a copy of $\boldsymbol{X}$:



Exercise 7.6. Check that if $\boldsymbol{X}$ and $\boldsymbol{Y}$ are linearly ordered sets, then $\boldsymbol{X} \boxtimes \boldsymbol{Y}$ is linearly ordered as well. Moreover, show that if $\boldsymbol{X}$ and $\boldsymbol{Y}$ are well-ordered, then so is $\boldsymbol{X} \boxtimes \boldsymbol{Y}$.

Definition 7.6 (Multiplication of ordinals)**.** Let α, $\beta \in \mathbf{Ord}$. Viewing α and β as well-ordered sets, we see that by Exercise 7.6, $\alpha \boxtimes \beta$ is also well-ordered. Hence, we can define the **product** of α and β as the order-type or $\alpha \boxtimes \beta$:

$$\alpha\beta \;:=\; \mathrm{type}(\alpha \boxtimes \beta).$$

Example 7.7. Every ordinal α satisfies $\alpha \cdot 2 = \alpha + \alpha$ (for instance, $2 \cdot 2 = 4$). This is because the ordered sets $\alpha \boxplus \alpha$ and $\alpha \boxtimes 2$ are literally equal to each other: we have

$$\alpha \sqcup \alpha \;=\; (\alpha \times \{0\}) \cup (\alpha \times \{1\}) \;=\; \alpha \times \{0, 1\} \;=\; \alpha \times 2,$$

and the orderings on this set given by Definitions 7.1 and 7.5 coincide.

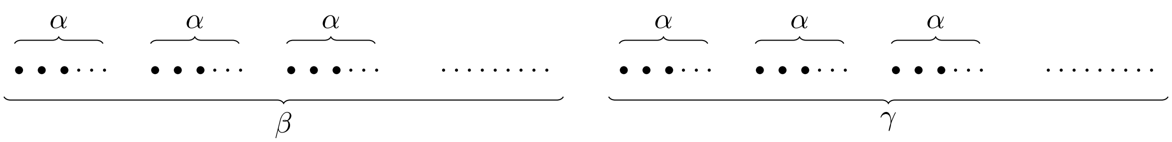
Exercise 7.7. Verify the following facts about multiplication of ordinals:

- Multiplication of ordinals is associative.
- For all $\alpha \in \mathbf{Ord}$, $0 \cdot \alpha = \alpha \cdot 0 = 0$.

- For all $\alpha \in \mathbf{Ord}$, $1 \cdot \alpha = \alpha \cdot 1 = \alpha$.

Proposition 7.8. *For all ordinals α, β, γ, we have $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$. That is, multiplication of ordinals is left-distributive over addition.*

Proof. Intuitively, the ordered sets $\alpha \boxtimes (\beta \boxplus \gamma)$ and $(\alpha \boxtimes \beta) \boxplus (\alpha \boxtimes \gamma)$ are isomorphic because they both look like this:



Explicitly, the following mapping is an order-isomorphism from $\alpha \boxtimes (\beta \boxplus \gamma)$ to $(\alpha \boxtimes \beta) \boxplus (\alpha \boxtimes \gamma)$:

$$\Big(\underbrace{\delta}_{<\alpha}, \big(\underbrace{\varepsilon}_{\substack{<\beta \text{ if } i=0,\\ <\gamma \text{ if } i=1}}, \underbrace{i}_{0 \text{ or } 1}\big)\Big) \quad \mapsto \quad \big((\delta, \varepsilon), i\big).$$

The details are left as an exercise. ■

In general, multiplication of ordinals is not commutative. For instance, $2 \cdot \omega = \omega \neq \omega + \omega = \omega \cdot 2$. (Exercise: check that $2 \cdot \omega$ is indeed equal to ω.) Also, multiplication is not right-distributive:

$$(1+1) \cdot \omega \;=\; \omega \;\neq\; \omega + \omega \;=\; 1 \cdot \omega + 1 \cdot \omega.$$

Of course, for *certain* ordinals α, β, we do have $\alpha + \beta = \beta + \alpha$ and $\alpha\beta = \beta\alpha$. For example, the arithmetic on the natural numbers has all the expected properties.

Theorem 7.9. *If n, $m < \omega$, then $n + m = m + n$.*

Proof. The proof is by induction on m. If $m = 0$, then $n + 0 = 0 + n = n$ by Exercise 7.3. Now suppose that for some $m < \omega$, we have $n+m = m+n$. Our goal is to show that $n+(m+1) = (m+1)+n$. To that end, we write

$$\begin{aligned}
n + (m+1) &= (n+m) + 1 && \text{(associativity)}\\
&= (m+n) + 1 && \text{(inductive hypothesis)}\\
&= m + (n+1) && \text{(associativity)}\\
&\overset{?}{=} m + (1+n) &&\\
&= (m+1) + n. && \text{(associativity)}
\end{aligned}$$

The only missing step is to argue that $1 + n = n + 1$. This we show by induction on n. If $n = 0$, then $1 + 0 = 0 + 1 = 1$. Now suppose we have $1 + n = n + 1$ for some $n < \omega$ and want to conclude that $1 + (n+1) = (n+1) + 1$. Using associativity and the inductive hypothesis, we obtain

$$1 + (n+1) \;=\; (1+n) + 1 \;=\; (n+1) + 1,$$

and the proof is complete. ■

Exercise 7.8. Show that if n, $m < \omega$, then $nm = mn$.

Exercise 7.9. Show that if n, $m < \omega$, then $n + m$, $nm < \omega$ as well.

In principle, one can now proceed to derive the entire subject of number theory from first principles by rigorously establishing all the necessary facts about the arithmetic on the natural numbers.

7.2. Recursive definitions for operations on ordinals

Recall from Exercise 5.2 that for a set X of ordinals, $\sup X$ is the least ordinal greater than or equal to every element of X, and we have $\sup X = \bigcup X$. The following lemma is extremely useful for computing order-types of well-ordered sets:

Lemma 7.10. *Let $(X, \prec)$ be a well-ordered set. If S is a set of downward closed subsets of X such that $X = \bigcup S$, then*

$$\mathrm{type}(X, \prec) \;=\; \sup_{D \in S} \mathrm{type}(D, \prec\restriction D).$$

PROOF. For brevity, given $A \subseteq X$, we write $\mathrm{type}(A) \coloneqq \mathrm{type}(A, \prec\restriction A)$. Our goal is to prove

$$\mathrm{type}(X) \;=\; \sup_{D \in S} \mathrm{type}(D).$$

Let $\alpha \coloneqq \sup_{D \in S} \mathrm{type}(D)$. To begin with, note that for each $D \in S$,

$$\mathrm{type}(D) \;\cong\; D \;\subseteq\; X \;\cong\; \mathrm{type}(X).$$

Hence, there is a strictly increasing map from $\mathrm{type}(D)$ to $\mathrm{type}(X)$. By Exercise 5.1, it follows that $\mathrm{type}(D) \leqslant \mathrm{type}(X)$, and thus $\mathrm{type}(X) \geqslant \alpha$. This part of the argument works when S is any subset of $\mathcal{P}(X)$ (it doesn't matter that its elements are downward closed and their union is X).

Now suppose for contradiction that $\alpha < \mathrm{type}(X)$, i.e., $\alpha \in \mathrm{type}(X)$. Let $f \colon \mathrm{type}(X) \to X$ be the (unique) order-isomorphism between $\mathrm{type}(X)$ and $(X, \prec)$ and consider the element $f(\alpha) \in X$. Since $X = \bigcup S$, there is $D \in S$ with $f(\alpha) \in D$. As D is downward closed and f is increasing, we have $f(\beta) \in D$ for all $\beta \leqslant \alpha$. In other words, $f\restriction\{\beta \in \mathbf{Ord} : \beta \leqslant \alpha\} = f\restriction(\alpha + 1)$ is a strictly increasing function from $\alpha + 1$ to D. By Exercise 5.1, it follows that $\alpha + 1 \leqslant \mathrm{type}(D)$, which is a contradiction as $\mathrm{type}(D) \leqslant \alpha$. Therefore, $\mathrm{type}(X) = \alpha$ and the proof is complete. ■

Using Lemma 7.10, we can describe addition and multiplication of ordinals via recursive formulas:

Theorem 7.11. *For all α, $\beta \in \mathbf{Ord}$,*

$$\alpha + \beta \;=\; \begin{cases} \alpha & \text{if } \beta = 0, \\ (\alpha + \gamma) + 1 & \text{if } \beta = \gamma + 1, \\ \sup_{\gamma < \beta}(\alpha + \gamma) & \text{if } \beta \text{ is a limit,} \end{cases} \qquad \alpha\beta \;=\; \begin{cases} 0 & \text{if } \beta = 0, \\ \alpha\gamma + \alpha & \text{if } \beta = \gamma + 1, \\ \sup_{\gamma < \beta}(\alpha\gamma) & \text{if } \beta \text{ is a limit.} \end{cases}$$

PROOF. We already know that $\alpha + 0 = \alpha$ and $\alpha + (\gamma + 1) = (\alpha + \gamma) + 1$. Suppose β is a limit ordinal. Then $\beta = \bigcup_{\gamma < \beta} \gamma$ (Exercise 3.12), so

$$\alpha \boxplus \beta \;=\; \bigcup_{\gamma < \beta} (\alpha \boxplus \gamma).$$

Moreover, for each $\gamma < \beta$, the set $\alpha \sqcup \gamma$ is clearly downward closed in $\alpha \boxplus \beta$, so, by Lemma 7.10,

$$\alpha + \beta \;=\; \mathrm{type}(\alpha \boxplus \beta) \;=\; \sup_{\gamma < \beta} \mathrm{type}(\alpha \boxplus \gamma) \;=\; \sup_{\gamma < \beta}(\alpha + \gamma).$$

The proof for multiplication is similar and left as an exercise. ■

Depending on the situation, it may be more convenient to analyze addition and multiplication of ordinals directly using the definition or via the recursive formulas from Theorem 7.11. For example, it is clear from Theorem 7.11 that addition and multiplication are strictly monotone in the second argument, meaning that if $\gamma < \beta$, then $\alpha + \gamma < \alpha + \beta$ and $\alpha\gamma < \alpha\beta$. Note, however, that these operations are monotone, but not *strictly* monotone, in the first argument. In other words, if $\gamma < \alpha$, then we have $\gamma + \beta \leqslant \alpha + \beta$ and $\gamma\beta \leqslant \alpha\beta$, but neither inequality must be strict. For example, $1 + \omega = 2 + \omega$ and $1 \cdot \omega = 2 \cdot \omega$.

Recursive formulas analogous to the ones in Theorem 7.11 give a useful general strategy for defining operations on ordinals. As an example, here is a recursive definition of ordinal exponentiation:

Definition 7.12 (Exponentiation of ordinals)**.** Given ordinals α, β, we define an ordinal α^β using the following recursive formula:

$$\alpha^\beta \;=\; \begin{cases} 1 & \text{if } \beta = 0, \\ \alpha^\gamma \cdot \alpha & \text{if } \beta = \gamma + 1, \\ \sup_{\gamma < \beta} \alpha^\gamma & \text{if } \beta \text{ is a limit.} \end{cases}$$

Exercise 7.10. Verify the following facts about exponentiation of ordinals:

- For all $\alpha \in \mathbf{Ord}$, $\alpha^0 = 1$.
- If $0 < \alpha \in \mathbf{Ord}$, then $0^\alpha = 0$.
- For all $\alpha \in \mathbf{Ord}$, $\alpha^1 = \alpha$ and $1^\alpha = 1$.
- For all α, β, $\gamma \in \mathbf{Ord}$, $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$ and $(\alpha^\beta)^\gamma = \alpha^{\beta\gamma}$.

Note that there are ordinals α, β, γ such that $(\alpha\beta)^\gamma \neq \alpha^\gamma\beta^\gamma$. For example,

$$(\omega \cdot 2)^2 \;=\; \omega \cdot \underbrace{2 \cdot \omega}_{\omega} \cdot 2 \;=\; \omega^2 \cdot 2 \;<\; \omega^2 \cdot 2^2.$$

Exercise 7.11. Show that $2^\omega = \omega$.

7.3. Application: Goodstein's theorem

As an application of the machinery developed in this section, we shall now use infinitary techniques to prove a surprising result from elementary number theory due to Reuben Goodstein. To state it, we need a few definitions. Given a positive integer n and an integer $b \geqslant 2$, a **base-b expansion** of n is an expression of the form

$$n \;=\; b^k \cdot d_k + b^{k-1} \cdot d_{k-1} + \cdots + b \cdot d_1 + d_0,$$

where $k \in \mathbb{N}$ and $d_0, \ldots, d_k$ are integers between 0 and $b - 1$, called the **digits** of the expansion. It is a well-known and easy fact that every $n \geqslant 1$ has a base-b expansion for all $b \geqslant 2$; furthermore, if we additionally require that $d_k \neq 0$, then the base-b expansion of n is unique.[iv] For instance, the base-2, base-3, base-6, and base-10 expansions of 100 are

$$100 \;=\; 2^6 + 2^5 + 2^2 \;=\; 3^4 + 3^2 \cdot 2 + 1 \;=\; 6^2 \cdot 2 + 6 \cdot 4 + 4 \;=\; 10^2.$$

(For better readability we have omitted the terms whose corresponding digits are 0 and simplified the expressions such as $b^j \cdot 1$ to b^j.) The **hereditary base-b expansion** of n is obtained from the ordinary base-b expansion by replacing every exponent by *its* own base-b expansion, then replacing all the exponents *inside* the exponents by *their* base-b expansions, etc. This idea is best understood through an example. Here are hereditary base-2 and base-3 expansions of 100:

$$100 \;=\; 2^{2^2+2} + 2^{2^2+1} + 2^2 \qquad \text{and} \qquad 100 \;=\; 3^{3+1} + 3^2 \cdot 2 + 1. \tag{7.1}$$

And here's the hereditary base-2 expansion of 1000000:

$$1000000 \;=\; 2^{2^{2^2}+2+1} + 2^{2^{2^2}+2} + 2^{2^{2^2}+1} + 2^{2^{2^2}} + 2^{2^{2+1}+2^2+2} + 2^{2^{2+1}+1} + 2^{2^2+2}.$$

A **Goodstein sequence** is a sequence $(n_b)_{2 \leqslant b < \omega}$ of natural numbers obtained via the following recursive construction. Start with any $n_2 \in \omega$. Then, for each $b \geqslant 2$, if $n_b = 0$, then set $n_{b+1} := 0$. On the other hand, if $n_b \geqslant 1$, then n_{b+1} is obtained from n_b by replacing each "b" in the hereditary base-b expansion of n_b by "$b + 1$" and then subtracting 1 from the result.

[iv]Here and throughout the remainder of these notes we shall take such basic facts about natural numbers for granted, since this is a course in set theory, not number theory.

Example 7.13. Let us find the first few terms of the Goodstein sequence starting with $n_2 = 100$. To determine n_3, we compute the hereditary base-2 expansion of n_2, which is given by (7.1). We then replace each "2" by "3" and subtract 1:

$$n_3 \;=\; 3^{3^3+3} + 3^{3^3+1} + 3^3 \;\; - 1 \;=\; 228767924549636.$$

Next, we compute the hereditary base-3 expansion of n_3, which is

$$228767924549636 \;=\; 3^{3^3+3} + 3^{3^3+1} + 3^2 \cdot 2 + 3 \cdot 2 + 2,$$

replace each "3" by "4," and subtract 1:

$$n_4 \;=\; 4^{4^4+4} + 4^{4^4+1} + 4^2 \cdot 2 + 4 \cdot 2 + 2 \;\; - 1 \;\approx\; 3 \cdot 10^{156}.$$

As you can see, Goodstein sequences typically experience explosive growth. That is what makes the following result so shocking:

Theorem 7.14 (Goodstein)**.** *Every Goodstein sequence reaches* 0 *in finitely many steps.*

Example 7.15. Before we give a proof of Goodstein's theorem, it is worthwhile to consider what happens for small values of n_2. The theorem is trivial for $n_2 = 0$. For $n_2 = 1$, we have $n_3 = 0$, while for $n_2 = 2$, we have $n_3 = 2$, $n_4 = 1$, and $n_5 = 0$. If $n_2 = 3$, we reach 0 at the n_7 stage:

$$n_2 = 3, \quad n_3 = 3, \quad n_4 = 3, \quad n_5 = 2, \quad n_6 = 1, \quad n_7 = 0.$$

But already for $n_2 = 4$, the sequence seems to increase steadily:

$$n_2 = 4, \quad n_3 = 26, \quad n_4 = 41, \quad n_5 = 60, \quad n_6 = 83, \quad n_7 = 109, \quad \ldots$$

Nonetheless, as Goodstein's theorem predicts, it does reach 0 eventually... namely on step

$$3 \cdot 2^{402653211} - 1.$$

And with $n_2 = 5$, the sequence reaches 0 after the number of steps that is much, much greater than

$$10^{10^{10^{10000}}}.$$

P R O O F. Here's the proof idea: On step b, instead of merely replacing each b by $b+1$, go "all in" and replace each b by the *infinite* ordinal ω. Until we reach 0, this operation will produce a *strictly decreasing* sequence of ordinals (due to subtracting 1 on each stage), which cannot be infinite.

Now to fill in some details. For each $b \geqslant 2$, let $F_b \colon \omega \to \mathbf{Ord}$ be the function defined as follows: $F_b(0) := 0$, and to determine $F_b(n)$ for $n \geqslant 1$, we first compute the hereditary base-b expansion of n and then replace each b by ω, interpreting the addition, multiplication, and exponentiation as the corresponding operations of ordinal arithmetic. For instance, using (7.1), we see that

$$F_2(100) \;=\; \omega^{\omega^\omega+\omega} + \omega^{\omega^\omega+1} + \omega^\omega \qquad \text{and} \qquad F_3(100) \;=\; \omega^{\omega+1} + \omega^2 \cdot 2 + 1.$$

It is important to keep in mind that the order of addition and multiplication matters (since the operations of ordinal arithmetic are not commutative). Specifically, the terms are being added in the decreasing order, and the multiplication by the digits is on the right.

Lemma 7.16. *For each $b \geqslant 2$, the function $F_b \colon \omega \to$* **Ord** *is strictly increasing.*

Proof. It is enough to show that for all $n \in \mathbb{N}$, we have $F_b(n+1) > F_b(n)$. The proof is by induction on n. Note that $F_b(0) = 0 < 1 = F_b(1)$. Now suppose that $n \geqslant 1$ and for all $m < n$, we have $F_b(m+1) > F_b(m)$. Let the base-b expansion of n be

$$n \;=\; \sum_{i=0}^{k} b^i \cdot d_i.$$

Set $d_{k+1} \coloneqq 0$ and let j be the least index such that $d_j \neq b-1$. The standard elementary school algorithm for addition with carry shows that the base-b expansion of $n+1$ is

$$n+1 \;=\; \sum_{i=j+1}^{k+1} b^i \cdot d_i \;+\; b^j \cdot (d_j+1).$$

Keeping in mind that, by the choice of j, $b_i = n-1$ for all $i < j$, we see that

$$F_b(n) \;=\; \sum_{i=j+1}^{k+1} \omega^{F_b(i)} \cdot d_i \;+\; \omega^{F_b(j)} \cdot d_j \;+\; \sum_{i=0}^{j-1} \omega^{F_b(i)} \cdot (b-1);$$

$$\text{and} \qquad F_b(n+1) \;=\; \sum_{i=j+1}^{k+1} \omega^{F_b(i)} \cdot d_i \;+\; \omega^{F_b(j)} \cdot (d_j+1).$$

(We emphasize that in the above expressions, the summation indicated by "$\sum$" should be taken in *decreasing* order.) Since ordinal addition is strictly monotone in the second argument, to prove $F_b(n+1) > F_b(n)$, it suffices to argue that

$$\omega^{F_b(j)} \;>\; \sum_{i=0}^{j-1} \omega^{F_b(i)} \cdot (b-1).$$

If $j = 0$, then $\omega^{F_b(j)} = 1 > 0$. On the other hand, if $j > 0$, then, since, by the inductive hypothesis, the function F_b is strictly increasing on $\{0, \ldots, n\}$, we have

$$\begin{aligned}\sum_{i=0}^{j-1} \omega^{F_b(i)} \cdot (b-1) \;&=\; \omega^{F_b(j-1)} \cdot (b-1) \;+\; \omega^{F_b(j-2)} \cdot (b-1) \;+\; \cdots \;+\; \omega^{F_b(0)} \cdot (b-1) \\ &\leqslant\; \omega^{F_b(j-1)} \cdot ((b-1)j) \;<\; \omega^{F_b(j-1)} \cdot \omega \;=\; \omega^{F_b(j-1)+1} \;\leqslant\; \omega^{F_b(j)},\end{aligned}$$

as desired. ☒

Now consider an arbitrary Goodstein sequence $(n_b)_{2 \leqslant b < \omega}$. We associate to it a sequence of ordinals $(\alpha_b)_{2 \leqslant b < \omega}$ by setting $\alpha_b \coloneqq F_b(n_b)$. If $n_b \geqslant 1$, then, by definition, $n_{b+1}+1$ is obtained from the base-b expansion of n_b by replacing each "b" by "$b+1$." Hence, by Lemma 7.16

$$\alpha_b \;=\; F_b(n_b) \;=\; F_{b+1}(n_{b+1}+1) \;>\; F_{b+1}(n_{b+1}) \;=\; \alpha_{b+1}.$$

Therefore, if $n_b \geqslant 1$ for all b, the sequence $(\alpha_b)_{2 \leqslant b < \omega}$ is an infinite strictly decreasing sequence of ordinals, which is impossible. ■

We remark that our use of infinitary techniques to prove Goodstein's theorem is not coincidental. With a little work, it is possible to formulate Theorem 7.14 without assuming any infinite sets exist. For example, most of the general properties of ordinals we established did not rely on the Axiom of Infinity, and although we used the Axiom of Infinity to define the natural numbers, it can be avoided by saying that n is a natural number if and only if n is an ordinal and every ordinal $m \leqslant n+1$ is either 0 or a successor. Using this definition as a starting point, a large part of number theory can be developed without ever having to invoke the existence of infinite sets. Nevertheless, it was shown by Laurence Kirby and Jeff Paris that although Goodstein's theorem is a natural "finitary" statement about elementary arithmetic, it *cannot* be proved using ZFC without the Axiom of Infinity.

8. Cardinal arithmetic

8.1. Addition and multiplication of cardinals

Note that if X and Y are well-orderable sets, then $X \sqcup Y$ and $X \times Y$ are also well-orderable (via taking the sum or the product of arbitrary well-orderings on X and Y). Therefore, these sets have well-defined cardinalities, and the following definition makes sense:

Definition 8.1 (Addition and multiplication of cardinals)**.** If κ and λ are cardinals, we define their **sum** and **product** by

$$\kappa \oplus \lambda \;:=\; |\kappa \sqcup \lambda| \;=\; |\kappa + \lambda| \quad \text{and} \quad \kappa \otimes \lambda \;:=\; |\kappa \times \lambda| \;=\; |\kappa\lambda|.$$

We remark that in the literature, it is common to denote the sum and the product of cardinals κ and λ simply by $\kappa + \lambda$ and $\kappa\lambda$. However, we shall use the symbols $\oplus$ and $\otimes$ to avoid confusion with the operations of ordinal arithmetic.

Example 8.2. If n, $m < \omega$, then $n \oplus m = n + m$ and $n \otimes m = nm$, because the finite ordinals $n + m$ and nm are cardinals. On the other hand, $\omega \oplus 1 = |\omega + 1| = \omega < \omega + 1$.

Proposition 8.3. *Addition and multiplication of cardinals are associative and commutative. Multiplication of cardinals distributes over addition. Every cardinal κ satisfies $\kappa \oplus 0 = \kappa$, $\kappa \otimes 0 = 0$, and $\kappa \otimes 1 = \kappa$.*

Proof. We will prove commutativity, leaving the rest of the properties as exercises. Take κ, $\lambda \in \mathbf{Card}$. Then $\kappa \sqcup \lambda \approx \lambda \sqcup \kappa$ via the map $(\gamma, i) \mapsto (\gamma, 1 - i)$. Therefore, $\kappa \oplus \lambda = |\kappa \sqcup \lambda| = |\lambda \sqcup \kappa| = \lambda \oplus \kappa$. Similarly, $\kappa \times \lambda \approx \lambda \times \kappa$ via the map $(\gamma\delta) \mapsto (\delta, \gamma)$, so $\kappa \otimes \lambda = |\kappa \times \lambda| = |\lambda \times \kappa| = \lambda \otimes \kappa$. ■

Theorem 8.4. *Every infinite cardinal κ satisfies $\kappa \otimes \kappa = \kappa$.*

Before proving Theorem 8.4, we observe that it implies that arithmetic on infinite cardinals is extremely simple:

Corollary 8.5. *Let κ, $\lambda \in$ **Card**. If at least one of κ, λ is infinite, then*

$$\kappa \oplus \lambda \;=\; \max\{\kappa, \lambda\}.$$

If at least one of κ, λ is infinite and neither of them is 0, then

$$\kappa \otimes \lambda \;=\; \max\{\kappa, \lambda\}.$$

Proof. For concreteness, let $\lambda \leqslant \kappa$ and assume that $\kappa \geqslant \omega$. Clearly, $\kappa \lesssim \kappa \sqcup \lambda$, so $\kappa \leqslant \kappa \oplus \lambda$. On the other hand, since $\lambda \leqslant \kappa$, we have $\kappa \sqcup \lambda \subseteq \kappa \sqcup \kappa = \kappa \times \{0, 1\} \subseteq \kappa \times \kappa$, and thus $\kappa \oplus \lambda \leqslant \kappa \otimes \kappa = \kappa$. Therefore, $\kappa \oplus \lambda = \kappa$, as desired. The part concerning multiplication is left as an exercise. ■

Corollary 8.6. *If A, B are infinite well-orderable sets, then $|A \cup B| = \max\{|A|, |B|\}$.*

Proof. Clearly, $\max\{|A|, |B|\} \leqslant |A \cup B|$. On the other hand, we have a surjection $A \sqcup B \to A \cup B$ given by $(x, i) \mapsto x$. Therefore, $|A \cup B| \leqslant |A \sqcup B| = |A| \oplus |B| = \max\{|A|, |B|\}$. ■

Exercise 8.1. Show that if A is an infinite well-orderable set and $B \subset A$ is a subset with $|B| < |A|$, then $|A \backslash B| = |A|$.

Proof *of Theorem 8.4.* Clearly, $\kappa \leqslant \kappa \otimes \kappa$. Suppose, toward a contradiction, that κ is the least cardinal such that $\kappa < \kappa \otimes \kappa$.

Claim 8.7. *Every cardinal $\lambda < \kappa$ satisfies $\lambda \otimes \lambda < \kappa$.*

Proof. If λ is finite, then $\lambda \otimes \lambda \leqslant \omega < \kappa$ (see Exercise 7.9). On the other hand, if λ is infinite, then $\lambda \otimes \lambda = \lambda < \kappa$ by the choice of κ. ⊠

Claim 8.8. *There exists a well-ordering $\prec$ on $\kappa \times \kappa$ such that for each ordinal $\gamma < \kappa$, the set $\gamma \times \gamma$ is downward closed in $\prec$.*

Proof. We have $(\alpha, \beta) \in \gamma \times \gamma$ if and only if $\alpha < \gamma$ and $\beta < \gamma$, or, equivalently, $\max\{\alpha, \beta\} < \gamma$. Let $\lhd$ be an arbitrary well-ordering on $\kappa \times \kappa$ (e.g., the one given by Definition 7.5) and define

$$(\alpha, \beta) \prec (\alpha', \beta') \quad :\Longleftrightarrow \quad \max\{\alpha, \beta\} < \max\{\alpha', \beta'\} \\ \text{or } \big(\max\{\alpha, \beta\} = \max\{\alpha', \beta'\} \text{ and } (\alpha, \beta) \lhd (\alpha', \beta')\big).$$

It is an easy exercise that $\prec$ is a well-ordering. Furthermore, if $(\alpha, \beta) \prec (\alpha', \beta') \in \gamma \times \gamma$, then

$$\max\{\alpha, \beta\} \leqslant \max\{\alpha', \beta'\} < \gamma,$$

so $(\alpha, \beta) \in \gamma \times \gamma$ as well, which shows that $\gamma \times \gamma$ is downward closed. ☒

Let $\prec$ be the well-ordering from Claim 8.8 and define, for each $\gamma < \kappa$,

$$\alpha_\gamma := \mathrm{type}(\gamma \times \gamma, \prec\restriction(\gamma \times \gamma)).$$

Since $\alpha_\gamma \approx \gamma \times \gamma$, we have $|\alpha_\gamma| = |\gamma \times \gamma| = |\gamma| \otimes |\gamma| < \kappa$ by Claim 8.7, and hence $\alpha_\gamma < \kappa$ by (6.2). It follows that $\kappa \geqslant \sup_{\gamma<\kappa} \alpha_\gamma$. On the other hand, since κ is an infinite cardinal, it is a limit ordinal, and thus $\kappa \times \kappa = \bigcup_{\gamma<\kappa}(\gamma \times \gamma)$. Therefore,

$$\begin{aligned} \kappa &\geqslant \sup_{\gamma<\kappa} \alpha_\gamma \\ \text{[by Lemma 7.10]} \qquad &= \mathrm{type}(\kappa \times \kappa, \prec) \geqslant |\kappa \times \kappa| = \kappa \otimes \kappa > \kappa, \end{aligned}$$

a contradiction. ■

Under AC, Theorem 8.4 shows that every infinite set X is equinumerous with $X \times X$. Remarkably, this statement is actually *equivalent* to AC, as shown by Alfred Tarski; see Exercise 9.6.

The next result also relies on the Axiom of Choice:

Theorem 8.9 (ZFC$^-$)**.** *The union of countably many countable sets is countable. More generally, if κ, $\lambda \in$ **Card** and X is a set with $|X| \leqslant \kappa$ and $|Y| \leqslant \lambda$ for all $Y \in X$, then $|\bigcup X| \leqslant \kappa \otimes \lambda$.*

PROOF. We will prove the statement for countable sets, leaving the general case as an exercise. Let X be a countable set of countable sets. Then there is a surjection $f : \omega \to X$ and, moreover, for each $Y \in X$, there is a surjection $\omega \to Y$. Using AC, we obtain a function $X \to \mathcal{U} : Y \mapsto g_Y$ such that for each $Y \in X$, $g_Y : \omega \to Y$ is a surjection. Then the map $g : \omega \times \omega \to \bigcup X$ given by $g(n, m) := g_{f(n)}(m)$ is surjective, and hence $|\bigcup X| \leqslant |\omega \times \omega| = \aleph_0$, as desired. ■

The use of AC in the proof of Theorem 8.9 is essential. For example, assuming ZF is consistent, it is also consistent that ZF holds and $\mathcal{P}(\omega)$ is the union of countably many countable sets!

8.2. Cardinal exponentiation

In this section we work in ZFC$^-$, so every set has a well-defined cardinality. Recall that we use the notation ${}^XY$ for the set of all functions from X to Y.

Definition 8.10 (Exponentiation of cardinals)**.** Given cardinals κ, λ, the cardinal κ^λ is defined by

$$\kappa^\lambda := |{}^\lambda\kappa|.$$

A word of caution is in order. We have now defined two exponentiation operations: ordinal exponentiation (Definition 7.12) and cardinal exponentiation (Definition 8.10). Unfortunately, they use the same notation, so there is some possibility of confusion. We will always try to make it clear which type of exponentiation we are referring to. In particular, most of the time we will be concerned with *cardinal* exponentiation, and we will make a note whenever *ordinal* exponentiation is meant. Also, we will typically write "ω" for the first infinite ordinal and "$\aleph_0$" for the first infinite cardinal (even though it is actually the same set). For instance, $2^\omega = \omega$ (ordinal exponentiation!), while $2^{\aleph_0}$ is an uncountable cardinal:

Proposition 8.11. *For every cardinal κ, $|\mathcal{P}(\kappa)| = 2^\kappa > \kappa$.*

PROOF. For any set X, we have a bijection $\mathcal{P}(X) \to {}^X 2$, where each set $A \subseteq X$ corresponds to its **characteristic function** $\mathbf{1}_A \colon X \to 2$ given by

$$\mathbf{1}_A(x) := \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A. \end{cases}$$

Therefore, $|\mathcal{P}(\kappa)| = |{}^\kappa 2| = 2^\kappa$. The fact that $2^\kappa > \kappa$ follows by Cantor's Theorem 6.4. ■

Proposition 8.12. *For all cardinals κ, λ, η, we have $(\kappa^\lambda)^\eta = \kappa^{\lambda \otimes \eta}$.*

PROOF. This follows from the general fact, provable in ZF^-, that for any sets X, Y, Z,

$${}^{X \times Y} Z \approx {}^X \left({}^Y Z\right).$$

In other words, there is a one-to-one correspondence between the functions that take a pair of arguments $(x, y) \in X \times Y$ and output an element of Z and the functions that take a single argument $x \in X$ and output *another* function, now from Y to Z. This one-to-one correspondence is called **currying** (after Haskell Curry) and is defined as follows: to each $f \colon X \times Y \to Z$, we associate the map $\mathsf{curry}(f) \colon X \to {}^Y Z$ given by

$$\Big(\big(\mathsf{curry}(f)\big)(x)\Big)(y) := f(x, y).$$

Checking that $\mathsf{curry} \colon {}^{X \times Y} Z \to {}^X \left({}^Y Z\right)$ is bijective is a routine exercise. ■

Exercise 8.2. Verify the following facts about exponentiation of cardinals:

- For all $\kappa \in \mathbf{Card}$, $\kappa^0 = 1$.
- If $0 < \kappa \in \mathbf{Card}$, then $0^\kappa = 0$.
- For all $\kappa \in \mathbf{Card}$, $\kappa^1 = \kappa$ and $1^\kappa = 1$.
- For all κ, λ, $\eta \in \mathbf{Card}$, $\kappa^{\lambda \oplus \eta} = \kappa^\lambda \otimes \kappa^\eta$.

Proposition 8.13. *If λ is an infinite cardinal and $\kappa \in$ **Card** satisfies $2 \leqslant \kappa \leqslant \lambda$, then $\kappa^\lambda = 2^\lambda$.*

PROOF. We have $2^\lambda \leqslant \kappa^\lambda \leqslant \lambda^\lambda \leqslant (2^\lambda)^\lambda = 2^{\lambda \otimes \lambda} = 2^\lambda$. ■

Example 8.14. Consider the standard number systems ω, $\mathbb{Z}$ (integers), $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers), and $\mathbb{C}$ (complex numbers). We know that $|\omega| = \aleph_0$. The map $2 \times \omega \to \mathbb{Z}$ given by

$$(i, n) \mapsto \begin{cases} n & \text{if } i = 0, \\ -n-1 & \text{if } i = 1 \end{cases}$$

is a bijection, so $|\mathbb{Z}| = \aleph_0 \oplus \aleph_0 = \aleph_0$. The function $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ given by $(n, m) \mapsto n/m$ is surjective, so $|\mathbb{Q}| \leqslant \aleph_0 \otimes \aleph_0 = \aleph_0$. As $\mathbb{Z} \subset \mathbb{Q}$, we obtain $|\mathbb{Q}| = \aleph_0$. Now consider $\mathbb{R}$. The function

$$\mathcal{P}(\omega) \to \mathbb{R} \quad : \quad A \mapsto \sum_{n \in A} \frac{1}{10^n}$$

is injective (exercise!), so $\mathcal{P}(\omega) \lesssim \mathbb{R}$. Conversely, the map

$$\mathbb{R} \to \mathcal{P}(\mathbb{Q}) \quad : \quad x \mapsto \{q \in \mathbb{Q} \,:\, q < x\}$$

is also injective, and hence $\mathbb{R} \lesssim \mathcal{P}(\mathbb{Q}) \approx \mathcal{P}(\omega)$. This, $\mathbb{R} \approx \mathcal{P}(\omega)$, which implies $|\mathbb{R}| = 2^{\aleph_0}$. Similarly, we have $|\mathbb{C}| = 2^{\aleph_0}$ (exercise!).

Exercise 8.3. Write down explicit bijections witnessing that $\omega \approx \mathbb{Z} \approx \mathbb{Q}$ and $\mathcal{P}(\omega) \approx \mathbb{R} \approx \mathbb{C}$.

8.3. Applications of cardinality

In this section we continue working in ZFC^-. The following application appears in the original 1874 paper in which Cantor introduced the concept of cardinality. A real number x is called **algebraic** if it is a root of a nonzero polynomial with integer coefficients; otherwise, x is **transcendental**. For example, $\sqrt{2}$ is algebraic since it is a root of $x^2 - 2$. On the other hand, π and e are transcendental—but that is quite difficult to prove! Indeed, it is still not known (and considered to be an extremely challenging problem) whether, for example, $e + \pi$ is transcendental. Even the existence of *any* transcendental numbers is far from obvious. Historically, the first example was found by Joseph Liouville, who showed in 1844 that

$$\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

is transcendental. A remarkable consequence of the theory of cardinality is a simple proof of the existence of transcendental numbers. Moreover, *most* numbers are transcendental:

Theorem 8.15 (Cantor). *The set $A \subseteq \mathbb{R}$ of all algebraic numbers is countable. Therefore, the set $\mathbb{R} \setminus A$ of all transcendental numbers has cardinality $2^{\aleph_0}$.*

PROOF. Let P_d be the set of all polynomials of degree at most d with integer coefficients. Each such polynomial has precisely $d+1$ coefficients, so we have $P_d \approx \mathbb{Z}^{d+1}$[v], and thus the set P_d is countable. The set $P = \bigcup_{d=0}^{\infty} P_d$ of all polynomials with integer coefficients is then countable by Theorem 8.9. Finally, since every polynomial has finitely many roots, A is the union of countably many finite sets, so A is countable by Theorem 8.9 again. ■

The next application showcases a powerful way in which cardinality can be of assistance in recursive constructions. When we define a function $f \colon \alpha \to \mathfrak{U}$ recursively, we describe how to compute $f(\beta)$ for each $\beta < \alpha$ given the values $f(\gamma)$ for all $\gamma < \beta$. If α happens to be a cardinal, then the set of all values that have already been determined—i.e., $\{f(\gamma) : \gamma < \beta\}$—has cardinality $|\beta| < \alpha$. In other words, at each individual stage of the recursive construction, most values of the function are still left undefined. This may provide the necessary flexibility for the construction to go forward.

Theorem 8.16 (Lindenbaum). *Let $f \colon \mathbb{R} \to \mathbb{R}$ be an arbitrary function. Then there exist injective functions g, $h \colon \mathbb{R} \to \mathbb{R}$ such that $f = g + h$ (i.e., $f(x) = g(x) + h(x)$ for every $x \in \mathbb{R}$).*

PROOF. Use AC to fix a bijection $2^{\aleph_0} \to \mathbb{R} \colon \alpha \mapsto x_\alpha$ (so $\mathbb{R} = \{x_\alpha : \alpha < 2^{\aleph_0}\}$). We also fix a choice function choice for $\mathcal{P}(\mathbb{R}) \setminus \{\varnothing\}$. We shall define the values $g(x_\alpha)$ and $h(x_\alpha)$ for all $\alpha < 2^{\aleph_0}$ recursively. Suppose that α is an ordinal less than $2^{\aleph_0}$ and that the values $g(x_\beta)$ and $h(x_\beta)$ for all $\beta < \alpha$ are already determined. Let

$$A_\alpha := \{g(x_\beta) : \beta < \alpha\} \qquad \text{and} \qquad B_\alpha := \{f(x_\alpha) - h(x_\beta) : \beta < \alpha\}.$$

To ensure that g is injective, we must assign to $g(x_\alpha)$ a value not in A_α; similarly, to ensure that h is injective, we must assign to $g(x_\alpha)$ a value not in B_α (since we must have $h(x_\alpha) = f(x_\alpha) - g(x_\alpha)$). Observe that, since $|\alpha| \leqslant \alpha < 2^{\aleph_0}$,

$$|A_\alpha \cup B_\alpha| \leqslant |A_\alpha| \oplus |B_\alpha| \leqslant |\alpha| \oplus |\alpha| < 2^{\aleph_0},$$

and hence $\mathbb{R} \neq A_\alpha \cup B_\alpha$ and $\mathbb{R} \setminus (A_\alpha \cup B_\alpha) \neq \varnothing$. Therefore, we can set

$$\begin{aligned} g(x_\alpha) &:= \mathsf{choice}\big(\mathbb{R} \setminus (A_\alpha \cup B_\alpha)\big), \\ h(x_\alpha) &:= f(x_\alpha) - g(x_\alpha). \end{aligned}$$ ■

Exercise 8.4. Prove Theorem 8.16 without using AC.

[v] Technically, we should be writing ${}^{d+1}\mathbb{Z}$, but that would be too cruel.

The next example is a curious application of the concept of cardinality in Ramsey theory, i.e., the study of patterns that must appear in every sufficiently large structure of a certain type.

Exercise 8.5. You invited infinitely many people to a party. Every two guests at the party are either friends or enemies (the friendship and enmity relations are symmetric). Show that among the guests, there is either an infinite set of mutual friends or an infinite set of mutual enemies. (This is known as *Ramsey's theorem.*)

Proposition 8.17. *For all $k < \omega$ and every function $f \colon \omega \to k$, there exist four distinct numbers a, b, c, $d \in \omega$ such that $f(a) = f(b) = f(c) = f(d)$ and $a + b = c + d$.*

Proof. Take $k < \omega$ and let $f \colon \omega \to k$. We proceed via a series of claims.

Claim 8.18. *For each $x \in \omega$, there exist a, $b < k + 1$ and $i < k$ such that:*

- *$a < b$, and*
- *$f(a + x) = f(b + x) = i$.*

Proof. Otherwise the map $a \mapsto f(x + a)$ would be an injection from $k + 1$ to k. ⊠

For each $x \in \omega$, let $\tau(x) = (a, b, i) \in (k + 1) \times (k + 1) \times k$ be an arbitrary triple satisfying the conditions of Claim 8.18 (we may as well use AC for this, although it is not necessary).

Claim 8.19. *There exist $x < y < z \in \omega$ such that $\tau(x) = \tau(y) = \tau(z)$.*

Proof. Otherwise $x \mapsto \tau(x)$ is an ($\leqslant 2$)-to-1 function from ω to $(k + 1) \times (k + 1) \times k$, implying the absurd inequality $\omega \leqslant 2(k + 1)^2 k$. ⊠

Claim 8.20. *There exist $x < y \in \omega$ such that $\tau(x) = \tau(y) = (a, b, i)$ and $y - x \neq b - a$.*

Proof. Take $x < y < z \in \omega$ with $\tau(x) = \tau(y) = \tau(z) = (a, b, i)$. If $y - x = b - a$, then $z - x > b - a$, so the pair (x, z) is as desired. ⊠

Let $x < y$ be such that $\tau(x) = \tau(y) = (a, b, i)$ and $y - x \neq b - a$. Note that, by the definition of τ,

$$f(a + x) \; = \; f(b + x) \; = \; f(a + y) \; = \; f(b + y) \; = \; i.$$

We also have $(a + x) + (b + y) = (b + x) + (a + y)$. It remains to notice that the condition $y - x \neq b - a$ ensures the numbers $a + x$, $b + y$, $b + x$, $a + y$ are distinct. ■

We now ask: What happens if in Proposition 8.17 we replace ω by $\mathbb{R}$? If we look at a function $f \colon \mathbb{R} \to k$ for some $k < \omega$, then the result is the same (just consider the restriction of f to $\omega \subset \mathbb{R}$). But what if we enlarge the codomain of f and consider functions $f \colon \mathbb{R} \to \omega$? The answer turns out to depend on additional set-theoretic assumptions, specifically the Continuum Hypothesis:

Theorem 8.21 (Erdős)**.** *The following statements are equivalent.*

(1) *For every function $f \colon \mathbb{R} \to \omega$, there exist four distinct numbers a, b, c, $d \in \mathbb{R}$ such that $f(a) = f(b) = f(c) = f(d)$ and $a + b = c + d$.*

(2) *The Continuum Hypothesis is false.*

Proof. (2) $\Longrightarrow$ (1): Suppose CH fails, i.e., $|\mathbb{R}| = 2^{\aleph_0} > \aleph_1$. Fix a set $A \subset \mathbb{R}$ of cardinality exactly $\aleph_1$ (e.g., take the image of $\aleph_1$ under any bijection $2^{\aleph_0} \to \mathbb{R}$). We prove (1) following essentially the same outline as in the proof of Proposition 8.17, but replacing ω by $\mathbb{R}$, $k + 1$ by A, and k by ω.

Claim 8.22. *For each $x \in \mathbb{R}$, there exist a, $b \in A$ and $i \in \omega$ such that:*

- *$a < b$, and*
- *$f(a + x) = f(b + x) = i$.*

Proof. Otherwise $a \mapsto f(x + a)$ would be an injection $A \to \omega$, which is impossible since $|A| = \aleph_1$. ⊠

For each $x \in \mathbb{R}$, let $\tau(x) = (a, b, i) \in A \times A \times \omega$ be an arbitrary triple satisfying the conditions of Claim 8.22 (here we really must use AC).

Claim 8.23. *There exist reals $x < y < z$ such that $\tau(x) = \tau(y) = \tau(z)$.*

Proof. Otherwise $x \mapsto \tau(x)$ is an ($\leqslant 2$)-to-1 function from $\mathbb{R}$ to $A \times A \times \omega$, implying that $2^{\aleph_0} \leqslant 2 \otimes \aleph_1 \otimes \aleph_1 \otimes \aleph_0 = \aleph_1$, which contradicts our assumption that CH fails. ☒

Claim 8.24. *There exist reals $x < y$ such that $\tau(x) = \tau(y) = (a, b, i)$ and $y - x \neq b - a$.*

Proof. Same as Claim 8.20. ☒

Let $x < y$ be such that $\tau(x) = \tau(y) = (a, b, i)$ and $y - x \neq b - a$. Then, exactly as in the proof of Proposition 8.17, the four numbers $x + a$, $y + b$, $x + b$, $y + a$ are as desired.

(1) $\Longrightarrow$ (2): We start by introducing some general notation. For a set $X \subseteq \mathbb{R}$, define a sequence of sets $(X_n)_{n<\omega}$ recursively as follows:

$$X_0 \ :=\ X \cup \{0\}, \qquad X_{n+1} \ :=\ X_n \cup \{a + b,\ a - b \ :\ a,\, b \in X\}.$$

Let $\langle X \rangle := \bigcup_{n<\omega} X_n$.[vi]

Lemma 8.25. *The operation $X \mapsto \langle X \rangle$ has the following properties:*

- *$X \subseteq \langle X \rangle$,*
- *if $X \subseteq Y$, then $\langle X \rangle \subseteq \langle Y \rangle$,*
- *$\langle X \rangle$ is closed under addition and subtraction,*
- *if X is countable, then $\langle X \rangle$ is countable.*

Proof. We only verify the last bullet point, leaving the rest as exercises. The set $X_0 = X$ is countable by assumption. If X_n is countable, then $|X_{n+1}| \leqslant 2 \otimes |X_n| \otimes |X_n| \leqslant \aleph_0$, so $|X_{n+1}|$ is countable as well. Therefore, all sets X_n are countable. Hence $\langle X \rangle$ is the union of countably many countable sets, so it is also countable. ☒

Now suppose CH holds—i.e., $2^{\aleph_0} = \aleph_1$—and fix a bijection $\aleph_1 \to \mathbb{R} \colon \alpha \mapsto x_\alpha$. Our goal is to construct a function $f \colon \mathbb{R} \to \omega$ such that there are no four distinct numbers a, b, c, $d \in \mathbb{R}$ with $f(a) = f(b) = f(c) = f(d)$ and $a + b = c + d$. To this end, let $X_\alpha := \{x_\beta \ :\ \beta < \alpha\}$. It follows from the first two bullet points in Lemma 8.25 that $(\langle X_\alpha \rangle)_{\alpha<\aleph_1}$ is a non-decreasing sequence of sets with $\bigcup_{\alpha<\aleph_1} \langle X_\alpha \rangle = \mathbb{R}$. Note that for each $\alpha < \aleph_1$, $|X_\alpha| = |\alpha| < \aleph_1$, i.e., every set X_α is countable. By Lemma 8.25, $\langle X_\alpha \rangle$ is countable as well. Therefore, using the Axiom of Choice, we may fix an injection $f_\alpha \colon \langle X_\alpha \rangle \to \omega$. Now we define $f \colon \mathbb{R} \to \omega$ as follows:

$$f(x) \ :=\ f_\alpha(x), \quad \text{where } \alpha < \aleph_1 \text{ is the least ordinal such that } x \in \langle X_\alpha \rangle.$$

Suppose we have four distinct real numbers a, b, c, d with $a + b = c + d$, and let α, β, γ, $\delta < \aleph_1$ be the least ordinals such that $a \in \langle X_\alpha \rangle$, $b \in \langle X \rangle_\beta$, $c \in \langle X \rangle_\gamma$, and $d \in \langle X \rangle_\delta$.

Claim 8.26. *At least two of α, β, γ, δ are equal.*

Proof. Assume for concreteness that $\alpha = \max\{\alpha, \beta, \gamma, \delta\}$ and let $\varepsilon := \max\{\beta, \gamma, \delta\}$. Clearly, $\varepsilon \leqslant \alpha$. On the other hand, b, c, $d \in \langle X_\varepsilon \rangle$, which implies that $a = c + d - b \in \langle X_\varepsilon \rangle$ as well, because $\langle X_\varepsilon \rangle$ is closed under addition and subtraction. Therefore, $\alpha \leqslant \varepsilon$, and thus $\alpha = \varepsilon$, as claimed. ☒

If, say, $\alpha = \beta$, then $f(a) = f_\alpha(a) \neq f_\alpha(b) = f(b)$ because $f_\alpha \colon \langle X_\alpha \rangle \to \omega$ is injective. Similarly, not all of $f(a)$, $f(b)$, $f(c)$, and $f(d)$ are the same whenever any two of α, β, γ, δ are equal. Hence statement (1) fails for f, which is what we wanted. ■

Exercise 8.6 (Fox)**.** For each $2 \leqslant n < \omega$, the following statements are equivalent.

[vi]The reader may recognize that $\langle X \rangle$ is simply the subgroup of $(\mathbb{R}, +)$ generated by X.

(i) For every function $f\colon \mathbb{R} \to \omega$, there exist distinct numbers x, y, z_1, …, $z_n \in \mathbb{R}$ such that $f(x) = f(y) = f(z_1) = \cdots = f(z_n)$ and $x + (n-1)y = z_1 + \cdots + z_n$.

(ii) $2^{\aleph_0} \geqslant \aleph_n$.

8.4. Cofinality

In this section we go back to working in ZF^-.

Example 8.27. Consider the cardinal $\aleph_\omega$. By definition,

$$\aleph_\omega \;=\; \sup_{n<\omega} \aleph_n \;=\; \bigcup_{n<\omega} \aleph_n.$$

This means that $\aleph_\omega$ can be expressed as a union of *countably many sets of strictly smaller cardinality*. The notion of cofinality is a convenient tool for understanding phenomena of this sort.

Definition 8.28. Let α and β be ordinals. A function $f\colon \alpha \to \beta$ is called **cofinal** (**in** β) if for each $\delta < \beta$ there is some $\gamma < \alpha$ with $f(\gamma) \geqslant \delta$. The **cofinality** of an ordinal β, denoted $\mathrm{cf}(\beta)$, is the least ordinal α such that there is a cofinal function $f\colon \alpha \to \beta$.

Exercise 8.7. Show that if $\alpha, \beta \in \mathbf{Ord}$ and β is a limit ordinal, then $f\colon \alpha \to \beta$ is cofinal if and only if $\sup \mathrm{ran}(f) = \beta$.

Example 8.29. We have

$$\mathrm{cf}(0) = 0, \quad \mathrm{cf}(1) = 1, \quad \mathrm{cf}(100) = 1, \quad \mathrm{cf}(\omega) = \omega, \quad \mathrm{cf}(\omega + 100) = 1, \quad \mathrm{cf}(\omega + \omega) = \omega.$$

Also, as shown in Example 8.27, we have $\mathrm{cf}(\aleph_\omega) = \omega$.

Exercise 8.8 (important)**.** If β is a successor, then $\mathrm{cf}(\beta) = 1$, while if β is a limit, then $\mathrm{cf}(\beta) \geqslant \omega$.

Exercise 8.9 (important)**.** Let $\beta \in \mathbf{Ord}$. Show that $\mathrm{cf}(\beta)$ is a cardinal and $\mathrm{cf}(\beta) \leqslant |\beta| \leqslant \beta$.

Exercise 8.10. Since ω^ω is a countable limit ordinal, we have $\mathrm{cf}(\omega^\omega) = \omega$. Give an explicit example of a cofinal function $\omega \to \omega^\omega$.

The next two lemmas are useful tools for computing cofinalities.

Lemma 8.30. *Let β be an ordinal. Then there is a strictly increasing cofinal function $\mathrm{cf}(\beta) \to \beta$.*

Proof. Let $f\colon \mathrm{cf}(\beta) \to \beta$ be an arbitrary cofinal function. Consider the set

$$S \;\coloneqq\; \{\gamma < \mathrm{cf}(\beta) \;:\; f(\gamma) > f(\delta) \text{ for all } \delta < \gamma\}.$$

The function $f{\restriction}S\colon S \to \beta$ is strictly increasing and cofinal (why?). Since S is well-ordered, there is a strictly increasing bijection $g\colon \alpha \to S$ for some ordinal α. The existence of a strictly increasing function from α to $\mathrm{cf}(\beta)$ shows that $\alpha \leqslant \mathrm{cf}(\beta)$; on the other hand, the function $f \circ g\colon \alpha \to \beta$ is cofinal, and hence $\alpha \geqslant \mathrm{cf}(\beta)$. Therefore, $\alpha = \mathrm{cf}(\beta)$ and the function $f \circ g$ is as desired. ■

Lemma 8.31. *Let α and β be ordinals. If there is a strictly increasing cofinal function $f\colon \alpha \to \beta$, then $\mathrm{cf}(\alpha) = \mathrm{cf}(\beta)$.*

Proof. Let $g\colon \mathrm{cf}(\alpha) \to \alpha$ be a cofinal function. We claim that $f \circ g\colon \mathrm{cf}(\alpha) \to \beta$ is cofinal in β, from which it follows that $\mathrm{cf}(\beta) \leqslant \mathrm{cf}(\alpha)$. Indeed, take any $\varepsilon < \beta$. Since f is cofinal, there is $\delta < \alpha$ such that $f(\delta) \geqslant \varepsilon$. Similarly, since g is cofinal, there is $\gamma < \mathrm{cf}(\alpha)$ such that $g(\gamma) \geqslant \delta$. It remains to note that since f is increasing, $(f \circ g)(\gamma) = f(g(\gamma)) \geqslant f(\delta) \geqslant \varepsilon$.

Now consider any cofinal function $h\colon \mathrm{cf}(\beta) \to \beta$. Since f is cofinal in β, given any $\gamma < \mathrm{cf}(\beta)$, there is some $\delta < \alpha$ such that $f(\delta) \geqslant h(\gamma)$. Thus, we can define $\varphi\colon \mathrm{cf}(\beta) \to \alpha$ as follows:

$$\varphi(\gamma) \;\coloneqq\; \min\{\delta < \alpha \;:\; f(\delta) \geqslant h(\gamma)\}.$$

We claim that φ is cofinal in α, proving that $\mathrm{cf}(\beta) \geqslant \mathrm{cf}(\alpha)$. Indeed, consider any $\delta < \alpha$. Since h is cofinal in β, there is some $\gamma < \mathrm{cf}(\beta)$ with $h(\gamma) \geqslant f(\delta)$. Then $\varphi(\gamma) \geqslant \delta$ (why?), and we are done. ■

Exercise 8.11. Show that the operation cf is **idempotent**, i.e., for each $\beta \in \mathbf{Ord}$, we have

$$\mathrm{cf}(\mathrm{cf}(\beta)) = \mathrm{cf}(\beta).$$

Exercise 8.12. Show that if α is a limit ordinal, then $\mathrm{cf}(\aleph_\alpha) = \mathrm{cf}(\alpha)$.

Example 8.32. As observed before, we have $\mathrm{cf}(\aleph_\omega) = \mathrm{cf}(\omega) = \omega$. Similarly,

$$\mathrm{cf}(\aleph_{\aleph_{\omega^2}}) \;=\; \mathrm{cf}(\aleph_{\omega^2}) \;=\; \mathrm{cf}(\omega^2) \;=\; \omega.$$

By Exercise 8.12, we know that $\mathrm{cf}(\aleph_\alpha) = \mathrm{cf}(\alpha)$ if α is a limit ordinal. What happens if α is a successor? For instance, what is $\mathrm{cf}(\aleph_1)$? The answer (under AC) is given by the following theorem:

Theorem 8.33 (ZFC^-)**.** *Let κ be an infinite cardinal. Then* $\mathrm{cf}(\kappa^+) = \kappa^+$.

Proof. Let $f\colon \alpha \to \kappa^+$ be a cofinal function. Then we can write

$$\kappa^+ \;=\; \sup \mathrm{ran}(f) \;=\; \bigcup_{\beta<\alpha} f(\beta). \tag{8.1}$$

For each $\beta < \alpha$, we have $f(\beta) < \kappa^+$, and hence $|f(\beta)| < \kappa^+$, from which it follows that $|f(\beta)| \leqslant \kappa$. Therefore, (8.1) expresses κ^+ as a union of $|\alpha|$-many sets of cardinality at most κ, and hence

$$\kappa^+ \;\leqslant\; |\alpha| \otimes \kappa \;=\; \max\{|\alpha|,\, \kappa\},$$

by Theorem 8.9. This implies that $\alpha \geqslant |\alpha| \geqslant \kappa^+$, as desired. ■

Example 8.34. Under AC, we have $\mathrm{cf}(\aleph_1) = \aleph_1$, $\mathrm{cf}(\aleph_{\omega+5}) = \aleph_{\omega+5}$, and $\mathrm{cf}(\aleph_{\aleph_{\aleph_3}}) = \aleph_3$.

Remark 8.35. Perhaps somewhat surprisingly, without AC Theorem 8.33 may fail, even though it talks about cardinals, which are by definition well-ordered. In fact, under some standard assumptions, Moti Gitik showed that, without AC, it is possible that all infinite cardinals have cofinality ω!

Definition 8.36. An infinite cardinal κ is **regular** if $\mathrm{cf}(\kappa) = \kappa$; otherwise, κ is **singular**.

Thus, Theorem 8.33 asserts that infinite successor cardinals are regular.

Definition 8.37. A cardinal κ is called **weakly inaccessible** if $\kappa > \omega$, κ is regular, and κ is a limit cardinal (i.e., $\kappa > \lambda^+$ for all cardinals $\lambda < \kappa$). A cardinal κ is called **strongly inaccessible** (or just **inaccessible**) if $\kappa > \omega$, κ is regular, and $\kappa > 2^\lambda$ for all cardinals $\lambda < \kappa$.

Let κ be a weakly inaccessible cardinal. We can write $\kappa = \aleph_\alpha$ for some (limit) ordinal α. Then

$$\kappa \;=\; \mathrm{cf}(\kappa) \;=\; \mathrm{cf}(\aleph_\alpha) \;=\; \mathrm{cf}(\alpha) \;\leqslant\; \alpha \;\leqslant\; \kappa,$$

so $\kappa = \alpha$. In other words, κ satisfies $\kappa = \aleph_\kappa$, i.e., κ is a fixed point of the aleph function. This property, however, is not sufficient for weak inaccessibility. For instance, the cardinal

$$\lambda \;:=\; \sup\{\aleph_0,\, \aleph_{\aleph_0},\, \aleph_{\aleph_{\aleph_0}},\, \ldots\}$$

satisfies $\lambda = \aleph_\lambda$, but $\mathrm{cf}(\lambda) = \omega$, so λ is not regular.

The word "inaccessible" is justified here because an inaccessible cardinal κ cannot be approximated from below by any sequence of smaller cardinals of length less than κ. It turns out that inaccessible cardinals must be so "large" that their existence cannot be proved within ZFC. One indication of their size is that, as we show later, if κ is an inaccessible cardinal, then the *set* V_κ is so "rich" that the structure $(V_\kappa, \in)$ satisfies all the axioms of ZFC! Inaccessibility is a basic example of what is called a "large cardinal property." A significant part of modern set theory is done under the assumption that certain "sufficiently large" inaccessible cardinals exist.

8.5. König's lemma

Lemma 8.38 (König)**.** *Let κ be an infinite cardinal. Then there is no surjection $\kappa \to {}^{\mathrm{cf}(\kappa)}\kappa$. Hence, assuming* AC*, we have $\kappa^{\mathrm{cf}(\kappa)} > \kappa$.*

PROOF. Suppose, toward a contradiction, that $\kappa \to {}^{\mathrm{cf}(\kappa)}\kappa \colon \alpha \mapsto f_\alpha$ is a surjection; that is, for each $\alpha < \kappa$, f_α is a function from $\mathrm{cf}(\kappa)$ to κ and ${}^{\mathrm{cf}(\kappa)}\kappa = \{f_\alpha : \alpha < \kappa\}$. Fix a cofinal function $g \colon \mathrm{cf}(\kappa) \to \kappa$. We define $f \colon \mathrm{cf}(\kappa) \to \kappa$ as follows. For each $\gamma < \mathrm{cf}(\kappa)$, consider the set

$$S_\gamma := \{f_\alpha(\gamma) : \alpha < g(\gamma)\} \subseteq \kappa.$$

By definition, $|S| \leqslant |g(\gamma)| < \kappa$, so the set $\kappa \setminus S_\gamma$ is nonempty. Let

$$f(\gamma) := \min(\kappa \setminus S_\gamma).$$

Since f is a function from $\mathrm{cf}(\kappa)$ to κ, there must exist some $\alpha < \kappa$ such that $f = f_\alpha$. Let $\gamma < \mathrm{cf}(\kappa)$ be an arbitrary ordinal such that $g(\gamma) > \alpha$ (such γ exists since g is cofinal in κ and κ is a limit ordinal). Then $f_\alpha(\gamma) \in S_\gamma$, while $f(\gamma) \notin S_\gamma$ by definition; this contradiction completes the proof. ■

Corollary 8.39 (ZFC$^-$)**.** $2^{\aleph_0} \neq \aleph_\omega$. *More generally, if κ is an infinite cardinal, then $\mathrm{cf}(2^\kappa) > \kappa$.*

PROOF. If $\mathrm{cf}(2^\kappa) \leqslant \kappa$, then, by König's lemma,

$$2^\kappa < (2^\kappa)^{\mathrm{cf}(2^\kappa)} \leqslant (2^\kappa)^\kappa = 2^{\kappa \otimes \kappa} = 2^\kappa,$$

a contradiction. ■

Exercise 8.13 (ZFC$^-$)**.** Let I be an arbitrary index set and let $\{A_i : i \in I\}$ and $\{B_i : i \in I\}$ be two families of sets indexed by I. Let

$$\bigsqcup\{A_i : i \in I\} := \bigcup\{A_i \times \{i\} : i \in I\}$$

denote the **disjoint union** of the sets A_i, and let

$$\prod\{B_i : i \in I\} := \{f : f \text{ is a function with } \mathrm{dom}(f) = I \text{ and } f(i) \in B_i \text{ for all } i \in I\}$$

be the **product** of the sets B_i. Suppose that for each $i \in I$, we have $|A_i| < |B_i|$. Show that

$$\left|\bigsqcup\{A_i : i \in I\}\right| < \left|\prod\{B_i : i \in I\}\right|.$$

For the remainder of this section, we work in ZFC. From Corollary 8.39, we see that the class function $F \colon \mathbf{Card} \setminus \omega \to \mathbf{Card}$ given by $F(\kappa) = 2^\kappa$ satisfies the following two conditions:

(E1) if $\kappa \leqslant \lambda$, then $F(\kappa) \leqslant F(\lambda)$,

(E2) for every infinite cardinal κ, $\mathrm{cf}(F(\kappa)) > \kappa$.

A remarkable fact, due to William Easton, is that (E1) and (E2) are the *only* constraints on the values for 2^κ when κ is a regular cardinal (i.e., an infinite cardinal such that $\mathrm{cf}(\kappa) = \kappa$). That is, if F is any class function satisfying (E1) and (E2), then ZFC is consistent with the statement that $2^\kappa = F(\kappa)$ for all regular cardinals κ.[vii] For instance, it is possible that

$$2^{\aleph_0} = \aleph_2, \quad 2^{\aleph_1} = \aleph_2, \quad 2^{\aleph_2} = \aleph_{\aleph_5}, \quad 2^{\aleph_3} = \aleph_{\aleph_{\aleph_{2024}}}, \quad \ldots$$

It is also possible that $2^{\aleph_n} = \aleph_{n+1}$ for all $n < 100$, but $2^{\aleph_{100}} = \aleph_{200}$ (for example), i.e., $\aleph_{100}$ is the least cardinal for which GCH fails.

Easton's theorem completely describes the behavior of the function $\kappa \mapsto 2^\kappa$ for regular cardinals κ. The situation with singular cardinals turns out to be much more mysterious. The first indication

[vii] We are deliberately making this statement somewhat informal; a precise formulation would take us too far outside the scope of this course.

of that was given by a theorem of Jack Silver, who showed that $\aleph_{\aleph_1}$ (or any other singular cardinal of uncountable cofinality) cannot be the least counterexample to GCH. That is,

$$2^{\aleph_\alpha} = \aleph_{\alpha+1} \text{ for all } \alpha < \aleph_1 \quad \Longrightarrow \quad 2^{\aleph_{\aleph_1}} = \aleph_{\aleph_1+1}.$$

A powerful approach to studying exponentiation of singular cardinals of *countable* cofinality is the *PCF* (*possible cofinalities*) *theory* due to Saharon Shelah. A famous result in this theory is that

$$2^{\aleph_n} < \aleph_\omega \text{ for all } n < \omega \quad \Longrightarrow \quad 2^{\aleph_\omega} < \aleph_{\aleph_4}.$$

It is conjectured that the "4" here can be replaced by a "1" (which would be best possible).

9. Problem set 3

The default axiom system for the following exercises is ZF$^-$.

Exercise 9.1. Let $(A, \prec)$ be a partially ordered set. A subset $C \subseteq A$ is called a **chain** if C is linearly ordered by $\prec$. An **upper bound** for a chain $C \subseteq A$ is an element $a \in A$ such that $c \preccurlyeq a$ for all $c \in C$. An element $a \in A$ is **maximal** if there is no $b \in A$ with $a \prec b$. The following extremely useful statement is known as **Zorn's lemma**:

Lemma 9.1 (Zorn)**.** *Suppose that $(A, \prec)$ is a partially ordered set such that every chain $C \subseteq A$ has an upper bound. Then A has a maximal element.*

Use the Axiom of Choice to prove Zorn's lemma.

Exercise 9.2. Let F be a set of nonempty sets. We call a function f a **partial choice function** for F if $\mathrm{dom}(f) \subseteq F$ and for all $x \in \mathrm{dom}(f)$, we have $f(x) \in x$. Let $\mathbb{P}_F$ denote the set of all partial choice functions for F, equipped with the subset ordering $\subset$. (Recall that functions are sets of pairs, so it makes sense to write $f \subset g$ for functions f and g.)

- *(a)* Show that every chain C in the partially ordered set $(\mathbb{P}_F, \subset)$ has an upper bound.
- *(b)* Conclude that Zorn's lemma implies the Axiom of Choice.

Exercise 9.3. This is a problem about ordinal arithmetic.

- *(a)* Let α be a nonzero ordinal. Show that α is a limit if and only if $2 \cdot \alpha = \alpha$.
- *(b)* Let α be an ordinal. Show that $\alpha \geqslant \omega$ if and only if $2 \cdot \alpha < \alpha \cdot 2$.
- *(c)* Which one is greater: $(\omega + 1)^\omega$ or $\omega^{\omega+1}$?

Exercise 9.4. Let α and β be ordinals. Recall that the ordinal α^β is defined recursively by:

$$\alpha^\beta \;\coloneqq\; \begin{cases} 1 & \text{if } \beta = 0, \\ \alpha^\gamma \cdot \alpha & \text{if } \beta = \gamma + 1, \\ \sup_{\gamma < \beta} \alpha^\gamma & \text{if } \beta \text{ is a limit.} \end{cases}$$

In this problem we establish a "concrete" representation for the order type α^β.

For a function $f \colon \beta \to \alpha$, its **support** is the set $\mathrm{supp}(f) \coloneqq \{\gamma < \beta \,:\, f(\gamma) \neq 0\}$. Let

$$\mathbb{F}(\beta, \alpha) \;\coloneqq\; \{f \in {}^\beta\alpha \,:\, \mathrm{supp}(f) \text{ is finite}\}.$$

We equip the set $\mathbb{F}(\beta, \alpha)$ with the **colexicographical ordering** as follows. Take any two distinct functions f, $g \in \mathbb{F}(\beta, \alpha)$. Since $\mathrm{supp}(f)$ and $\mathrm{supp}(g)$ are finite, f and g differ on only finitely many elements of β, so we can let γ be the largest ordinal such that $f(\gamma) \neq g(\gamma)$. Then

$$f \prec_{\text{colex}} g \quad :\Longleftrightarrow \quad f(\gamma) < g(\gamma).$$

Show that the ordered set $(\mathbb{F}(\beta, \alpha), \prec_{\text{colex}})$ is order-isomorphic to the ordinal α^β.

Exercise 9.5. Let A and B be sets.

- *(a)* Show that if $A \neq \varnothing$ and $A \lesssim B$, then there is a surjection $B \to A$.
- *(b)* Assuming AC, show that if there is a surjection $B \to A$, then $A \lesssim B$.

It is an open problem whether the statement in *(b)* is *equivalent* to AC.

Exercise 9.6. The purpose of this exercise is to prove the following theorem of Tarski:

Theorem 9.2. AC *is equivalent to the statement that $X \times X \approx X$ for every infinite set X.*

We already know that under AC, $|X \times X| = |X|$ for all infinite X. Now assume that every infinite set X satisfies $X \times X \approx X$ (we will call that the **squaring hypothesis**). Let A be an arbitrary set. Our goal is to show that A can be well-ordered, thus proving AC. If A is finite (i.e., if there is a bijection $A \to n$ for some $n < \omega$), then A can be well-ordered, so let A be infinite. Recall that by Hartogs' theorem, there is a cardinal κ such that $\kappa \not\lesssim A$.

(a) Use the squaring hypothesis to show that $A \times \kappa \lesssim A \cup \kappa$.

(b) Use an arbitrary injection $f\colon A \times \kappa \to A \cup \kappa$ to construct an injection $A \to \kappa$.

(c) Conclude that A can be well-ordered.

An amusing anecdote is that when Tarski tried to publish his proof of Theorem 9.2 in 1924, it was rejected by two (rather famous) referees: Fréchet and Lebesgue. Fréchet said that an equivalence of two well-known propositions is not a new result, while Lebesgue said that an equivalence between two false propositions is not interesting.

10. Comparing set sizes without AC

10.1. Overview

In this section we will work in the axiom system ZF^-. Since we are not assuming AC, we shall use the following formulation of the Generalized Continuum Hypothesis:

> If X is an infinite set and $X \lesssim A \lesssim \mathcal{P}(X)$, then $X \approx A$ or $A \approx \mathcal{P}(X)$.

The ultimate goal of this section is to prove the following theorem:

Theorem 10.1 (Sierpiński)**.** GCH *implies* AC*.*

Our proof will rely on the following result of Tarski (Theorem 9.2):

> AC is equivalent to the statement that $X \times X \approx X$ for every infinite set X.

Here's the idea behind the proof of Theorem 10.1. Assume GCH. We wish to show, given any infinite set X, that $X \approx X \times X$. It is, of course, clear that $X \lesssim X \times X$. If we could show that

$$(1)\ X \times X \lesssim \mathcal{P}(X) \qquad \text{and} \qquad (2)\ \mathcal{P}(X) \not\lesssim X \times X,$$

then GCH will give us $X \approx X \times X$, as desired. Of these two statements, the second one is in some sense more "profound," and the majority of this section will be devoted to proving it. Along the way, we will encounter a number of techniques and ideas that are generally helpful when comparing sizes of sets without assuming the Axiom of Choice.

For a set X, let ${}^{<\omega}X$ denote the set of all finite sequences of the elements of X:

$${}^{<\omega}X := \bigcup_{n<\omega} {}^{n}X.$$

The central technical result in this section is the following theorem of Halbeisen and Shelah:

Theorem 10.2 (Halbeisen–Shelah)**.** *Let X be a set such that $\omega \lesssim X$. Then $\mathcal{P}(X) \not\lesssim {}^{<\omega}X$.*

From Theorem 10.2, we will derive the following:

Theorem 10.3 (Specker)**.** *Let X be a set such that $5 \lesssim X$. Then $\mathcal{P}(X) \not\lesssim X \times X$.*

Although $X \times X \lesssim {}^{<\omega}X$, Specker's theorem is not simply a special case of the Halbeisen–Shelah theorem. For one, the set X in Specker's theorem is allowed to be finite. More importantly, even if X is infinite, this does not necessarily mean (without assuming some part of the Axiom of Choice) that $\omega \lesssim X$; see Exercise 6.2.

10.2. Warm-up

We start with the following very modest strengthening of Cantor's theorem:

Lemma 10.4. *If X is an infinite set, then $\mathcal{P}(X) \not\lesssim X \sqcup 1$.*

Here $\sqcup$ denotes, as usual, disjoint union.

Proof. For convenience, assume that $0 \notin X$ and replace $X \sqcup 1$, which technically is equal to $(X \times \{0\}) \cup (1 \times \{1\})$, simply by $X \cup \{0\}$. The lemma is easy to verify if $\omega \lesssim X$. Indeed, suppose $\omega \to X : n \mapsto x_n$ is an injection. Define a function $f : X \cup \{0\} \to X$ as follows:

$$f(x) := \begin{cases} x_0 & \text{if } x = 0, \\ x_{n+1} & \text{if } x = x_n, \\ x & \text{otherwise.} \end{cases}$$

Then f is a bijection, so $X \cup \{0\} \approx X$ and we are done since $\mathcal{P}(X) \not\lesssim X$ by Cantor's theorem. Unfortunately, sans AC, there may exist infinite sets X such that $\omega \not\lesssim X$. However, we will argue that every *counterexample to the lemma* must satisfy $\omega \lesssim X$, which will complete the proof.

Suppose $f\colon \mathcal{P}(X) \to X \cup \{0\}$ is an injection. We may assume, without loss of generality, that $f(X) = 0$ (why?), so f injects $\mathcal{P}(X) \setminus \{X\}$ into X. Define a sequence $\omega \to X\colon n \mapsto x_n$ recursively by

$$x_n := f(\{x_i : i < n\}).$$

Since X is infinite, $X \neq \{x_i : i < n\}$, hence $x_n \in X$. Furthermore, since f is injective, the elements $x_0, x_1, \ldots$ are pairwise distinct. Therefore, $\omega \lesssim X$, and the proof is complete. ■

Corollary 10.5. *Assume* GCH. *If X is an infinite set, then $X \approx X \sqcup 1$ and hence $\omega \lesssim X$.*

Proof. Clearly, $X \lesssim X \sqcup 1$. Also, $X \sqcup 1 \lesssim \mathcal{P}(X)$ (why?). By GCH, either $X \approx X \sqcup 1$ (and we win), or $X \sqcup 1 \approx \mathcal{P}(X)$. The latter case is impossible due to Lemma 10.4. ■

10.3. Uniform bijections between ordinals and their powers

Consider an infinite ordinal α. We already know that $\alpha \approx \alpha \times \alpha$. Namely, we have

$$\alpha \approx |\alpha| \approx |\alpha| \times |\alpha| \approx \alpha \times \alpha. \tag{10.1}$$

But can we write down an *explicit* bijection between α and $\alpha \times \alpha$? Note that our proof that $\kappa = \kappa \otimes \kappa$ for an infinite cardinal κ (see Theorem 8.4) actually *does* give a concrete bijection $\kappa \times \kappa \to \kappa$ (exercise!), so the bijection between $|\alpha|$ and $|\alpha| \times |\alpha|$ in (10.1) is "explicit." Unfortunately, there is no "canonical" choice for a bijection from α to $|\alpha|$ (that is why, for example, cofinality may behave strangely if AC is not assumed). Nevertheless, in this section we will prove that there *is* an explicit choice of a bijection $\alpha \times \alpha \to \alpha$, in the following sense:

Lemma 10.6. *There is a class function* $\mathbf{Ord} \setminus \omega \to \mathcal{U}\colon \alpha \mapsto q_\alpha$ *defined by a formula without parameters such that for every infinite ordinal α, q_α is a bijection from $\alpha \times \alpha$ to α.*

From this, we will deduce an apparent strengthening:

Theorem 10.7. *There is a class function* $\mathbf{Ord} \setminus \omega \to \mathcal{U}\colon \alpha \mapsto p_\alpha$ *defined by a formula without parameters such that for every infinite ordinal α, p_α is a bijection from ${}^{<\omega}\alpha$ to α.*

Exercise 10.1. Show (before reading the rest) that if α is an infinite ordinal, then $\alpha \approx {}^{<\omega}\alpha$.

The main tool we use to prove Lemma10.6 and Theorem 10.7 is the following result of Cantor:

Theorem 10.8 (Cantor normal form)**.** *For every ordinal α, there exist a unique finite sequence of ordinals $\beta_1 > \cdots > \beta_k$ and a sequence of positive integers $d_1, \ldots, d_k$ such that*

$$\alpha = \omega^{\beta_1} \cdot d_1 + \cdots + \omega^{\beta_k} \cdot d_k.$$

(*The operations are in ordinal arithmetic.*) *This expression is called the* **Cantor normal form** *of α.*

Remark 10.9. We have already seen something similar in connection with Goodstein's theorem (see §7.3): the Cantor normal form of α is like a "base-ω" expansion of α with digits $d_1, \ldots, d_k$.

Remark 10.10. Note that in Theorem 10.8, we always have $\alpha \geqslant \beta_1$ (why?). On the other hand, it can happen that $\alpha = \beta_1$. For instance, the Cantor normal form of the ordinal

$$\varepsilon_0 := \sup \left\{\omega, \omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \ldots\right\}$$

is $\varepsilon_0 = \omega^{\varepsilon_0}$. As an exercise, what is the Cantor normal form of $\aleph_1$?

PROOF. The proof is essentially the same as the proof that every natural number has a base-b expansion, but with b replaced by ω. We argue by induction on α. If $\alpha = 0$, then we take $k = 0$ (the Cantor normal form is empty), so assume $\alpha > 0$. Consider the set

$$S \coloneqq \{\beta : \omega^\beta \leqslant \alpha\}.$$

We claim that S has a largest element. Indeed,

$$\omega^{\sup S} = \sup\{\omega^\beta : \beta \in S\} \leqslant \alpha,$$

so $\sup S \in S$. Let $\beta \coloneqq \max S$ and let d be the largest positive natural number such that $\omega^\beta \cdot d \leqslant \alpha$. (Such d exists since $\omega^\beta \cdot \omega = \omega^{\beta+1} > \alpha$ by the choice of β). Now we can write

$$\alpha = \omega^\beta \cdot d + \alpha'$$

for some (unique) ordinal $\alpha' < \omega^\beta \leqslant \alpha$. By the inductive assumption, α' has a Cantor normal form

$$\alpha' = \omega^{\beta_1} \cdot d_1 + \cdots + \omega^{\beta_k} \cdot d_k.$$

By the choice of β and d, we have $\beta > \beta_1$, hence

$$\alpha = \omega^\beta \cdot d + \omega^{\beta_1} \cdot d_1 + \cdots + \omega^{\beta_k} \cdot d_k$$

is a Cantor normal form for α. The uniqueness of the Cantor normal form is left as an exercise. ■

Fix an arbitrary bijection $f \colon \omega \times \omega \to \omega$ with the property that $f(0,0) = 0$ definable by a formula without parameters. For example, the following f works (exercise!):

$$f(n,m) \coloneqq \frac{(n+m)(n+m+1)}{2} + n.$$

For any two ordinals α, β, we define their **fusion** $\alpha * \beta$ as follows: By Theorem 10.8, there exist a finite sequence $\gamma_1 > \cdots > \gamma_k$ of ordinals and natural numbers $c_1, \ldots, c_k, d_1, \ldots, d_k$ (some of which may be zero) such that

$$\alpha = \omega^{\gamma_1} \cdot c_1 + \cdots + \omega^{\gamma_k} \cdot c_k \qquad \text{and} \qquad \beta = \omega^{\gamma_1} \cdot d_1 + \cdots + \omega^{\gamma_k} \cdot d_k.$$

Then $\alpha * \beta$ is the ordinal

$$\alpha * \beta \coloneqq \omega^{\gamma_1} \cdot f(c_1, d_1) + \cdots + \omega^{\gamma_k} \cdot f(c_k, d_k).$$

(This is well-defined because $f(0,0) = 0$.) For instance,

$$(\omega^2 \cdot 7 + 3) * (\omega + 1) = \omega^2 \cdot f(7,0) + \omega \cdot f(0,1) + f(3,1).$$

Exercise 10.2. Show that the class function $\mathbf{Ord} \times \mathbf{Ord} \to \mathbf{Ord} \colon (\alpha, \beta) \mapsto \alpha * \beta$ is a bijection.

Furthermore, if α, $\beta < \omega^\gamma$, then $\alpha * \beta < \omega^\gamma$ as well, and so the function

$$\omega^\gamma \times \omega^\gamma \to \omega^\gamma \colon (\alpha, \beta) \to \alpha * \beta$$

is a bijection. With these preliminary observations, we are now ready to prove Lemma 10.6.

PROOF *of Lemma 10.6.* Let α be an infinite ordinal. Using the Cantor normal form, we can write $\alpha = \omega^\beta \cdot d + \alpha'$, where d is a positive natural number, β and α' are ordinals, and $\alpha' < \omega^\beta$. Since α is infinite, $\beta \geqslant 1$. There is an obvious bijection between $\alpha = \omega^\beta \cdot d + \alpha'$ and $\alpha' + \omega^\beta \cdot d$. But

$$\alpha' + \omega^\beta \cdot d = (\alpha' + \omega^\beta) + \omega^\beta \cdot (d-1) = \omega^\beta + \omega^\beta \cdot (d-1) = \omega^\beta \cdot d,$$

where we use the result of the following exercise:

Exercise 10.3. If γ, β are ordinals and $\gamma < \omega^\beta$, then $\gamma + \omega^\beta = \omega^\beta$.

Next, there is a natural bijection $\omega^\beta \cdot d \approx d \cdot \omega^\beta$. But $d \cdot \omega^\beta = \omega^\beta$, because $\beta \geqslant 1$ and hence ω^β is a limit ordinal. Thus, we have constructed a bijection from α to ω^β:

$$\alpha \;=\; \omega^\beta \cdot d + \alpha' \;\approx\; \alpha' + \omega^\beta \cdot d \;=\; \omega^\beta \cdot d \;\approx\; d \cdot \omega^\beta \;=\; \omega^\beta.$$

The function $\omega^\beta \times \omega^\beta \to \omega^\beta \colon (\gamma, \delta) \mapsto \gamma * \delta$ is a bijection, which we can combine with the above bijection $\alpha \to \omega^\beta$ to finally obtain the desired bijection $q_\alpha \colon \alpha \times \alpha \to \alpha$:

$$\alpha \times \alpha \;\approx\; \omega^\beta \times \omega^\beta \;\approx \omega^\beta \;\approx \alpha. \qquad \blacksquare$$

PROOF *of Theorem 10.7.* Let $\alpha \in \mathbf{Ord} \setminus \omega$. We wish to construct a bijection $p_\alpha \colon {}^{<\omega}\alpha \to \alpha$. To begin with, note that it suffices to construct an *injection* ${}^{<\omega}\alpha \to \alpha$, since there is an obvious injection $\alpha \to {}^{<\omega}\alpha$, and the proof of the Cantor/Schröder–Bernstein theorem (Theorem 6.3) can be used to assemble a bijection out of two injections.

For each $n < \omega$, we shall fix an injection $\varphi_n \colon {}^{n}\alpha \to \alpha$ (in fact, for all $n \geqslant 1$, φ_n will be a bijection). To begin with, ${}^{0}\alpha = \{\varnothing\}$ and we can, for example, set $\varphi_0(\varnothing) := 0$. For $n = 1$, we set $\varphi_1 \colon \alpha \to \alpha$ to be the identity map.[viii] For larger n, we will use the bijection $q_\alpha \colon \alpha \times \alpha \to \alpha$ from Lemma 10.6. For $n = 2$, we can just set $\varphi_2 := q_\alpha$. For $n = 3$, we need to apply q_α twice:

$$\varphi_3 \colon \alpha \times \alpha \times \alpha \to \alpha \colon (\beta_1, \beta_2, \beta_3) \mapsto q_\alpha(q_\alpha(\beta_1, \beta_2), \beta_3).$$

In general, we define the function $\varphi_{n+1} \colon {}^{n+1}\alpha \to \alpha$ recursively by

$$\varphi_{n+1} \colon {}^{n+1}\alpha \to \alpha \colon (\beta_1, \ldots, \beta_{n+1}) \mapsto q_\alpha(\varphi_n(\beta_1, \ldots, \beta_n), \beta_{n+1}).$$

Now we combine the functions φ_n to produce an injection $\varphi \colon {}^{<\omega}\alpha \to \omega \times \alpha$ by setting

$$\varphi(s) \;:=\; (n, \varphi_n(s)) \qquad \text{for all } n < \omega \text{ and } s \in {}^{n}\alpha.$$

And now we are done, as the following diagram illustrates:

$${}^{<\omega}\alpha \xrightarrow{\text{injection}} \omega \times \alpha \subseteq \alpha \times \alpha \xrightarrow{q_\alpha} \alpha.$$

The proof of Theorem 10.7 is complete. $\blacksquare$

10.4. The Halbeisen–Shelah theorem

PROOF *of Theorem 10.2.* Let X be a set such that $\omega \lesssim X$. Fix an injection $\omega \to X \colon n \mapsto a_n$ (in other words, a_0, a_1, … is an infinite sequence of distinct elements of X). Suppose, toward a contradiction, that there is an injection $f \colon \mathcal{P}(X) \to {}^{<\omega}X$. We will use f to construct an injective class function $\Phi \colon \mathbf{Ord} \to X$, yielding the desired contradiction.

The definition of the class function Φ is recursive. For each $n < \omega$, we use that $\omega \lesssim X$ and set $\Phi(n) := a_n$. Now let α be an infinite ordinal and suppose that the values $\Phi(\beta)$ for all $\beta < \alpha$ are already determined. Let $S := \Phi[\alpha] = \{\Phi(\beta) \,:\, \beta < \alpha\}$. The function Φ establishes a bijection between α and S, so we can use Theorem 10.7 to get an explicit bijection $h \colon {}^{<\omega}S \to S$:

$${}^{<\omega}S \;\to\; {}^{<\omega}\alpha \;\xrightarrow{p_\alpha}\; \alpha \;\xrightarrow{\Phi}\; S.$$

This already shows that $S \neq X$. Indeed, if S were equal to X, then, by composing f with h, we would obtain an injection $\mathcal{P}(X) \to X$, which is impossible by Cantor's theorem:

$$\mathcal{P}(X) \xrightarrow{f} {}^{<\omega}X \;=\; {}^{<\omega}S \xrightarrow{h} S \;=\; X.$$

It might be tempting to conclude that, as $X \setminus S \neq \varnothing$, we can just take any element $x \in X \setminus S$ as the value for $\Phi(\alpha)$; unfortunately, we would need AC to "pick out" this x. Thus, what we have to do now is to describe how to choose a *specific* element from $X \setminus S$. It turns out that simply repeating the proof of Cantor's theorem in this setting does the trick.

[viii] Strictly speaking, ${}^{1}\alpha$ is not α itself, but the set of all one-element sequences of elements of α. Similarly, ${}^{2}\alpha \neq \alpha \times \alpha$ since elements of ${}^{2}\alpha$ are functions from 2 to α, not ordered pairs of elements of α. Nevertheless, we will ignore these annoying distinctions as there are obvious bijections ${}^{1}\alpha \approx \alpha$, ${}^{2}\alpha \approx \alpha \times \alpha$, etc.

Specifically, let Cantor be the class function from Cantor's Theorem 6.4. That is, Cantor is defined by a formula without parameters and, given any set A and a function $\varphi\colon A \to \mathcal{P}(A)$, we have

$$\mathsf{Cantor}(A, \varphi) \in \mathcal{P}(A)\backslash\mathrm{ran}(\varphi).$$

Define a function $\varphi\colon S \to \mathcal{P}(S)$ as follows:

$$\varphi(s) := \begin{cases} S' & \text{if } S' \subseteq S,\ f(S') \in {}^{<\omega}S, \text{ and } h(f(S')) = s, \\ S & \text{if no such } S' \text{ exists.} \end{cases}$$

(This is a well-defined function because $f\colon \mathcal{P}(X) \to {}^{<\omega}X$ is injective and $h\colon {}^{<\omega}S \to S$ is bijective, which implies that a set S' as above must be unique if it exists.) Let

$$C := \mathsf{Cantor}(S, \varphi).$$

By construction, C is a subset of S that is not in the range of φ. This implies that $f(C) \notin {}^{<\omega}S$ (otherwise, letting $s := h(f(C))$, we would have $\varphi(s) = C$). This means that $f(C) = (x_1, \ldots, x_k)$, where $k \in \omega$ and at least one of $x_1, \ldots, x_k$ is an element of $X\backslash S$. Thus, we can set

$$\Phi(\alpha) := x_i, \text{ where } i \text{ is the least index such that } x_i \in X\backslash S.$$

This finishes the definition of the class function Φ and hence the proof of Theorem 10.2. ■

Now we can deduce Specker's theorem from the Halbeisen–Shelah theorem.

PROOF *of Theorem 10.3.* Let X be a set with $5 \lesssim X$. We wish to show that there is no injection $\mathcal{P}(X) \to X \times X$. If X is finite, this statement follows from the following exercise:

Exercise 10.4. Let $5 \leqslant n < \omega$. Show that $2^n > n^2$.

Thus, we may assume X is infinite. If $\omega \lesssim X$, then we are done by Theorem 10.2. We will now show how to construct an injection $\omega \to X\colon n \mapsto a_n$ from a given injection $f\colon \mathcal{P}(X) \to X \times X$, in a manner similar to the construction in the proof of Lemma 10.4.

So, let X be infinite and let $f\colon \mathcal{P}(X) \to X \times X$ be injective. We choose distinct values a_0, a_1, a_2, a_3, $a_4 \in X$ arbitrarily. Now suppose that $5 \leqslant n \in \omega$ and for all $m < n$, the value a_m is already determined. We have to find a specific element of X distinct from $a_0, \ldots, a_{n-1}$ and call it a_n. To that end, let $S := \{a_m : m < n\}$. Then S is a set of size $n \geqslant 5$; hence, $|\mathcal{P}(S)| = 2^n > n^2 = |S \times S|$. This implies that there is a subset $A \subseteq S$ such that $f(A) \notin S \times S$. Furthermore, we can choose a *specific* such set A, using the following observation:

Exercise 10.5. Show that there is a function $\omega \to \mathcal{U}\colon n \mapsto \prec_n$ such that for each $n \in \omega$, $\prec_n$ is a linear ordering (and hence a well-ordering) on $\mathcal{P}(n)$.

Since S is in a bijection with n (given by the map $m \mapsto a_m$), Exercise 10.5 gives us an explicit linear ordering $\prec$ on $\mathcal{P}(S)$. Every linear ordering on a finite set is a well-ordering (exercise!), so we can take A to be the $\prec$-least element of $\mathcal{P}(S)$ satisfying $f(A) \notin S \times S$. Then $f(A) = (x_1, x_2)$ with at least one of x_1, x_2 in not in S. This allows us to set

$$a_n := \begin{cases} x_1 & \text{if } x_1 \notin S; \\ x_2 & \text{if } x_1 \in S \text{ (and hence } x_2 \notin S), \end{cases}$$

finishing the construction. ■

Exercise 10.6. Show that if X is a set such that $23 \lesssim X$, then $\mathcal{P}(X) \not\lesssim X \times X \times X \times X \times X$.

10.5. GCH implies AC

We now have all the tools to prove Theorem 10.1, i.e., that GCH implies AC.

PROOF *of Theorem 10.1.* Assume GCH and let X be an infinite set. We know from Corollary 10.5 that $X \approx X \sqcup 1$ and $\omega \lesssim X$.

Claim 10.11. $X \approx X \sqcup X$.

Proof. We rely on the following observation:

Exercise 10.7. Show that $\mathcal{P}(X) \sqcup \mathcal{P}(X) \approx \mathcal{P}(X \sqcup 1)$.

Using the fact that $X \sqcup 1 \approx X$, we now have

$$X \lesssim X \sqcup X \lesssim \mathcal{P}(X) \sqcup \mathcal{P}(X) \approx \mathcal{P}(X \sqcup 1) \approx \mathcal{P}(X).$$

Since $X \sqcup X \lesssim {}^{<\omega}X$ (exercise!), by the Halbeisen–Shelah theorem, $\mathcal{P}(X) \not\lesssim X \sqcup X$. By GCH, this yields $X \sqcup X \approx X$, as claimed. ⊠

Claim 10.12. $X \approx X \times X$.

Proof. The proof is very similar to the proof of the previous claim.

Exercise 10.8. Show that $\mathcal{P}(X) \times \mathcal{P}(X) \approx \mathcal{P}(X \sqcup X)$.

Using the previous claim, we obtain

$$X \lesssim X \times X \lesssim \mathcal{P}(X) \times \mathcal{P}(X) \approx \mathcal{P}(X \sqcup X) \approx \mathcal{P}(X).$$

By the Halbeisen–Shelah theorem, $\mathcal{P}(X) \not\lesssim X \times X$, which yields $X \times X \approx X$, as claimed. ⊠

Since the assertion that $X \approx X \times X$ for every infinite set X is equivalent to AC, the proof of Theorem 10.1 is complete. ■

11. Problem set 4

The default axiom system for the following exercises is ZFC, unless stated otherwise.

Exercise 11.1. In this problem, $\mathbb{R}^3 := \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ denotes, as usual, the 3-dimensional Euclidean space, i.e., the set of all ordered triples of real numbers.[ix] Show that there is a set L of pairwise disjoint straight lines in $\mathbb{R}^3$ such that $\bigcup L = \mathbb{R}^3$ and no two lines in L are parallel to each other.

Exercise 11.2. The goal of this exercise is to prove that the Continuum Hypothesis, CH, is equivalent to the following statement:

The plane $\mathbb{R}^2$ can be decomposed as $\mathbb{R}^2 = A \cup B$ so that for every horizontal (resp. vertical) line $\ell \subset \mathbb{R}^2$, the set $\ell \cap A$ (resp. $\ell \cap B$) is countable. $(\sharp)$

Here we say that a line ℓ in the plane is **horizontal** if $\ell = \{(x, c) \,:\, x \in \mathbb{R}\}$ for some fixed $c \in \mathbb{R}$; similarly, ℓ is **vertical** if $\ell = \{(c, y) \,:\, y \in \mathbb{R}\}$ for some fixed $c \in \mathbb{R}$.

(a) Show that CH implies $(\sharp)$.

For the other direction, assume $(\sharp)$ and suppose that CH fails. Fix a decomposition $\mathbb{R}^2 = A \cup B$ as in $(\sharp)$ and consider any set $S \subset \mathbb{R}$ such that $\aleph_0 < |S| < 2^{\aleph_0}$.

(b) Show that for every $x \in \mathbb{R}$, there is some $y \in S$ with $(x, y) \in A$.

(c) Show that there is $y \in S$ such that we have $(x, y) \in A$ for uncountably many $x \in \mathbb{R}$.

(d) Finish the proof that $(\sharp)$ implies CH.

Exercise 11.3.

(c) Let $(A, \prec)$ be a linearly ordered set. Show that there is a subset $B \subseteq A$ such that B is well-ordered by $\prec$ and *cofinal* in A, meaning that for all $x \in A$, there is $y \in B$ with $x \preccurlyeq y$.

(d) Let F be a set that is linearly ordered by the subset relation $\subset$. Suppose that κ is a cardinal such that $|A| < \kappa$ for all $A \in F$. Show that $|\bigcup F| \leqslant \kappa$.

(e) Give an example of a set F that is linearly ordered by the subset relation $\subset$ such that

$$\left|\bigcup F\right| > \sup\{|A| \,:\, A \in F\}.$$

Exercise 11.4. For a set X, let $[X]^{\leqslant\omega}$ denote the set of all countable subsets of X.

(c) Show that for every infinite cardinal κ, $|[\kappa]^{\leqslant\omega}| = \kappa^{\aleph_0}$.

(d) Show that for every $n < \omega$, $\aleph_{n+1}^{\aleph_0} = \aleph_{n+1} \otimes \aleph_n^{\aleph_0}$.

(e) Conclude that for every $n < \omega$, $\aleph_n^{\aleph_0} = \max\{\aleph_n, 2^{\aleph_0}\}$.

Exercise 11.5 (ZF$^-$). Prove the following "uniform" version of Cantor's theorem:

Theorem 11.1. *There is a class function Φ defined by a formula without parameters such that, given any set X and a function $f\colon \mathcal{P}(X) \to X$, we have $\Phi(X, f) = (A, B)$, where A and B are two distinct subsets of X such that $f(A) = f(B)$ (thus witnessing the non-injectivity of f).*

Exercise 11.6 (ZF). Show that the following statements are equivalent:

(i) There is a class function $\mathsf{G}\colon \mathfrak{U} \to \mathfrak{U}$ such that for every nonempty set A, $\mathsf{G}(A) \in A$.

(ii) There is a bijective class function $\mathbf{Ord} \to \mathfrak{U}$.

(iii) For every proper class $\mathcal{C}$, there is a bijective class function $\mathbf{Ord} \to \mathcal{C}$.

(iv) For every two proper classes $\mathcal{C}$, $\mathcal{D}$, there is a bijective class function $\mathcal{C} \to \mathcal{D}$.

(v) AC holds and for every proper class $\mathcal{C}$, there is an injective class function $\mathbf{Ord} \to \mathcal{C}$.

Statement (i) is known as the **Principle of Global Choice**. (It is referred to as a "principle" and not an "axiom" because it involves quantification over all class functions.)

[ix] Technically, we should be writing ${}^3\mathbb{R}$, but $\mathbb{R}^3$ is the standard notation.

12. Journey to other universes

12.1. Introduction

Set theory is supposed to provide a framework for encoding all of mathematics. Hence, it is desirable to know whether the accepted axioms of set theory are *consistent*, meaning that they do not contradict each other. In this regard, it is important to keep in mind that the currently accepted formulation of set theory is incredibly subtle. Statements such as Russell's paradox serve as examples of contradictions that crept up in earlier versions of set theory; the modern approach professes to exorcise them, but how can we be sure that there are no other contradictions to worry about?

The short answer is, we can't. According to the celebrated *incompleteness theorem* of Gödel[x], if, say, ZFC is consistent, then no *proof* of ZFC's consistency can be carried out *within* ZFC *itself*. Hence, if we agree that all mathematics should, at least in principle, be doable in ZFC, then there is no "mathematical" justification for thinking that ZFC is consistent. As far as we are concerned, the consistency of ZFC remains an empirical fact: no one has found a contradiction in ZFC yet, hence it appears likely to be consistent.

Nevertheless, there are some nontrivial results concerning consistency of set theory that we *can* try to prove. For instance, we may isolate a particularly "suspicious" axiom and ask whether that axiom is consistent with the rest of set theory *assuming* that the rest of set theory is consistent on its own. For example, assuming ZF is consistent, can we argue that ZFC is consistent as well? It turns out that one can establish surprisingly strong results along these lines. For instance, we will eventually prove that if ZF^- (i.e., "basic" set theory without Foundation or Choice) is consistent, then so is ZFC + GCH.

How can one prove such "relative consistency" results? Suppose, for example, that we want to show the consistency of ZF^- implies the consistency of ZF. Let $\mathcal{U}$ be a universe of set theory satisfying ZF^-. We can then consider the class V (i.e., the von Neumann universe), as defined in $\mathcal{U}$. As such, V is a collection of sets equipped with the binary relation $\in$, so it makes sense to ask which statements in the language of set theory V satisfies. Well, it turns out that V satisfies all of the axioms of ZF! Hence, ZF must be consistent. In this and the following sections, we shall explore the power of arguments of this type.

12.2. Relativizing formulas

Fix a universe $\mathcal{U}$ of set theory and let $\mathcal{C}$ be a class. Given a formula φ in the language of set theory, we write $\varphi^{\mathcal{C}}$ for the formula obtained from φ by restricting every quantifier to $\mathcal{C}$, i.e., by replacing each quantifier of the form "$\forall x$" (resp. "$\exists x$") by "$\forall x \in \mathcal{C}$" (resp. "$\exists x \in \mathcal{C}$"). If φ is a formula with no free variables and with parameters from $\mathcal{C}$, we say that φ **holds in** $\mathcal{C}$, or $\mathcal{C}$ **satisfies** φ, in symbols $\mathcal{C} \models \varphi$, if $\varphi^{\mathcal{C}}$ is true (in $\mathcal{U}$).

Example 12.1. Let $A := \{\varnothing, \{\varnothing\}, \{\varnothing, \{\{\varnothing\}\}\}\}$. Then A does not satisfy the Axiom of Extensionality Ext. Indeed, Ext is given by the following formula:

$$\mathsf{Ext} \quad : \quad \forall x \forall y\, (\forall z\, (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

Thus, the relativized formula Ext^A is

$$\mathsf{Ext}^A \quad : \quad \forall x \in A\, \forall y \in A\, (\forall z \in A\, (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

In other words, Ext^A says that if x, $y \in A$ have the same elements *in* A, then $x = y$. But this is false, since the distinct sets $x := \{\varnothing\}$ and $y := \{\varnothing, \{\{\varnothing\}\}\}$ both have the same unique element in A, namely $\varnothing$. Another way in which A "disagrees" with the ambient universe $\mathcal{U}$ is that, letting $x := \{\varnothing\}$ and $y := \{\varnothing, \{\{\varnothing\}\}\}$, we have $A \models y \subseteq x$. Indeed, "$y \subseteq x$" is a shortcut for the formula

$$y \subseteq x \quad : \quad \forall z\, (z \in y \rightarrow z \in x).$$

[x] More precisely, his *second* incompleteness theorem.

Relativizing to A, we get

$$(y \subseteq x)^A \quad : \quad \forall z \in A\,(z \in y \;\rightarrow\; z \in x).$$

The only member of A that is an element of y is $\varnothing$, which also belongs to x, so $(y \subseteq x)^A$ is true.

To avoid the nastiness of Example 12.1, we usually restrict our attention to so-called transitive classes. A class $\mathcal{C}$ is **transitive** if for all $x \in \mathcal{C}$, we have $x \subseteq \mathcal{C}$; in other words, if $y \in x \in \mathcal{C}$, then $y \in \mathcal{C}$. Note that if $\mathcal{C}$ is a set, then this agrees with our usual definition of a transitive set.

Lemma 12.2. *If $\mathcal{U} \models \mathsf{Ext}$ and $\mathcal{C}$ is a transitive class, then $\mathcal{C} \models \mathsf{Ext}$ as well.*

PROOF. The formula $\mathsf{Ext}^{\mathcal{C}}$ looks like this:

$$\mathsf{Ext}^{\mathcal{C}} \quad : \quad \forall x \in \mathcal{C}\,\forall y \in \mathcal{C}\,(\forall z \in \mathcal{C}\,(z \in x \;\leftrightarrow\; z \in y) \;\rightarrow\; x = y).$$

Take x, $y \in \mathcal{C}$. Since $\mathcal{C}$ is transitive, x, $y \subseteq \mathcal{C}$. This means that if *for all z in* $\mathcal{C}$, $z \in x \;\leftrightarrow\; z \in y$, then indeed *for all z in* $\mathcal{U}$, $z \in x \;\leftrightarrow\; z \in y$, and hence $x = y$ by Ext in $\mathcal{U}$. ■

Many statements have the same "meaning" in $\mathcal{U}$ and in any transitive class $\mathcal{C}$. Specifically, we say that φ is a **Δ_0-formula** if every quantifier in φ is **bounded**, i.e., of the form "$\forall x \in y$" or "$\exists x \in y$," where x is a variable and y is either a variable or a parameter. We often say (somewhat loosely) that a property or a relation is Δ_0 if it can be expressed by a Δ_0-formula. For example, the statement "$x \subseteq y$" can be expressed by the following Δ_0-formula:

$$x \subseteq y \quad : \quad \forall z \in x\,(z \in y).$$

The utility of Δ_0-formulas is captured by the following observation:

Lemma 12.3. *If $\mathcal{C}$ is a transitive class and φ is a Δ_0-formula with no free variables and with parameters from $\mathcal{C}$, then $\mathcal{C} \models \varphi$ if and only if $\mathcal{U} \models \varphi$.*

PROOF. When a bounded quantifier such as "$\forall x \in y$" or "$\exists x \in y$" is restricted to $\mathcal{C}$, the result is "$\forall x \in \mathcal{C} \cap y$" or "$\exists x \in \mathcal{C} \cap y$." Since $\mathcal{C}$ is transitive, for all $y \in \mathcal{C}$, we have $\mathcal{C} \cap y = y$. Hence, $\varphi^{\mathcal{C}}$ has exactly the same meaning as φ. ■

As the following exercise shows, lots of useful properties can be expressed by Δ_0-formulas.

Exercise 12.1 (important!). Assuming that $\mathcal{U} \models \mathsf{ZF}^-$, show that the following properties and relations can be expressed by Δ_0-formulas without parameters:

(*a*) $x = \varnothing$, $x \subseteq y$, $x = \{y, z\}$, $x = (y, z)$, $x = y \cap z$, $x = y \backslash z$, $x = y \times z$, $x = \bigcup y$;

(*b*) f is a function, $y = f(x)$, $x = \mathrm{dom}(f)$, $x = \mathrm{ran}(f)$, f is an injection, $f \colon x \to y$ is bijective;

(*c*) $\prec$ is a linear order on x, x is a transitive set.

Additionally, assuming that $\mathcal{U} \models \mathsf{ZF}$, show that the following properties and relations also can be expressed by Δ_0-formulas without parameters:

(*d*) α is an ordinal, α is a limit ordinal, α is a successor ordinal;

(*e*) n is a natural number, $x = \omega$.

Here x, y, z, f, α, n are to be treated as free variables.

The next exercise is somewhat long and tedious, but it will be quite useful, as it shows that for most axioms of ZF^-, it is rather clear how to check whether they hold in a given transitive class $\mathcal{C}$.

Exercise 12.2 (important!). Suppose $\mathcal{U} \models \mathsf{ZF}^-$. Let $\mathcal{C}$ be a transitive class.

(*a*) Show that $\mathcal{C}$ satisfies the Empty Set Axiom if and only if $\varnothing \in \mathcal{C}$.

(*b*) Show that $\mathcal{C}$ satisfies the Pairing Axiom if and only if for all x, $y \in \mathcal{C}$, we have $\{x, y\} \in \mathcal{C}$.

(c) Show that $\mathcal{C}$ satisfies the Union Axiom if and only if for every $x \in \mathcal{C}$, we have $\bigcup x \in \mathcal{C}$.

(d) Show that $\mathcal{C}$ satisfies the Powerset Axiom if and only if for all $x \in \mathcal{C}$, we have

$$\mathcal{P}(x) \cap \mathcal{C} = \{y \in \mathcal{C} : y \subseteq x\} \in \mathcal{C}.$$

(e) Show that if $\omega \in \mathcal{C}$, then $\mathcal{C}$ satisfies the Infinity Axiom.

(f) Show that $\mathcal{C}$ satisfies the Comprehension Schema if and only if for all $x \in \mathcal{C}$ and for every formula $\varphi(z)$ with a single free variable z and parameters from $\mathcal{C}$, we have

$$\{z \in x : \mathcal{C} \models \varphi(z)\} \in \mathcal{C}.$$

Here you should notice that $\{z \in x : \mathcal{C} \models \varphi(z)\}$ is indeed a well-defined set in $\mathcal{U}$, because we can apply Comprehension in $\mathcal{U}$ to the relativized formula $\varphi^{\mathcal{C}}(z)$.

(g) Show that $\mathcal{C}$ satisfies the Replacement Schema if and only if the following statement holds. Let $\varphi(x, y)$ be a formula with two free variables x, y and parameters from $\mathcal{C}$ such that $\varphi(x, y)$ defines a class function in $\mathcal{C}$; in other words,

$$\forall x \in \mathcal{C}\, \forall y \in \mathcal{C}\, \forall z \in \mathcal{C}\, (\varphi^{\mathcal{C}}(x, y) \wedge \varphi^{\mathcal{C}}(x, z) \to y = z).$$

Then for every set $X \in \mathcal{C}$, we have

$$\{y \in \mathcal{C} : \exists x \in X\, (\mathcal{C} \models \varphi(x, y))\} \in \mathcal{C}.$$

Again, here we need to observe that $\{y \in \mathcal{C} : \exists x \in X\, (\mathcal{C} \models \varphi(x, y))\}$ is a well-defined set in $\mathcal{U}$, because we can apply Replacement in $\mathcal{U}$ to the formula

$$x \in \mathcal{C} \wedge y \in \mathcal{C} \wedge \varphi^{\mathcal{C}}(x, y),$$

which defines a class function in $\mathcal{U}$.

Exercise 12.3. Show that if $\mathcal{U} \models \mathsf{ZF}$ and $\mathcal{C}$ is a class such that $\mathcal{C} \models \mathsf{ZF}^-$, then $\mathcal{C} \models \mathsf{ZF}$ as well.

Exercise 12.4. If $\mathcal{U} \models \mathsf{ZF}^-$ and $\mathcal{C}$ is a transitive class, when does $\mathcal{C}$ satisfy the Axiom of Choice?

A particularly useful type of potential universes of set theory are the so-called **inner models**, i.e., transitive classes $\mathcal{C}$ such that $\mathbf{Ord} \subseteq \mathcal{C}$. The simplest interesting example of an inner model is the von Neumann universe V, which will be discussed in the next subsection. Another example that we'll be working with is the so-called *constructible universe*, usually denoted by L, which will be the central object of study in §§14 and 16.

Example 12.4. Let $\mathcal{U} \models \mathsf{ZF}^-$ and consider the class $\mathbf{Ord}$. We claim that $\mathbf{Ord}$ satisfies the Powerset Axiom. Indeed, since $\mathbf{Ord}$ is a transitive class, we can apply the result of Exercise 12.2(d) and only check that for each $\alpha \in \mathbf{Ord}$, the following set is an ordinal:

$$\alpha' := \mathcal{P}(\alpha) \cap \mathbf{Ord} = \{\beta \in \mathbf{Ord} : \beta \subseteq \alpha\}.$$

But $\beta \subseteq \alpha$ if and only if $\beta \leqslant \alpha$, so $\alpha' = \{\beta \in \mathbf{Ord} : \beta \leqslant \alpha\} = \alpha + 1$. In other words, from the point of view of $\mathbf{Ord}$, the powerset of α is $\alpha + 1$!

Exercise 12.5. For a class $\mathcal{C}$, we let $\mathbf{Ord}^{\mathcal{C}}$ and $\mathbf{Card}^{\mathcal{C}}$ denote the ordinals and the cardinals "from the point of view of $\mathcal{C}$." More precisely, define

$$\mathbf{Ord}^{\mathcal{C}} := \{x \in \mathcal{C} : \mathcal{C} \models \text{“}x \text{ is an ordinal”}\} \quad \text{and} \quad \mathbf{Card}^{\mathcal{C}} := \{x \in \mathcal{C} : \mathcal{C} \models \text{“}x \text{ is a cardinal”}\}.$$

What are $\mathbf{Ord}^{\mathbf{Ord}}$ and $\mathbf{Card}^{\mathbf{Ord}}$?

12.3. The relative consistency of AF

Theorem 12.5. *If $\mathcal{U} \models \mathsf{ZF}^-$, then $V \models \mathsf{ZF}$. Therefore, if ZF^- is consistent, then so is ZF.*

PROOF. We first check that $V \models \mathsf{ZF}^-$. Since V is transitive, Exercise 12.2 makes this rather easy; the key observation is that for every set x, $x \in V$ if and only if $x \subseteq V$ (see Proposition 3.12).

- $V \models \mathsf{Ext}$ by Lemma 12.2.
- $V \models \mathsf{Empty}$: $\varnothing \in V$.
- $V \models \mathsf{Pair}$: If $x, y \in V$, then $\{x, y\} \subseteq V$, hence $\{x, y\} \in V$.
- $V \models \mathsf{Union}$: exercise!
- $V \models \mathsf{Pow}$: If $x \in V$, then $\mathcal{P}(x) \subseteq V$, so $\mathcal{P}(x) \in V$.
- $V \models \mathsf{Inf}$: $\omega \in V$.
- $V \models \mathsf{Comp}$: exercise!
- $V \models \mathsf{Rep}$: Let $\varphi(x, y)$ be a formula with free variables x, y and parameters from V that defines a class function in V. We need to argue that for all $X \in V$, the following set is in V:
$$Y := \{y \in V : \exists x \in X\, (V \models \varphi(x, y))\}.$$
This is indeed the case since, by definition, $Y \subseteq V$, and thus $Y \in V$.

It remains to verify that $V \models \mathsf{AF}$. Recall that by Theorem 3.13, assuming ZF^-, AF is equivalent to
$$\forall x \left(x \neq \varnothing \longrightarrow \exists y\, (y \in x \wedge x \cap y = \varnothing)\right).$$
Consider any $\varnothing \neq x \in V$. Let $\alpha := \min\{\mathrm{rank}(z) : z \in x\}$ and let $y \in x$ be an arbitrary element with $\mathrm{rank}(y) = \alpha$. We claim that $x \cap y = \varnothing$, as desired. Indeed, if $z \in y$, then $\mathrm{rank}(z) < \mathrm{rank}(y) = \alpha$, while if $z \in x$, then $\mathrm{rank}(z) \geqslant \alpha$ by the choice of α. Hence, y and x have no elements in common. ■

Exercise 12.6. Show that if $\mathcal{U} \models \mathsf{ZF}^- + \mathsf{AC}$, then $V \models \mathsf{ZFC}$.

12.4. Inaccessible cardinals and models of set theory

Assumption. Throughout this subsection we assume that $\mathcal{U} \models \mathsf{ZFC}$.

Recall that an infinite cardinal κ is **regular** if $\mathrm{cf}(\kappa) = \kappa$. Equivalently, an infinite cardinal κ is regular if and only if a set of cardinality κ cannot be written as a union of strictly fewer than κ-many sets of cardinality strictly less than κ. An uncountable cardinal κ is (**strongly**) **inaccessible** if κ is regular and $\kappa > 2^\lambda$ for every cardinal $\lambda < \kappa$.

Theorem 12.6. *If κ is an inaccessible cardinal, then $V_\kappa \models \mathsf{ZFC}$.*

A remarkable feature of Theorem 12.6 is that V_κ is merely a *set*, but it is so "rich" that all of our usual set theory–and hence all of mathematics—could in principle be done inside it!

Recall how in the proof of Theorem 12.5 we heavily relied on the fact that $x \in V \iff x \subseteq V$. To prove Theorem 12.6, we need a version of this property for V_κ:

Lemma 12.7. *If κ is an inaccessible cardinal, then $|V_\kappa| = \kappa$ and for every set x, we have*
$$x \in V_\kappa \iff x \subseteq V_\kappa \text{ and } |x| < \kappa. \tag{12.1}$$

PROOF. Since $\kappa = \mathbf{Ord} \cap V_\kappa \subseteq V_\kappa$, we have $|V_\kappa| \geqslant \kappa$. To prove the opposite inequality, recall that, by definition, $V_\kappa = \bigcup\{V_\alpha : \alpha < \kappa\}$. We will show that $|V_\alpha| < \kappa$ for all $\alpha < \kappa$. This implies that V_κ is a union of κ-many sets of cardinality less than κ, and hence $|V_\kappa| \leqslant \kappa \otimes \kappa = \kappa$, as desired. The proof that $|V_\alpha| < \kappa$ for all α is by induction on α.

<u>*Case 1*</u>: $\alpha = 0$. We have $|V_0| = |\varnothing| = 0 < \kappa$.

Case 2: $\alpha = \beta + 1$. We have

$$|V_{\beta+1}| \;=\; |\mathcal{P}(V_\beta)| \;=\; 2^{|V_\beta|} \;<\; \kappa,$$

since κ is inaccessible and $|V_\beta| < \kappa$ by the inductive hypothesis.

Case 3: *α is a limit.* Then $V_\alpha = \bigcup\{V_\gamma \,:\, \gamma < \alpha\}$. In other words, V_α is a union of $|\alpha|$-many sets, each of cardinality less than κ. Since κ is regular, this implies that $|V_\alpha| < \kappa$.

Now we turn to proving (12.1). First, suppose that $x \in V_\kappa$. Since V_κ is transitive, we conclude that $x \subseteq V_\kappa$. Furthermore, if we let $\alpha := \mathrm{rank}(x)$, then $\alpha < \kappa$ and $x \subseteq V_\alpha$, so $|x| \leqslant |V_\alpha| < \kappa$.

Finally, suppose that $x \subseteq V_\kappa$ and $|x| < \kappa$. Since κ is regular, the function $x \to \kappa \colon y \mapsto \mathrm{rank}(y)$ cannot be cofinal. Hence, $\alpha := \sup\{\mathrm{rank}(y) \,:\, y \in x\} < \kappa$. Then $x \subseteq V_\alpha$, so $x \in V_{\alpha+1} \subset V_\kappa$. ■

Proof *of Theorem 12.6.* We will only verify that V_κ satisfies Replacement and Choice, leaving the rest of the axioms as exercises.

To show that $V_\kappa \models \mathsf{Rep}$, let $\varphi(x, y)$ be a formula with free variables x, y and parameters from V_κ that defines a class function in V_κ. We need to argue that for every $X \in V_\kappa$, the following set belongs to V_κ:

$$Y \;:=\; \{y \in V_\kappa \,:\, \exists x \in X\,(V_\kappa \models \varphi(x, y))\}.$$

By definition, $Y \subseteq V_\kappa$. Also, Y is the image of X under a function, so $|Y| \leqslant |X| < \kappa$. Therefore, $Y \in V_\kappa$ by Lemma 12.7.

To prove that $V_\kappa \models \mathsf{AC}$, let $X \in V_\kappa$ be a set of nonempty sets. Since AC holds in $\mathcal{U}$, there is a choice function f for X in $\mathcal{U}$, and we only need to show that $f \in V_\kappa$. To that end, note that $f \subseteq V_\kappa$ (why?) and $|f| = |X| < \kappa$, hence $f \in V_\kappa$ by Lemma 12.7. ■

Taken together, Theorem 12.6 and Lemma 12.7 paint a very satisfying picture of the structure of the set V_κ for inaccessible κ. First, V_κ satisfies ZFC. Second, every class in V_κ (i.e., a collection of elements of V_κ defined by a formula) is a *subset* of V_κ from the point of view of $\mathcal{U}$, but V_κ "thinks" that it is a *proper class* whenever its cardinality (in $\mathcal{U}$) is κ.

Exercise 12.7. Let κ be the least inaccessible cardinal. Show that

$$V_\kappa \models \text{"there are no inaccessible cardinals."}$$

Conclude that if ZFC is consistent, then so is ZFC together with the assertion that there are no inaccessible cardinals.

Exercise 12.8. Show that V_ω satisfies all of the axioms of ZFC except one (which one?).

13. Talking about logic in $\mathcal{U}$

13.1. The endgame

Our overarching goal in §14 is to define an inner model, denoted by L, that satisfies ZF and is "as thin as possible." What do we mean by that? Due to the Comprehension Schema, a universe of set theory must include, together with every set X, each of its subsets of the form $\{x \in X : \varphi(x) \text{ if true}\}$, where φ is some formula with one free variable x. Calling such subsets of X "*definable*," we would like to form the "*definable powerset*"

$$\mathcal{D}(X) := \text{“}\{A \subseteq X : A \text{ is definable}\}.\text{”}$$

(We are using quotes because we haven't defined what "definable" means yet.) Then the universe of "necessary" sets can be built recursively as follows:

$$L_\alpha := \begin{cases} \varnothing & \text{if } \alpha = 0; \\ \mathcal{D}(L_\beta) & \text{if } \alpha = \beta + 1; \\ \bigcup\{L_\gamma : \gamma < \alpha\} & \text{if } \alpha \text{ is a limit ordinal,} \end{cases}$$

$$L := \bigcup\{L_\alpha : \alpha \in \mathbf{Ord}\}.$$

In other words, we mimic the construction of V but replace each powerset operation by its "definable" counterpart.

In order to carry out this construction, we need to have a rigorous definition of the definable powerset operation $\mathcal{D}(\cdot)$. In particular, in order for $\mathcal{D}(X)$ to really be a subset of $\mathcal{P}(X)$, we must ensure that the statement "A is definable" can be expressed by a formula in the language of set theory. The subtle issue here is that we cannot directly talk about formulas inside the language of set theory, because formulas are not sets. Nevertheless, if we believe that set theory is expressive enough to model all of mathematics, then in particular we should be able to "encode" formulas and logic within set theory. Developing such an "encoding" is the aim of this section.

13.2. $\mathcal{U}$-formulas

For the remainder of §13, we fix a universe $\mathcal{U}$ of set theory satisfying ZF. A $\mathcal{U}$-formula, roughly speaking, is a set in $\mathcal{U}$ that "represents" a formula in the language of set theory. The precise definition is recursive. First, we fix sets in $\mathcal{U}$ that will represent logical symbols. Say, let

$$\dot{=} := 0, \quad \dot{\in} := 1, \quad \dot{\wedge} := 2, \quad \dot{\neg} := 3, \quad \dot{\exists} := 4.$$

In other words, we shall use the numbers 0, 1, 2, 3, 4 to play the roles of the symbols "$=$," "$\in$," "$\wedge$," "$\neg$," "$\exists$," and we put a dot above each symbol to indicate that we are talking about the corresponding member of $\mathcal{U}$.[xi] Next, we let

$$\mathsf{Var} := \{n \in \omega : n \geqslant 5\}.$$

We refer to the elements of Var as **$\mathcal{U}$-variables**. They will be used as variables in our $\mathcal{U}$-formulas. Note that the set of all $\mathcal{U}$-variables is countably infinite. Define

$${}_0\mathcal{F} := \{(\dot{=}, x, y), (\dot{\in}, x, y) : x, y \in \mathsf{Var}\}.$$

The elements of the set ${}_0\mathcal{F}$ are called **atomic $\mathcal{U}$-formulas**. An atomic $\mathcal{U}$-formula of the form $(\dot{=}, x, y)$ represents the formula "$x = y$," while $(\dot{\in}, x, y)$ represents "$x \in y$." Now, for each $n \in \omega$, we let

$${}_{n+1}\mathcal{F} := {}_n\mathcal{F} \cup \{(\dot{\wedge}, f, g), (\dot{\neg}, f), (\dot{\exists}, x, f) : f, g \in {}_n\mathcal{F}, x \in \mathsf{Var}\}.$$

[xi] "Where are $\vee$, $\rightarrow$, and $\forall$?" I hear you ask. In the interest of saving space, we got rid of them. For instance, instead of "$\forall x\,(\ldots)$," we can always write "$\neg\exists x\,\neg(\ldots)$." Using more symbols would not change the rest of the construction in any substantial way.

Here $(\dot{\wedge}, f, g)$, $(\dot{\neg}, f)$, and $(\dot{\exists}, x, f)$ represent "$f \wedge g$," "$\neg f$," and "$\exists x\, f$," respectively. Finally, we set

$$\mathcal{F} := \bigcup_{n \in \omega} {}_n\mathcal{F},$$

and refer to the elements of the set $\mathcal{F}$ as $\mathcal{U}$-**formulas**. The "$\mathcal{U}$" in "$\mathcal{U}$-formulas" is supposed to emphasize that $\mathcal{U}$-formulas are *sets in* $\mathcal{U}$. It should be clear from this definition that every "actual" formula φ can be naturally represented by a $\mathcal{U}$-formula, which we denote by $\ulcorner\varphi\urcorner$. For instance, if φ is a formula asserting that $x = \varnothing$, i.e., $\varphi = (\neg\exists y\,(y \in x))$, then we have

$$\ulcorner\varphi\urcorner = \ulcorner\neg\exists y\,(y \in x)\urcorner = \Big(\dot{\neg},\, \Big(\dot{\exists},\, y,\, (\dot{\in},\, y,\, x)\Big)\Big).$$

The precise details of the above construction of $\mathcal{U}$-formulas are not really important; what matters is that such a construction exists. In particular, to improve readability, we will usually write simply "$x \doteq y$" instead of "$(\doteq, x, y)$," "$f \mathbin{\dot{\wedge}} g$" instead of "$(\dot{\wedge}, f, g)$," etc. We will also use symbols such as "$\dot{\vee}$" and "$\dot{\to}$" as obvious shortcuts.

Exercise 13.1. Show that every $\mathcal{U}$-formula is a finite set. Moreover, show that $\mathcal{F} \subseteq V_\omega$. Conclude that the set $\mathcal{F}$ is countable (because V_ω is countable).

Exercise 13.2 ($\mathcal{U}$-formulas with parameters)**.** For a set W, recursively define the set $\mathcal{F}_W$ of all $\mathcal{U}$-**formulas with parameters from** W. You should express $\mathcal{F}_W$ as a union

$$\mathcal{F}_W = \bigcup_{n \in \omega} {}_n\mathcal{F}_W,$$

where ${}_0\mathcal{F}_W$ is the set of all **atomic** $\mathcal{U}$-**formulas with parameters from** W.

If $\mathcal{C}$ is a class, we define the class $\mathcal{F}_\mathcal{C}$ of all $\mathcal{U}$-**formulas with parameters from** $\mathcal{C}$ as follows:

$$\mathcal{F}_\mathcal{C} := \{f : f \in \mathcal{F}_W \text{ for some set } W \subseteq \mathcal{C}\}.$$

(Here we use that every individual $\mathcal{U}$-formula involves only a finite *set* of parameters.)

Exercise 13.3. Assuming AC, show that if W is an infinite set, then $|\mathcal{F}_W| = |W|$.

13.3. Induction/recursion on the complexity of $\mathcal{U}$-formulas

Recall that the set $\mathcal{F}$ of all $\mathcal{U}$-formulas is defined as the union

$$\mathcal{F} = \bigcup_{n \in \omega} {}_n\mathcal{F},$$

where $\{{}_n\mathcal{F} : n \in \omega\}$ is a recursively defined sequence starting with the set ${}_0\mathcal{F}$ of atomic $\mathcal{U}$-formulas. For a $\mathcal{U}$-formula $f \in \mathcal{F}$, we define its **complexity** $\mathrm{comp}(f)$ as the least $n \in \omega$ such that $f \in {}_n\mathcal{F}$. One similarly defines the complexity of a $\mathcal{U}$-formula with parameters.

A standard way of proving things related to $\mathcal{U}$-formulas is by induction on their complexity. To illustrate this idea, let us formally define the set of all free variables in a $\mathcal{U}$-formula f. We recursively define a sequence of functions $\mathsf{FVar}_n \colon {}_n\mathcal{F} \to \mathcal{P}(\mathsf{Var})$, for all $n \in \omega$, as follows. For $n = 0$, let

$$\mathsf{FVar}_0(f) := \{x, y\} \text{ if } f = (x \doteq y) \text{ or } f = (x \mathbin{\dot{\in}} y).$$

If FVar_n is already defined, then for each $f \in {}_{n+1}\mathcal{F}$, let

$$\mathsf{FVar}_{n+1}(f) := \begin{cases} \mathsf{FVar}_n(f) & \text{if } \mathrm{comp}(f) \leqslant n; \\ \mathsf{FVar}_n(g) \cup \mathsf{FVar}_n(h) & \text{if } f = (g \mathbin{\dot{\wedge}} h); \\ \mathsf{FVar}_n(g) & \text{if } f = (\dot{\neg}\, g); \\ \mathsf{FVar}_n(g) \setminus \{x\} & \text{if } f = (\dot{\exists} x\, g). \end{cases} \tag{13.1}$$

Finally, let

$$\mathsf{FVar}(f) := \mathsf{FVar}_n(f) \text{ whenever } \mathrm{comp}(f) = n,$$

and call $\mathsf{FVar}(f)$ the set of all **free variables** in f. The above definition is usually phrased (somewhat loosely) in the following more concise form: We define the set $\mathsf{FVar}(f) \subseteq \mathsf{Var}$ as follows:

$$\mathsf{FVar}(f) := \begin{cases} \{x, y\} & \text{if } f = (x \mathbin{\dot{=}} y) \text{ or } f = (x \mathbin{\dot{\in}} y); \\ \mathsf{FVar}(g) \cup \mathsf{FVar}(h) & \text{if } f = (g \mathbin{\dot{\wedge}} h); \\ \mathsf{FVar}(g) & \text{if } f = (\dot{\neg}\, g); \\ \mathsf{FVar}(g) \backslash \{x\} & \text{if } f = (\dot{\exists} x\, g). \end{cases} \tag{13.2}$$

Exercise 13.4. Extend the above recursive definition of the set $\mathsf{FVar}(f)$ to all $\mathcal{U}$-formulas f with parameters from a given set W.

Exercise 13.5. Give a recursive definition of the set $\mathsf{Sub}(f)$ of all subformulas of a $\mathcal{U}$-formula f, i.e., the $\mathcal{U}$-formulas that appear in the construction of f. For instance,

$$\mathsf{Sub}(\ulcorner \neg\exists y\,(y \in x)\urcorner) = \{\ulcorner y \in x\urcorner, \ulcorner \exists y\,(y \in x)\urcorner, \ulcorner \neg\exists y\,(y \in x)\urcorner\}.$$

Exercise 13.6. Show that if f is a $\mathcal{U}$-formula, then the sets $\mathsf{FVar}(f)$ and $\mathsf{Sub}(f)$ are finite.

A $\mathcal{U}$-formula f such that $\mathsf{FVar}(f) = \varnothing$ is called a $\mathcal{U}$-**sentence**. The set of all $\mathcal{U}$-sentences with parameters from a set W is denoted by $\mathcal{F}_W^0$. More generally, $\mathcal{F}_W^k$ is the set of all $\mathcal{U}$-formulas with parameters from W and with exactly k free variables, and similarly, $\mathcal{F}^k$ is the set of all $\mathcal{U}$-formulas with k variables and no parameters (in other words, $\mathcal{F}^k := \mathcal{F}_\varnothing^k$).

Remark 13.1. We can now explain our use of the somewhat clumsy notation "${}_n\mathcal{F}$" instead of the more agreeable options "$\mathcal{F}_n$" and "$\mathcal{F}^n$": these expressions are reserved for other purposes. Indeed,

- ${}_n\mathcal{F}$ is the set of all $\mathcal{U}$-formulas without parameters of complexity at most n,
- $\mathcal{F}_n$ is the set of all $\mathcal{U}$-formulas with parameters from the set $n = \{0, 1, \ldots, n-1\}$,
- $\mathcal{F}^n$ is the set of all $\mathcal{U}$-formulas without parameters and with n free variables.

Exercise 13.7. Let W be a set. For a $\mathcal{U}$-formula $f \in \mathcal{F}_W^1$ and an element $a \in W$, give a recursive definition of the $\mathcal{U}$-sentence $f(a) \in \mathcal{F}_W^0$ obtained by plugging in a in place of the free variable in f.

Note that if $\mathcal{C}$ is a proper class, then we can also define the classes

$${}_n\mathcal{F}_\mathcal{C} := \bigcup \{{}_n\mathcal{F}_W \,:\, W \text{ is a subset of } \mathcal{C}\}.$$

However, one has to be extremely careful with recursive definitions involving such classes. For instance, look at our definition of the function FVar. Formally, instead of defining FVar "in one go," as in (13.2), we actually had to first construct a sequence of functions $\mathsf{FVar}_n \colon {}_n\mathcal{F} \to \mathcal{P}(\mathsf{Var})$ using the recursive formula (13.1). This sequence is itself a function defined on ω and sending each n to FVar_n. Here it is important that each FVar_n is a *set*, which makes it an allowable value for a function. Imagine now trying to do something similar on a proper class $\mathcal{F}_\mathcal{C}$. Then each FVar_n would be defined on the proper class ${}_n\mathcal{F}_\mathcal{C}$, i.e., FVar_n would have to be a *class function*, not a *set function*. As a result, FVar_n would fail to be a valid value for a function, so it would be meaningless to talk about the "function" $n \mapsto \mathsf{FVar}_n$, and the recursive construction will break down.

This is a general feature of recursive definitions. It is important that the value of a recursively defined function on any given input is determined by the values it takes on some *set* (not a proper class!) of previously considered inputs. For example, when we recursively define a class function $\Phi \colon \mathbf{Ord} \to \mathcal{U}$, each $\Phi(\alpha)$ has to be expressed in terms of the values $\Phi(\beta)$ for $\beta < \alpha$, and all such β form a set (namely α itself). Similarly, (13.2) reduces computing $\mathsf{FVar}(f)$ for a $\mathcal{U}$-formula f with $\mathrm{comp}(f) = n$ to knowing the values $\mathsf{FVar}(g)$ for all g of complexity less than n, and such $\mathcal{U}$-formulas g form a set.

Of course, we still can define the set of all free variables in a $\mathcal{U}$-formula $f \in \mathcal{F}_\mathcal{C}$, because in fact $f \in \mathcal{F}_W$ for some sub*set* $W \subseteq \mathcal{C}$. This might make the above discussion seem like unnecessary pedantry; however, in the next subsection we will see an important example where extending recursive definitions to formulas with arbitrary parameters becomes not just technically problematic, but in fact impossible.

Exercise 13.8. Extend the result of Exercise 13.7 by defining a class function

$$\mathcal{F}^1_{\mathcal{U}} \times \mathcal{U} \to \mathcal{F}^0_{\mathcal{U}} \colon (f, a) \mapsto f(a).$$

13.4. Truth of $\mathcal{U}$-formulas

Formulas are useful because they assert something. Similarly, we want to view $\mathcal{U}$-formulas as statements that have meaning and hence can be true or false. Unfortunately, an attempt to define what it means for a $\mathcal{U}$-formula to be true leads to unexpected difficulties:[xii]

Lemma 13.2 (Truth is not definable)**.** *Let $\mathcal{F}^0_{\mathcal{U}}$ be the class of all $\mathcal{U}$-sentences with arbitrary parameters. There is no class function $\mathsf{Truth} \colon \mathcal{F}^0_{\mathcal{U}} \to \{0, 1\}$ satisfying the following equation:*

$$\mathsf{Truth}(f) \;=\; \begin{cases} 1 & \text{if } f = (a \mathbin{\dot{=}} b) \text{ and } a = b; \\ 1 & \text{if } f = (a \mathbin{\dot{\in}} b) \text{ and } a \in b; \\ 1 & \text{if } f = (g \mathbin{\dot{\wedge}} h) \text{ and } \mathsf{Truth}(g) = \mathsf{Truth}(h) = 1; \\ 1 & \text{if } f = (\dot{\neg}\, g) \text{ and } \mathsf{Truth}(g) = 0; \\ 1 & \text{if } f = (\dot{\exists} x\, g) \text{ and } \exists a\, (\mathsf{Truth}(g(a)) = 1); \\ 0 & \text{otherwise.} \end{cases} \tag{13.3}$$

Equation (13.3) looks an awful lot like a definition by recursion on the complexity of f (similar to (13.2)), so it might seem strange that, according to Lemma 13.2, it doesn't actually define anything. But remember the discussion from the end of §13.3! To compute the value $\mathsf{Truth}(\dot{\exists} x\, g)$ using (13.3), we have to first determine the values $\mathsf{Truth}(g(a))$ for *every* $a \in \mathcal{U}$, i.e., we need to already know a *proper class* of values of Truth. That is why (13.3) cannot be converted into a correct recursive definition (such as (13.1)). This observation, of course, doesn't by itself prove that there is no *other* way to define a class function satisfying (13.3); but that we shall do now.

Proof. Suppose that Truth is such a class function. Consider an arbitrary $\mathcal{U}$-formula $f \in \mathcal{F}^1_{\mathcal{U}}$. Since f has one free variable, we can plug in any set a into f and obtain a $\mathcal{U}$-sentence $f(a)$ (see Exercise 13.8), which should be either true or false, depending on whether $\mathsf{Truth}(f(a))$ is 1 or 0. Since f itself is a set, we can plug f into itself[xiii] and get a $\mathcal{U}$-sentence $f(f)$. For some f, $\mathsf{Truth}(f(f)) = 1$, while for others, $\mathsf{Truth}(f(f)) = 0$. For example, if $f = \ulcorner x$ is a $\mathcal{U}$-formula$\urcorner$, then $\mathsf{Truth}(f(f)) = 1$, because f is a $\mathcal{U}$-formula. On the other hand, if $f = \ulcorner x$ is infinite$\urcorner$, then $\mathsf{Truth}(f(f)) = 0$, because, like any $\mathcal{U}$-formula, f is finite (see Exercise 13.1). Now we define the following $\mathcal{U}$-formula with one free variable, denoted below by f:

$$g \;:=\; \ulcorner f \text{ is a } \mathcal{U}\text{-formula with one free variable and } \mathsf{Truth}(f(f)) = 0\urcorner. \tag{13.4}$$

The statement within the $\ulcorner \ldots \urcorner$ in (13.4) can be written out as a formula in the language of set theory—because, by our assumption, Truth is a class function. Therefore, the above definition of g makes sense. And now the punchline: What is $\mathsf{Truth}(g(g))$? If $\mathsf{Truth}(g(g)) = 1$, then g is a $\mathcal{U}$-formula satisfying $\mathsf{Truth}(g(g)) = 0$; a contradiction. But, conversely, if $\mathsf{Truth}(g(g)) = 0$, then g is a $\mathcal{U}$-formula such that $\mathsf{Truth}(g(g)) \neq 0$; a contradiction again. ■

In view of Lemma 13.2, you may wonder if there is any point in talking about $\mathcal{U}$-formulas at all, given that there is no coherent way to define what it means for a $\mathcal{U}$-formula to be true. Thankfully, there is still *something* we can do. Recall that the troubles in Lemma 13.2 stem from our desire to

[xii] Or maybe they should have been expected? If we could define truth, would philosophy departments still exist?
[xiii] Galaxy brain moment.

treat $\mathcal{U}$-formulas with parameters ranging over the entire universe. We could be more modest and restrict our parameters and quantifiers to some set W; indeed, this restriction turns (13.3) into an appropriate recursive definition:

Theorem 13.3 (Truth in a model)**.** *There exists a unique class function* Truth *with domain* $\{(W, f) : f \in \mathcal{F}^0_W\}$ *and range* $\{0, 1\}$*, such that for every set* W *and for all* $f \in \mathcal{F}^0_W$*,*

$$\mathsf{Truth}(W, f) = \begin{cases} 1 & \text{if } f = (a \mathbin{\dot{=}} b) \text{ and } a = b; \\ 1 & \text{if } f = (a \mathbin{\dot{\in}} b) \text{ and } a \in b; \\ 1 & \text{if } f = (g \mathbin{\dot{\wedge}} h) \text{ and } \mathsf{Truth}(W, g) = \mathsf{Truth}(W, h) = 1; \\ 1 & \text{if } f = (\dot{\neg}\, g) \text{ and } \mathsf{Truth}(W, g) = 0; \\ 1 & \text{if } f = (\dot{\exists} x\, g) \text{ and } \exists a \in W\, (\mathsf{Truth}(W, g(a)) = 1); \\ 0 & \text{otherwise.} \end{cases} \tag{13.5}$$

PROOF. The restriction to the *set* $\mathcal{F}^0_W$ turns (13.5) into a valid definition by recursion on the complexity of f that can be converted into a standard recursive definition analogous to (13.1). To really drive the point home, we do this explicitly here.

Given a set W, we recursively define functions $T_n \colon {}_n\mathcal{F}^0_W \to \{0, 1\}$, for all $n \in \omega$. For $n = 0$, let

$$T_0(f) := \begin{cases} 1 & \text{if } f = (a \mathbin{\dot{=}} b) \text{ and } a = b; \\ 1 & \text{if } f = (a \mathbin{\dot{\in}} b) \text{ and } a \in b; \\ 0 & \text{otherwise.} \end{cases}$$

If T_n is already defined, then for each $f \in {}_{n+1}\mathcal{F}^0_W$, define

$$T_{n+1}(f) := \begin{cases} T_n(f) & \text{if } \operatorname{comp}(f) \leqslant n; \\ 1 & \text{if } f = (g \mathbin{\dot{\wedge}} h) \text{ and } T_n(g) = T_n(h) = 1; \\ 1 & \text{if } f = (\dot{\neg}\, g) \text{ and } T_n(g) = 0; \\ 1 & \text{if } f = (\dot{\exists} x\, g) \text{ and } \exists a \in W\, (T_n(g(a)) = 1); \\ 0 & \text{otherwise.} \end{cases}$$

Finally, we let $\mathsf{Truth}(W, f) := T_n(f)$ whenever $\operatorname{comp}(f) = n$. Checking that this definition satisfies the requirements of the theorem and that such a class function Truth is unique are left as exercises. ■

Let Truth be the class function from Theorem 13.3. When $\mathsf{Truth}(W, f) = 1$, we say that f **holds in** W, or W **satisfies** f, and write $W \models f$. Note that if φ is a formula, then the expressions $W \models \varphi$ and $W \models \ulcorner\varphi\urcorner$ are equivalent. The moral of this story can be summed up as follows:

> *There is no meaningful sense in which a $\mathcal{U}$-formula is true or false "in the universe"; but we can nonetheless talk about $\mathcal{U}$-formulas that hold or don't hold in a given set.*

Exercise 13.9. Show that there exists a class function $T \colon {}_{100}\mathcal{F}^0_{\mathcal{U}} \to \{0, 1\}$ such that:

$$T(f) = \begin{cases} 1 & \text{if } f = (a \mathbin{\dot{=}} b) \text{ and } a = b; \\ 1 & \text{if } f = (a \mathbin{\dot{\in}} b) \text{ and } a \in b; \\ 1 & \text{if } f = (g \mathbin{\dot{\wedge}} h) \text{ and } T(g) = T(h) = 1; \\ 1 & \text{if } f = (\dot{\neg}\, g) \text{ and } T(g) = 0; \\ 1 & \text{if } f = (\dot{\exists} x\, g) \text{ and } \exists a\, (T(g(a)) = 1); \\ 0 & \text{otherwise,} \end{cases}$$

for every $\mathcal{U}$-sentence f with arbitrary parameters of complexity at most 100.

14. Gödel's constructible universe L

14.1. Definable subsets and definable powersets

Definition 14.1 (Definable subsets)**.** Let W be a set. A subset $A \subseteq W$ is **definable in** W if there is a $\mathcal{U}$-formula $f \in \mathcal{F}^1_W$ (i.e., with one free variable and with parameters from W) such that

$$A = \{a \in W : W \models f(a)\}.$$

In this case, we say that f **defines** A **in** W. The **definable powerset** of W is the set

$$\mathcal{D}(W) := \{A \subseteq W : A \text{ is definable in } W\}.$$

Prototypical examples of definable subsets of W are of the form $\{a \in W : W \models \varphi(a)\}$, where φ is a formula with one free variable and with parameters from W. Indeed, such a set is defined by the corresponding $\mathcal{U}$-formula $\ulcorner\varphi\urcorner$. Some concrete examples of definable subsets of W are:

- W itself: $W = \{a \in W : W \models a \dot{=} a\}$,
- the empty set: $\varnothing = \{a \in W : W \models \dot{\neg}(a \dot{=} a)\}$,
- every one-element subset of W: if $b \in W$, then

$$\{b\} = \{a \in W : W \models a \dot{=} b\}$$

  (here b is used as a parameter).

The last example can be generalized to show that every finite subset of W is definable in W. Indeed, if $k \in \omega$ and $a_1, \ldots, a_k \in W$, then

$$\{a_1, \ldots, a_k\} = \{a \in W : W \models (a \dot{=} a_1) \dot{\vee} \ldots \dot{\vee} (a \dot{=} a_k)\}.$$

In particular, if W is finite, then $\mathcal{D}(W) = \mathcal{P}(W)$. Not so if W is infinite:

Lemma 14.2. *Assume* AC. *If W is an infinite set, then $|\mathcal{D}(W)| = |W|$. Hence, $\mathcal{D}(W) \neq \mathcal{P}(W)$.*

Proof. Since every one-element subset of W is in $\mathcal{D}(W)$, we have $|W| \leqslant |\mathcal{D}(W)|$. For the opposite inequality, notice that $|\mathcal{D}(W)| \leqslant |\mathcal{F}^1_W| \leqslant |\mathcal{F}_W|$, since the function

$$\mathcal{F}^1_W \to \mathcal{D}(W) \colon f \mapsto \{a \in W : W \models f(a)\}$$

is surjective. By Exercise 13.3, $|\mathcal{F}_W| = |W|$, and we are done. ∎

Exercise 14.1. Show, without AC, that if W is a countable set, then $\mathcal{D}(W)$ is also countable. More generally, show that if W is an infinite well-orderable set, then $\mathcal{D}(W)$ is also well-orderable and $|W| = |\mathcal{D}(W)|$ (cf. Lemma 16.2).

Exercise 14.2. Show that for any set W, $\mathcal{D}(W)$ is an **algebra** over W, meaning that if $A, B \in \mathcal{D}(W)$, then $A \cup B$, $A \cap B$, $A \backslash B \in \mathcal{D}(W)$ as well.

Note that if $X \subseteq Y$, then $\mathcal{P}(X) \subseteq \mathcal{P}(Y)$. For definable powersets, this property may fail. Indeed, if $X \notin \mathcal{D}(Y)$, then $\mathcal{D}(X) \nsubseteq \mathcal{D}(Y)$ as $X \in \mathcal{D}(X)$. Nevertheless, we have the following:

Lemma 14.3. *If X and Y are sets such that $X \subseteq Y$ and $X \in Y$, then $\mathcal{D}(X) \subseteq \mathcal{D}(Y)$.*

Proof. Take any $A \in \mathcal{D}(X)$. We want to show that $A \in \mathcal{D}(Y)$. Write

$$A = \{a \in X : X \models f(a)\}$$

for some $f \in \mathcal{F}^1_X$. We can (exercise!) recursively build a $\mathcal{U}$-formula f^X by restricting the domain of every quantifier in f to X. Then all the parameters in f^X come from Y. (Note that f^X uses X as a parameter, but, thankfully, $X \in Y$.) This allows us to write

$$A = \{a \in Y : Y \models (a \dot{\in} X) \dot{\wedge} f^X(a)\} \in \mathcal{D}(Y).$$ ∎

14.2. The definition and basic properties of L

We can formally define L. For each ordinal α, we recursively build a set L_α as follows:

$$L_\alpha \ := \ \begin{cases} \varnothing & \text{if } \alpha = 0; \\ \mathcal{D}(L_\beta) & \text{if } \alpha = \beta + 1; \\ \bigcup\{L_\gamma \,:\, \gamma < \alpha\} & \text{if } \alpha \text{ is a limit ordinal,} \end{cases}$$

Gödel's constructible universe is the class L given by

$$L \ := \ \bigcup\{L_\alpha \,:\, \alpha \in \mathbf{Ord}\}.$$

A set x is called **constructible** if $x \in L$. The **order** of a constructible set x is

$$\mathrm{order}(x) \ := \ \min\{\alpha \in \mathbf{Ord} \,:\, x \in L_\alpha\}.$$

(This is analogous to the definition of rank for sets in V.)

Lemma 14.4. *Let α be an ordinal. Then:*

- *$L_\gamma \subseteq L_\alpha$ for all $\gamma \leqslant \alpha$, and*
- *the set L_α is transitive.*

Therefore, L is a transitive class.

Proof. There is a reason why we combined these two statements in one lemma: we will prove them simultaneously by induction on α. The cases when $\alpha = 0$ and α is a limit ordinal are clear (exercise!), so consider the case when $\alpha = \beta + 1$. By the inductive hypothesis, $L_\gamma \subseteq L_\beta$ for all $\gamma \leqslant \beta$, so to prove the first part of the lemma, we just need to show that $L_\beta \subseteq L_{\beta+1}$. Let $A \in L_\beta$. By the inductive assumption, L_β is transitive, so $A \subseteq L_\beta$. Then we may use A as a parameter and obtain

$$A \ = \ \{a \in L_\beta \,:\, L_\beta \models a \,\dot{\in}\, A\} \ \in \ \mathcal{D}(L_\beta) \ = \ L_{\beta+1},$$

as desired. To show that $L_{\beta+1}$ is transitive, consider any element $A \in L_{\beta+1}$. Then A is a definable subset of L_β. But we have already shown that $L_\beta \subseteq L_{\beta+1}$, so $A \subseteq L_\beta \subseteq L_{\beta+1}$, and we are done. ■

Exercise 14.3. Show that for each $\alpha \in \mathbf{Ord}$, $L_\alpha = \bigcup_{\gamma<\alpha} \mathcal{D}(L_\gamma)$.

Exercise 14.4. Show that for every constructible set x, $\mathrm{order}(x)$ is a successor ordinal, and if $y \in x$, then y is also constructible with $\mathrm{order}(y) < \mathrm{order}(x)$.

Exercise 14.5. Show that $L_\alpha \subseteq V_\alpha$ for all $\alpha \in \mathbf{Ord}$, and hence $L \subseteq V$.

Since for a finite set W, $\mathcal{D}(W) = \mathcal{P}(W)$, we conclude that

$$L_n = V_n \text{ for all } n \in \omega,$$

and hence also $L_\omega = V_\omega$. But on the next level the two hierarchies separate, as $L_{\omega+1} \neq V_{\omega+1}$, because $L_{\omega+1} = \mathcal{D}(L_\omega)$ is countable (see Exercise 14.1), while $V_{\omega+1} = \mathcal{P}(V_\omega)$ is not.

Lemma 14.5. *Every ordinal α is constructible with $\mathrm{order}(\alpha) = \alpha + 1$. In other words, for all $\alpha \in \mathbf{Ord}$, we have $\mathbf{Ord} \cap L_\alpha = \alpha$.*

Proof. The proof is by induction on α, so suppose that for all $\gamma < \alpha$, we have $\mathbf{Ord} \cap L_\gamma = \gamma$. Since $\mathbf{Ord} \cap L_\alpha \subseteq \mathbf{Ord} \cap V_\alpha = \alpha$, we only need to show that $\alpha \subseteq L_\alpha$. In other words, given any $\gamma < \alpha$, we have to argue that $\gamma \in L_\alpha$. But

$$\begin{aligned} \gamma \ = \ \mathbf{Ord} \cap L_\gamma \ &= \ \{x \in L_\gamma \,:\, x \text{ is an ordinal}\} \\ &= \ \{x \in L_\gamma \,:\, L_\gamma \models \ulcorner x \text{ is an ordinal}\urcorner\} \ \in \ \mathcal{D}(L_\gamma) \ = \ L_{\gamma+1} \ \subseteq \ L_\alpha, \end{aligned}$$

where we are using that being an ordinal can be defined by a Δ_0-formula (see Exercise 12.1(d)). ■

The proof of Lemma 14.5 can be summarized as follows: to construct the next ordinal, simply take the set of all ordinals that you have already constructed.

Corollary 14.6. *L is an inner model.*

PROOF. L is a transitive class by Lemma 14.4 and $\mathbf{Ord} \subseteq L$ by Lemma 14.5. ■

14.3. A preview of further results about L

Here we summarize the main properties of L that we will eventually demonstrate:

Theorem 14.7. *If $\mathcal{U} \models \mathsf{ZF}$, then $L \models \mathsf{ZFC} + \mathsf{GCH}$. Hence, if ZF is consistent, then so is $\mathsf{ZFC} + \mathsf{GCH}$.*

To advertise L even more, let us state a simple application of the above result. We say that a formula φ without parameters is **arithmetical** if all of its quantifiers are bounded by V_ω, i.e., are of the form "$\exists x \in V_\omega$" or "$\forall x \in V_\omega$."[xiv] The word "arithmetical" is used because V_ω is a countable set all of whose elements are finite, so arithmetical formulas are really statements about finite sets, and as such can be "encoded" as statements about natural numbers. Here are some examples of statements that can be formulated as arithmetical formulas:

Example 14.8. **Fermat's Last Theorem** is the assertion that

$$\forall x,\, y,\, z,\, n \in \omega \quad (x,\, y,\, z, \geqslant 1 \;\wedge\; n \geqslant 3 \quad \longrightarrow \quad x^n + y^n \neq z^n).$$

This statement was a notorious open problem for over 350 years (even though Pierre de Fermat claimed in 1637 that he had found "a truly marvelous proof of this, which this margin is too narrow to contain"), until it was finally proved by Andrew Wiles in 1994.

Example 14.9. Prime numbers p and q are called **twin primes** if $|p - q| = 2$. The **Twin Primes Conjecture** is the statement that there are infinitely many pairs of twin primes. It may seem "there are infinitely many" is an expression involving quantifying over infinite sets, but in fact the Twin Primes Conjecture can be written as an arithmetical statement:

$$\forall n \in \omega\, \exists p,\, q \in \omega \quad (p \geqslant n \;\wedge\; q \geqslant n \;\wedge\; p \text{ and } q \text{ are twin primes}).$$

This conjecture is still widely open.

Example 14.10. Another famous open problem that can be formulated as an arithmetical statement is the P **vs.** NP **Problem**. Roughly speaking, $\mathsf{P} \neq \mathsf{NP}$ is the statement that a certain computational problem called SAT (for "satisfiability") cannot be solved by a computer program whose running time is polynomial in the size of its input. In contrast to the previous examples, it is less clear why this is an arithmetical statement; the idea is that a computer program is a finite piece of text, and so it can be represented by a finite set in V_ω. The problem of whether $\mathsf{P} \neq \mathsf{NP}$ is one of the most celebrated open questions in mathematics. In particular, it is included on the list of the Millennium Prize Problems, so if you manage to solve it, the Clay Mathematics Institute will pay you $\$10^6$.

Since many important open problems can be formulated as arithmetical statements, it is natural to wonder whether stronger set-theoretic assumptions can simplify their solution. Recall, for example, Goodstein's Theorem 7.14: it is an arithmetical statement about natural numbers, and yet its proof involves arithmetic on infinite ordinals! However, Theorem 14.7 shows that the truth of arithmetical statements cannot be contingent on assumptions such as AC or CH:

Corollary 14.11. *Let φ be an arithmetical sentence. If φ can be proved in $\mathsf{ZFC} + \mathsf{GCH}$, then φ can be proved in ZF alone.*

PROOF. Suppose that φ is provable in $\mathsf{ZFC} + \mathsf{GCH}$ and let $\mathcal{U} \models \mathsf{ZF}$. By Theorem 14.7, $L \models \mathsf{ZFC} + \mathsf{GCH}$, and so $L \models \varphi$. But all quantifiers in φ are restricted to V_ω, and "V_ω" has the same meaning in $\mathcal{U}$ and in L (why?), so φ^L is equivalent to φ. Hence, $\mathcal{U} \models \varphi$, as desired. ■

[xiv] We do not view V_ω here as a parameter, because a formula of the form "$\exists x \in V_\omega\, (\ldots)$" can be rewritten as $\exists x\, (x \in V_\omega \wedge (\ldots))$," and the property "$x \in V_\omega$" can be expressed by a formula without parameters.

14.4. L satisfies ZF; the Reflection Principle

We begin our analysis by showing that L satisfies all of the axioms of ZF except for the Axiom Schemas of Comprehension and Replacement.

Lemma 14.12. *If* $\mathcal{U} \models \mathsf{ZF}$*, then* $L \models \mathsf{ZF} - \mathsf{Comp} - \mathsf{Rep}$.

PROOF. The axioms Ext, Empty, Inf, and AF are immediate.

- $L \models \mathsf{Pair}$: Take $x, y \in L$ and let $\alpha := \max\{\mathrm{order}(x), \mathrm{order}(y)\}$. Then $\{x, y\}$ is a finite (hence definable) subset of L_α, so $\{x, y\} \in L_{\alpha+1}$.
- $L \models \mathsf{Union}$: If $x \in L_\alpha$, then, since L_α is transitive, we have $\bigcup x \subseteq L_\alpha$, and thus
$$\bigcup x \;=\; \{z \in L_\alpha \,:\, L_\alpha \models \exists y \in x (z \in y)\} \;\in\; \mathcal{D}(L_\alpha) \;=\; L_{\alpha+1}.$$
- $L \models \mathsf{Pow}$: Let $x \in L$. We must argue that the following set is in L:
$$P \;:=\; \{y \in L \,:\, y \subseteq x\}.$$
To that end, let $\alpha := \sup\{\mathrm{order}(y) \,:\, y \in P\}$. Note that α is a well-defined ordinal, because P is a set and each $y \in P$ is constructible (so $\mathrm{order}(y)$ makes sense). Then $P \subseteq L_\alpha$, so
$$P \;=\; \{y \in L_\alpha \,:\, L_\alpha \models y \subseteq x\} \;\in\; \mathcal{D}(L_\alpha) \;=\; L_{\alpha+1}. \qquad \blacksquare$$

Next we want to show L satisfies the Axiom Schema of Comprehension. Let X, a_1, ..., $a_k \in L$ and let $\varphi(x, a_1, \ldots, a_k)$ be a formula with a free variable x and parameters a_1, ..., a_k. We need to prove that the following set is in L:
$$Y \;:=\; \{a \in X \,:\, L \models \varphi(a, a_1, \ldots, a_k)\}.$$
Take $\alpha \in \mathbf{Ord}$ such that X, a_1, ..., $a_k \in L_\alpha$ and define
$$Y' \;:=\; \{a \in X \,:\, L_\alpha \models \varphi(a, a_1, \ldots, a_k)\} \;=\; \{a \in L_\alpha \,:\, L_\alpha \models \varphi(a, a_1, \ldots, a_k) \wedge a \in X\} \;\in\; L_{\alpha+1}.$$
It would be great is we could show that $Y = Y'$, i.e., that L_α and L "agree" in their opinions on the formula φ. But how can we ensure that L_α "knows" what L will eventually "think" is true? The solution is provided by a general result known as the **Reflection Principle**.

First, we require some terminology. We say that $\mathcal{C} = \bigcup\{C_\alpha \,:\, \alpha \in \mathbf{Ord}\}$ is a **stratified class** if $\mathbf{Ord} \to \mathcal{U} \colon \alpha \mapsto C_\alpha$ is a class function such that:

- if $\alpha \leqslant \beta$, then $C_\alpha \subseteq C_\beta$,
- if α is a limit ordinal, then $C_\alpha = \bigcup\{C_\gamma \,:\, \gamma < \alpha\}$.

Prototypical examples of stratified classes are
$$V \;=\; \bigcup\{V_\alpha \,:\, \alpha \in \mathbf{Ord}\} \qquad \text{and} \qquad L \;=\; \bigcup\{L_\alpha \,:\, \alpha \in \mathbf{Ord}\}.$$
We wish to prove that if $\mathcal{C} = \bigcup\{C_\alpha \,:\, \alpha \in \mathbf{Ord}\}$ is a stratified class, then we can find an ordinal β such that the set C_β in some sense "reflects" the properties of the entire class $\mathcal{C}$.

Let $\mathcal{D} \subseteq \mathcal{C}$ be classes. Let $\varphi(x_1, \ldots, x_k)$ be a formula with free variables x_1, ..., x_k and without parameters. We say that φ is **absolute** between $\mathcal{D}$ and $\mathcal{C}$ if for all a_1, ..., $a_k \in \mathcal{D}$,
$$\mathcal{D} \models \varphi(a_1, \ldots, a_k) \quad\Longleftrightarrow\quad \mathcal{C} \models \varphi(a_1, \ldots, a_k).$$
In other words, φ is absolute between $\mathcal{D}$ and $\mathcal{C}$ if $\mathcal{D}$ and $\mathcal{C}$ agree on the truth value of φ whenever it is applied to elements of $\mathcal{D}$. Now we can state the aforementioned Reflection Principle:

Theorem 14.13 (Reflection Principle)**.** *Let* $\mathcal{C} = \bigcup\{C_\alpha \,:\, \alpha \in \mathbf{Ord}\}$ *be a stratified class and let* φ_1*, ...,* φ_n *be a finite list of formulas without parameters. Then there is an ordinal* β *such that all the formulas* φ_1*, ...,* φ_n *are absolute between* C_β *and* $\mathcal{C}$.

Note that Theorem 14.13 is really a "theorem schema," in the sense that it cannot be phrased as a single formula in the language of set theory, since it involves quantification over finite lists of formulas. (Here we mean *really* finite, not indexed by an element of ω.) On a related note, it is impossible to replace "formulas" by "$\mathcal{U}$-formulas" in Theorem 14.13, because there is no sense in which $\mathcal{C} \models f$ if f is a $\mathcal{U}$-formula and $\mathcal{C}$ is a proper class (see §13.4).

Example 14.14. Suppose that $\varphi_1, \ldots, \varphi_n$ are sentences satisfied by V (for instance, $\varphi_1, \ldots, \varphi_n$ could be some of the axioms of ZF). By the Reflection Principle, there is an ordinal β such that $\varphi_1, \ldots, \varphi_n$ are absolute between V_β and V; in other words, $V_\beta \models \varphi_1 \wedge \ldots \wedge \varphi_n$. Thus, we can always find V_β in which any given *finite* part of ZF holds! (Compare this to Theorem 12.6.)

The Reflection Principle is often applied in the form of the following corollary:

Corollary 14.15. *Let $\mathcal{C} = \bigcup\{C_\alpha : \alpha \in \mathbf{Ord}\}$ be a stratified class and let $\varphi_1, \ldots, \varphi_n$ be a finite list of formulas without parameters. Then for every $\gamma \in \mathbf{Ord}$, there is $\beta \geqslant \gamma$ such that $\varphi_1, \ldots, \varphi_n$ are absolute between C_β and $\mathcal{C}$.*

Proof. For each $\alpha \in \mathbf{Ord}$ define $C'_\alpha := C_{\gamma+\alpha}$. Then $\mathcal{C} = \bigcup\{C'_\alpha : \alpha \in \mathbf{Ord}\}$ is still a stratified class, so, by Theorem 14.13, there is $\delta \in \mathbf{Ord}$ such that $\varphi_1, \ldots, \varphi_n$ are absolute between $C'_\delta = C_{\gamma+\delta}$ and $\mathcal{C}$. Setting $\beta := \gamma + \delta$ finishes the proof. ■

Exercise 14.6. Deduce from Theorem 14.13 the following strengthening: Let $\mathcal{C} = \bigcup\{C_\alpha : \alpha \in \mathbf{Ord}\}$ be a stratified class and let $\varphi_1, \ldots, \varphi_n$ be a finite list of formulas without parameters. Then there is an infinite cardinal κ such that $\varphi_1, \ldots, \varphi_n$ are absolute between C_κ and $\mathcal{C}$.

With the help of the Reflection Principle, we can now finish the proof that $L \models \mathsf{ZF}$:

Theorem 14.16. *If $\mathcal{U} \models \mathsf{ZF}$, then $L \models \mathsf{ZF}$.*

Proof. Thanks to Lemma 14.12, it only remains to show that L satisfies Comprehension and Replacement. We shall prove $L \models \mathsf{Comp}$, leaving $L \models \mathsf{Rep}$ as an exercise.

Let $X, a_1, \ldots, a_k \in L$ and let $\varphi(x, a_1, \ldots, a_k)$ be a formula with a free variable x and parameters $a_1, \ldots, a_k$. As discussed earlier, we want to prove that the following set is in L:

$$Y := \{a \in X : L \models \varphi(a, a_1, \ldots, a_k)\}.$$

Let γ be an ordinal such that $X, a_1, \ldots, a_k \in L_\gamma$. By the Reflection Principle, there is an ordinal $\beta \geqslant \gamma$ such that φ is absolute between L_β and L. Then

$$\begin{aligned} Y &= \{a \in L_\beta : L \models \varphi(a, a_1, \ldots, a_k) \wedge a \in X\} \\ \text{[by absoluteness]} \quad &= \{a \in L_\beta : L_\beta \models \varphi(a, a_1, \ldots, a_k) \wedge a \in X\} \in L_{\beta+1}. \end{aligned}$$ ■

In the next subsection, we shall prove Theorem 14.13.

14.5. Proof of the Reflection Principle

Suppose that $\mathcal{C} = \bigcup\{C_\alpha : \alpha \in \mathbf{Ord}\}$ is a stratified class and let $\varphi_1, \ldots, \varphi_n$ be a finite list of formulas without parameters. For simplicity, we will assume that the formulas φ_i are constructed using only $\in$, $=$, $\wedge$, $\neg$, and $\exists$ as logical symbols (but not $\vee$ and $\forall$). (See footnote [xi].) More importantly, we shall assume that the list $\varphi_1, \ldots, \varphi_n$ together with each formula φ contains *all of φ's subformulas*. For instance, if the formula

$$\exists y\, (y \in x \wedge \neg\exists z\, (z \in y)) \qquad \text{(i.e., } \varnothing \in x\text{)}$$

is on the list, then so should be

$$y \in x \wedge \neg\exists z\, (z \in y), \qquad y \in x, \qquad \neg\exists z\, (z \in y), \qquad \exists z\, (z \in y), \qquad \text{and} \qquad z \in y.$$

Finally, we reorder the list $\varphi_1, \ldots, \varphi_n$ in such a way that for each formula φ_i, all its subformulas appear among $\varphi_1, \ldots, \varphi_i$. For instance, we could have $n = 6$ and

$$\begin{aligned}
\varphi_1 &= z \in y, \\
\varphi_2 &= \exists z\,(z \in y); \\
\varphi_3 &= \neg\exists z\,(z \in y), \\
\varphi_4 &= y \in x, \\
\varphi_5 &= y \in x \ \wedge\ \neg\exists z\,(z \in y), \\
\varphi_6 &= \exists y\ (y \in x\ \wedge\ \neg\exists z\,(z \in y)).
\end{aligned} \tag{14.1}$$

Consider any $\alpha \in \mathbf{Ord}$ and suppose that not all of $\varphi_1, \ldots, \varphi_n$ are absolute between C_α and $\mathcal{C}$. Let i be the smallest index such that φ_i is not absolute between C_α and $\mathcal{C}$ and set $\varphi := \varphi_i$. Suppose that φ has k free variables $x_1, \ldots, x_k$. By the choice of φ, all φ's subformulas, except φ itself, are absolute between C_α and $\mathcal{C}$. What can φ look like? It certainly cannot be a basic formula of the form $x = y$ or $x \in y$, because such formulas are always absolute. Neither can it be of the form $\varphi = \psi_1 \wedge \psi_2$: if it were, then the subformulas ψ_1 and ψ_2 would be absolute between C_α and $\mathcal{C}$, and thus, for all $a_1, \ldots, a_k \in C_\alpha$, we would have

$$\begin{aligned}
C_\alpha \models \varphi(a_1, \ldots, a_k) \quad &\Longleftrightarrow \quad C_\alpha \models \psi_1(a_1, \ldots, a_k) \text{ and } C_\alpha \models \psi_2(a_1, \ldots, a_k) \\
&\Longleftrightarrow \quad \mathcal{C} \models \psi_1(a_1, \ldots, a_k) \text{ and } \mathcal{C} \models \psi_2(a_1, \ldots, a_k) \\
&\Longleftrightarrow \quad \mathcal{C} \models \varphi(a_1, \ldots, a_k).
\end{aligned}$$

Similarly, φ cannot be of the form $\varphi = \neg\psi$, for then ψ would be absolute between C_α and $\mathcal{C}$, and so φ would be absolute as well. Therefore, φ must be of the form

$$\varphi(x_1, \ldots, x_k) \ =\ \exists x\,\psi(x, x_1, \ldots, x_k). \tag{14.2}$$

Again, the subformula ψ is absolute between C_α and $\mathcal{C}$, which yields that for all $a_1, \ldots, a_k \in C_\alpha$,

$$\begin{aligned}
C_\alpha \models \varphi(a_1, \ldots, a_k) \quad &\Longleftrightarrow \quad \exists a \in C_\alpha \text{ such that } C_\alpha \models \psi(a, a_1, \ldots, a_k) \\
&\Longleftrightarrow \quad \exists a \in C_\alpha \text{ such that } \mathcal{C} \models \psi(a, a_1, \ldots, a_k) \\
&\Longrightarrow \quad \exists a \in \mathcal{C} \text{ such that } \mathcal{C} \models \psi(a, a_1, \ldots, a_k) \\
&\Longleftrightarrow \quad \mathcal{C} \models \varphi(a_1, \ldots, a_k).
\end{aligned}$$

Thus, the only reason why φ is not absolute is that for some $a_1, \ldots, a_k \in C_\alpha$, we have

$$\exists a \in \mathcal{C} \text{ such that } \mathcal{C} \models \psi(a, a_1, \ldots, a_k), \qquad \text{but} \qquad \neg\exists a \in C_\alpha \text{ such that } \mathcal{C} \models \psi(a, a_1, \ldots, a_k).$$

This discussion motivates the following definition: Given a formula φ of the form (14.2) and elements $a_1, \ldots, a_k \in \mathcal{C}$, let $W_\varphi(a_1, \ldots, a_k)$ denote the least ordinal α such that

$$\exists a \in C_\alpha \text{ with } \mathcal{C} \models \psi(a, a_1, \ldots, a_k),$$

if such α exists (i.e., if $\mathcal{C} \models \varphi(a_1, \ldots, a_k)$), and 0 otherwise. The letter "W" here stands for "*witness*": the truth of the statement "$\mathcal{C} \models \varphi(a_1, \ldots, a_k)$" is *witnessed* by some $a \in C_{W_\varphi(a_1, \ldots, a_k)}$. Given an ordinal α, define

$$W_\varphi(\alpha) \ :=\ \sup\{W_\varphi(a_1, \ldots, a_k) \ :\ a_1, \ldots, a_k \in C_\alpha\},$$

and let

$$W(\alpha) \ :=\ \max\{W_\varphi(\alpha) \ :\ \varphi \text{ is on the list } \varphi_1, \ldots, \varphi_n\}. \tag{14.3}$$

At this point, we should emphasize that the expression on the right-hand side of (14.3) is defined by listing *explicitly* the relevant formulas (rather than by quantifying over them, which is not allowed). For instance, if our list of formulas were given by (14.1), then we would write

$$W(\alpha) \ :=\ \max\{W_{\exists z\,(z \in y)}(\alpha),\ W_{\exists y\,(y \in x\,\wedge\,\neg\exists z\,(z \in y))}(\alpha)\}.$$

Now we recursively define ordinals β_m for $m \in \omega$ by setting

$$\beta_0 := 0, \qquad \text{and} \qquad \beta_{m+1} := W(\beta_m) \text{ for all } m \in \omega.$$

Finally, let

$$\beta := \sup\{\beta_m : m \in \omega\}.$$

We claim that the formulas $\varphi_1, \ldots, \varphi_n$ are absolute between C_β and $\mathcal{C}$, as desired. As observed above, we only have to argue that if φ is one of the formulas among $\varphi_1, \ldots, \varphi_n$ of the form (14.2), then for all $a_1, \ldots, a_k \in C_\beta$,

$$\mathcal{C} \models \varphi(a_1, \ldots, a_k) \quad \Longrightarrow \quad \exists a \in C_\beta \text{ such that } \mathcal{C} \models \psi(a, a_1, \ldots, a_k). \tag{14.4}$$

To that end, notice that $0 = \beta_0 \leqslant \beta_1 \leqslant \beta_2 \leqslant \cdots \leqslant \beta$ (exercise!), so

$$C_\beta = \bigcup\{C_{\beta_m} : m \in \omega\}.$$

This means that for any $a_1, \ldots, a_k \in C_\beta$, there is some $m \in \omega$ with $a_1, \ldots, a_k \in C_{\beta_m}$. Assuming that $\mathcal{C} \models \varphi(a_1, \ldots, a_k)$, this implies that there is some $a \in C_{\beta_{m+1}} \subseteq C_\beta$ satisfying $\mathcal{C} \models \psi(a, a_1, \ldots, a_k)$, which yields (14.4) and finishes the proof.

Exercise 14.7. Pinpoint exactly every place in this argument where we used the assumption that $\mathcal{C} = \bigcup\{C_\alpha : \alpha \in \mathbf{Ord}\}$ is a stratified class.

14.6. Σ_1-formulas and the Axiom of Constructibility

The **Axiom of Constructibility** is the assertion that every set is constructible, i.e., that $\mathcal{U} = L$.[xv]:

Constructibility

Every set is constructible.

The goal of this section is to prove that the Axiom of Constructibility holds in L:

Theorem 14.17. *L satisfies the Axiom of Constructibility.*

Theorem 14.17 can be understood as follows. Consider a universe $\mathcal{U}$ satisfying ZF. Then, by Theorem 14.16, the class L, as defined in $\mathcal{U}$, also satisfies ZF. This means that the definition of L can be interpreted inside L, producing some subclass $L' \subseteq L$. In other words, L' is L's version of L: it is the class of all sets $x \in L$ such that $L \models$ "x is constructible." Theorem 14.17 then asserts that, in fact, $L' = L$; or, using the terminology developed in §14.4, the property of being constructible is absolute between L and $\mathcal{U}$.

How can we prove Theorem 14.17? It would be ideal if the statement "x is constructible" were equivalent to a Δ_0-formula, because then it would automatically be absolute between L and $\mathcal{U}$. Unfortunately, it is not necessarily equivalent to a Δ_0-formula; however, it is equivalent to a formula in a somewhat wider class—namely to a Σ_1-*formula*.

Let φ be a formula in the language of set theory. We say that φ is a Σ_1-**formula** if it is obtained from a Δ_0-formula by adding a sequence of *existential* and *bounded universal* quantifiers. For instance, if ψ is a Δ_0-formula, then

$$\exists x\, \exists y\, \forall z \in y\, \exists u\, \forall v \in u\, \exists w \quad \psi$$

is a Σ_1-formula. Also, a Π_1-**formula** is a formula that is obtained from Δ_0-formula by adding a sequence of *universal* and *bounded existential* quantifiers. For instance, if ψ is Δ_0, then

$$\forall x\, \forall y\, \exists z \in y\, \forall u\, \exists v \in u\, \forall w \quad \psi$$

is Π_1. Observe that the negation of any Σ_1-formula is equivalent to a Π_1-formula; conversely, every Π_1-formula is equivalent to the negation of some Σ_1-formula.

[xv] Often it is stated as "$V = L$," because $\mathcal{U} = V$ by AF.

Example 14.18. The statement "x is finite" can be expressed by a Σ_1-formula:

$$x \text{ is finite} \iff \exists n \, \exists f \, (\underbrace{n \in \omega \text{ and } f \text{ is a bijection from } n \text{ to } x}_{\Delta_0}).$$

Assuming AC, it can also be expressed by a *negation* of a Σ_1-formula (and hence by a Π_1-formula):

$$x \text{ is finite} \iff \neg \exists f \, (\underbrace{f \text{ is an injection from } \omega \text{ to } x}_{\Delta_0}).$$

Example 14.19. The statement "x is countable" can be expressed by a Σ_1-formula:

$$x \text{ is countable} \iff \exists f \, (\underbrace{f \text{ is an injection from } x \text{ to } \omega}_{\Delta_0}).$$

Exercise 14.8. Let φ and ψ be Σ_1-formulas (resp. Π_1-formulas). Show that $\varphi \wedge \psi$ and $\varphi \vee \psi$ are also equivalent to Σ_1-formulas (resp. Π_1-formulas).

Example 14.20. The statement "κ is a cardinal" can be expressed by a Π_1-formula:

$$\kappa \text{ is a cardinal} \iff \underbrace{\kappa \in \mathbf{Ord}}_{\Delta_0} \wedge \neg \underbrace{\exists \alpha \in \kappa \, \exists f \, (f \text{ is a bijection from } \alpha \text{ to } \kappa)}_{\Sigma_1}.$$

Example 14.21. The statement "$y = \mathcal{P}(x)$" can be expressed by a Π_1-formula:

$$y = \mathcal{P}(x) \iff \forall z \, (z \in y \longleftrightarrow z \subseteq x).$$

Exercise 14.9. Show that the statement "R is a well-ordering on a set S" can be expressed both by a Σ_1-formula and by a Π_1-formula.

Exercise 14.10. Assuming AC, show that every Σ_1-formula is equivalent to a formula of the form $\exists x \, \psi$, where ψ is Δ_0.

In contrast to Δ_0-formulas, Σ_1-formulas may not have the same truth value in $\mathcal{U}$ and in a transitive class $\mathcal{C}$. However, *if* a transitive class $\mathcal{C}$ satisfies a Σ_1-formula φ, *then* φ holds in $\mathcal{U}$ as well:

Exercise 14.11 (important!). Show that if $\mathcal{C}$ is a transitive class and φ is a Σ_1-formula with no free variables and with parameters from $\mathcal{C}$, then

$$\mathcal{C} \models \varphi \implies \mathcal{U} \models \varphi.$$

Example 14.22. Suppose that $\mathcal{C}$ is a transitive class containing **Ord**. Then $\mathbf{Card}^{\mathcal{C}} \supseteq \mathbf{Card}$, because the statement "x is not a cardinal" is Σ_1.

We say that a class $\mathcal{C}$ is Σ_1 (resp. Π_1) if there exists a Σ_1-formula (resp. a Π_1-formula) $\varphi(x)$ *without parameters* such that $x \in \mathcal{C} \iff \varphi(x)$. Similarly, we say that a class function Φ is Σ_1 (resp. Π_1) if there is a Σ_1-formula (resp. a Π_1-formula) $\varphi(x, y)$ without parameters such that $\Phi(x) = y \iff \varphi(x, y)$. Unless explicitly stated otherwise, we always assume that the "background theory" is ZF. For instance, the class of all finite sets is Σ_1 (and it is Π_1 if AC holds; see Example 14.18).

Lemma 14.23. *Let Φ be a Σ_1-class function such that* $\mathrm{dom}(\Phi)$ *is a Π_1-class. Then Φ is also Π_1.*

Proof. Since Φ is a class function, for every $x \in \mathrm{dom}(\Phi)$, there is precisely one set y such that $\Phi(x) = y$. Hence, we can write

$$\Phi(x) = y \iff \underbrace{x \in \mathrm{dom}(\Phi)}_{\Pi_1} \wedge \forall z \, (z = y \vee \overbrace{\neg(\underbrace{\Phi(x) = z}_{\Sigma_1})}^{\Pi_1}).$$ ■

Before moving on, let us make a few observations that will help us show that certain classes and class functions are Σ_1. We say that a set A is Σ_1-**identifiable** if the class $\{A\}$ is Σ_1; in other words, if there is a Σ_1-formula $\varphi(x)$ without parameters such that

$$x = A \iff \varphi(x).$$

For instance, ω is Σ_1-identifiable, since the property "$x = \omega$" can be expressed by a Δ_0-formula (and every Δ_0-formula is Σ_1). If A is a Σ_1-identifiable set, then quantifiers ranging over A (i.e., of the form "$\exists x \in A$" and "$\forall x \in A$") can be used in Σ_1-definitions:

$$\exists x \in A\,(\ldots) \iff \exists z\,(z = A \ \wedge\ \exists x \in z\,(\ldots));$$

$$\forall x \in A\,(\ldots) \iff \exists z\,(z = A \ \wedge\ \forall x \in z\,(\ldots)).$$

In particular, we can freely quantify over ω when defining Σ_1-classes and Σ_1-class functions. Another observation is that if Φ is a Σ_1-class function (i.e., the statement "$\Phi(x) = y$" is given by a Σ_1-formula without parameters), then the statement "$z \in \Phi(x)$" can be expressed by a Σ_1-formula as follows:

$$z \in \Phi(x) \iff \exists y\,(\Phi(x) = y \ \wedge\ z \in y).$$

Exercise 14.12. Let Φ and Ψ be Σ_1-functions. Show that the composition $\Phi \circ \Psi$ is also Σ_1, i.e., the statement "$z = \Phi(\Psi(x))$" is equivalent to a Σ_1-formula without parameters.

Our next observation is that *recursive definitions* are naturally Σ_1. To make this statement precise, we need to recall some terminology from §3.3. Let $\mathcal{E}$ be a class function. A function f is called $\mathcal{E}$-**inductive** if the domain of f is an ordinal α and, for all $\beta < \alpha$, we have $f(\beta) = \mathcal{E}(f{\restriction}\beta)$. We also say that a class function $F\colon \mathbf{Ord} \to \mathcal{U}$ is $\mathcal{E}$-**inductive** if $F(\beta) = \mathcal{E}(F{\restriction}\beta)$ for all $\beta \in \mathbf{Ord}$, i.e., if for all $\alpha \in \mathbf{Ord}$, the function $F{\restriction}\alpha$ is $\mathcal{E}$-inductive. The class version of transfinite recursion (Theorem 3.11) says that if every $\mathcal{E}$-inductive function belongs to $\mathrm{dom}(\mathcal{E})$, then there is a unique $\mathcal{E}$-inductive class function $F\colon \mathbf{Ord} \to \mathcal{U}$. It turns out that if $\mathcal{E}$ is Σ_1, then F is Σ_1 as well:

Theorem 14.24 (Σ_1-Recursion)**.** *Let $\mathcal{E}$ be a Σ_1-class function such that every $\mathcal{E}$-inductive function belongs to* $\mathrm{dom}(\mathcal{E})$. *Then the unique $\mathcal{E}$-inductive class function $F\colon \mathbf{Ord} \to \mathcal{U}$ is also Σ_1.*

PROOF. We have

$$\begin{aligned} F(\alpha) = y \iff\ & \overbrace{\alpha \in \mathbf{Ord}}^{\Delta_0} \ \wedge \\ & \exists f\,(\underbrace{f \text{ is a function}}_{\Delta_0} \ \wedge\ \underbrace{\mathrm{dom}(f) = \alpha + 1}_{\Delta_0} \ \wedge\ f \text{ is } \mathcal{E}\text{-inductive} \ \wedge\ \underbrace{f(\alpha) = y}_{\Delta_0}). \end{aligned}$$

It remains to check that "f is $\mathcal{E}$-inductive" is a Σ_1-statement. By definition,

$$\begin{aligned} f \text{ is } \mathcal{E}\text{-inductive} &\iff \forall \beta \leqslant \alpha\,(f(\beta) = \mathcal{E}(f{\restriction}\beta)) \\ &\iff \forall \beta \in \alpha\,(f(\beta) = \mathcal{E}(f{\restriction}\beta)) \ \wedge\ f(\alpha) = \mathcal{E}(f{\restriction}\alpha). \end{aligned}$$

At this point, we just have to show that the statement "$f(\beta) = \mathcal{E}(f{\restriction}\beta)$" is Σ_1. This follows from Exercise 14.12; explicitly, we can write

$$f(\beta) = \mathcal{E}(f{\restriction}\beta) \iff \exists g\,\exists z\,(\underbrace{g = f{\restriction}\beta}_{\Delta_0} \ \wedge\ \underbrace{z = \mathcal{E}(g)}_{\Sigma_1} \ \wedge\ \underbrace{f(\beta) = z}_{\Delta_0}).$$ ■

Exercise 14.13. State and prove the version of Theorem 14.24 for recursion up to ω.

Example 14.25. For a set x, let $\mathrm{cl}(x)$ denote the transitive closure of x, i.e., the smallest transitive set y such that $x \subseteq y$. The class function $x \mapsto \mathrm{cl}(x)$ is clearly Π_1:

$$y = \mathrm{cl}(x) \iff y \text{ is transitive} \ \wedge\ x \subseteq y \ \wedge\ \forall z\,((z \text{ is transitive} \ \wedge\ x \subseteq z) \longrightarrow y \subseteq z)\,.$$

On the other hand, the transitive closure of x can be defined recursively, showing that the class function $x \mapsto \mathrm{cl}(x)$ is Σ_1. Indeed, if we set

$$f(0) := x, \qquad \text{and} \qquad f(n+1) := \bigcup f(n) \text{ for all } n \in \omega,$$

then $\mathrm{cl}(x) = \bigcup_{n\in\omega} f(n)$, so we may invoke Theorem 14.24 (or rather Exercise 14.13) to conclude that $x \mapsto \mathrm{cl}(x)$ is a Σ_1-class function. Explicitly, we can write

$$\begin{aligned} y = \mathrm{cl}(x) \quad \iff \quad & \exists f \Big(f \text{ is a function } \wedge \mathrm{dom}(f) = \omega \wedge \\ & f(0) = x \wedge \forall n \in \omega \left(f(n+1) = \bigcup f(n) \right) \wedge y = \bigcup_{n\in\omega} f(n) \Big), \end{aligned}$$

and it is not hard to verify that this definition is Σ_1 (exercise!).

Now we can apply these results to the study of the constructible universe L:

Lemma 14.26. *The class function* **Ord** $\to \mathcal{U}\colon \alpha \mapsto L_\alpha$ *is* Σ_1*.*

Proof. We begin by noting that various constructions that have to do with $\mathcal{U}$-formulas are defined recursively and hence are Σ_1. These include:

the class $\{\mathcal{F}\}$, the class function $W \mapsto \mathcal{F}_W$, the class function $(f, a) \mapsto f(a)$,

and so on. Proving that these classes and class functions are Σ_1 involves an analysis similar to that performed in Example 14.25, and we omit it (but the reader is encouraged to do at least some of it as an exercise). Of particular importance is the class function Truth given by Theorem 13.3:

$$\mathsf{Truth}(W, f) = \begin{cases} 1 & \text{if } W \models f, \\ 0 & \text{if } W \models \neg f. \end{cases}$$

To see that the class function Truth is Σ_1, one can either invoke Theorem 14.24, or explicitly write

$$\begin{aligned} \mathsf{Truth}(W, f) = i \quad \iff \quad & f \in \mathcal{F}^0_W \wedge \exists T\, (T \text{ is a function } \wedge \mathrm{dom}(T) = \mathcal{F}^0_W \wedge \\ & \forall g \in \mathcal{F}^0_W \left[T(g) = \begin{cases} 1 & \text{if } g = (a \doteq b) \text{ and } a = b; \\ 1 & \text{if } g = (a \mathbin{\dot\in} b) \text{ and } a \in b; \\ 1 & \text{if } g = (h \mathbin{\dot\wedge} h') \text{ and } T(h) = T(h') = 1; \\ 1 & \text{if } g = (\dot\neg\, h) \text{ and } T(h) = 0; \\ 1 & \text{if } g = (\dot\exists x\, h) \text{ and } \exists a \in W\, (T(h(a)) = 1); \\ 0 & \text{otherwise.} \end{cases} \right] \\ & \wedge\ T(f) = i). \end{aligned}$$

Next we observe that the statement "$A = \{a \in W : W \models f(a)\}$," where $f \in \mathcal{F}^1_W$, is Σ_1:

$$\begin{aligned} A = \{a \in W : W \models f(a)\} \quad \iff \quad & f \in \mathcal{F}^1_W \wedge \forall a \in A\, (a \in W \wedge \mathsf{Truth}(W, f(a)) = 1) \wedge \\ & \forall a \in W\, (\mathsf{Truth}(W, f(a)) = 0 \vee a \in A). \end{aligned}$$

Therefore, the statement "A is a definable subset of W" is also Σ_1:

$$A \text{ is definable in } W \quad \iff \quad \exists f \in \mathcal{F}^1_W\, (A = \{a \in W : W \models f(a)\}).$$

Hence, the class function $W \mapsto \mathcal{D}(W)$ is Σ_1:

$$\begin{aligned} \mathcal{D}(W) = Y \quad \iff \quad & \forall A \in Y\, (A \text{ is definable in } W) \wedge \\ & \forall f \in \mathcal{F}^1_W\, \exists A \in Y\, (A = \{a \in W : W \models f(a)\}). \end{aligned}$$

Notice the slight subtlety in this definition. Its second line is intended to say that every definable subset of W is in Y, but we are not allowed to quantify over all *subsets* of W, so instead we use a quantifier ranging over $\mathcal{F}^1_W$, which is acceptable because the class function $W \mapsto \mathcal{F}^1_W$ is Σ_1.

Finally, the class function $\alpha \mapsto L_\alpha$ is defined recursively by repeatedly applying the definable powerset operation, so, by Theorem 14.24, it is Σ_1. Again, the explicit Σ_1-definition of this class function is as follows:

$$\begin{aligned} W = L_\alpha \quad \iff \quad & \alpha \in \mathbf{Ord} \ \wedge \ \exists f \Big(f \text{ is a function } \wedge \ \mathrm{dom}(f) = \alpha + 1 \ \wedge \ f(0) = \varnothing \ \wedge \\ & \forall \beta < \alpha \, (f(\beta + 1) = \mathcal{D}(f(\beta))) \ \wedge \\ & \forall \beta \leqslant \alpha \, \Big(\beta \text{ is a limit} \to f(\beta) = \bigcup \{ f(\gamma) \,:\, \gamma < \beta \}\Big) \ \wedge \ f(\alpha) = W \Big). \end{aligned}$$ ■

Proof *of Theorem 14.17.* By Lemma 14.26, there is a Σ_1-formula $\varphi(x, y)$ such that $\varphi(\alpha, W)$ holds if and only if $\alpha \in \mathbf{Ord}$ and $W = L_\alpha$. Consider the class L and let α be an arbitrary ordinal. By Theorem 14.16, $L \models \mathsf{ZF}$. In particular,

$$L \models \text{“there is a unique set } W \text{ such that } \varphi(\alpha, W)\text{,”}$$

since the statement that for every ordinal α, there is a unique set W with $\varphi(\alpha, W)$, is a *theorem* of ZF. Let $W_\alpha \in L$ be the unique set such that $L \models \varphi(\alpha, W_\alpha)$; in other words, W_α is “L's version” of L_α. Since φ is a Σ_1-formula, by Exercise 14.11, the truth of φ “lifts” from L to $\mathcal{U}$, and thus

$$L \models \varphi(\alpha, W_\alpha) \quad \Longrightarrow \quad \mathcal{U} \models \varphi(\alpha, W_\alpha).$$

But $\mathcal{U} \models \varphi(\alpha, W_\alpha)$ means that $W_\alpha = L_\alpha$; i.e., “L's version” of L_α must actually coincide with the “real” L_α. And now we are done, since $L \models$ “every set is constructible” is equivalent to

$$L \ = \ \bigcup \{ W_\alpha \ : \ \alpha \in \mathbf{Ord} \},$$

which is true since $W_\alpha = L_\alpha$ for all $\alpha \in \mathbf{Ord}$ and $L = \bigcup \{L_\alpha, : \ \alpha \in \mathbf{Ord}\}$ by definition. ■

Exercise 14.14. Let $\mathcal{C} \supseteq \mathbf{Ord}$ be a transitive class such that $\mathcal{C} \models \mathsf{ZF}$. Show that $L \subseteq \mathcal{C}$.

Exercise 14.15 (Condensation lemma)**.** Let S be a transitive set such that

$$S \models \mathsf{ZF} + \text{“all sets are constructible.”}$$

Show that $S = L_\alpha$ for some ordinal α.

15. Problem set 5

The default axiom system is for the following problems is ZF.

Exercise 15.1. Show that the following properties and relations can be expressed by Δ_0-formulas without parameters:

(*a*) $x = y \times z$,

(*b*) f is a function,

(*c*) f is a bijection from x to y,

(*d*) n is a natural number,

(*e*) $x = \omega$.

Here x, y, z, f, α, and n should be treated as free variables.

Exercise 15.2. Show that the statement

$$\text{“}R \text{ is a well-ordering on a set } S,\text{”}$$

where S and R are free variables, is equivalent both to a Σ_1-formula and to a Π_1-formula.

Exercise 15.3. Fix a finite tuple $\vec{p} = (p_1, \ldots, p_n)$. A set a is **ordinal-definable over** $\vec{p}$ if there exist:

- a natural number $k \in \omega$,
- a sequence of ordinals $\alpha_1, \ldots, \alpha_k, \beta$ with $\beta > \alpha_1, \ldots, \alpha_k$ and $p_1, \ldots, p_n \in V_\beta$, and
- a $\mathcal{U}$-formula $f \in \mathcal{F}^{k+n+1}$ with $k + n + 1$ free variables and no parameters, such that

$$\{a\} \;=\; \{x \in V_\beta \,:\, V_\beta \models f(x, \alpha_1, \ldots, \alpha_k, p_1, \ldots, p_n)\}.$$

That is, a is ordinal-definable over $\vec{p}$ if there is a $\mathcal{U}$-formula f such that a is the unique element of some V_β for which f holds in V_β, where f is allowed to use $p_1, \ldots, p_n$ and arbitrary ordinals as parameters. The class of all sets that are ordinal-definable over $\vec{p}$ is denoted by $\mathbf{OD}(\vec{p})$. (Before moving on, you should convince yourself that $\mathbf{OD}(p)$ is indeed a class!) We also write $\mathbf{OD} \coloneqq \mathbf{OD}(\varnothing)$ and call sets $a \in \mathbf{OD}$ **ordinal-definable**. For example, every ordinal α is ordinal-definable:

$$\{\alpha\} \;=\; \{x \in V_{\alpha+1} \,:\, V_{\alpha+1} \models (x = \alpha)\}.$$

Similarly, for $\alpha, \beta \in \mathbf{Ord}$, the set $\{\alpha, \beta\}$ is ordinal-definable via

$$\{\{\alpha, \beta\}\} \;=\; \{x \in V_\gamma \,:\, V_\gamma \models (\alpha \in x \;\wedge\; \beta \in x \;\wedge\; \forall y \in x\, (y = \alpha \;\vee\; y = \beta))\},$$

where $\gamma = \max\{\alpha, \beta\} + 2$.

With these definitions, we are ready to state the problem. Let $\varphi(x, \vec{\alpha}, \vec{p})$ be a formula (not a $\mathcal{U}$-formula!) with a single free variable x and with parameters

$$\vec{\alpha} = (\alpha_1, \ldots, \alpha_k) \qquad \text{and} \qquad \vec{p} = (p_1, \ldots, p_n),$$

where $\alpha_1, \ldots, \alpha_k \in \mathbf{Ord}$. Suppose that a is the unique set satisfying $\varphi(a, \vec{\alpha}, \vec{p})$, i.e.,

$$\{a\} \;=\; \{x \,:\, \mathcal{U} \models \varphi(x, \alpha_1, \ldots, \alpha_k, p_1, \ldots, p_n)\}.$$

Show that $a \in \mathbf{OD}(\vec{p})$.

Exercise 15.4. Fix a finite tuple $\vec{p} = (p_1, \ldots, p_n)$.

(*a*) Let ${}^{<\omega}\mathbf{Ord}$ be the class of all finite tuples of ordinals. Show that there exists a bijective class function $\Phi \colon \mathbf{Ord} \to {}^{<\omega}\mathbf{Ord}$ defined by a formula without parameters.

(*b*) Show that there is a single formula $\xi(x, y, \vec{p})$ in the language of set theory with two free variables x, y and with parameters $\vec{p}$ such that for every $\gamma \in \mathbf{Ord}$, there is at most one set a for which $\xi(a, \gamma, \vec{p})$ holds, and

$$\mathbf{OD}(\vec{p}) \;=\; \{a \,:\, \exists \gamma \in \mathbf{Ord}\, \xi(a, \gamma, \vec{p})\}.$$

Exercise 15.5. Recall the Principle of Global Choice (GC) from Exercise 11.6:

There is a class function $\mathsf{G} \colon \mathcal{U} \to \mathcal{U}$ *such that for every set* $A \neq \varnothing$, $\mathsf{G}(A) \in A$.

Show that GC is equivalent to the assertion that there exists a finite tuple $\vec{p}$ such that every set is ordinal-definable over $\vec{p}$. This means that while the original statement of GC involves quantification over all class functions, it is actually equivalent to a single axiom:

$$\exists \vec{p} \left(\vec{p} \text{ is a finite tuple and } \forall a \, (a \in \mathbf{OD}(\vec{p}))\right).$$

Exercise 15.6. A set a is **hereditarily ordinal-definable** if a and all the elements of its transitive closure are ordinal-definable. The class of all hereditarily ordinal-definable sets is denoted by $\mathbf{HOD}$.

In this exercise, we establish the following result:

Theorem 15.1. *If* $\mathcal{U} \models \mathsf{ZF}$, *then* $\mathbf{HOD} \models \mathsf{ZFC}$.

(a) Show that $\mathbf{HOD}$ is a transitive class and $\mathbf{Ord} \subseteq \mathbf{HOD}$.

(b) Prove the following claims:

- $\mathbf{HOD}$ satisfies the Union Axiom,
- $\mathbf{HOD}$ satisfies the Powerset Axiom,
- $\mathbf{HOD}$ satisfies the Comprehension Schema,
- $\mathbf{HOD}$ satisfies the Replacement Schema.

(c) Show that $\mathbf{HOD}$ satisfies AC. **Caution:** You have to be careful because $\mathbf{HOD}$ might fail to satisfy GC. (This does not contradict the result of Exercise 15.5—do you see why?)

16. Further properties of L

16.1. L satisfies AC and the Principle of Global Choice

The goal of this subsection is to prove that $L \models \mathsf{AC}$, thus showing that if ZF is consistent, then ZFC is consistent as well. In fact, we will show that L satisfies a stronger version of AC, called the **Principle of Global Choice** (GC):

Global Choice (GC)

There is a class function $\mathsf{G}\colon \mathcal{U} \to \mathcal{U}$ such that for every nonempty set A, $\mathsf{G}(A) \in A$

See Exercise 11.6 for a list of statements equivalent to this principle. Note that the above statement of GC as well as its equivalent formulations given in Exercise 11.6 involve quantification over class functions (that is why we are calling it a "principle" and not an "axiom"). Nevertheless, it turns out to be equivalent to a certain single axiom—see Exercise 15.5.

Theorem 16.1. *The Axiom of Constructibility implies* GC*.*

From Theorems 14.17 and 16.1, it follows that L always satisfies GC (and hence AC), even if $\mathcal{U}$ does not. This is why we proved Theorem 14.17 first: now instead of worrying about the differences between L and $\mathcal{U}$, we may just assume that every set is constructible, i.e., $\mathcal{U} = L$.

The proof of Theorem 16.1 hinges on the following observation:

Lemma 16.2. *There exists a class function that, given a set W and a well-ordering $\prec$ on W, outputs a well-ordering $\prec^*$ on $\mathcal{D}(W)$.*

Proof. Every definable subset of W is given by a $\mathcal{U}$-formula with one free variable and with parameters from W, so we just have to well-order the set $\mathcal{F}^1_W$. To that end, we fix an arbitrary well-ordering $\lhd$ of $\mathcal{F}$, which exists since $\mathcal{F}$ is countable (see Exercise 13.1). Every $\mathcal{U}$-formula in $\mathcal{F}^1_W$ can be written as $f(x, \vec{a})$, where x is the free variable and $\vec{a} = (a_1, \ldots, a_k)$ is a finite tuple of parameters from W. Hence, we may identify the elements of $\mathcal{F}^1_W$ with pairs of the form $(f, \vec{a})$, where

$$f \;=\; f(x, x_1, \ldots, x_k) \in \mathcal{F} \qquad \text{and} \qquad \vec{a} \;=\; (a_1, \ldots, a_k) \in {}^{<\omega}W.$$

(Recall that ${}^{<\omega}W$ is the set of all finite tuples of elements of W.) The set ${}^{<\omega}W$ can be well-ordered, for example, lexicographically:

$$(a_1, \ldots, a_k) \prec_{\text{lex}} (b_1, \ldots, b_\ell) \quad :\Longleftrightarrow \quad (k < \ell) \text{ or } (k = \ell \text{ and } a_i \prec b_i, \text{ where } i \text{ is the least index such that } a_i \neq b_i).$$

This allows us to put a well-ordering $\lhd_{(W,\prec)}$ on $\mathcal{F}^1_W$ as follows:

$$(f, \vec{a}) \lhd_{(W,\prec)} (g, \vec{b}) \quad :\Longleftrightarrow \quad (f \lhd g) \text{ or } (f = g \text{ and } \vec{a} \prec_{\text{lex}} \vec{b}).$$

Finally, for each $A \in \mathcal{D}(W)$, let f_A be the $\lhd_{(W,\prec)}$-least $\mathcal{U}$-formula in $\mathcal{F}^1_W$ such that

$$A \;=\; \{a \in W \,:\, W \models f_A(a)\}.$$

Then we obtain a desired well-ordering on $\mathcal{D}(W)$ by setting

$$A \prec^* B \quad :\Longleftrightarrow \quad f_A \lhd_{(W,\prec)} f_B. \qquad \blacksquare$$

Proof *of Theorem 16.1.* Suppose every set is constructible, i.e., $\mathcal{U} = L$. We will show that there is a well-ordering of $\mathcal{U}$, which is a statement equivalent to GC (cf. Exercise 11.6). To this end, we recursively define well-orderings $\prec_\alpha$ on L_α, $\alpha \in \mathbf{Ord}$, as follows. To begin with, let $\prec_0$ be the empty ordering on $\varnothing = L_0$. Next, let $\beta \in \mathbf{Ord}$ and suppose that $\prec_\beta$ is already defined. Let $\prec_\beta^*$ be the well-ordering of $\mathcal{D}(L_\beta) = L_{\beta+1}$ given by Lemma 16.2. Then for each $x, y \in L_{\beta+1}$, we let

$$\begin{aligned} x \prec_{\beta+1} y \quad :\Longleftrightarrow \quad & (x, y \in L_\beta \text{ and } x \prec_\beta y) \text{ or} \\ & (x \in L_\beta \text{ and } y \in L_{\beta+1} \backslash L_\beta) \text{ or} \\ & (x, y \in L_{\beta+1} \backslash L_\beta \text{ and } x \prec_\beta^* y). \end{aligned}$$

This definition ensures that the ordering $\prec_{\beta+1}$ extends $\prec_\beta$ and that L_β is $\prec_{\beta+1}$-downward closed. This allows us to define, for limit ordinals α,

$$\prec_\alpha \,:=\, \bigcup_{\gamma<\alpha} \prec_\alpha .$$

Now let $\prec \,:=\, \bigcup\{\prec_\alpha \colon \alpha \in \mathbf{Ord}\}$. Then $\prec$ is a well-ordering of $L = \mathcal{U}$, and thus GC holds. ■

16.2. L satisfies GCH

Finally, we will prove in this subsection that L satisfies the Generalized Continuum Hypothesis:

Theorem 16.3. *The Axiom of Constructibility implies* GCH*.*

Again, by Theorem 14.17, L satisfied the Axiom of Constructibility, so Theorem 16.3 implies that $L \models \mathsf{GCH}$. This, in turn, means that if ZF is consistent, then so is ZF + GCH.

Recall that, by Theorem 10.1, GCH implies AC. Therefore, it is a consequence of Theorem 16.3 that $L \models \mathsf{AC}$. However, we will actually *use* that L satisfies AC in the proof of Theorem 16.3. In fact, for the remainder of this subsection we shall be working in ZFC.

The main ingredient in the proof of Theorem 16.3 is a remarkable fact concerning the cardinality of sets that can be identified using a Σ_1-formula.

Definition 16.4 (Σ_1-identifiable sets)**.** Let a be a set. We say that a set b is **Σ_1-identifiable over** a if there is a Σ_1-formula $\varphi(x, y)$ with two free variables x, y and without parameters such that

$$y = b \quad \Longleftrightarrow \quad \varphi(a, y),$$

i.e., if $\{y : \varphi(a, y)\} = \{b\}$.

How large, in terms of its cardinality, can a set that is Σ_1-identifiable over a given set a be? On the one hand, ω is Σ_1-identifiable (even without using a), and $|\omega| = \aleph_0$. On the other hand, a itself is Σ_1-identifiable over a (via the formula $y = a$); furthermore, by Example 14.25, the set $\mathrm{cl}(a)$ (i.e., the transitive closure of a) is also Σ_1-identifiable over a. It turns out that no set of strictly greater cardinality could be Σ_1-identifiable over a:

Lemma 16.5 (Gödel's Magic Lemma)**.** *Assume that* $\mathcal{U} \models \mathsf{ZFC}$*. Let a and b be sets and suppose that b is Σ_1-identifiable over a. Then*

$$|b| \leqslant \max\{\aleph_0, |\mathrm{cl}(a)|\}.$$

We will prove Lemma 16.5 in §16.3. It is a perfect example of the power of mathematical logic, in that it turns "syntactic" assumptions into "semantic" consequences. Using this lemma one can, simply by looking at a definition of a set b and making sure that it involves no unbounded universal quantifiers, obtain a sharp upper bound on $|b|$, without trying to understand what the definition actually *means* at all!

Proof *of Theorem 16.3* (*from Lemma 16.5*). Assume $\mathcal{U} = L$. By Theorem 16.1, this implies that AC holds, so we can talk about cardinalities and use Lemma 16.5.

We start by making two observations:

Observation 16.6. *For every infinite ordinal α, we have $|L_\alpha| = |\alpha|$.*

Proof. Since $\alpha \subseteq L_\alpha$, $|\alpha| \leqslant |L_\alpha|$. On the other hand, by Lemma 14.26, the set L_α is Σ_1-identifiable over α, and thus, by Lemma 16.5, we have

$$|L_\alpha| \leqslant \max\{\aleph_0, |\mathrm{cl}(\alpha)|\} = |\alpha|,$$

where we are using that $\mathrm{cl}(\alpha) = \alpha \geqslant \omega$. ☒

Recall that for a constructible set a, $\mathrm{order}(a)$ is the least ordinal α such that $a \in L_\alpha$.

Observation 16.7. *For every $a \in L$, $|\mathrm{order}(a)| \leqslant \max\{\aleph_0, |\mathrm{cl}(a)|\}$.*

Proof. In view of Lemma 16.5, we just have to show that $\mathrm{order}(a)$ is Σ_1-identifiable over a. And indeed, using Lemma 14.26, we obtain:

$$\begin{aligned}\alpha = \mathrm{order}(a) &\iff \alpha \in \mathbf{Ord} \wedge a \in L_\alpha \wedge \forall \beta < \alpha\, (a \notin L_\beta)\\ &\iff \alpha \in \mathbf{Ord} \wedge \exists W\, (\underbrace{W = L_\alpha}_{\Sigma_1} \wedge a \in W) \wedge \forall \beta \in \alpha\, \exists U\, (\underbrace{U = L_\beta}_{\Sigma_1} \wedge a \notin U).\end{aligned}$$ ☒

Let κ be an infinite cardinal. We have to show that $2^\kappa = |\mathcal{P}(\kappa)| \leqslant \kappa^+$. To that end, consider an arbitrary subset $A \subseteq \kappa$. Since $\mathcal{U} = L$, A is constructible, and, by Observation 16.7,

$$|\mathrm{order}(A)| \leqslant \max\{\aleph_0, |\mathrm{cl}(A)|\} \leqslant \kappa,$$

where we are using that κ is a transitive set and hence $\mathrm{cl}(A) \subseteq \kappa$. Therefore, $\mathrm{order}(A) < \kappa^+$, so

$$A \in L_{\kappa^+}.$$

Since this holds for every subset $A \subseteq \kappa$, we conclude that $\mathcal{P}(\kappa) \subseteq L_{\kappa^+}$, and thus, by Observation 16.6,

$$|\mathcal{P}(\kappa)| \leqslant |L_{\kappa^+}| = \kappa^+.$$ ■

Exercise 16.1. Suppose that $\mathcal{U} = L$. Show that for every ordinal α, $V_{\omega+\alpha} \subseteq L_{\aleph_\alpha}$.

Exercise 16.2. Suppose that $\mathcal{U} = L$ and let κ be a cardinal such that $\kappa = \aleph_\kappa$. Show that $V_\kappa = L_\kappa$.

16.3. Proof of Gödel's Magic Lemma

The proof of Lemma 16.5 relies on a combination of two important tools, the first of which is the so-called **Löwenheim–Skolem theorem**:

Theorem 16.8 (Löwenheim–Skolem)**.** *Assume $\mathcal{U} \models \mathsf{ZFC}$. Let $A \subseteq B$ be sets. Then there exists a set A^* such that $A \subseteq A^* \subseteq B$, $|A^*| \leqslant \max\{\aleph_0, |A|\}$, and for every $\mathcal{U}$-sentence $f \in \mathcal{F}^0_{A^*}$, we have*

$$A^* \models f \iff B \models f.$$

Theorem 16.8 might seem similar to the Reflection Principle, and with good reason: its proof relies on a similar process of adding witnesses to existential statements (called *Skolemization*).

Proof. Let $S \subseteq B$ and suppose that there is some $\mathcal{U}$-formula $f \in \mathcal{F}^0_S$ such that $S \models f \not\Longleftrightarrow B \models f$. Consider such f of the lowest possible complexity. The same analysis as in the proof of the Reflection Principle (see §14.5) shows that f must be of the form $f = \dot{\exists} x\, g(x)$ for some $g \in \mathcal{F}^1_S$, which yields the following result, known as the **Tarski–Vaught test**:

Exercise 16.3 (Tarski–Vaught test)**.** Let $S \subseteq B$ and suppose that for all $g \in \mathcal{F}^1_S$,

$$B \models \dot{\exists} x\, g(x) \implies \exists a \in S \text{ such that } B \models g(a).$$

Show that for all $f \in \mathcal{F}^0_S$, we have $S \models f \iff B \models f$.

Fix a choice function $\mathsf{choice}\colon \mathcal{P}(B)\setminus\{\varnothing\} \to B$. For a $\mathcal{U}$-formula $g \in \mathcal{F}^1_B$ with $B \models \dot{\exists} x\, g(x)$, define

$$W(g) \coloneqq \mathsf{choice}(\{a \in B \,:\, B \models g(a)\}),$$

and for a subset $S \subseteq B$, let

$$W(S) \coloneqq \{W(g) \,:\, g \in \mathcal{F}^1_S \text{ such that } B \models \dot{\exists} x\, g(x)\}.$$

Note that $S \subseteq W(S)$, since for each $a \in S$, we have

$$a \,=\, W(x \doteq a).$$

Now we recursively define a sequence of sets A_n, $n \in \omega$, by

$$A_0 \coloneqq A \qquad \text{and} \qquad A_{n+1} \coloneqq W(A_n) \text{ for all } n \in \omega.$$

(Note that $A_0 \subseteq A_1 \subseteq A_2 \subseteq \ldots$) Finally, set

$$A^* \coloneqq \bigcup_{n\in\omega} A_n.$$

We claim that A^* has all the required properties. By definition, $A = A_0 \subseteq A^* \subseteq B$. Next take any $g \in \mathcal{F}^1_{A^*}$ such that $B \models \dot{\exists} x\, g(x)$. Since g uses only finitely many parameters from A^*, there is some $n \in \omega$ such that all the parameters in g come from A_n, i.e., $g \in \mathcal{F}^0_{A_n}$. But then $W(g) \in A_{n+1} \subseteq A^*$, and, by definition, $B \models g(W(a))$. Thus, A^* passes the Tarski–Vaught test, and we conclude that for all $f \in \mathcal{F}^0_{A^*}$, we have $A^* \models f \iff B \models f$, as desired.

It remains to bound $|A^*|$. To that end, recall that for every set S, we have $|\mathcal{F}_S| = \max\{\aleph_0, |S|\}$ (see Exercise 13.3). Hence, we can inductively show that for all $n \in \omega$,

$$|A_{n+1}| \leqslant |\mathcal{F}^1_{A_n}| \,=\, \max\{\aleph_0, |A_n|\} \leqslant \max\{\aleph_0, |A|\}.$$

Thus, A^* is a union of countably many sets, each of cardinality at most $\max\{\aleph_0, |A|\}$, and

$$|A^*| \leqslant \aleph_0 \otimes \max\{\aleph_0, |A|\} \,=\, \max\{\aleph_0, |A|\}. \qquad \blacksquare$$

Here's an interesting application of the Löwenheim–Skolem theorem. Suppose that $\mathcal{U} \models \mathsf{ZFC}$ and let κ be an inaccessible cardinal. By Theorem 12.6, we have $V_\kappa \models \mathsf{ZFC}$. Applying the Löwenheim–Skolem theorem with $A = \varnothing$ and $B = V_\kappa$ gives a countable set $A^* \subset V_\kappa$ such that for all $f \in \mathcal{F}^0_{A^*}$, we have $A^* \models f \iff V_\kappa \models f$. In particular,

$$A^* \models \mathsf{ZFC}.$$

In other words, under the assumption that there is an inaccessible cardinal, we can find a *countable set that satisfies all the axioms of* ZFC. This observation is known as **Skolem's paradox**.[xvi] Skolem himself found it so counter-intuitive that he believed it fully discredits the logical foundations of set theory. For instance, the existence of an uncountable set is a theorem of ZFC, and thus

$$A^* \models \text{"there is an uncountable set,"}$$

even though A^* itself is countable. However, *we* know that there is nothing paradoxical about this: the statement "there is an uncountable set" really means that

$$\exists S\, \neg\exists f\, (f \text{ is an injection } S \to \omega),$$

so $A^* \models$ "there is an uncountable set" simply means that there is some $S \in A^*$ such that *there is no f in A^** with $A^* \models$ "f is an injection $S \to \omega$," which does not contradict the fact that such an injection f *exists in* $\mathcal{U}$.

Let's investigate the structure of this set A^* a bit more. Since $A^* \models \mathsf{ZFC}$, we have

$$A^* \models \exists S\, (S = \omega),$$

where "$S = \omega$" is a shorthand for a formula without parameters that identifies ω. Let $S \in A^*$ be the set such that $A^* \models S = \omega$. The statement "$S = \omega$" can be expressed by a $\mathcal{U}$-formula using S as

[xvi] Named after the Norwegian mathematician Thoralf Skolem.

a parameter, and thus we must have $V_\kappa \models S = \omega$. But this means that S *actually is* ω; in other words, $\omega \in A^*$. Similarly, A^* satisfies the Powerset Axiom, and hence

$$A^* \models \exists P\, (P = \mathcal{P}(\omega)).$$

Again, letting $P \in A^*$ be the set such that $A^* \models P = \mathcal{P}(\omega)$, we conclude that $V_\kappa \models P = \mathcal{P}(\omega)$, which implies that P *is* the powerset of ω (exercise!). But this means that $\mathcal{P}(\omega) \in A^*$. So, even though A^* itself is a countable set, it contains as an element the *uncountable* set $\mathcal{P}(\omega)$. Continuing in like manner, we see that the following sets are elements of A^*:

$$V_\omega, \qquad V_{\omega+1}, \qquad V_{\omega+\omega}, \qquad V_{\omega^\omega}, \qquad V_{\aleph_1}, \qquad V_{\aleph_{\aleph_{\aleph_1}}}, \qquad \text{etc.}$$

One consequence of the above discussion is that A^* is definitely *not* a transitive set, as it has lots of uncountable elements. Nevertheless, it turns out that we can replace A^* by an isomorphic transitive set using a trick known as the **Mostowski collapse**, which is the second tool we need to establish the Magic Lemma:

Theorem/Definition 16.9 (Mostowski collapse)**.** *Let $\mathcal{C}$ be a class such that $\mathcal{C} \models \mathsf{Ext}$. Then there is a unique class function $j\colon \mathcal{C} \to \mathcal{U}$ such that:*

(M1) *j is injective,*

(M2) *$\mathrm{ran}(j)$ is a transitive class, and*

(M3) *for all $x, y \in \mathcal{C}$, we have $y \in x \iff j(y) \in j(x)$.*

The class function $j\colon \mathcal{C} \to \mathrm{ran}(j)$ is called the **Mostowski collapse** *of $\mathcal{C}$.*

Proof. By recursion on the rank of $x \in \mathcal{C}$, define

$$j(x) \coloneqq \{j(y) \,:\, y \in x \cap \mathcal{C}\}. \tag{16.1}$$

The fact that $\mathcal{C} \models \mathsf{Ext}$ guarantees that j is injective. The details are left as an exercise. ■

Example 16.10. To see why it's necessary to assume in Theorem 16.9 that $\mathcal{C} \models \mathsf{Ext}$, consider the set $A \coloneqq \{\varnothing, \{\varnothing\}, \{\varnothing, \{\{\varnothing\}\}\}\}$ from Example 12.1. Recall that Ext fails in A, because the sets $\{\varnothing\}$ and $\{\varnothing, \{\{\varnothing\}\}\}$ have the same (unique) element in A, namely $\varnothing$. Thus, if we were to define a function $j\colon A \to \mathcal{U}$ using (16.1), it wouldn't be injective:

$$j(\varnothing) = \varnothing, \qquad j(\{\varnothing\}) = j(\{\varnothing, \{\{\varnothing\}\}\}) = \{\varnothing\}.$$

Example 16.11. Consider the set $E \coloneqq \{n \in \omega \,:\, n \text{ is even}\}$. Then $E \models \mathsf{Ext}$ (exercise!). We claim that the Mostowski collapse of E is the function $j\colon E \to \omega \colon n \mapsto n/2$. Indeed, j is certainly injective and its range, ω, is a transitive set. Furthermore, if $n, m \in E$, then

$$n \in m \iff n < m \iff n/2 < m/2 \iff n/2 \in m/2.$$

On the other hand, we could obtain the same result by induction using formula (16.1):

$$\begin{aligned}
j(0) &= j(\varnothing) = \varnothing = 0,\\
j(2) &= j(\{0,1\}) = \{j(0)\} = \{0\} = 1,\\
j(4) &= j(\{0,1,2,3\}) = \{j(0), j(2)\} = \{0,1\} = 2,\\
j(6) &= j(\{0,1,2,3,4,5\}) = \{j(0), j(2), j(4)\} = \{0,1,2\} = 3, \qquad \text{etc.}
\end{aligned}$$

Exercise 16.4. Let $\mathcal{C} \subseteq \mathbf{Ord}$ be a proper class. Show that the unique order-isomorphism $\mathcal{C} \to \mathbf{Ord}$ coincides with the Mostowski collapse of $\mathcal{C}$.

Exercise 16.5. Let $\mathcal{C}$ be a transitive class. Show that the Mostowski collapse of $\mathcal{C}$ is the identity class function $\mathrm{id}_\mathcal{C}\colon \mathcal{C} \to \mathcal{C}$. More generally, let $\mathcal{C}$ be a class such that $\mathcal{C} \models \mathsf{Ext}$ and let $\mathcal{A} \subseteq \mathcal{C}$ be a transitive subclass. Let j be the Mostowski collapse of $\mathcal{C}$. Show that $j \restriction \mathcal{A} = \mathrm{id}_\mathcal{A}$.

Let $\mathcal{C}$ be a class such that $\mathcal{C} \models \mathsf{Ext}$ and let $j\colon \mathcal{C} \to \mathcal{C}'$ be the Mostowski collapse of $\mathcal{C}$, where $\mathrm{ran}(j) = \mathcal{C}'$. By definition, j is an isomorphism between the structures

$$(\mathcal{C}, \in) \qquad \text{and} \qquad (\mathcal{C}', \in).$$

It follows that any statement that holds in $\mathcal{C}$ must also hold in $\mathcal{C}'$ and vice versa. More precisely, let $\varphi(a_1, \ldots, a_k)$ be a formula without free variables and with parameters $a_1, \ldots, a_k \in \mathcal{C}$. Then

$$\mathcal{C} \models \varphi(a_1, \ldots, a_k) \iff \mathcal{C}' \models \varphi(j(a_1), \ldots, j(a_k)),$$

where $j(a_1), \ldots, j(a_k)$ are treated as parameters from $\mathcal{C}'$. Similarly, if A is a set such that $A \models \mathsf{Ext}$ and $j\colon A \to A'$ is the Mostowski collapse of A with $\mathrm{ran}(j) = A'$ (which is also a set by Replacement), then the above observation extends to $\mathcal{U}$-formulas; that is, for every $\mathcal{U}$-formula $f(a_1, \ldots, a_k) \in \mathcal{F}^0_A$ with parameters $a_1, \ldots, a_k \in A$,

$$A \models f(a_1, \ldots, a_k) \iff A' \models f(j(a_1), \ldots, j(a_k)),$$

where $j(a_1), \ldots, j(a_k)$ are treated as parameters from A' (and so $f(j(a_1), \ldots, j(a_k)) \in \mathcal{F}_{A'}$).

Corollary 16.12 (Löwenheim and Skolem meet Mostowski)**.** *Assume that $\mathcal{U} \models \mathsf{ZFC}$. Let $A \subseteq B$ be sets. Suppose that A is transitive and $B \models \mathsf{Ext}$. Then there exists a transitive set $A' \supseteq A$ such that $|A'| \leqslant \max\{\aleph_0, |A|\}$ and for all $f \in \mathcal{F}^0_A$, we have*

$$A' \models f \iff B \models f.$$

Note that Corollary 16.12 does not claim that $A' \subseteq B$.

Proof. First we apply the Löwenheim–Skolem theorem to obtain a set A^* such that $A \subseteq A^* \subseteq B$, $|A^*| \leqslant \max\{\aleph_0, |A|\}$, and for all $f \in \mathcal{F}^0_{A^*}$, $A^* \models f \iff B \models f$. Since $B \models \mathsf{Ext}$, we conclude that $A^* \models \mathsf{Ext}$ as well, and thus we can consider the Mostowski collapse $j\colon A^* \to A'$, where $A' := \mathrm{ran}(j)$. By construction, A' is a transitive set with $|A'| = |A^*| \leqslant \max\{\aleph_0, |A|\}$. By Exercise 16.5, since A is a transitive subset of A^*, we have $j{\restriction}A = \mathrm{id}_A$ and hence $A = j[A] \subseteq A'$. Finally, if $f \in \mathcal{F}^0_A$, then $A' \models f \iff A^* \models f \iff B \models f$, as desired. (Here we are using again that j acts as the identity function on the elements of A.) ■

Example 16.13. It follows that if $\mathcal{U} \models \mathsf{ZFC}$ and there is an inaccessible cardinal κ, then there exists a transitive countable set that satisfies ZFC: simply apply Corollary 16.12 with $A = \varnothing$ and $B = V_\kappa$. This is a nice example of a combinatorial statement about the existence of a *countable* structure with certain properties that relies on the existence of a large *uncountable* cardinal κ. (Also, see Exercise 16.7.)

Exercise 16.6. Suppose that $\mathcal{U} \models \mathsf{ZFC}$ and let $\varphi_1, \ldots, \varphi_n$ be a finite list of axioms of ZFC. Show that there is a transitive countable set S such that $S \models \varphi_1 \wedge \ldots \wedge \varphi_n$.

We are now ready to prove Lemma 16.5:

Proof *of Gödel's Magic Lemma.* Recall the set-up: we are assuming that $\mathcal{U} \models \mathsf{ZFC}$, a and b are sets, and b is Σ_1-identifiable over a. Fix a Σ_1-formula $\varphi(x, y)$ such that

$$y = b \iff \varphi(a, y). \tag{16.2}$$

Consider the formula $\psi(x) := \exists y\, \varphi(x, y)$ with one free variable x. By the Reflection Principle, there is an ordinal β such that $a \in V_\beta$ and ψ is absolute between V_β and $V = \mathcal{U}$. In particular, since $\mathcal{U} \models \psi(a)$ (as witnessed by b), we also have $V_\beta \models \psi(a)$. Let $A := \mathrm{cl}(\{a\}) = \mathrm{cl}(a) \cup \{a\}$ (i.e., A is the smallest transitive set that has a as an element). Since V_β is transitive, we have $A \subseteq V_\beta$ and $V_\beta \models \mathsf{Ext}$, so we may apply Corollary 16.12 to A and V_β, obtaining a transitive set A' such that:

- $A \subseteq A'$,
- $|A'| \leqslant \max\{\aleph_0, |A|\} = \max\{\aleph_0, |\mathrm{cl}(a)|\}$, and
- for all $f \in \mathcal{F}^0_A$, $A' \models f \iff V_\beta \models f$.

In particular, since $a \in A$ and $V_\beta \models \psi(a)$, we also have $A' \models \psi(a)$, i.e.,

$$A' \models \exists y\, \varphi(a, y).$$

Let $b' \in A'$ be a set such that $A' \models \varphi(a, b')$. Since A' is transitive and φ is a Σ_1-formula, the truth of $\varphi(a, b')$ "lifts" from A' to $\mathcal{U}$ (see Exercise 14.11), and hence $\mathcal{U} \models \varphi(a, b')$. But, by (16.2), this means that $b' = b$. It remains to notice that, by the transitivity of A', $b = b' \subseteq A'$, and hence

$$|b| \leqslant |A'| \leqslant \max\{\aleph_0, |A|\}. \qquad \blacksquare$$

Exercise 16.7. Suppose that there is a transitive set S such that $S \models \mathsf{ZF}$. (This happens, e.g., if there exists an inaccessible cardinal.) Show that there is a countable ordinal α such that $L_\alpha \models \mathsf{ZFC}$.

17. The Perfect Set Property for subsets of $\mathbb{R}^n$

17.1. Topology on $\mathbb{R}^n$

Throughout this section, unless explicitly indicated otherwise, we shall work in ZFC. Recall that the Continuum Hypothesis (CH) is the statement that every subset $A \subseteq \mathbb{R}$ is either countable or of cardinality $2^{\aleph_0}$. While in its full generality CH can neither be proved nor disproved in ZFC, it is reasonable to try to establish CH for sets A satisfying some extra assumptions. This line of inquiry was initiated by Cantor himself, who proved the following:

Theorem 17.1 (Cantor)**.** *If $C \subseteq \mathbb{R}^n$ is closed, then either $|C| \leqslant \aleph_0$, or else, $|C| = 2^{\aleph_0}$.*

(Here and in what follows, n denotes a positive natural number.)

To understand Theorem 17.1, we have to briefly review the fundamentals of topology on $\mathbb{R}^n$. (This material is extremely standard and we only include it here for completeness.) Given points x, $y \in \mathbb{R}^n$, we write $\mathsf{dist}(x, y)$ for the usual (Euclidean) distance between x and y, i.e.,

$$\mathsf{dist}((x_1, \ldots, x_n), (y_1, \ldots, y_n)) = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}.$$

For $x \in \mathbb{R}^n$ and $r \in \mathbb{R}^+ := (0, +\infty)$, let

$$B(x, r) := \{y \in \mathbb{R}^n : \mathsf{dist}(x, y) < r\} \qquad \text{and} \qquad \overline{B}(x, r) := \{y \in \mathbb{R}^n : \mathsf{dist}(x, y) \leqslant r\}$$

denote the **open** and **closed balls** around x or radius r, respectively. In general, given an open ball B, we write $\overline{B}$ for the corresponding closed ball. A subset $U \subseteq \mathbb{R}^n$ is **open** if for every $x \in U$, there is $r \in \mathbb{R}^+$ such that $B(x, r) \subseteq U$. A set $C \subseteq \mathbb{R}^n$ is **closed** is its complement $\mathbb{R}^n \setminus C$ is open.

Exercise 17.1. Let $x \in \mathbb{R}^n$ and $r \in \mathbb{R}^+$. Show that $B(x, r)$ is open and $\overline{B}(x, r)$ is closed. In other words, open balls are open sets, while closed balls are closed sets.

Note that there are lots of sets that are neither open nor closed (say, the half-open interval $[0, 1) \subset \mathbb{R}$ is neither open nor closed in $\mathbb{R}$). Furthermore, there are sets that are *both* open and closed. Specifically, viewed as subsets of $\mathbb{R}^n$, $\varnothing$ and $\mathbb{R}^n$ are open and closed. Sets that are simultaneously open and closed are sometimes called **clopen** (although some people still consider it a colloquialism).

Exercise 17.2 (trickier than it looks)**.** Show that the only clopen subsets of $\mathbb{R}^n$ are $\varnothing$ and $\mathbb{R}^n$.[xvii]

Lemma 17.2. *Let F be a set of open subsets of $\mathbb{R}^n$. Then $\bigcup F$ is also open.*

PROOF. Take any $x \in \bigcup F$. By definition, there is $U \in F$ such that $x \in U$. But U is open, so there is some $r \in \mathbb{R}^+$ with $B(x, r) \subseteq U \subseteq \bigcup F$, as desired. ■

Lemma 17.3. *If U_1, $U_2 \subseteq \mathbb{R}^n$ are open, then so is $U \cap V$.*

PROOF. Take any $x \in U_1 \cap U_2$. Then there exist r_1, $r_2 \in \mathbb{R}^+$ with $B(x, r_1) \subseteq U_1$ and $B(x, r_2) \subseteq U_2$. Without loss of generality, assume that $r_1 \leqslant r_2$. Then $B(x, r_1) \subseteq U_1 \cap U_2$, as desired. ■

Exercise 17.3. Generalize Lemma 17.3 as follows: For any finite collection $U_1, \ldots, U_k \subseteq \mathbb{R}^n$ of open subsets of $\mathbb{R}^n$, the set $U_1 \cap \ldots \cap U_k$ is also open.

Lemmas 17.2 and 17.3 can be naturally restated in terms of closed sets:

Exercise 17.4.

(*a*) Let F be a nonempty set of closed subsets of $\mathbb{R}^n$. Show that $\bigcap F$ is also closed.

(*b*) Show that for any finite family $C_1, \ldots, C_k \subseteq \mathbb{R}^n$ of closed sets, $C_1 \cup \ldots \cup C_k$ is also closed.

[xvii] The notions of open and closed sets can be extended beyond just subsets of $\mathbb{R}^n$ to a very general framework of *topological spaces*. In contrast to $\mathbb{R}^n$, some topological spaces have lots of clopen subsets; in fact, from the point of view of a set theorist, such spaces (called 0-*dimensional spaces*) are much nicer to work with than $\mathbb{R}^n$.

The result of Exercise 17.3 does not extend to infinite intersections. For instance, the set $\{0\}$ can be expressed as the intersection of a countable collection of open subsets of $\mathbb{R}$:

$$\{0\} \;=\; \bigcap_{k\in\omega}(-2^{-k}, 2^{-k}).$$

Some intersections of countable families of open sets are neither open nor closed; for instance,

$$[0,1) \;=\; \bigcap_{k\in\omega}(-2^{-k}, 1).$$

If a set $A \subseteq \mathbb{R}^n$ can be expressed as $A = \bigcap\{U_k \,:\, k \in \omega\}$, where each $U_k \subseteq \mathbb{R}^n$ is open, then A is called a G_δ-**subset** of $\mathbb{R}^n$. Similarly, if $A \subseteq \mathbb{R}^n$ can be expressed as $A = \bigcup\{C_k \,:\, k \in \omega\}$ where each $C_k \subseteq \mathbb{R}^n$ is closed, then A is an F_σ-**subset** of $\mathbb{R}^n$.[xviii] Obviously, open sets are G_δ and closed sets are F_σ. Somewhat less obviously, we have the following:

Exercise 17.5. Show that every closed set $C \subseteq \mathbb{R}^n$ is G_δ and every open set $U \subseteq \mathbb{R}^n$ is F_σ.

It is clear that every nonempty open subset of $\mathbb{R}^n$ has cardinality $2^{\aleph_0}$, since it must contain an open ball. On the other hand, closed sets can have a much more intricate structure. A good example of a somewhat "complicated" closed set is the middle thirds Cantor set.

Example 17.4 (Middle thirds Cantor set)**.** The **middle thirds Cantor set** is the subset of $\mathbb{R}$ obtained as follows. Start with the closed unit interval $[0,1]$. Next, remove the open interval $(1/3, 2/3)$ (the eponymous "middle third"), leaving a pair of closed intervals $[0,1/3] \cup [2/3,1]$. On the next stage, remove the "middle thirds" of these two intervals, obtaining four closed intervals, each of length $1/9$: $[0,1/9] \cup [2/9,1/3] \cup [2/3,7/9] \cup [8/9,1]$. Then remove the "middle thirds" of these four intervals, then the "middle thirds" of the remaining eight intervals, and so on, for ω-many steps. The middle thirds Cantor set is the set of all points that never get removed during this process (see Fig. 1). We denote the middle thirds Cantor set by $C_{1/3}$.

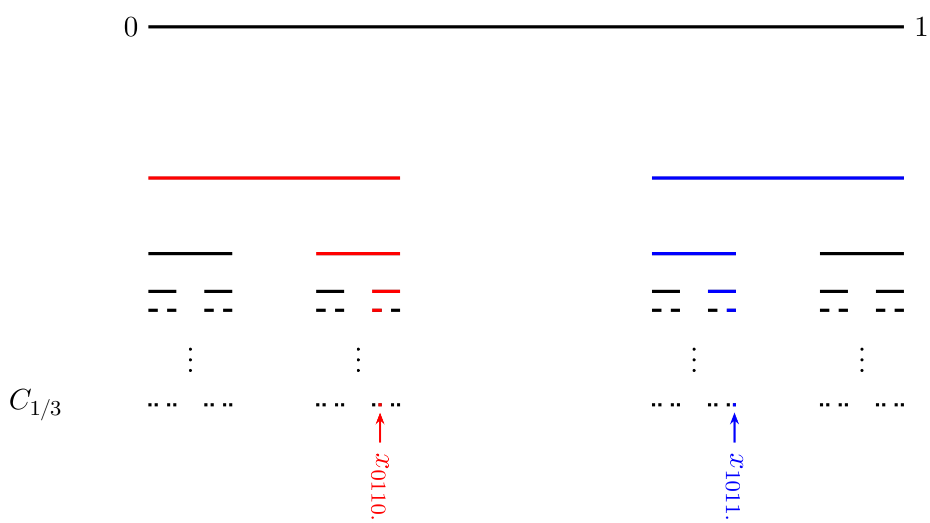


Figure 1. The construction of the middle thirds Cantor set.

Clearly, $C_{1/3}$ is a closed subset of $\mathbb{R}$, since it is obtained by *removing* open sets (so $\mathbb{R}\backslash C_{1/3}$ a union of open sets—and hence it is itself open by Lemma 17.2). It is also easy to see that $C_{1/3}$ does not

[xviii] The term G_δ comes from the German *Gebiet* 'neighborhood' + *Durchschnitt* 'intersection'. By contrast, F_σ is derived from the French *fermé* 'closed' + *somme* 'union'.

contain any interval as a subset. One could say that $C_{1/3}$ looks just like "dust" or the result of using the "spray paint tool." Nevertheless, we claim that

$$|C_{1/3}| = 2^{\aleph_0}.$$

Indeed, for each $f \in {}^{\omega}2$, we can obtain a corresponding point $x_f \in C_{1/3}$ as follows. Define a sequence of closed intervals $I_0, I_1, I_2, \ldots$ by setting

$$I_0 := \begin{cases} [0, 1/3] & \text{if } f(0) = 0, \\ [2/3, 1] & \text{if } f(0) = 1, \end{cases}$$

and then making I_{n+1} be the left third of I_n if $f(n+1) = 0$ and the right third of I_n if $f(n+1) = 1$. The resulting sequence of intervals is, by construction, decreasing:

$$I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots,$$

and the intersection $I_0 \cap I_1 \cap I_2 \cap \ldots$ contains precisely one point, which we denote x_f (see Fig. 1). This construction gives an injective (in fact, bijective) function ${}^{\omega}2 \to C_{1/3}$, proving that $|C| \geqslant 2^{\aleph_0}$.

The argument in Example 17.4 relied on the following exceptionally useful property of $\mathbb{R}^n$:

Fact 17.5. *If $\overline{B}_1 \supseteq \overline{B}_2 \supseteq \cdots$ is a decreasing sequence of closed balls in $\mathbb{R}^n$ such that*

$$\lim_{k\to\infty} \text{radius}(B_k) = 0,$$

then $\bigcap_{k\in\omega} \overline{B}_k \neq \varnothing$; in fact, the intersection $\bigcap_{k\in\omega} \overline{B}_k$ contains precisely one point.[xix]

We will not prove Fact 17.5 here (as it is proved in every introductory real analysis course). Note that we haven't formally *defined* the real numbers in these notes. There exist several (equivalent) ways of defining $\mathbb{R}$, some of which incorporate Fact 17.5 into the definition.

Fact 17.5 can be strengthened by replacing closed *balls* by arbitrary closed *sets*. Define the **diameter** of a set $A \subseteq \mathbb{R}^n$ by

$$\text{diam}(A) := \sup\{\mathsf{dist}(x, y) : x, y \in A\}.$$

Thus, diam(A) is either a nonnegative real number or ∞.

Exercise 17.6. Show that if $A \subseteq \mathbb{R}^n$ has finite diameter, then there is a closed ball $\overline{B}$ of radius at most diam(A) such that $A \subseteq \overline{B}$.

Corollary 17.6. *If $C_1 \supseteq C_2 \supseteq \cdots$ is a decreasing sequence of nonempty closed subsets of $\mathbb{R}^n$ with*

$$\lim_{k\to\infty} \text{diam}(C_k) = 0,$$

then $\bigcap_{k\in\omega} C_k \neq \varnothing$; in fact, the intersection $\bigcap_{k\in\omega} C_k$ contains precisely one point.

PROOF. Clearly $|\bigcap_{k\in\omega} C_k| \leqslant 1$ (why?), so we only need to show $\bigcap_{k\in\omega} C_k \neq \varnothing$. Without loss of generality, assume that diam$(C_k) < \infty$ for all $k \in \omega$. Since diam$(C_k) \to 0$, we can use Exercise 17.6 to obtain (how?) a decreasing sequence

$$\overline{B}_1 \supseteq \overline{B}_2 \supseteq \cdots$$

of closed balls whose radii converge to 0 such that $\overline{B}_k \supseteq C_k$ for all $k \in \omega$. By Fact 17.5, there is a unique point $x \in \bigcap_{k\in\omega} \overline{B}_k$. We claim that $x \in \bigcap_{k\in\omega} C_k$. Suppose not, i.e., there is some $k \in \omega$ with $x \notin C_k$. Since C_k is closed, there is $r \in \mathbb{R}^+$ such that $B(x, r) \cap C_k = \varnothing$. Take $\ell \in \omega$ so large that the radius of $\overline{B}_\ell$ is less than $r/2$. Since $x \in \overline{B}_\ell$, we have $C_\ell \subseteq \overline{B}_\ell \subseteq B(x, r)$. But this means that $C_\ell \cap C_k = \varnothing$, contradicting the fact that $\varnothing \neq C_\ell \subseteq C_k$. ■

[xix] This statement can be summarized as: $\mathbb{R}^n$ *is a complete metric space.*

17.2. Perfect sets

Let $P \subseteq \mathbb{R}^n$. An **isolated point** of P is a point $x \in P$ such that there is $r \in \mathbb{R}^+$ with $B(x,r) \cap P = \{x\}$. A subset $P \subseteq \mathbb{R}^n$ is **perfect** if it is closed and has no isolated points. Examples of perfect sets are closed balls and the middle thirds Cantor set (see Example 17.4).

Exercise 17.7. Give an example of a set without isolated points that is not perfect.

Theorem 17.1 is a consequence of the following two facts:

Theorem 17.7 (Cantor). *If $P \subseteq \mathbb{R}^n$ is nonempty and perfect, then $|P| = 2^{\aleph_0}$.*

Theorem 17.8 (Cantor–Bendixson). *Let $C \subseteq \mathbb{R}^n$ be a closed set. Then C can be decomposed as $C = P \cup U$, where $P \cap U = \varnothing$, U is countable, and P is perfect.*

PROOF *of Theorem 17.1.* Let $C \subseteq \mathbb{R}^n$ be closed. Write $C = P \cup U$, where U is countable and P is perfect. If $P = \varnothing$, then $C = U$ is countable; otherwise, $|C| = |P| = 2^{\aleph_0}$. ■

In this subsection we prove Theorem 17.7 by a modification of the argument from Example 17.4. First, we need a lemma:

Lemma 17.9. *Let $P \subseteq \mathbb{R}^n$ be a perfect set and suppose that $U \subseteq \mathbb{R}^n$ is an open set such that $U \cap P \neq \varnothing$. Then, for any $\varepsilon \in \mathbb{R}^+$, there exist open balls B_0 and B_1 such that:*

- *the sets $B_0 \cap P$ and $B_1 \cap P$ are nonempty,*
- *the radii of $\overline{B}_0$ and $\overline{B}_1$ are at most ε, and*
- *$\overline{B}_0 \cap \overline{B}_1 = \varnothing$ and $\overline{B}_0 \cup \overline{B}_1 \subseteq U$.*

PROOF. Since $U \cap P \neq \varnothing$, we can take a point $x \in U \cap P$. Since P is perfect, x is not isolated in P, and hence there is another point $y \in U \cap P$ (we are using here that U is open). Let $r_1, r_2 \in \mathbb{R}^+$ be such that $B(x, r_1)$, $B(y, r_2) \subseteq U$, and set

$$r := \min\left\{\varepsilon, \frac{\mathsf{dist}(x,y)}{3}, \frac{r_1}{2}, \frac{r_2}{2}\right\}.$$

Then we can take $B_0 := B(x,r)$ and $B_1 := B(y,r)$. ■

PROOF *of Theorem 17.7.* Recall that ${}^{<\omega}2$ is the set of all finite sequences of 0s and 1s. We use $^\frown$ to indicate concatenation of finite sequences; in particular, for $s \in {}^{k}2$ and $i \in \{0,1\}$, we write $s^\frown i$ to denote the sequence of length $(k+1)$ such that $(s^\frown i)\restriction k = s$ and $(s^\frown i)(k) = i$.

To each $s \in {}^{<\omega}2$, we shall associate an open ball B_s in $\mathbb{R}^n$ so that, for all $s \in {}^{k}2$:

- $B_s \cap P \neq \varnothing$,
- the radius of B_s is at most 2^{-k},
- $\overline{B}_{s^\frown 0} \cap \overline{B}_{s^\frown 1} = \varnothing$ and $\overline{B}_{s^\frown 0} \cup \overline{B}_{s^\frown 1} \subseteq B_s$.

The construction of the balls B_s is recursive, based on the length of s. Since $P \neq \varnothing$, we can take any point $x \in P$ and set $B_\varnothing := B(x,1)$. When B_s is determined for some $s \in {}^{<\omega}2$, we can find suitable $B_{s^\frown 0}$ and $B_{s^\frown 1}$ by applying Lemma 17.9 with $U = B_s$ (the details are left as an exercise).

Once the balls B_s for all $s \in {}^{<\omega}2$ are chosen, we can define an injection ${}^{\omega}2 \to P$ as follows. Take any $f \in {}^{\omega}2$. Consider the finite sequences

$$f\restriction 0, \qquad f\restriction 1, \qquad f\restriction 2, \qquad f\restriction 3, \qquad \ldots.$$

For instance, if $f = (010\ldots)$, then we look at the finite sequences

$$\varnothing, \qquad 0, \qquad 01, \qquad 010, \qquad \ldots.$$

The corresponding balls form a decreasing sequence

$$\overline{B}_{f\restriction 0} \supseteq \overline{B}_{f\restriction 1} \supseteq \overline{B}_{f\restriction 2}, \supseteq \overline{B}_{f\restriction 3} \supseteq \cdots,$$

so, by Corollary 17.6, the intersection $\bigcap_{k\in\omega}(\overline{B}_{f\restriction k}\cap P)$ contains precisely one point x_f. By construction, $x_f \in P$, so it remains to show that the mapping ${}^{\omega}2 \to P\colon f \mapsto x_f$ is injective. To that end, let f, $g \in {}^{\omega}2$ be distinct and let k be the least index such that $f(k) \neq g(k)$. Set $s := f\restriction k = g\restriction k$ and suppose, for concreteness, that $f(k) = 0$ while $g(k) = 1$. Then

$$x_f \in \overline{B}_{s^\frown 0}, \qquad \text{while} \qquad x_g \in \overline{B}_{s^\frown 1},$$

and the sets $\overline{B}_{s^\frown 0}$ and $\overline{B}_{s^\frown 1}$ are disjoint, which implies that $x_f \neq x_g$, as desired. ■

17.3. The Cantor–Bendixson theorem

For a closed set $C \subseteq \mathbb{R}^n$, let $I(C) := \{x \in C : x \text{ is isolated in } C\}$ and let $C' := C \setminus I(C)$. The set C' is called the **Cantor–Bendixson derivative**[xx] of C.

Lemma 17.10. *Let $C \subseteq \mathbb{R}^n$ be a closed set. Then $I(C)$ is countable.*

PROOF. For each $x \in I(C)$, pick $r_x \in \mathbb{R}^+$ so that $B(x, r_x) \cap C = \{x\}$. Then for distinct x, $y \in I(C)$,

$$B(x, r_x/3) \;\cap\; B(y, r_y/3) \;=\; \varnothing. \tag{17.1}$$

Every ball (of positive radius) contains a point with rational coordinates, so let q_x be an arbitrary element of $\mathbb{Q}^n \cap B(x, r_x/3)$. Due to (17.1), the function $I(C) \to \mathbb{Q}^n : x \mapsto q_x$ is injective. But the set $\mathbb{Q}^n$ is countable; hence, $I(C)$ is countable as well. ■

Exercise 17.8. Let $C \subseteq \mathbb{R}^n$ be a closed set. Show that C' is also closed.

By definition, a closed set C is perfect is and only if $C = C'$. Since $C = C' \cup I(C)$ and $I(C)$ is countable, one might hope that C' is perfect, i.e., *removing* all isolated points from C leaves a set *without* isolated points. Unfortunately, this may not be the case; for example,

$$\Big(\{0\} \cup \{2^{-k} : k \in \omega\}\Big)' \;=\; \{0\},$$

and the set $\{0\}$ has 0 as an isolated point (see Fig. 2).

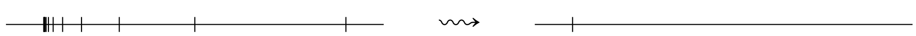


Figure 2. The Cantor–Bendixson derivative may create new isolated points.

The next idea is to apply the Cantor–Bendixson derivative again and remove all isolated points from C'; but the resulting set C'' may also be not perfect—see Fig. 3.

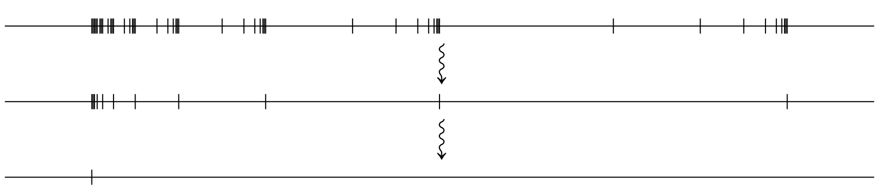


Figure 3. Applying the Cantor–Bendixson derivative twice.

Cantor's insight was that the derivative operation can be iterated *transfinitely*; as a matter of fact, this was the very first application of ordinals! Given a closed set $C \subseteq \mathbb{R}^n$, for each $\alpha \in \mathbf{Ord}$, we recursively define sets $C^{(\alpha)}$ as follows:

$$C^{(\alpha)} \;:=\; \begin{cases} C & \text{if } \alpha = 0, \\ (C^{(\beta)})' & \text{if } \alpha = \beta + 1, \\ \bigcap_{\gamma<\alpha} C^{(\gamma)} & \text{if } \alpha \text{ is a limit.} \end{cases}$$

[xx]No relation to derivatives from calculus.

The sets $C^{(\alpha)}$ are closed (why?), and we have $C^{(\beta)} \supseteq C^{(\alpha)}$ whenever $\beta \leqslant \alpha$.

Theorem 17.11 (Cantor–Bendixson). *Let $C \subseteq \mathbb{R}^n$ be a closed set. Then there is a countable ordinal α such that $C^{(\alpha+1)} = C^{(\alpha)}$ (i.e., the set $C^{(\alpha)}$ is perfect).*

From Theorem 17.11, Theorem 17.8 follows immediately:

PROOF *of Theorem 17.8.* Let $C \subseteq \mathbb{R}^n$ be a closed set. By Theorem 17.11, there is $\alpha < \aleph_1$ such that $C^{(\alpha+1)} = C^{(\alpha)}$. Then we can write $C = P \cup U$ with $P := C^{(\alpha)}$ and

$$U \;:=\; C \backslash C^{(\alpha)} \;=\; \bigcup \{C^{(\gamma)} \backslash C^{(\gamma+1)} \;:\; \gamma < \alpha\} \;=\; \bigcup \{I(C^{\gamma}) \;:\; \gamma < \alpha\}.$$

Since U is a union of countably many countable sets, it is itself countable, and hence we are done. ■

For a closed set $C \subseteq \mathbb{R}^n$, the least ordinal α such that $C^{(\alpha+1)} = C^{(\alpha)}$ is called the **Cantor–Bendixson rank**[xxi] of C and is denoted by $\mathrm{rank}_{\mathrm{CB}}(C)$. By Theorem 17.11, $\mathrm{rank}_{\mathrm{CB}}(C) < \aleph_1$.

Exercise 17.9. Show that for every countable ordinal α, there is a countable closed set $C \subseteq \mathbb{R}$ such that $\mathrm{rank}_{\mathrm{CB}}(C) = \alpha$.

To prove Theorem 17.11, we need a way to control open subsets of $\mathbb{R}^n$. A set $\mathcal{B}$ of open subsets of $\mathbb{R}^n$ is called an **open base** for $\mathbb{R}^n$ if for every open set $U \subseteq \mathbb{R}^n$, we have

$$U \;=\; \bigcup \{B \in \mathcal{B} \;:\; B \subseteq U\};$$

in other words, $\mathcal{B}$ is an open base if open subsets of $\mathbb{R}^n$ are precisely the unions of sets in $\mathcal{B}$.

Lemma 17.12. *There is a countable open base $\mathcal{B}$ for $\mathbb{R}^n$ consisting of open balls.*

PROOF. For example, we can take

$$\mathcal{B} \;:=\; \{B(x,r) \;:\; x \in \mathbb{Q}^n,\, r \in \mathbb{Q}^+\}.$$

The details are left as an exercise. ■

Corollary 17.13. *The cardinality of the set of all open subsets of $\mathbb{R}^n$ is $2^{\aleph_0}$.*

PROOF. Let $\mathcal{B}$ be a countable open base for $\mathbb{R}^n$. Then the function

$$\{U \subseteq \mathbb{R}^n \;:\; U \text{ is open}\} \to \mathcal{P}(\mathcal{B}) : \, U \mapsto \{B \in \mathcal{B} \;:\; B \subseteq U\}$$

is injective, which implies that the cardinality of the set of all open subsets of $\mathbb{R}^n$ is at most $|\mathcal{P}(\mathcal{B})| = 2^{\aleph_0}$. On the other hand, it is easy to exhibit $2^{\aleph_0}$ distinct open subsets of $\mathbb{R}^n$. ■

Exercise 17.10. What is the cardinality of the set of all close subsets of $\mathbb{R}^n$? All G_δ subsets of $\mathbb{R}^n$?

PROOF *of Theorem 17.11.* Let $C \subseteq \mathbb{R}^n$ be a closed set and suppose, toward a contradiction, that for all $\alpha < \aleph_1$, $C^{(\alpha+1)} \subset C^{(\alpha)}$. Fix a countable open base $\mathcal{B}$ for $\mathbb{R}^n$. For each $\alpha < \aleph_1$, let

$$\mathcal{B}_\alpha \;:=\; \{B \in \mathcal{B} \;:\; B \subseteq \mathbb{R}^n \backslash C^{(\alpha)}\}.$$

Since $C^{(\alpha+1)} \subset C^{(\alpha)}$, we have $\mathcal{B}_{\alpha+1} \supset \mathcal{B}_\alpha$, i.e, $\mathcal{B}_{\alpha+1} \backslash \mathcal{B}_\alpha \neq \varnothing$. Pick any $B_\alpha \in \mathcal{B}_{\alpha+1} \backslash \mathcal{B}_\alpha$. Then the function $\aleph_1 \to \mathcal{B} \colon \alpha \mapsto B_\alpha$ is injective, which is impossible as $\mathcal{B}$ is countable. ■

Exercise 17.11. It is possible to prove Theorem 17.8 "in one step," i.e., without transfinite recursion (although this approach gives less information about the structure of closed sets). Fix a closed set $C \subseteq \mathbb{R}^n$. Say that an open set $U \subseteq \mathbb{R}^n$ is C-**small** if $U \cap C$ is countable. Let W denote the union of all C-small open sets. Note that W is itself open.

(*a*) Show that W is C-small (i.e., $W \cap C$ is countable).

(*b*) Show that $C \backslash W$ is perfect.

(*c*) Conclude that $C = P \cup U$ where $P \cap U = \varnothing$, P is prefect, and U is countable.

[xxi] No relation to von Neumann rank.

Exercise 17.12. Show that for every closed $C \subseteq \mathbb{R}^n$, the partition $C = P \cup U$ as in Theorem 17.8 is unique.

Exercise 17.13 (important!)**.** Let $A \subseteq \mathbb{R}^n$ and suppose that $U \subseteq \mathbb{R}^n$ is an open set such that $U \cap A$ is uncountable. Then, for any $\varepsilon \in \mathbb{R}^+$, there exist open balls B_0 and B_1 such that:

- the sets $B_0 \cap A$ and $B_1 \cap A$ are uncountable,
- the radii of $\overline{B}_0$ and $\overline{B}_1$ are at most ε, and
- $\overline{B}_0 \cap \overline{B}_1 = \varnothing$ and $\overline{B}_0 \cup \overline{B}_1 \subseteq U$.

Moreover, if $\mathcal{B}$ is a countable open base for $\mathbb{R}^n$ consisting of open balls, then we may additionally arrange that $B_0, B_1 \in \mathcal{B}$. (Cf. Lemma 17.9.)

17.4. The Perfect Set Property

Theorem 17.8 shows that closed subsets of $\mathbb{R}^n$ satisfy CH "for a good reason": every uncountable closed set $C \subseteq \mathbb{R}^n$ must have a nonempty perfect subset, and all nonempty perfect sets have cardinality $2^{\aleph_0}$ by Theorem 17.7. In general, a set $A \subseteq \mathbb{R}^n$ has the **Perfect Set Property** (or the **PSP**, for short) if either A is countable, or else, A has a nonempty perfect subset. Thus, we have shown that every closed set has the PSP.

Exercise 17.14. Show that if $A \subset \mathbb{R}^n$ is countable, then $\mathbb{R}^n \backslash A$ has the PSP.

Exercise 17.15. Show that every G_δ subset $A \subseteq \mathbb{R}^n$ has the PSP.

The PSP provides a nice refinement of CH. While the existence of subsets of $\mathbb{R}^n$ whose cardinality is strictly between $\aleph_0$ and $2^{\aleph_0}$ is a matter that cannot be settled within ZFC, there do exist sets without the PSP (and their construction crucially relies on AC):

Theorem 17.14. *There exists a set $A \subseteq \mathbb{R}$ without the PSP. In fact, there is a set $A \subseteq \mathbb{R}$ such that $|A| = |\mathbb{R}\backslash A| = 2^{\aleph_0}$ and for every nonempty perfect set $P \subseteq \mathbb{R}$, we have $A \cap P \neq \varnothing$ and $P\backslash A \neq \varnothing$.*

PROOF. The set of all nonempty perfect subsets $P \subseteq \mathbb{R}$ has cardinality $2^{\aleph_0}$ (see Exercise 17.10), so we can fix a bijection

$$2^{\aleph_0} \to \{P \subseteq \mathbb{R} \,:\, P \text{ is nonempty and perfect}\} : \alpha \mapsto P_\alpha.$$

(This requires AC.) We shall recursively define a pair of injections

$$2^{\aleph_0} \to \mathbb{R} \colon x \mapsto x_\alpha, \qquad 2^{\aleph_0} \to \mathbb{R} \colon y \mapsto y_\alpha,$$

so that $\{x_\alpha \,:\, \alpha < 2^{\aleph_0}\} \cap \{y_\alpha \,:\, \alpha < 2^{\aleph_0}\} = \varnothing$ and $x_\alpha, y_\alpha \in P_\alpha$ for all $\alpha < 2^{\aleph_0}$. Once this is done, setting $A := \{x_\alpha \,:\, \alpha < 2^{\aleph_0}\}$ completes the proof (why?).

Let $\alpha < 2^{\aleph_0}$ and assume that x_β and y_β for all $\beta < \alpha$ are already determined. Let

$$X_\alpha := \{x_\beta \,:\, \beta < \alpha\} \qquad \text{and} \qquad Y_\alpha := \{y_\beta \,:\, \beta < \alpha\}.$$

Then $|X_\alpha| = |Y_\alpha| = |\alpha| < 2^{\aleph_0}$, while $|P_\alpha| = 2^{\aleph_0}$ by Theorem 17.7, so we can use AC and make x_α and y_α be arbitrary distinct elements of $P_\alpha \backslash (X_\alpha \cup Y_\alpha)$. ■

So, on the one hand, some sets fail to have the PSP, while, on the other hand, closed or even G_δ sets have the PSP (see Exercise 17.15). In the next few subsections, we will prove a far-reaching generalization of Cantor's Theorem 17.1 and see that a class of sets with the PSP is quite wide, so any counterexample to CH, if one exists, must be quite complicated. The key tool that we will use to achieve this is the concept of *infinite games*.

17.5. Infinite games and the PSP

A useful perspective on the PSP and similar regularity properties of subsets of $\mathbb{R}^n$ is provided by considering infinite games. To each subset $A \subseteq {}^{\omega}\omega$, we associate a two-player game $\mathsf{G}(A)$ that is played as follows: Players I and II alternately pick natural numbers:

Player I	a_0		a_2		$\ldots$	a_{2k}		$\ldots$
Player II		a_1		a_3	$\ldots$		a_{2k+1}	$\ldots$

This generates an infinite sequence of natural numbers

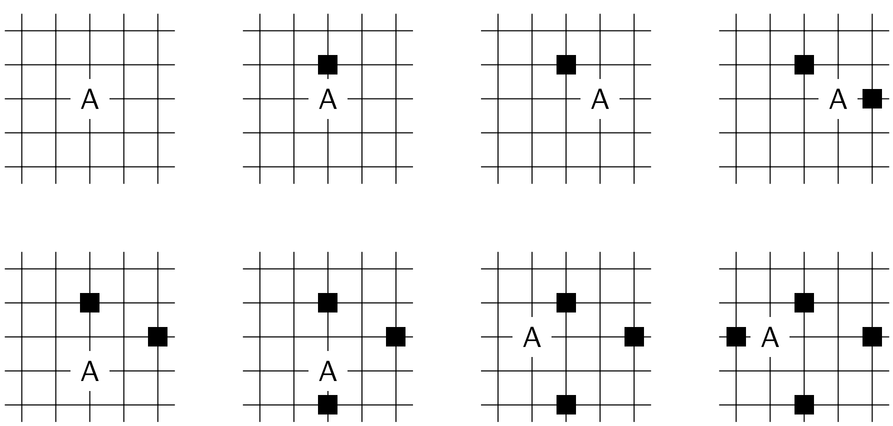
$$a \coloneqq (a_0, a_1, a_2, \ldots) \in {}^{\omega}\omega.$$

The sequence a is referred to as the **run** of the game. The set A is used to determine which player is the winner. Namely, Player I wins if $a \in A$; otherwise, Player II wins.

Example 17.15. Let $A \coloneqq \{a \in {}^{\omega}\omega \,:\, a_k = 0 \text{ for infintiely many } k \in \omega\}$. Player I can easily win the game $\mathsf{G}(A)$, regardless of what Player II does, simply by always playing 0.

Of course, there is no reason to restrict the possible moves of the players to be natural numbers; any countable set can be used instead. Furthermore, it is possible to add **rules** to the game, i.e., to restrict the allowed moves of each player based on the current position in the game. This is formalized by modifying the set A to stipulate that the first player who breaks the rules loses.

Example 17.16 (Conway's Angel and Devil Game)**.** This is an example of an interesting infinite game introduced by John Horton Conway. Fix a natural number p. The **Angel and Devil Game** $\mathsf{AD}(p)$ is played between two players: the Angel (A) and the Devil (D). The game is played on an infinite Go board[xxii], which we can think of as the set $\mathbb{Z} \times \mathbb{Z}$. At the start of the game, the Angel is located at the origin $(0, 0)$, while the rest of the board is empty. On each turn, the Angel must jump from its current location (x, y) to any different empty location (x', y'), with the restriction that $\max\{|x - x'|, |y - y'|\} \leqslant p$ (in other words, the new location can be reached from the old one by a sequence of at most p moves of the chess king). The Devil then "blocks" any single location not currently occupied by the Angel (the Angel may leap over "blocked" locations but cannot land on them). The Devil wins if the Angel is unable to move, while the Angel wins if the game continues indefinitely. For example, the first few moves in $\mathsf{AD}(1)$ may look like this:



The question of which player has the winning strategy in the game $\mathsf{AD}(p)$, depending on p, is surprisingly subtle. Already back in 1982, Elwyn Berlekamp showed that the Devil has a winning strategy in $\mathsf{AD}(1)$. Whether there is any p such that the Angel has a winning strategy in $\mathsf{AD}(p)$ remained an open problem. Finally, after more than two decades of slow progress, in 2006 four (!)

[xxii]Or an infinite chessboard, if one is more readily available.

independent solutions emerged, due to Brian Bowditch, Peter Gács, Oddvar Kloster, and András Máthé. The proofs by Kloster and Máthé actually show that the Angel has a winning strategy already in $\mathsf{AD}(2)$.

The above description of the Angel and Devil Game is not exactly following the general set-up discussed earlier: instead of simply naming arbitrary natural numbers, the players make certain moves on an infinite board. However, as mentioned previously, one can encode this game as a game of the form $\mathsf{G}(A)$ for a suitable set $A \subseteq {}^{\omega}\omega$. For the sake of illustration, we sketch the (somewhat technical but straightforward) encoding below.

Let us agree that the Angel moves first by landing on $(0,0)$. Every move of the Angel involves naming a pair $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ indicating the location on which the Angel should land, while every move of the Devil involves naming a pair $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ indicating the position the Devil wishes to "block." Since the set $\mathbb{Z} \times \mathbb{Z}$ is countable, we can fix a bijection $f \colon \omega \to \mathbb{Z} \times \mathbb{Z}$ and have the players name elements of ω instead of $\mathbb{Z} \times \mathbb{Z}$. Of course, not every move is allowed: the Angel's new location must be close enough to the old one but different from it, and the Devil cannot "block" the Angel's current location. All of this information can be encoded in the set A. Given a sequence $a = (a_0, a_1, \ldots) \in {}^{\omega}\omega$, we say that $n \in \omega$ is a **legal move** in a if:

- either $n = 0$ and $f(a_0) = (0,0)$;
- or $n \geqslant 2$ is even and:
  - $f(a_n) \notin \{f(a_k) \,:\, k < n \text{ is odd}\}$, and
  - $f(a_n) \neq f(a_{n-2})$, and
  - $f(a_n)$ can be reached from $f(a_{n-2})$ by at most p moves of the chess king;
- or n is odd and $f(a_n) \neq f(a_{n-1})$.

Say that a sequence $a = (a_0, a_1, \ldots) \in {}^{\omega}\omega$ is **legal** if all $n \in \omega$ are legal moves in a; otherwise, say that a is **illegal**. In other words, a is legal if it represents a sequence of allowed moves in the game $\mathsf{AD}(p)$. If a is illegal, then let $!(a)$ be the least $n \in \omega$ that is not a legal move in a. Now set

$$A := \{a \in {}^{\omega}\omega \,:\, a \text{ is legal or } !(a) \text{ is odd}\}.$$

Player I (i.e., the Angel) wins in $\mathsf{G}(A)$ if and only if either the game continues indefinitely with both players making allowed moves, *or* Player II (the Devil) breaks the rules first. Thus, the game $\mathsf{G}(A)$ is "equivalent" to $\mathsf{AD}(p)$.

In what follows, we will refer to games with rules, like the Angel and Devil Game, without bothering to write out the corresponding set A explicitly, as it is usually just as straightforward (and just as technical) as in the above example.

We are interested in winning strategies for infinite games. We write $\mathsf{P} := {}^{<\omega}\omega$ and refer to the elements $p \in \mathsf{P}$ as **game positions**. Let

$$\mathsf{P}_{\mathrm{I}} := \{p \in \mathsf{P} \,:\, \mathrm{length}(p) \text{ is even}\} \qquad \text{and} \qquad \mathsf{P}_{\mathrm{II}} := \{p \in \mathsf{P} \,:\, \mathrm{length}(p) \text{ is odd}\}.$$

Thus, P_{I} (resp. P_{II}) is the set of all game positions where it's Player I's (resp. Player II's) time to make a move. A **strategy** for Player I (resp. II) is then a function $\sigma \colon \mathsf{P}_{\mathrm{I}} \to \omega$ (resp. $\sigma \colon \mathsf{P}_{\mathrm{II}} \to \omega$). In other words, a strategy is telling the player what move to make based on the current position. A run $a = (a_0, a_1, \ldots) \in {}^{\omega}\omega$ is **compatible** with a strategy σ for Player I (resp. II) if for all even (resp. odd) $n \in \omega$, we have $a_n = \sigma(a{\restriction}n)$. Thus, if σ is a strategy for Player I, then a run compatible with σ looks like this:

Player I	$a_0 := \sigma(\varnothing)$		$a_2 := \sigma(a_0, a_1)$		$a_4 := \sigma(a_0, a_1, a_2, a_3)$	$\ldots$
Player II		a_1		a_3		$\ldots$

On the other hand, if σ is a strategy for Player II, then a run compatible with σ would look like this:

Player I	a_0		a_2		a_4		$\ldots$
Player II		$a_1 := \sigma(a_0)$		$a_3 := \sigma(a_0, a_1, a_2)$		$a_5 := \sigma(a_0, a_1, a_2, a_3, a_4)$	$\ldots$

A strategy σ for Player I (resp. II) is **winning** in the game $\mathsf{G}(A)$ with $A \subseteq {}^\omega\omega$ if for every run a compatible with σ, we have $a \in A$ (resp. $a \notin A$); in other words, the player following σ is guaranteed to win, regardless of their opponent's moves.

The above discussion goes to show that the intuitive notion of a winning strategy can be formalized in the language of set theory: whether or not a player has a winning strategy in a game of the form $\mathsf{G}(A)$ is really a question of whether or not there exists a function with certain properties.

Exercise 17.16. Let $A \subseteq {}^\omega\omega$. Show that *at most one* of the players has a winning strategy in $\mathsf{G}(A)$.

In contrast to Exercise 17.16, the problem of whether *at least one* of the players has a winning strategy is quite a bit more subtle. Say that a game $\mathsf{G}(A)$ is **determined** if one of the players has a wining strategy. The following statement is known as the **Axiom of Determinacy**:

Determinacy (AD)

For every $A \subseteq {}^\omega\omega$, the game $\mathsf{G}(A)$ is determined.

The reason that we call AD an *axiom* and not a *theorem* is that it cannot be proved in ZFC; in fact, assuming ZFC, AD is false! The reason is that AD is incompatible with AC.

Exercise 17.17. Show that the sets

$$S_{\mathrm{I}} := \{\sigma : \sigma \text{ is a strategy for Player I}\} \qquad \text{and} \qquad S_{\mathrm{II}} := \{\sigma : \sigma \text{ is a strategy for Player II}\}$$

have cardinality $2^{\aleph_0}$ and fix bijections $2^{\aleph_0} \to S_{\mathrm{I}} \colon \alpha \mapsto \sigma^{\mathrm{I}}_\alpha$ and $2^{\aleph_0} \to S_{\mathrm{II}} \colon \alpha \mapsto \sigma^{\mathrm{II}}_\alpha$. Using transfinite recursion, build a set $A \subseteq {}^\omega\omega$ such that for each $\alpha < 2^{\aleph_0}$, neither $\sigma^{\mathrm{I}}_\alpha$ nor $\sigma^{\mathrm{II}}_\alpha$ is a winning strategy in $\mathsf{G}(A)$. Finally, conclude that the game $\mathsf{G}(A)$ is not determined and hence AD fails.

What does all of this have to do with the PSP? It turns out that the failure of AD is a consequence of Theorem 17.14, i.e., the existence of sets without the PSP:

Theorem 17.17. *Assuming* ZF + AD, *every subset* $A \subseteq \mathbb{R}^n$ *has the PSP.*

The connection between AD and the PSP is established by means of a certain game, called the PSP game. Let $A \subseteq \mathbb{R}^n$. The **PSP game** associated to A, denoted $\mathsf{PSP}(A)$, is played as follows. Fix a countable open base $\mathcal{B}$ for $\mathbb{R}^n$ consisting of open balls (which exists by Lemma 17.12). A run of the game $\mathsf{PSP}(A)$ looks like this:

Player I	$B_0(0)$, $B_0(1)$		$B_1(0)$, $B_1(1)$		...	$B_k(0)$, $B_k(1)$		...
Player II		B_0		B_1	...		B_k	...

Set $B_{-1} := \mathbb{R}^n$. On step k, Player I plays a pair of sets $B_k(0)$, $B_k(1) \in \mathcal{B}$ such that:

- the radii of $\overline{B}_k(0)$ and $\overline{B}_k(1)$ are at most 2^{-k},
- $\overline{B}_k(0) \cap \overline{B}_k(1) = \varnothing$ and $\overline{B}_k(0) \cup \overline{B}_k(1) \subseteq B_{k-1}$.

In response, Player II chooses a set $B_k \in \{B_k(0), B_k(1)\}$.[xxiii] The rules of the game, together with Fact 17.5, guarantee that the intersection $\bigcap_{k\in\omega} \overline{B}_k$ contains precisely one point (check this!). Call this point x. Player I wins if $x \in A$; otherwise, Player II wins.

The following fact establishes a link between game theory and the Perfect Set Property:

Theorem 17.18. *Let* $A \subseteq \mathbb{R}^n$. *Then:*

- *Player I has a winning strategy in* $\mathsf{PSP}(A)$ *if and only if* A *has a nonempty perfect subset;*
- *Player II has a winning strategy in* $\mathsf{PSP}(A)$ *is and only if* A *is countable.*

In particular, the game $\mathsf{PSP}(A)$ *is determined if and only if* A *has the PSP.*

[xxiii] This game is an infinite version of the "cut-and-choose" method for dividing a cake.

Proof. There are four implications to prove.

If A has a nonempty perfect subset, then Player I has a winning strategy in $\mathsf{PSP}(A)$. Let $P \subseteq A$ be nonempty and perfect. In order to win the game, Player I ensures that the set $B_k \cap P$ is nonempty, for all $k \in \{-1\} \cup \omega$. This is vacuously true for $k = -1$. If $B_{k-1} \cap P \neq \varnothing$, then, by Lemma 17.9, Player I can choose sets $B_k(0)$ and $B_k(1)$ that satisfy the requirements for being a valid move, while also making the sets $B_k(0) \cap P$ and $B_k(1) \cap P$ nonempty. Then, no matter which one of the sets $B_k(0)$, $B_k(1)$ Player II chooses, it will hold that $B_k \cap P \neq \varnothing$, as desired. By following this strategy, Player I ensures that the unique point $x \in \bigcap_{k\in\omega} \overline{B}_k = \bigcap_{k\in\omega}(\overline{B}_k \cap P)$ belongs to P (see Corollary 17.6), and hence to A, guaranteeing Player I's victory.

If Player I has a winning strategy in $\mathsf{PSP}(A)$*, then A has a nonempty perfect subset.* Let σ be a winning strategy for Player I. To each sequence $f \in {}^{\omega}2$, we associate a point $x_f \in A$ as follows: Follow the run of the game $\mathsf{PSP}(A)$ in which Player I follows the strategy σ, while Player II always sets $B_k := B_k(f(k))$, and let x_f be the resulting point in $\bigcap_{k\in\omega} \overline{B}_k$. Since σ is a winning strategy for Player I, we are guaranteed that $x_f \in A$. Furthermore, as $\overline{B}_k(0) \cap \overline{B}_k(1) = \varnothing$ for all $k \in \omega$, the mapping $f \mapsto x_f$ is injective (check this!). This already shows that $|A| = 2^{\aleph_0}$. To see that A actually contains a nonempty perfect subset, we have to verify that the set $\{x_f : f \in {}^{\omega}2\}$ is perfect. This is left as an exercise.

If A is countable, then Player II has a winning strategy in $\mathsf{PSP}(A)$. Let $A = \{a_k : k \in \omega\}$. Here's a winning strategy for Player II: on step k, choose a set $B_k \in \{B_k(0), B_k(1)\}$ such that $a_k \notin \overline{B}_k$ (such a choice is possible as $\overline{B}_k(0) \cap \overline{B}_k(1) = \varnothing$). If Player II follows this strategy, it is guaranteed that $a_i \notin \bigcap_{k\in\omega} \overline{B}_k$ for every $i \in \omega$, and hence Player II wins.

If Player II has a winning strategy in $\mathsf{PSP}(A)$*, then A is countable.* This is the subtlest and most interesting part of the theorem. Let σ be a winning strategy for Player II. Let P^σ denote the set of all game positions (i.e., finite sequences of moves) **compatible** with σ, i.e., such that can arise when Player II follows the strategy σ. Also, let

$$\mathsf{P}^\sigma_{\mathrm{I}} := \{p \in \mathsf{P}^\sigma : \mathrm{length}(p) \text{ is even}\} \qquad \text{and} \qquad \mathsf{P}^\sigma_{\mathrm{II}} := \{p \in \mathsf{P}^\sigma : \mathrm{length}(p) \text{ is odd}\}.$$

Note that the sets P^σ, $\mathsf{P}^\sigma_{\mathrm{I}}$, and $\mathsf{P}^\sigma_{\mathrm{II}}$ are countable (why?). Let $x \in A$ and consider a position

$$p = ((B_0(0), B_0(1)), B_0, \ldots, (B_{k-1}(0), B_{k-1}(1)), B_{k-1}) \in \mathsf{P}^\sigma_{\mathrm{I}}.$$

We say that p is **critical for** x if $x \in \overline{B}_{k-1}$, but no matter what next move $(B_k(0), B_k(1))$ Player I makes, the strategy σ instructs Player II to choose a set $B_k \in \{B_k(0), B_k(1)\}$ with $x \notin \overline{B}_k$.

Claim 17.19. *For every $x \in A$, there is a position $p \in \mathsf{P}^\sigma_{\mathrm{I}}$ that is critical for x.*

Proof. Suppose, toward a contradiction, that no position $p \in \mathsf{P}^\sigma_{\mathrm{I}}$ is critical for some $x \in A$. Then Player I can win the game while Player II follows the strategy σ, contradicting the assumption that σ is winning; namely, Player I can always ensure that $x \in \overline{B}_k$. Trivially, this holds with $k = -1$. Now, suppose that the game has continued for $k - 1$ moves and the current position is

$$p = ((B_0(0), B_0(1)), B_0, \ldots, (B_{k-1}(0), B_{k-1}(1)), B_{k-1}) \in \mathsf{P}^\sigma_{\mathrm{I}},$$

where $x \in \overline{B}_{k-1}$. Then, since p is not critical for x, there is a valid move $(B_k(0), B_k(1))$ for Player I such that, following σ, Player II chooses a set $B_k \in \{B_k(0), B_k(1)\}$ with $x \in \overline{B}_k$, and we are done. ⊠

Claim 17.20. *If x, $y \in A$ and $p \in \mathsf{P}^\sigma_{\mathrm{I}}$ is a position that is critical both for x and for y, then $x = y$.*

Proof. Write

$$p =: ((B_0(0), B_0(1)), B_0, \ldots, (B_{k-1}(0), B_{k-1}(1)), B_{k-1}).$$

As p is critical for x and y, we have x, $y \in \overline{B}_{k-1}$. Suppose, toward a contradiction, that $x \neq y$. Then Player I can play a pair of sets $(B_k(0), B_k(1))$ so that $x \in B_k(0)$ and $y \in B_k(1)$. Following the strategy σ, Player II chooses either $B_k(0)$ or $B_k(1)$ as B_k; for concreteness, assume that she picks $B_k = B_k(0)$. But then $x \in \overline{B}_k$, so p is not critical for x, a contradiction. ⊠

Now it is easy to finish the argument. For each $x \in A$, let p_x be any position that is critical for x (we can choose one such position using AC, but actually the use of AC can be avoided as there is an explicit well-ordering on P^σ—exercise!). By Claim 17.20, the mapping $A \to \mathsf{P}^\sigma_{\mathrm{I}} \colon x \mapsto p_x$ is injective. Since the set $\mathsf{P}^\sigma_{\mathrm{I}}$ is countable, so is A, as desired. ■

17.6. Borel sets, analytic sets, and the Perfect Set Property

Recall that a set is F_σ if it is the union of countably many closed sets, and G_δ if it is the intersection of countably many open sets. We can then consider countable unions of G_δ-sets, countable intersections of F_σ-sets, countable unions of countable intersections of F_σ-sets, countable intersections of countable unions of G_δ-sets, etc. The sets that can be obtained by iterating countable unions and intersections in this manner are called *Borel*. Formally, we define the class of all Borel sets recursively:

Definition 17.21 (Borel sets)**.** Let $\mathfrak{C}(\mathbb{R}^n)$ denote the set of all closed subsets of $\mathbb{R}^n$. We recursively define sets $\mathfrak{B}_\alpha(\mathbb{R}^n)$ for $\alpha \in \mathbf{Ord}$ as follows:

$$\mathfrak{B}_\alpha(\mathbb{R}^n) \coloneqq \begin{cases} \mathfrak{C}(\mathbb{R}^n) & \text{if } \alpha = 0, \\ \left\{ \bigcup F, \bigcap F \,:\, F \subseteq \mathfrak{B}_\beta(\mathbb{R}^n) \text{ is countable} \right\} & \text{if } \alpha = \beta + 1, \\ \bigcup_{\gamma < \alpha} \mathfrak{B}_\gamma(\mathbb{R}^n) & \text{if } \alpha \text{ is a limit.} \end{cases}$$

Let $\mathfrak{B}(\mathbb{R}^n) \coloneqq \mathfrak{B}_{\aleph_1}(\mathbb{R}^n)$. The sets in the family $\mathfrak{B}(\mathbb{R}^n)$ are called the **Borel** subsets of $\mathbb{R}^n$.

Proposition 17.22. *The family $\mathfrak{B}(\mathbb{R}^n)$ is the smallest collection of subsets of $\mathbb{R}^n$ that includes $\mathfrak{C}(\mathbb{R}^n)$ and is closed under countable unions and countable intersections.*

PROOF. A simple induction on α shows that if $\mathfrak{C}(\mathbb{R}^n) \subseteq \mathfrak{F} \subseteq \mathcal{P}(\mathbb{R}^n)$ and $\mathfrak{F}$ is closed under countable unions and intersections, then $\mathfrak{B}_\alpha(\mathbb{R}^n) \subseteq \mathfrak{F}$ for all $\alpha \in \mathbf{Ord}$, and thus $\mathfrak{B}(\mathbb{R}^n) \subseteq \mathfrak{F}$. It remains to verify that $\mathfrak{B}(\mathbb{R}^n)$ itself is closed under countable unions and intersections (i.e., $\mathfrak{B}_{\aleph_1+1}(\mathbb{R}^n) = \mathfrak{B}_{\aleph_1}(\mathbb{R}_n)$, which is why we stop at $\aleph_1$). Let $F \subseteq \mathfrak{B}(\mathbb{R}^n)$ be countable. For each $S \in F$, let $\alpha_S < \aleph_1$ be the least ordinal such that $F \in \mathfrak{B}_{\alpha_S}(\mathbb{R}^n)$. Since $\mathrm{cf}(\aleph_1) = \aleph_1 > |F|$, the ordinal $\alpha \coloneqq \sup\{\alpha_S \,:\, S \in F\}$ is less than $\aleph_1$. But then both $\bigcup F$ and $\bigcap F$ belong to $\mathfrak{B}_{\alpha+1}(\mathbb{R}^n) \subseteq \mathfrak{B}_{\aleph_1}(\mathbb{R}^n) = \mathfrak{B}(\mathbb{R}^n)$, as desired. ■

By definition, all closed sets are Borel (they belong to $\mathfrak{B}_0(\mathbb{R}^n)$), and so are all open sets (they belong to $\mathfrak{B}_1(\mathbb{R}^n)$ by Exercise 17.5). All F_σ-subsets of $\mathbb{R}^n$ belong to $\mathfrak{B}_1(\mathbb{R}^n)$, while all G_δ-subsets are in $\mathfrak{B}_2(\mathbb{R}^n)$. In general, Borel sets can be much more complicated than that: for every countable ordinal $\alpha < \aleph_1$, there exists a Borel set $S \subseteq \mathbb{R}^n$ such that $S \in \mathfrak{B}_{\alpha+1}(\mathbb{R}^n)$ but $S \notin \mathfrak{B}_\alpha(\mathbb{R}^n)$ (we won't prove this here). Thus, in addition to Theorem 17.11, Definition 17.21 provides another "real (mathematical) life" example where one must use recursion going beyond ω.

Exercise 17.18. Show that if $B \subseteq \mathbb{R}^n$ is a Borel set, then so is its complement $\mathbb{R}^n \setminus B$; moreover, $\mathfrak{B}(\mathbb{R}^n)$ is the smallest collection of subsets of $\mathbb{R}^n$ that includes $\mathfrak{C}(\mathbb{R}^n)$ and is closed under countable unions and complements.

We now have the following generalization of Theorem 17.1:

Theorem 17.23. *Every Borel set $B \subseteq \mathbb{R}^n$ has the PSP, and thus either $|B| \leqslant \aleph_0$ or $|B| \geqslant 2^{\aleph_0}$.*

To prove Theorem 17.23, we introduce another, even larger class of subsets of $\mathbb{R}^n$. We start with a few definitions.[xxiv] Given a (simple undirected) graph G, we let $\mathcal{M}(G)$ be the family of all **maximal cliques** in G, i.e., all subsets $M \subseteq V(G)$ such that:

- every two distinct vertices in M are neighbors in G (i.e., M is a **clique**), and
- if $v \in V(G) \setminus M$, then there is a vertex $w \in M$ that is not adjacent to v.

[xxiv] Our presentation is somewhat unorthodox but it will make our analysis particularly streamlined.

The second condition means that if we add any vertex to M, it will stop being a clique—hence M is indeed a *maximal* clique.

A $\mathfrak{C}(\mathbb{R}^n)$-**labeled graph** is a pair (G, λ), where G is a graph and $\lambda\colon V(G) \to \mathfrak{C}(\mathbb{R}^n)$. We say that a $\mathfrak{C}(\mathbb{R}^n)$-labeled graph (G, λ) is **countable** if G has countably many vertices. For $S \subseteq V(G)$, we let

$$\lambda(S) \coloneqq \bigcap_{v \in S} \lambda(v) \subseteq \mathbb{R}^n.$$

Note that $\lambda(S)$ is a closed set by Exercise 17.4. Given a $\mathfrak{C}(\mathbb{R}^n)$-labeled graph (G, λ), we define

$$\mathcal{A}(G, \lambda) \coloneqq \bigcup_{M \in \mathcal{M}(G)} \lambda(M).$$

The operation $\mathcal{A}$ is called the **Suslin operation**.

Definition 17.24 (Analytic sets)**.** A subset $A \subseteq \mathbb{R}^n$ is called **analytic**[xxv] if $A = \mathcal{A}(G, \lambda)$ for some countable $\mathfrak{C}(\mathbb{R}^n)$-labeled graph (G, λ). The family of all analytic subsets of $\mathbb{R}^n$ is denoted by $\mathfrak{A}(\mathbb{R}^n)$.

The next few lemmas showcase the richness of $\mathfrak{A}(\mathbb{R}^n)$.

Lemma 17.25. *Every closed subset of $\mathbb{R}^n$ is analytic.*

Proof. If $C \subseteq \mathbb{R}^n$ is closed, then $C = \mathcal{A}(G, \lambda)$, where G is a graph with a single vertex v and λ sends v to C (note that the only maximal clique in G is $\{v\}$). ■

Lemma 17.26. *The family $\mathfrak{A}(\mathbb{R}^n)$ of analytic subsets of $\mathbb{R}^n$ is closed under countable unions and countable intersections.*

Proof. Let $\{A_k : k \in \omega\}$ be a countable set of analytic subsets of $\mathbb{R}^n$. Write $A_k = \mathcal{A}(G_k, \lambda_k)$, where (G_k, λ_k) is a countable $\mathfrak{C}(\mathbb{R}^n)$-labeled graph. We may (and do) assume that the vertex sets of the graphs G_k, $k \in \omega$, are disjoint. Define a new $\mathfrak{C}(\mathbb{R}^n)$-labeled graph (G, λ) by

$$V(G) \coloneqq \bigcup_{k \in \omega} V(G_k), \qquad E(G) \coloneqq \bigcup_{k \in \omega} E(G_k), \qquad \text{and} \qquad \lambda \coloneqq \bigcup_{k \in \omega} \lambda_k.$$

In other words, (G, λ) is the disjoint union of the graphs (G_k, λ_k). Notice that a set M of vertices is a maximal clique in G if and only if M is a maximal clique in G_k for some $k \in \omega$ (why?). Therefore,

$$\mathcal{A}(G, \lambda) = \bigcup_{M \in \mathcal{M}(G)} \lambda(M) = \bigcup_{k \in \omega} \bigcup_{M \in \mathcal{M}(G_k)} \lambda_k(M_k) = \bigcup_{k \in \omega} \mathcal{A}(G_k, \lambda_k) = \bigcup_{k \in \omega} A_k,$$

showing that the set $\bigcup_{k \in \omega} A_k$ is analytic. Next we form a graph G' by adding to G all edges between the vertices in $V(G_i)$ and $V(G_j)$ for all $i \neq j$. A set M of vertices is a maximal clique in G' if and only if $M = \bigcup_{k \in \omega} M_k$, where each M_k is a maximal clique in G_k (why?). Thus, $x \in \mathcal{A}(G', \lambda)$ if and only if there exist $M_k \in \mathcal{M}(G_k)$ for all $k \in \omega$ such that $x \in \lambda(\bigcup_{k \in \omega} M_k) = \bigcap_{k \in \omega} \lambda_k(M_k)$, which holds precisely when $x \in \mathcal{A}(G_k, \lambda_k)$ for all $k \in \omega$. It follows that

$$\mathcal{A}(G', \lambda) = \bigcap_{k \in \omega} \mathcal{A}(G_k, \lambda_k) = \bigcap_{k \in \omega} A_k,$$

so $\bigcap_{k \in \omega} A_k$ is analytic. ■

Theorem 17.27. *All Borel subsets of $\mathbb{R}^n$ are analytic.*

Proof. Follows from Lemmas 17.25 and 17.26 and Proposition 17.22. ■

Suslin proved in 1917 that some analytic sets are not Borel; in fact, the class of analytic sets is not closed under taking complements. (Indeed, an analytic set is Borel if and only if its complement is also analytic.) Nevertheless, we can strengthen Theorem 17.23 as follows:

Theorem 17.28. *Every analytic set $A \subseteq \mathbb{R}^n$ has the PSP.*

[xxv] No relation to analytic functions from complex analysis.

To prove Theorem 17.28 (and hence also its corollary, Theorem 17.23), we let (G, λ) be a countable $\mathfrak{C}(\mathbb{R}^n)$-labeled graph and consider the following variation of the PSP game, denoted $\mathsf{PSP}^*(G, \lambda)$. Since G is countable, we may write $V(G) = \{v_k : k \in \omega\}$. Fix a countable open base $\mathcal{B}$ for $\mathbb{R}^n$ consisting of open balls (see Lemma 17.12). A run of the game $\mathsf{PSP}^*(G, \lambda)$ looks like this:

Player I	$B_0(0),\ B_0(1),\ w_0$		$B_1(0),\ B_1(1),\ w_1$		$\ldots$	$B_k(0),\ B_k(1),\ w_k$		$\ldots$
Player II		B_0		B_1	$\ldots$		B_k	$\ldots$

Set $B_{-1} := \mathbb{R}^n$. On step k, Player I plays sets $B_k(0),\ B_k(1) \in \mathcal{B}$ and a vertex $w_k \in V(G)$ so that:

(R1) the radii of $\overline{B}_k(0)$ and $\overline{B}_k(1)$ are at most 2^{-k},

(R2) $\overline{B}_k(0) \cap \overline{B}_k(1) = \varnothing$ and $\overline{B}_k(0) \cup \overline{B}_k(1) \subseteq B_{k-1}$,

(R3) either $w_k = v_k$ or w_k is not a neighbor of v_k in G,

(R4) the set $\{w_0, \ldots, w_k\}$ is a clique in G,

(R5) $\overline{B}_k(0) \cap \lambda(\{w_0, \ldots, w_k\}) \neq \varnothing$ and $\overline{B}_k(1) \cap \lambda(\{w_0, \ldots, w_k\}) \neq \varnothing$.

If Player I cannot make a move following these requirements, then he loses the game. On her turn, as in the PSP game, Player II chooses a set $B_k \in \{B_k(0), B_k(1)\}$. If the game continues indefinitely (i.e., if Player I is always able to make a move allowed by the rules), then Player I wins the game.

Lemma 17.29. *Let (G, λ) be a countable $\mathfrak{C}(\mathbb{R}^n)$-labeled graph and let $A := \mathcal{A}(G, \lambda)$. If Player I has a winning strategy in $\mathsf{PSP}^*(G, \lambda)$, then Player I has a winning strategy in $\mathsf{PSP}(A)$ as well.*

PROOF. Consider a run of the game $\mathsf{PSP}^*(G, \lambda)$ won by Player I:

Player I	$B_0(0),\ B_0(1),\ w_0$		$B_1(0),\ B_1(1),\ w_1$		$\ldots$	$B_k(0),\ B_k(1),\ w_k$		$\ldots$
Player II		B_0		B_1	$\ldots$		B_k	$\ldots$

Rules (R1) and (R2), together with Fact 17.5, ensure that there is a unique point $x \in \bigcap_{k \in \omega} \overline{B}_k$. We claim that $x \in A$. Indeed, let $M := \{w_k : k \in \omega\}$. By (R4), M is a clique in G, while (R3) implies that M is maximal. Suppose, toward a contradiction, that $x \notin \lambda(M)$. Then there is some $k \in \omega$ such that $x \notin \lambda(w_k)$. Since $\lambda(w_k)$ is closed, there is $r \in \mathbb{R}^+$ such that $B(x, r) \cap \lambda(w_k) = \varnothing$. Rule (R1) implies that for all large enough N, $\overline{B}_N \subseteq B(x, r)$, so $\overline{B}_N \cap \lambda(w_k) = \varnothing$, contradicting (R5). Therefore, $x \in \lambda(M) \subseteq A$, as claimed. It follows that Player I wins the following run of $\mathsf{PSP}(A)$:

Player I	$B_0(0),\ B_0(1)$		$B_1(0),\ B_1(1)$		$\ldots$	$B_k(0),\ B_k(1)$		$\ldots$
Player II		B_0		B_1	$\ldots$		B_k	$\ldots$

Hence, if Player I has a winning strategy σ for $\mathsf{PSP}^*(G, \lambda)$, it can be transformed into a winning strategy for Player I in $\mathsf{PSP}(A)$: Player I plays following σ but ignores the vertices $w_0, w_1, \ldots$. ■

Lemma 17.30. *Let (G, λ) be a countable $\mathfrak{C}(\mathbb{R}^n)$-labeled graph. If $A := \mathcal{A}(G, \lambda)$ is uncountable, then Player I has a winning strategy in $\mathsf{PSP}^*(G, \lambda)$.*

PROOF. Given a clique $W \subseteq V(G)$, let A_W be the set

$$A_W := \bigcup \{\lambda(M) : M \in \mathcal{M}(G),\ W \subseteq M\}.$$

Note that $A_W \subseteq \lambda(W)$. We call a position

$$p = ((B_0(0),\ B_0(1),\ w_0),\ B_0,\ \ldots,\ (B_{k-1}(0),\ B_{k-1}(1),\ w_{k-1}),\ B_{k-1}) \tag{17.2}$$

good for Player I if Player I has not lost yet (i.e., Rules (R1)–(R5) are satisfied so far) and the set $B_{k-1} \cap A_{\{w_0, \ldots, w_{k-1}\}}$ is uncountable. The following claim is the key to the proof:

Claim 17.31. *If a position p as in (17.2) is good for Player I, then there is a legal move $(B_k(0), B_k(1), w_k)$ for Player I such that the sets $B_k(0) \cap A_{\{w_0, \ldots, w_k\}}$ and $B_k(1) \cap A_{\{w_0, \ldots, w_k\}}$ are uncountable.*

Proof. Let X be the set of all vertices w such that $\{w_0, \dots w_{k-1}, w\}$ is a clique and either $w = v_k$ or w is not a neighbor of v_k. Every $M \in \mathcal{M}(G)$ with $\{w_0, \dots, w_{k-1}\} \subseteq M$ includes a vertex $w \in X$, so

$$A_{\{w_0,\dots,w_{k-1}\}} = \bigcup_{w \in X} A_{\{w_0,\dots,w_{k-1},w\}}.$$

Since p is good for Player I and X is countable, there exists $w \in X$ such that $B_{k-1} \cap A_{\{w_0,\dots,w_{k-1},w\}}$ is uncountable. Exercise 17.13 then yields open balls B_0, $B_1 \in \mathcal{B}$ such that

- the sets $B_0 \cap A_{\{w_0,\dots,w_{k-1},w\}}$ and $B_1 \cap A_{\{w_0,\dots,w_{k-1},w\}}$ are uncountable,
- the radii of $\overline{B}_0$ and $\overline{B}_1$ are at most 2^{-k}, and
- $\overline{B}_0 \cap \overline{B}_1 = \varnothing$ and $\overline{B}_0 \cup \overline{B}_1 \subseteq B_{k-1}$.

Setting $(B_k(0), B_k(1), w_k) := (B_0, B_1, w)$ finishes the proof. ☒

Assume A is uncountable. Then the starting position $\varnothing$ is good for Player I. We claim the following is a winning strategy for Player I:

Given a position p as in (17.2), pick your next move $(B_k(0), B_k(1), w_k)$ so that the sets $B_k(0) \cap A_{\{w_0,\dots,w_k\}}$ and $B_k(1) \cap A_{\{w_0,\dots,w_k\}}$ are uncountable.

If Player I follows this strategy, then, regardless of Player II's choices, Player I will always be in a good position. In particular, Player I will never break the rules of the game, which means he will not lose. Therefore, the strategy is winning for Player I. ■

PROOF *of Theorem 17.28.* Let $A \subseteq \mathbb{R}^n$ be analytic and let (G, λ) be a countable $\mathfrak{C}(\mathbb{R}^n)$-labeled graph such that $A = \mathcal{A}(G, \lambda)$. Suppose A is uncountable. Then, by Lemma 17.30, Player I has a winning strategy in $\mathsf{PSP}^*(G, \lambda)$. By Lemma 17.29, Player I has a winning strategy in $\mathsf{PSP}(A)$ as well. By Theorem 17.18, it follows that A has a nonempty perfect subset, as desired. ■

As mentioned above, the class of all analytic sets is not closed under complementation. Complements of analytic sets are called **co-analytic**. At this point, it is natural to ask:

Do all co-analytic sets have the PSP?

The answer, surprisingly, is independent of ZFC! However, various additional assumptions on the universe of set theory settle this question one way or the other. For instance, if $\mathcal{U} = L$, then the answer is *no*: in L it is possible to construct an uncountable co-analytic set that does not have a nonempty perfect subset. (This has to do with the fact that it is "extremely easy" to well-order the reals in L.) On the other hand, assuming the existence of some sufficiently large inaccessible cardinals (incompatible with $\mathcal{U} = L$), one can show that every co-analytic set has the PSP.

Questions about the properties of Borel, analytic, etc. sets (such as whether or not they have the PSP) are studied in the area called **descriptive set theory**. The word "descriptive" here refers to the fact that Borel, analytic, etc. sets can be "described" explicitly, i.e., they are not produced by nonconstructive means such as AC. As the above discussion indicates, while descriptive set theory is concerned with subsets of "familiar" spaces such as $\mathbb{R}^n$, the answers to natural questions about such sets can depend in subtle ways on the structure of the ambient set-theoretic universe.

18. Extra problems

18.1. Without Choice

For the following problems, the default axiom system is ZF.

Exercise 18.1. Show that if α is a limit ordinal, then there is $\beta \in \mathbf{Ord}$ such that $\alpha = \omega \cdot \beta$.

Exercise 18.2. Show that if α is a limit ordinal, then $1^\alpha + 2^\alpha = 3^\alpha$ (ordinal exponentiation).

Exercise 18.3. Show that there is a class function $\Phi \colon \mathbf{Ord} \to \mathbf{Ord}$ such that for all $\alpha \in \mathbf{Ord}$, the preimage $\Phi^{-1}(\alpha) := \{\beta \in \mathbf{Ord} \,:\, \Phi(\beta) = \alpha\}$ is a proper class.

Exercise 18.4. Let $\alpha \in \mathbf{Ord}$ and let $f \colon \alpha \to \mathcal{U}$. Show that there is a function $g \colon \alpha \to \mathcal{U}$ such that

$$\bigcup_{\beta<\alpha} g(\beta) = \bigcup_{\beta<\alpha} f(\beta),$$

for all $\beta < \alpha$ we have $g(\beta) \subseteq f(\beta)$, and for all distinct $\beta, \gamma < \alpha$ we have $g(\beta) \cap g(\gamma) = \varnothing$.

Exercise 18.5. Let $\mathcal{C}$ be a class such that $\forall x\, \big((\forall y \in x\, (y \in \mathcal{C})) \to x \in \mathcal{C}\big)$. Show that $\mathcal{C} = \mathcal{U}$.

Exercise 18.6. Suppose X, Y are sets such that $X \times Y = X$. Show that $X = \varnothing$.

Exercise 18.7. Let $\mathcal{C}$ be a class and let $\mathcal{R}$ be a class equivalence relation on $\mathcal{C}$. Show that there is a class function $\Phi \colon \mathcal{C} \to \mathcal{U}$ such that for all $x, y \in \mathcal{C}$, we have $x \,\mathcal{R}\, y$ if and only if $\Phi(x) = \Phi(y)$.

Exercise 18.8. Suppose that $\mathcal{C}$ is a class that is stratified in two ways:

$$\mathcal{C} = \bigcup \{C_\alpha \,:\, \alpha \in \mathbf{Ord}\} = \bigcup \{C'_\alpha \,:\, \alpha \in \mathbf{Ord}\}.$$

Show that there is an ordinal α such that $C_\alpha = C'_\alpha$.

Exercise 18.9. Show that there is a finite list $\varphi_1, \ldots, \varphi_n$ of formulas without parameters (but possibly with free variables) such that if S is a transitive set and $\varphi_1, \ldots, \varphi_n$ are absolute between S and $\mathcal{U}$, then $S = V_\alpha$ for some limit ordinal α.

Exercise 18.10. Recall that ZF consists of infinitely many axioms. Assuming ZF is consistent, show that infinitely many axioms are necessary; i.e., there is no finite list $\varphi_1, \ldots, \varphi_n$ of formulas (with no free variables and without parameters) such that ZF is equivalent to $\varphi_1 \wedge \ldots \wedge \varphi_n$.

Exercise 18.11. Let $\alpha > \omega$ be a countable ordinal. Show that

$V_\alpha \models$ "there exists a well-ordering $\prec$ on some set that is *not* order-isomorphic to an ordinal."

Exercise 18.12. Show that $\mathcal{U} = \mathbf{OD}$ if and only if $\mathbf{OD} \models \mathsf{Ext}$.

Exercise 18.13. Let $\mathcal{W}$ be the class of all well-orderable sets. Show that if $\mathcal{W} \models \mathsf{ZF}$, then $\mathcal{W} = \mathcal{U}$.

Exercise 18.14. Let $\mathcal{C} \subseteq \mathbf{Ord}$ be a proper class. Show that the unique order-isomorphism $\mathcal{C} \to \mathbf{Ord}$ coincides with the Mostowski collapse of $\mathcal{C}$.

18.2. With Choice

For the following problems, the axiom system is ZFC.

Exercise 18.15.

(*a*) What is the cardinality of the set of all countable ordinals?

(*b*) What is the cardinality of the set of all well-orderings of ω?

Exercise 18.16.

(*a*) What is the cardinality of the set of all strictly increasing functions $\omega \to \omega$?

(*b*) What is the cardinality of the set of all strictly increasing functions $\mathbb{Q} \to \mathbb{Q}$?

(*c*) What is the cardinality of the set of all strictly increasing functions $\mathbb{Q} \to \mathbb{R}$?

(*d*) What is the cardinality of the set of all strictly increasing functions $\mathbb{R} \to \mathbb{R}$?

Exercise 18.17. What is the cardinality of the set of all continuous functions $\mathbb{R} \to \mathbb{R}$?

Exercise 18.18. Let E denote the equivalence relation on $\mathbb{R}$ such that for all $x, y \in \mathbb{R}$, $x \, E \, y$ if and only if $x - y \in \mathbb{Q}$. What is the cardinality of the quotient $\mathbb{R}/E$?

Exercise 18.19. Recall that for a set X, we use $[X]^{<\omega}$ (resp. $[X]^{\leqslant\omega}$) to denote the set of all finite (resp. countable) subsets of X.

(*a*) Does there exist a set X such that $X = [X]^{<\omega}$?

(*b*) Does there exist a set X such that $X = [X]^{\leqslant\omega}$?

(*c*) Does there exist a set X such that $X = \mathcal{P}(X)$?

Exercise 18.20. Let $\kappa \geqslant \aleph_0$ be a cardinal and let λ be a cardinal with $0 < \lambda < \mathrm{cf}(\kappa)$. Show that

$$\kappa^\lambda = \max\left\{\kappa, \ \sup\{\rho^\lambda : \rho < \kappa \text{ is a cardinal}\}\right\}.$$

Exercise 18.21. Show that there is a proper class of cardinals κ such that $\kappa^{\aleph_0} < \kappa^{\aleph_1}$.

Exercise 18.22. Let ρ be an infinite cardinal.

(*a*) Show that there is a proper class of cardinals κ such that $\kappa^\rho = \kappa$.

(*b*) Show that there is a proper class of cardinals κ such that $\kappa^\rho > \kappa$.

Exercise 18.23. Assuming GCH, show that for a cardinal $\kappa \geqslant 2$,

$$\kappa^{\aleph_0} < \kappa^{\aleph_1} < \kappa^{\aleph_2} \qquad \Longleftrightarrow \qquad \kappa \leqslant \aleph_1.$$

Exercise 18.24. Let $\Phi \colon \mathcal{U} \to \mathcal{U}$ be a class function and let S be a countable set. Show that there is a set S^* of cardinality at most $2^{\aleph_0}$ such that $S \subseteq S^*$ and for every countable $A \subseteq S^*$, $\Phi(A) \in S^*$.

Exercise 18.25. Let $f \colon \aleph_1 \to \aleph_1$ be a function such that for all $0 < \alpha < \aleph_1$, we have $f(\alpha) < \alpha$. Show that there is $\beta < \aleph_1$ such that the preimage $f^{-1}(\beta) := \{\alpha < \aleph_1 : f(\alpha) = \beta\}$ is uncountable.

Exercise 18.26. Show that there exists a cardinal κ with $\mathrm{cf}(\kappa) = \aleph_1$ and $\kappa = \aleph_\kappa$.

Exercise 18.27. Show that there exists a function $f \colon \mathbb{R} \to \mathbb{R}$ such that for any two real numbers a, $b \in \mathbb{R}$ with $a < b$, the image of the open interval (a, b) under f is equal to $\mathbb{R}$, i.e., $f[(a, b)] = \mathbb{R}$.

Exercise 18.28. Suppose that κ is a weakly inaccessible cardinal. Show that

$$L \models \text{“}\kappa \text{ is strongly inaccessible.”}$$

Exercise 18.29. Show that if there is an inaccessible cardinal, then for some $\alpha < \aleph_1$, $L_\alpha \models \mathsf{ZFC}$.

Exercise 18.30. What is the cardinality of the set of all Borel subsets of $\mathbb{R}^n$?