Set theory and logic

Gunter Fuchs

May 11, 2019

Contents

Introduction

These notes are based on lecture notes that I produced "on the fly" in Summer Semester 2009 at Münster University, Germany, when I taught the lecture course *Logic I.* They have been reworked when I taught a similar course at the Graduate Center of CUNY in Spring 2011, 2012, 2018 and and are now undergoing another revision in Spring 2019.

Even though the course is aimed at an audience familiar with the basics of predicate calculus, such as the concepts of a first order language, models/structures and ultraproducts, these notes are pretty much self-contained.

The approach I choose differs from traditional approaches in several respects. In the first chapter, I describe the syntax of first order logic and give the definition of the Tait calculus, a cut-free proof calculus which is the one preferred by proof-theorists. Being cut-free makes this calculus more amenable to methods from computer science, in particular automated theorem proving. Students with a background in logic have probably not seen this type of calculus, but are likely to have seen a Hilbert-style sequent calculus. So I hope nobody will be bored by this chapter.

I follow a very pure approach, in that I don't give any proofs in the first chapter. The reason is that I could be asked which theory I am proving the theorems in, that is, which meta theory I am using. So in chapter 2, I develop basic set theory. The theorems I am stating are proved in (fragments of) set theory, and in theory, they could be deduced using the Tait calculus I introduced in the first chapter. The main tool from that chapter that will be put to use later is the recursion theorem. I develop basic set theoretic concepts up to ordinals, trees and the axiom of choice with some equivalent formulations. Aside from serving as the meta theory for the further development, students will get to know the basics of set theory in this chapter.

In chapter 3, I use a weak background set theory to define the semantic notions like models and logical consequence. These concepts will most likely be known to the audience, so that this chapter will only be treated very briefly.

Chapter 4 contains proofs of the correctness and the completeness of the Tait-calculus. I prove completeness and compactness first for countable languages only. In a last section, I prove the general completeness and compactness theorems for arbitrary languages, using ultraproducts, and using full ZFC as the background theory. If the audience is familiar with a different correct and complete proof calculus, I may skip this chapter in the lecture, and in that case, it serves as a reference only.

Finally, in chapter 5, I prove Tarski's undefinability of truth theorem, Gödels incompleteness theorems, and develop the necessary background in recursion theory/computability theory. Instead of the traditional Gödel coding of formulas, I use Ackermann's isomorphism which allows to translate relations which are Δ_1 in the hereditarily finite sets to recursive/representable relations. Working in the hereditarily finite sets allows us to apply a weak set theory (without infinity) in order to see that the basic syntactical concepts are representable in arithmetic. I conclude with some large cardinal theory.

Gunter Fuchs, spring 2019

Chapter 1

Syntax

1.1 Words

Definition 1.1.1. Let Σ be a set (the *alphabet*). A free semi-group generated by Σ is a structure $\langle Z, ^\frown \rangle$ (the *words* over Σ), where $^\frown : Z^2 \longrightarrow Z$, satisfying the following axioms:

1. $(x^\frown y)^\frown z = x^\frown(y^\frown z)$. (I am using infix notation for $^\frown$ here, so $x^\frown y$ means $^\frown(x, y)$.)

2. there is an $e \in Z$ such that for all $z \in Z$, $z^\frown e = e^\frown z = z$. e is uniquely determined, and we'll write $\emptyset$ for the *empty word* e.

3. There is an injective map $s \mapsto s'$ from Σ to Z such that whenever $s' = x^\frown y$, then either $x = s'$ and $y = \emptyset$, or $x = \emptyset$ and $y = s'$.

4. every $z \in Z$ has the form $z = s_1'^\frown s_2'^\frown \dots ^\frown s_n'$, where $s_1, \dots, s_n \in \Sigma$. This holds for $z = \emptyset$ with $n = 0$, by convention.

5. if $s_1, \dots s_m$ and $t_1, \dots, t_n \in \Sigma$, then:

$$s_1'^\frown \dots ^\frown s_m' = t_1'^\frown \dots ^\frown t_n' \text{ iff } m = n \text{ and } s_i = t_i \text{ for all } i < n.$$

Remark 1.1.2. A free semi-group generated by a set Σ is uniquely determined by Σ, up to isomorphism. This means that any two semi-groups generated by Σ are isomorphic. That's why I'll refer to *the* semi-group generated by Σ, and I'll denote it by Σ^*. Σ^* may stand for the structure $\langle Z, ^\frown \rangle$ as well as for the set Z, and I'll just refer to it as the collection of words over the alphabet Σ. Also, to save space, I'll drop the connective $^\frown$, and just write xy in place of $x^\frown y$. Dropping the brackets is justified by 1. I'll also identify s and s', for $s \in \Sigma$, so that $\Sigma \subset \Sigma^*$. This just means that we can view symbols of the alphabet as words of length one.

Definition 1.1.3. A member $s \in \Sigma$ *occurs* in a word $w \in \Sigma^*$ if there are words w_0 and w_1 such that $w = w_0{}^\frown s^\frown w_1$. An *occurrence of s in w* is a triple $\langle w_0, s, w_1 \rangle$ such that $w = w_0{}^\frown s^\frown w_1$.

1.2 Languages

Definition 1.2.1. A *first order language* is a quadruple $\mathcal{L} = \langle \mathbb{C}, \mathbb{P}, \mathbb{F}, \# \rangle$ such that

1. $\mathbb{C}, \mathbb{P}$ and $\mathbb{F}$ are pairwise disjoint,

2. $\# : (\mathbb{P} \cup \mathbb{F}) \longrightarrow \mathbb{N}$.

The *alphabet of* $\mathcal{L}$, $\Sigma(\mathcal{L})$, is the least set containing $\mathbb{C}$, $\mathbb{P}$, $\mathbb{F}$ and the following distinct elements:

1. v_n, for $n \in \mathbb{N}$, in the sense that the map $n \mapsto v_n$ exists.
2. $\dot\wedge$, $\dot\vee$, $\dot\neg$, $\dot\forall$, $\dot\exists$, $\dot($, $\dot)$, $\dot;$.
3. $\dot=$. [1]

I'll denote the set $\{v_n \mid n < \omega\}$ by $\mathsf{Var}(\mathcal{L})$.

The *Tait-alphabet* of $\mathcal{L}$, $\Sigma_T(\mathcal{L})$, is the least set containing $\mathbb{C}$, $\mathbb{P}$, $\mathbb{F}$ and the following distinct elements:

1. v_n, for $n \in \mathbb{N}$, in the sense that the map $n \mapsto v_n$ exists.
2. $\dot\wedge$, $\dot\vee$, $\dot\forall$, $\dot\exists$, $\dot($, $\dot)$, $\dot;$. So $\dot\neg$ is missing!
3. $\dot=$ and $\dot{\neq}$.
4. An element $\bar{P}$, for every $P \in \mathbb{P}$, in the sense that the map $P \mapsto \bar{P}$ is injective, and all the elements $\bar{P}$ are new. Let's define $\bar{\bar{P}} = P$, $\overline{\dot=} = \dot{\neq}$ and $\overline{\dot{\neq}} = \dot=$.

1.2.1 Terms

Definition 1.2.2. Let $\mathcal{L} = \langle \mathbb{C}, \mathbb{P}, \mathbb{F}, \# \rangle$ be a language with alphabet $\Sigma(\mathcal{L})$. The set of *terms* of $\mathcal{L}$ is the least subset X of $\Sigma(\mathcal{L})^*$ with the following properties:

1. $\mathsf{Var}(\mathcal{L}) \cup \mathbb{C} \subseteq X$,
2. if $f \in \mathbb{F}$, $n = \#(f)$ and $t_1, \ldots, t_n \in X$, then
$$f^\frown \dot(^\frown t_1{}^\frown \dot;^\frown t_2{}^\frown \dot;\ldots\dot;^\frown t_n{}^\frown \dot) \in X.$$

1.2.2 Formulas

Definition 1.2.3. Let $\mathcal{L} = \langle \mathbb{C}, \mathbb{P}, \mathbb{F}, \# \rangle$ be a language with alphabet $\Sigma(\mathcal{L})$. I shall define what atomic and compound formulas are, and at the same time which occurrences of variables in these formulas are *free* and which are *bound*. Then I'll do the same thing for atomic Tait formulas and compound Tait formulas. Every occurrence of a variable will be either free or bound.

The set of *atomic formulas* of $\mathcal{L}$ is the least subset X of $\Sigma(\mathcal{L})^*$ with the following properties:

1. If t_1 and t_2 are terms of $\mathcal{L}$, then $t_1 \dot= t_2 \in X$.
2. If $P \in \mathbb{P}$, $n = \#(P)$ and $t_1, \ldots, t_n$ are terms of $\mathcal{L}$, then $P\dot(t_1\dot;t_2\dot;\ldots\dot;t_n\dot) \in X$.

Every occurrence of a variable in an atomic formula is free.

The set of *compound formulas* is the least subset X of $\Sigma(\mathcal{L})^*$ with the following properties:

1. If φ_1 and φ_2 are atomic formulas or members of X, then $\dot(\varphi_1 \circ \varphi_2\dot) \in X$, for $\circ = \dot\wedge$ or $\circ = \dot\vee$. An occurrence $\langle \dot(w_0, v_m, w_1 \circ \varphi_2\dot) \rangle$ of v_m in $\dot(\varphi_1 \circ \varphi_2\dot)$ is free (bound) if $\langle w_0, v_m, w_1 \rangle$ is a free (bound) occurrence of v_m in φ_1. Similarly, an occurrence $\langle \dot(\varphi_0 \circ w_0, v_m, w_1\dot) \rangle$ of v_m in $\dot(\varphi_1 \circ \varphi_2\dot)$ is free (bound) if $\langle w_0, v_m, w_1 \rangle$ is a free (bound) occurrence of v_m in φ_2.

[1] This symbol is usually part of the alphabet. In some rare occasions, one may want to work without it though. Still, the default is that it is part of the alphabet.

2. If φ is an atomic formula or a member of X, then $\dot{\neg}{}^\frown\varphi \in X$. An occurrence $\langle\dot{\neg}w_0, v_m, w_1\rangle$ in $\dot{\neg}\varphi$ is free (bound) if $\langle w_0, v_m, w_1\rangle$ is free (bound) in φ.

3. If φ is an atomic formula or a member of X, and $Q = \dot{\forall}$ or $Q = \dot{\exists}$, then $Qv_m\varphi \in X$, for every $m \in \mathbb{N}$ such that v_m does not occur as a bound variable in φ . Every occurrence of v_m in $Qv_m\varphi$ is bound. If $n \neq m$, then every occurrence $\langle Qv_m w_0, v_n, w_1\rangle$ of v_n in $Qv_m\varphi$ is free (bound) if $\langle w_0, v_n, w_1\rangle$ is a free (bound) occurrence of v_n in φ.

The set of *atomic Tait formulas* is the least subset X of $\Sigma_T(\mathcal{L})^*$ with the following properties:

1. If t_1 and t_2 are terms of $\mathcal{L}$, then $t_1 \dot{=} t_2 \in X$ and $t_1 \dot{\neq} t_2 \in X$.

2. If $P \in \mathbb{P}$, $n = \#(P)$ and $t_1, \ldots, t_n$ are terms of $\mathcal{L}$, then $P\dot{(}t_1\dot{,}t_2\dot{,}\ldots\dot{,}t_n\dot{)} \in X$, and also $\bar{P}\dot{(}t_1\dot{,}t_2\dot{,}\ldots\dot{,}t_n\dot{)} \in X$.

Every occurrence of a variable in an atomic Tait formula is free.

The set of *compound Tait formulas* is the least subset X of $\Sigma(\mathcal{L})^*$ with the following properties:

1. If φ_1 and φ_2 are atomic Tait formulas or members of X, then $\dot{(}\varphi_1 \circ \varphi_2\dot{)} \in X$, for $\circ = \dot{\wedge}$ or $\circ = \dot{\vee}$. Whether an occurrence of a variable is free or bound is defined as above.

2. If φ is an atomic Tait formula or a member of X, and $Q = \dot{\forall}$ or $Q = \dot{\exists}$, then $Qv_m\varphi \in X$, for every $m \in \mathbb{N}$ such that v_m does not occur as a bound variable in φ. Again, whether an occurrence of a variable is free or bound is defined as above.

If φ is a formula (or a Tait formula), then a variable v is a *free variable* of φ if there is a free occurrence of v in φ. It is a *bound variable* of φ if there is a bound occurrence of v in φ. It is a *(Tait) sentence* if it has no free variable.

Definition 1.2.4. If φ is a Tait formula, then $\sim\varphi$ is the Tait formula arising by swapping the following symbols:

1. $\dot{\wedge}$ and $\dot{\vee}$,

2. $\dot{\forall}$ and $\dot{\exists}$,

3. $\dot{=}$ and $\dot{\neq}$,

4. P and $\bar{P}$ (for $P \in \mathbb{P}$).

If Γ is a set of Tait formulas, then set

$$\sim\Gamma := \{\sim\varphi \mid \varphi \in \Gamma\}.$$

If φ is a formula, v_m is a free variable of φ, and t is a term, then we want to define $\varphi({}^{v_m}/_{t})$ to basically be the formula arising from φ by replacing every free occurrence of v_m by t. If v_m is the only free variable of φ, then the intended meaning is that $\varphi({}^{v_m}/_{t})$ should express that φ is true of t. There is a phenomenon called collision of variables which complicates matters a little. For example, consider the formula $\varphi = \exists v_0 \quad v_0 \neq v_1$. $\varphi(v_1)$ just says that there is something other than v_1. So $\varphi({}^{v_1}/_{v_0})$ should express that there is something other than v_0. But if we define $\varphi({}^{v_1}/_{v_0})$ by just replacing every free occurrence of v_1 by v_0, the result is the formula $\exists v_0 \quad v_0 \neq v_0$, which says that there is something different from itself, which is not what we expect to express. We would also expect that v_0 should be free in $\varphi({}^{v_1}/_{v_0})$, which is not the case if we perform this simple substitution.

The problem in defining $\varphi({}^{v_m}/_t)$ arises if there are free variables of t that occur as bound variables in φ. It is resolved by passing to an *alphabetic variant* of φ, i.e., a formula which arises from φ by renaming some of its bound variables.

Definition 1.2.5. Let φ be a formula or a Tait formula, v_m a variable and t a term. Let $v_{l_0}, v_{l_1}, \ldots, v_{l_{n-1}}$ be the list of free variables of t that occur as bound variables in φ, if any (ordered according to their indices). Let $v_{m_0}, v_{m_1}, \ldots, v_{m_{n-1}}$ be the first n variables that occur neither in φ nor in t. Let φ' arise from φ by replacing every bound occurrence of v_{l_i} by v_{m_i}, for $i < n$. φ' is called an *alphabetic variant* of φ. No bound variable of φ' occurs in t. Now let $\varphi({}^{v_m}/_t)$ be the formula which arises from φ' by replacing every free occurrence of v_m in φ with t.

If Γ is a set of formulas (or of Tait formulas), then $\Gamma({}^{v_m}/_t) = \{\varphi({}^{v_m}/_t) \mid \varphi \in \Gamma\}$.

So, returning to the example above, we had $\varphi = \exists v_0 \quad v_0 \neq v_1$ and we wanted to make sense of $\varphi({}^{v_1}/_{v_0})$. According to our definition, we get $\varphi' = \exists v_2 \quad v_2 \neq v_1$, and $\varphi({}^{v_1}/_{v_0})$ is the result of replacing v_1 by v_0 in φ', so we get $\varphi({}^{v_1}/_{v_0}) = \exists v_2 \quad v_2 \neq v_0$. This formula expresses that there is something other than v_0, as wished, and v_0 occurs as a free variable.

Usually, I will tacitly assume that no free variable of the term t occurs as a bound variable in φ when forming $\varphi({}^{v_m}/_t)$. Having understood the problem once is sufficient, dealing with it all the time just adds a layer of notational complexity that conceals sometimes simple ideas and reveals nothing (even though it of course would be more correct). So the passage to alphabetic variants by renaming bound variables happens tacitly...

1.3 Proofs

For more on the proof calculus introduced in this section, I refer the reader to [Poh09].

Note: When writing down a formula in some given language, I will use the binary connective $\rightarrow$, even though I don't consider it part of the language. It is meant as an abbreviation, as follows:

$$(\varphi \rightarrow \psi) \text{ means } (\neg\varphi \vee \psi).$$

When using the symbol in Tait formulas, it is to be understood as follows:

$$(\varphi \rightarrow \psi) \text{ means } (\sim\varphi \vee \psi).$$

Definition 1.3.1. Fix a language $\mathcal{L} = \mathcal{L}(\mathbb{C}, \mathbb{P}, \mathbb{F}, \#)$. The *identity axioms* of $\mathcal{L}$ are the following formulas:

Equivalence Relation

(a) $\forall v_0 \forall v_1 \quad (v_0 = v_1 \rightarrow v_1 = v_0)$,

(b) $\forall v_0 \forall v_1 \forall v_2 \quad ((v_0 = v_1 \wedge v_1 = v_2) \rightarrow v_0 = v_2)$,

(c) $\forall v_0 \quad (v_0 = v_0)$

Congruence over functions

For every $F \in \mathbb{F}$ with $n = \#(F)$, the sentence

$$\forall v_0 \forall v_1 \ldots \forall v_{n-1} \forall v_n \forall v_{n+1} \ldots \forall v_{2n-1} \quad (((v_0 = v_n) \wedge (v_1 = v_{n+1}) \wedge \ldots \wedge (v_{n-1} = v_{2n-1})) \rightarrow F(v_0, v_1, \ldots, v_{n-1}) = F(v_n, v_{n+1}, \ldots, v_{2n-1})).$$

Congruence over predicates

For every $P \in \mathbb{P} \cup \bar{\mathbb{P}}$ with $n = \#(P)$, the sentence

$$\forall v_0 \forall v_1 \ldots \forall v_{n-1} \forall v_n \forall v_{n+1} \ldots \forall v_{2n-1} \quad (((v_0 = v_n) \wedge (v_1 = v_{n+1}) \wedge \ldots \wedge (v_{n-1} = v_{2n-1})) \rightarrow (P(v_0, v_1, \ldots, v_{n-1}) \rightarrow P(v_n, v_{n+1}, \ldots, v_{2n-1}))).$$

These formulas can be viewed as being regular formulas or Tait formulas; both are intertranslatable. Let's write Identity for the collection of these axioms.

Definition 1.3.2. Fix a language $\mathcal{L}$. Say that $\vdash_T \Gamma$ if Γ is a finite set of Tait formulas which belongs to the least collection of finite sets of Tait formulas X with the following properties:

1. (Tertium non datur) $\Delta \in X$ whenever there is an atomic Tait formula φ such that $\varphi \in \Delta$ and $\sim\varphi \in \Delta$.
2. ($\wedge$-rule) If $\Delta \cup \{\varphi\} \in X$ *and* $\Delta \cup \{\psi\} \in X$, then $\Delta \cup \{(\varphi \wedge \psi)\} \in X$.
3. ($\vee$-rule) If $\Delta \cup \{\varphi\} \in X$ *or* $\Delta \cup \{\psi\} \in X$, then $\Delta \cup \{(\varphi \vee \psi)\} \in X$.
4. ($\forall$-rule) If $\Delta \cup \{\varphi({}^{v_m}/_{v_n})\} \in X$, where v_n does not occur as a free variable in any formula of $\Delta \cup \{\varphi\}$, then $\Delta \cup \{\forall v_m \varphi\} \in X$.
5. ($\exists$-rule) If $\Delta \cup \{\varphi({}^{x}/_{t})\} \in X$, for some term t, then $\Delta \cup \{\exists x \varphi\} \in X$.

If Γ is a set of $\mathcal{L}_T$-formulas and φ is a $\mathcal{L}_T$-formula, we write $\Gamma \vdash \varphi$ if there is a finite set Γ_0 of $\mathcal{L}_T$-formulas consisting of formulas which are in Γ or an identity-axiom of $\mathcal{L}$, such that $\vdash_T \sim\Gamma_0 \cup \{\varphi\}$.

Note that these rules make a lot of sense when you read "$\vdash_T \Delta \cup \{\varphi\}$" as "$\vdash_T (\bigwedge \sim \Delta) \longrightarrow \varphi$". Note also that in writing $\Delta \cup \{\varphi\}$, it is not assumed that φ doesn't occur in Δ! For more on the proof calculus introduced in this section, I refer the reader to [Poh09].

We have now defined what it means that $\Gamma \vdash \varphi$, i.e., that Γ proves φ, or φ is provable from Γ, for a set Γ of $\mathcal{L}_T$-formulas. But for later reference, it will be useful to formally capture the notion of "proof" that goes with this notion of provability.

Definition 1.3.3. A *derivation* of a finite set Δ of Tait formulas is a finite sequence $\langle \Delta_i \mid i \leq n \rangle$ of finite sets of Tait formulas such that $\Delta_n = \Gamma$, and for each $i \leq n$, one of the following possibilities hold:

1. There is an atomic formula φ such that $\varphi, \sim\varphi \in \Delta_i$.
2. There are $j, k < i$, a set $\bar{\Delta}$ and formulas φ_0, φ_1 such that $\Delta_j = \bar{\Delta} \cup \{\varphi_0\}$, $\Delta_k = \bar{\Delta} \cup \{\varphi_1\}$, and $\Delta_i = \bar{\Delta} \cup \{(\varphi_0 \wedge \varphi_1)\}$.
3. There are $j < i$, a set $\bar{\Delta}$ and formulas φ_0, φ_1 such that $\Delta_j = \bar{\Delta} \cup \{\varphi_0\}$ or $\Delta_j = \bar{\Delta} \cup \{\varphi_1\}$, and $\Delta_i = \bar{\Delta} \cup \{(\varphi_0 \vee \varphi_1)\}$.
4. There are $j < i$, a set $\bar{\Delta} \subseteq \Delta_i$, a formula of the form $\forall v_m \varphi$ and a variable v_n which doesn't occur as a free variable in any of the formulas from $\bar{\Delta} \cup \{\varphi\}$, such that $\Delta_j = \bar{\Delta} \cup \{\varphi({}^{v_m}/_{v_n})\}$ and $\Delta_i = \bar{\Delta} \cup \{\forall v_m \varphi\}$.
5. There are $j < i$, a set $\bar{\Delta}$, a formula of the form $\exists v_m \varphi$ and a term t such that $\Delta_j = \bar{\Delta} \cup \{\varphi({}^{v_m}/_{t})\}$ and $\Delta_i = \bar{\Delta} \cup \{\exists v_m \varphi\}$.

Now let Γ be a set of Tait formulas, and let ψ be a Tait formula. A *proof of ψ from Γ* is a derivation of a finite set Δ of Tait formulas such that for every $\varphi \in \Delta$, at least one of the following hold:

1. φ is the negation of a formula in Γ (i.e., $\sim\varphi \in \Gamma$),
2. φ is the negation of an identity axiom (i.e., $\sim\varphi$ is an identity axiom),
3. $\varphi = \psi$.

Note: The finite subset $\bar{\Delta}$ of Δ_i in the previous definition always is either equal to Δ_i or results from Δ_i by omitting one formula. Also, it is easy to check that $\vdash_T \Delta$ iff there is a derivation of Δ, and $\Gamma \vdash \psi$ iff there is a proof of ψ from Γ.

Chapter 2

Sets

Recommended literature for this chapter: [Jec03], [Kun80].

The role of set theory is two-fold: On the one hand, (a fragment of) it serves as the meta-theory. On the other hand, it can be viewed as a formal theory to which we can apply the logical methods we are going to develop. The theorems I am going to prove could be proved formally, using the calculus introduced in the first chapter. But of course, I am not going to give formal proofs. It's just good to know that in theory, it would be possible to do so.

The aim is to axiomatize the usage of sets in mathematics without running into contradictions. Formally, the language we are going to use only consists of one binary predicate, denoted by $\dot{\in}$. In addition, we have the equality symbol at our disposal, which belongs to every language (by our convention). In fact, it will turn out that equality becomes definable in set theory.

As a first attempt to axiomatizing set theory, let's look at a quote of Georg Cantor:

> Unter einer "Menge" verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die "Elemente" von M genannt werden) zu einem Ganzen.

This translates (loosely) to: We understand a "set" to be any collection M of certain distinct objects of our thinking or our visualization/intuition/perception (called the "elements" of M) to a whole.

Let's try to formalize this approach rigorously. The obvious questions are what a collection should be, and what the objects of our thinking should be. One might at first expect objects of mathematical thinking to be things like natural numbers, integers, rationals, real numbers, etc., which then can be used to form more complicated structures. The purest and simplest approach to set theory, however, seems to be the one in which every object is a set. This way, we don't have to distinguish between different types of objects of our thinking. And sooner or later, we are going to have to deal with sets anyway (such as sets of numbers, sets of functions, etc.), for we can think about them. So restricting our attention to sets simplifies things, and in formalizing Cantor's idea, we can neglect the question about the nature of the objects of our thinking, and focus instead on the question what a collection should be. Again, the most naive approach would be to say that anything that can be defined by a property should be a collection (like, for example, the collection of all even numbers). That x has a property would be formalized by saying that some formula $\varphi = \varphi(x, \vec{z})$[1] is true of x. So one might demand that

$$\{x \mid \varphi(x, \vec{z})\}$$

[1]When writing $\psi(x, \vec{y})$, I mean that $x, \vec{y}$ are the free variables of ψ.

is a set. More formally, this would mean:

$$\forall\vec{z}\exists y \quad y = \{x \mid \varphi(x,\vec{z})\},$$

or, in other words:

$$\forall\vec{z}\exists y\forall x(x \in y \leftrightarrow \varphi(x,\vec{z})).$$

Here, I use $(\varphi \leftrightarrow \psi)$ as an abbreviation for $((\varphi \to \psi)\wedge(\psi \to \varphi))$, which, in turn, is an abbreviation for a longer formula.

The problem is that this leads to a contradiction: let's apply the above principle to the formula $\varphi = (x = x)$. We'd get that $\mathrm{V} := \{x \mid x = x\}$ is a set, or more precisely, there would be a set V such that for all x, we have that $x \in \mathrm{V}$ iff $x = x$. Clearly, it would satisfy

$$\mathrm{V} = \mathrm{V}$$

since it is an identity axiom that for any object z, $z = z$ holds. So by definition of V,

$$\mathrm{V} \in \mathrm{V}.$$

This contradicts the common view of a set: a set should not be a member of itself. It is not a formal contradiction, though, and one can formalize set theory without excluding this possibility. But let's investigate the sets which do not have themselves as a member some more:

$$A = \{x \mid x \notin x\}.$$

In other words, we have that $x \in A$ iff $x \notin x$. According to our strong set existence principle, there would have to be such a set A. So:

$$\text{Either } A \in A \text{ or } A \notin A.$$

But by definition of A, we have:

$$A \in A \iff A \notin A.$$

This is known as Russel's antinomy. Note that the contradiction only arose because we assumed that A is a set. For A is the collection of all *sets* that don't contain themselves as elements. So if A is not a set, then clearly, $A \notin A$ - A only contains sets. So, a different way of looking at Russel's antinomy is that it shows by contradiction that A is not a set. So not every collection of sets that can be defined by having a property in common is a set, which shows that we have to use somewhat weaker set existence principles. I shall develop these in the following.

2.1 Fragments of ZFC

Literature: Any book on axiomatic set theory will do, but to be specific, I refer to [Jec03]. The approach chosen there is close to the one I use.

The language of set theory I shall use is $\mathcal{L} = \mathcal{L}_{ST} = \langle \mathbb{C}, \mathbb{P}, \mathbb{F}, \# \rangle$, where $\mathbb{C} = \mathbb{F} = \emptyset$, $\mathbb{P} = \{\dot{\in}\}$ and $\#(\dot{\in}) = 2$. As usual, I will use the infix notation for the predicates $\dot{\in}$ and $\dot{=}$, and also, I shall drop the dots most of the time. Thus, e.g., I shall write

$$\forall x(x \in y \to x = z)$$

instead of

$$\forall x(\dot{\in}(x,y) \to \dot{=}(x,z)).$$

Also, I shall use $x, y, z, u, v, w, etc.$ as meta-variables for variables. So x is really some v_m, but I don't say which.

The axioms I am going to introduce together will form the axiom system called ZFC. ZF stands for Zermelo-Fraenkel and is named after the founders of the system. The "C" stands for the axiom of choice that I will introduce in Section 2.4.

The first axiom I want to introduce is the *Set Existence* Axiom,

$$\exists x \quad x = x.$$

This axiom is really a logical axiom, since usually one does not consider models with empty domain. Sometimes it is formulated to express that there is a set which has no elements, i.e., $\exists x \forall y \neg y \in x$. This form of the axiom will be a consequence of the other axioms, though.

The second basic axiom I need is the *Extensionality* Axiom, saying:

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y).$$

It expresses that if two sets have the same members, then they are equal. The converse is true anyway, by the identity axioms.

Before introducing further axioms, let me introduce a simpler way of writing them down. Namely, if $\varphi(x, y_1, \ldots, y_n)$ is a formula with free variables shown, then I will call a syntactical object of the form

$$\{x \mid \varphi(x, y_1, \ldots, y_n)\}$$

a *class term.* Often I shall write $\vec{y}$ in place of $y_1, \ldots, y_n$. I will also consider any variable a class term.

I shall use capital letters for class terms; for example, I set:

$$\mathrm{V} := \{x \mid x = x\}.$$

A class term is either a variable or given by a formula as above. I am going to use class terms in formulas, but these class terms can always be eliminated, producing a regular $\mathcal{L}_{ST}$-formula. This is how it works. If A is a class term, then

$$x \dot{\in} A := \begin{cases} x \in v_m & \text{if } A \text{ is the variable } v_m, \\ \varphi(^u/_x) & \text{if } A \text{ is the class term } \{u \mid \varphi(u, \vec{y})\}. \end{cases}$$

Note that I haven't defined the meaning of $A \in B$, if A is not a variable; the x above stands for a variable only. Before explaining this though, let me stipulate:

$$A \dot{=} B := \forall x (x \in A \leftrightarrow x \in B).$$

For definiteness, we may specify that $x = v_m$, where m is least such that v_m does not occur in A or in B. Note that the meaning of $x \in A$ and $x \in B$ is defined above. Note also that this interpretation of $A = B$ conforms with the axiom of extensionality. Now I'm ready to explain the meaning of $A \in B$:

$$A \dot{\in} B := \exists x (x \in B \wedge x = A).$$

Boolean combinations of formulas with class terms are handled in the usual way. Thus, if φ, ψ are formulas in which class terms occur, and if φ' and ψ' are their translations to regular $\mathcal{L}_{ST}$ formulas, then the translation of $(\varphi \circ \psi)$ is $(\varphi' \circ \psi')$, for $\circ = \wedge$ or $\circ = \vee$, and the translation of $\neg\varphi$ is $\neg\varphi'$.

Finally, let's consider the translation of $\exists x \varphi$. It will only be defined if x occurs as a free variable in φ, but not as a bound variable. If class terms are allowed to occur in φ, then we also require that x does not occur as a bound variable in any of the class terms occurring in φ. Here, a variable y occurs as a bound variable in the class term $\{z \mid \chi(z, \vec{w})\}$ if y occurs as a bound variable in χ, or if it is equal to z. Similarly, the free variables of $\{z \mid \chi(z, \vec{w})\}$ are the ones that are free in $\chi(z, \vec{w})$ but different from z. Now, in the case that x occurs as a free variable in φ, but not as a bound one, then we can translate $\exists x \varphi$ as $\exists x \varphi'$.

Class terms other than variables are not allowed to appear right after a quantifier, so it is clear now how to eliminate class terms from formulas. Note that the introduction of these terms is a mere convenience, making formulas more easily readable. While we're at it, I would like to define some operations on class terms. Again, these are just abbreviations.

Definition 2.1.1. Let A and B be class terms.

1. $A \cup B := \{x \mid (x \in A \vee x \in B)\}$,
2. $A \cap B := \{x \mid (x \in A \wedge x \in B)\}$,
3. $A^c := \{x \mid \neg x \in A\}$,
4. $A \setminus B := A \cap B^c$.

Also, I want to use the following reserved class terms:

$$\mathrm{V} = \{x \mid x = x\}, \quad \emptyset = \mathrm{V}^c = \{x \mid \neg x = x\}.$$

It is sometimes useful to allow class terms of the form

$$\{A_1, \ldots, A_n\},$$

where each A_j is a class-term. The interpretation is:

$$\{A_1, \ldots, A_n\} = \{x \mid x = A_1 \vee x = A_2 \vee \ldots \vee x = A_n\}.$$

Finally, I also want to consider class terms of the form

$$\{A|_{\vec{y}} \varphi(\vec{x}, \vec{y})\},$$

where A is a class term with free variables $\vec{y}$. The intended meaning is

$$\{A \mid_{\vec{y}} \varphi(\vec{x}, \vec{y})\} = \{z \mid \exists \vec{y}(\varphi(\vec{x}, \vec{y}) \wedge z = A)\}.$$

Usually, the variables $\vec{x}$ will occur as free variables in A as well, but not necessarily. And usually, $A = A(\vec{x}, \vec{y}, \vec{z})$ will always be a set when $\varphi(\vec{x}, \vec{y})$ holds. The purpose of the subscript $\vec{y}$ is to clarify that the variables $\vec{y}$ are bound.

Note that the set existence axiom can be expressed as $\mathrm{V} \neq \emptyset$. The next axiom is the *Pairing* Axiom:

$$\forall x \forall y \{x, y\} \in \mathrm{V}.$$

Unraveling this formula, eliminating the class terms, yields a formula equivalent to this:

$$\forall x \forall y \exists z \forall u (u \in z \leftrightarrow (u = x \vee u = y)).$$

I hope the advantage of using class terms is becoming clearer now. I'll use another operation on class terms:

Definition 2.1.2. If A is a class term, then let $\bigcup A$ be the following class term:

$$\bigcup A := \{z \mid \exists y(y \in A \wedge z \in y)\},$$

where z and y do not occur in A (as usual). This is called the inner union of A. Sometimes it is written as $\bigcup_{z\in A} z$. I also use the notation

$$A \cup B := \{z \mid z \in A \vee z \in B.$$

Analogously $\bigcap A$ is short for

$$\bigcap A := \{z \mid \forall y(y \in A \to z \in y)\}$$

and

$$A \cap B := \{z \mid z \in A \wedge z \in B\}.$$

The remarks above apply. Finally, I'll write $A \subseteq B$ as a short form for the statement

$$\forall x(x \in A \to x \in B).$$

In order to get familiar with these concepts, the reader may try to figure out what $\bigcap \emptyset$ is... The next axiom I'll introduce is the *Union* axiom:

$$\forall x \bigcup x \in \mathrm{V}.$$

I trust the reader will be able to retranslate this into a $\mathcal{L}_{ST}$-formula.

Lemma 2.1.3. *It is provable from the axioms introduced thus far that*

1. $\forall x \forall y \quad x \cup y \in \mathrm{V}$.
2. $\forall x_1 \forall x_2 \ldots \forall x_n \quad \{x_1, x_2, \ldots, x_n\} \in \mathrm{V}$.

Proof. This is true in the sense that if Γ is the set of axioms introduced thus far,

$$\Gamma \vdash \forall x \forall y x \cup y \in \mathrm{V},$$

and the same applies to the second sentence. But instead of trying to obtain a formal proof, I shall argue informally. Later, we shall see that such informal arguments can be translated into a formal proof, in principle.

For 1., let x, y be given. By the Pairing Axiom, $\{x, y\} \in \mathrm{V}$. By the Union Axiom, $\bigcup\{x, y\} \in \mathrm{V}$. But by definition, $\bigcup\{x, y\}$ is the same as $x \cup y$, so we're done.

For 2., let $x_1, x_2, \ldots, x_n$ be given. By Pairing, $\{x_1\} \in \mathrm{V}$, $\{x_2\} \in \mathrm{V}$, ..., $\{x_n\} \in \mathrm{V}$. Applying 1. (n-1) times, it follows that $\{x_1\} \cup \{x_2\} \cup \ldots \cup \{x_n\} \in \mathrm{V}$. But that's just $\{x_1, x_2, \ldots, x_n\}$. □

The next axiom is a way of avoiding Russel's antinomy, while still allowing us to collect sets which satisfy a certain property into one set. It is called the *Separation* Axiom. For every class term A, it says:

$$\forall x \; A \cap x \in \mathrm{V}.$$

More formally, one should demand that x does not occur in A, and one should take the universalization of this formula, meaning that one prefixes it with $\forall y_1 \forall y_2 \ldots \forall y_n$, where $\vec{y}$ lists the free variables occurring in A.

I will take this as a convention: If free variables occur in an axiom, then I mean the sentence obtained by prefixing the formula with universal quantifiers which bind these variables. Remember that class terms may contain "concealed" free variables, as is the case in the Separation Axiom.

So this axiom does not say that the collection of all sets having some property is a set, but that the collection of all sets having some property *and* being a member of some fixed set is a set. The idea is that since this fixed set is a set, we have understood it well enough that we can understand the collection of its members which satisfy some property, so that we don't run into a contradiction.

If Γ is a set of $\mathcal{L}_{ST}$-formulas, then Γ-Separation is formulated like the Separation-Axiom, but only for class terms A whose formula is in Γ.

Lemma 2.1.4. *The following are consequences of the axioms introduced thus far:*

1. $\emptyset \in \mathrm{V}$.
2. $\forall x \quad (A \subseteq x \to A \in \mathrm{V})$.
3. $(A \neq \emptyset \to \bigcap A \in \mathrm{V})$.
4. $\mathrm{V} \notin \mathrm{V}$.
5. $\forall x \quad x^c \notin \mathrm{V}$.

Proof. 1. By Set Existence, there exists some set x. By Separation, $x \cap \emptyset \in \mathrm{V}$. By definition of $\emptyset$, $x \cap \emptyset = \emptyset$.

2. If $A \subseteq x$, then $A = A \cap x \in \mathrm{V}$, by Separation.

3. Pick $a \in A$ (so $a \in \mathrm{V}$). Then $\bigcap A \subseteq a$, so by 2., $\bigcap A \in \mathrm{V}$.

4. Suppose $v := \mathrm{V} \in \mathrm{V}$. As in the introduction to this chapter, let $A = \{x \mid x \notin x\}$. Clearly, $A \subseteq v$, so by 2., $a := A \in \mathrm{V}$. But then, $a \in a \leftrightarrow a \notin a$.

5. If $x^c \in \mathrm{V}$, then $x \cup x^c \in \mathrm{V}$, by Lemma 2.1.3, 1. But clearly, $x \cup x^c = \mathrm{V}$. □

The following class term will often be very useful:

Definition 2.1.5.
$$\langle A, B \rangle := \{\{A\}, \{A, B\}\}.$$
$\langle A, B \rangle$ is the *ordered pair* of A and B.

Just as in the case of class terms of the form $\{A, B\}$, the ordered pair only is useful for class terms A and B which are sets.

Lemma 2.1.6. *For $x, y, v, w \in \mathrm{V}$:*

1. $\langle x, y \rangle \in \mathrm{V}$,
2. $(\langle x, y \rangle = \langle v, w \rangle \to (x = v \wedge y = w))$.

Proof. Exercise. □

One can generalize the formation of ordered pairs to produce finite tuples:

Definition 2.1.7. Set:

$$\begin{aligned} \langle x \rangle &= x \\ \langle x_1, \ldots, x_{n+1} \rangle &= \langle x_1, \langle x_2, \ldots, x_{n+1} \rangle \rangle. \end{aligned}$$

Clearly then:

Lemma 2.1.8. *For all sets $x_1, \ldots, x_n$, $y_1, \ldots, y_n$:*

1. $\langle x_1, \ldots, x_n \rangle \in \mathrm{V}$,
2. *if* $\langle \vec{x} \rangle = \langle \vec{y} \rangle$, *then* $x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n$.

Having ordered pairs and tuples at our disposal enables us to define Cartesian products, relations and functions.

Definition 2.1.9.

$$\begin{aligned} A \times B &:= \{\langle x, y \rangle \mid x \in A \wedge y \in B\}, \\ A_1 \times \ldots \times A_n &:= A_1 \times (A_2 \times \ldots \times A_n), \\ A^n &:= \underbrace{A \times \ldots \times A}_{n \text{ times}}. \end{aligned}$$

Definition 2.1.10. A class term R is a *relation* if $R \subseteq \mathrm{V}^2$. We shall often write xRy instead of $\langle x, y \rangle \in R$. R is an n-ary relation if $R \subseteq \mathrm{V}^n$ (for $n \geq 2$).

When writing "R is a relation", I really mean the formula that $R \subseteq \mathrm{V}^2$ is a short form for. Remember that R is either a variable or a class term; in the latter case, R is basically given by a defining formula.

Note that $\mathrm{V}^n \subseteq \mathrm{V}$, and if $n \geq m$, then $\mathrm{V}^n \subseteq \mathrm{V}^m$, because of the particular way n-tuples were defined.

Definition 2.1.11.

$$\begin{aligned} \mathrm{dom}(R) &= \{x \mid \exists y \quad yRx\}, \\ \mathrm{ran}(R) &= \{y \mid \exists x \quad yRx\}, \\ \mathrm{fld}(R) &= \mathrm{dom}(R) \cup \mathrm{ran}(R), \\ R \upharpoonright A &= \{\langle y, x \rangle \mid x \in A \wedge yRx\}, \\ R``A &= \{y \mid \exists x \; x \in A \wedge yRx\}, \\ R^{-1} &= \{\langle x, y \rangle \mid yRx\} \end{aligned}$$

Definition 2.1.12. If F is a class term, then "F is a function" stands for the following formula:

$$\text{"}F \text{ is a relation"} \wedge \forall y_0 \forall y_1 \forall x ((y_0 F x \wedge y_1 F x) \rightarrow y_0 = y_1).$$

In case F is a function with $x \in \mathrm{dom}(F)$, I shall write $F(x)$ for the uniquely determined y such that yFx. Note that this can be expressed as a class term, as follows:

$$F(x) = \bigcap \{y \mid yFx\}.$$

If $\mathrm{dom}(F) \subseteq \mathrm{V}^n$, then I shall write $F(x_1, \ldots, x_n)$ in place of $F(\langle x_1, \ldots, x_n \rangle)$.

Now I'm ready to introduce the Replacement Axiom:

$$\forall x \quad (\text{"}F \text{ is a function"} \rightarrow F``x \in \mathrm{V}).$$

Again, this is a scheme of axioms, one formula for each class term.

Lemma 2.1.13. *The Separation Axiom scheme is provable from the Replacement Axiom scheme.*

Proof. Let $\mathrm{id} = \{\langle x, x\rangle \mid x \in \mathrm{V}\}$; this is clearly a function. Now, given any class term A and any set a, it follows that $\mathrm{id}\restriction A$ is also a function, and $A \cap a = (\mathrm{id}\restriction A)``a \in \mathrm{V}$, by Replacement. □

The axioms introduced so far form the weakest fragment of the axioms of set theory we shall work with. I call it ZF^{--}, which is an ad-hoc name. So it consists of the following axioms:

- Set Existence
- Pairing
- Union
- Extensionality
- Separation
- Replacement

Lemma 2.1.14. *The following are consequences of the* ZF^{--} *axioms:*

1. $\forall x \forall y \quad x \times y \in \mathrm{V}$,
2. $\forall x_1 \forall x_2 \ldots \forall x_n \quad x_1 \times \ldots \times x_n \in \mathrm{V}$,
3. $\forall x($*"F is a function"* $\rightarrow F\restriction x \in \mathrm{V})$.

Proof. 1.) Fix x and y. First note:

$$\forall z \quad x \times \{z\} \in \mathrm{V}.$$

To see this, fix z. We know already that for any set u, $\langle u, z\rangle \in \mathrm{V}$. So the following defines a function with domain x:

$$F_z := \{\langle\langle u, z\rangle, u\rangle \mid u \in x\},$$

i.e., $F_z(u) = \langle u, z\rangle$, for $u \in x$. By Replacement, $F_z``x \in \mathrm{V}$, and by definition,

$$F_z``x = \{\langle u, z\rangle \mid u \in x\} = x \times \{z\}.$$

Knowing this, we can now define a function G as follows:

$$G := \{\langle x \times \{z\}, z\rangle \mid z \in y\},$$

i.e., $G(z) = x \times \{z\}$, for $z \in y$. Applying Replacement again yields that $G``y \in \mathrm{V}$, and by definition of $G$, $a := G``y = \{x \times \{z\} \mid z \in y\}$. But then $\bigcup a \in \mathrm{V}$, by the Union axiom, and $\bigcup a = x \times y$, as is easily checked.

2.) Follows by induction from 1.)

3.) Fix F and x. Then $F\restriction x = F \cap ((F``x) \times x)$. $F``x \in \mathrm{V}$ by Replacement, so that $(F``x) \times x \in \mathrm{V}$ by 1., so that $F \cap ((F``x) \times x) \in \mathrm{V}$ by Separation. □

The next axiom I'll introduce is the Power Set Axiom. Given a class term A, let

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}$$

be its power class. The Power Set Axiom says:

$$\forall x\ \mathcal{P}(x) \in \mathrm{V},$$

i.e., the power class of a set is a set. A lot of set theory can be done without the power set axiom, and there are natural models of set theory that don't satisfy it, so I shall sometimes not assume it.

The last axiom I want to introduce at this early stage has to do with the question raised in the introduction to this chapter: Can/should there be a set x with $x \in x$? The Foundation Axiom excludes this possibility (among others). To formulate it, I need the following:

Definition 2.1.15. x is $\in$-minimal in A if $x \in A$ and for all $y \in x$, $y \notin A$.

The Foundation Axiom now is the following scheme of sentences:

$$A \neq \emptyset \to \exists x \; x \text{ is } \in\text{-minimal in } A,$$

one for each class term. I call the system of axioms comprised of ZF^{--}, together with the Foundation axiom scheme ZF^{--}_F.

Lemma 2.1.16 (ZF^{--}_F)**.** *There is no finite sequence of sets $x_1 \ni x_2 \ni \ldots \ni x_n \ni x_1$.*

Proof. Otherwise $\{x_1, x_2, \ldots, x_n\}$ has no $\in$-minimal member. □

2.2 Well-founded Relations

In this section, I shall work with the axioms introduced thus far, save Power Set and Foundation, unless stated otherwise. This is what I refer to as ZF^{--} in these notes.

Definition 2.2.1. Given class terms A and R, we say that x is *R-minimal* in A to express that R is a relation, $x \in A$ and for all y, if yRx, then $y \notin A$. A relation R is *set-like* if for all x, $R``\{x\} \in \mathrm{V}$. Saying that R is *well-founded* stands for the scheme of formulas

$$(A \neq \emptyset \to \exists x \quad x \text{ is } R\text{-minimal in } A),$$

one formula for each class term A. R is *strongly well-founded* if R is well-founded and set-like. A is R-closed if $R``A \subseteq A$.

If $r \subseteq \mathrm{V}^2$ is a relation which is a set, then in a slight abuse of notation, I will call r well-founded if every nonempty *set* has an r-minimal element. Note that this is equivalent to the scheme version of well-foundedness in this case, but expressible in by one formula.

Lemma 2.2.2. *Let $R \subseteq \mathrm{V}^2$ be set-like. Then:*

1. *$\forall u \quad R``u \in \mathrm{V}$,*
2. *If u is R-closed, for all $u \in A$, then $\bigcap A$ and $\bigcup A$ are R-closed,*
3. *Suppose R is well-founded. Then for every set u there is a set v which is minimal wrt. inclusion such that $u \subseteq v$ and v is R-closed.*

Remark 2.2.3. We shall see later that the last point of this lemma follows from an axiom that I have not introduced yet, the infinity axiom, without assuming R is well-founded.

Proof. 1.) $R``u = \bigcup\{R``\{x\} \mid x \in u\} = \bigcup F``u \in \mathrm{V}$, where $F(x) = R``\{x\}$, by Replacement and Union.

2.) This is trivial.

3.) Given any set x, I first claim that there is a set w such that $x \in w$ and w is R-closed. For if not, consider the class A of sets for which this fails. Pick x R-minimal in A. Then $R``\{x\} \in \mathrm{V}$, and every $y \in R``\{x\}$ (i.e., yRx) is not in A. So, momentarily fixing such a y, the class B_y of sets z which are R-closed and have $y \in z$ is non-empty. Hence $w_y := \bigcap B_y$ is a set, by 2.) it's R-closed (and by definition, it's the $\subseteq$-minimal set which has y as a member and which is R-closed). Now define $F(y) = w_y$ for $y \in R``\{x\}$. Then by Replacement and Union, $\{x\} \cup \bigcup F``R``\{x\} \in \mathrm{V}$, and clearly, this set is R-closed and has x as an element. This is a contradiction.

It now follows that given any set x, there is a least set w_x (wrt. inclusion) having x as a member and being R-closed (as in the first part of the proof, this is just the intersection of all sets which have these properties; since there is such a set, the intersection is again a set).

Now given an arbitrary set u, one can form $\bigcup\{w_x \mid x \in u\} = \bigcup G``u \in \mathrm{V}$, where $G(x) := w_x$. □

Definition 2.2.4. Given class terms F, A and B, write $F : A \to B$ to express that F is a function, $\mathrm{dom}(F) = A$ and $\mathrm{ran}(F) \subseteq B$. Write $F : A \rightarrowtail B$ to express that $F : A \to B$ and for all $x, y \in A$, $x \neq y \to F(x) \neq F(y)$. Write $F : A \twoheadrightarrow B$ to express that $F : A \to B$ and $B = F``A$. Finally, $F : A \rightarrowtail\!\!\!\!\!\twoheadrightarrow B$ expresses that $F : A \rightarrowtail B$ and $F : A \twoheadrightarrow B$.

Theorem 2.2.5 (Recursion Theorem)**.** *Let R be a strongly well-founded relation, $R \subseteq A^2$. Let $G : A \times \mathrm{V} \to B$. Then there is a unique $F : A \longrightarrow B$ such that for all $x \in A$,*

$$F(x) = G(x, F{\restriction}R``\{x\}).$$

This means that, given class terms R, A, G, there is a class term F such that it is provable from our axioms, together with the scheme expressing that R is a strongly well-founded relation and the other assumptions of the theorem, that F satisfies $F(x) = G(x, F{\restriction}R``\{x\})$, for all $x \in A$, and that F is uniquely determined by this (as a class, not as a class term).

Remark 2.2.6. Since "R is well-founded" is a scheme of formulae, the Recursion Theorem is really formulated in the theory ZF^{--} + "R is well-founded". However, the case where $R = \in$ is a ZF^{--}_F theorem. Also, if $R \in \mathrm{V}$, then the well-foundedness of R can be expressed in a single formula, and hence that version of the theorem is expressible as a ZF^{--} theorem.

Proof. Uniqueness: Let F and F' be two such functions. Suppose they were different. Let $x \in A$ be R-minimal such that $F(x) \neq F'(x)$. Then since both satisfy the equation,

$$F(x) = G(x, F{\restriction}R``\{x\}) = G(x, F'{\restriction}R``\{x\}) = F'(x),$$

since by R-minimality of x, $F{\restriction}R``\{x\} = F'{\restriction}R``\{x\}$. So $F(x) = F'(x)$ after all.

Existence: Let $\mathcal{F}$ be the class consisting of all sets of the form $\langle f, u\rangle$ with:

1. $u \subseteq A$ is R-closed,
2. $f : u \to B$,
3. $\forall x \in u \quad f(x) = G(x, f \restriction R``\{x\})$.

(1) *$\mathcal{F}$ is a function.*

Proof of (1). Suppose $\langle f, u\rangle, \langle f', u\rangle \in \mathcal{F}$. The above proof of uniqueness shows that $f = f'$. Note that here, we did not use that u is R-closed. $\square_{(1)}$

Let $D = \mathrm{dom}(\mathcal{F})$, and write $\mathcal{F}(u)$ for the unique f with $f\mathcal{F}u$.

(2) *If $u \in D$ and $v \subseteq u$ is R-closed, then $v \in D$ and $\mathcal{F}(v) = (\mathcal{F}(u)){\restriction}v$.*

Proof. Letting $f := \mathcal{F}(u)\restriction v$, $\langle f, v\rangle$ clearly satisfies 1.-3. of the definition of $\mathcal{F}$. The claim follows, since $\mathcal{F}$ is a function. Here, it was crucial that v is R-closed (i.e., if we dropped R-closure in condition 1. above, the proof would not go through). Namely, to see $\langle f, v\rangle$ satisfies 3., let $g = \mathcal{F}(u)$. We have that $\langle g, u\rangle$ satisfies 1.-3. It's obvious that $\langle f, v\rangle$ satisfies 1. and 2. For 3., note that if $x \in v$, then $f\restriction R``\{x\} = (g\restriction v)\restriction R``\{x\} = g\restriction R``\{x\}$ because $R``\{x\} \subseteq v$. This is why we have that $f(x) = G(x, f\restriction R``\{x\})$. $\square_{(2)}$

(2') *If $u, v \in D$, then $u \cap v \in D$ and $\mathcal{F}(u)\restriction(u \cap v) = \mathcal{F}(u \cap v) = \mathcal{F}(v)\restriction(u \cap v)$.*

Proof of (2'). By Lemma 2.2.2, $u \cap v$ is R-closed. The claim follows directly from (2). $\square_{(2)}$

Let $X = \bigcup D$, $F := \bigcup\{\mathcal{F}(u) \mid u \in D\}$. So F is a relation with $X = \mathrm{dom}(F)$ and $\mathrm{ran}(F) \subseteq B$.

(3) *If $u \in D$, then $F\restriction u = \mathcal{F}(u)$.*

Proof of (3). By definition of F, $\mathcal{F}(u) \subseteq F$. For the other direction, assume $\langle y, x\rangle \in F\restriction u$, i.e., $x \in u$ and $\langle y, x\rangle \in F$. By definition of F again, there is some $v \in D$ such that $\langle y, x\rangle \in \mathcal{F}(v)$. Note that then, $x \in v$. So $x \in u \cap v$. By (2'), $\mathcal{F}(u \cap v) = \mathcal{F}(u)\restriction(u \cap v) = \mathcal{F}(v)\restriction(u \cap v)$. Hence, $\langle y, x\rangle \in \mathcal{F}(u)$. $\square_{(3)}$

(4) $F : X \longrightarrow B$.

Proof of (4). It has to be shown that F is a function. Suppose $\langle y, x\rangle, \langle z, x\rangle \in F$. Pick $u \in D$ such that $x \in u$. Then $\langle y, x\rangle, \langle z, x\rangle \in F\restriction u = \mathcal{F}(u)$, by (3). The latter is a function, so it follows that $y = z$. $\square_{(4)}$

(5) *For $x \in X$, $F(x) = G(x, F\restriction R``\{x\})$.*

Proof of (5). Let $x \in X$. Pick $u \in D$ such that $x \in u$. Then $F(x) = (F\restriction u)(x) = \mathcal{F}(u)(x) = G(x, \mathcal{F}(u)\restriction R``\{x\})$. But since $R``\{x\} \subseteq u$, as u is R-closed, and since $F\restriction u = \mathcal{F}(u)$, it follows that $F\restriction R``\{x\} = \mathcal{F}(u)\restriction R``\{x\}$. This shows that $F(x) = G(x, F\restriction R``\{x\})$, as wished. $\square_{(5)}$

(6) $X = A$.

Proof of (6). Clearly, $X \subseteq A$. Suppose $X \subsetneqq A$. Pick x R-minimal in $A \setminus X$. So $x \notin X$, but since $R``\{x\} \subseteq A$, $R``\{x\} \subseteq X$ (for if there were a zRx with $z \notin X$, then $z \in A \setminus X$, contradicting R-minimality of x). Let u be the least R-closed set which contains $R``\{x\}$ (with respect to inclusion); this exists by Lemma 2.2.2.3. Since $X$ is $R$-closed (being a union of $R$-closed sets; see Lemma 2.2.2.2), it follows that $u \subseteq X$ (note that $u \cap X$ is an $R$-closed set (by Lemma 2.2.2.2) that contains $R``\{x\}$, so that $u \subseteq u \cap X$, that is, $u \subseteq X$). By (5), it follows that $u \in D$ and that $\mathcal{F}(u) = F\restriction u$. Set:

$$\begin{aligned} v &= u \cup \{x\}, \\ g &= F\restriction u \cup \{\langle G(x, F\restriction R``\{x\}), x\rangle\}. \end{aligned}$$

Then clearly, v is R-closed, and $\langle g, v\rangle \in \mathcal{F}$. So $x \in v \in D$, hence $x \in X$, which is a contradiction, since x was chosen to be R-minimal in $A \setminus X$. This concludes the proof. $\square$

Remark 2.2.7. Looking back at the proof of the Recursion Theorem, one can extract a formula defining F:

$$\begin{aligned} y = F(x) \quad \leftrightarrow \quad (x \in A \wedge \exists f \quad & (\text{"}f \text{ is a function"} \\ & \wedge \text{"dom}(f) \text{ is } R\text{-closed"} \wedge x \in \mathrm{dom}(f) \\ & \wedge \forall z \in \mathrm{dom}(f) \quad f(z) = G(z, f\restriction R``\{z\}) \\ & \wedge y = f(x))) \end{aligned}$$

Definition 2.2.8. T is *transitive* if

$$\forall x \forall y \quad ((y \in T \wedge x \in y) \rightarrow x \in T).$$

Definition 2.2.9. Let $R \subseteq U \times U$. Then (U, R) is *extensional* if for every $y, z \in U$,

$$R``\{y\} = R``\{z\} \rightarrow y = z.$$

So this means that members of U are uniquely determined by their R-predecessors. (U, R) is (strongly) well-founded if R is.

So for example, $(\mathrm{V}, \in)$ is extensional, and assuming Foundation, it is strongly well-founded.

Definition 2.2.10. If (U, R), (V, S) are such that $R \subseteq U^2$ and $S \subseteq V^2$, then $F : (U, R) \overset{\sim}{\longleftrightarrow} (V, S)$ means:

1. $F : U \rightarrowtail\!\!\!\!\twoheadrightarrow V$,
2. $\forall x \forall y \quad (xRy \leftrightarrow F(x) S F(y)$.

For sets $\langle u, r\rangle$ and $\langle v, s\rangle$, saying that $\langle u, r\rangle \cong \langle v, s\rangle$ means that there is an f such that $f : (u, r) \overset{\sim}{\longleftrightarrow} (v, s)$.

Theorem 2.2.11 (Mostowski's Isomorphism Theorem)**.** *Suppose (U, R) is extensional and strongly well-founded. Then there are uniquely determined F, V such that*

$$F : (U, R) \overset{\sim}{\longleftrightarrow} (V, \in \upharpoonright V)$$

and V is transitive. F satisfies the following equation, for all $x \in U$:

($*$) $F(x) = F``R``\{x\} = \{F(y) \mid yRx\}$.

Proof. Existence: By the Recursion Theorem, there exists a unique function F satisfying ($*$) - use the function $G : U \times \mathrm{V} \longrightarrow \mathrm{V}$ defined by

$$G(x, f) = \begin{cases} \mathrm{ran}(f) & \text{if } f \text{ is a function,} \\ \emptyset & \text{otherwise.} \end{cases}$$

Set $V = F``U$. It suffices to show that (F, V) is as wished.

(1) *V is transitive.*

Proof of (1). Let $x \in y \in V = F``U$. Let $\bar{y} \in U$ be such that $y = F(\bar{y})$. By ($*$), $F(\bar{y}) = \{F(\bar{x}) \mid \bar{x} R \bar{y}\}$, so since $x \in F(\bar{y})$, there is some $\bar{x} R \bar{y}$ such that $x = F(\bar{x})$. In particular, $x \in F``U$, showing that V is transitive. $\square_{(1)}$

(2) *$xRy \rightarrow F(x) \in F(y)$.*

Proof of (2). By ($*$). $\square_{(2)}$

(3) *$F : U \rightarrowtail\!\!\!\!\twoheadrightarrow V$.*

Proof of (3). F is surjective, by definition. Suppose it was not injective. Then pick $x \in U$ $\in$-minimal such that there is a $y \in U$ with $y \neq x$, such that $F(x) = F(y)$. Let y witness this, i.e., $x \neq y$, $F(x) = F(y)$. I'll show:

$$R``\{x\} = R``\{y\},$$

which is a contradiction, since this would imply that $x = y$, by extensionality of (U, R).

For the direction from left to right, let zRx. Then $F(z) \in F(x) = F(y) = F``R``\{y\}$. So there is $z'Ry$ such that $F(z) = F(z')$. Supposing $\neg zRy$, it follows that $z \neq z'$, since $z'Ry$. So we have zRx, and there is a w with $z \neq w$ and $F(z) = F(w)$, namely $w := z'$. This contradicts the R-minimality of x with this property.

The converse is entirely analogous: Let zRy. Then $F(z) \in F(y) = F(x) = F``R``\{x\}$, so there is a $z'Rx$ such that $F(z') = F(z)$. Suppose $\neg zRx$. Since $z'Rx$, this implies that $z \neq z'$. So we have: $z'Rx$, and there is a w (as witnessed by z) such that $z' \neq w$ and $F(z') = F(w)$. This again contradicts the R-minimality of x. $\Box_{(3)}$

(4) $F(x) \in F(y) \to xRy$

Proof of (4). Let $F(x) \in F(y)$. Since $F(y) = F``R``\{y\}$, there is $x'Ry$ such that $F(x) = F(x')$. But since F is injective, $x' = x$. So xRy. $\Box_{(4)}$

This finishes the proof of existence.

Turning to *uniqueness*: By the Recursion theorem, there is only one F satisfying $(*)$. So it suffices to show:

(5) *If W is transitive and $G : (U, R) \overset{\sim}{\longleftrightarrow} (W, \in \restriction W)$, then for all $u \in U$, $G(u) = \{G(\bar{u}) \mid \bar{u}Ru\}$.*

Proof of (5). Fix $u \in U$. If vRu, then $G(v) \in G(u)$, since G is R-preserving, so this shows that $\{G(\bar{u}) \mid \bar{u}Ru\} \subseteq G(u)$. For the opposite direction, let $v \in G(u)$. So $v \in G(u) \in W$, which by transitivity of W implies that $v \in W$. So v has a pre-image under G, as G is onto. So let $\bar{u} \in U$ be such that $v = G(\bar{u})$. Since $G(\bar{u}) \in G(u)$, it follows that $\bar{u}Ru$. So $v = G(\bar{u})$, where $\bar{u}Ru$, which shows that $G(u) \subseteq G``R``\{u\}$, as wished. $\Box_{(5)}$

This finishes the proof. $\Box$

2.3 Ordinal Numbers and Infinity

2.3.1 Well-orders

Definition 2.3.1 (Linear orders)**.** If $R \subseteq U^2$, then (U, R) is a (strict) *linear order* if for all $x, y, z \in U$:

1. $\neg(xRx)$ (irreflexivity),

2. $xRyRz \to xRz$ (transitivity),

3. $xRy \lor x = y \lor yRx$ (connectedness).

While we're at it, I'll call a class U *connected* if $(U, \in \cap U^2)$ is connected. This means that for all $x, y \in U$, either $x = y$, $x \in y$, or $y \in x$.

Observation 2.3.2. *Iff (U, R) is linear, then it is extensional.*

Proof. Let $x, y \in U$ have the same R-predecessors. Suppose $x \neq y$. Then xRy or yRx. In the first case, it follows that xRx, contradicting irreflexivity, and in the second it follows that yRy, again contradicting irreflexivity. □

In principle, the same issue that we encountered previously regarding the expressibility of the well-foundedness of a structure arises again with linear orders. However, there is a simple way around it, as follows.

Definition 2.3.3. A relation R is well-founded with respect to sets if every nonempty *set* has an R-minimal element.

In general, this is a weaker notion than full well-foundedness. However, in the context of set-like linear orders, or more generally, of set-like transitive orders, there is no difference, as we shall see below.

Definition 2.3.4. A linear order (U, R) is a *well-order* if R is well-founded. It is a *strong well-order* if R is set-like and well-founded with respect to sets.

The apparent asymmetry in the definition is justified as follows.

Lemma 2.3.5. *Suppose $R \subseteq \mathrm{V}^2$ is set-like and transitive (meaning that if xRy and yRz, then xRz), and that R is well-founded with respect to sets. Let A be a class. If $A \neq \emptyset$, then A has an R-minimal element.*

Proof. In the situation of the lemma, let $a \in A$. If a is R-minimal in A, then we are done. Otherwise, consider the set $b = \{x \mid xRa\} \cap A$. This is a set, since R is set-like, and by Separation. Thus, since R is well-founded with respect to sets, there is a $c \in b$ that's R-minimal in b. It follows that c is R-minimal in A, because if there were a $d \in A$ with dRc, then by transitivity of R, it would follow that dRa, since dRc and cRa (as $c \in b$), and hence that $d \in b$. But c is R-minimal in b, so this cannot be. □

Thus, if R is a set-like, transitive relation that's well-founded with respect to sets, then provably in ZF^{--} every instance of the scheme "R is well-founded" holds. In particular, this is the case if (U, R) is a strong well-order.

So, by Observation 2.3.2 and Lemma 2.3.5, the following definition makes sense:

Definition 2.3.6. If (U, R) is a strong well-order, then let $\mathrm{otp}(U, R)$, the order-type of (U, R), be the uniquely determined transitive class Γ such that $(\Gamma, \in\restriction\Gamma) \cong (U, R)$ (by Mostowski's Isomorphism Theorem).

The natural numbers $(\mathbb{N}, <)$ form a well-order. What are the natural numbers? This is a somewhat philosophical question, but if they exist, then since they form a strong well-order, they have an order-type, $\mathrm{otp}(\mathbb{N}, <)$. It is this transitive class that we consider to be the class of natural numbers. The infinity axiom says that it is a set. I will shortly introduce this axiom more formally.

2.3.2 Ordinals

It would be natural to assume the Foundation Axiom for the development of the theory of the ordinals, but it is not necessary to do so, and it seems worthwhile to do without it. So the system I work in for this subsection is ZF^{--}. I give some proofs in these notes that I omit in the lecture.

Definition 2.3.7. $\mathrm{On} = \{\mathrm{otp}(s) \mid s \text{ is a well-order}\}$. On is the class of *ordinal numbers*.

So the class of ordinal numbers is the collection of order-types of set-sized well-orders.

Lemma 2.3.8 (Counting Lemma). *Let $S = (U, R)$ be a strong well-order. Let $\Gamma = \mathrm{otp}(S)$, and let $F : S \overset{\sim}{\longleftrightarrow} (\Gamma, \in\restriction\Gamma)$ be the collapse. Then $(\Gamma, \in\restriction\Gamma)$ is a strong well-order. Moreover, if $x \in U$, then, letting $u_x = R``\{x\}$, it follows that*

$$F\restriction u_x : \langle u_x, R\restriction u_x\rangle \overset{\sim}{\longleftrightarrow} \langle F(x), \in\restriction F(x)\rangle$$

is the Mostowski collapse of the well-order $\langle u_x, R\restriction u_x\rangle$. In particular, $F(x) \in \mathrm{On}$.

Note that if we assume that $S \in \mathrm{V}$, then this lemma can be expressed in ZF^{--}, while otherwise, we really have to work in ZF^{--} + "S is a strong well-order".

Proof. It is obvious that $\langle\Gamma, \in\restriction\Gamma\rangle$ is a strong well-order, being isomorphic to one. Fix $x \in U$. It is easily checked that, letting $r_x = R\restriction u_x$, $\langle u_x, R\restriction u_x\rangle$ is a (strong) well-order. I claim that for $y \in u_x$, $F(y) = \{F(z) \mid z r_x y\}$. Since F is the Mostowski-isomorphism of (U, R), we know that $F(y) = \{F(z) \mid zRy\}$. So it suffices to see that $R``\{y\} = r_x``\{y\}$. The direction from right to left is trivial, so suppose zRy. Since $r_x = R\restriction R``\{x\}$, to see that $z r_x y$, we only need to know that yRx, but we do know that, since $y \in u_x$. By the way, the reader is invited to check that $R\restriction u_x = R \cap (u_x)^2$. In any case, $F\restriction u_x$ satisfies the definition of the Mostowski collapse of $\langle u_x, r_x\rangle$, and hence it *is* the collapse. By definition, $F(x) = F``R``\{x\} = F``u_x$, which completes the proof. □

In the future, α, β, ... will be reserved for ordinals.

Corollary 2.3.9. *If S is a strong well-order, then* $\mathrm{otp}(S)$ *is a transitive subclass of* On.

Corollary 2.3.10. On *is transitive.*

Proof. If $\beta \in \mathrm{On}$, then $\beta = \mathrm{otp}(s)$, for some well-order s, and by the previous corollary, $\mathrm{otp}(s) \subseteq \mathrm{On}$. □

In the absence of the axiom of $\mathsf{Foundation}$, the following definition is not vacuous.

Definition 2.3.11. A transitive class U is well-founded (with respect to sets) if every nonempty set $a \subseteq U$ has an $\in$-minimal element.

Lemma 2.3.12. *Let U be transitive and well-founded (with respect to sets). Then:*

1. *U is connected iff $(U, \in\restriction U)$ is a strong well-order.*
2. *If U is connected, then $U = \mathrm{otp}(U, \in\restriction U)$.*

Proof. If U is connected, then it follows that $(U, \in\restriction U)$ is a set-like linear order that's well-founded with respect to sets, which means that it is a strong well-order. The rest is clear. □

Corollary 2.3.13.

$$\mathrm{On} = \{x \mid x \textit{ is transitive, connected and well-founded}\}.$$

Note that if we assume $\mathsf{Foundation}$, then every transitive set is well-founded, so in ZF^{--}_F, it follows that $\mathrm{On} = \{x \mid x \text{ is transitive and connected}\}$.

Corollary 2.3.14. *If Γ is transitive, connected and well-founded, then $\Gamma \subseteq \mathrm{On}$. Again, assuming* $\mathsf{Foundation}$*, well-foundedness is vacuous.*

Proof. $(\Gamma, \in\restriction\Gamma)$ is a strong well-order, and $\Gamma = \mathrm{otp}(\Gamma, \in\restriction\Gamma) \subseteq \mathrm{On}$. □

Lemma 2.3.15. *Let Γ be transitive, connected and well-founded. Let U be transitive with $U \subseteq \Gamma$. Then either $U = \Gamma$ or $U \in \Gamma$.*

Proof. Assume that $U \neq \Gamma$, so that $U \subsetneqq \Gamma$. Since $(\Gamma, \in \restriction\Gamma)$ is a well-order, it follows that Γ is well-founded with respect to classes, by Lemma 2.3.5. So we can let α be $\in$-minimal in $\Gamma \setminus U$. I claim that $\alpha = U$ (at which point the proof is complete, because then $U = \alpha \in \Gamma$).

(1) $U \subseteq \alpha$.

Proof of (1). Let $\gamma \in U$. Since $U \subseteq \Gamma$, $\gamma \in \Gamma$. Since $\alpha \in \Gamma$ too, and since Γ is connected, one of the following must be true: $\gamma \in \alpha$, $\alpha \in \gamma$, or $\alpha = \gamma$. It cannot be the case that $\alpha \in \gamma$, since otherwise $\alpha \in \gamma \in U$, so $\alpha \in U$. It can't be that $\alpha = \gamma$ either, since $\alpha \notin U$, while $\gamma \in U$. So the only possibility is that $\gamma \in \alpha$. $\square_{(1)}$

(2) $\alpha \subseteq U$.

Proof of (2). α is $\in$-minimal in $\Gamma \setminus U$. So if $\gamma \in \alpha$, then it can't be that $\gamma \in \Gamma \setminus U$. But since Γ is transitive, $\gamma \in \Gamma$. So it must be that $\gamma \in U$, or else γ would be in $\Gamma \setminus U$. $\square_{(2)}$

So $U = \alpha \in \Gamma$. $\square$

Definition 2.3.16. For ordinals α, β, set

$$\begin{aligned} \alpha < \beta &\iff \alpha \in \beta \\ \alpha \leq \beta &\iff \alpha < \beta \vee \alpha = \beta. \end{aligned}$$

Corollary 2.3.17. *$\alpha \leq \beta \iff \alpha \subseteq \beta$.*

Proof. $\boxed{\Longrightarrow}$ $\alpha \in \beta \implies \alpha \subseteq \beta$, as β is transitive, and $\alpha = \beta$ trivially implies $\alpha \subseteq \beta$.

$\boxed{\Longleftarrow}$ β is transitive, connected and well-founded, so that the previous lemma applies. $\square$

Lemma 2.3.18. *If α and β are ordinals, then $\alpha \leq \beta$ or $\beta \leq \alpha$.*

Proof. If not, then $\alpha \not\subseteq \beta$ and $\beta \not\subseteq \alpha$. This means that

$$\alpha \cap \beta \subsetneqq \alpha \text{ and } \alpha \cap \beta \subsetneqq \beta.$$

But $\alpha \cap \beta$ is transitive (being transitive is the same as being $\in$-closed, and the intersection of R-closed sets is R-closed, for any binary relation). So again, by Lemma 2.3.15, $\alpha \cap \beta \in \alpha$, and also $\alpha \cap \beta \in \beta$. So $\alpha \cap \beta \in \alpha \cap \beta$. But α is well-founded, while $\{\alpha \cap \beta\} \subseteq \alpha$ has no $\in$-minimal element, a contradiction. $\square$

Lemma 2.3.19. $(\mathrm{On}, <)$ *is a strong well-order, and* $\mathrm{otp}(\mathrm{On}, <) = \mathrm{On}$.

Proof. By the previous lemma, $(\mathrm{On}, <)$ is connected, and we've known for a while that On is transitive. Since $< = \in\restriction\mathrm{On}$, we also know that it is set-like. We can show directly show that $(\mathrm{On}, <)$ is well-founded (which of course implies that it is well-founded with respect to sets, and hence that it is a strong well-order). So let $\emptyset \neq A \subseteq \mathrm{On}$. Pick $\alpha \in A$. If α is $<$-minimal in A, we are done. Otherwise, consider $a = A \cap \alpha$. This is a nonempty subset of α, and α is well-founded, being an ordinal. Pick β $\in$-minimal in a. Then β is $<$-minimal in A: If $\gamma < \beta$, then $\gamma \notin a$, because $\gamma \in \alpha$. So $\gamma \notin A$, or else $\gamma \in A \cap \alpha = a$. The second part follows since On is transitive. $\square$

Corollary 2.3.20. $\mathrm{On} \notin \mathrm{V}$.

Proof. Otherwise $\mathrm{On} = \mathrm{otp}(\mathrm{On}, <) \in \mathrm{On}$, but then $\{\mathrm{On}\} \subseteq \mathrm{On}$ has no $<$-minimal element, contradicting that $(\mathrm{On}, <)$ is a well-order. $\square$

Corollary 2.3.21. *Let S be a strong well-order. Then* $\mathrm{otp}(S) \in \mathrm{On}$ *or* $\mathrm{otp}(S) = \mathrm{On}$. *So, writing* ∞ *for* On *and expanding the meaning of* $<, \leq$ *in the obvious way,* $\mathrm{otp}(S) \leq \infty$.

Proof. We know already that $\mathrm{otp}(S) \subseteq \mathrm{On}$. So if $\mathrm{otp}(S) \neq \mathrm{On}$, then $\mathrm{otp}(S) \in \mathrm{On}$, as On is strongly well-founded, transitive and connected, and since $\mathrm{otp}(S)$ is transitive – see Lemma 2.3.15. □

Lemma 2.3.22. *Let $A \subseteq \Delta \leq \infty$. Then $(A, < \restriction A)$ is a strong well-order. Letting $F : (A, < \restriction A) \longrightarrow \Gamma$ be its collapse, it follows that for all $\alpha \in A$, $F(\alpha) \leq \alpha$, and that $\Gamma \leq \Delta$. Hence the name* collapse.

Proof. $(A, < \restriction A)$ is a strong well-order: It is set-like by Separation, and it is a well-order, because $(\mathrm{On}, <)$ is.

Turning to the main claim: If not, let α be the minimal counterexample in $(A, < \restriction A)$. By definition, $F(\alpha) = \{F(\beta) \mid \beta \in A \cap \alpha\} \in \mathrm{On}$. By assumption, $\alpha \in F(\alpha)$. So let $\beta \in A \cap \alpha$ be such that $\alpha = F(\beta)$. Then $\beta < \alpha$, and β is also a counterexample, contradicting the minimality of α.

Finally, it follows that $\Gamma \leq \Delta$: If not, then $\Delta \in \Gamma = \mathrm{ran}(F)$. Let $\alpha \in A$ be s.t. $F(\alpha) = \Delta$. Then $\Delta = F(\alpha) \leq \alpha < \Delta$, contradicting Δ's well-foundedness. □

Definition 2.3.23. $s\alpha = \alpha \cup \{\alpha\}$.

I shall often write $\alpha + 1$ instead of $s\alpha$.

Lemma 2.3.24.

1. $\emptyset \in \mathrm{On}$.
2. $s\alpha \in \mathrm{On}$.
3. $\alpha \leq \beta \iff \alpha < s\beta$.
4. $\alpha < \beta \iff s\alpha \leq \beta$.

Proof. For 4.:

$$\alpha < \beta \iff \alpha \in \beta \iff \alpha \cup \{\alpha\} \subseteq \beta \iff s\alpha \leq \beta.$$

□

Corollary 2.3.25. $s\alpha = \min\{\nu \mid \nu > \alpha\}$.

Proof. Clearly, $\alpha \in \alpha \cup \{\alpha\} = s\alpha$, which shows "$\geq$". Vice versa, if $\beta < s\alpha$, then $\beta \leq \alpha$, so that $\beta \not> \alpha$ (or else $\alpha \in \beta \subseteq \alpha$, contradicting the well-foundedness of On). □

Lemma 2.3.26. *Let $A \subseteq \mathrm{On}$. Then $\bigcup A \leq \infty$, and $\bigcup A$ is the supremum of A, that is, if A is bounded in* On*, then $\bigcup A$ is the least β such that for every $\alpha \in A$, $\alpha \leq \beta$, and if A is unbounded in* On*, then $\bigcup A = \infty$.*

Proof. Since every member of A is transitive, so is $\bigcup A$. Moreover, $\bigcup A \subseteq \mathrm{On}$, since if $\gamma \in \bigcup A$, then $\gamma \in \alpha$, for some $\alpha \in A$, and then $\alpha \subseteq \mathrm{On}$, and so, $\gamma \in \mathrm{On}$. This implies that either $\bigcup A = \mathrm{On}$ or $\bigcup A \in \mathrm{On}$, by Lemma 2.3.15.

Now, if $\alpha \in A$, then $\alpha \leq \bigcup A$, because the latter just means that $\alpha \subseteq \bigcup A$. And if $\Gamma \leq \infty$ is such that for every $\alpha \in A$, $\alpha \leq \Gamma$, then this just means that for every $\alpha \in A$, $\alpha \subseteq \Gamma$, which is the same as to say that $\bigcup A \subseteq \Gamma$. This shows that $\bigcup A$ is the supremum of A.

Finally, if A is unbounded in On, then for every β, there is an $\alpha \in A$ such that $\beta \in \alpha$, and so, $\mathrm{On} \subseteq \bigcup A \subseteq \mathrm{On}$, so $\bigcup A = \infty$, and if A is bounded in On, say $A \subseteq \beta$, then A is a set by Separation, and so, $\bigcup A$ is a set as well, by Union, so $\bigcup A \neq \mathrm{On}$, by Corollary 2.3.20, so $\bigcup A \in \mathrm{On}$. ☐

Definition 2.3.27. Let α be an ordinal. α is a *successor ordinal* if $\alpha = s\beta$, for some β. α is a limit ordinal if $\alpha \neq 0$ and α is not a successor ordinal.

Thus, a successor ordinal is a nonzero ordinal α such that whenever $\beta < \alpha$, $s\beta < \alpha$ as well. From the axioms we have introduced thus far, one cannot show that there is a limit ordinal. We will introduce the axiom needed in the next section.

2.3.3 The Natural Numbers

Definition 2.3.28.

$$\omega = \mathrm{On} \cap \bigcap \{\alpha \in \mathrm{On} \mid 0 \in \alpha \wedge \forall \beta < \alpha \quad s\beta \in \alpha\}.$$

ω is the class of natural numbers. We write m, n, ... for members of ω.

So ω is the least class (wrt. inclusion) that's transitive, well-founded, connected, closed under $x \mapsto sx$ and that contains $\emptyset$ as a member, since it is the intersection of all such classes. It follows that either $\omega = \mathrm{On}$, or $\omega \in \mathrm{On}$.

Definition 2.3.29. The axiom of infinity (Infinity) says: $\omega \in \mathrm{V}$.

This axiom is equivalent to saying that there is a limit ordinal. We'll not assume this axiom for now. So we continue working in ZF^{--}.

Lemma 2.3.30.

1. $\emptyset \in \omega$.
2. $n \in \omega \implies sn \in \omega$.

Definition 2.3.31. $0 := \emptyset$, $1 := s0$, $2 := s1$, ...

Lemma 2.3.32. *If $n \in \omega$, then either $n = 0$, or there is an $m \in n$ with $sm = n$.*

Proof. If not, then picking a least counterexample gives an s-closed member of ω which contains 0, contradicting the minimality of ω. ☐

Lemma 2.3.33 (Induction Scheme)**.** *If $A \subseteq \omega$ satisfies:*

1. $0 \in A$,
2. $\forall n \in A \quad sn \in A$,

then $A = \omega$.

Proof. Otherwise, let $n = \min(\omega \setminus A)$. Since $0 \in A$, $n \neq 0$. $n = sm$, for some m. Then $m < n$, so that $m \in A$, by minimality of n. But then, by 2., $n = sm \in A$ after all. ☐

So ω is the smallest class which contains 0 and is s-closed. For if X is such a class, then $X \cap \omega = \omega$, by induction.

There are simple versions of the recursion theorem for ω, which can be used to define the usual arithmetical operations on the natural numbers. This will be done in the exercises.

Definition 2.3.34. Say that x and y are equinumerous iff there is an bijection $f : x \rightarrowtail\!\!\!\!\rightarrow y$. We'll write $x \sim y$ for this relation.

Lemma 2.3.35. *$\sim$ is an equivalence relation.*

Definition 2.3.36. x is finite iff there is an $n \in \omega$ with $x \sim n$.

Lemma 2.3.37. *If $m < n < \omega$, then $m \not\sim n$. Hence, if x is finite, then there is a unique n with $x \sim n$.*

Proof. If not, let $m \in \omega$ be least such that there is an $n > m$ with $m \sim n$. Clearly, $m, n \neq 0$. Let $m = s\bar{m}$, $n = s\bar{n}$. Let $f : m \rightarrowtail\!\!\!\!\rightarrow n$.

Case 1: $f(\bar{m}) = \bar{n}$.

Then $f{\restriction}\bar{m} : \bar{m} \rightarrowtail\!\!\!\!\rightarrow \bar{n}$, contradicting the minimality of m.

Case 2: $f(\bar{m}) < \bar{n}$.

Then let $f(k) = \bar{n}$. Define $g : \bar{m} \to \bar{n}$ by:

$$g(l) = \begin{cases} f(l) & \text{if } l \neq k, \\ f(\bar{m}) & \text{if } l = k. \end{cases}$$

Clearly, $g : \bar{m} \rightarrowtail\!\!\!\!\rightarrow \bar{n}$, contradicting the minimality of m. □

Definition 2.3.38. For a finite set x, let $\overline{\overline{x}}$, the cardinality of x, be the uniquely determined $n < \omega$ with $x \sim n$.

Lemma 2.3.39. *Let $u \subseteq n < \omega$. Then $\mathrm{otp}(\langle u, <{\restriction}u\rangle) \leq n$. In particular, u is finite. If $u \subsetneqq n$, then $\mathrm{otp}(\langle u, <{\restriction}u\rangle) < n$.*

Proof. The first part of the lemma we know already: It's Lemma 2.3.22. For the second part, assume the contrary. Let n be minimal such that there is a counterexample u. Then $n = sm$. It follows that $m \in u$, for otherwise $u \subseteq m$, and we already know that then $\mathrm{otp}(\langle u, < {\restriction}u\rangle) \leq m$. But then, $u \cap m \subsetneqq m$. By minimality of n, it follows that $p = \mathrm{otp}(\langle u \cap m, <\rangle) < m$. Let F be the Mostowski collapse of $\langle u \cap m, <\rangle$. By the Counting Lemma, $F = G{\restriction}(u \cap m)$, where G is the collapse of $\langle u, <\rangle$. So $G(m) = \{F(j) \mid j \in u \cap m\} = p$, so that $\mathrm{otp}(\langle u, <\rangle) = sp$. But since $p < m$, it follows that $sp < n$, so that u wasn't a counterexample after all. □

Lemma 2.3.40. *If v is finite and $u \subseteq v$, then u is finite, too. If moreover $u \subsetneqq v$, then $\overline{\overline{u}} < \overline{\overline{v}}$.*

Proof. For the first part, let $f : v \rightarrowtail\!\!\!\!\rightarrow n$, where $n = \overline{\overline{v}} \in \omega$. Let $u' = f``u \subseteq n$. Then $s = \langle u', \in \cap (u')^2\rangle$ is a well-order. Let $g : s \stackrel{\sim}{\longleftrightarrow} \mathrm{otp}(s)$ be its collapse. Then $\mathrm{otp}(s) \leq n \in \omega$. So $g \circ f{\restriction}u : u \rightarrowtail\!\!\!\!\rightarrow \mathrm{otp}(s) \in \omega$, proving that u is finite.

For the second part: $u' \subsetneqq n$. So $m = \mathrm{otp}(\langle u', <{\restriction}u'\rangle) < n$. In particular, $\overline{\overline{u'}} = m$. □

Corollary 2.3.41. *A set $a \subseteq \omega$ is finite if and only if it is bounded in ω, i.e., if there is an $n \in \omega$ with $a \subseteq n$. Also, in that case, $\overline{\overline{a}} = \mathrm{otp}(\langle a, \in{\restriction}a\rangle)$.*

Proof. Clearly, if $a \subseteq n$, then $\mathrm{otp}(\langle a, <\rangle) \leq n$, and so $\overline{\overline{a}} \leq n$, showing that a is finite. It also follows that $\mathrm{otp}(\langle a, <\rangle) = \overline{\overline{a}}$. This is because the collapse of $\langle a, <\rangle$ is a bijection between a and $\mathrm{otp}(\langle a, <\rangle)$, which is a natural number (at most n).

Vice versa, assume that a is finite but unbounded in ω. Pick such an a of minimal cardinality $n \in \omega$. Let $f : a \rightarrowtail\!\!\!\!\rightarrow n \in \omega$, $n = m + 1$. Let $a' = f^{-1}``m$. Then $a' = a \setminus \{f^{-}1(m)\}$, and $f{\restriction}a' : a' \rightarrowtail\!\!\!\!\rightarrow m$. By minimality of $\overline{\overline{a}}$, it follows that a' is bounded, say by $p \in \omega$. But then a is bounded by $p \cup s(f^{-1}(m)) \in \omega$. □

Lemma 2.3.42. *If u is finite and $f : u \twoheadrightarrow v$, then v is finite, and $\overline{\overline{v}} \leq \overline{\overline{u}}$.*

Proof. Let $g : u \rightarrowtail\!\!\!\!\twoheadrightarrow n = \overline{\overline{u}}$. Then g induces a well-order $<^*$ on u, defined by $x <^* y \iff g(x) \in g(y)$. Define $h : v \rightarrowtail\!\!\!\!\twoheadrightarrow u' \subseteq u$ by letting $h(m) = \min_{\langle u,<^*\rangle}(\{l \in u \mid f(l) = m\})$. Then $g \circ h : v \rightarrowtail\!\!\!\!\twoheadrightarrow a \subseteq n$. Letting $k : \langle a, <\rangle \overset{\sim}{\longleftrightarrow} \langle l, <\rangle$ be the collapse, it follows that $l \leq n$, so that $k \circ g \circ h : v \rightarrowtail\!\!\!\!\twoheadrightarrow l \leq n$, showing that $\overline{\overline{v}} \leq \overline{\overline{u}}$. □

Another way to put the previous Lemma is to say that the finite sets satisfy Replacement.

Using the recursion theorem, one can define extensions of the usual arithmetic operations, addition and multiplication and exponentiation on the ordinal numbers, as follows.

Definition 2.3.43. There are class terms P, T, E defining functions from On^2 to On such that, writing $\alpha + \beta, \alpha \cdot \beta, \alpha^\beta$ for $P(\alpha, \beta), T(\alpha, \beta), E(\alpha, \beta)$, respectively, the following hold for ordinals α, β and limit ordinals λ:

- $\alpha + 0 = \alpha$, $\alpha + s\beta = s(\alpha + \beta)$, $\alpha + \lambda = \bigcup\{\alpha + \beta \mid \beta < \lambda\}$
- $\alpha \cdot 0 = 0$, $\alpha \cdot s\beta = \alpha \cdot \beta + \alpha$, $\alpha \cdot \lambda = \bigcup\{\alpha \cdot \beta \mid \beta < \lambda\}$,
- $\alpha^0 = 1$, $\alpha^{s\beta} = \alpha^\beta \cdot \alpha$, $\alpha^\lambda = \bigcup\{\alpha^\beta \mid \beta < \lambda\}$.

Lemma 2.3.44. *Let u and v be finite sets.*

1. *If u and v are disjoint sets, then $\overline{\overline{u \cup v}} = \overline{\overline{u}} + \overline{\overline{v}}$.*
2. *$\overline{\overline{u \times v}} = \overline{\overline{u}} \cdot \overline{\overline{v}}$.*
3. *If u is finite, then $\overline{\overline{\mathcal{P}(u)}} = 2^{\overline{\overline{u}}}$.*

Proof. 1.) By induction on n, show: If u is finite, $\overline{\overline{v}} = n$ and $u \cap v = \emptyset$, then $\overline{\overline{u \cup v}} = \overline{\overline{u}} + \overline{\overline{v}}$. For this, use the fact that $+$ is defined correctly, i.e., that $p + (sq) = s(p + q)$.

2.) By induction on n, show: If u is finite and v is finite with $\overline{\overline{v}} = n$, then $\overline{\overline{u \times v}} = \overline{\overline{u}} \cdot \overline{\overline{v}}$. Again, use that $p \cdot (sq) = (p \cdot q) + p$.

3.) By induction on n, show: If u is finite with $\overline{\overline{u}} = n$, then $\overline{\overline{\mathcal{P}(u)}} = 2^{\overline{\overline{u}}}$. □

Corollary 2.3.45. *If u is finite, then $\mathcal{P}(u) \in \mathrm{V}$.*

So the finite sets satisfy Power Set also. We can define recursively:

Definition 2.3.46.

$$\begin{aligned} \mathrm{V}_0 &= \emptyset, \\ \mathrm{V}_{n+1} &= \mathcal{P}(\mathrm{V}_n), \\ \mathrm{V}_\omega &= \bigcup_{n<\omega} \mathrm{V}_n. \end{aligned}$$

Lemma 2.3.47.

1. *V_n is a finite, transitive set.*
2. *$m < n \implies \mathrm{V}_m \in \mathrm{V}_n$.*
3. *$\mathrm{V}_n \cap \omega = n$.*
4. *Every $x \in \mathrm{V}_\omega$ is finite.*
5. *If $u \subseteq \mathrm{V}_\omega$ is finite, then $u \in \mathrm{V}_\omega$.*

Proof. 1.-3. are shown by simultaneous induction on n, and 4. follows easily. To see 5., let $u \subseteq \mathrm{V}_\omega$ be finite. Define $F : u \longrightarrow \omega$ by letting $F(x)$ be the least n with $x \in \mathrm{V}_n$. Let $a = \mathrm{ran}(F)$. So $a \in \mathrm{V}$, and actually, $F \in \mathrm{V}$. Since $F : u \twoheadrightarrow a$ and u is finite, so is a. So a is a finite set of natural numbers, hence a is bounded. Let n be such that $a \subseteq n$. Then $u \subseteq \mathrm{V}_n$, which means that $u \in \mathrm{V}_{n+1} \subseteq \mathrm{V}_\omega$. □

The following lemma uses the Foundation axiom.

Lemma 2.3.48 (ZF_F^{--})**.** *The following are equivalent:*

1. Infinity,
2. *There is a set which is not finite,*
3. $\mathrm{V} \neq \mathrm{V}_\omega$.

Proof. 1. $\Longrightarrow$ 2.: $\omega \in \mathrm{V}$ is not finite, or else it would be bounded in itself.
2. $\Longrightarrow$ 3.: Every member of V_ω is finite.
3. $\Longrightarrow$ 1.: Let x be $\in$-minimal in $\mathrm{V} \setminus \mathrm{V}_\omega$. Then $x \subseteq \mathrm{V}_\omega$. As before, let $F : x \longrightarrow \omega$ be defined by letting $F(y)$ be the least n such that $y \in \mathrm{V}_n$. Let $a = \mathrm{ran}(F) \in \mathrm{V}$. Then a must be unbounded in ω, or else $x \in \mathrm{V}_\omega$ would follow. So $\bigcup a = \omega$. □

2.3.4 Foundation

A lot can be said without the Foundation axiom. First, I want to extend the V_n hierarchy transfinitely, for which I will have to assume the Power Set axiom.

Definition 2.3.49 (ZF^{--}+Power Set)**.** The sequence $\langle \mathrm{V}_\alpha \mid \alpha \in \mathrm{On}\rangle$ is defined as follows:

- $\mathrm{V}_0 = \emptyset$,
- $\mathrm{V}_{\alpha+1} = \mathcal{P}(\mathrm{V}_\alpha)$,
- $\mathrm{V}_\lambda = \bigcup_{\alpha<\lambda} \mathrm{V}_\alpha$ if λ is a limit ordinal.

Define $\mathrm{V}_\infty = \bigcup_{\alpha<\infty} \mathrm{V}_\alpha$.

Some of Lemma 2.3.47 carries over to the transfinite hierarchy.

Lemma 2.3.50.

1. V_α *is a transitive set.*
2. $\alpha < \beta \implies \mathrm{V}_\alpha \in \mathrm{V}_\beta$.
3. $\mathrm{V}_\alpha \cap \mathrm{On} = \alpha$.

What can be said about V_∞? It turns out that this question is closely related to well-foundedness. We have previously defined a transitive class A to be well-founded (wrt. sets) if every nonempty set $a \subseteq A$ has an $\in$-minimal element. I'll now extend this definition to transitive sets.

Definition 2.3.51. A set x is well-founded if there is a transitive set y such that $x \subseteq y$ and y is well-founded in the previously defined sense, i.e., every nonempty subset of y has an $\in$-minimal element. Let WF be the class of well-founded sets.

Lemma 2.3.52.

1. WF *is transitive.*

2. *If* $a \in \mathsf{WF}$*, then* $\{a\} \in \mathsf{WF}$*.*

Proof. For (1), let $b \in a \in \mathsf{WF}$. Let t witness that $a \in \mathsf{WF}$, that is, $a \subseteq t$, t transitive and well-founded. Then $b \in a \subseteq t$, so $b \in t$, so $b \subseteq t$, as t is transitive. So t witnesses that $b \in \mathsf{WF}$.

For (2), let $a \in \mathsf{WF}$, and let t witness this, that is, t is transitive, well-founded and $a \subseteq t$. Let $t' = t \cup \{a\}$. Then t' is easily seen to be transitive, because if $x \in y \in t \cup \{a\}$, then either $y \in t$, in which case $x \in t$ by transitivity of t, or $y = a$, in which case $x \in y = a \subseteq t$, so again, $x \in t$.

t' is also well-founded. To see this, let $\emptyset \neq A \subseteq t'$. If $A \cap t \neq \emptyset$, then let b be $\in$-minimal in $A \cap t$. It follows that b is $\in$-minimal in A. For if $c \in b$, then we know by $\in$-minimality of b that $c \notin A \cap t$. So if we had $c \in A$, it would have to be that $c = a$, which would mean that $a \in b \in t$, so $a \in t$. But then $a \in A \cap t$ and $a \in b$, again contradicting the $\in$-minimality of b in $A \cap t$. The other case is that $A \cap t = \emptyset$, that is, $A = \{a\}$. In this case, we have to convince ourselves that a is $\in$-minimal in A. But if this were not the case, then $a \in a \subseteq t$, so $a \in t$, so $a \in A \cap t = \emptyset$, a contradiction. □

The following theorem says that the class of well-founded sets is well-founded with respect to classes.

Theorem 2.3.53. *Let* $\emptyset \neq A \subseteq \mathsf{WF}$*. Then* A *has an* $\in$*-minimal element.*

Proof. Let $a \in A$. If a is $\in$-minimal in A, then we're done, so let's assume this is not the case. We know that since $a \in \mathsf{WF}$, so is $\{a\}$. So let t be transitive and well-founded, with $a \in t$. Let $\tilde{a} = A \cap t$. Then $\tilde{a} \neq \emptyset$, because $a \in \tilde{a}$. By well-foundedness of t, let b be $\in$-minimal in $\tilde{a}$. It follows that b is $\in$-minimal in A: otherwise, there would be a $c \in b$ with $c \in A$. But since $c \in b \in t$, it would then follow that $c \in t$, as t is transitive. So $c \in A \cap t = \tilde{a}$. This contradicts the $\in$-minimality of b in $\tilde{a}$. □

Theorem 2.3.54 (ZF^{--}+Power Set)**.** $\mathrm{V}_\infty = \mathsf{WF}$*.*

Proof. For the inclusion from left to right, recall that we have seen that each V_α is transitive. It thus suffices to show that each V_α is well-founded, because then, if $a \in \mathrm{V}_\infty$, there is an α such that $a \in \mathrm{V}_\alpha$, which implies that $a \subseteq \mathrm{V}_\alpha$, and thus, V_α witnesses that $a \in \mathsf{WF}$.

To see that for all α, V_α is well-founded, assume the contrary. By the well-foundedness of $(\mathrm{On}, <)$, let α be a (the) minimal counterexample. Let $\emptyset \neq a \subseteq \mathrm{V}_\alpha$ be such that a has no $\in$-minimal element. Note that it has to be that $\alpha > 0$. Pick $b \in a$. Then $b \in \mathrm{V}_\alpha$. It follows that for some $\beta < \alpha$, $b \subseteq \mathrm{V}_\beta$: either α is a successor ordinal, say $\alpha = \beta + 1$, in which case $b \in \mathrm{V}_\alpha = \mathcal{P}(\mathrm{V}_\beta)$, so $b \subseteq \mathrm{V}_\beta$, as wished. Or α is a limit ordinal, in which case there is a $\beta < \alpha$ such that $b \in \mathrm{V}_\beta$, and since V_β is transitive, it follows that $b \subseteq \mathrm{V}_\beta$.

Now let $\tilde{a} = \mathrm{V}_\beta \cap a$. Then $\tilde{a} \neq \emptyset$, since b is not $\in$-minimal in a: there is an $x \in b$ with $x \in a$. Since $b \subseteq \mathrm{V}_\beta$, it follows that $x \in \mathrm{V}_\beta \cap a = \tilde{a}$. Now by minimality of α, V_β is well-founded. So let c be $\in$-minimal in $\tilde{a}$. It then follows that c is $\in$-minimal in a, because if not, let $d \in c$, $d \in a$. Then $d \in c \in \tilde{a} \subseteq \mathrm{V}_\beta$, so $d \in c \in \mathrm{V}_\beta$, so $d \in \mathrm{V}_\beta$, so $d \in \mathrm{V}_\beta \cap a = \tilde{a}$. So a had an $\in$-minimal element after all. This contradiction proves the inclusion from left to right.

Let's now prove the inclusion from right to left. Suppose it fails. Then $\mathsf{WF} \setminus \mathrm{V}_\infty \neq \emptyset$. By Theorem 2.3.53, there is then an $\in$-minimal element a in $\mathsf{WF} \setminus \mathrm{V}_\infty$. But then it follows that $a \subseteq \mathrm{V}_\infty$, because if $b \in a$, then $b \in \mathsf{WF}$, as WF is transitive (by Lemma 2.3.52), so if it were the case that $b \notin \mathrm{V}_\infty$, we'd have that $b \in \mathsf{WF} \setminus \mathrm{V}_\infty$, contradicting the $\in$-minimality of a in this class. Now, for every $x \in a$, we can let $F(x)$ be the least α such that $x \in \mathrm{V}_\alpha$. Letting $\lambda = \bigcup F``a$, it then follows that $a \subseteq \mathrm{V}_\lambda$, so $a \in \mathrm{V}_{\lambda+1} \subseteq \mathrm{V}_\infty$. So $a \in \mathrm{V}_\infty$ after all, a contradiction. □

Corollary 2.3.55 ($\mathsf{ZF}^{--} + \neg\mathsf{Infinity}$)**.** $\mathrm{V}_\infty = \mathsf{WF}$.

Proof. The proof of Theorem 2.3.54 goes through, because the only use of the Power Set axiom in that proof was that for every $\alpha \in \mathrm{On}$, $\mathrm{V}_\alpha \in \mathrm{V}$. This holds under $\neg$Infinity as well. □

Corollary 2.3.56. *The following theories are equivalent:*

1. $\mathsf{ZF}^{--}_F + \mathsf{Power\ Set}$
2. $\mathsf{ZF}^{--} + \mathsf{Power\ Set} + \mathrm{V}_\infty = \mathrm{V}$.

Proof. $1 \Longrightarrow 2$: By Theorem 2.3.54, $\mathsf{ZF}^{--}_F + \mathsf{Power\ Set}$ proves that $\mathrm{V}_\infty = \mathsf{WF}$. But it follows from Foundation that every set is contained in a transitive set (as follows from Lemma 2.2.2) and moreover obviously that every transitive set is well-founded, that is, $\mathrm{V} = \mathsf{WF}$. Putting these two equalities together, it follows that $\mathrm{V} = \mathrm{V}_\infty$.

$2 \Longrightarrow 1$: $\mathsf{ZF}^{--} + \mathsf{Power\ Set} + \mathrm{V}_\infty = \mathrm{V}$ implies that $\mathrm{V} = \mathrm{V}_\infty = \mathsf{WF}$ by Theorem 2.3.54 again. But $\mathrm{V} = \mathsf{WF}$ implies every instance of Foundation, by Theorem 2.3.53. □

Corollary 2.3.57. *The following theories are equivalent:*

1. $\mathsf{ZF}^{--}_F + \neg\mathsf{Infinity}$
2. $\mathsf{ZF}^{--} + \neg\mathsf{Infinity} + \mathrm{V}_\infty = \mathrm{V}$.

Proof. Like the proof of Corollary 2.3.56, using Corollary 2.3.55 instead of Theorem 2.3.54. □

In particular, in the theories $\mathsf{ZF}^{--} + \neg\mathsf{Infinity}$ or $\mathsf{ZF}^{--} + \mathsf{Power\ Set}$, the Foundation scheme can be expressed as one sentence: $\mathrm{V}_\infty = \mathrm{V}$. It's not so clear how to do that in $\mathsf{ZF}^{--} + \mathsf{Infinity} + \neg\mathsf{Power\ Set}$, however.

The point of this subsection was to show that all the Foundation axiom does is to restrict the domain of sets we talk about to the class WF. One can show that if one takes a model M of set theory without the Foundation axiom and restricts it to $\{a \in M \mid M \models a \in \mathsf{WF}\}$, then the resulting model will be a model of set theory together with Foundation. Thus, there is no risk of running into inconsistencies in adding Foundation. From now on, I will assume the Foundation axiom.

2.3.5 Trees

Trees are very useful in many contexts, such as the analysis of sets of real numbers. Also, the natural representation of a formula and its subformulas, their subformulas, and so on, is a tree. Trees can also be used to serve as a model for the space in which a derivation is searched for. Such trees are called search trees, and I shall make use of such trees later, when proving the Completeness Theorem for the Tait calculus. Somewhat longer trees occur in combinatorial set theory as well, and they will come up much later, in the third sequel of this lecture course. The current subsection should really be called *short sequent trees.*

Definition 2.3.58. If f is a function with domain α and x is a set, let $f^\frown x := f \cup \{\langle x, \alpha\rangle\}$.

Definition 2.3.59. A (sequent) tree T on a set X is a set of functions (sequences) $f : n \to X$ closed under initial segments. So every member of T is a function whose domain is a natural number, and whose range is contained in X. Moreover, for all $f \in T$ and for all natural numbers m, $f{\restriction}m \in T$. If T is a tree and $p \in T$, then

$$\mathrm{succ}_T(p) := \{x \mid p^\frown x \in T\}.$$

T is *locally finite* if for every $p \in T$, $\mathrm{succ}_T(p)$ is finite. A (cofinal/infinite) *branch* of a tree T is a function $b : \omega \longrightarrow X$ such that for every $n \in \omega$, $b{\upharpoonright}n \in T$.

Definition 2.3.60. Let T be a tree on X, $T \in \mathrm{V}$. Given $s,t \in T$, I write $t >_T s$ if $s \subsetneq t$. T is *well-founded* if the structure $\langle T, >_T\rangle$ (the ordering is reversed here!) is well-founded. [2] Otherwise, the tree is *ill-founded.*

Lemma 2.3.61. *Let $\langle u, r\rangle$ be a structure with $r \subseteq u^2$. Let u be well-ordered by some relation $<_u$. Then $\langle u, r\rangle$ is ill-founded if and only if there is a function $f : \omega \longrightarrow u$ such that for all $n < \omega$, $f(n+1) r f(n)$.*

Proof. Suppose $f : \omega \longrightarrow u$ is such a decreasing sequence. Then the set $f``\omega$ has no r-minimal element, so that $\langle u, r\rangle$ is ill-founded.

Vice versa, suppose $\langle u, r\rangle$ is ill-founded. Now let $\emptyset \neq a \subseteq T$ have no $>_T$-minimal member. It is now possible to define a sequence $\langle s_n \mid n < \omega\rangle$ recursively, by letting s_0 be the $\prec$-minimal member of a. Since a has no r-minimal member, let s_1 be the $\prec$-minimal member of a such that $s_1 r s_0$. In general, having defined s_n, we can let s_{n+1} be $\prec$-minimal such that $s_{n+1} \in a$ and $s_{n+1} r_T s_n$. Then $f(n) := s_n$ is as wished. □

Theorem 2.3.62 (König, ZF^-). *Every infinite, locally finite tree on a well-ordered set X has an infinite branch.*

Proof. Let T be an infinite, locally finite tree on X. Consider the set I consisting of those $f \in T$ such that the set $T^f := \{g \in T \mid f \subseteq g\}$ is infinite. It follows that I is a tree: It is obviously closed under initial segments. Moreover, I is ill-founded: Firstly, $I \neq \emptyset$ because $\emptyset \in I$, as T is infinite, by assumption. Secondly, if $f \in I$, then T^f is infinite. But

$$T^f = \{f\} \cup \bigcup_{x \in \mathrm{succ}_T(f)} T^{f^\frown x}$$

is a partition of the infinite (since $f \in I$) set T^f into finitely many pieces (as T is locally finite, so that $\mathrm{succ}_T(f)$ is finite). Hence, there must be an $x \in \mathrm{succ}_T(f)$ such that $T^{f^\frown x}$ is infinite, in other word, such that $f^\frown x \in I$. So f is not $>_T$-minimal in I. Since f was an arbitrary member of I, this shows that I is ill-founded. T inherits a well-ordering from X in a canonical way: Let $<_X$ be a well-order on X. For example, if $s,t \in T$ such that $s \neq t$, let $s \prec t$ if $\mathrm{dom}(s) < \mathrm{dom}(t)$, or if $\mathrm{dom}(s) = \mathrm{dom}(t)$ and for the least l such that $s{\upharpoonright}l \neq t{\upharpoonright}l$, $s(l) <_X t(l)$. The reader is invited to check that this is a well-ordering on T. The restriction of this well-ordering to I is of course a well-order on I, so Lemma 2.3.61 is applicable. It shows that I has an infinite branch $>_T$-decreasing sequence, and such a sequence will generate a branch of T in the obvious way. □

2.4 Cardinal Numbers and Choice

2.4.1 Comparing size without choice

There are several natural ways to compare the sizes of sets. Recall Definition 2.3.34, which defined sets x and y to be equinumerous ($x \sim y$) if there is a bijection between them. The following definition expresses that x is at most as large as y, in the sense that "x can be put inside y."

[2] The structure $\langle T, <_T\rangle$ is always well-founded. Note also that since T is a set, the scheme expressing that $\langle T, >_T\rangle$ is well-founded is actually equivalent to the formula saying that every nonempty sub*set* of T has a $>_T$-minimal member. In this case, I take "$\langle T, >_T\rangle$ is well-founded" to stand for this formula.

Definition 2.4.1. For sets x and y, write $x \preceq y$ to express that there is an injection $g : x \rightarrowtail y$.

Note that if $x \preceq y$, then there is a surjection $h : y \twoheadrightarrow x$. The existence of a surjection from y onto x is also a natural concept expressing that y is at least as large as x, in the sense that x "can be covered by y." It is not provable in ZF that this latter notion implies that $x \preceq y$. I'll work in ZF for awhile now, until I'll add the axiom of choice. Recall that ZF is ZF^{--}_{F}+Infinity+Power Set.

Lemma 2.4.2 (Hartogs, ZF)**.** *For every set x, there is an ordinal α such that there is no surjection from x onto α. In particular, $\alpha \not\preceq x$.*

Proof. The point is that if $f : x \twoheadrightarrow \beta$, then f can be coded by the relation r_f on x defined by $a r_f b \iff f(a) < f(b)$. Namely, r_f is a well-founded relation on x, and f is the unique function satisfying, for all $a \in x$: $f(a) = \bigcup\{f(b) \mid b r_f a\}$. This is also known as the rank function of r_f. (Another way to think of this coding is as follows: the relation e on x defined by $aeb \iff f(a) = f(b)$ is an equivalence relation, and if x/e is the set of e-equivalence classes, then for $u, v \in x/e$, one can define $u R_f v \iff \forall a \in u \forall b \in v\ f(a) < f(b)$. Then R_f is a well-order of x/e, and if $F : x/e \longrightarrow \mathrm{On}$ is the Mostowski collapse of $\langle x/e, R_f\rangle$, then $f(a) = F([a]_e)$, where $[a]_e$ is the e-equivalence class of $a \in x$. So f can be read off of R_f and e. But of course, e and R_f can be defined from r_f, as aeb iff $\neg(a r_f b)$ and $\neg(b r_f a)$.)

Thus, if we consider the class $A = \{f \mid \exists\alpha \quad f : x \twoheadrightarrow \alpha\}$, then the map $G : A \longrightarrow \mathcal{P}(x \times x)$ defined by $G(f) = r_f$ is injective, and hence, its inverse $G^{-1} : \mathrm{ran}(G) \twoheadrightarrow A$ exists. But $\mathrm{ran}(G) \subseteq \mathcal{P}(x \times x)$ is a set, by Separation, and so, A is a set as well, by Replacement. Hence, the set $\{\mathrm{ran}(f) + 1 \mid f \in A\}$ is a set as well, thus so is $\theta = \bigcup\{\mathrm{ran}(f) + 1 \mid f \in A\}$, by Union. The latter is the least ordinal greater than every ordinal of the form $\mathrm{ran}(f)$, for any $f \in A$. Thus, there is no surjection from x onto θ. □

Theorem 2.4.3 (Cantor)**.** *For any set x, $x \preceq \mathcal{P}(x)$, but there is no surjection $f : x \twoheadrightarrow \mathcal{P}(x)$. So in particular, $\mathcal{P}(x) \not\preceq x$.*

Proof. The function $a \mapsto \{a\}$ is an injection from x to $\mathcal{P}(x)$, so $x \preceq \mathcal{P}(x)$. Now let's assume there was a surjection $f : x \twoheadrightarrow \mathcal{P}(x)$. Let $a = \{b \in x \mid b \notin f(b)\}$. Since $a \in \mathcal{P}(x)$, there has to be a $c \in x$ such that $f(c) = a$. But then $c \in a \iff c \notin f(c)$, by definition of a, and since $f(c) = a$, this means that $c \in a \iff c \notin a$, a contradiction. □

Theorem 2.4.4 (Schröder-Bernstein, Dedekind)**.** *If $u \preceq v$ and $v \preceq u$, then $u \sim v$.*

Proof. Let $f : u \rightarrowtail v$ and $g : v \rightarrowtail u$. Recursively define sequences $\langle u_n \mid n < \omega\rangle$ and $\langle v_n \mid n < \omega\rangle$ by setting $u_0 = u$, $u_{n+1} = gf``u_n$ and $v_0 = v$, $v_{n+1} = fg``v_n$. By induction on n, one can easily verify that these sequences are nested as follows:

$$u_n \supseteq g``v_n \supseteq u_{n+1} \text{ and} v_n \supseteq f``u_n \supseteq v_{n+1}.$$

Clearly, $f``(u_n \setminus g``v_n) = (f``u_n) \setminus v_{n+1}$, and $g``(v_n \setminus f``u_n) = g``v_n \setminus u_{n+1}$. Let $u^* = \bigcap_{n<\omega} u_n$, $v^* = \bigcap_{n<\omega} v_n$. Then

$$f``u^* = \bigcap_{n<\omega} f``u_n = \bigcap_{n<\omega} v_{n+1} = v^*,$$

because of the nested pattern $v_n \supseteq f``u_n \supseteq v_{n+1}$. Thus, if we set

$$h = f\upharpoonright\left(u^* \cup \bigcup_{n<\omega}(u_n \setminus g``v_n)\right) \cup g^{-1}\upharpoonright \bigcup_{n<\omega}(g``v_n \setminus u_{n+1}),$$

then $h : u \rightarrowtail\!\!\!\!\twoheadrightarrow v$, as wished. □

2.4.2 Equivalents of the axiom of choice

The axiom of choice will allow us to measure the sizes of sets on a linear scale.

Definition 2.4.5. The *axiom of choice* (AC) says that every set has a cardinality. I.e., for every set x, there is an $\alpha \in \mathrm{On}$ such that $x \sim \alpha$. The *cardinality* of a set x is the least α such that $x \sim \alpha$.

Note that if $\mathrm{V} = \mathrm{V}_\omega$, then every set is finite, so that the axiom of choice automatically holds. So under Foundation, AC is only interesting if we assume Infinity.

Theorem 2.4.6 (ZF). *The following are equivalent:*

1. AC,
2. *every set can be well-ordered (i.e., for all x, there is an $r \subseteq x^2$ such that $\langle x, r\rangle$ is a well-order),*
3. *every set of nonempty sets has a choice function, i.e., for all x, if $\forall y \in x \quad y \neq \emptyset$, then there is a function $f : x \longrightarrow \bigcup x$, so that $\forall y \in x \quad f(y) \in y$.*[3]

Proof. $1 \Longrightarrow 2$: Given a set x, let $f : x \rightarrowtail\!\!\!\!\twoheadrightarrow \alpha$. Then x inherits a well-order $<_x$ from $\langle \alpha, < \restriction \alpha\rangle$ via $y <_x z \iff f(y) < f(z)$.

$2 \Longrightarrow 3$: Let x be a set of non-empty sets. Let $\langle \bigcup x, r\rangle$ be a well-order. Define $F : x \longrightarrow \bigcup x$ by letting $F(y)$ be the r-minimal member of y. F is definable, so that $F = F \cap ((\bigcup x) \times x) \in \mathrm{V}$.

$3 \Longrightarrow 1$: Let x be a set. We have to find f and γ such that $f : x \rightarrowtail\!\!\!\!\twoheadrightarrow \gamma$. Consider $z := \mathcal{P}(x)\setminus\{\emptyset\}$ (so here, the Power Set axiom is used). This is a set of nonempty sets, so there is a choice function $g : z \longrightarrow \bigcup z$. Now we can define by recursion a function $F : \mathrm{On} \longrightarrow x$ as follows:

$$F(\xi) = \begin{cases} g(x \setminus F``\xi) & \text{if defined} \\ \{x\} & \text{otherwise} \end{cases}$$

Let $\Gamma = \bigcup\{\xi \mid F(\xi) \neq \{x\}\}$. Then $F\restriction\Gamma : \Gamma \rightarrowtail x$. So F^{-1} is a function, which means that $\Gamma = F^{-1}``x \in \mathrm{V}$, i.e., $\gamma := \Gamma < \infty$. It follows that $F : \gamma \twoheadrightarrow x$ as well, so $f := F \cap (x \times \gamma) \in \mathrm{V}$ is a bijection from γ onto x. □

Note that only in the proof of (3) $\Longrightarrow$ (1) did we use the Power Set axiom. Thus, in the absence of the Power Set axiom, it is conceivable that the formulation (1) of the axiom of choice is stronger than the formulation (3). Since it is (1) that we usually need, I chose to take that formulation as the official definition of AC. This way, even in the absence of Power Set, if we assume AC, we have the strongest form of choice at our disposal.

Definition 2.4.7. $\langle x, \leq_x\rangle$ is a *partial order* if $\leq_x \subseteq x^2$ is reflexive and transitive. It is a partial order *in the strict sense* if in addition, it is *anti-symmetric*, meaning that if $u \leq_x v$ and $v \leq_x u$, then $u = v$. A *chain* in a partial order $\langle x, \leq_x\rangle$ is a set $c \subseteq x$ such that for any $u, v \in c$, $u \leq_x v$ or $v \leq_x u$. Such a partial order is *chain-closed* if for any chain $c \subseteq x$, c has a *bound* in $\langle x, \leq_x\rangle$, i.e., there is a $b \in x$ such that for all $u \in c$, $u \leq_x b$. If $\langle x, \leq_x\rangle$ is a partial order, write $<_x$ for the binary relation on x defined by letting $u <_x v$ iff $u \leq_x v$ and $u \neq v$. $m \in x$ is *maximal* in $\langle x, \leq_x\rangle$ if there is no $u \in x$ with $u >_x m$.

Note: If $\langle x, \leq_x\rangle$ is a partial order in the strict sense, then $\langle x, <_x\rangle$ is irreflexive and transitive. Irreflexivity is clear by definition, and to see transitivity, suppose that $u <_x v$ and $v <_x w$. Then $u \leq_x v$ and $v \leq_x w$, so that $u \leq_x w$, as $\leq_x$ is transitive. To see that $u <_x w$, it must be verified that $u \neq w$. But if it were the case that $u = w$, then we'd have $u \leq_x v \leq_x u$, so since $\langle x, \leq_x\rangle$ is

[3] This is usually the official definition of the axiom of choice.

a partial order in the strict sense, it would follow that $u = v$, contradicting the assumption that $u <_x v$.

Note also that there may be many maximal elements in a chain-closed partial order.

Lemma 2.4.8 (Zorn's Lemma, ZF). *The following are equivalent:*

1. *Whenever* $\langle x, \leq_x \rangle$ *is a chain-closed partial order in the strict sense (with* $x \neq \emptyset$*), it has a maximal element.*

2. *The axiom of choice.*

Proof. $2 \Longrightarrow 1$: By the axiom of choice, fix a well-ordering R of x. Define a function $F : \mathrm{On} \longrightarrow x \cup \{x\}$ by setting:

$$F(\alpha) = \begin{cases} \text{The } R\text{-minimal member } u \text{ of } x \text{ with} & \\ \quad \forall z \in F``\alpha \quad z <_x u & \text{if this exists,} \\ x & \text{otherwise.} \end{cases}$$

Let $\Gamma = \{\alpha \mid F(\alpha) \neq x\}$. Then $f := F{\restriction}\Gamma$ is injective, so $\Gamma < \infty$. Moreover, if $\alpha < \beta < \Gamma$, then $f(\alpha) <_x f(\beta)$, by definition of F. Also, if λ is a limit ordinal and $\lambda \subseteq \Gamma$, then $\lambda \in \Gamma$. This is because $F``\lambda$ is a chain in $\langle x, \leq_x \rangle$, so that it has a bound $y$. But then this bound is a strict bound, i.e., $y >_x z$, for all $z \in F``\lambda$ - this is because if $z = F(\alpha)$, for some $\alpha < \lambda$, then $z <_x F(\alpha + 1) \leq_x y$, so that $z <_x y$. So Γ is a successor ordinal, say $\Gamma = \delta + 1$. Then $F(\delta)$ is a maximal element of $\langle x, <_x \rangle$: Since $F(\delta + 1) = x$, by definition, there is no y with $y >_x F(\delta)$.

$1 \Longrightarrow 2$: Let's verify the axiom of choice in the form stating every set of nonempty sets has a choice function. So let u be a set of nonempty sets, and consider the set F consisting of the functions whose domain is a subset of u and which are choice functions for their domain (which naturally is a set of nonempty sets). Consider the partial order $\langle F, \subseteq {\restriction}(F^2) \rangle$. This is a partial order in the strict sense, and it is chain closed, as is easily verified (the point is that the union of a chain of functions is again a function). So let $f \in F$ be maximal. The claim is that $\mathrm{dom}(f) = u$. For if not, then let $y \in u \setminus \mathrm{dom}(f)$. Since $y \neq \emptyset$, pick $z \in y$, and set $f' = f \cup \{\langle z, y \rangle\}$. Then $f' \in F$, and $f \subsetneqq f'$, contradicting the maximality of f.

So $\mathrm{dom}(f) = u$, which means that f is a choice function for u. □

2.4.3 Basic cardinal arithmetic

Definition 2.4.9. An ordinal κ is a cardinal if $\kappa = \overline{\overline{\kappa}}$, that is, if there is no $\alpha < \kappa$ with $\alpha \sim \kappa$. The class of all cardinals is denoted Card.

Lemma 2.4.10 (AC).

1. $u \sim v \iff \overline{\overline{u}} = \overline{\overline{v}}$.

2. $\overline{\overline{u}} \in \mathrm{Card}$.

3. $u \preceq v \implies \overline{\overline{u}} \leq \overline{\overline{v}}$.

4. $\nu \leq \omega \implies \nu \in \mathrm{Card}$.

Definition 2.4.11. Let $\Gamma \leq \infty$, and let $A \subseteq \Gamma$. Then A is *unbounded* in Γ if $\forall \alpha < \Gamma \exists \beta < \Gamma (\beta > \alpha \wedge \beta \in A)$. An ordinal $\lambda > 0$ is a *limit point* of A if $A \cap \lambda$ is unbounded in λ. A is *closed* in Γ if whenever $\lambda < \Gamma$ is a limit point of A, then $\lambda \in A$.

Lemma 2.4.12. Card *is closed and unbounded in* ∞.

Proof. To see that Card is unbounded in ∞, let $\alpha < \infty$ be given. By Lemma 2.4.2, there is a β such that there is no surjection from α onto β. Let β be the least such. Clearly, $\beta > \alpha$. It follows that $\beta \in \text{Card}$, because otherwise, $\overline{\overline{\beta}} < \beta$, and by minimality of β, there is a surjection from α onto $\overline{\overline{\beta}}$, but composing this surjection with a bijection between $\overline{\overline{\beta}}$ and β gives a surjection from α onto β, a contradiction.

To see that Card is closed in ∞, let λ be a limit point of Card. Suppose $\lambda \notin \text{Card}$. Then $\overline{\overline{\lambda}} < \lambda$. Since λ is a limit point of Card, we can pick a cardinal κ with $\overline{\overline{\lambda}} < \kappa < \lambda$. Then $\kappa \preceq \lambda \sim \overline{\overline{\lambda}}$, so by composing the witnessing functions, we see that $\kappa \preceq \overline{\overline{\lambda}}$. But clearly, $\overline{\overline{\lambda}} \preceq \kappa$ as well, since $\overline{\overline{\lambda}} < \kappa$. So by Theorem 2.4.4, $\kappa \sim \overline{\overline{\lambda}} < \kappa$, so $\overline{\overline{\kappa}} < \kappa$, contradicting that $\kappa \in \text{Card}$. □

Observation 2.4.13. $\overline{\overline{\alpha}} = \max\{\beta \leq \alpha \mid \beta \in \text{Card}\}$.

Proof. Let $X = \{\beta \leq \alpha \mid \beta \in \text{Card}\}$. So $\overline{\overline{\alpha}} \in X$. Suppose $\overline{\overline{\alpha}} < \beta = \max X$. Then $\overline{\overline{\alpha}} < \beta \leq \alpha$, $\beta \in \text{Card}$. This gives a contradiction as in the previous proof. □

Definition 2.4.14. Let $\langle \aleph_\nu \mid \nu < \infty \rangle$ be the enumeration of $\text{Card} \setminus \omega$ (the infinite cardinals). So $\aleph_0 = \omega$. I will often write ω_ν for $\aleph_\nu$.

Observation 2.4.15. *Since* Card *is closed, the function* $\nu \mapsto \aleph_\nu$ *is a normal function, meaning that it is strictly increasing and continuous, i.e., if* λ *is a limit ordinal, then* $\aleph_\lambda = \sup_{\nu<\lambda} \aleph_\nu$.

Definition 2.4.16. For $\alpha < \infty$, let $\alpha^+ = \min(\text{Card} \setminus (\alpha + 1))$, i.e., α^+ is the least cardinal greater than α.

So we have: $\aleph_0 = \omega$, $\aleph_{\nu+1} = \aleph_\nu^+$ and for limit λ, $\aleph_\lambda = \bigcup_{\nu<\lambda} \aleph_\nu$.

The basic cardinal arithmetic operations are defined as follows. I will use the same notation as for ordinal arithmetic - the meaning will be clear from context.

Definition 2.4.17. Let $\alpha, \beta \in \text{Card}$. Then

$$\begin{aligned} \alpha + \beta &= \overline{\overline{\alpha \times \{0\} \cup \beta \times \{1\}}} \\ \alpha \cdot \beta &= \overline{\overline{\alpha \times \beta}} \end{aligned}$$

Note that this is the same definition that we also used for these operations on the natural numbers.

Lemma 2.4.18 (AC)**.** *Let* $\alpha, \beta, \gamma \in \text{Card}$.

1. $u \cap v = \emptyset \implies \overline{\overline{u \cup v}} = \overline{\overline{u}} + \overline{\overline{v}}$.
2. *If* $\alpha, \beta < \omega$*, then the ordinal sum/product of* α *and* β *is the same as the cardinal sum/product.*
3. $\overline{\overline{u \times v}} = \overline{\overline{u}} \cdot \overline{\overline{v}}$.
4. $\alpha + 0 = \alpha$, $\alpha + \beta = \beta + \alpha$, $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.
5. $\alpha \leq \beta \implies \alpha + \gamma \leq \beta + \gamma$.
6. $\alpha \cdot 0 = 0$, $\alpha \cdot 1 = \alpha$, $\alpha \cdot 2 = \alpha + \alpha$.
7. $\alpha \cdot \beta = \beta \cdot \alpha$, $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.
8. $\alpha \leq \beta \implies \alpha \cdot \gamma \leq \beta \cdot \gamma$.
9. $\beta \geq 1 \implies \alpha \leq \alpha \cdot \beta$.

Definition 2.4.19 (Gödel)**.** Define a relation $<^* \subseteq \mathrm{On} \times \mathrm{On}$ by setting $\langle\alpha, \beta\rangle <^* \langle\gamma, \delta\rangle$ iff either $\max(\alpha, \beta) < \max(\gamma, \delta)$, or $\max(\alpha, \beta) = \max(\gamma, \delta)$ but $\alpha < \gamma$, or $\max(\alpha, \beta) = \max(\gamma, \delta)$ and $\alpha = \gamma$, but $\beta < \delta$.

Lemma 2.4.20. *The structure* $(\mathrm{On} \times \mathrm{On}, <^*)$ *is strongly well-founded.*

Proof. The relation $<^*$ is easily seen to be linear (for example by observing that it can be viewed as a lexicographical ordering, namely, $\langle\alpha, \beta\rangle <^* \langle\gamma, \delta\rangle$ iff $\langle\max\{\alpha, \beta\}, \alpha, \beta\rangle <_{\mathrm{lex}} \langle\max\{\gamma, \delta\}, \gamma, \delta\rangle$). It is set-like because the set of $<^*$-predecessors of some fixed pair $\langle\alpha, \beta\rangle$ is contained in $\mu \times \mu$, where $\mu = \max\{\alpha, \beta\} + 1$. It is well-founded, because given any nonempty $A \subseteq \mathrm{On} \times \mathrm{On}$, one can let $\mu = \min\{\max\{\alpha, \beta\} \mid \langle\alpha, \beta\rangle \in A\}$, then let $\alpha_0 = \min\{\alpha \mid \exists\beta \quad \max(\alpha, \beta) = \mu \wedge \langle\alpha, \beta\rangle \in A\}$ (i.e., minimize the first coordinate), then let $\beta_0 = \min\{\beta \mid \max\{\alpha_0, \beta\} = \mu \wedge \langle\alpha_0, \beta\rangle \in A\}$ (i.e., minimize the second coordinate). It follows that $\langle\alpha_0, \beta_0\rangle$ is the $<^*$-minimum of A. □

It follows from the previous lemma that $\mathrm{otp}(\mathrm{On} \times \mathrm{On}, <^*) = \infty$, and the following definition makes sense.

Definition 2.4.21. Let $\Gamma : (\mathrm{On} \times \mathrm{On}, <^*) \longrightarrow \mathrm{On}$ be the Mostowski isomorphism. Γ is called *Gödel's Pairing Function*. Often, $\Gamma(\alpha, \beta)$ is denoted $\prec\alpha, \beta\succ$.

Lemma 2.4.22. *Let* $\kappa \geq \omega$ *be a cardinal. Then*

$$\Gamma\restriction(\kappa \times \kappa) : \kappa \times \kappa \rightarrowtail\!\!\!\!\rightarrow \kappa.$$

Proof. We have to show that if $\kappa \geq \omega$ is a cardinal, then $\Gamma``(\kappa \times \kappa) = \kappa$. The direction from right to left here is easy to see: if $\gamma < \kappa$, then $\langle 0, \gamma\rangle \in \kappa \times \kappa$, and the function $f : \gamma + 1 \longrightarrow \mathrm{On}$ defined by $f(\delta) = \Gamma(0, \delta)$ is strictly increasing, and hence, clearly, $f(\delta) \geq \delta$ (this can be shown by induction on δ). Thus, $\Gamma(0, \gamma) \geq \gamma$. So if $\Gamma(0, \gamma) = \gamma$, then we are done. Otherwise, $\gamma \in \Gamma(0, \gamma) = \{\Gamma(\alpha, \beta) \mid \langle\alpha, \beta\rangle < *\langle 0, \gamma\rangle\}$, so there is a pair $\langle\alpha, \beta\rangle <^* \langle 0, \gamma\rangle$ such that $\Gamma(\alpha, \beta) = \gamma$. By the definition of $<^*$, it follows that $\alpha, \beta < \gamma$, so in particular, $\langle\alpha, \beta\rangle \in \kappa \times \kappa$.

For the converse, we show by induction on $\nu \in \mathrm{On}$ that $\Gamma``(\aleph_\nu \times \aleph_\nu) \subseteq \aleph_\nu$.

In the case $\nu = 0$, we are showing $\Gamma``\omega \times \omega \subseteq \omega$. Given $\langle m, n\rangle \in \omega \times \omega$, we have that

$$\Gamma(m, n) = \{\Gamma(k, l) \mid \langle k, l\rangle <^* \langle m, n\rangle\} \subseteq \{\Gamma(k, l) \mid \langle k, l\rangle \in p \times p\},$$

where $p = \max\{m, n\} + 1 < \omega$. So $\Gamma(m, n)$ has only finitely many elements, and it is an ordinal, it has to be less than ω.

In the case that ν is a successor ordinal, say $\nu = \gamma + 1$, let $\langle\alpha, \beta\rangle \in \aleph_{\gamma+1} \times \aleph_{\gamma+1}$ be given. We have that

$$\Gamma(\alpha, \beta) = \{\Gamma(\xi, \zeta) \mid \langle\xi, \zeta\rangle <^* \langle\alpha, \beta\rangle\} \subseteq \{\Gamma(\xi, \zeta) \mid \langle\xi, \zeta\rangle \in \mu \times \mu\},$$

where $\mu = \max(\alpha, \beta) + 1$. Now since $\alpha < \aleph_{\gamma+1}$, it follows that $\overline{\overline{\alpha}} \leq \aleph_\gamma$, and similarly for $\overline{\overline{\beta}}$. So $\overline{\overline{\max\{\alpha, \beta\}}} \leq \aleph_\gamma$, and this clearly implies that $\overline{\overline{\mu}} \leq \aleph_\gamma$. Thus, there is an injective function $f : \mu \rightarrowtail \aleph_\gamma$. But then, there is an injective map $g : \Gamma(\alpha, \beta) \longrightarrow \aleph_\gamma$, defined by $g(\Gamma(\xi, \zeta)) = \Gamma(f(\xi), f(\zeta)) < \aleph_\gamma$, because $f(\xi), f(\zeta) < \aleph_\gamma$ and inductively, $\Gamma``\aleph_\gamma \times \aleph\gamma \subseteq \aleph_\gamma$. Thus, $\overline{\overline{\Gamma(\alpha, \beta)}} \leq \aleph_\gamma$, which implies that $\Gamma(\aleph, \beta) < \aleph_{\gamma+1}$, as was to be shown.

The limit case is immediate: let ν be a limit ordinal. If $\langle\alpha, \beta\rangle \in \aleph_\nu \times \aleph_\nu$, then it follows that there is a $\bar{\nu} < \nu$ such that $\langle\alpha, \beta\rangle \in \aleph_{\bar{\nu}} \times \aleph_{\bar{\nu}}$. But then, inductively, $\Gamma(\alpha, \beta) < \aleph_{\bar{\nu}} < \aleph_\nu$, and we are done. □

Corollary 2.4.23. *Let* κ, λ *be cardinals,* $\lambda \geq \omega$*.*

1. $\lambda \cdot \lambda = \lambda$.
2. $\kappa \cdot \lambda = \max\{\kappa, \lambda\}$ *if* $\kappa > 0$.
3. $\kappa + \lambda = \max\{\kappa, \lambda\}$.

Proof. Point 1 follows from Lemma 2.4.22:

$$\lambda \sim \lambda \times \lambda \sim \lambda \cdot \lambda.$$

Since λ is a cardinal, this implies that $\lambda \cdot \lambda = \lambda$.

Now let $\gamma = \max\{\kappa, \lambda\}$. Then point 2 follows, using Lemma 2.4.18:

$$\gamma \leq \kappa \cdot \lambda \leq \gamma \cdot \gamma = \gamma.$$

And point 3 follows then because

$$\gamma \leq \kappa + \lambda \leq \gamma + \gamma \leq \gamma \cdot 2 \leq \gamma \cdot \gamma = \gamma.$$

□

Definition 2.4.24 (AC)**.** For sets x, y, define

$${}^{y}x = \{f \mid f : y \longrightarrow x\}.$$

For cardinals κ, λ, let

$$\kappa^\lambda = \overline{\overline{{}^{\lambda}\kappa}}.$$

Lemma 2.4.25. *Let* $\kappa, \lambda, \mu \in \mathrm{Card}$. *Then*

1. $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$.
2. $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$.
3. $2^\kappa = \overline{\overline{\mathcal{P}(\kappa)}}$.

Proof. For 1, it suffices to show that

$${}^{\lambda \times \{0\} \cup \mu \times \{1\}}\kappa \sim {}^{\lambda}\kappa \times {}^{\mu}\kappa.$$

This is witnessed by the function F defined as follows: let $g : \lambda \times \{0\} \cup \mu \times \{1\} \longrightarrow \kappa$ be given. Then define $F(g) = \langle g_0, g_1 \rangle$, where $g_0 : \lambda \longrightarrow \kappa$ and $g_1 : \mu \longrightarrow \kappa$ are defined by

$$g_i(\xi) = g(\xi, i),$$

for $i < 2$. Clearly, F is a bijection.

For 2, it suffices to find a bijection

$$F : {}^{\mu}({}^{\lambda}\kappa) \rightarrowtail\!\!\!\!\!\rightarrow {}^{\lambda \times \mu}\kappa.$$

We define F as follows. Let $f \in {}^{\mu}({}^{\lambda}\kappa)$ be given. Thus, $f : \mu \longrightarrow {}^{\lambda}\kappa$. Thus, for each $\xi < \mu$, $f(\xi) : \lambda \to \kappa$. Define $F(f) : \lambda \times \mu \longrightarrow \kappa$ by

$$(F(f))(\xi, \zeta) = (f(\zeta))(\xi).$$

Again, clearly, F is a bijection.

Finally, for 3, we have to show that there is a function $F : {}^{\kappa}2 \rightarrowtail\!\!\!\!\!\rightarrow \mathcal{P}(\kappa)$, which is easily achieved by setting:

$$F(f) = \{\alpha < \kappa \mid f(\alpha) = 1\}$$

where $f : \kappa \longrightarrow 2$. □

Lemma 2.4.26. *On ω, ordinal and cardinal addition and subtraction coincide.*

Lemma 2.4.27. *Let κ be a cardinal. Then*

1. $\kappa^0 = 1^\kappa = 1$.

2. $\kappa^1 = \kappa$.

3. $\kappa^2 = \kappa \cdot \kappa = \kappa$.

Definition 2.4.28. Let $\langle a_i \mid i \in I\rangle$ be a sequence of sets. Then

$$\prod_{i\in I} = \{f \mid f : I \longrightarrow \mathrm{V} \wedge \forall i \in I \ f(i) \in a_i\}.$$

Recall that for a set s of ordinals, $\sup s = \bigcup s$ is the least ordinal greater than or equal to all elements of s. If $\langle \xi_i \mid i \in I\rangle$ is a sequence of ordinals, then I write $\sup_{i\in I} \xi_i$ for $\sup\{\xi_i \mid i \in I\}$.

Lemma 2.4.29 (AC)**.** *Set $\langle x_i \mid i \in I\rangle \in \mathrm{V}$. Then*

1. $\overline{\overline{\bigcup_{i\in I} x_i}} \leq \overline{\overline{I}} \cdot \sup\limits_{i\in I} \overline{\overline{x_i}}$.

2. $\overline{\overline{\prod_{i\in I} x_i}} \leq (\sup\limits_{i\in I} \overline{\overline{x_i}})^{\overline{\overline{I}}}$.

Proof. For $i \in I$, let $g_i : x_i \rightarrowtail\!\!\!\!\twoheadrightarrow \overline{\overline{x_i}}$ be a bijection.

For 1, it suffices to find an injective function $F : \bigcup_{i\in I} x_i \rightarrowtail \bigcup_{i\in I} \overline{\overline{x_i}}$. To this end, for $z \in \bigcup_{i\in I} x_i$, let $i(z) \in I$ be such that $z \in x_{i(z)}$. Define $F(z) = \langle i(z), g_{i(z)}(z)\rangle$. It is easy to see that F is into.

For 2, it suffices to find an injection $G : \prod_{i\in I} x_i \rightarrowtail {}^I(\bigcup_{i\in I} \overline{\overline{x_i}})$. To this end, define, for $f \in \prod_{i\in I} x_i$,

$$G(f)(i) = g_i(f(i)).$$

It is again easy to see that G is injective. □

2.5 Subsystems of set theory

The axiom system $\mathsf{ZF} + \mathsf{AC}$ is called ZFC.

ZF^- is the system which results from ZF_F^{--} by adding the Infinity axiom and replacing the Replacement scheme with the following Collection scheme:

$$\forall u \exists v \forall x \in u((\exists y \langle x, y\rangle \in A) \longrightarrow (\exists y \in v \langle x, y\rangle \in A)).$$

As usual, the universal form of these formulas needs to be taken (i.e., the free variables occurring in A have to be bound by universal quantifiers in the beginning of the formula). The difference between Replacement and Collection is subtle. Collection implies Replacement, but the converse is not true, modulo ZF_F^{--}. Once the Power Set axiom is added, though, the subtle difference vanishes, so in ZF, Collection holds as a consequence of Replacement and Power Set. In an analysis of Σ_1 predicates, we will encounter a place where it matters that we have Collection at our disposal, when proving closure under bounded quantification.

Similarly, ZFC^- is $\mathsf{ZF}^- + \mathsf{AC}$.

Chapter 3

Semantics

In this chapter, I am returning to what was done in the first chapter. There, I introduced first order languages, without talking about the *meaning* of expressions in such languages. I augmented these languages with an appropriate notion of proof, but still everything was basically about words, that is, sequences of symbols. In this chapter, I want to introduce interpretations of languages, so that, e.g., a formula $\exists x\varphi$ gets a meaning, namely that there exists an x such that φ is true of x.

I will work in the theory ZF^-, although one can work with less in many cases. For example, ZF^{--} will suffice for many purposes, though at the cost of having to deal with proper classes instead of sets.

It is easy to see that in ZF^-, given a set X, one can construct a canonical free halfgroup generated by X (this will be done in the exercises). Fixing a language $\mathcal{L} = \langle \mathbb{C}, \mathbb{P}, \mathbb{F}, \# \rangle$, the collection of $\mathcal{L}$-terms, $\mathsf{Term}_{\mathcal{L}}$ and the collection of $\mathcal{L}$-formulas, $\mathsf{Fml}_{\mathcal{L}}$, then form sets. The same is true for the set of Tait formulas, $\mathsf{Fml}^T_{\mathcal{L}}$.

3.1 Models

Definition 3.1.1. A *model* for $\mathcal{L}$ is a set of the form $\mathcal{M} = \langle X, I \rangle$ with $X \neq \emptyset$ and $I : \mathbb{C} \cup \mathbb{P} \cup \mathbb{F} \longrightarrow \mathrm{V}$ so that

1. For $c \in \mathbb{C}$, $I(c) \in X$. I will write $c^{\mathcal{M}}$ for $I(c)$.
2. For $P \in \mathbb{P}$, $I(P) \subseteq X^{\#(P)}$. I will write $P^{\mathcal{M}}$ in place of $I(P)$.
3. For $F \in \mathbb{F}$, $I(F) : X^{\#(F)} \longrightarrow X$. As expected, $F^{\mathcal{M}}$ will stand for $I(F)$.

It is sometimes convenient to pretend that $\doteq$ is a member of $\mathbb{P}$ and set

$$\doteq^{\mathcal{M}} := \{\langle x, x \rangle \mid x \in |\mathcal{M}|\}.$$

I'll write $|\mathcal{M}|$ for X. This is called the *universe*, or the *domain* of the model $\mathcal{M}$.

Finally, if $P \in \mathbb{P}$ and $\bar{P}$ is the corresponding symbol in the Tait-alphabet of $\mathcal{L}$, then set:

$$\bar{P}^{\mathcal{M}} := |\mathcal{M}|^{\#(P)} \setminus P^{\mathcal{M}},$$

and viewing $\neq$ as $\bar{\doteq}$, the corresponding holds:

$$\neq^{\mathcal{M}} := \{\langle x, y \rangle \mid x \in |\mathcal{M}|,\ y \in |\mathcal{M}| \text{ and } x \neq y\}.$$

I will use the Recursion Theorem in order to define when a model satisfies a formula (with some assignment of its free variables). The relation used will be that of being a subformula. The point is that it is well-founded. The reader will gladly verify the following:

Lemma 3.1.2. *Let $\langle v, s\rangle$ be a well-founded system (i.e., $s \subseteq v^2$ and s is well-founded). Let $\langle u, r\rangle$ be such that $r \subseteq u^2$, and let $f : \langle u, r\rangle \longrightarrow \langle v, s\rangle$ be a homomorphism, meaning that if xry, then $f(x)sf(y)$. Then $\langle u, r\rangle$ is well-founded.*

I will state the following two lemmas without proofs:

Lemma 3.1.3 (Unique Readability of Terms)**.** *If t is a term in a fixed language $\mathcal{L}$, then precisely one of the following possibilities holds true:*

1. *$t = v_m$, for some (unique) variable v_m,*
2. *$t = c$, for some (unique) constant symbol c,*
3. *there is a (unique) function symbol F and a (unique) list $t_0, \ldots, t_{n-1}$, where $n = \#(F)$, such that $t = F(t_0, \ldots, t_{n-1})$. In this case, $t_0, \ldots, t_{n-1}$ will be called the* immediate subterms *of t.*

Lemma 3.1.4 (Unique Readability of formulas)**.** *If φ is a formula in a fixed language $\mathcal{L}$, then precisely one of the following possibilities holds:*

1. *$\varphi = P(t_0, \ldots, t_{n-1})$, for a (unique) $P \in \mathbb{P}$ and a (unique) sequence $t_0, \ldots, t_{n-1}$ with $n = \#(P)$, such that each t_i is a term. For convenience, I allow the possibility $P = \doteq$ here.*
2. *there is a (unique) formula ψ (the* immediate subformula of *φ) such that $\varphi = \neg\psi$,*
3. *there are (unique) formulas ψ_0, ψ_1 (the immediate subformulas of φ) such that $\varphi = (\psi_0 \wedge \psi_1)$,*
4. *there are (unique) formulas ψ_0, ψ_1 (the immediate subformulas of φ) such that $\varphi = (\psi_0 \vee \psi_1)$,*
5. *there is a variable v_m and a formula ψ (the immediate subformula of φ) such that $\varphi = \exists v_m \psi$,*
6. *there is a variable v_m and a formula ψ (the immediate subformula of φ) such that $\varphi = \forall v_m \psi$.*

Of course, the obvious version of this lemma for Tait formulas holds as well.

The relation over which I am going to define whether a formula holds in a given model, with a given assignment of its free variables, will be that of being an immediate subformula. It is clear that the formulas in a given language form a set. The map sending a formula to its length maps an immediate subformula of a formula to a strictly smaller natural number. So since the natural numbers, together with their natural ordering are well-founded, the formulas, with the "immediate subformula" relation, are also well-founded, by Lemma 3.1.2, and the corresponding statement is true of the terms, with the "immediate subterm" relation.

Lemma 3.1.5. *Let $\mathcal{M}$ be a model of some language. An* assignment *in $\mathcal{M}$ is a finite partial function from the set of variables to $|\mathcal{M}|$. Let $\mathsf{Assign}_{\mathcal{M}}$ be the set of assignments in $\mathcal{M}$.*

Definition 3.1.6 (Evaluation of Terms)**.** Let $\mathcal{M}$ be a model of a fixed language $\mathcal{L}$. By recursion on the immediate subterm relation, define a function I whose domain is the set $\mathsf{Term}_{\mathcal{L}}$, so that for every term t, $I(t) : \mathsf{Assign}_{\mathcal{M}} \longrightarrow \mathcal{M} \cup \{|\mathcal{M}|\}$. [1] Writing $t^{\mathcal{M}}(a)$ for $(I(t))(a)$, the definition proceeds as follows.

$$t^{\mathcal{M}}(a) = \begin{cases} a(v_m) & \text{if } t = v_m \text{ and } v_m \in \mathrm{dom}(a), \\ |\mathcal{M}| & \text{if } t \text{ is a variable not in } \mathrm{dom}(a), \\ c^{\mathcal{M}} & \text{if } c \in \mathbb{C}, \\ F^{\mathcal{M}}(t_0^{\mathcal{M}}(a), \ldots, t_{n-1}^{\mathcal{M}}(a)) & \text{if } t = F(t_0, \ldots, t_{n-1}) \text{ and } t_i^{\mathcal{M}}(a) \in M, \text{ for all } i < n, \\ |\mathcal{M}| & \text{if for an immediate subterm } s \text{ of } t,\ s^{\mathcal{M}}(a) = |\mathcal{M}|. \end{cases}$$

Definition 3.1.7. If $a \in \mathsf{Assign}_{\mathcal{M}}$, v_m is a variable and $b \in |\mathcal{M}|$, then let $a({}^{v_m}/_b)$ be the assignment with domain $\mathrm{dom}(a) \cup \{v_m\}$ defined by:

$$(a({}^{v_m}/_b))(x) = \begin{cases} a(x) & \text{if } x \in \mathrm{dom}(a) \text{ and } x \neq v_m, \\ b & \text{if } x = v_m. \end{cases}$$

Now I'm ready to define when a formula is true in a model, given an assignment of its free variables:

Definition 3.1.8 (Satisfaction)**.** Let $\mathcal{M}$ be an $\mathcal{L}$-model. Define a function $F = F^{\mathcal{M}} : \mathsf{Fml} \longrightarrow \mathcal{P}(\mathsf{Assign}_{\mathcal{M}})$ by recursion on the immediate subformula relation. $F(\varphi)$ will be the set of assignments under which φ is satisfied in $\mathcal{M}$. Write $\mathsf{FV}(\varphi)$ for the set of free variables occurring in φ. If φ is an atomic formula of the form $P(t_0, \ldots, t_{n-1})$, where $P \in \mathbb{P}$ (including the possibility that $P = \doteq$), $\#(P) = n$ and $t_0, \ldots, t_{n-1}$ are terms, then let

$$F(\varphi) = \{a \in \mathsf{Assign}_{\mathcal{M}} \mid \langle t_0^{\mathcal{M}}(a), \ldots, t_{n-1}^{\mathcal{M}}(a)\rangle \in P^{\mathcal{M}} \wedge \mathsf{FV}(\varphi) \subseteq \mathrm{dom}(a)\}.$$

Note that the requirement $\mathsf{FV}(\varphi) \subseteq \mathrm{dom}(a)$ could be dropped here, since $t^{\mathcal{M}}(a) = |\mathcal{M}|$ if the free variables of t are not contained in $\mathrm{dom}(a)$. Boolean combinations of formulas are dealt with using the following stipulations:

$$\begin{aligned} F(\varphi_0 \wedge \varphi_1) &:= F(\varphi_0) \cap F(\varphi_1), \\ F(\varphi_0 \vee \varphi_1) &:= F(\varphi_0) \cup F(\varphi_1), \\ F(\neg\varphi) &:= \{a \in \mathsf{Assign}_{\mathcal{M}} \mid (\mathsf{FV}(\varphi) \subseteq \mathrm{dom}(a) \wedge a \notin F(\varphi))\}. \end{aligned}$$

Turning to quantifications, set:

$$\begin{aligned} F(\exists v_m \varphi) &:= \{a \in \mathsf{Assign}_{\mathcal{M}} \mid \exists b \in \mathcal{M} \quad a({}^{v_m}/_b) \in F(\varphi)\}, \\ F(\forall v_m \varphi) &:= \{a \in \mathsf{Assign}_{\mathcal{M}} \mid \forall b \in \mathcal{M} \quad a({}^{v_m}/_b) \in F(\varphi)\}. \end{aligned}$$

Finally, I write

$$\mathcal{M} \models \varphi[a]$$

to express that $a \in F^{\mathcal{M}}(\varphi)$, where $a \in \mathsf{Assign}_{\mathcal{M}}$ with $\mathsf{FV}(\varphi) \subseteq a$.

This definition can be viewed as defining $\mathcal{M} \models \varphi[a]$ also for Tait formulas, by treating $\bar{P}, \dot{\neq}$ as elements of $\mathbb{P}$. The $\neg$-step of the definition is then obsolete.

[1] $(I(t))(a) = |\mathcal{M}|$ will be used to indicate that there is a free variable in t which is not in the domain of a. So it basically means that the interpretation of t given a is undefined. $|\mathcal{M}|$ is just conveniently a set that does not belong to $| < |$.

Note: The above recursive definition of F is stated in ZF, and generally works only if $\mathsf{Infinity}$ and $\mathsf{Power\ Set}$ are assumed. It could be reformulated, though, by defining a function $F' : \mathsf{Fml} \times \mathsf{Assign}_{\mathcal{M}} \longrightarrow 2$ by recursion on the relation R defined by letting $\langle\varphi, a\rangle R\langle\psi, b\rangle$ if φ is an immediate subformula of ψ, $b\restriction \mathsf{FV}(\psi) \subseteq a$, and $\mathrm{dom}(a) = \mathsf{FV}(\varphi)$. This is a set-like relation, and it is obviously well-founded. F' can now be defined in such a way that $a \in F(\varphi)$ iff $F(\varphi, a) = 1$. That definition works without assuming $\mathsf{Power\ Set}$ or $\mathsf{Infinity}$.

Definition 3.1.9. If $a, b \in \mathsf{Assign}_{\mathcal{M}}$ and u is a finite set of variables, then $a \sim_u b$ if $a\restriction u = b\restriction u$. If t is a term, I will write $a \sim_t b$ if $a \sim_{\mathsf{FV}(t)} b$. Analogously, if φ is a formula, then I write $a \sim_\varphi b$ if $a \sim_{\mathsf{FV}(\varphi)} b$.

Lemma 3.1.10. *Let φ be a formula, and let $a, b \in \mathsf{Assign}_{\mathcal{M}}$ be such that $\mathsf{FV}(\varphi) \subseteq \mathrm{dom}(a) \cap \mathrm{dom}(b)$ and $a \sim_\varphi b$. Then*

$$\mathcal{M} \models \varphi[a] \iff \mathcal{M} \models \varphi[b].$$

Proof. This is a typical example of a proof by induction on φ. So I'll prove that the lemma holds true for all atomic formulas, and then that if it holds true for formulas φ_0 and φ_1, then it also holds true for $(\varphi_0 \wedge \varphi_1)$, $(\varphi_0 \vee \varphi_1)$, $\neg\varphi_0$, $\exists v_n\varphi_0$, $\forall v_n\varphi_0$, where v_n does not occur as a bound variable in φ_0. It follows that it holds true for all formulas, since otherwise, one could pick a formula φ contradicting it, which is minimal with respect to the "immediate subformula" relation (the point is that this relation is well-founded). Then φ cannot be atomic, and it cannot have an immediate subformula either, which completes the proof. This is the principle of induction. As a first step to proving the lemma, one has to prove the following, by induction on terms:

($*$) *If $t \in \mathsf{Term}_{\mathcal{L}}$ and $a, b \in \mathsf{Assign}_{\mathcal{M}}$ with $\mathsf{FV}(t) \subseteq \mathrm{dom}(a) \cap \mathrm{dom}(b)$ and $a \sim_t b$, then*

$$t^{\mathcal{M}}(a) = t^{\mathcal{M}}(b).$$

I leave the proof of ($*$) (which follows the same pattern as the rest of the proof of the lemma) to the reader. Assuming ($*$), I'll now prove the lemma. First, suppose $\varphi = P(t_0, \ldots, t_{n-1})$ is an atomic formula, and a, $b \in \mathsf{Assign}_{\mathcal{M}}$ is as in the statement of the lemma. Then

$$\begin{aligned} \mathcal{M} \models P(t_0, \ldots, t_{n-1})[a] &\iff \langle t_0^{\mathcal{M}}(a), \ldots, t_{n-1}^{\mathcal{M}}(a)\rangle \in P^{\mathcal{M}} \\ &\iff \langle t_0^{\mathcal{M}}(b), \ldots, t_{n-1}^{\mathcal{M}}(b)\rangle \in P^{\mathcal{M}} \\ &\iff \mathcal{M} \models P(t_0, \ldots, t_{n-1})[b], \end{aligned}$$

noting that since $a \sim_\varphi b$, it follows that $\mathsf{FV}(t_i) \subseteq \mathrm{dom}(a) \cap \mathrm{dom}(b)$ and $a \sim_{t_i} b$ for every $i < n$, as $\mathsf{FV}(t_i) \subseteq \mathsf{FV}(\varphi)$. So ($*$) is applicable here, showing that $t_i^{\mathcal{M}}(a) = t_i^{\mathcal{M}}(b)$, for $i < n$.

The induction step covering Boolean combinations is trivial, as is mostly the case. Since this is the first occurrence of a proof by induction of formulas, I'll carry it out anyway: Suppose φ_0 and φ_1 are formulas for which the claim of the lemma holds. Let a and b be assignments such that $\mathsf{FV}(\varphi_0 \wedge \varphi_1) \subseteq \mathrm{dom}(a) \cap \mathrm{dom}(b)$ and $a \sim_{(\varphi_0 \wedge \varphi_1)} b$. Since $\mathsf{FV}(\varphi_0 \wedge \varphi_1) = \mathsf{FV}(\varphi_0) \cup \mathsf{FV}(\varphi_1)$, it follows that $\mathsf{FV}(\varphi_i) \subseteq \mathrm{dom}(a) \cap \mathrm{dom}(b)$ and $a \sim_{\varphi_i} b$, for $i < 2$. So since the lemma holds for φ_0 and φ_1, by assumption, we can apply it to φ_0, a, b, and also to φ_1, a, b. This yields:

$$\mathcal{M} \models \varphi_i[a] \iff \mathcal{M} \models \varphi_i[b],$$

for $i < 2$. So we get:

$$\begin{aligned} \mathcal{M} \models (\varphi_0 \wedge \varphi_1)[a] &\iff (\mathcal{M} \models \varphi_0[a]) \text{ and } (\mathcal{M} \models \varphi_1[a]) \\ &\iff (\mathcal{M} \models \varphi_0[b]) \text{ and } (\mathcal{M} \models \varphi_1[b]) \\ &\iff \mathcal{M} \models (\varphi_0 \wedge \varphi_1)[b]. \end{aligned}$$

The $\vee$-step is analogous, and the $\neg$-step is equally trivial. Let's check the $\exists v_m$-step. So let $\varphi = \exists v_m\psi$, where v_m does not occur as a bound variable in ψ, and the lemma holds for ψ. Let a, b be as in the statement of the lemma, for $\exists v_m\psi$. Note that then the statement of the lemma holds for ψ, $a({}^{v_m}/_c)$, $b({}^{v_m}/_c)$, whenever $c \in |\mathcal{M}|$. The point is that $\mathsf{FV}(\psi) \subseteq (\mathrm{dom}(a) \cup \{v_m\}) \cap (\mathrm{dom}(b) \cup \{v_m\})$. So we know (inductively) that

$$\mathcal{M} \models \psi[a({}^{v_m}/_c)] \iff \mathcal{M} \models \psi[b({}^{v_m}/_c)]$$

in this situation. So assume now that

$$\mathcal{M} \models \exists v_m\psi[a].$$

By definition, this means that *there is* a $c \in |\mathcal{M}|$ such that

$$\mathcal{M} \models \psi[a({}^{v_m}/_c)].$$

By the above, this is equivalent to

$$\mathcal{M} \models \psi[b({}^{v_m}/_c)].$$

In particular, there is a c with this property, so that

$$\mathcal{M} \models \exists v_m\psi[b].$$

The converse follows by swapping a and b (or, in fact, the above steps work both ways).

The remaining $\forall v_m$-step is analogous and left to the reader. □

So whether or not a model satisfies a formula, given an assignment, depends only on the behavior of the assignment on the formula's free variables. This motivates the following two definitions.

Definition 3.1.11. Let $\mathcal{M}$ be a model. A function $a : \mathsf{Var} \longrightarrow |\mathcal{M}|$ is called a *full assignment in* $\mathcal{M}$. The set of full assignments in $\mathcal{M}$ is denoted by $\mathsf{Assign}^+_{\mathcal{M}}$. If φ is a formula and a is a full assignment in $\mathcal{M}$, then

$$\mathcal{M} \models \varphi[a] \iff \mathcal{M} \models \varphi[a{\upharpoonright}\mathsf{FV}(\varphi)].$$

Definition 3.1.12. If φ is a formula with free variables $v_{m_0}, \ldots, v_{m_{n-1}}$ (in increasing order), then I write

$$\mathcal{M} \models \varphi[b_0, \ldots, b_{n-1}]$$

to express that $\mathcal{M} \models \varphi[a]$, where $a(v_{m_i}) = b_i$, for all $i < n$. If φ is a *sentence*, i.e., if φ has no free variables, then $\mathcal{M} \models \varphi$ iff $\mathcal{M} \models \varphi[\emptyset]$.

The reader is invited to check the following:

Lemma 3.1.13. *If φ is a Tait formula and $a \in \mathsf{Assign}^+_{\mathcal{M}}$, for some $\mathcal{L}$-model $\mathcal{M}$, then*

$$\mathcal{M} \models {\sim}\varphi[a] \iff \mathcal{M} \not\models \varphi[a].$$

3.2 Consequence

Definition 3.2.1 (Logical Consequence)**.** If Γ is a set of $\mathcal{L}$-formulas or of Tait formulas, then let $\mathsf{FV}(\Gamma) = \bigcup_{\psi\in\Gamma}\mathsf{FV}(\psi)$. If $\mathcal{M}$ is an $\mathcal{L}$-model and $a \in \mathsf{Assign}^+_{\mathcal{M}}$, or $a \in \mathsf{Assign}$ is such that $\mathsf{FV}(\Gamma) \subseteq \mathrm{dom}(a)$, then write $\mathcal{M} \models \Gamma[a]$ to express that $\mathcal{M} \models \psi[a]$, for every $\psi \in \Gamma$.

If φ is an $\mathcal{L}$-formula, then

$$\Gamma \models \varphi \quad\iff\quad \text{for every } \mathcal{L}\text{-model } \mathcal{M} \text{ and every } a \in \mathsf{Assign}^+_{\mathcal{M}},\ \mathcal{M} \models \Gamma[a] \implies \mathcal{M} \models \varphi[a].$$

If $\Gamma = \emptyset$, I write $\models \varphi$ instead of $\emptyset \models \varphi$.

Chapter 4

Same same... but different

By now, I have introduced two notions of "consequence": Given a theory T in a fixed language $\mathcal{L}$, and an $\mathcal{L}$-sentence φ, I have defined what it means that φ is *provable* from T, $T \vdash_T \varphi$, and what it means that φ is a logical consequence, $T \models \varphi$. These are two very different concepts, the first one being based on purely syntactical concepts such as proofs, and the second one on semantical concepts such as models. In the following two sections, I am going to show that these concepts nevertheless are equivalent, for countable T! The direction $T \vdash \varphi \implies T \models \varphi$ is known as the Correctness Theorem. It holds for arbitrary T, not only countable. The converse, $T \models \varphi \implies T \vdash \varphi$ is the Completeness Theorem. I'll prove it first only for countable T, and later, the axiom of choice will allow to drop that assumption.

4.1 Correctness

Given a finite set of (Tait-)formulas Δ, let $\bigvee \Delta$ denote the disjunction of all formulas occurring in Δ (in some fixed enumeration). The order in which the formulas are listed is irrelevant. The meaning is that $\mathcal{M} \models (\bigvee \Delta)[a]$ iff there is a formula $\varphi \in \Delta$ such that $\mathcal{M} \models \varphi[a]$. So in fact, it makes sense to take the disjunction of arbitrarily many formulas, but we won't need to do this here.

Theorem 4.1.1 (Soundness)**.** *If Δ is a (finite) set of Tait formulas such that $\vdash_T \Delta$, then $\models \bigvee \Delta$.*

Proof. By induction on rules.

Case 1: $\vdash_T \Delta$ because of *tertium non datur.*

In this case, there is a formula φ such that $\varphi \in \Delta$ and $\sim\varphi \in \Delta$. Now let $\mathcal{M}$ be an arbitrary $\mathcal{L}$-model and a an arbitrary full assignment in $\mathcal{M}$. Then either $\mathcal{M} \models \varphi[a]$ or $\mathcal{M} \not\models \varphi[a]$. But the latter is equivalent to $\mathcal{M} \models \sim\varphi[a]$. So $\mathcal{M} \models \varphi[a]$ or $\mathcal{M} \models \sim\varphi[a]$, in particular, $\mathcal{M} \models \bigvee \Delta$.

Case 2: $\vdash_T \Delta \cup \{(\varphi \wedge \psi)\}$ because $\vdash_T \Delta \cup \{\varphi\}$ and $\vdash_T \Delta \cup \{\psi\}$, i.e., by applying the $\wedge$-rule.

Let $\mathcal{M}$ be an arbitrary $\mathcal{L}$-model with a full assignment a. Inductively, $\mathcal{M} \models \bigvee(\Delta \cup \{\varphi\})[a]$ and $\mathcal{M} \models \bigvee(\Delta \cup \{\psi\})[a]$. If there is a formula $\chi \in \Delta$ such that $\mathcal{M} \models \chi[a]$, then $\mathcal{M} \models \bigvee \Delta[a]$, and we're done. If not, then since there is a formula χ' in $\Delta \cup \{\varphi\}$ such that $\mathcal{M} \models \chi'[a]$, this must be true for $\chi' = \varphi$. Analogously, it follows that $\mathcal{M} \models \psi[a]$. But if $\mathcal{M} \models \varphi[a]$ and $\mathcal{M} \models \psi[a]$, then this means that $\mathcal{M} \models (\varphi \wedge \psi)[a]$. In particular, $\mathcal{M} \models \bigvee(\Delta \cup \{(\varphi \wedge \psi)\})$, as claimed.

Case 3: $\vdash_T \Delta \cup \{(\varphi \vee \psi)\}$ because of the $\vee$-rule. So we have $\vdash_T \Delta \cup \{\varphi\}$ or $\vdash_T \Delta \cup \{\psi\}$.

Inductively, we know that, given $\mathcal{M}$ and a as before, $\mathcal{M} \models \bigvee(\Delta \cup \{\varphi\})[a]$ or $\mathcal{M} \models \bigvee(\Delta \cup \{\psi\})[a]$. Let's assume the first possibility holds true. If there is some $\chi \in \Delta$ such that $\mathcal{M} \models \chi[a]$, then clearly $\mathcal{M} \models \bigvee(\Delta \cup \{\varphi \vee \psi\})[a]$, so we're fine. Otherwise, we know that $\mathcal{M} \models \varphi[a]$. But by definition of the satisfaction relation, this clearly implies that $\mathcal{M} \models (\varphi \vee \psi)[a]$, which, in turn, implies that $\mathcal{M} \models \bigvee(\Delta \cup \{(\varphi \vee \psi)\})[a]$. The other case is entirely symmetric.

Case 4: $\vdash_T \Delta \cup \{\forall v_m \varphi\}$ because of the $\forall$-rule. I.e., $\vdash_T \Delta \cup \{\varphi(^{v_m}/_{v_n})\}$, where $v_n \notin \mathsf{FV}(\Delta)$.

Let $\mathcal{M}$ and a be as above. So $\mathsf{FV}(\Delta \cup \{\forall v_m \varphi\}) \subseteq \mathrm{dom}(a)$. Inductively, we know that for any $c \in |\mathcal{M}|$,

$$\mathcal{M} \models \bigvee(\Delta \cup \{\varphi(^{v_m}/_{v_n})\})[a(^{v_n}/_c)],$$

since this holds for any assignment. If there is a $\chi \in \Delta$ such that $\mathcal{M} \models \chi[a(^{v_n}/_c)]$, for some c, then since $a(^{v_n}/_c) \sim_\chi a$ (as v_n is not a free variable of χ), it follows that $\mathcal{M} \models \chi[a]$ (by Lemma 3.1.10), and hence $\mathcal{M} \models \bigvee(\Delta \cup \{\forall v_m \varphi\})$. Now assume the contrary. Then for all $c \in |\mathcal{M}|$,

$$\mathcal{M} \models \varphi(^{v_m}/_{v_n})[a(^{v_n}/_c)].$$

This is of course equivalent to saying that for all $c \in |\mathcal{M}|$,

$$\mathcal{M} \models \varphi[a(^{v_m}/_c)].$$

This means precisely that $\mathcal{M} \models \forall v_m \varphi[a]$, as wished.

Case 5: $\vdash_T \Delta \cup \{\exists v_m \varphi\}$ because of the $\exists$-rule. I.e., $\vdash_T \Delta \cup \{\varphi(^{v_m}/_t)\}$, for some $t \in \mathsf{Term}_\mathcal{L}$.

Suppose $\mathcal{M}$, a are arbitrary, as above. Inductively, we know that $\mathcal{M} \models \bigvee(\Delta \cup \{\varphi(^{v_m}/_t)\})[a]$. As usual, if there is a $\chi \in \Delta$ such that $\mathcal{M} \models \chi[a]$, then $\mathcal{M} \models \chi[a]$ and we're done. Otherwise, we know that $\mathcal{M} \models \varphi(^{v_m}/_t)[a]$. This means that $\mathcal{M} \models \varphi[a(^{v_m}/_{t^{\mathcal{M}}(a)})]$. In particular, there is some $c \in |\mathcal{M}|$ such that $\mathcal{M} \models \varphi[a(^{v_m}/_c)]$, namely $c = t^{\mathcal{M}}(a)$. So by definition, this means that $\mathcal{M} \models \exists v_m \varphi[a]$, and in particular, $\mathcal{M} \models \bigvee(\Delta \cup \{\exists v_m \varphi\})$. □

Soundness can be used to prove correctness. Since the traditional Correctness Theorem refers to regular formulas, not Tait formulas, a translation procedure is needed:

Definition 4.1.2. Define a function $\varphi \mapsto \varphi^T$ by induction on formulas as follows:

$$\begin{aligned}
(P(t_0, \ldots, t_{n-1}))^T &:= P(t_0, \ldots, t_{n-1}),\\
(t_0 \dot{=} t_1)^T &:= t_0 \dot{=} t_1,\\
(\neg\varphi)^T &:= \sim(\varphi^T),\\
(\varphi_0 \wedge \varphi_1)^T &:= (\varphi_0^T \wedge \varphi_1^T),\\
(\varphi_0 \vee \varphi_1)^T &:= (\varphi_0^T \vee \varphi_1^T),\\
(\exists v_m \varphi)^T &:= \exists v_m(\varphi^T),\\
(\forall v_m \varphi)^T &:= \forall v_m(\varphi^T).
\end{aligned}$$

Lemma 4.1.3. *Given any $\mathcal{L}$-model $\mathcal{M}$ and any $\mathcal{L}$-formula φ, φ^T is a Tait formula of $\mathcal{L}$ such that for any full assignment a in $\mathcal{M}$,*

$$\mathcal{M} \models \varphi[a] \iff \mathcal{M} \models \varphi^T[a].$$

Proof. Exercise. □

There is an obvious translation procedure in the other direction which will be developed as an exercise, too. So the expressive power of formulas and Tait formulas is the same.

Definition 4.1.4. For a set $\Sigma \subseteq \mathsf{Fml}_\mathcal{L}$, let $\Sigma^T = \{\varphi^T \mid \varphi \in \Sigma\}$. If moreover, ψ is an $\mathcal{L}$-formula, write $\Sigma \vdash \psi$ to mean that $\Sigma^T \vdash \psi^T$.

Theorem 4.1.5 (Correctness)**.** *Let $\Sigma \cup \{\varphi\} \subseteq \mathsf{Fml}_\mathcal{L}$ be a set of formulas. Then*

$$\Sigma \vdash \varphi \implies \Sigma \models \varphi.$$

Proof. Assume $\Sigma \vdash \varphi$, i.e., $\Sigma^T \vdash \varphi^T$. Let Σ_0 be a finite set of formulas each of which is an identity axiom or a member of Σ^T such that $\vdash_T (\sim\Sigma_0 \cup \{\varphi^T\})$. Let $\mathcal{M}$ be a model and a a full assignment such that $\mathcal{M} \models \Sigma[a]$, or, equivalently, $\mathcal{M} \models \Sigma^T[a]$. Since every model satisfies the identity axioms, it follows that $\mathcal{M} \models \Sigma_0[a]$. By soundness, we know that $\mathcal{M} \models \bigvee(\sim\Sigma_0 \cup \{\varphi^T\})[a]$. But since $\mathcal{M} \models \Sigma^T[a]$, there is no $\psi \in \sim\Sigma_0$ such that $\mathcal{M} \models \psi[a]$. So the only possibility is that $\mathcal{M} \models \varphi^T[a]$, or equivalently, $\mathcal{M} \models \varphi[a]$. □

4.2 Completeness

To prove the Completeness Theorem, let $\mathcal{L}$ be a fixed language. Let Σ be a set of $\mathcal{L}$-formulas which is *at most* countable (meaning countable or finite). Fix an enumeration $\vec{\Sigma}$ of Σ. Let us require that there are infinitely many variables that don't occur in any formula from Σ. [1] Let Δ be a finite set of $\mathcal{L}$-formulas. It is then easy to see that there are at most countably many, but infinitely many, terms which can be built up from constants, function symbols occurring in $\Sigma \cup \Delta$, and from arbitrary variables. Let $\vec{t} := \langle t_i \mid i < \omega \rangle$ be an enumeration of these terms, which I shall call the *relevant terms*.

The aim is to show that if $\Sigma \models \bigvee \Delta$, then $\vdash_T \sim\Sigma_0 \cup \Delta$, for some finite $\Sigma_0 \subseteq \Sigma$.[2] This will literally only be true if the identity axioms are part of Σ, but the search tree construction can be carried out without that assumption.

The argument will proceed as follows: Supposing there is no such Σ_0, we will build a tree "searching" for such a Σ_0 and such a derivation. Since by assumption, there is no such Σ_0, the search will be unsuccessful, thus producing an infinite tree. The tree will be locally finite, and hence will have an infinite branch. Such a branch will determine a term model M and a full assignment a such that in M all formulas from Σ hold, while none of the formulas in Δ hold under the assignment a.

To define the tree, view Δ as a finite sequence $\vec{\Delta}$ which lists all (of the finitely many) formulas in Δ in some order. If $\vec{\Gamma}$ is some finite list of formulas, let the *redex* of $\vec{\Gamma}$, $R(\vec{\Gamma})$, be the formula with least index in $\vec{\Gamma}$ which is not atomic, if there is such a formula - otherwise, it is undefined. If it is defined, then $\vec{\Gamma}^r$ will be the sequence of formulas obtained from $\vec{\Gamma}$ by omitting $R(\vec{\Gamma})$. The tree $S := S^{\vec{\Sigma}}_{\vec{\Delta},\vec{t}}$ we are about to construct is a *labeled* tree. We construct it together with a labeling function $\delta : S \to {}^{<\omega}\mathsf{Fml}_{\mathcal{L}}$. The tree will be at most 2-splitting, meaning that every node will have at most two immediate successors. In fact, it will be a tree on the set 2. It will be constructed by recursion on its levels, together with δ. To start off,

($S_\emptyset$) *$\emptyset \in S$ and $\delta(\emptyset) = \vec{\Delta}$.*

Now assume $s \in S$. If $\mathrm{ran}(\delta(s))$ is an axiom according to *tertium non datur* (i.e., there is an atomic formula φ such that $\{\varphi, \sim\varphi\} \subseteq \mathrm{ran}(\delta(s))$), then s has no successors in S.

Now suppose this is not the case. Then it is determined which of $s^\frown 0$ and $s^\frown 1$ are in S, and what the values $\delta(s^\frown 0)$ and $\delta(s^\frown 1)$ are, by the following clauses. For ease of notation, assuming $\delta(s{\restriction}n)$ has been defined for all $n \le \mathrm{dom}(s)$, set $\delta_{\le}(s) = \bigcup_{n \le \mathrm{dom}(s)} \mathrm{ran}(\delta(s{\restriction}n))$.

(S_{id}) *If $R(\delta(s)) = \emptyset$, then $s^\frown 0 \in S$. If there is a formula in Σ whose negation does not occur in $\delta_{\le}(s)$, then let ψ be the one that's mentioned first in the fixed enumeration of Σ, and set $\delta(s^\frown 0) = \delta(s)^\frown{\sim}\psi$. If there is no such formula, then let $\delta(s^\frown 0) = \delta(s)$.*

[1] If only at most finitely many variables don't occur in Σ, then one can replace every occurrence of v_l in $\Sigma \cup \Delta$ with v_{2l}, simultaneously. Denoting the resulting sets by Σ' and Δ', this renaming does not change anything about our assumptions. So if $\Sigma \models \bigvee \Delta$, also $\Sigma' \models \bigvee \Delta'$, and for a finite subset $\Sigma_0 \subseteq \Sigma$, $\vdash_T \sim\Sigma_0 \cup \Delta$ iff $\vdash_T \sim\Sigma_0' \cup \Delta'$, where Σ_0' is the result of renaming the variables occurring in Σ_0 as described. Σ' satisifies our assumption.

[2] Here, I used the notation $\sim\Gamma = \{\sim\varphi \mid \varphi \in \Gamma\}$, for a set Γ of Tait formulas.

($S_\wedge$) *If $R(\delta(s))$ is of the form $(\varphi_0 \wedge \varphi_1)$, then both $s^\frown 0$ and $s^\frown 1$ are in S, and $\delta(s^\frown i) = \delta(s)^{r\frown}\varphi_i$, for $i < 2$.*

($S_\forall$) *If $R(\delta(s))$ is of the form $\forall v_m \varphi$, then $s^\frown 0 \in S$, $s^\frown 1 \notin S$, and $\delta(s^\frown 0) = \delta(s)^{r\frown}\varphi({}^{v_m}/_{v_n})$, where n is least such that v_n does not occur in $\delta(s) \cup \Sigma$.*

($S_\vee$) *If $R(\delta(s))$ is of the form $(\varphi_0 \vee \varphi_1)$, then $s^\frown 0 \in S$ and $s^\frown 1 \notin S$. Let $Y := \delta_{\leq}(s)$. Define $\delta(s^\frown 0)$ to be $\delta(s)^{r\frown}\varphi_0{}^\frown\varphi_1$, if $\varphi_0, \varphi_1 \notin Y$. If $\varphi_0 \in Y$, omit φ_0, and if $\varphi_1 \in Y$, omit φ_1.*

($S_\exists$) *If $R(\delta(s))$ is of the form $\exists v_m \varphi$, then $s^\frown 0 \in S$ and $s^\frown 1 \notin S$. Let t be the first relevant term mentioned in the enumeration such that $\varphi({}^{v_m}/_t) \notin \delta_{\leq}(s)$. Let $x = \delta(s)^{r\frown}\varphi({}^{v_m}/_t)$, otherwise $x = \delta(s)^r$. Further, let χ be the first formula mentioned in the enumeration of Σ such that $\sim\chi \notin \delta_{\leq}(s)$, if such a formula exists. In that case, let $x' = x^\frown{\sim}\chi$, otherwise, $x' = x$. Finally, $\delta(s^\frown 0) = x'^\frown R(\delta(s))$.*

In a way, this tree can be viewed as searching simultaneously for a proof of $({\sim}\Sigma_0) \cup \Delta$, for some finite $\Sigma_0 \subseteq \Sigma$, and (in case this search fails) for a model of $\Sigma \cup \bigwedge {\sim}\Delta$.

Lemma 4.2.1 (Syntactical Main Lemma, Schütte)**.** *If S is well-founded, then for every $s \in S$, there is a finite set $\Sigma_s \subseteq \Sigma$ such that $\vdash_T {\sim}\Sigma_s \cup \mathrm{ran}(\delta(s))$.*

Proof. Suppose this were not the case. Since S is well-founded by assumption, there must be a $>_S$-minimal counterexample (that is, a $<_S$-maximal one).

Case 1. s has no successors in S.

This is only possible if $\mathrm{ran}(\delta(s))$ is an axiom according to *tertium non datur*. So in this case, $\vdash_T \mathrm{ran}(\delta(s))$, which means that $\Sigma_s := \emptyset$ is as wished. So s is no counterexample and this case is excluded.

Case 2. Case 1 fails.

Then we have to distinguish subcases according to the nature of $R(\delta(s))$.

Case 2.1 $R(\delta(s)) = \emptyset$.

Then $s^\frown 0$ is the sole successor of s in S. By minimality, we know that there is a finite subset $\Sigma_{s^\frown 0} \subseteq \Sigma$ such that $\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s^\frown 0))$.

If $X := \Sigma \setminus \delta_{\leq}(s)) \neq \emptyset$, then letting ψ be the member of X that's mentioned first in the fixed enumeration of Σ, $\delta(s^\frown 0) = \delta(s)^\frown{\sim}\psi$. So letting $\Sigma_s := \Sigma_{s^\frown 0} \cup \{\psi\}$, it follows that ${\sim}\Sigma_s \cup \mathrm{ran}(\delta(s)) = {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s^\frown 0))$, so that $\vdash_T {\sim}\Sigma_s \cup \mathrm{ran}(\delta(s))$.

If $X = \emptyset$, then $\delta(s^\frown 0) = \delta(s)$, so setting $\Sigma_s := \Sigma_{s^\frown 0}$ will do.

Case 2.2. $R(\delta(s)) = (\varphi_0 \wedge \varphi_1)$.

In this case, $s^\frown 0$ and $s^\frown 1$ both are successors of s in S, and $\delta(s^\frown 0) = \delta(s)^{r\frown}\varphi_0$, $\delta(s^\frown 1) = \delta(s)^{r\frown}\varphi_1$. So by minimality, we know that there are $\Sigma_{s^\frown 0}$ and $\Sigma_{s^\frown 1}$ such that $\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s)^{r\frown}\varphi_0)$ and $\vdash_T {\sim}\Sigma_{s^\frown 1} \cup \mathrm{ran}(\delta(s)^{r\frown}\varphi_1)$. Let $\Sigma_s = \Sigma_{s^\frown 0} \cup \Sigma_{s^\frown 1}$. Then by monotonicity (the structural rule, saying that if $\vdash_T \Gamma$ and $\Gamma \subseteq \Gamma'$, then $\vdash_T \Gamma'$, which was proven in the exercises), we have that

$$\vdash_T ({\sim}\Sigma_s \cup \mathrm{ran}(\delta(s)^r)) \cup \{\varphi_0\}$$

and

$$\vdash_T ({\sim}\Sigma_s \cup \mathrm{ran}(\delta(s)^r)) \cup \{\varphi_1\}.$$

So by the $\wedge$-rule, it follows that

$$\vdash_T {\sim}\Sigma_s \cup \mathrm{ran}(\delta(s)^r) \cup \{(\varphi_0 \wedge \varphi_1)\}.$$

But $(\varphi_0 \wedge \varphi_1) = R(\delta(s))$, which is omitted in $\delta(s)^r$. So this just means that

$$\vdash_T {\sim}\Sigma_s \cup \mathrm{ran}(\delta(s)),$$

as desired.

Case 2.3 $R(\delta(s)) = \forall v_m \varphi$.

Then $s^\frown 0$ is the only successor of s in S. Moreover, letting n be minimal such that v_n does not occur in $\mathrm{ran}(\delta(s)) \cup \Sigma$, by definition, $\delta(s^\frown 0) = \delta(s)^{r\frown}\varphi({}^{v_m}/_{v_n})$. So by minimality, there is a finite set $\Sigma_{s^\frown 0} \subseteq \Sigma$ such that $\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s)^r) \cup \{\varphi({}^{v_m}/_{v_n})\}$. Since v_n is a new variable, the $\forall$-rule yields that $\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s)^r) \cup \{\forall v_m \varphi\}$, or, in other words, that $\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s))$. So setting $\Sigma_s := \Sigma_{s^\frown 0}$ does the job.

Case 2.4 $R(\delta(s)) = (\varphi_0 \vee \varphi_1)$.

Then $s^\frown 0 \in S$ is the unique successor of s in S. Let $Y := \delta_{\leq}(s)$. Then $\delta(s^\frown 0)$ is $\delta(s)^r$, with φ_0, φ_1 added (depending on whether or not these formulas occur in Y). In any case, since inductively, $\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s^\frown 0))$, it follows by monotonicity that $\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s^\frown 0)) \cup \{\varphi_0\}$, and hence, by the $\vee$-rule (possibly applied twice, in the case that $\varphi_0, \varphi_1 \notin Y$), that $\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s))$. So we can set $\Sigma_s = \Sigma_{s^\frown 0}$.

Case 2.5 $R(\delta(s)) = \exists v_m \varphi$.

Then $s^\frown 0$ is the unique successor of s in S. Let t be the first relevant term mentioned in the enumeration such that $\varphi({}^{v_m}/_t) \notin \delta_{\leq}(s)$. Let $x = \delta(s)^{r\frown}\varphi({}^{v_m}/_t)$. Further, let χ be the first formula mentioned in the enumeration of Σ such that ${\sim}\chi \notin \delta_{\leq}(s)$, if such a formula exists. In that case, let $x' = x^\frown{\sim}\chi$, otherwise, $x' = x$. Finally, $\delta(s^\frown 0) = x'^\frown R(\delta(s))$.

Inductively, we know that there is a finite set $\Sigma_{s^\frown 0} \subseteq \Sigma$ such that $\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \mathrm{ran}(\delta(s^\frown 0))$. This assumption is weakest if both t and χ exist (by the structural rule/monotonicity). So in this case, we have

$$\vdash_T {\sim}\Sigma_{s^\frown 0} \cup \underbrace{\mathrm{ran}(\delta(s)^r) \cup \{R(\delta(s))\}}_{=\delta(s)} \cup \{{\sim}\chi\} \cup \{\varphi({}^{v_m}/_t)\}.$$

So setting $\Sigma_s := \Sigma_{s^\frown 0} \cup \{\chi\}$, this is the same as to say that

$$\vdash_T {\sim}\Sigma_s \cup \mathrm{ran}(\delta(s)) \cup \{\varphi({}^{v_m}/_t)\}$$

(if χ doesn't exist, then taking $\Sigma_s = \Sigma_{s^\frown 0}$ will do). Applying the $\exists$-rule yields

$$\vdash_T {\sim}\Sigma_s \cup \mathrm{ran}(\delta(s)),$$

since $\exists v_m \varphi = R(\delta(s)) \in \mathrm{ran}(\delta(s))$. Again, applying the $\exists$-rule is only necessary if t is defined.

Thus, there is no counterexample, and the lemma is proven. □

The following is an adaptation of the classical lemma, dealing with pure logic, to logic with identity.

Lemma 4.2.2 (Semantical Main Lemma, Schütte)**.** *If S is ill-founded and Σ contains the identity axioms, then there is a model $\mathcal{M}$ and a full assignment a in $\mathcal{M}$ such that $\mathcal{M} \models (\Sigma \cup {\sim}\Delta)[a]$.*

Proof. Let $f : \omega \longrightarrow 2$ be a cofinal branch of S. Let $\delta(f) := \bigcup\{\mathrm{ran}(\delta(f{\restriction}n)) \mid n < \omega\}$. The following properties are crucial:

1. If an atomic formula occurs in $\mathrm{ran}(\delta(f{\restriction}m))$, for some $m < \omega$, then it also occurs in $\mathrm{ran}(\delta(f{\restriction}n))$, for every $n > m$.
2. ${\sim}\Sigma \subseteq \delta(f)$.
3. If a non-atomic formula φ occurs in some $\mathrm{ran}(\delta(f{\restriction}m))$, then there is an $n \geq m$ such that $\varphi = R(\delta(f{\restriction}n))$.

4. If a formula of the form $(\varphi_0 \wedge \varphi_1)$ occurs in $\delta(f)$, then there is an $i < 2$ such that φ_i occurs in $\delta(f)$.

5. If a formula of the form $\forall v_m \varphi$ occurs in $\delta(f)$, then there is a variable v_n such that $\varphi({}^{v_m}/_{v_n})$ occurs in $\delta(f)$.

6. If a formula of the form $(\varphi_0 \vee \varphi_1)$ occurs in $\delta(f)$, then $\{\varphi_0, \varphi_1\} \subseteq \delta(f)$.

7. If a formula of the form $\exists v_m \varphi$ occurs in $\delta(f)$, then $\varphi({}^{v_m}/_t)$ occurs in $\delta(f)$, for every relevant term t.

Let's check these properties: 1 is clear, because atomic formulas are never discarded. Only the redex is sometimes thrown away, and this is never an atomic formula, by definition.

To see 2, note that it cannot be the case that only for finitely many n, $R(f\upharpoonright n)$ is of the form $\exists v_m \varphi$ or undefined. This is because otherwise, there is some n such that for all $m > n$, $R(\delta(f\upharpoonright m))$ either of the form $(\varphi_0 \wedge \varphi_1)$, $\forall v_i \varphi$, or $(\varphi_0 \vee \varphi_1)$, which means that $\delta(f\upharpoonright(m+1))$ is either of the form $\delta(s)^r{}^\frown\varphi_0$, $\delta(s)^r{}^\frown\varphi_1$, $\delta(s)^r$, $\delta(s)^\frown\varphi_0{}^\frown\varphi_1$, or $\delta(s)^r{}^\frown\varphi({}^{v_i}/_{v_j})$. Any formula ψ has at most $2^{|\psi|}$ many subformulas, where $|\psi|$ is the length of ψ - this is of course a ridiculously crude upper bound. It is obvious now that, letting $b = \sum_{\psi \in \mathrm{ran}(\delta(f\upharpoonright n))} 2^{|\psi|}$, the redex of $\delta(f\upharpoonright(n+b))$ would have to be undefined, a contradiction.

Property 3 is clear: Suppose a non-atomic formula φ occurs in $\mathrm{ran}(\delta(f\upharpoonright m))$. If there were no $n \geq m$ such that $R(\delta(f\upharpoonright n)) = \varphi$, then for every $n \geq m$, there would be a non-atomic formula which occurs before the first occurrence of φ in $\delta(f\upharpoonright n)$. But clearly, the number of non-atomic formulas occurring in $\delta(f\upharpoonright n)$ before the first occurrence of φ would have to be strictly decreasing (for $n \geq m$), which is a contradiction.

Property 4 is clear by definition of S.

Property 5 follows from 3: If $\forall v_m \varphi \in \delta(f)$, then let k be such that $\forall v_m \varphi \in \mathrm{ran}(\delta(f\upharpoonright k))$. By 3, there is some $n > k$ such that $R(\delta(f\upharpoonright n)) = \forall v_m \varphi$, and then, by definition, $\varphi({}^{v_m}/_{v_l}) \in \mathrm{ran}(\delta(f\upharpoonright(n+1)))$, for some l.

Properties 6 and 7 are easily checked.

(∗) *If φ is an atomic formula in $\delta(f)$, then $\sim\varphi \notin \delta(f)$.*

Proof of (∗). This is because $\sim\varphi$ is also an atomic formula. Suppose both φ and $\sim\varphi$ were in $\delta(f)$. Once an atomic formula is in $\delta(f\upharpoonright m)$, it stays in (meaning it is in $\delta(f\upharpoonright n)$, for all $n > m$). So pick n large enough so that $\{\varphi, \sim\varphi\} \subseteq \delta(f\upharpoonright n)$. Then $\mathrm{ran}(\delta(f\upharpoonright n))$ is a tertium non datur axiom, so that $f\upharpoonright n$ is a terminal node of S, and hence, f can't be a cofinal branch. $\square_{(*)}$

Now define a relation $\equiv$ on relevant terms:

$$t_0 \equiv t_1 \iff t_0 \dot{\neq} t_1 \in \delta(f).$$

This is an equivalence relation:

Reflexivity: Since $\forall v_0 (v_0 = v_0)$ is an identity axiom, this formula is in Σ, so $\sim\forall v_0(v_0 = v_0) = \exists v_0(v_0 \neq v_0) \in \sim\Sigma \subseteq \delta(f)$, by 2. But then by 7, it follows that $t \neq t \in \delta(f)$, in other words, that $t \equiv t$.

The proofs of *symmetry* and *transitivity* follow the same pattern and are left to the reader.

Moreover, $\equiv$ is a "congruence" relation over the predicates:

$(C1)$ *If $P \in \mathbb{P} \cup \bar{\mathbb{P}}$ with $\#(P) = n$, $s_0, \ldots, s_{n-1}$ and $t_0, \ldots, t_{n-1}$ are relevant terms with $s_i \equiv t_i$, for all $i < n$, then $\sim P(\vec{s}) \in \delta(f)$ iff $\sim P(\vec{t}) \in \delta(f)$.*

Proof. Suppose $\sim P(\vec{s}) \in \delta(f)$. By assumption, $s_i \dot{\neq} t_i \in \delta(f)$, for all $i < n$. Moreover, the Tait negation of the adequate identity axiom (of the category "congruence over predicates") is in $\sim\Sigma$, and hence in $\delta(f)$:

$$\exists v_0 \exists v_1 \ldots \exists v_{n-1} \exists v_n \exists v_{n+1} \ldots \exists v_{2n-1} \qquad (((v_0 = v_n) \wedge (v_1 = v_{n+1}) \wedge \ldots \wedge (v_{n-1} = v_{2n-1})) \wedge (P(v_0, v_1, \ldots, v_{n-1}) \wedge \sim P(v_n, v_{n+1}, \ldots, v_{2n-1}))).$$

By property 7, the following "instance" of this formula is in $\delta(f)$:

$$(s_0 = t_0 \wedge s_1 = t_n \wedge \ldots \wedge s_{n-1} = t_{n-1} \wedge P(s_0, s_1, \ldots, s_{n-1}) \wedge \sim P(t_0, t_1, \ldots, t_{n-1})).$$

By property 4, at least one conjunct of this formula must be in $\delta(f)$. By assumption $s_i \dot{\neq} t_i \in \delta(f)$, for all $i < n$, so that by $(*)$, $s_i \doteq t_i \notin \delta(f)$. Analogously, $\sim P(s_0, s_1, \ldots, s_{n-1}) \in \delta(f)$ by assumption, so that $P(s_0, s_1, \ldots, s_{n-1}) \notin \delta(f)$. So the only possibility that's left is that $\sim P(t_0, t_1, \ldots, t_{n-1}) \in \delta(f)$, which is what we want. The converse is proven analogously.

One has to use the corresponding identity axiom of the category "congruence over functions" for the following claim:

$(C2)$ *If $F \in \mathbb{F}$ with $\#(F) = n$ and $s_0, \ldots, s_{n-1}$ and $t_0, \ldots, t_{n-1}$ are relevant terms with $s_i \equiv t_i$, for all $i < n$, then $F(\vec{s}) \equiv F(\vec{t})$.*

Now I'm ready to define the desired model $\mathcal{M}$: Let $|\mathcal{M}|$ consist of the $\equiv$-equivalence classes of relevant terms. So, writing $[t]$ for the $\equiv$-equivalence class of the relevant term t,

$$|\mathcal{M}| = \{[t] \mid t \text{ is a relevant term}\}.$$

Set:

$$\begin{array}{rcl} F^{\mathcal{M}}([t_0], \ldots, [t_{n-1}]) & = & [F(t_0, \ldots, t_{n-1})], \text{ for } F \in \mathbb{F} \text{ such that } F \text{ occurs in } \Sigma \cup \Delta, \\ \langle [t_0], \ldots, [t_{n-1}] \rangle \in P^{\mathcal{M}} & \iff & \sim P(t_0, \ldots, t_{n-1}) \in \delta(f), \text{ for } P \in \mathbb{P}, \\ c^{\mathcal{M}} & = & [c], \text{ for relevant } c \in \mathbb{C}. \end{array}$$

The interpretation of function symbols and constant symbols which don't occur in $\Sigma \cup \Delta$ is irrelevant and can be prescribed in some simple, arbitrary way.

The correctness of these definitions follows from $(C1)$ and $(C2)$. Define a full assignment a in $\mathcal{M}$ in the obvious way:

$$a(v_m) := [v_m].$$

It follows by induction on terms t that

$$t^{\mathcal{M}}(a) = [t].$$

Further, it follows by induction on formulas φ that:

(D) $\sim\varphi \in \delta(f) \implies \mathcal{M} \models \varphi[a]$.

Starting with the atomic case: If $\varphi = P(t_0, \ldots, t_n)$, where $P \in \mathbb{P}$ and $\sim\varphi \in \delta(f)$, then by definition, $\mathcal{M} \models P([t_0], \ldots, [t_{n-1}])$, which means precisely that $\mathcal{M} \models P(t_0, \ldots, t_{n-1})[a]$, by the previous remark. This argument works for the case $P = \doteq$ as well. Now assume $\varphi = \bar{P}(t_0, \ldots, t_{n-1})$, and $\sim\varphi \in \delta(f)$. By $(*)$, $\varphi \notin \delta(f)$. So $\sim P(t_0, \ldots, t_{n-1}) \notin \delta(f)$, which means that by definition of $P^{\mathcal{M}}$, $\langle [t_0], \ldots, [t_{n-1}] \rangle \notin P^{\mathcal{M}}$. So by definition, $\langle [t_0], \ldots, [t_{n-1}] \rangle \in \bar{P}^{\mathcal{M}}$, or, in other words, $\mathcal{M} \models \bar{P}(t_0, \ldots, t_{n-1})[a]$. Again, this argument works for $P = \doteq$ as well.

In the rest of the argument, the properties 4-7 will be used.

So suppose $\sim(\varphi_0 \vee \varphi_1) \in \delta(f)$. By the definition of Tait-negation, this means that $(\sim\varphi_0 \wedge \sim\varphi_1) \in \delta(f)$. By property 4, let $i < 2$ be such that $\sim\varphi_i \in \delta(f)$. Inductively, we know that $\mathcal{M} \models \varphi_i[a]$. But then $\mathcal{M} \models (\varphi_0 \vee \varphi_1)[a]$ also.

Now assume that $\sim\exists v_m \varphi \in \delta(f)$, which means that $\forall v_m \sim\varphi \in \delta(f)$. By 5, pick v_n such that $\sim\varphi({}^{v_m}/_{v_n}) \in \delta(f)$. Inductively, $\mathcal{M} \models \varphi({}^{v_m}/_{v_n})[a]$. In particular, $\mathcal{M} \models \exists v_m \varphi[a]$.

If $\sim(\varphi_0 \wedge \varphi_1) \in \delta(f)$, then this means that $(\sim\varphi_0 \vee \sim\varphi_1) \in \delta(f)$, and by 6, this, in turn, means that both $\sim\varphi_0$ and $\sim\varphi_1$ are in $\delta(f)$, so that inductively, $\mathcal{M} \models \varphi_0[a]$ and $\mathcal{M} \models \varphi_1[a]$. This means, of course, that $\mathcal{M} \models (\varphi_0 \wedge \varphi_1)[a]$.

If $\sim\forall v_m \varphi \in \delta(f)$, i.e., $\exists v_m \sim\varphi \in \delta(f)$, then by 7, $\sim\varphi({}^{v_m}/_t) \in \delta(f)$, for every relevant term t. So inductively, $\mathcal{M} \models \varphi({}^{v_m}/_t)[a]$, for every relevant term t. In other words, $\mathcal{M} \models \varphi[a({}^{v_m}/_{t^{\mathcal{M}}(a)})]$, for every relevant term t (this is a general fact that can easily be shown by induction on terms). But since $t^{\mathcal{M}}(a) = [t]$, and $|\mathcal{M}|$ consists precisely of such $[t]$, this previous statement can be rephrased as saying that $\mathcal{M} \models \varphi[a({}^{v_m}/_b)]$, for every $b \in |\mathcal{M}|$. This means that $\mathcal{M} \models \forall v_m \varphi[a]$, as wished.

Now it is an immediate consequence that $\mathcal{M} \models \Sigma[a]$, since if $\varphi \in \Sigma$, i.e., $\sim\varphi \in \sim\Sigma \subseteq \delta(f)$ (by property 2), it follows from (D) that $\mathcal{M} \models \varphi[a]$. To see that $\mathcal{M} \models \sim\Delta$, note that $\Delta = \mathrm{ran}(\delta(f{\restriction}0)) \subseteq \delta(f)$. So given $\varphi \in \Delta$, $\sim(\sim\varphi) \in \delta(f)$, so that by (D), $\mathcal{M} \models \sim\varphi[a]$. □

Theorem 4.2.3 (Completeness)**.** *Let Σ be a countable set of $\mathcal{L}$-formulas and φ be a formula such that $\Sigma \models \varphi$. Then $\Sigma \vdash \varphi$.*

Proof. We may assume only variables with even index occur in $\Sigma \cup \{\varphi\}$. Having said this, the reader may forget about this technicality, see the beginning of the definition of the search tree. Also, replace Σ by $\Sigma^T = \{\varphi^T \mid \varphi \in \Sigma\}$ and φ by φ^T, so that we are actually dealing with Tait formulas. Let Σ^* be Σ, together with the identity axioms.

Let $\vec{t}$ enumerate the at most countably many terms which can be built up using constants and function symbols occurring in $\Sigma^* \cup \{\varphi\}$, and variables, the relevant terms. Fix also an enumeration $\vec{\Sigma^*}$ of Σ^*. Let $S = S^{\vec{\Sigma^*}}_{\{\varphi\},\vec{t}}$, δ be the search tree determined by these objects, together with its labeling function.

S must be well-founded: Otherwise, it is ill-founded, so that the Semantical Main Lemma 4.2.2 applies, giving a model $\mathcal{M}$ and a full assignment a with $\mathcal{M} \models (\Sigma^* \cup \{\sim\varphi\})[a]$, which contradicts the assumption that $\Sigma \models \varphi$. So S is well-founded, which means that the Syntactical Main Lemma 4.2.1 applies. This gives, for every $s \in S$, a finite set $\Sigma^*_s \subseteq \Sigma^*$ such that $\vdash_T \sim\Sigma_s \cup \mathrm{ran}(\delta(s))$. For $s = \emptyset$, this means: $\Sigma^*_\emptyset \subseteq \Sigma^*$ is finite and $\vdash_T \sim\Sigma^*_0 \cup \{\varphi^T\}$, where Σ^*_0 is a finite set of formulas each of which is an identity axiom or a member of Σ^T. By definition, this means that $\Sigma \vdash \varphi$. □

4.3 Compactness

Work in a fixed countable language.

Theorem 4.3.1. *If $\Sigma \models \varphi$, then there is a finite $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \models \varphi$.*

Proof. By the completeness theorem, $\Sigma \vdash \varphi$. This means there is a finite set $\Sigma_0 \subseteq \Sigma$ and a finite set Γ of identity axioms such that $\vdash_T \sim(\Sigma_0 \cup \Gamma) \cup \{\varphi\}$. By correctness, this means that $\Sigma_0 \cup \Gamma \models \varphi$. But since every model satisfies the identity axioms, as the identity symbol is always interpreted by the true identity relation, this implies that $\Sigma_0 \models \varphi$. □

Definition 4.3.2. Let Σ be a set of formulas. Σ is *consistent*, $\mathsf{con}(\Sigma)$, is the statement that there is a formula φ such that it is not the case that $\Sigma \vdash \varphi$.

Σ *has a model* if there is a model $\mathcal{M}$ and a full assignment a in $\mathcal{M}$ such that $\mathcal{M} \models \Sigma[a]$.

Theorem 4.3.3. *A set Σ of formulas is consistent if and only if it has a model.*

Proof. Suppose Σ is not consistent. Then for every φ, $\Sigma \vdash \varphi$. If there were a model of Σ, witnessed by $\mathcal{M}$ and a, then it would follow that $\mathcal{M} \models \varphi[a]$, for every φ, by correctness. This is of course a contradiction, since it would follow that $\mathcal{M} \models \varphi[a]$ and $\mathcal{M} \models \neg\varphi[a]$, which means that $\mathcal{M} \not\models \varphi[a]$. Vice versa, if there is no model of Σ, then $\Sigma \models \varphi$, for any formula φ, by fiat. So by completeness, $\Sigma \vdash \varphi$. □

Theorem 4.3.4. *If every finite subset of Σ has a model, then Σ has a model.*

Proof. Suppose Σ has no model. Then Σ is inconsistent. Let φ be a sentence. Then $\Sigma \vdash \varphi$ and $\Sigma \vdash \neg\varphi$. So there is a finite subset Σ_0 of Σ such that $\Sigma_0 \vdash \varphi$ and $\Sigma_0 \vdash \neg\varphi$; I tacitly used the monotonicity of the deductive calculus here, namely that if $\Gamma_0 \subseteq \Gamma_1$ and $\Gamma_0 \vdash \psi$, then $\Gamma_1 \vdash \psi$. It follows that Σ_0 has no model, a contradiction. □

4.4 Ultrafilters and Ultraproducts

In this section, I'll develop a useful tool for constructing models. As a motivation, suppose $\langle \mathcal{M}_i \mid i \in I \rangle$ is a sequence of models of a (not necessarily countable) fixed language $\mathcal{L}$. We want to construct a model $\mathcal{M}$ such that a sentence φ is true in $\mathcal{M}$ if "for almost every $i \in I$", φ is true in $\mathcal{M}_i$. The first step is to make the meaning of "for almost every $i \in I$" precise. This is done using the concept of ultrafilters.

4.4.1 Filters and ultrafilters

Definition 4.4.1. Let $I \neq \emptyset$ be a set. A *filter* on I is a set F of subsets of I with the following properties:

1. $\emptyset \notin F$, $I \in F$.
2. If $X \in F$ and $X \subseteq Y \subseteq I$, then $Y \in F$.
3. If $X, Y \in F$, then $X \cap Y \in F$.

A filter F on I is an *ultrafilter* on I if in addition, for every $X \subseteq I$, $X \in F$ or $I \setminus X \in F$.

F is a principal filter on I if there is an $i \in I$ such that $F = \{X \subseteq I \mid i \in X\}$. Clearly, a principal filter is an ultrafilter on I.

Lemma 4.4.2. *Let F be a filter on I. Then the following are equivalent:*

1. *F is an ultrafilter on I.*
2. *There is no filter G on I with $F \subsetneq G$. (I.e., F is a maximal filter.)*

Proof. 1. $\Longrightarrow$ 2.: Suppose there were such a G, Pick $X \in G \setminus F$. Since F is ultra, $I \setminus X \in F$. Since $F \subseteq G$, $I \setminus X \in G$. So $\emptyset = X \cap (I \setminus X) \in G$, a contradiction.

2. $\Longrightarrow$ 1.: Let $X \subseteq I$. Suppose neither $X \in F$ nor $(I \setminus X) \in F$. Let $G = \{Y \subseteq I \mid \exists Z \in F \quad Z \cap X \subseteq Y\}$. Obviously, $F \subseteq G$. Also, $X \in G \setminus F$. But G is a filter: $I \in G$, since $I \in F \subseteq G$.

Suppose $\emptyset \in G$. Then pick $Z \in F$ such that $Z \cap X = \emptyset$. This means that $Z \subseteq (I \setminus X)$. Since $Z \in F$, it would follow that $I \setminus X \in F$, a contradiction.

Let $Y_0, Y_1 \in G$. We have to see that $Y_0 \cap Y_1 \in G$. Pick $Z_0, Z_1 \in F$ such that $X \cap Z_0 \subseteq Y_0$, $X \cap Z_1 \subseteq Y_1$. Then $X \cap (Z_0 \cap Z_1) \subseteq (Y_0 \cap Y_1)$, and since F is a filter, $Z_0 \cap Z_1 \in F$. So $Y_0 \cap Y_1 \in G$.

Finally, it's obvious that if $Y_0 \in G$ and $Y_0 \subseteq Y_1 \subseteq I$, it follows that $Y_1 \in G$. For if Z witnesses that $Y_0 \in G$, then it also witnesses that $Y_1 \in G$.

So altogether, we have that $F \subsetneqq G$, and G is a filter on I, a contradiction. □

Theorem 4.4.3 (Ultrafilter Theorem, ZFC)**.** *Suppose $I \neq \emptyset$ and F is a filter on I. Then there is an ultrafilter U on I such that $F \subseteq U$.*

Proof. Let F be given. Consider the partial order P consisting of all filters on I which contain F, ordered by inclusion. This is obviously a partial order in the strict sense. Moreover, it is chain-closed: If $C \subseteq |P|$ is a chain, then $\bigcup C$ is a filter: Clearly, $I \in \bigcup C$. $\emptyset \notin \bigcup C$, since $\emptyset \notin H$, for any $H \in C$. Given $X, Y \in \bigcup C$, there is *one* $H \in C$ with $X, Y \in H$ (here it is crucial that C is a chain!). Hence, $X \cap Y \in H$, and so, $X \cap Y \in \bigcup C$. Finally, if $X \in \bigcup C$ and $X \subseteq Y \subseteq I$, then there is $H \in C$ with $X \in H$, so $Y \in H$, so $Y \in \bigcup C$. So by Zorn's lemma, there is a maximal member of P, and by the previous lemma, this maximal member is an ultrafilter on I. □

4.4.2 Ultraproducts

Definition 4.4.4. Let $\langle \mathcal{M}_i \mid i \in I \rangle$ be a sequence of models of a fixed language $\mathcal{L}$. Then $\prod_{i\in I} |\mathcal{M}_i|$ is the set of functions f with domain I such that for all $i \in I$, $f(i) \in |\mathcal{M}_i|$.

Given a formula φ with free variables $v_{m_0}, v_{m_1}, \ldots, v_{m_{n-1}}$ (in increasing order) and functions $f_0, \ldots, f_{n-1} \in \prod_{i\in I} |\mathcal{M}_i|$, let

$$||\varphi[f_0, \ldots, f_{n-1}]|| = \{i \in I \mid \mathcal{M}_i \models \varphi[f_0(i), \ldots, f_{n-1}(i)]\}.$$

Let F be a filter on I. Given f, $g \in \prod_{i\in I} |\mathcal{M}_i|$, define

$$f \sim_F g \iff \{i \in I \mid f(i) = g(i)\} \in F.$$

So $f \sim_F g$ iff $||f = g|| \in F$.

Lemma 4.4.5. *In the situation of the previous definition, if P is an n-ary predicate symbol (including the possibility that $P = \dot{=}$), then for any $f_0, \ldots, f_{n-1}$, $g_0, \ldots, g_{n-1} \in \prod_{i\in I} |\mathcal{M}_i|$ with $f_0 \sim_F g_0, \ldots, f_{n-1} \sim_F g_{n-1}$, it follows that*

$$||P[f_0, \ldots, f_{n-1}]|| \in F \iff ||P[g_0, \ldots, g_{n-1}]|| \in F.$$

Proof. The situation is symmetric, so it suffices to prove the direction from left to right. Let $X = ||P[f_0, \ldots, f_{n-1}]|| \cap ||f_0 = g_0|| \cap \ldots \cap ||f_{n-1} = g_{n-1}||$. Since F is a filter, $X \in F$. For $i \in X$, since $i \in ||P[f_0, \ldots, f_{n-1}]||$, it follows that $\mathcal{M}_i \models P[f_0(i), \ldots, f_{n-1}(i)]$. Since $i \in ||f_0 = g_0|| \cap \ldots \cap ||f_{n-1} = g_{n-1}||$, it follows that $f_0(i) = g_0(i), \ldots, f_{n-1}(i) = g_{n-1}(i)$. So $\mathcal{M}_i \models P[g_0(i), \ldots, g_{n-1}(i)]$. This means that $i \in ||P[g_0, \ldots, g_{n-1}||$. So $X \in F$, $X \subseteq ||P[g_0, \ldots, g_{n-1}||$, which shows that $||P[g_0, \ldots, g_{n-1}]|| \in F$, as claimed. □

Analogously:

Lemma 4.4.6. *If H is an n-ary function symbol, then for any $f_0, \ldots, f_{n-1}$, $g_0, \ldots, g_{n-1} \in \prod_{i\in I} |\mathcal{M}_i|$ with $f_0 \sim_F g_0, \ldots, f_{n-1} \sim_F g_{n-1}$, it follows that*

$$||H(f_0, \ldots, f_{n-1}) = H(g_0, \ldots, g_{n-1})|| \in F,$$

meaning that the set of i with $H^{\mathcal{M}_i}(f_0(i), \ldots, f_{n-1}(i)) = H^{\mathcal{M}_i}(g_0(i), \ldots, g_{n-1}(i))$ is in F.

Moreover, $\sim_F$ is an equivalence relation on $\prod_{i\in I}|\mathcal{M}_i|$: Given $f,g,h\in\prod_{i\in I}|\mathcal{M}_i|$, it follows that $f\sim_F f$, since $||f=f||=I\in F$, $f\sim_F g \implies g\sim_F f$, since $||f=g||=||g=f||$, and if $f\sim_F g$ and $g\sim_F h$, it follows that $||f=g||\cap||g=h||\subseteq||f=h||\in F$, so that $f\sim_F h$. This, together with the previous lemma, allows us to turn $\prod_{i\in I}|\mathcal{M}_i|$ into a model, giving the correctness of the following definition.

Definition 4.4.7. In the notation of the previous definition, define a model $\mathcal{M}:=\prod_{i\in I}\mathcal{M}_i/F$ as follows. $|\mathcal{M}|$ consists of the $\sim_F$-equivalence classes of functions $f\in\prod_{i\in I}|\mathcal{M}_i|$. Write $[f]_F$ for the $\sim_F$-equivalence class of f. Then the interpretations of the symbols in $\mathcal{M}$ are given by:

$$\begin{aligned}
c^{\mathcal{M}} &:= [\langle c^{\mathcal{M}_i}\mid i\in I\rangle]_F,\ \text{for } c\in\mathbb{C},\\
\langle[f_0]_F,\ldots,[f_{n-1}]_F\rangle\in P^{\mathcal{M}} &\iff ||P[f_0,\ldots,f_{n-1}]||\in F,\ \text{for } P\in\mathbb{P} \text{ with } \#(P)=n,\\
F^{\mathcal{M}}([f_0]_F,\ldots,[f_{n-1}]_F) &= [\langle F^{\mathcal{M}_i}(f_0(i),\ldots,f_{n-1}(i))\mid i\in I\rangle]_F.
\end{aligned}$$

The following is the *Hauptsatz* on ultraproducts.

Theorem 4.4.8 (Łoś)**.** *Let $\langle\mathcal{M}_i\mid i\in I\rangle$ be a sequence of models of a fixed language $\mathcal{L}$, $I\neq\emptyset$. Let U be an ultrafilter on I. Let φ be an $\mathcal{L}$-formula with free variables $v_{m_0},\ldots,v_{m_{n-1}}$ (in increasing order) and let $f_0,\ldots,f_{n-1}\in\prod_{i\in I}|\mathcal{M}_i|$. Then*

$$\left(\prod_{i\in I}\mathcal{M}_i/U\models\varphi[[f_0]_U,\ldots,[f_{n-1}]_U]\right)\iff(||\varphi[f_0,\ldots,f_{n-1}]||\in U).$$

Proof. Set $\mathcal{M}:=\prod_{i\in I}\mathcal{M}_i/U$.

First, one shows by a straightforward induction on terms t that if $\vec{f}\sim_U\vec{g}$, it follows that $[\langle t^{\mathcal{M}_i}(\vec{f}(i))\rangle]_U=[\langle t^{\mathcal{M}_i}(\vec{g}(i))\rangle]_U$. Knowing this, the theorem is now proved by induction on φ. It's clear for atomic formulas.

Now consider the case $\varphi=(\varphi_0\wedge\varphi_1)$. Then

$$\begin{aligned}
\mathcal{M}\models\varphi[[f_0]_U,\ldots,[f_{n-1}]_U] &\iff \mathcal{M}\models\varphi_0[[f_0]_U,\ldots,[f_{n-1}]_U] \text{ and } \mathcal{M}\models\varphi_1[[f_0]_U,\ldots,[f_{n-1}]_U]\\
&\iff ||\varphi_0[f_0,\ldots,f_{n-1}]||\in U \text{ and } ||\varphi_0[f_0,\ldots,f_{n-1}]||\in U\\
&\iff ||\varphi_0[f_0,\ldots,f_{n-1}]||\cap||\varphi_0[f_0,\ldots,f_{n-1}]||\in U\\
&\iff ||(\varphi_0\wedge\varphi_1)[f_0,\ldots,f_{n-1}]||\in U\\
&\iff ||\varphi[f_0,\ldots,f_{n-1}]||\in U
\end{aligned}$$

The $\vee$-step is similar, with one little additional argument: The first relevant observation is that $||(\varphi_0\vee\varphi_1)[f_0,\ldots,f_{n-1}]||=||\varphi_0[f_0,\ldots,f_{n-1}]||\cup||\varphi_1[f_0,\ldots,f_{n-1}||$. The additional argument is that if $X\cup Y\in U$, then $X\in U$ or $Y\in U$. The reason is that if both possibilities failed, it would follow that both $I\setminus X\in U$ and $I\setminus Y\in U$, since U is an *Ultra*filter. So $(I\setminus X)\cap(I\setminus Y)=I\setminus(X\cup Y)\in U$. But then $\emptyset=(X\cup Y)\cap I\setminus(X\cup Y)\in U$, a contradiction.

It becomes more obvious how the ultrafilter property of U is used in the $\neg$-step (and actually, since $(\varphi_0\vee\varphi_1)$ is equivalent to $\neg(\neg\varphi_0\wedge\neg\varphi_1)$, the $\vee$-step can be reduced to the $\wedge$-step and the $\neg$-step). We get:

$$\begin{aligned}
\mathcal{M}\models\neg\varphi[[f_0]_U,\ldots,[f_{n-1}]_U] &\iff \mathcal{M}\not\models\varphi[[f_0]_U,\ldots,[f_{n-1}]_U]\\
&\iff ||\varphi[f_0,\ldots,f_{n-1}]||\notin U\\
&\iff I\setminus||\varphi[f_0,\ldots,f_{n-1}]||\in U\\
&\iff ||\neg\varphi[f_0,\ldots,f_{n-1}]||\in U.
\end{aligned}$$

The ∃-step is of interest, since the axiom of choice is needed here. Consider a formula of the form $\exists v_m\varphi$, where wlog m is larger than the index of all the free variables of that formula.

$$\begin{aligned}\mathcal{M} \models \exists v_m\varphi[f_1,\ldots,f_{n-1}] &\iff \text{there is a } [f]_U \in |\mathcal{M}| \text{ such that } \mathcal{M} \models \varphi[[f_0]_U,\ldots,[f_{n-1}]_U,[f]_U] \\ &\iff \text{there is an } f \in \prod_{i\in I}|\mathcal{M}_i| \text{ such that } \underbrace{||\varphi[f_0,\ldots,f_{n-1},f]||}_{\subseteq||\exists v_m\varphi[f_0,\ldots,f_{n-1}]||} \in U. \\ &\implies ||\exists v_m\varphi[f_0,\ldots,f_{n-1}]|| \in U.\end{aligned}$$

For the converse, assume $X := ||\exists v_m\varphi[f_0,\ldots,f_{n-1}]|| \in U$. For $i \in X$, the set

$$X_i := \{c \in |\mathcal{M}_i| \mid \mathcal{M}_i \models \varphi[f_0(i),\ldots,f_{n-1}(i),c]\}$$

is nonempty. For $i \notin X$, let $X_i = |\mathcal{M}_i|$. By the axiom of choice, there is a function $f : I \longrightarrow \prod_{i\in I} X_i$. I.e., for all $i \in I$, $f(i) \in |\mathcal{M}_i|$, and if $i \in X$, then $f(i) \in X_i$. Then clearly, $X = ||\varphi[f_0,\ldots,f_{n-1},f]|| \in U$, which, by induction hypothesis, means that $\mathcal{M} \models \varphi[[f_0]_U,\ldots,[f_{n-1}]_U,[f]_U]$. So in particular, $\mathcal{M} \models \exists v_m\varphi[[f_0]_U,\ldots,[f_{n-1}]_U]$.

The remaining case, $\forall v_m\varphi$, can in principle be reduced to $\neg\exists v_m\neg\varphi$, and is left to the reader. □

4.4.3 Compactness revisited

Here is a direct proof of the general version of the compactness theorem, in which it is not necessary to assume that the language is countable.

Theorem 4.4.9 (Compactness Theorem, AC)**.** *If Σ is a set formulas of a fixed language such that every finite subset of Σ has a model. Then Σ has a model.*

Proof. Let I be the collection of finite subsets of Σ. For $\sigma \in I$, let $\mathcal{M}_\sigma$ be a model and a_σ a full assignment in $\mathcal{M}_\sigma$ with $\mathcal{M}_\sigma \models \sigma[a_\sigma]$. For $\sigma \in I$, let

$$\langle\sigma\rangle = \{\tau \in I \mid \sigma \subseteq \tau\}.$$

Clearly, for $\sigma, \tau \in I$, it follows that

$$\langle\sigma\rangle \cap \langle\tau\rangle = \langle\sigma \cup \tau\rangle.$$

Let

$$F = \{X \subseteq I \mid \exists\sigma \in I \quad \langle\sigma\rangle \subseteq X\}.$$

It follows that F is a filter (it's the filter generated by $\{\langle\sigma\rangle \mid \sigma \in I\}$). For example, $\emptyset \notin F$, since if $X \in F$, there is a $\sigma \in I$ s.t. $\sigma \in \langle\sigma\rangle \subseteq X$. To see that if $X, Y \in F$, then also $X \cap Y \in F$, pick $\sigma, \tau \in I$ s.t. $\langle\sigma\rangle \subseteq X$, $\langle\tau\rangle \subseteq Y$. Then $\langle\sigma \cup \tau\rangle = \langle\sigma\rangle \cap \langle\tau\rangle \subseteq X \cap Y \in F$. By the ultrafilter theorem, let $U \supseteq F$ be an ultrafilter on I. Let

$$\mathcal{M} := \prod_{\sigma\in I} \mathcal{M}_\sigma/U.$$

For a variable v_n, define $a_{v_n} \in \prod_{\sigma\in I}|\mathcal{M}_\sigma|$ by:

$$a_{v_n}(\sigma) = a_\sigma(v_n).$$

Define a full assignment a in $\mathcal{M}$ by:

$$a(v_n) := [a_{v_n}]_U.$$

It follows that $\mathcal{M} \models \Sigma[a]$: Let $\varphi \in \Sigma$, where φ has the free variables $v_{m_0}, \ldots, v_{m_{n-1}}$ (in increasing enumeration). Then for all $\sigma \in I$ with $\varphi \in \sigma$, $\mathcal{M}_\sigma \models \varphi[a_\sigma]$, which means that $\mathcal{M}_\sigma \models \varphi[a_\sigma(v_{m_0}), \ldots, a_\sigma(v_{m_{n-1}})]$. So $\langle\{\varphi\}\rangle \subseteq ||\varphi[a_{v_{m_0}}, \ldots, a_{v_{m_{n-1}}}]||$. By the construction of U, $\langle\{\varphi\}\rangle \in U$, so $||\varphi[a_{v_{m_0}}, \ldots, a_{v_{m_{n-1}}}]|| \in U$, which means (by the Łoś Theorem) that $\mathcal{M} \models \varphi[[a_{v_{m_0}}]_U, \ldots, [a_{v_{m_{n-1}}}]_U]$. Since $a(v_{m_i}) = [a_{v_{m_i}}]_U$, this means precisely that $\mathcal{M} \models \varphi[a]$. □

This theorem has the general completeness theorem as a consequence:

Theorem 4.4.10 (Completeness, AC)**.** *Assume* $\Sigma \models \varphi$*, where* $\Sigma \cup \{\varphi\}$ *is a set of formulas in an arbitrary fixed language. Then* $\Sigma \vdash \varphi$*.*

Proof. By the general compactness theorem, there is a finite set $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \models \varphi$. For otherwise, every finite subset of $\Sigma \cup \{\neg\varphi\}$ would have a model, which by compactness would mean that $\Sigma \cup \{\neg\varphi\}$ has a model, but this would contradict the assumption that $\Sigma \models \varphi$. Now we can apply the completeness theorem to Σ_0, yielding $\Sigma_0 \vdash \varphi$, in particular, $\Sigma \vdash \varphi$. □

Chapter 5

Incompleteness

This exposition of incompleteness phenomena follows [End72].

5.1 Arithmetic with Exponentiation and Representability

The language of number theory is given by: $\mathbb{C} = \{0\}$, $\mathbb{P} = \{<\}$, $\mathbb{F} = \{S, +, \cdot, E\}$, $\#(<) = 2$, $\#(S) = 1$, $\#(+) = 2$, $\#(\cdot) = 2$, $\#(E) = 2$.

I will use infix notation for the function symbols $+$ and $\cdot$, and for the predicate symbol $<$. Of course, the canonical model for this language is $\mathfrak{N} := \langle \omega, 0, <, S, +, \cdot, E \rangle$ where S is the successor function and E is exponentiation of natural numbers. We will use a fragment of the theory of this model, i.e., a subset of the set of sentences true in $\mathfrak{N}$. Following [End72], this fragment is called A_E. It consists of the following axioms:

(S1) $\forall v_0 \quad \neg S(v_0) = 0$

(S2) $\forall v_0 \forall v_1 \quad (S(v_0) = S(v_1) \to v_0 = v_1)$

(L1) $\forall v_0 \forall v_1 (v_0 < S(v_1) \leftrightarrow (v_0 < v_1 \vee v_0 = v_1))$

(L2) $\forall v_0 \quad \neg v_0 < 0$

(L3) $\forall v_0 \forall v_1 (v_0 < v_1 \vee v_0 = v_1 \vee v_1 < v_0)$

(A1) $\forall v_0 \quad v_0 + 0 = v_0$

(A2) $\forall v_0 \forall v_1 \quad (v_0 + S(v_1) = S(v_0 + v_1))$

(M1) $\forall v_0 \quad v_0 \cdot 0 = 0$

(M2) $\forall v_0 \forall v_1 \quad (v_0 \cdot S(v_1) = (v_0 \cdot v_1) + v_0)$

(E1) $\forall v_0 \quad E(v_0, 0) = S(0)$

(E2) $\forall v_0 \forall v_1 \quad E(v_0, S(v_1)) = E(v_0, v_1) \cdot v_0$

For every natural number n, there is a canonical name in the language of A_E, namely $S^n(0)$. This is called the numeral for n, and I'll write $\dot{n}$ for it.

Definition 5.1.1. A relation $R \subseteq \omega^n$ is *represented* by a a formula $\varphi(v_0, \ldots, v_{n-1})$ with the free variables listed, if for every tuple $\langle m_0, \ldots, m_{n-1}\rangle \in \omega^n$,

$$\begin{array}{lcl} \langle m_0, \ldots, m_{n-1}\rangle \in R & \to & A_E \vdash \varphi(^{v_0}/_{\dot{m}_0}) \ldots (^{v_{n-1}}/_{\dot{m}_{n-1}}), \text{ and} \\ \langle m_0, \ldots, m_{n-1}\rangle \notin R & \to & A_E \vdash \neg\varphi(^{v_0}/_{\dot{m}_0}) \ldots (^{v_{n-1}}/_{\dot{m}_{n-1}}) \end{array}$$

R is representable if there is a formula which represents R.

A function $f : \omega^n \longrightarrow \omega$ is represented by a formula if that formula represents the relation

$$\{\langle m_0, \ldots, m_{n-1}, f(m_0, \ldots, m_{n-1})\rangle \mid \langle m_0, \ldots, m_{n-1}\rangle \in \mathrm{dom}(f)\}$$

which I shall refer to as the *graph of f*. f is representable if there is a formula which represents the graph of f.

A formula $\varphi(v_0, v_1, \ldots, v_n)$ *functionally* represents the function $f : \omega^n \to \omega$ if for all natural numbers $m_0, \ldots, m_{n-1}$,

$$A_E \vdash \forall v_n(\varphi(^{v_0}/_{\dot{m}_0}) \cdots (^{v_{n-1}}/_{\dot{m}_{n-1}}) \leftrightarrow v_n = S^{f(m_0,\ldots,m_{n-1})}(0)).$$

I shall often write $\varphi(\dot{m}_0, \ldots, \dot{m}_{n-1})$ in place of $\varphi(^{v_0}/_{\dot{m}_0}) \ldots (^{v_{n-1}}/_{\dot{m}_{n-1}})$, to save some space. If a relation R as above is representable, then there is a computer program for an idealized computer which can check, given $\vec{m}$, whether $\vec{m} \in R$ or not. This works as follows: Let φ witness that R is representable. Given $\vec{m}$, let $\varphi' = \varphi(\dot{m}_0, \ldots, \dot{m}_{n-1})$ (this is a different formula, actually a sentence). The program can search for a proof (from A_E) of φ' or of $\neg\varphi'$, simultaneously. Since either $A_E \vdash \varphi'$ or $A_E \vdash \neg\varphi'$, by our assumption that R is represented by φ, after finitely many steps, the program will have found a proof. When this occurs, the program halts and outputs "yes" if the search for a proof of φ' was successful, and "no" if the search for a proof of $\neg\varphi'$ was. It is less obvious but nevertheless true that every relation that is computable in this way is also representable.

In the following, I will provide some facts about the class of representable relations and functions.

Definition 5.1.2. A formula $\varphi(v_0, \ldots, v_{n-1})$ is *numeralwise determined* by A_E if for every tuple $\langle m_0, \ldots, m_{n-1}\rangle$ of natural numbers, either

$$A_E \vdash \varphi(\dot{m}_0, \ldots, \dot{m}_{n-1})$$

or

$$A_E \vdash \neg\varphi(\dot{m}_0, \ldots, \dot{m}_{n-1}).$$

Also, if $\mathcal{M}$ is a model of some language, and $\varphi(v_0, \ldots, v_{n-1})$ is a formula of that language, then *the relation defined in $\mathcal{M}$ by φ* is

$$\{\langle a_0, \ldots, a_{n-1}\rangle \in |\mathcal{M}|^n \mid \mathcal{M} \models \varphi[a_0, \ldots, a_{n-1}]\}.$$

In this case, this set is lightface-definable over $\mathcal{M}$. A relation $R \subseteq |\mathcal{M}|^i$ is boldface-definable over $\mathcal{M}$ if there is a formula φ as above and members $a_i, a_{i-1}, \ldots, a_{n-1}$ of $|\mathcal{M}|$, with $i < n$, such that

$$R = \{\langle a_0, \ldots, a_{i-1}\rangle \mid \mathcal{M} \models \varphi[a_0, \ldots, a_{n-1}]\}.$$

In this case, I say that R is defined by φ in the parameters $a_i, \ldots, a_{n-1}$ over $\mathcal{M}$.

The following lemma describes the connection between definability in $\mathfrak{N}$ and representability of a relation.

Lemma 5.1.3. *A formula $\varphi(v_0,\ldots,v_{n-1})$ represents a relation if and only if φ is numeralwise determined by A_E. In that case, the relation represented by φ is the relation defined by φ over $\mathfrak{N}$.*

Proof. It's clear by the definition of what it means that φ represents a relation that this implies φ is numeralwise determined.

Conversely, suppose φ is numeralwise determined. Let $R = \{\langle m_0,\ldots,m_{n-1}\rangle \in \omega^n \mid A_E \vdash \varphi(\dot{m}_0,\ldots,\dot{m}_{n-1})\}$. Clearly, φ represents R. Moreover, R is defined by φ over $\mathfrak{N}$: Let $\vec{m} := \langle m_0,\ldots,m_{n-1}\rangle \in \omega^n$ be given. If $\vec{m} \in R$, then $A_E \vdash \varphi(\dot{m}_0,\ldots,\dot{m}_{n-1})$, and since $\mathfrak{N} \models A_E$, it follows that $\mathfrak{N} \models \varphi(\dot{m}_0,\ldots,\dot{m}_{n-1})$, which means that $\mathfrak{N} \models \varphi[m_0,\ldots,m_{n-1}]$, since $(S^m(0))^{\mathfrak{N}} = m$, for every natural number m. If $\vec{m} \notin R$, then by definition, $A_E \nvdash \varphi(\dot{m}_0,\ldots,\dot{m}_{n-1})$, so since φ is numeralwise determined, $A_E \vdash \neg\varphi(\dot{m}_0,\ldots,\dot{m}_{n-1})$, which means that $\mathfrak{N} \models \neg\varphi(\dot{m}_0,\ldots,\dot{m}_{n-1})$, so $\mathfrak{N} \not\models \varphi[m_0,\ldots,m_{n-1}]$. □

So in order to see that some relation is representable (and in particular, computable), it suffices to check that it is definable in $\mathfrak{N}$ by a formula which is numeralwise determined by A_E. That's why it is useful to develop some criteria for when a formula is numeralwise determined by A_E. First, let's give a name to a concept that occurs frequently.

Definition 5.1.4. If Σ is a set of formulas and φ is a sentence, then Σ *decides* φ if $\Sigma \vdash \varphi$ or $\Sigma \vdash \neg\varphi$.

So a formula $\varphi(v_0,\ldots,v_{n-1})$ is numeralwise determined if A_E decides $\varphi(\dot{m}_0,\ldots,\dot{m}_{n-1})$, for all $m_0,\ldots,m_{n-1} < \omega$.

Lemma 5.1.5. *1. If φ_0 and φ_1 are sentences that are decided by a set of formulas Σ, then so are $\neg\varphi_0$, $(\varphi_0 \wedge \varphi_1)$, $(\varphi_0 \vee \varphi_1)$ and $(\varphi_0 \longrightarrow \varphi_1)$.*

2. For any natural number n,

$$A_E \vdash \forall v_0(v_0 < S^{n+1}(0) \leftrightarrow \bigvee_{j\leq n} v_0 = S^j(0)).$$

3. For any variable-free term t, there is a unique natural number n such that $A_E \vdash t = \dot{n}$.

4. Every quantifier-free sentence is decided by A_E.

Proof. I shall tacitly use the completeness theorem all the time. Basically, I am arguing by replacing $\vdash$ with $\models$. This would not be necessary, but it makes the arguments less formalistic and maybe more transparent. Part of the reason for this is that the choice of the particular definition of $\vdash$ is less canonical than the definition of $\models$.

Let's prove 1. So suppose φ_0 and φ_1 are decided by Σ. If $\Sigma \vdash \varphi_0$ and $\Sigma \vdash \varphi_1$, then $\Sigma \vdash (\varphi_0 \wedge \varphi_1)$, and we are done. If not, then $\Sigma \vdash \neg\varphi_i$, for $i = 0$ or $i = 1$. It follows that $\Sigma \vdash \neg(\varphi_0 \wedge \varphi_1)$, since φ_i is false in any model of Σ. To see that $\neg\varphi_0$ is decided: If $\Sigma \vdash \varphi_0$, then $\Sigma \vdash \neg(\neg\varphi_0)$, so it decides $\neg\varphi_0$ in the negative. If $\Sigma \vdash \neg\varphi_0$, then it decides $\neg\varphi_0$ in the positive. The claim about $(\varphi_0 \vee \varphi_1)$ reduces to $\neg(\neg\varphi_0 \wedge \neg\varphi_1)$. And $(\varphi_0 \longrightarrow \varphi_1)$ is just short for $(\neg\varphi_0 \vee \varphi_1)$.

For 2, argue by induction on n. Work in an arbitrary model $\mathcal{M}$ of A_E. For $n = 0$, we have to show that for any $a \in |\mathcal{M}|$, $a <^{\mathcal{M}} S(0)^{\mathcal{M}}$ iff $a = 0^{\mathcal{M}}$. From left to right, by (L1) we have that $a <^{\mathcal{M}} 0^{\mathcal{M}}$ or $a = 0^{\mathcal{M}}$. By (L2), it cannot be that $a <^{\mathcal{M}} 0^{\mathcal{M}}$, so it must be that $a = 0^{\mathcal{M}}$, i.e., $a = S^0(0)^{\mathcal{M}}$. I'll drop the superscripts in similarly simple arguments to follow. The direction from right to left is clear again by (L1), with $v_0 = a$ and $v_1 = 0$.

Now suppose 2 has been shown for n, we try to prove it for $n + 1$. We again use (L1): $\mathcal{M} \models a < S^{n+1}(0)$ means that $\mathcal{M} \models a < S(S^n(0))$, which by (L1) is equivalent to $\mathcal{M} \models$

$a = S^n(0) \vee a < S^n(0)$. Inductively, the latter is equivalent to $\mathcal{M} \models \bigvee_{j<n} v_0 = S^j(0)$ in case $n > 0$, and it is false in case $n = 0$ by (L2). Let's take the disjunction $\bigvee_{j<n} v_0 = S^j(0)$ to be nothing in case $n = 0$, and an empty disjunction to be false in any model. Then putting the two disjunctions together gives $\mathcal{M} \models \bigvee_{j<n+1} v_0 = S^j(0)$, as desired. All these transformations work in both directions, so we have shown the desired equivalence.

For 3, uniqueness is easily seen. For suppose $A_E \vdash t = S^m(0)$ and $A_E \vdash t = S^n(0)$. Since $\mathfrak{N} \models A_E$, it follows that $\mathfrak{N} \models S^m(0) = S^n(0)$, i.e., $m = n$. For existence, argue by induction on t. If $t = 0$, then $A_E \vdash t = S^0(0)$. Now suppose $t = S(u)$, where $A_E \vdash u = S^m(0)$. Then $A_E \vdash S(u) = S^{m+1}(0)$. Now suppose u_0 and u_1 are terms such that $A_E \vdash u_0 = S^{m_0}(0)$ and $A_E \vdash u_1 = S^{m_1}(0)$, for some natural numbers m_0 and m_1. By applying $(A2)$ m_1 times and $(A1)$ once, it follows that

$$\begin{aligned} S^{m_0}(0) + S^{m_1}(0) &= S^{m_0}(0) + S(S^{m_1-1}(0)) \\ &= S(S^{m_0}(0) + S^{m_1-1}(0)) \\ &= S(S(S^{m_0}(0) + S^{m_1-2}(0))) \\ &= \cdots \\ &= S^{m_1}(S^{m_0}(0) + 0) \\ &= S^{m_1}(S^{m_0}(0)) \\ &= S^{m_0+m_1}(0). \end{aligned}$$

So this shows the claim for $t = u_0 + u_1$. For $t = u_0 \cdot u_1$, we use $(M2)$ and $(M1)$ instead of $(A2)$ and $(A1)$ to conclude that

$$A_E \vdash S^{m_0}(0) \cdot S^{m_1}(0) = \underbrace{S^{m_0}(0) + S^{m_0}(0) + \cdots + S^{m_0}(0)}_{m_1 \text{ times}}.$$

But by the above, $A_E \vdash S^{m_0}(0) + S^{m_0}(0) = S^{2m_0}(0)$, and so on, so that by $m_1 - 1$ applications of the above, it follows that

$$A_E \vdash S^{m_0}(0) \cdot S^{m_1}(0) = S^{m_0 \cdot m_1}(0),$$

which proves the claim for $t = u_0 \cdot u_1(0)$. The case $t = u_0 E u_1$ relates to the case $t = u_0 \cdot u_1$ as the case $t = u_0 \cdot u_1$ relates to the case $t = u_0 + u_1$.

For 4, note that it suffices to prove that every *atomic* sentence is decided by A_E, in view of 1, since one can then argue by induction on quantifier free sentences.

Let φ be of the form $t_0 = t_1$. By 3, fix m_0 and m_1 such that $A_E \vdash (t_0 = S^{m_0}(0) \wedge t_1 = S^{m_1}(0))$.

If $m_0 = m_1$, then clearly, $A_E \vdash t_0 = t_1$, since if $\mathcal{M}$ is an arbitrary model of A_E, $\mathcal{M} \models t_0 = S^{m_0}(0) = S^{m_1}(0) = t_1$. If $m_0 \neq m_1$, then wlog, let $m_0 < m_1$. I claim that $A_E \vdash t_0 \neq t_1$. If not, then there would be a model $\mathcal{M} \models A_E$ with $\mathcal{M} \models t_0 = t_1$. Then, arguing inside $\mathcal{M}$, it follows that $S^{m_0-1}(0) = S^{m_1-1}(0)$, by (S2), which, in turn, implies that $S^{m_0-2}(0) = S^{m_1-2}(0)$, again by (S2). Applying (S2) m_0 times, it follows that $0 = S^{m_1-m_0}(0)$, and $m_1 - m_0 > 0$. So letting $a = S^{m_1-m_0-1}(0)$, in $\mathcal{M}$, $0 = S(a)$, which contradicts (S1).

Now let φ be of the form $t_0 < t_1$. Again, fix m_0 and m_1 such that $A_E \vdash t_i = S^{m_i}(0)$, by 3.

If $m_0 < m_1$, then it follows that $A_E \vdash t_0 < t_1$. For if $\mathcal{M} \models A_E$, then by 2, $\mathcal{M} \models \forall x(x < S^{m_1}(0) \leftrightarrow \bigvee_{j<m_1} x = S^j(0)$. Substituting t_0 for x in the inner formula shows that $\mathcal{M} \models (t_0 < t_1 \leftrightarrow \bigvee_{j<m_1} t_0 = S^j(0))$. But the disjunction on the right hand side is true in $\mathcal{M}$ by assumption, as $m_0 < m_1$. So $\mathcal{M} \models t_0 < t_1$, as claimed.

Now suppose $m_1 \leq m_0$. I claim that then, $A_E \vdash \neg t_0 < t_1$. To see this, let $\mathcal{M} \models A_E$, and assume, towards a contradiction that $\mathcal{M} \models t_0 < t_1$, i.e., $\mathcal{M} \models S^{m_0}(0) < S^{m_1}(0)$, where

$m_1 \le m_0$. As above, arguing in $\mathcal{M}$, it follows that $S^{m_0-1}(0) < S^{m_1-1}(0)$, by (S2). Applying (S2) $m_1 - 1$ more times, it follows that $S^{m_0-m_1}(0) < 0$, which contradicts the axiom (L2) of A_E. So such an $\mathcal{M}$ cannot exist, which shows that $A_E \vdash \neg(t_0 < t_1)$, as desired. This concludes the proof of the atomic case. Boolean combinations are covered by 1. □

Theorem 5.1.6. *1. Any quantifier-free formula is numeralwise determined by A_E.*

2. If φ and ψ are numeralwise determined by A_E, then so are $\neg\varphi$, $(\varphi \vee \psi)$, $(\varphi \wedge \psi)$ and $(\varphi \to \psi)$.

3. If φ is numeralwise determined by A_E, then so are the "bounded quantifications" $\forall x(x < y \to \varphi)$ and $\exists x(x < y \wedge \varphi)$. From now on, I'll write $\forall x < y \quad \varphi$ for the first formula and $\exists x < y \quad \varphi$ for the second.

Proof. For 1, let $\varphi(x_0, \ldots, x_{n-1})$ be a quantifier-free formula. Given $m_0, \ldots, m_{n-1} \in \omega$, and letting $\psi := \varphi(S^{m_0}(0), \ldots, S^{m_{n-1}}(0))$, it follows that ψ is a quantifier-free sentence, so by Lemma 5.1.5.4, it is decided by A_E.

For 2, let φ and ψ be numeralwise determined by A_E. Let $v_0, \ldots, v_{k-1}$ list the free variables of $(\varphi \wedge \psi)$, and let $a_0 \ldots, a_{k-1} \in \omega$. Then $(\varphi \wedge \psi)(^{v_0}/_{S^{a_0}(0)}) \cdots (^{v_{k-1}}/_{S^{a_{k-1}}(0)}) = (\varphi' \wedge \psi')$, where φ' and ψ' are obvious instances of φ and ψ, respectively. Then A_E decides φ' and A_E decides ψ'. These instances are decided by A_E, so by Lemma 5.1.5.1, so is $(\varphi' \wedge \psi')$. The argument for the other Boolean combinations is similar.

For 3, first note that $\neg(\exists x < y \quad \varphi)$ is logically equivalent to $\forall x < y \quad \neg\varphi$. By 2, φ is numeralwise determined by A_E iff $\neg\varphi$ is. So it suffices to prove that if φ is numeralwise determined by A_E, then so is $\exists x < y \quad \varphi$. This is because knowing that, one can argue that given a ψ which is numeralwise determined by A_E, it follows that $\neg\psi$ is numeralwise determined by A_E, hence so is $\exists x < y \quad \neg\psi$, which is the same as to say that $\neg\forall x < y \quad \psi$ is numeralwise determined by A_E, and hence, so is $\forall x < y \quad \psi$.

So let φ be numeralwise determined by A_E. Let $y, z_0, \ldots, z_{n-1}$ be the free variables of the formula $\exists x < y \quad \psi$. Fix natural numbers $a, b_0, \ldots, b_{n-1}$.

Case 1. $\mathfrak{N} \models (\exists x < y \quad \psi)(S^a(0), S^{b_0}(0), \ldots, S^{b_{n-1}}(0))$.

Let $c \in \omega$ witness this formula, meaning that $c < a$ and

$$\mathfrak{N} \models \psi(^x/_{S^c(0)})(^y/_{S^a(0)})(^{z_0}/_{S^{b_0}(0)}) \ldots (^{z_{n-1}}/_{S^{b_{n-1}}(0)}).$$

Since ψ is numeralwise determined, it follows that

$$A_E \vdash \psi(^x/_{S^c(0)})(^y/_{S^a(0)})(^{z_0}/_{S^{b_0}(0)}) \ldots (^{z_{n-1}}/_{S^{b_{n-1}}(0)}),$$

since it cannot be that A_E proves the negation of this sentence, as it holds in $\mathfrak{N}$. But of course, $A_E \vdash S^c(0) < S^a(0)$ by Lemma 5.1.5.4 as this is an atomic formula which is true in $\mathfrak{N}$. But then clearly,

$$A_E \vdash (\exists x < y \ \psi)(^y/_{S^a(0)})(^{z_0}/_{b_0}) \ldots (^{z_{n-1}}/_{b_{n-1}}),$$

as this is witnessed by $S^c(0)$.

Case 2. Case 1 fails.

In that case, $\mathfrak{N} \models (\neg\exists x < y \quad \psi)(S^a(0), S^{b_0}(0), \ldots, S^{b_{n-1}}(0))$. I claim that A_E proves this sentence. Assuming the contrary, there is a model $\mathcal{M} \models A_E$ in which the negation holds:

$$\mathcal{M} \models (\exists x < y \quad \psi)(S^a(0), S^{b_0}(0), \ldots, S^{b_{n-1}}(0)).$$

Let $c \in |\mathcal{M}|$ witness this. I.e.,

$$\mathcal{M} \models c < S^a(0) \text{ and } \mathcal{M} \models \psi(^y/_{S^a(0)})(^{z_0}/_{S^{b_0}(0)}) \ldots (^{z_{n-1}}/_{S^{b_{n-1}}(0)})[(^x/_c)].$$

By Lemma 5.1.5.2, there is a natural number $c' < a$ such that

$$\mathcal{M} \models c = S^{c'}(0).$$

Hence,

$$\mathcal{M} \models \psi({}^{x}/_{S^{c'}(0)})({}^{y}/_{S^{a}(0)})({}^{z_0}/_{S^{b_0}(0)}) \ldots ({}^{z_{n-1}}/_{S^{b_{n-1}}(0)}).$$

Since ψ is numeralwise determined, it follows that this sentence is actually provable in A_E, or else the negation would be provable, and hence the negation would have to hold in $\mathcal{M}$. But if it is provable in A_E, then it has to hold in $\mathfrak{N}$ as well:

$$\mathfrak{N} \models \psi({}^{x}/_{S^{c'}(0)})({}^{y}/_{S^{a}(0)})({}^{z_0}/_{S^{b_0}(0)}) \ldots ({}^{z_{n-1}}/_{S^{b_{n-1}}(0)}).$$

But then c' witnesses that

$$\mathfrak{N} \models (\exists x < y \quad \psi)(S^{a}(0), S^{b_0}(0), \ldots, S^{b_{n-1}}(0)),$$

contrary to our assumption. □

Now we'll clarify the relationship between representable functions and functionally representable functions.

Lemma 5.1.7. *If a formula $\varphi(v_0, \ldots, v_n)$ functionally represents a function $f : \omega^n \longrightarrow \omega$, then φ also represents the graph of f.*

Proof. Let $\vec{m} := \langle m_0, m_1, \ldots, m_n\rangle \in \omega^{n+1}$ be given. If $\langle m_0, \ldots, m_n\rangle$ is in the graph of f, i.e., $m_n = f(m_0, \ldots, m_{n-1})$, then since φ functionally represents f, this means that

$$A_E \vdash \forall v_n(\varphi({}^{v_0}/_{S^{m_0}(0)}) \cdots ({}^{v_{n-1}}/_{S^{m_{n-1}}(0)}) \leftrightarrow v_n = S^{f(m_0,\ldots,m_{n-1})}(0)).$$

So in an arbitrary model $\mathcal{M} \models A_E$, this sentence is true. Since

$$\mathcal{M} \models v_n = S^{f(m_0,\ldots,m_{n-1}}(0)[({}^{v_n}/_{S^{f(m_0,\ldots,m_{n-1})}(0)^{\mathcal{M}}})],$$

this means that

$$\mathcal{M} \models \varphi({}^{v_0}/_{S^{m_0}(0)}) \cdots ({}^{v_{n-1}}/_{S^{m_{n-1}}(0)})({}^{v_n}/_{S^{f(m_0,\ldots,m_{n-1})}(0)}),$$

so that A_E proves that sentence, as $\mathcal{M}$ was arbitrary.

On the other hand, if $\langle m_0, \ldots, m_n\rangle$ is not in the graph of f, then $f(m_0, \ldots, m_{n-1}) \neq m_n$. It follows that in the above formula, the right hand side of the equivalence over which the $\forall$-quantifier is ranging is false if $S^{m_n}(0)$ is substituted for v_n. As before, this means that

$$A_E \vdash \neg\varphi({}^{v_0}/_{S^{m_0}(0)}) \cdots ({}^{v_{n-1}}/_{S^{v_{n-1}}m_{n-1}})({}^{v_n}/_{S^{f(m_0,\ldots,m_{n-1})}(0)}).$$

This is the other half of what was to be shown in order to see that φ represents the graph of f. □

Lemma 5.1.8. *If the graph of a function f is representable, then f is also functionally representable.*

Proof. Let $\varphi(v_0, \ldots, v_n)$ represent the graph of f. Let θ be the formula

$$(\varphi \wedge \forall v_{n+1} < v_n \quad \neg\varphi({}^{v_n}/_{v_{n+1}})).$$

So $\theta(v_0,\ldots,v_n)$ expresses that v_n is least such that $\varphi(v_0,\ldots,v_n)$ holds. Let natural numbers $m_1,\ldots,m_n$ be given. In order to see that θ functionally represents f, it has to be shown that

$$A_E \vdash \forall v_n(\theta({}^{v_0}/_{S^{m_0}(0)})\cdots({}^{v_{n-1}}/_{S^{m_{n-1}}(0)}) \leftrightarrow v_n = S^{f(m_0,\ldots,m_{n-1})}(0)).$$

So fix a model $\mathcal{M} \models A_E$, and fix an element $a \in |\mathcal{M}|$. We have to see that

$$\mathcal{M} \models \theta[({}^{v_0}/_{S^{m_0}(0)^{\mathcal{M}}})\cdots({}^{v_{n-1}}/_{S^{m_{n-1}}(0)^{\mathcal{M}}})({}^{v_n}/_a)] \iff \mathcal{M} \models a = S^{f(m_0,\ldots,m_{n-1})}(0).$$

For the direction from right to left: Since φ represents the graph of f,

$$\mathcal{M} \models \varphi[({}^{v_0}/_{S^{m_0}(0)^{\mathcal{M}}})\cdots({}^{v_{n-1}}/_{S^{m_{n-1}}(0)^{\mathcal{M}}})({}^{v_n}/_a)],$$

and there can be no $c \in \mathcal{M}$ such that $\mathcal{M} \models c < a$ and

$$\mathcal{M} \models \varphi[({}^{v_0}/_{S^{m_0}(0)^{\mathcal{M}}})\cdots({}^{v_{n-1}}/_{S^{m_{n-1}}(0)^{\mathcal{M}}})({}^{v_n}/_c)],$$

for since $\mathcal{M} \models a = S^{f(m_0,\ldots,m_{n-1})}(0)$, it would follow that $\mathcal{M} \models c = S^k(0)$, for some $k < f(m_0,\ldots,m_{n-1})$ (by Lemma 5.1.5.2), and hence that $\langle m_0,\ldots,m_{n-1},k\rangle \in f$, as φ represents the graph of f as a relation. But this would mean that $f(m_0,\ldots,m_{n-1}) = k < f(m_0,\ldots,m_{n-1})$, a contradiction.

For the converse, the argument is similar, but let me argue a little less formally. The point is that there is a natural number k, namely $k = f(m_1,\ldots,m_n)$, such that

$$\mathcal{M} \models \varphi(S^{m_0}(0)^{\mathcal{M}},\ldots,S^{m_{n-1}}(0)^{\mathcal{M}},S^k(0)^{\mathcal{M}}),$$

because the graph of f is represented by φ. Below a numeral, there are only numerals, so since a is least (in $\mathcal{M}$) such that $\mathcal{M} \models \varphi[S^{m_0}(0)^{\mathcal{M}},\ldots,S^{m_{n-1}}(0)^{\mathcal{M}},a]$, it follows that $a \le S^k(0)$ in $\mathcal{M}$, and hence, a is equal to a numeral $S^l(0)^{\mathcal{M}}$, $l \le k$. So we have $\mathcal{M} \models \varphi(S^{m_0}(0),\ldots,S^{m_{n-1}}(0),S^l(0))$, which means that $l = f(m_0,\ldots,m_0) = k$, and in particular,

$$\mathcal{M} \models a = S^{f(m_0,\ldots,m_{n-1})}(0).$$

□

These facts allow us to formulate some closure properties of the class of representable functions.

Lemma 5.1.9. *Suppose $f_0,\ldots,f_{m-1}$ are representable functions with $\mathrm{dom}(f_0) = \ldots = \mathrm{dom}(f_{m-1}) = \omega^k$, and that $g : \omega^m \longrightarrow \omega$ is representable. Then the function $h = g\circ(f_0,\ldots,f_{m-1}) : \omega^k \longrightarrow \omega$, defined by*

$$h(a_0,\ldots,a_{k-1}) := g(f_0(a_0,\ldots,a_{k-1}),\ldots,f_{m-1}(a_0,\ldots,a_{k-1}))$$

is representable.

Proof. We may by Lemma 5.1.8 choose functional representations $\varphi_0,\ldots,\varphi_{m-1},\gamma$ of $f_0,\ldots,f_{m-1},g$. Note that the set of free variables of φ_i is contained in $\{v_0,v_1,\ldots,v_k\}$. Choose variables $x_0,\ldots,x_{m-1}$ which do not occur in any of these formulas. Let η be the following formula:

$$\exists x_0\ldots\exists x_{m-1}\left(\left(\bigwedge_{0<l<m}\underbrace{\varphi_l({}^{v_k}/_{x_l})}_{\text{“}x_l=f_l(v_0,\ldots,v_{k-1})\text{”}}\right)\wedge\underbrace{\gamma({}^{v_0}/_{x_0})\cdots({}^{v_{m-1}}/_{x_{m-1}})}_{\text{“}v_m=g(x_0,\ldots,x_{k-1})\text{”}}\right).$$

We check that η represents the graph of h:

Let $\langle a_0, \ldots, a_{k-1}, b\rangle \in \omega^{k+1}$. There are two cases.

Case 1: $b = h(a_0, \ldots, a_{k-1})$.

Then let $b_0 = f_0(a_0, \ldots, a_{k-1}), \ldots, b_m = f_m(a_0, \ldots, a_{k-1})$. Let $\mathcal{M}$ be an arbitrary model of A_E. Since φ_i represents f_i, for $0 < i < k$, it follows that for each such i, we have:

$$\mathcal{M} \models \varphi_i({}^{v_0}/_{S^{a_0}(0)}), \ldots, ({}^{v_{k-1}}/_{S^{a_{k-1}}(0)})({}^{v_k}/_{S^{b_i}(0)}),$$

and trivially also that

$$\mathcal{M} \models \varphi_i({}^{v_0}/_{S^{a_0}(0)}), \ldots, ({}^{v_{k-1}}/_{S^{a_{k-1}}(0)})({}^{v_k}/_{x_i})({}^{x_i}/_{S^{b_i}(0)}).$$

Moreover, since γ represents g, it follows that

$$\mathcal{M} \models \gamma({}^{v_0}/_{S^{b_0}(0)}) \cdots ({}^{v_{m-1}}/_{S^{b_{m-1}}(0)})({}^{v_m}/_{S^{b}(0)}),$$

so that

$$\mathcal{M} \models \left(\left(\bigwedge_{i<m} \varphi_i({}^{v_0}/_{S^{a_0}(0)}) \ldots ({}^{v_{k-1}}/_{S^{a_{k-1}}(0)})({}^{v_k}/_{x_i})({}^{x_i}/_{S^{b_i}(0)})\right) \wedge \gamma({}^{v_0}/_{S^{b_0}(0)}) \cdots ({}^{v_{m-1}}/_{S^{b_{m-1}}(0)})({}^{v_m}/_{S^{b}(0)})\right).$$

So the terms $S^{b_0}(0), \ldots, S^{b_{m-1}}(0)$ witness that

$$\mathcal{M} \models \eta({}^{v_0}/_{a_0}) \cdots ({}^{v_{k-1}}/_{a_{k-1}})({}^{v_m}/_{S^{b}(0)}).$$

Since $\mathcal{M}$ was arbitrary, this means that

$$A_E \vdash \eta({}^{v_0}/_{a_0}) \cdots ({}^{v_{k-1}}/_{a_{k-1}})({}^{v_k}/_{S^{b}(0)}),$$

as wished.

Case 2: $b \neq h(a_0, \ldots, a_{k-1})$.

Let $\mathcal{M}$ be an arbitrary model of A_E. We have to show that

$$\mathcal{M} \models \neg\eta({}^{v_0}/_{S^{a_0}(0)}) \cdots ({}^{v_{k-1}}/_{S^{a_{k-1}}(0)})({}^{v_0}/_{S^{b}(0)}).$$

Assuming the contrary means that there are $b_0, \ldots, b_{m-1} \in |\mathcal{M}|$ such that for every $i < m$,

$$\mathcal{M} \models \varphi_i({}^{v_0}/_{S^{a_0}(0)}) \cdots ({}^{v_{k-1}}/_{S^{a_{k-1}}(0)})[({}^{v_k}/_{b_i})]$$

and

$$\mathcal{M} \models \gamma[({}^{v_0}/_{b_0}) \cdots ({}^{v_{m-1}}/_{b_{m-1}})({}^{v_m}/_{S^{b}(0)^{\mathcal{M}}})].$$

Since φ_i functionally represents f_i, it follows from the former that

$$\mathcal{M} \models b_i = S^{f_i(a_1,\ldots,a_k)}(0).$$

And hence, the latter means that

$$\mathcal{M} \models \gamma({}^{v_0}/_{S^{f_0(a_0,\ldots,a_{k-1})}(0)}) \cdots ({}^{v_{m-1}}/_{S^{f_{m-1}(a_0,\ldots,a_{k-1})}(0)})({}^{v_m}/_{S^{b}(0)}),$$

which, since γ represents g, means that

$$b = g(f_0(a_0, \ldots, a_{k-1}), \ldots, f_{m-1}(a_0, \ldots, a_{k-1})) = h(a_0, \ldots, a_{k-1}),$$

a contradiction. □

Definition 5.1.10. Given a relation $R \subseteq \omega^n$, let χ_R be its characteristic function, $\chi_R : \omega^n \longrightarrow 2$, defined by: $\chi_R(m_0, \ldots, m_{n-1}) = 1$ iff $\langle m_0, \ldots, m_{n-1}\rangle \in R$.

Theorem 5.1.11. *A relation R is representable iff its characteristic function is.*

Proof. From left to right, let $\varphi(v_0, \ldots, v_{n-1})$ represent R. Let $\varphi'(v_0, \ldots, v_{n-1}, v_n)$ be the formula

$$((\varphi \wedge v_n = S(0)) \vee (\neg\varphi \wedge v_n = 0)).$$

Clearly, φ' is numeralwise determined by A_E, being a Boolean combination of such formulas. And φ' obviously defines χ_R over $\mathfrak{N}$.

From right to left, let $\varphi(v_0, \ldots, v_n)$ represent χ_R. Let $\varphi'(v_0, \ldots, v_{n-1})$ be the formula

$$\varphi({}^{v_n}/_{S(0)}).$$

It follows immediately that φ' is numeralwise determined by A_E, since φ is. Again, φ' defines R over $\mathfrak{N}$, so we're done. □

Lemma 5.1.12. *Suppose $R \subseteq \omega^n$ is representable and $f_0, f_1, \ldots, f_{n-1}$ are representable functions with domain ω^k. Then so is the relation*

$$S = \{\langle m_0, \ldots, m_k\rangle \mid \langle f_0(\vec{m}), \ldots, f_{n-1}(\vec{m})\rangle \in R\}.$$

Proof. Since

$$\chi_S = \chi_R \circ (f_0, \ldots, f_{n-1}),$$

and $\chi_R, f_0, \ldots, f_{n-1}$ are representable, χ_S is also representable. □

Theorem 5.1.13. *Let $g : \omega^{n+1} \longrightarrow \omega$ be representable, and let g have the property that for every tuple $\langle m_0, \ldots, m_{n-1}\rangle$, there is an m such that $g(m_0, \ldots, m_{n-1}, m) = 0$. Then the function $f : \omega^n \longrightarrow \omega$ defined by*

$$f(m_0, \ldots, m_{n-1}) = \min\{m \mid g(m_0, \ldots, m_{n-1}, m) = 0\}$$

is representable.

Proof. Let $\gamma(v_0, \ldots, v_{n+1})$ be a functional representation of g. Then the following formula defines the graph of f over $\mathfrak{N}$:

$$\left(\gamma({}^{v_{n+1}}/_0) \wedge \forall v_{n+2} < v_n \neg\gamma({}^{v_n}/_{v_{n+2}})({}^{v_{n+1}}/_0)\right).$$

I leave it to the reader to convince him- or herself that the formula $\gamma({}^{v_{n+1}}/_0)$ is numeralwise determined. It follows then from Lemma 5.1.6 that the entire formula is numeralwise determined. Hence, by Lemma 5.1.3, it represents the graph of f. □

Theorem 5.1.14. *The following relations are representable:*

1. *$P := \{p \mid p$ is a prime number$\}$,*
2. *$Q := \{\langle p, q\rangle \mid p < q$ and $[p, q] \cap P = \{p, q\}\}$,*
3. *The monotone enumeration p of P.*

Proof. 1.) P is represented by the following formula:

$$\Pi(v_0) := (0 < v_0 \wedge \forall v_1 < v_0 \forall v_2 < v_0 \neg v_1 \cdot v_2 = v_0).$$

2.) Here is a formula which represents Q:

$$(\Pi(v_0) \wedge \Pi(v_1) \wedge v_0 < v_1 \wedge \forall v_2 < v_1 (v_0 < v_2 \to \neg\Pi(^{v_0}/_{v_2}))),$$

where in $\Pi(^{v_0}/_{v_2})$, an implicit replacement of the bound variable v_2 occurs, by our convention. In the future, I shall sometimes abuse notation and write instead:

$$\text{“}v_0 \in P\text{”} \wedge \text{“}v_1 \in P\text{”} \wedge v_0 < v_1 \wedge \forall v_2 < v_1 (v_0 < v_2 \to \text{“}v_2 \notin P\text{”}).$$

3.) Instead of writing down a formula representing the set in question explicitly, I will use abbreviations as in the proof of 2.). The reader will no doubt be able to translate this into a genuine formula. The formula should express the following:

“$v_1 \in P$” and there is an $a \le v_1^{v_0^2}$ such that

1. 2 does not divide a,
2. for all $u, v < a$, if $\langle u, v\rangle \in Q$, then for all $i < v_0$:
$$\text{“}u^i \text{ divides } a\text{”} \leftrightarrow \text{“}v^{S(i)}\text{divides } a\text{”}.$$
3. v_1 is the least prime number r such that r^{v_0} divides a.

It is obvious that the relation $\{\langle u, v\rangle \in \omega^2 \mid u \text{ divides } v\}$ is representable (by a bounded formula). So the above formula results from substituting the representable functions $\langle x, y\rangle \mapsto x^{y^2}$, $\langle x, y\rangle \mapsto x^y$ and $\langle x, y\rangle \mapsto x^{S(y)}$ into a representable relation. The result is a representable relation, by Lemma 5.1.12.

To see that the relation defined over $\mathfrak{N}$ by the above formula actually is the graph of the monotone enumeration of P, two directions have to be verified. First, assume that $p(m) = n$. Then let $a = p(0)^0 \cdot p(1)^1 \cdot \dots \cdot p(m)^m$. Clearly, 1.-3. above hold in $\mathfrak{N}$ with $v_0 = m$ and $v_1 = p(m)$, and $a \le p(m)^{m^2}$. For the converse, assume that 1.-3. hold in $\mathfrak{N}$, with $v_0 = m$ and $v_1 = q$, where q is a prime number, and with $a \le q^{m^2}$. By induction on $i \le m$, it follows that $p(i)^i$ divides a but $p(i)^{i+1}$ doesn't, using 1. for the start of the induction and 2. for the induction step. It follows that $q = p(m)$, since $p(m)^m$ divides a, and it is the least prime number with this property, as is q, so they must be equal. □

5.2 A different Gödelization: Ackermann's coding of V_ω

Definition 5.2.1 (Ackermann)**.** For a natural number n, let u_n be the uniquely determined finite set of natural numbers such that

$$n = \sum_{m \in u_n} 2^m.$$

Define a relation $\tilde{\in} \subseteq \omega^2$ by:

$$m \tilde{\in} n \iff m \in u_n.$$

So $m\tilde{\in}n$ iff the m-th digit in the binary representation of n is 1. Note that

$$m \tilde{\in} n \implies m < n.$$

Theorem 5.2.2. *$\tilde{\in}$ is representable.*

Proof. $v_0 \tilde{\in} v_1$ iff, in $\mathfrak{N}$, there is $b \le p(v_0)^{v_0 \cdot v_1}$ such that:

1. 2^{v_1} divides b but $2^{S(v_1)}$ does not (think of 2 as $p(0)$ here).
2. For all $i < v_0$, for all $j < v_1 + 2$:
$$\text{“}p(i)^j \text{ divides } b\text{”} \iff \text{“}p(i+1)^{[j:2]} \text{ divides } b.\text{”}$$
3. The largest $i < S(v_1)$ such that $p(v_0)^i$ divides b is odd.

Here $[j : 2]$ is the result of dividing j by 2 and discarding the remainder. It's clear that the relation defined by the above clauses is representable. To see that it defines $\tilde{\in}$ over $\mathfrak{N}$, let $n \in \omega$ be given, and define a sequence $\langle a_i \mid i < k \rangle$ by: $a_0 = [n : 2]$, and if $a_i > 0$, then $a_{i+1} = [a_i : 2]$; otherwise $k = i + 1$. Clearly, $n = \sum_{i<k} 2^{l_i}$, where $l_i = 1$ if a_i is odd, and $l_i = 0$ otherwise. In other words, $u_n = \{i \mid a_i \text{ is odd}\}$, or, $i \tilde{\in} n$ iff a_i is odd. This characterization can be used to see that the above formula defines $\tilde{\in}$ over $\mathfrak{N}$.

For one direction, suppose $m \tilde{\in} n$. Then 1. -3. hold with $v_0 = m$, $v_1 = n$ and $b = \prod_{i \le m} p(i)^{a_i} \le p(m)^{mn}$.

Vice versa, suppose the clauses hold for $v_0 = m$, $v_1 = n$ and b in $\mathfrak{N}$. By induction on $i \le m$, it can be shown that a_i is the largest l such that $p(i)^l$ divides b. So it follows from the last clause that a_m is odd, which means that $m \tilde{\in} n$. □

Theorem 5.2.3 (Ackermann)**.** *The structure $\langle \omega, \tilde{\in} \rangle$ is well-founded and extensional. So it is isomorphic via the Mostowski collapse to a transitive structure. In fact, letting π be the collapse, it follows that*
$$\pi : \langle \omega, \tilde{\in} \rangle \overset{\sim}{\longleftrightarrow} \langle \mathrm{V}_\omega, \in \restriction \mathrm{V}_\omega \rangle.$$

Definition 5.2.4. Let $\pi : \langle \omega, \tilde{\in} \rangle \overset{\sim}{\longleftrightarrow} \langle \mathrm{V}_\omega, \in \restriction \mathrm{V}_\omega \rangle$ be the Mostowski isomorphism. For $R \subseteq (\mathrm{V}_\omega)^n$, let
$$\widetilde{R} = \{\langle m_0, \ldots, m_{n-1} \rangle \mid \langle \pi(m_0), \ldots, \pi(m_{n-1}) \rangle \in R\}.$$

Definition 5.2.5. A *bounded quantifier* in the language of set theory is a quantifier of the form $\exists x \in y$ or $\forall x \in y$, where x and y are variables. Occurrences of these bounded quantifiers can be eliminated and so these quantifiers can be viewed as being abbreviations:
$$\exists x \in y\ \varphi \text{ means } \exists x (x \in y \wedge \varphi),$$
and
$$\forall x \in y\ \varphi \text{ means } \forall x (x \in y \longrightarrow \varphi).$$
A Σ_0*-formula* is a formula in which all quantifiers are bounded. Such formulas are sometimes also referred to as Δ_0*-formulas.*

Theorem 5.2.6. *If $R \subseteq \mathrm{V}_\omega^n$ is definable over $\langle \mathrm{V}_\omega, \in \rangle$ by a Σ_0-formula (using parameters), then $\widetilde{R}$ is representable.*

Proof. By induction on formulas φ in the language of set theory (with bounded quantifiers), I show:

(∗) *If φ is Σ_0, then there is a numeralwise determined formula $\widetilde{\varphi}$ in the language of A_E with the same free variables as φ, such that for all $a_1, \ldots, a_n \in \mathrm{V}_\omega$,*
$$\langle \mathrm{V}_\omega, \in \rangle \models \varphi[a_1, \ldots, a_n] \iff \mathfrak{N} \models \widetilde{\varphi}[\pi^{-1}(a_1), \ldots, \pi^{-1}(a_n)].$$

It will be clear in each case that the displayed claim holds, but I'll check that the formulas produced are numeralwise determined. To start off, let's deal with the atomic cases. If $\varphi = x \dot{=} y$, then we can let $\widetilde{\varphi} = \varphi$. If $\varphi = x \dot{\in} y$, then let

$$\tilde{\varphi} = \text{“}x \tilde{\in} y\text{”},$$

where “$x \tilde{\in} y$” stands for the formula representing $\tilde{\in}$ according to the previous lemma, with x and y substituted for v_0 and v_1, respectively.

Boolean combinations are trivial. Thus, $\widetilde{(\varphi_0 \wedge \varphi_1)} = (\widetilde{\varphi_0} \wedge \widetilde{\varphi_1})$, et cetera. This produces numeralwise determined formulas, since Boolean combinations of numeralwise determined formulas are numeralwise determined.

Finally, let's turn to bounded quantification. Suppose $\psi = \exists x \in y\ \varphi$, where $\widetilde{\varphi}$ is already defined. By renaming the bounded variables of $\widetilde{\varphi}$ if necessary, wma x and y don't occur as bound variables in $\widetilde{\varphi}$. Then set

$$\widetilde{\psi} = \exists x < y(\text{“}x \tilde{\in} y\text{”} \wedge \widetilde{\varphi}).$$

The crucial point here is that $m \tilde{\in} n \implies m < n$. Since bounded quantification over numeralwise determined formulas produces numeralwise determined formulas, this produces a numeralwise determined formula. The case of bounded universal quantification is analogous, so we are done. □

Definition 5.2.7. A formula in the language of set theory is Σ_1 if it is of the form $\exists x \varphi$, where φ is Σ_0. Given a model of set theory $\mathcal{M}$, a relation $R \subseteq |\mathcal{M}|^n$ is $\Sigma_1(\mathcal{M})$ if it is definable over $\mathcal{M}$ by a Σ_1-formula. It is $\Delta_1(\mathcal{M})$ if both R and $\neg R := |\mathcal{M}|^n \setminus R$ are $\Sigma_1(\mathcal{M})$.

I'll also say that a formula $\varphi(x_0, \ldots, x_{n-1})$ is Σ_1^T, where T is some theory, if there is a Σ_1-formula $\sigma(x_0, \ldots, x_{n-1})$ such that $T \vdash \varphi \leftrightarrow \sigma$. It is Δ_1^T if φ and $\neg\varphi$ both are Σ_1^T.

The importance of $\Delta_1(\mathrm{V}_\omega)$-relations is evidenced by the following theorem:

Theorem 5.2.8. *If $R \subseteq \mathrm{V}_\omega^n$ is $\Delta_1(\langle \mathrm{V}_\omega, \in \rangle)$, then $\widetilde{R}$ is representable.*

Before beginning the proof, let me remark that we don't need to worry about parameters that might occur in a $\Delta_1(\mathrm{V}_\omega)$ definition of a relation over V_ω, because the inverse image of such a parameter is a natural number, represented by a numeral, so that by substituting the numeral for the preimage of the parameter, it disappears.

Proof. Let R be defined over V_ω by $\varphi = \exists x \overline{\varphi}$ and $\neg R$ by $\psi = \exists x \overline{\psi}$, where $\overline{\varphi}$ and $\overline{\psi}$ are Σ_0-formulas. By claim $(*)$ of the proof of the previous lemma, it follows that $\widetilde{R}$ is defined by $\exists x \widetilde{\overline{\varphi}}$ and $\neg R$ is defined by $\exists x \widetilde{\overline{\psi}}$ over $\mathfrak{N}$. Note that $\widetilde{\overline{\varphi}}$ and $\widetilde{\overline{\psi}}$ are numeralwise determined formulas, by the previous lemma. I claim that the following formula φ^* represents $\widetilde{R}$:

$$\exists x(\widetilde{\overline{\varphi}} \wedge \forall \bar{x} < x(\neg \widetilde{\overline{\varphi}}(^x/_{\bar{x}}) \wedge \neg \widetilde{\overline{\psi}}(^x/_{\bar{x}}))).$$

To see this, we have to check two things:

First, suppose $\vec{a} \in \widetilde{R}$. Then $\mathfrak{N} \models \exists x \widetilde{\overline{\varphi}}[\vec{a}]$. Let $n \in \omega$ be the least witness. Then

$$\mathfrak{N} \models \widetilde{\overline{\varphi}}[S^{\vec{a}}(0), S^n(0)] \wedge \forall \bar{x} < n(\neg \widetilde{\overline{\varphi}}(^x/_{\bar{x}})(S^{\vec{a}}(0)) \wedge \neg \widetilde{\overline{\psi}}(^x/_{\bar{x}})(S^{\vec{a}}(0))).$$

But this is a numeral instance of a numeralwise determined formula, so A_E proves it. So $A_E \vdash \varphi^*(S^{\vec{a}}(0))$.

Secondly, suppose $\vec{a} \notin \widetilde{R}$. Then $\mathfrak{N} \models \exists x \widetilde{\widetilde{\psi}}(S^{\vec{a}}(0))$. Pick the least witness n. So

$$\mathfrak{N} \models \underbrace{\widetilde{\widetilde{\psi}}(S^{\vec{a}}(0), S^n(0)) \wedge \forall \bar{x} < S^n(0)(\neg\widetilde{\widetilde{\varphi}}(^x/_{\bar{x}})[\vec{a}] \wedge \neg\widetilde{\widetilde{\psi}}(^x/_{\bar{x}})[\vec{a}]))}_{\chi}.$$

So $A_E \vdash \chi$. I claim that $A_E \vdash \neg\varphi^*(S^{\vec{a}}(0))$. If not, then let $\mathcal{M} \models A_E$ be such that $\mathcal{M} \models \varphi^*(S^{\vec{a}}(0))$. Pick a witness $b \in |\mathcal{M}|$, so that

$$\mathcal{M} \models \widetilde{\varphi}(S^{\vec{a}}(0))[b] \wedge \forall \bar{x} < b(\neg\widetilde{\widetilde{\varphi}}(^x/_{\bar{x}})(S^{\vec{a}}(0)) \wedge \neg\widetilde{\widetilde{\psi}}(^x/_{\bar{x}})(S^{\vec{a}}(0)))).$$

Moreover, $\mathcal{M} \models \chi$. It is impossible that $\mathcal{M} \models S^n(0) < b$, since $\mathcal{M} \models \chi$, and hence, $\mathcal{M} \models \widetilde{\widetilde{\psi}}(S^{\vec{a}}(0), S^n(0))$. So $\mathcal{M} \models b \leq S^n(0)$ (by (L3)). But we've known for a long time that there are only numerals below numerals (Lemma 5.1.5.2), so that this implies that $\mathcal{M} \models b = S^l(0)$, for some $l \leq n$. So then, $\mathcal{M} \models \widetilde{\widetilde{\varphi}}(S^{\vec{a}}(0), S^l(0))$. But this is a numeral instance of a numeralwise determined formula, and hence decided by A_E. So $A_E \vdash \widetilde{\widetilde{\varphi}}(S^{\vec{a}}(0), S^l(0))$, and in particular, $\mathfrak{N} \models \widetilde{\widetilde{\varphi}}(S^{\vec{a}}(0), S^l(0))$. So $\mathfrak{N} \models \exists x \widetilde{\widetilde{\varphi}}(S^{\vec{a}}(0))$, i.e., $\vec{a} \in \widetilde{R}$, a contradiction. □

Theorem 5.2.9. *Let $T = \mathsf{ZF}^- - \mathsf{Infinity} - \mathsf{Foundation}$.*

1. *If $\varphi(x_0, \ldots, x_{n-1})$ is Σ_1^T, then so is $\exists x_i \varphi$, for $i < n$.*
2. *If φ_0 and φ_1 are Σ_1^T, then so are $(\varphi_0 \wedge \varphi_1)$ and $(\varphi_0 \vee \varphi_1)$.*
3. *If $\varphi(x_0, \ldots, x_{n-1})$ is Σ_1^T, and y, z are variables which don't occur as bound variables in φ, then the formulas $\exists y \in z\varphi$ and $\forall y \in z\varphi$ are also Σ_1^T.*
4. *If $\mathcal{M} \models T$ and $F : |\mathcal{M}| \to |\mathcal{M}|$ is a function whose graph is $\Sigma_1(\mathcal{M})$, then it is $\Delta_1(\mathcal{M})$.*

Proof. 1.) Suppose φ is of the form $\exists z\psi(x_0, \ldots, x_{n-1})$. Then, provably in T,

$$\exists x_i \exists z \psi(x_0, \ldots, x_{n-1}) \leftrightarrow \exists u \exists x_i \in u \exists z \in u \psi(x_0, \ldots, x_{n-1}),$$

where u is some new variable that doesn't occur in φ. This uses the pairing axiom.

2.) Wlog, we may assume that φ_0 and φ_1 are Σ_1-formulas, and also that they don't have a bound variable in common. Let $\varphi_0 = \exists x \varphi_0'$ and $\varphi_1 = \exists y \varphi_1'$. Then, provably in T,

$$(\varphi_0 \wedge \varphi_1) \leftrightarrow \exists u \exists x \in u \exists y \in u(\varphi_0 \wedge \varphi_1),$$

and analogously for $\vee$.

3.) Wlog, let φ be a Σ_1-formula, say $\varphi = \exists x \varphi'(x, x_0, \ldots, x_{n-1})$, where φ' is Σ_0. So $\exists y \in z\varphi$ is equivalent to the formula

$$\exists y(y \in z \wedge \varphi),$$

which is Σ_1^T, by 1. and 2.

Now consider the formula $\forall y \in z\varphi$, i.e., $\forall y \in z \exists x \varphi'(x, y, z, x_0, \ldots, x_{n-1})$. I claim that it is equivalent, in T, to the formula

$$\exists v \forall y \in z \exists x \in v \varphi'(x, y, z, x_0, \ldots, x_{n-1}).$$

To see this, recall that the theory T contains the $\mathsf{Relativization}$ scheme:

$$\forall z \exists v \forall y \in z((\exists x \langle x, y\rangle \in A) \longrightarrow (\exists x \in v \langle x, y\rangle \in A)).$$

Applying this scheme to $A = \{\langle x, \langle y, z, x_0, \ldots, x_{n-1}\rangle\rangle \mid \varphi'(x, x_0, \ldots, x_{n-1})\}$ proves the desired equivalence.

One can argue without using Relativization, but using Power Set instead (indeed, Power Set and Replacement, together with ZF^{--}, imply Relativization): I'll need the following basic tool: Since I'm assuming the Power Set axiom, I can define, by recursion on the ordinals, a function $\alpha \mapsto \mathrm{V}_\alpha$, by letting $\mathrm{V}_0 = \emptyset$, $\mathrm{V}_{s(\alpha)} = \mathcal{P}(\mathrm{V}_\alpha)$ and $\mathrm{V}_\lambda = \bigcup_{\alpha<\lambda} \mathrm{V}_\alpha$, for limit ordinals λ. I have introduced the first $\omega + 1$ steps of this recursion already. Just as then, it follows from the Foundation axiom that $\mathrm{V} = \bigcup_{\alpha\in\mathrm{On}} \mathrm{V}_\alpha$. Now, working in some model $\mathcal{M}$ of T, and fixing $a_0, \ldots, a_{n-1} \in |\mathcal{M}|$, assume that

$$\mathcal{M} \models \forall y \in z \exists x \varphi'[a_0, \ldots, a_{n-1}].$$

Working in $\mathcal{M}$, let F be the function defined by: $F(y)$ =the least α such that if there is a b with $\varphi'[a_0, \ldots, a_{n-1}(^x/_b)]$, then there is such a $b \in \mathrm{V}_\alpha$. By replacement, the range of F is a set of ordinals which has a supremum, say λ. So

$$\mathcal{M} \models \exists w \forall y \in z \exists x \in w \varphi'[a_0, \ldots, a_{n-1}],$$

as witnessed by $w = \mathrm{V}_\lambda^{\mathcal{M}}$. Vice versa, if this latter formula holds in $\mathcal{M}$ then $\mathcal{M}$ models that $\forall y \in z \exists x \varphi'[a_0, \ldots, a_{n-1}]$ is true. Since $\mathcal{M}$ was arbitrary, this shows that the original formula is, provably in T, equivalent to the Σ_1-formula $\exists w \forall y \in z \exists x \in w \varphi'$.

4.) Let φ define the graph of F over $\mathcal{M}$. Then $\langle a, b_0, \ldots, b_{n-1}\rangle \in \neg F$ iff $a \neq F(b_0, \ldots, b_{n-1})$ iff

$$\mathcal{M} \models \exists z (z \neq a \wedge \varphi(z, b_0, \ldots, b_{n-1})).$$

□

We'll keep working with the fragment T of set theory that was used in the previous theorem.

Theorem 5.2.10. *Let $\mathcal{M}$ be a model of T. Let $R \subseteq |\mathcal{M}|^n$ be a $\Sigma_1(\mathcal{M})$ relation, and let F_i be an m-ary partial $\Sigma_1(\mathcal{M})$-function, for $i < n$. Then the relation $S \subseteq |\mathcal{M}|^m$ defined by*

$$S(a_0, \ldots, a_{m-1}) \iff R(F_0(a_0, \ldots, a_{m-1}), \ldots, F_{n-1}(a_0, \ldots, a_{m-1}))$$

is (uniformly) $\Sigma_1(\mathcal{M})$.

Proof. Saying that S is uniformly $\Sigma_1(\mathcal{M})$ means that given a Σ_1-formula $\varphi_R(x_0, \ldots, x_{n-1}, \vec{w})$ defining R over $\mathcal{M}$, and given Σ_1-formulas $\varphi_i(y_0, \ldots, y_{m-1}, y_m, \vec{w}^i)$ defining the function F_i, for $i < n$,[1] there is a Σ_1-formula $\psi(x_0, \ldots, x_{n-1}, \vec{w}, \vec{w}^0, \ldots, \vec{w}^{n-1})$ which is defined only referring to the formulas $\varphi_R, \varphi_0, \ldots, \varphi_{n-1}$, and not to $\mathcal{M}$. I.e., the formula ψ defines the desired relation in any model $\mathcal{M}'$ of T in which the F_i's define functions.

The following formula does this:

$$\exists u_0 \ldots \exists u_{n-1} \left((\bigwedge_{i<n} \varphi_{F_i}(^{y_m}/_{u_i})) \wedge \varphi_R(u_0, \ldots, u_{n-1}) \right)$$

as the definition of ψ. This is equivalent to a Σ_1-formula. □

Remark 5.2.11. It is possible that a Σ_1-formula φ defines a function in one model of set theory, but not in another. Expressing that φ defines a function has complexity Π_1.

Lemma 5.2.12. *The following formulas are Δ_1^T:*

[1]The variables $\vec{w}, \vec{w}^0, \ldots, \vec{w}^{n-1}$ come from the parameters that may or may not have been used in the definitions of $R, F_0, \ldots, F_{n-1}$.

1. *"$v_0 = \emptyset$"*

2. *"$v_1 = \{v_0\}$"*

3. *"$v_n = \langle v_0, \ldots, v_{n-1}\rangle$."*

4. *"v_0 is a function."*

5. *"$v_1 = \mathrm{ran}(v_0)$."*

6. *"$v_1 = \mathrm{dom}(v_0)$."*

7. *"$v_2 = v_0 \restriction v_1$."*

8. *"$v_2 = v_0(v_1)$."*

Proof. Exercise.

Theorem 5.2.13 (T)**.** *Suppose $G : A \times \mathrm{V} \longrightarrow \mathrm{V}$ is defined by a Σ_1-formula (in parameters), $R \subseteq A \times A$ is strongly well-founded, and the function $A \ni x \mapsto R``\{x\}$ is Σ_1. Then the uniquely determined function $F : A \longrightarrow \mathrm{V}$ (given by the Recursion Theorem) such that*

$$\forall x \in A \quad F(x) = G(x, F{\restriction}R``\{x\})$$

is a Σ_1-function.

Proof. By the recursion theorem, the following formula defines F:

$$\exists f(\varphi(f) \wedge f(v_0) = v_1),$$

where $\varphi(f)$ expresses the following:

- f is a function,
- $\mathrm{dom}(f)$ is closed under R,
- for all $x \in \mathrm{dom}(f)$, $f(x) = G(x, f{\restriction}R``\{x\})$.

The second point is expressed by the formula $\forall y \in \mathrm{dom}(f)\forall z \in R``\{y\} z \in \mathrm{dom}(f)$. The third one is obviously expressible by a Σ_1-formula. □

Up to now, there were two equally acceptable views of what a formula is: One view is that it is an actual finite sequence of symbols, well-formed according to our definitions. When viewed this way, it is not an object about which we can prove things in set theory, since set theory only talks about sets, and not about real world objects. The other view, though, is that formula are members of the semi-group generated by some alphabet, which consists of sets. According to this view, everything we have proven thus far about logic (such as the completeness theorem) was actually a theorem of ZFC (of a fragment of that theory). It is this latter view that I would like to adopt from now on. The question arises then, how complicated is the formula that defines the set of all A_E-formulas. This and other questions are addressed in the following theorem.

Theorem 5.2.14. *The following functions and relations/sets are $\Delta_1(\mathrm{V}_\omega)$:*

1. *ω, and the functions $+$, $\cdot$ defined on ω.*

2. *The set Σ of symbols of the language of A_E, in some convenient coding.*

3. *The set of variables of that language, also the set of constants, the set of function symbols and the set of relation symbols (the latter three are finite).*
4. *The free semi-group generated by these symbols, in the following sense: There is a class* $Z \subseteq V_\omega$ *and a function* $\frown : Z \times Z \longrightarrow Z$ *such that* $\langle Z, \frown \rangle$ *is a free semi-group generated by* Σ*, and such that* Z *and* $\frown$ *are* $\Delta_1(V_\omega)$*.*
5. *The set of terms and the set of formulas.*
6. *The function* π*.*

5.3 Tarski's undefinability of truth

In order to make some notation more readable, let's introduce the following shorthand: If φ is a formula (or any element of V_ω), then let $\ulcorner\varphi\urcorner = S^{\pi^{-1}(\varphi)}(0)$. So $\ulcorner\varphi\urcorner$ is the canonical A_E-term that stands for φ. Anticipating a possible confusion, note, given a natural number n, the difference between $\dot{n}$ and $\ulcorner n\urcorner$!

Lemma 5.3.1 (Fixed-point lemma)**.** *Let* $\beta(x)$ *be a formula with one free variable* x*. Then there is a sentence* σ *such that*

$$A_E \vdash \left(\sigma \leftrightarrow \beta({}^x/_{S^{\pi^{-1}(\sigma)}(0)})\right).$$

So, using the shorthand introduced above:

$$A_E \vdash (\sigma \leftrightarrow \beta({}^x/_{\ulcorner\sigma\urcorner})).$$

Thus, in a way, the sentence σ expresses that β is true of (the code of) σ.

Proof. Consider the relation

$$R = \{\langle \varphi(y), \pi(r), \varphi({}^y/_{S^r(0)})\rangle \mid \varphi \text{ has the one free variable } y, \text{ and } r \in \omega\}.$$

It is easy to see that this relation is $\Sigma_1(V_\omega)$. It is actually a function, with the value in the last component. The expanded function f that maps $\langle u, v\rangle$ to 0 if there is no w such that $\langle u, v, w\rangle \in R$ is also $\Sigma_1(V_\omega)$ and total, and hence the pullback of that function is representable. So let $\theta(v_0, v_1, v_2)$ be a functional representation of the pullback $\tilde{f}$ of f, i.e., the function defined by $\tilde{f}(\pi^{-1}(u), \pi^{-1}(v)) = \pi^{-1}(f(u, v))$. So we have, for any formula $\varphi(y)$ with one free variable y and all natural numbers r:

$$(1)\quad A_E \vdash \forall v_2 \left(\theta({}^{v_0}/_{S^{\pi^{-1}(\varphi)}(0)})({}^{v_1}/_{S^r(0)}) \leftrightarrow v_2 = S^{\pi^{-1}(\varphi({}^y/_{S^r(0)}))}(0)\right).$$

Expressed less formally, (1) says: $A_E \vdash \forall v_2\, (\theta(\ulcorner\varphi\urcorner, \dot{r}, v_2) \leftrightarrow v_2 = \ulcorner\varphi({}^y/_{\dot{r}})\urcorner)$.

Now set:

$$\psi(v_1) := \forall v_2\, (\theta({}^{v_0}/_{v_1}) \longrightarrow \beta({}^x/_{v_2})).$$

Let $p = \pi^{-1}(\psi)$, and set:

$$\sigma := \psi({}^{v_1}/_{S^p(0)}),$$

or, in other words, $\sigma = \psi(\ulcorner\psi\urcorner)$, noting that $S^p(0) = \dot{p} = \ulcorner\psi\urcorner$. Unraveling a bit further,

$$\sigma = \forall v_2(\theta(\ulcorner\psi\urcorner, \ulcorner\psi\urcorner, v_2) \longrightarrow \beta({}^x/_{v_2})).$$

By (1), it follows that

(2) $A_E \vdash \forall v_2 \left(\theta({}^{v_0}/_{S^{\pi^{-1}(\psi)}(0)})({}^{v_1}/_{S^p(0)}) \leftrightarrow v_2 = S^{\pi^{-1}(\sigma)}(0) \right)$,

which is the same as to say that

(2') $A_E \vdash \forall v_2 \left(\theta({}^{v_0}/_{S^p(0)})({}^{v_1}/_{S^p(0)}) \leftrightarrow v_2 = S^{\pi^{-1}(\sigma)}(0) \right)$,

since $p = \pi^{-1}(\psi)$. As before, this can be expressed as follows, using the shorthand:

$$A_E \vdash \forall v_2 \left(\theta(\ulcorner \psi \urcorner, \dot{p}, v_2) \leftrightarrow v_2 = \ulcorner \sigma \urcorner \right)$$

I claim that σ is as desired. To see this, let $\mathcal{M}$ be an arbitrary model of A_E. It must be shown that

$$(\mathcal{M} \models \sigma) \iff (\mathcal{M} \models \beta({}^x/_{\ulcorner \sigma \urcorner}))\,.$$

For the direction from left to right, assume that $\mathcal{M} \models \sigma$. This means that $\mathcal{M} \models \psi({}^{v_1}/_{S^p(0)})$, by definition of σ. Unraveling further, by definition of ψ, this means that

(3) $\mathcal{M} \models \forall v_2 \left(\theta({}^{v_0}/_{S^p(0)})({}^{v_1}/_{S^p(0)}) \longrightarrow \beta({}^x/_{v_2}) \right)$.

Since $\mathcal{M} \models A_E$, the sentence that according to (2′) is a consequence of A_E holds in $\mathcal{M}$, so that

$$\mathcal{M} \models \forall v_2 \left(\theta({}^{v_0}/_{S^p(0)})({}^{v_1}/_{S^p(0)}) \leftrightarrow v_2 = S^{\pi^{-1}(\sigma)}(0) \right).$$

In particular,

$$\mathcal{M} \models \theta({}^{v_0}/_{S^{\pi^{-1}(\psi)}(0)})({}^{v_1}/_{S^p(0)})({}^{v_2}/_{S^{\pi^{-1}(\sigma)}(0)}),$$

which by (3) implies that $\mathcal{M} \models \beta({}^x/_{S^{\pi^{-1}(\sigma)}(0)})$, as desired.

For the converse, assume that $\mathcal{M} \models \beta({}^x/_{S^{\pi^{-1}(\sigma)}(0)})$. We have to show that $\mathcal{M} \models \sigma$, which means, unraveling as above, that (3) holds. In order to do this, we have to show that whenever $a \in \mathcal{M}$ is such that

$$\mathcal{M} \models \theta({}^{v_0}/_{S^p(0)})({}^{v_1}/_{S^p(0)})[({}^{v_2}/_a)],$$

then

$$\mathcal{M} \models \beta[({}^x/_a)].$$

But by (2'), we know that if $\mathcal{M} \models \theta({}^{v_0}/_{S^p(0)})({}^{v_1}/_{S^p(0)})[({}^{v_2}/_a)]$, it follows that $\mathcal{M} \models a = S^{\pi^{-1}(\sigma)}(0)$, and since our assumption is that $\mathcal{M} \models \beta({}^x/_{S^{\pi^{-1}(\sigma)}(0)})$, this means that $\mathcal{M} \models \beta[({}^x/_a)]$, as desired.

Let's rewrite this argument, using the more suggestive notation. We have:

(a) $A_E \vdash \forall v_2 \left(\theta(\ulcorner \psi \urcorner, \ulcorner \psi \urcorner, v_2) \leftrightarrow v_2 = \ulcorner \sigma \urcorner \right)$

(b) $\sigma = \forall v_2 (\theta(\ulcorner \psi \urcorner, \ulcorner \psi \urcorner, v_2) \longrightarrow \beta({}^x/_{v_2}))$

Letting $\mathcal{M} \models A_E$, we have to show that $\mathcal{M} \models \sigma$ iff $\mathcal{M} \models \beta({}^x/_{\ulcorner \sigma \urcorner})$.

From left to right, since $\mathcal{M} \models A_E$, by (a), $\mathcal{M} \models \forall v_2 \left(\theta(\ulcorner \psi \urcorner, \ulcorner \psi \urcorner, v_2) \leftrightarrow v_2 = \ulcorner \sigma \urcorner \right)$. In particular, $\mathcal{M} \models \theta(\ulcorner \psi \urcorner, \ulcorner \psi \urcorner, \ulcorner \sigma \urcorner)$. But since $\mathcal{M} \models \sigma$, (b) tells us that then, $\mathcal{M} \models \beta({}^x/_{\ulcorner \sigma \urcorner})$.

From right to left: Assume $\mathcal{M} \models \beta({}^x/_{\ulcorner \sigma \urcorner})$. To show that $\mathcal{M} \models \sigma$, we have to see by (b) that $\mathcal{M} \models \forall v_2 (\theta(\ulcorner \psi \urcorner, \ulcorner \psi \urcorner, v_2) \longrightarrow \beta({}^x/_{v_2}))$. So let $a \in |\mathcal{M}|$ be such that $\mathcal{M} \models \theta(\ulcorner \psi \urcorner, \ulcorner \psi \urcorner, a)$. By (a), $\mathcal{M} \models a = \ulcorner \sigma \urcorner$. So since $\mathcal{M} \models \beta({}^x/_{\ulcorner \sigma \urcorner})$, it follows that $\mathcal{M} \models \beta[({}^x/_a)]$. □

Definition 5.3.2. If $\mathcal{M}$ is a model of a language $\mathcal{L}$, then let $\mathsf{Th}(\mathcal{M})$ be the set of sentences which are true in $\mathcal{M}$.

Theorem 5.3.3 (Tarski's undefinability of truth). *The set* $\widetilde{\mathsf{Th}(\mathfrak{N})}$ *is not definable in* $\mathfrak{N}$.

Proof. Assume the contrary. Note that if $\mathsf{Th}(\mathfrak{N})$ was bold-face definable, then also lightface, since every parameter can be replaced by its numeral. So there would be a formula $\beta(v_0)$ such that for every sentence φ,

$$(\mathfrak{N} \models \varphi) \iff (\mathfrak{N} \models \beta(^{v_0}/_{\ulcorner\varphi\urcorner}))\,.$$

Now, by Lemma 5.3.1, applied to the formula $\neg\beta(v_0)$, let σ be a sentence such that A_E proves that $\sigma \leftrightarrow \neg\beta(^{v_0}/_{\ulcorner\sigma\urcorner})$. Since $\mathfrak{N} \models A_E$, this sentence holds in $\mathfrak{N}$, and we get:

$$\mathfrak{N} \models \sigma \iff \mathfrak{N} \models \neg\beta(\ulcorner\sigma\urcorner) \iff \mathfrak{N} \not\models \sigma,$$

a contradiction. □

5.4 Computability and Recursiveness

For further reading on this section, I recommend [Sip06].

5.4.1 Turing Machines

Definition 5.4.1. A *Turing machine* is a tuple (of finite sets) of the form $T = \langle Q, \Sigma, \Gamma, q_0, \delta, q_+, q_- \rangle$ with:

1. Σ is a set of symbols, called the *input alphabet*,
2. $\Sigma \subseteq \Gamma$, and Γ contains a special symbol which we shall denote $\llcorner\!\lrcorner$. Γ is called the *tape alphabet*,
3. Q is the set of states.
4. $q_0 \in Q$ is the *initial state* of T, $q_+ \in Q$ is the *accepting state* and q_- is the *rejecting state.*
5. $\delta : Q \times \Gamma \longrightarrow Q \times \Gamma \times \{\mathsf{L}, \mathsf{R}\}$ is a function, and L, R are distinct fixed symbols; for definiteness, let $\mathsf{L} = 0$, $\mathsf{R} = 1$.

A *snapshot*, or *constellation* of T is a tuple of the form $c = \langle t, p, q\rangle$ such that $t : n \longrightarrow \Gamma$, for some $n \in \omega$, $p < n$ and $q \in Q$. n is the length of c.

If $c = \langle t, p, q\rangle$ is a snapshot of T of length n, then the *T-next snapshot after* c is the snapshot $c' = \langle t', p', q'\rangle$ of length n' defined as follows: Let $\delta(t(p), q)) = \langle \tilde{q}, x, d\rangle$, where $d \in \{\mathsf{L}, \mathsf{R}\}$ and $x \in \Gamma$.

1. $q' = \tilde{q}$,
2. if $d = \mathsf{R}$, then $p' = p + 1$,
3. if $d = \mathsf{L}$ and $p > 0$, then $p' = p - 1$,
4. if $d = \mathsf{L}$ and $p = 0$, then $p' = p$,
5. if $d = \mathsf{R}$ and $p = n - 1$, then $n' = n + 1$, otherwise $n' = n$,
6. $t'(l) = \begin{cases} x & \text{if } l = p, \\ t(l) & \text{if } p \neq l < n, \\ \llcorner\!\lrcorner & \text{if } l = n < n'. \end{cases}$

An *input* is a function $i : n \longrightarrow \Sigma$. The *run of* T *on input* i is the following function r with domain $N \in \omega + 1$ whose values are snapshots of T:

1. $r(0) = \langle i^\frown \llcorner\!\lrcorner, 0, q_0 \rangle$.
2. If $r(k) = \langle t, p, q \rangle$ and $q \in \{q_+, q_-\}$, then $N = k + 1$, and otherwise, $N > k + 1$.
3. If $N > k + 1$, then $r(k + 1)$ is the T-next snapshot after $r(k)$.

If r is finite, then let $\text{dom}(r) = N > 0$. The last state of r is the unique member of $\{q_+, q_-\}$ which is the last component of $r(N - 1)$.

T *accepts* an input i if the run of T on input i is finite with last state q_+. It *rejects* an input i if the run is finite with last state q_-. If the run of T on input i is finite, T is said to *terminate* on input i.

Viewing an input, which is a function $s : n \longrightarrow \Sigma$, for some n, as a word over the alphabet Σ, let's define the *language of* T (or the *language recognized by* T), $L(T)$, to be the collection of all input words that T accepts. T *decides* $L(T)$ if it terminates on all inputs, equivalently, if T has no infinite runs, equivalently, if T rejects every word that doesn't belong to $L(T)$. A Turing machine that has no infinite run is called a *decider*.

A language (i.e., a collection of words over some finite alphabet) is *Turing-recognizable (or recursively enumerable, or computably enumerable)* if it is the language of some Turing machine. It is *decidable, or recursive, or computable* if it is the language of a decider.

A set R of natural numbers is *recursive* (or *decidable*, or *computable*) if the language $L = \{1^n \mid n \in R\}$ is decidable (here, 1^n stands for the word consisting of n consecutive 1s). It is *recursively enumerable* (or *computably enumerable*) if L is.

Example 5.4.2. The language $L = \{1^{2^n} \mid n \in \omega\}$ is decidable.

Proof. We have to construct a Turing machine that is a decider and that recognizes L. The idea is to define a Turing machine that will work as follows:

1. If the input word is empty, then reject.
2. Move the head from left to right, crossing off every other 1.
3. If the tape contains only a single 1, then accept.
4. If the tape contained an odd number of 1s (greater than 1), then reject.
5. Return the head to the left end of the tape.
6. Continue with stage 2.

If we succeed in building a Turing machine that performs these steps, then it will clearly decide the desired language. Let's set:

- $Q = \{q_0, q_1, q_2, q_3, q_4, q_+, q_-\}$,
- $\Sigma = \{1\}$,
- $\Gamma = \{1, \times, \llcorner\!\lrcorner\}$.

Let δ be given by the following table:

	q_0	q_1	q_2	q_3	q_4
1	$(q_1, ␣, \mathsf{R})$	$(q_2, \times, \mathsf{R})$	$(q_3, 1, \mathsf{R})$	$(q_2, \times, \mathsf{R})$	$(q_4, 1, \mathsf{L})$
$\times$	$(q_-, \times, \mathsf{R})$	$(q_1, \times, \mathsf{R})$	$(q_2, \times, \mathsf{R})$	$(q_3, \times \mathsf{R})$	$(q_4, \times, \mathsf{L})$
␣	$(q_-, ␣, \mathsf{R})$	$(q_+, ␣, \mathsf{R})$	$(q_4, ␣, \mathsf{L})$	$(q_-, ␣, \mathsf{R})$	$(q_1, ␣, \mathsf{R})$

The machine starts out in state q_0. If the tape is blank, i.e., if the first cell contains the symbol ␣, then the input is rejected. It also switches to the reject state if it reads the symbol $\times$, but this will actually never happen. If it reads a 1, then it overwrites it with a ␣, to mark the left end of the tape, and it switches to state q_1.

In state q_1, the machine moves the head right until it reads a symbol different from $\times$. If this symbol is a ␣, then it has reached the right "end" of the tape, so there was precisely one 1 on the tape (replaced by the ␣ symbol on the first cell), and the machine accepts. If it is a 1, then the symbol is crossed out, and the machine changes to state q_2. So being in state q_1 signifies that only one 1 (replaced by ␣) has been read so far.

From now on, the machine oscillates between states q_2 and q_3. In both states, it scans the tape to the right, looking for a symbol different from $\times$. In state q_2, if that symbol is a 1, it switches to state q_3 and writes nothing. In state q_3, if that symbol is a 1, it crosses it out and switches back to state q_2. If that symbol is a ␣, then the right end of the relevant part of the tape is reached. If this happens in state q_3, then there was an odd number of 1s on the tape, so the machine switches to the reject state. If it happens in state q_2, then the number of 1s was even, so now the machine moves the head back to the beginning of the tape; this happens in state q_4. So the machine moves left until it reads the symbol ␣, which is when it switches back to state q_1, for another scan.

5.4.2 Variants of Turing Machines, Simulation, Equivalence and Church's Thesis

As an example of a variant of the Turing Machine model, lets look at Turing Machines with a finite number k of tapes. This is called a Multi Tape Turing Machine. Formally, the difference to the usual Turing machine is that the transition function now takes the form $\delta : Q \times \Gamma^k \longrightarrow Q \times \Gamma^k \times \{\mathsf{L}, \mathsf{R}\}^k$. The input is written on the first tape, and as with usual Turing Machines, the computation stops when the accept or reject state is reached. If M is a Multi Tape Turing Machine, then the language of M, denoted $L(M)$, is the collection of words over the input alphabet that result in a computation that ends in the accept state.

Lemma 5.4.3. *Multi Tape Machines and One Tape Turing Machines are equivalent, in the following sense: If M is a Multi Tape Machine, then there is a One Tape Turing Machine T such that $L(M) = L(T)$, and conversely for every One Tape Turing Machine T there is a Multi Tape Machine M such that $L(T) = L(M)$.*

Proof. Note that the direction from One Tape TMs to Multi Tape Machines is trivial, since every One Tape TM is also a Multi Tape Machine.

The idea for the substantial direction is that the One Tape TM T will *simulate* the Multi Tape TM M. Say M has k tapes. Note that at any point during a computation, M will only have used a finite amount of cells on each of its tapes. T will keep track of these k tapes by writing their relevant contents next to one another on its single tape, separated by a new symbol, say $*$. In addition, it will keep track of the locations of the different heads, as follows: For each symbol a of Ms machine alphabet Γ, it has a symbol $\breve{a}$ which it will use to mark the cell above which the heads of M are located. So in the beginning, on input $w_0 \dots w_{n-1}$, M sets the tape up so that it looks like this:

$$*\check{w}_0 w_1 \dots w_{n-1} * \check{\sqcup} * \check{\sqcup} * \dots * \check{\sqcup} *$$

To simulate the next step of the computation of M, T does the following: Its state encodes the state M is in. T moves its head from left to right across the tape, remembering the symbols the k heads of the simulated machine are reading (by changing its state correspondingly). When the head of T reaches the $k+1$-st $*$ symbol, it knows the vector of symbols the heads of M are reading, and it knows the state M is in. Now Ms transition function tells us what to do next: T remembers the state M would switch to, and it remembers the vector of symbols to write and the vector of directions to move in. Now the head of T moves to the beginning of the tape, and then to the right, updating the contents of each tape: It replaces the marked symbols $\check{a}$ with the symbol the corresponding head has to write, and it moves the $\check{}$ mark in the correct direction. If it is being moved onto a $*$ symbol (i.e., if the head of the corresponding machine is moved into a previously unused region of its tape), that $*$ is replaced by a $\check{\sqcup}$, and the rest of the tape is moved one to the right. When all tape contents have been updated, the head is moved back to the beginning of the tape, and T is ready to simulate the next step of the computation of M. □

Corollary 5.4.4. *A language is Turing-recognizable iff it is recognizable by a Multi Tape Turing Machine. It is decidable iff it is decided by a Multi Tape Turing Machine.*

There are many other variants of Turing Machines, for example the nondeterministic ones, where the transition function takes the form $\delta : Q \times \Gamma \longrightarrow \mathcal{P}(Q \times \Gamma \times \{\mathsf{L}, \mathsf{R}\})$. The interpretation is that $\delta(q, a)$ gives a set of possible next steps in the computation. So there is a set of possible runs of such a machine. The language of a nondeterministic Turing Machine is the collection of words for which *there is* a run which terminates in the accept state. A nondeterministic TM is a decider if it has no infinite runs on any inputs.

The method of simulation can be used to show:

Lemma 5.4.5. *A language is Turing-recognizable iff it is recognizable by some nondeterministic Turing Machine. It is decidable iff it is recognized by some nondeterministic decider.*

Proof. I am leaving out the details of the construction here. The idea is that a nondeterministic Turing machine N can be simulated by a deterministic three tape TM as follows: The first tape contains the input word w and is not going to be changed. The second tape is the simulation tape, its contents will be the same as the contents of the simulated machine, along a branch of the computation tree. To explain what the third tape is for, note that since the set of states as well as the tape alphabet of the nondeterministic machine are finite, there is a natural number, call it b such that $\delta(q, x)$ has at most size b, for any state q and any symbol x. So the tree of possible runs of N on input w is at most b-branching, meaning that every node in that tree has at most b immediate successors. The content of the third tape will now contain a sequence of numbers less than b. If the sequence has length n, then this sequence can be viewed as specifying a node at the n-th level of the tree. This is going to be the sequence of choices that will be made next in simulating N. When such a sequence was unsuccessfully explored (i.e., the accepting state was not reached, or the sequence didn't correspond to a valid sequence of choices), then next, the third tape is updated (the lexicographically next sequence is calculated), the second tape is erased, and the next simulation is started. It is crucial that when the third tape is updated, the shorter sequences come earlier. So a width first search is performed, instead of a depth first search. If at some point, in the simulation of N along some branch, the accept state is reached, then w is accepted. This way, if there is an accepting run of N on input w, some shortest accepting run on input w will be found. Otherwise, the process will never terminate. This shows that the deterministic (simulating) TM recognizes the same language that N recognizes, and hence proves the first part of the lemma. For the second part, the procedure needs to be improved slightly so as to make sure that the simulating machine will always terminate, granted that N has no infinite run. Again, fix an input word w. Note that the tree of runs of N on input w is a finite branching tree which has no infinite branch. So by König's Lemma, the tree must be finite. This means that if the simulating machine never will find an accepting state, sooner or later it will try searching that tree beyond its height. When this happens, it has to look no further, so all that needs to be done is to make sure it will recognize this situation. This is easily achieved: We can use a flag that is initially set to 0. When a simulation ran successfully along the length of the content of the third tape (meaning that the third tape contained a valid path), it is set to 1. When the third tape is updated, and the lexicographically next sequence is longer than the previous one (say the next sequence has length $n + 1$), then the flag is checked: If it is still 0, that means that there was no valid sequence of length n. In that case, the simulating terminates in its reject state. Otherwise, the flag is set to 0, to check whether there is a valid sequence of length $n + 1$. □

The phenomenon that variations of the computational model don't affect the class of languages described is called *robustness*. It indicates that this class of languages is very canonical, and it led to the Church-Turing Thesis, which says that this class is precisely the class of languages membership to which can be decided by an algorithm.

5.4.3 Enumerating Languages

An enumerator E can be modeled as a two-tape Turing Machine with a special "print" state. Such a machine doesn't take an input. It just starts computing and continues calculating forever. The language described by the machine is the collection of words that are written on the output tape when the machine enters the "print" state. It is called the language enumerated by E.

Lemma 5.4.6. *A language is Turing-recognizable iff it is enumerated by some enumerator. (That's why Turing-recognizable languages are also referred to as recursively enumerable).*

5.4.4 The Acceptance and the Halting Problem

As was the case when dealing with formulas in the language of arithmetic, one crucial step towards fascinating results will again be some form of Gödelization. Before, we needed to code formulas by natural numbers, so as to put them (the formulas) in the domain of objects about which they (the formulas) can speak. In the context of Turing machines the corresponding step is to code Turing machines as words, which then can be input to Turing machines. This way, Turing machines can operate on Turing machines.

It should be clear that this can be done in many ways, and it is not important which way is chosen.

First off, note that it does not matter what the states of a Turing machine actually are; all that matters is how many states a Turing machine has. Also, it does not really matter what the symbols of the input or tape alphabet of a Turing machine are. Let's say that a Turing machine is *standard* if its set of states and its set of symbols are natural numbers (plus the symbol). It is then easy to "code" a standard Turing machine by a sequence of 0s, 1s, 2s and ␣ symbols: Say the machine is the 7-tuple $\langle Q, \Sigma, \Gamma, q_0, \delta, q_+, q_- \rangle$. The word coding that machine could be:

- Q, written in binary, followed by 2 (as a separator),
- Σ, written in binary, followed by a 2,

- q_0, written in binary, followed by a 2,
- q_+, written in binary, followed by a 2,
- q_-, written in binary, followed by a 2,
- the concatenation of all strings of the form $a2b2c2d2e2$, where a is a binary string representing a number k, b is either the symbol $\llcorner$ or a binary string representing a natural number - let l be either that number or the symbol $\llcorner$, c is again a binary string representing a number m, d is again either a number or the $\llcorner$ symbol - let n stand for that object, and e is either the symbol 0 or the symbol 1, *and*

$$\delta(k, l) = \langle m, n, e \rangle.$$

  In order to make the code of a standard Turing machine unique, one can insist that these strings be listed in the lexicographical order, with $\llcorner$ coming before 0, say.

One could be more economic in terms of the number of symbols needed to code a standard Turing machine. Indeed, the above coding uses 4 symbols. But note that every word over the alphabet $\{0, 1, 2, \llcorner\}$ can be viewed as a 4-ary number, and hence easily be coded by a natural number n. This number, in turn, can be coded by the string 1^n, which is formed over an alphabet with only one symbol. One could now enumerate those natural numbers which code a standard Turing machine, from smallest to largest, say in the sequence $\langle e_i \mid i < \omega \rangle$. It should be clear by now that the function $i \mapsto e_i$ is computable. So this function gives us yet another way of coding any standard Turing machine by a natural number: i codes the Turing machine whose code as a word over $\{0, 1, 2, \llcorner\}$ is the 4-ary expansion of the number e_i. This way, every natural number codes a standard Turing machine, and every standard Turing machine is coded by a natural number. Of course, as before, natural numbers can be coded by strings over the alphabet $\{1\}$.

Since it rarely will be important which type of coding is used, lets just write $\ulcorner M \urcorner$ for some simple coding (such as above) of a standard Turing machine M by a string over some fixed alphabet (such as $\{1\}$). And in general, when X is some finitary object (i.e., something that can be viewed as being a member of V_ω), then let $\ulcorner X \urcorner$ be a string coding X.

There are two interesting languages that can now be defined, using these conventions:

$$\begin{aligned} A &= \{\ulcorner \langle M, w \rangle \urcorner \mid M \text{ is a Turing machine that accepts } w\} \\ H &= \{\ulcorner \langle M, w \rangle \urcorner \mid M \text{ is a Turing machine that terminates on input } w\} \end{aligned}$$

The latter is called the *Halting Problem,* and I'll call the former the *Acceptance Problem.*

Universal Turing Machines

A universal Turing machine U works as follows: Given an input v over its alphabet, U checks whether this string codes a standard Turing machine M, followed by an input word w for M. If this is not the case, U rejects v. Otherwise, U starts simulating the run of M on input w. Making use of the tape to take notes, U can keep track of which state M is in at each stage of the computation, and in fact of the entire snapshots M goes through. When the simulated machine enters its accept state, U accepts v, and when it enters its reject state, U rejects v. If none of these states are ever entered, U does not terminate.

It may feel strange at first that a fixed Turing machine should be able to simulate all possible Turing machines, but it's not all that surprising after all. For example, it should be clear that it is possible to write an interpreter for a programming language, such as Java, in Java. This is then a program, written in Java, that can simulate every other program thats written in Java. Similar things happen in real life - that C-compilers are written in C, for example.

Corollary 5.4.7. *The Acceptance Problem is recognizable (recursively enumerable).*

Proof. Any universal Turing Machine recognizes A. □

Corollary 5.4.8. *The Halting Problem is recognizable (recursively enumerable).*

Proof. The following procedure describes how a Turing machine will work that will recognize H:

On input v, run a universal Turing machine U on v (as a subroutine). If U terminates, either accepting or rejecting, then accept v. Otherwise the subroutine doesn't terminate, so the entire machine does not terminate. □

Diagonalization, Undecidability and Reduction

The first proof using the diagonalization method was used by Cantor in order to prove that the set of real numbers is uncountable. Here is the argument:

Theorem 5.4.9 (Cantor)**.** *Given any set x, there is no surjection $f : x \twoheadrightarrow \mathcal{P}(x)$.*

Proof. Suppose f were such a surjection. Let $d = \{y \in x \mid y \notin f(y)\}$. Since d is a subset of x, there must be an $a \in x$ such that $f(a) = d$. The question is: Is $a \in d$ or is $a \notin d$? Well, saying $a \in d$ is (by definition of d) equivalent to saying that $a \notin f(a)$, but since $f(a) = d$, this is equivalent to saying that $a \notin d$. This is a contradiction. □

This proof can be viewed as constructing a set d in such a way that its characteristic function χ_d differs from the characteristic function of every element $f(y)$ of the range of f at y: $\chi_d(y) = 1 - \chi_{f(y)}(y)$.

Theorem 5.4.10. *The Acceptance Problem is undecidable.*

Proof. Assume T was a Turing-machine deciding A. So we'd have:

$$\begin{aligned} T \text{ accepts } \ulcorner M, w \urcorner &\iff M \text{ accepts } w \\ T \text{ rejects } \ulcorner M, w \urcorner &\iff M \text{ does not accept } w. \end{aligned}$$

(Let's restrict to inputs that encode pairs of Turing-machines and input words). Then we could construct a Turing-machine D that does the following on input $\ulcorner M \urcorner$: It passes the input $\ulcorner M, \ulcorner M \urcorner \urcorner$ to T and reverses the result. So D accepts $\ulcorner M \urcorner$ if T rejects $\ulcorner M, \ulcorner M \urcorner \urcorner$, and D rejects $\ulcorner M \urcorner$ if T accepts $\ulcorner M, \ulcorner M \urcorner \urcorner$. So we have:

$$\begin{aligned} D \text{ rejects } \ulcorner M \urcorner &\iff M \text{ accepts } \ulcorner M \urcorner \\ D \text{ accepts } \ulcorner M \urcorner &\iff M \text{ does not accept } \ulcorner M \urcorner. \end{aligned}$$

The question is now: What does D do with the input $\ulcorner D \urcorner$? Well, by the equivalence above, D accepts $\ulcorner D \urcorner$ iff D does not accept $\ulcorner D \urcorner$, a contradiction. □

Theorem 5.4.11. *The Halting Problem is undecidable.*

Proof. I'll present two ways to argue here.

For the first argument, suppose (towards a contradiction) that the Halting Problem was decidable, say by a Turing machine H. Here is then a way to decide the Acceptance problem: Given a Turing Machine T, and an input word w, run H on $\ulcorner T, w \urcorner$ to see whether T terminates on input w. If it doesn't, then reject $\ulcorner T, w \urcorner$. If it does terminate, then simulate the run of T on input w. If it ends in T's accept state, then accept, and if it ends in the reject state, then reject. This is a contradiction, since we have already seen that the Acceptance Problem is undecidable.

The second argument follows the same idea of showing that if the Halting Problem was decidable, then the Acceptance Problem would also be decidable. But it uses the framework of reductions which is useful in many situations. In general, a (recursive) *reduction* of a language L to a language L' (both over the same alphabet Σ, say) is a function $f : \Sigma^* \longrightarrow \Sigma^*$ (recall that Σ^* is the collection of all words over Σ) that is recursive (see the following subsection), so that for any $w \in \Sigma^*$, $w \in L$ iff $f(w) \in L'$. It is then clear that if L' is decidable, then so is L. For a decision procedure for L works like this: Given w, compute $f(w)$ and then use the decision procedure for L' to check whether $f(w)$ belongs to L'. Accept if the result is positive, otherwise reject. In many situations, it is the contrapositive of this that's most useful: If L is not decidable, then L' is not decidable either.

Let's reduce the Acceptance Problem to the Halting Problem. The reduction takes the input $\ulcorner M, q \urcorner$ and converts M to a Turing machine M' that terminates on input w iff M accepts w. M' looks almost like M, except that it has a new reject state that will never be reached, and the transition function of M' dictates that once the reject state of M is reached, then no matter what symbol is read, that symbol is written, the head moves to the right, and the machine stays in the same state. This conversion recursive, and it obviously reduces A to H. So this shows that H is not decidable, since A is not decidable. □

Lemma 5.4.12. *If a language and its complement are recognizable, then it is decidable.*

Corollary 5.4.13. *The complement of the Halting Problem is not recognizable.*

5.4.5 Recursive and partial recursive functions, and the Recursion Theorem

The purpose of this section is to develop some of the main concepts of the classical theory. For further reading, I recommend [Soa80].

Definition 5.4.14. Let Σ be an alphabet, and as before, let Σ^* be the collection of words formed using symbols from Σ. A Turing machine T with input alphabet Σ can be viewed as computing a partial function $f : \Sigma^* \longrightarrow \Sigma^*$, namely the function that maps the word w to the word that's written on the tape when T terminates its computation on input w (more precisely, say the longest initial segment of the tape contents that forms a word over Σ). If T does not terminate, then $f(w)$ is undefined.

A function $f : \Sigma^* \longrightarrow \Sigma^*$ is recursive if (f is total and) there is a Turing machine which computes f. It is a partial recursive function if f is a partial function that's computed by a Turing machine.

As usual, one can identify natural numbers with words over the alphabet $\{1\}$, and so it makes sense to talk about recursive and partial recursive functions from ω to ω. I.e., $f : \omega \longrightarrow \omega$ is recursive if the function $1^n \mapsto 1^{f(n)}$ is computed by a Turing machine. Similarly, if a partial function from ω to ω is computed by a Turing machine, it is called a partial recursive function. Finally, a function $f : \omega^n \longrightarrow \omega$ is recursive if the function $1^{m_0} \sqcup 1^{m_1} \ldots \sqcup 1^{m_{n-1}} \mapsto$

$1^{f(m_0,m_1,\ldots,m_{n-1})}$ is computed by a Turing machine. So here, we allow the input word to contain the ␣ symbol, in order to use it as a separator.

Fixing a coding of standard Turing machines by natural numbers, let $\varphi_e^{(n)}$ be the partial be the partial n-ary function computed by the Turing machine which is coded by the natural number e. Write φ_e for $\varphi_e^{(1)}$.

Theorem 5.4.15 (Enumeration Theorem)**.** *There is a partial recursive function $\varphi_z^{(2)}$ such that for all e and x,*

$$\varphi_z^{(2)}(e,x) = \varphi_e(x).$$

Proof. Basically, z is the code of a universal Turing machine U: On input e, x, U recovers the Turing machine coded by e and simulates its run on input x, until, if ever, it reaches its halting state, making sure that when U terminates, its tape contents will be those of the simulated machine. □

Of course, a similar theorem holds for partial recursive functions of several variables.

Theorem 5.4.16 (s-m-n Theorem)**.** *Given $n, m \geq 1$, there is an injective recursive function $s_n^m : \omega^{m+1} \longrightarrow \omega$ such that for all $x, y_0 \ldots, y_{m-1} \in \omega$, the following holds:*

$$\varphi^{(n)}_{s_n^m(x,y_0,\ldots,y_{m-1})}(z_0,\ldots,z_{n-1}) = \varphi_x^{(m+n)}(y_0,\ldots,y_{m-1},z_0,\ldots,z_{n-1}),$$

for all $z_0, \ldots, z_{n-1} \in \omega$ (in the sense that the left hand side of this equation is defined iff the right hand side is, and if defined, both sides are equal.

Proof. Here is how a Turing machine will work that will compute a preliminary function $\bar{s}_n^m$. On input $x, y_0, \ldots, y_{m-1}$:

1. Recover the Turing Machine with code x, call it T.
2. Modify T to produce a Turing Machine T' that works as follows:
   (a) On input $z_0, \ldots, z_{n-1}$, write $y_0, \ldots, y_{m-1}, z_0, \ldots, z_{n-1}$ on the tape.
   (b) Move the head to the beginning of the tape and switch to the start state of T.
   (c) Pass control to T.
3. Output the code of T'.

$\bar{s}_n^m$ might fail to be injective. Here is a procedure that fixes this, working with a two tape machine. On input $x, y_0, \ldots, y_{m-1}$:

1. For every input $x', y'_0, \ldots, y'_{m-1}$ that comes lexicographically not after $x, y_0, \ldots, y_{m-1}$ (when viewed as sequences of 1s and ␣s - as usual, shorter sequences come first):
   (a) Calculate $e = \bar{s}_n^m(x', y'_0, \ldots, y'_{m-1})$.
   (b) If that value is smaller than or equal to the number k that's stored on the second tape (which initially is 0), then modify the Turing Machine coded by e by adding unused states until the code of the modified Turing Machine is larger than k. Now write that number on the second tape.
2. Output the content of the second tape.

□

Theorem 5.4.17 (Recursion Theorem, Kleene)**.** *For every recursive function $f : \omega \longrightarrow \omega$, there is an n such that $\varphi_n = \varphi_{f(n)}$. (Such a number n is called a fixed point of f.)*

Proof. Consider the function ψ defined by:

$$\psi(u,z) = \begin{cases} \varphi_{\varphi_u(u)}(z) & \text{if } u \in \mathrm{dom}(\varphi_u) \text{ and } z \in \mathrm{dom}(\varphi_{\varphi_u(u)}), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

So ψ is a partial function from $\omega \times \omega$ to ω. Clearly, it is a partial recursive function. So let $\psi = \varphi_x^{(2)}$. Let $d(u) = s_1^1(x,u)$. So d is recursive, and we have:

$$\psi(u,z) = \varphi_x^{(2)}(u,z) = \varphi_{s_1^1(x,u)}(z) = \varphi_{d(u)}(z).$$

So we have now found a recursive function d (independent of f) with:

$$\varphi_{d(u)}(z) = \begin{cases} \varphi_{\varphi_u(u)}(z) & \text{if } u \in \mathrm{dom}(\varphi_u) \text{ and } z \in \mathrm{dom}(\varphi_{\varphi_u(u)}), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Of course, $f \circ d$ is recursive, too, so we can choose an index v so that

$$f \circ d = \varphi_v.$$

Let $n = d(v)$. The claim is that n is a fixed point of f. Note that φ_v is total, so that in particular, $v \in \mathrm{dom}(\varphi_v)$. So by definition of d, it follows that $\varphi_{d(v)} = \varphi_{\varphi_v(v)}$. We get:

$$\varphi_n = \varphi_{d(v)} = \varphi_{\varphi_v(v)} = \varphi_{f(d(v))} = \varphi_{f(n)}.$$

□

Definition 5.4.18. Let $W_e = \mathrm{dom}(\varphi_e)$. So $\langle W_e \mid e \in \omega \rangle$ enumerates all recursively enumerable sets of natural numbers.

To illustrate a use of the Recursion Theorem, here is an application.

Theorem 5.4.19. *There is no partial recursive function ψ such that for every x with the property that W_x is recursive, $\varphi_{\psi(x)}$ is the characteristic function of W_x.*

Proof. Assuming there was such a ψ, define a recursive set W_n by:

$$W_n = \begin{cases} \{0\} & \text{if } n \in \mathrm{dom}(\psi) \text{ and } \varphi_{\psi(n)}(0) = 0, \\ \emptyset & \text{otherwise.} \end{cases}$$

If the reader accepts that such a W_n can be found, then we have reached a contradiction, since $0 \in W_n$ iff $\varphi_{\psi(n)}(0) = 0$, so $\varphi_{\psi(n)}$ is not the characteristic function of W_n, even though W_n is recursive.

The above "definition" of W_n was an informal use of the Recursion Theorem, combined with the *s-m-n* Theorem. To fill in the details, let

$$\psi'(n,m) = \begin{cases} 1 & \text{if } m = 0, n \in \mathrm{dom}(\psi) \text{ and } \varphi_{\psi(n)}(0) = 0, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Since ψ' is partial recursive, we can find x such that $\psi' = \varphi_x^{(2)}$. Letting $f(n) = s_1^1(x,n)$, we get $\varphi_{f(n)}(m) = \psi'(n,m)$. Since f is recursive, the Recursion Theorem applies, so we can find an n such that $\varphi_{f(n)} = \varphi_n$. For this n, we have:

$$\varphi_n(m) = \begin{cases} 1 & \text{if } m = 0, n \in \mathrm{dom}(\psi) \text{ and } \varphi_{\psi(n)}(0) = 0, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

So W_n is as wished. □

5.5 Gödel's Incompleteness Theorems

The following theorem could have been shown right after defining the concept of a recursive set of natural numbers.

Theorem 5.5.1. *Let $A \subseteq \omega$. Then the following are equivalent:*

1. *A is recursive.*
2. *A is $\Delta_1(\mathrm{V}_\omega)$.*
3. *$\pi``A$ is $\Delta_1(\mathrm{V}_\omega)$.*
4. *A is representable.*

Proof. $1 \Longrightarrow 2$: Let T be a decider for A. Then $n \in A$ iff in V_ω, the following holds: There is a natural number m and a function with domain m such that "f is the run of T on input 1^n", and the state of $f(m-1)$ is the accept state of T. The statement "f is the run of T on input 1^n" is easily seen to be Σ_0 (but it suffices that it is Σ_1). So far, we have shown that A is $\Sigma_1(\mathrm{V}_\omega)$. But of course, the complement of A is similarly definable: $n \notin A$ iff in V_ω, there is a natural number m and a function with domain m such that "f is the run of T on input 1^n", and the state of $f(m-1)$ is the reject state of T. Note that T was used in the definition of A as a parameter here. Later, it will become clear that every element of V_ω can be defined in V_ω without using a parameter by a Δ_1-formula. So no parameters are actually needed, but that is not a major concern at this point.

$2 \Longrightarrow 3$: We had shown previously that π is $\Delta_1(\mathrm{V}_\omega)$. Using this, we see that

$$n \in \pi``A \iff \mathrm{V}_\omega \models \exists m\ (\underbrace{``m \in A"}_{\Sigma_1} \wedge \underbrace{``n = \pi(m)"}_{\Sigma_1}),$$

which is Σ_1, and similarly,

$$n \notin \pi``A \iff \mathrm{V}_\omega \models \exists m\ (\underbrace{``m \notin A"}_{\Sigma_1} \wedge \underbrace{``n = \pi(m)"}_{\Sigma_1}),$$

which is also Σ_1.

$3 \Longrightarrow 4$: By 3, $\pi``A$ is $\Delta_1(\mathrm{V}_\omega)$, so by Theorem 5.2.8, it follows that $A = \pi^{-1}``(\pi``A)$ is representable.

$4 \Longrightarrow 1$: That A is representable means that there is an A_E-formula $\varphi(v)$ such that for all $m < \omega$,

$$\begin{array}{rcl} m \in A & \iff & A_E \vdash \varphi(\dot{m}), \text{ and} \\ m \notin A & \iff & A_E \vdash \neg\varphi(\dot{m}). \end{array}$$

But the it is easy to make a Turing machine that decides A as follows: On input m, build the search trees S searching for a proof of $\varphi(\dot{m})$ and T searching for a proof of $\neg\varphi(\dot{m})$ simultaneously, level by level. One of them has to be finite (producing a proof), since φ is numeralwise determined. If it is S, then accept, and if it is T, then reject. $\square$

5.5.1 Incompleteness of Number Theory

Gödel's First Incompleteness Theorem

Recommended reading for this part: [End72, 3.7] Here is an immediate consequence of Tarski's undefinability of truth.

Corollary 5.5.2. *The set* $\widetilde{\mathsf{Th}(\mathfrak{N})}$ *is not recursive.*

Proof. If the set $\widetilde{\mathsf{Th}(\mathfrak{N})} = \pi^{-1}``\mathsf{Th}(\mathfrak{N})$ was recursive, then by the previous theorem, this would mean that it is representable. Being representable means precisely being definable over $\mathfrak{N}$ by a formula that's numeralwise determined. But Tarski's undefinability of truth says precisely that it is not definable over $\mathfrak{N}$, a contradiction. □

Definition 5.5.3. For a set Σ of sentences, let $\Sigma^{\vdash}$, the *deductive closure of* Σ, be the set of sentences which are provable from Σ. Σ is *complete* if for every sentence φ, φ or $\neg\varphi$ is in Σ.

Theorem 5.5.4 (Gödel's first Incompleteness Theorem)**.** *If* $\Sigma \subseteq \mathsf{Th}(\mathfrak{N})$ *is recursively enumerable (meaning that* $\pi^{-1}``\Sigma$ *is recursively enumerable), then* $\Sigma^{\vdash}$ *is incomplete.*

Proof. Suppose $\Sigma^{\vdash}$ was complete. Then $\pi^{-1}``(\Sigma^{\vdash})$ would be recursive: Given φ, either $\Sigma \vdash \varphi$ or $\Sigma \vdash \neg\varphi$. So searching for a proof of φ and a proof for $\neg\varphi$ from Σ in parallel is possible (since Σ is recursively enumerable), and it is a process that terminates and hence enables us to decide $\Sigma^{\vdash}$.

But at the same time, the assumption that $\Sigma^{\vdash}$ is complete has another consequence, namely that $\Sigma^{\vdash} = \mathsf{Th}(\mathfrak{N})$!

The inclusion from left to right follows since $\Sigma \subseteq \mathsf{Th}(\mathfrak{N})$, so $\Sigma^{\vdash} \subseteq \mathsf{Th}(\mathfrak{N})^{\vdash} = \mathsf{Th}(\mathfrak{N})$.

For the converse, let $\varphi \in \mathsf{Th}(\mathfrak{N})$. If $\varphi \notin \Sigma^{\vdash}$, then by completeness of $\Sigma^{\vdash}$, $\neg\varphi \in \Sigma^{\vdash}$, so that by the inclusion from left to right, $\neg\varphi \in \mathsf{Th}(\mathfrak{N})$, which is a contradiction.

So putting these two consequences together results in $\mathsf{Th}(\mathfrak{N})$ being recursive, which contradicts Corollary 5.5.2. □

Theorem 5.5.5 (Strong Undecidability)**.** *Let* T *be a set of* A_E*-sentences such that* $A_E \cup T$ *is consistent. Then* $T^{\vdash}$ *is not recursive.*

Proof. Assume $T^{\vdash}$ was recursive. Then $T' := (A_E \cup T)^{\vdash}$ would also be recursive: To decide whether a sentence φ belongs to T', do the following. Let χ be the conjunction of all A_E-axioms, and ask whether the sentence $(\chi \longrightarrow \varphi)$ is in $T^{\vdash}$. If so, φ belongs to T', and if not, it doesn't. The question whether $(\chi \longrightarrow \varphi)$ belongs to $T^{\vdash}$ is clearly decidable, so all that remains is to show that this is equivalent to the statement that $(A_E \cup T) \vdash \varphi$.

So it needs to be checked that

$$T \vdash (\chi \longrightarrow \varphi) \iff (A_E \cup T) \vdash \varphi.$$

For the direction from left to right, Let M be a model of $A_E \cup T$. In particular, $M \models T$. By the left hand side, $M \models (\chi \longrightarrow \varphi)$. But since $M \models A_E$, it follows that $M \models \chi$. So $M \models \varphi$. For the converse, let $M \models T$. We have to show that $M \models (\chi \longrightarrow \varphi)$, assuming the right hand side is true. If $M \models \neg\chi$, then nothing needs to be shown. But if $M \models \chi$, then $M \models (A_E \cup T)$, and hence, by the right hand side, $M \models \varphi$. But then, trivially, $M \models (\chi \longrightarrow \varphi)$.

So we have seen now that $T' = (A_E \cup T)^{\vdash}$ is recursive by our assumption that $T^{\vdash}$ is recursive. And by Theorem 5.5.1, this means that $\widetilde{T'}$ is representable by some formula $\beta(x)$. The Fixed Point Lemma 5.3.1, applied to the formula $\neg\beta$, now produces a sentence σ such that

$$A_E \vdash (\sigma \leftrightarrow \neg\beta(\ulcorner\sigma\urcorner).$$

So intuitively, σ says "I am not in T'". Now the question arises: Is σ in T' or not? (I.e., is σ true or false?)

If $\sigma \notin T'$, then $A_E \vdash \neg\beta(\ulcorner\sigma\urcorner)$, which is equivalent to $A_E \vdash \sigma$, which, in turn, means that σ is in $A_E^{\vdash}$, and in particular that $\sigma \in T'$. So this can't be.

So $\sigma \in T'$. But this means that $A_E \vdash \beta(\ulcorner\sigma\urcorner)$, and hence $A_E \vdash \neg\sigma$, which implies that $\neg\sigma \in T'$. So T' would contain both σ and $\neg\sigma$, rendering $A_E \cup T$ inconsistent. This is a contradiction. □

Theorem 5.5.6 (Church)**.** *The set of valid A_E-sentences $\emptyset^{\vdash}$ is not recursive.*

Proof. Apply the previous Theorem 5.5.5 with $T = \emptyset$. □

Corollary 5.5.7. *If a set of A_E-sentences T is such that T is recursive and $A_E \cup T$ is consistent, then $T^{\vdash}$ is not complete.*

Proof. If $T^{\vdash}$ was complete, then by the argument in the proof of Theorem 5.5.4, it would follow that $T^{\vdash}$ is recursive, but this contradicts Theorem 5.5.5. □

Gödel's Second Incompleteness Theorem

Lemma 5.5.8. *Let A be a recursive set of sentences. Then the set*

$$P_A := \{\langle d, \varphi\rangle \mid d \textit{ is a proof of } \varphi \textit{ from } A\}$$

is $\Delta_1(\mathrm{V}_\omega)$. So the pullback $\widetilde{P_A}$ is recursive, and hence representable in A_E.

So there is a formula $\varphi_A(x, y)$ such that

$$\begin{aligned}(A_E \vdash \varphi_A(\dot{d}, \ulcorner\psi\urcorner)) &\iff \pi(d) \text{ is a proof of } \psi \text{ from } A,\\ (A_E \vdash \neg\varphi_A(\dot{d}, \ulcorner\psi\urcorner)) &\iff \pi(d) \text{ is not a proof of } \psi \text{ from } A.\end{aligned}$$

I will write

$$\text{“}A \vdash \psi\text{” for the formula } \exists x\ \varphi_A(x, \ulcorner\psi\urcorner).$$

Lemma 5.5.9. *Let A be a recursive set of sentences.*

1. *If $A \vdash \varphi$, then $A_E \vdash$ "$A \vdash \varphi$".*
2. *If $A_E \subseteq A^{\vdash}$, then*

$$A \vdash \varphi \implies A \vdash \text{“}A \vdash \varphi\text{”}.$$

Proof. The second part follows immediately from the first part, since $A_E^{\vdash} \subseteq A^{\vdash}$, by assumption. But the first part is clear, since if $A \vdash \varphi$, then there is a proof p of φ from A. Letting $d = \pi^{-1}(p)$, this means that $A_E \vdash \varphi_A(\dot{d}, \ulcorner\varphi\urcorner)$. But then clearly, $A_E \vdash \exists x\ \varphi_A(x, \ulcorner\psi\urcorner)$. □

Definition 5.5.10. Let's say a recursive set of sentences is *sufficiently strong* if

1. $A_E \subseteq A^{\vdash}$ - so by Lemma 5.5.9, $A \vdash \varphi \implies A \vdash$ "$A \vdash \varphi$",
2. For every sentence φ, $A \vdash$ ("$A \vdash \varphi$" $\longrightarrow$ "$A \vdash$ "$A \vdash \varphi$""),
3. For any sentences φ and ψ:

$$A \vdash (\text{“}A \vdash (\varphi \longrightarrow \psi)\text{”} \longrightarrow (\text{“}A \vdash \varphi\text{”} \longrightarrow \text{“}A \vdash \psi\text{”})).$$

Definition 5.5.11. Let A be a recursive set of sentences, and let $T = A^{\vdash}$. Set:

$$\text{“}\mathsf{con}(T)\text{”} := \neg\text{“}A \vdash (0 = \dot{1})\text{”},$$

and $\mathsf{con}(A)$ has the same meaning.

Theorem 5.5.12 (Gödel's Second Incompleteness Theorem)**.** *Let $T = A^{\vdash}$ be a recursively axiomatizable, sufficiently strong theory. Then*

$$T \vdash \text{“}\mathsf{con}(T)\text{”} \iff T \textit{ is inconsistent.}$$

Proof. Suppose $T \vdash$ "$\mathsf{con}(T)$". By the Fixed Point Lemma, let σ be a sentence such that

$$A_E \vdash (\sigma \longleftrightarrow \neg\text{“}A \vdash \sigma\text{”}).$$

Then

$$A \vdash (\sigma \longrightarrow (\text{“}A \vdash \sigma\text{”} \longrightarrow (0 = \dot{1}))),$$

since $A \vdash (\sigma \longrightarrow \neg\text{“}A \vdash \sigma\text{”})$. By 1.) of Definition 5.5.10, it follows that

$$A \vdash \text{“}A \vdash (\sigma \longrightarrow (\text{“}A \vdash \sigma\text{”} \longrightarrow (0 = \dot{1})))\text{”},$$

which yields, by 3.),

$$A \vdash \text{“}A \vdash \sigma\text{”} \longrightarrow \text{“}(A \vdash \text{“}A \vdash \sigma\text{”} \longrightarrow \neg\text{“}\mathsf{con}(T)\text{”})\text{”},$$

using Modus Ponens. More precisely, let's write $\psi = \text{“}A \vdash \sigma\text{”} \longrightarrow (0 = \dot{1})$. Then we have seen that

$$A \vdash (\sigma \longrightarrow \psi).$$

By property 1.), we get

$$A \vdash \text{“}A \vdash (\sigma \longrightarrow \psi)\text{”}.$$

Independently of this, property 3.) tells us that

$$A \vdash (\text{“}A \vdash (\sigma \longrightarrow \psi)\text{”} \longrightarrow (\text{“}A \vdash \sigma\text{”} \longrightarrow \text{“}A \vdash \psi\text{”})).$$

But since $A \vdash \text{“}A \vdash (\sigma \longrightarrow \psi)\text{”}$, this implies that

$$A \vdash (\text{“}A \vdash \sigma\text{”} \longrightarrow \text{“}A \vdash \psi\text{”})).$$

Substituting ψ gives:

$$A \vdash (\underbrace{\text{“}A \vdash \sigma\text{”}}_{\chi_1} \longrightarrow \underbrace{\text{“}A \vdash (\text{“}A \vdash \sigma\text{”} \longrightarrow (0 = \dot{1}))\text{”}}_{\chi_2})).$$

Using 3.) again,

$$A \vdash (\underbrace{\text{“}A \vdash (\text{“}A \vdash \sigma\text{”} \longrightarrow (0 = \dot{1}))\text{”}}_{\chi_2} \longrightarrow \underbrace{(\text{“}A \vdash \text{“}A \vdash \sigma\text{””} \longrightarrow \text{“}A \vdash (0 = \dot{1})\text{”})}_{\chi_3})$$

Putting these last lines together, we can conclude that $A \vdash (\chi_1 \longrightarrow \chi_3)$, i.e.,

$$A \vdash (\text{“}A \vdash \sigma\text{”} \longrightarrow (\text{“}A \vdash \text{“}A \vdash \sigma\text{””} \longrightarrow \underbrace{\text{“}A \vdash (0 = \dot{1})\text{”}}_{\neg\text{“}\mathsf{con}(T)\text{”}})).$$

Since $A \vdash (\text{“}A \vdash \sigma\text{”} \longrightarrow \text{“}A \vdash \text{“}A \vdash \sigma\text{””})$, it follows that

$$A \vdash (\text{“}A \vdash \sigma\text{”} \longrightarrow \neg\text{“}\mathsf{con}\, T\text{”}).$$

This is equivalent to

$$A \vdash (\text{“}\mathsf{con}\, T\text{”} \longrightarrow \neg\text{“}A \vdash \sigma\text{”}).$$

Note that so far, we didn't use the assumption that $T \vdash \mathsf{con}(T)$. All of the above uses only that T is sufficiently strong and the choice of σ. But now, since $T \vdash \mathsf{con}(T)$ by assumption, it follows that

$$A \vdash \neg\text{“}A \vdash \sigma\text{”}.$$

But by our choice of σ,

$$A \vdash (\sigma \longleftrightarrow \neg\text{“}A \vdash \sigma\text{”}),$$

so

$$A \vdash \sigma,$$

which implies that

$$A \vdash \text{“}A \vdash \sigma\text{”},$$

by Lemma 5.5.9. So $A \vdash \text{“}A \vdash \sigma\text{”}$ and $A \vdash \neg\text{“}A \vdash \sigma\text{”}$, which means that A, and hence T, is inconsistent. □

Definition 5.5.13. Peano Arithmetic (PA) is the set of sentences consisting of the axioms A_E, together with the induction scheme

$$(\varphi(0) \wedge (\forall x(\varphi(x) \longrightarrow \varphi(S(x))))) \longrightarrow \forall x \varphi(x).$$

Fact 5.5.14. *Peano Arithmetic is sufficiently strong.*

5.5.2 Incompleteness of Set Theory

It would be possible to derive a version of the Second Incompleteness Theorem 5.5.12 by "interpreting A_E in set theory", as is done in [End72]. Instead, let's try to redo the relevant steps in Set Theory directly. So we try to replace A_E with ZFC (or a weaker sub-theory thereof, such as ZF^{--}_F). One relevant difference between A_E and ZFC is that in A_E, we had numerals at our disposal, which enabled us to easily transform formulas using natural numbers as parameters into sentences. In set theory, we don't have any constant or function symbols, so we have to find a substitute for this. The solution is that we can define each natural number by a formula: If n is a natural number, then $x = n$ iff x is transitive, linearly ordered by ϵ, and x has exactly n elements. The latter can be expressed by the formula saying that there are distinct $x_0 \in x$, $x_1 \in x$, ..., $x_{n-1} \in x$ such that for every $y \in x$, $y = x_0$ or $y = x_1$ or ... or $y = x_{n-1}$. Let's denote the Σ_0-formula expressing that $x = n$ by $\varphi_n(x)$. This already allows us to imitate the substitution of a numeral for a free variable in a formula. But it would be even more convenient to be able to substitute any elements of V_ω in a formula. This can be done using the definition of $\pi : \omega \longrightarrow \mathrm{V}_\omega$ - we saw that it is $\Delta_1(\mathrm{V}_\omega)$. Thus, let us use the following notation: If $\varphi(x)$ is a formula and $a \in \mathrm{V}_\omega$, then let $\varphi(\ulcorner a \urcorner)$ be the sentence defined as follows: Let $a = \pi(n)$. Then

$$\varphi(\ulcorner a \urcorner) = \exists x \exists y \quad (\varphi_n(y) \wedge \text{“}x = \pi(y)\text{”} \wedge \varphi(x))$$

where "$x = \pi(y)$" is substituted by the formula defining π. Note that if we develop logic within set theory, and consequently may view φ itself as a member of V_ω, then the map $\langle \varphi, a \rangle \mapsto \varphi(\ulcorner a \urcorner)$ is $\Delta_1(\mathrm{V}_\omega)$, and hence recursive. We can now redo the Fixed Point Lemma:

Lemma 5.5.15. *For any formula $\beta(x)$ in the language of set theory, there is a sentence σ such that*

$$\mathsf{ZFC} \vdash (\sigma \longleftrightarrow \beta(\ulcorner\sigma\urcorner)).$$

Theorem 5.5.16. *Let T be a set of sentences in the language of set theory such that $\mathsf{ZFC} \cup T$ is consistent. Then $T^{\vdash}$ is not recursive.*

Proof. (Sketch) Recall that it was crucial in the proof of the corresponding theorem in the context of number theory that the axiom system A_E is finite. The first step in the proof was to show that if T was recursive, then $(A_E \cup T)^{\vdash}$ would be recursive. Here, it is not the case that ZFC is finite. But the proof of the original theorem can be imitated as follows: In ZFC, the structure $\langle \omega, 0, S, +, \cdot, E\rangle$ is definable. Using the formulas defining ω and the arithmetic operations, the axioms A_E can be expressed in the language of set theory. For example, the axiom $\forall v_0\ \neg S(v_0) = 0$ becomes $\forall v_0(v_0 \in \omega \longrightarrow \neg(v_0 = \{\emptyset\}))$. So there is a translation of A_E-formulas φ to formulas in the language of set theory $t(\varphi)$. Of course, all translations of A_E-formulas are provable in ZFC, and also, the formula $\omega \neq \emptyset$ and the formulas expressing that $+$, $\cdot$ and E are binary functions on ω and that S is a unary function on ω are provable in ZFC. Let χ be the conjunction of all of these formulas. Suppose that $T' = (T \cup \{\chi\})^{\vdash}$ was recursive. Let Δ be the set of A_E-sentences whose translations are in T'. It follows that Δ is consistent (since any model of T' gives rise to a model of Δ in a straightforward way), and that $A_E \subseteq \Delta$. So Δ is not recursive, by 5.5.5. But then it follows that T is not recursive. For if T were recursive, we could decide whether a sentence φ belongs to Δ by checking whether $(\chi \longrightarrow t(\varphi))$ belongs to T - the translation t is recursive. This is a contradiction. □

For more on the method of translating formulas as in the previous proof ("interpretations between theories"), see [End72, 2.7].

And as before, we emphasize the special case where $T = \emptyset$, and note a corollary:

Theorem 5.5.17. *The set of valid sentences in the language of set theory is not recursive.*

Corollary 5.5.18. *If a set T of sentences in the language of set theory is recursive and $\mathsf{ZFC} \cup T$ is consistent, then $T^{\vdash}$ is not complete. (In particular, $\mathsf{ZFC}^{\vdash}$ is not complete).*

Let's now head for the Second Incompleteness Theorem for Set Theory. Let A be a set of sentences in the language of set theory that's $\Delta_1(\mathrm{V}_\omega)$. As before, it follows that the relation

$$P_A = \{\langle d, \varphi\rangle \mid d \text{ is a proof of } \varphi \text{ from } A\}$$

is $\Delta_1(\mathrm{V}_\omega)$. Let $\varphi_A(x, y)$ be a Σ_1-formula defining P_A, and let "$A \vdash \varphi$" stand for the Σ_1 sentence

$$\exists d \quad \varphi_A(d, \ulcorner\varphi\urcorner).$$

Note that when we wrote $A \vdash \varphi$ in these notes, then since logic is developed within set theory, it is actually the sentence "$A \vdash \varphi$" that we mean. So the distinction between $A \vdash \varphi$ and "$A \vdash \varphi$" is not really necessary, but it emphasizes the parallels to the development in the previous section.

We then get the following analog of Lemma 5.5.9:

Lemma 5.5.19. *Let A be a recursive set of sentences in the language of set theory.*

1. *If $A \vdash \varphi$, then $\mathsf{ZFC} \vdash$ "$A \vdash \varphi$".*
2. *If $\mathsf{ZFC} \subseteq A^{\vdash}$, then*

$$A \vdash \varphi \implies A \vdash \text{"}A \vdash \varphi\text{"}.$$

To see this, one could repeat the proof of the original theorem. Alternatively, it follows because ZFC (or even a fragment thereof) serves as our metatheory.

Theorem 5.5.20. *Let $\mathsf{ZFC} \subseteq A^{\vdash}$, where A is a recursive set of sentences in the language of set theory. Then A is sufficiently strong:*

1. $A \vdash \varphi \implies A \vdash$ "$A \vdash \varphi$",
2. *For every sentence φ,* $A \vdash$ ("$A \vdash \varphi$" $\longrightarrow$ "$A \vdash$ "$A \vdash \varphi$""),
3. *For any sentences φ and ψ:*

$$A \vdash (\text{“}A \vdash (\varphi \longrightarrow \psi)\text{”} \longrightarrow (\text{“}A \vdash \varphi\text{”} \longrightarrow \text{“}A \vdash \psi\text{”})).$$

Proof. 1 is part two of Lemma 5.5.19.

To see 2, consider what part 1 of the lemma says: $A \vdash \varphi \implies A \vdash$ "$A \vdash \varphi$". We proved this in ZFC. So what we actually showed was:

$$\mathsf{ZFC} \vdash (A \vdash \varphi \implies A \vdash \text{“}A \vdash \varphi\text{”}).$$

But this is just a less precise way of saying that

$$\mathsf{ZFC} \vdash (\text{“}A \vdash \varphi\text{”} \longrightarrow \text{“}A \vdash \text{“}A \vdash \varphi\text{””}).$$

Since $\mathsf{ZFC} \subseteq A^{\vdash}$, part 2 follows.

Part 3 follows similarly. Note that it is generally true, for any theory T, that if $T \vdash (\varphi \longrightarrow \psi)$, then $T \vdash \varphi$ implies $T \vdash \psi$. For example, this can be seen using Correctness and Completeness. All of these arguments have been carried out with ZFC as the metatheory. So what we have actually shown is (replacing T with A):

$$\mathsf{ZFC} \vdash (\text{“}A \vdash (\varphi \longrightarrow \psi)\text{”} \longrightarrow (\text{“}A \vdash \varphi\text{”} \longrightarrow \text{“}A \vdash \psi\text{”})).$$

Again, the claim follows from the assumption that $\mathsf{ZFC} \subseteq A^{\vdash}$. □

Definition 5.5.21. Let A be a recursive set of sentences in the language of set theory, and let $T = A^{\vdash}$. Write $\mathsf{con}(T)$ for the sentence

$$\neg\text{“}A \vdash \exists x\ (x \neq x)\text{”}.$$

Theorem 5.5.22 (Gödel's Second Incompleteness Theorem for Set Theory)**.** *Let $T = A^{\vdash}$ be a recursively axiomatizable theory in the language of set theory such that $\mathsf{ZFC} \subseteq T$. Then*

$$T \vdash \mathsf{con}(T) \iff T \text{ is inconsistent.}$$

Proof. By Theorem 5.5.20, T is sufficiently strong, since $\mathsf{ZFC} \subseteq T$. So the proof of Theorem 5.5.12 goes through. □

5.6 Large Cardinals

Recall Lemma 2.3.47, which, among other things, said:

1. Every $x \in \mathrm{V}_\omega$ is finite.
2. If $u \subseteq \mathrm{V}_\omega$ is finite, then $u \in \mathrm{V}_\omega$.

The import of the second point is that it implies that V_ω satisfies Replacement: If $F : \mathrm{V}_\omega \longrightarrow \mathrm{V}_\omega$ is a function (definable over V_ω, but that's not needed for the argument) and $a \in \mathrm{V}_\omega$, then since a is finite, it follows that $F``a$ is finite, hence a finite subset of V_ω, and hence a member of V_ω. All the other axioms of ZFC, except for Infinity, hold in V_ω as well. So it would be worthwhile to search for an ordinal larger than ω that still satisfies the corresponding analogs of the above properties. Recall Definition 2.4.5, where we defined the cardinality of a set to be the smallest ordinal such that there is a bijection between the set and the ordinal. A cardinal is an ordinal κ whose cardinality is κ itself. So we are looking for a cardinal $\kappa > \omega$ such that:

1. Every $x \in \mathrm{V}_\kappa$ has cardinality less than κ.
2. If $u \subseteq \mathrm{V}_\kappa$ has cardinality less than κ, then $u \in \mathrm{V}_\kappa$.

Let's call such a cardinal κ (strongly) inaccessible.

Lemma 5.6.1. *Suppose κ is inaccessible. Then $M := \langle \mathrm{V}_\kappa, \in \restriction \mathrm{V}_\kappa \rangle \models \mathsf{ZFC}$.*

Proof. To clarify, we are assuming ZFC in the meta-theory here. Note that what the lemma says is that the statement "$\forall \kappa$ (if κ is inaccessible, then $\forall x \in \mathsf{ZFC} \quad \langle \mathrm{V}_\kappa, \in \restriction \mathrm{V}_\kappa \rangle \models x$" is provable in ZFC. Notice the difference between this and the related statement that for every ZFC-axiom φ, ZFC proves that if κ is inaccessible, then $\langle \mathrm{V}_\kappa, \in \restriction \mathrm{V}_\kappa \rangle \models \varphi$. The difference is that in the statement we are about to prove, we actually quantify over the ZFC-axioms at the object level (and these do not necessarily correspond to actual ZFC-axioms in the meta-theory), while the other (weaker) version of the statement is a scheme of ZFC-theorems, one for each ZFC-axioms (and the quantification over the ZFC-axioms occurs in the meta-theory).

It is obvious that Set Existence holds in M. To check foundation, let $\varphi(x, y)$ be any formula (in the object level - this may not correspond to an actual meta-theoretical formula; it is a set). Since it matters here, let me write u for this formula. So $u \in \mathrm{V}_\omega$. Let $b \in M$, and let $A = \{a \in M \mid M \models u[a, b]\} \neq \emptyset$. Then $A \subseteq M$ is a nonempty set, and by Foundation in V, it has an $\in$-minimal member, c. It follows that $c \in A \subseteq M$, and it is not hard to see that M also believes that c is minimal in the set defined by u, using b as a parameter.

Since κ is a limit ordinal, M satisfies Pairing and Union. Note that in verifying the details, it is useful that Σ_0 statements are absolute between M and V, since M is transitive. V_κ satisfies Power Set: Let $a \in \mathrm{V}_\kappa$. Let $\alpha < \kappa$ be such that $a \in \mathrm{V}_\alpha$. Since V_α is transitive, it follows that $a \subseteq \mathrm{V}_\alpha$. But then, every $b \subseteq a$ is also a subset of V_α, and hence a member of $\mathrm{V}_{\alpha+1}$. So $\mathcal{P}(a) \subseteq \mathrm{V}_{\alpha+1}$. So $\mathcal{P}(a) \in \mathrm{V}_{\alpha+2} \subseteq \mathrm{V}_\kappa$. So again, Power Set just follows from the fact that κ is a limit ordinal. Separation holds in V_κ just because it holds in V. The crucial axiom is replacement. But this follows exactly as in the case of V_ω: If $F : \mathrm{V}_\kappa \longrightarrow \mathrm{V}_\kappa$ and $a \in \mathrm{V}_\kappa$, then the cardinality of a is less than κ, so the cardinality of $F``a$ is less than $\kappa$, and hence, $F``a$ is a subset of V_κ of size less than κ, so $F``a \in \mathrm{V}_\kappa$. □

Something even stronger is true: For every $A \subseteq \mathrm{V}_\kappa$, $\langle \mathrm{V}_\kappa, A, \in \rangle \models \mathsf{ZFC}_A$, where in ZFC_A, the formulas occurring in the axiom schemes are formed in the language with a predicate symbol for A. In fact, this characterization is equivalent to the strong inaccessibility of κ.

Let IA be the statement that there is an inaccessible cardinal. It is fairly easy to see that IA not provable in ZFC: Let M be a model of ZFC. If M has no inaccessible cardinal, we are done. Otherwise, in M, let κ be the least inaccessible cardinal. Then V_κ^M is a model of ZFC which has no inaccessible cardinal. But even more is true:

Theorem 5.6.2. *Assuming that ZFC is consistent, it is not provable (in ZFC) that $\mathsf{con}(\mathsf{ZFC}) \implies (\mathsf{con}(\mathsf{ZFC} + IA))$.*

Proof. Suppose $\mathsf{ZFC} \vdash (\mathsf{con}(\mathsf{ZFC}) \implies (\mathsf{con}(\mathsf{ZFC} + IA)))$. Then, by monotonicity

(1) $(\mathsf{ZFC} + IA) \vdash (\mathsf{con}\,\mathsf{ZFC} \implies \mathsf{con}(\mathsf{ZFC} + IA))$.

But we have seen that

(2) $(\mathsf{ZFC} + IA) \vdash \mathsf{con}(\mathsf{ZFC})$.

Thus, by modus ponens, it follows that

(3) $(\mathsf{ZFC} + IA) \vdash \mathsf{con}(\mathsf{ZFC} + IA)$.

This means, by Gödel's Second Incompleteness Theorem for Set Theory, Theorem 5.5.22, that

(4) $\mathsf{ZFC} + IA$ *is inconsistent.*

But we assumed that $\mathsf{ZFC} \vdash (\mathsf{con}(\mathsf{ZFC}) \implies (\mathsf{con}(\mathsf{ZFC} + IA)))$, so, since ZFC is our metatheory, in particular, we have that the consistency of ZFC implies the consistency of $\mathsf{ZFC} + IA$. In other words, the inconsistency of $\mathsf{ZFC}+IA$ implies the inconsistency of ZFC. So, by (4), it follows that ZFC is inconsistent. This is a contradiction to our assumption. □

So, the existence of an inaccessible cardinal, IA, is much like the existence of an infinite set, the Infinity Axiom. Adding the axiom strengthens the theory, and hence allows it to prove new theorems, but it also has the potential for producing an inconsistent theory. However, one might argue that IA is at least a very natural axiom, since it so closely resembles the Infinity Axiom. Inaccessible cardinals are among the weakest Large Cardinal Axioms in a long hierarchy that have been considered as natural extensions of ZFC. We will explore the next step in this hierarchy after inaccessibility. In the following, we will use the concepts of closed and unbounded sets of ordinals, see Definition 2.4.11. The next definition introduces the concept of the cofinality of a limit ordinal. It is an important measure of largeness, different from cardinality, and it has many effects on cardinal arithmetic.

Definition 5.6.3. Let α be a limit ordinal. A function $f : \beta \longrightarrow \alpha$ is *cofinal* in α if $f``\beta$ is unbounded in α. The cofinality of α, $\mathrm{cf}(\alpha)$, is the least ordinal β such that there is a function $f : \beta \longrightarrow \alpha$.

Lemma 5.6.4. *Let α be a limit ordinal. Then there is function $f : \mathrm{cf}(\alpha) \longrightarrow \alpha$ that's normal (for the meaning of normality, see Observation 2.4.15).*

Proof. Exercise. □

Observation 5.6.5. *Let α be a limit ordinal.*

1. $\mathrm{cf}(\alpha) \leq \overline{\overline{\alpha}}$.

2. $\mathrm{cf}(\mathrm{cf}(\alpha)) = \mathrm{cf}(\alpha)$.

Proof. For clause (1), note that there is a function $f : \overline{\overline{\alpha}} \rightarrowtail\!\!\!\!\to \alpha$. Clearly, f is cofinal.

For clause (2), if not, then by (1), $\mathrm{cf}(\mathrm{cf}(\alpha)) < \mathrm{cf}(\alpha)$. By Lemma 5.6.4, let $f : \mathrm{cf}(\alpha) \longrightarrow \alpha$ and $g : \mathrm{cf}(\mathrm{cf}(\alpha)) \longrightarrow \mathrm{cf}(\alpha)$ be normal and cofinal. Then $f \circ g : \mathrm{cf}(\mathrm{cf}(\alpha)) \longrightarrow \alpha$ is cofinal, where $\mathrm{cf}(\mathrm{cf}(\alpha)) < \mathrm{cf}(\alpha)$, contradicting the minimality of $\mathrm{cf}(\alpha)$. □

Definition 5.6.6. A limit ordinal α is *regular* if $\mathrm{cf}(\alpha) = \alpha$. Otherwise, α is *singular*.

Observation 5.6.7. *Let α be a limit ordinal.*

1. $\mathrm{cf}(\alpha)$ *is regular.*

2. If α is regular, then α is a cardinal.

3. *If α is an infinite successor cardinal, then α is regular.*

Proof. The first point follows by clause 2 of Observation 5.6.5. The second one follows from clause 1 of that observation. For the third clause, suppose $\alpha = \beta^+$, $\beta \in \mathrm{Card}$, and suppose α were singular. Thus, $\mathrm{cf}(\alpha) \leq \beta$. Let $f : \beta \longrightarrow \alpha$ be cofinal. For every $\xi < \beta$, $f(\xi) < \beta^+$, so fix a surjection $g_\xi : \beta \twoheadrightarrow f(\xi)$. Define $h : \beta \times \beta \longrightarrow \alpha$ by $h(\xi, \zeta) = g_\xi(\zeta)$. Then $h : \beta \times \beta \twoheadrightarrow \beta^+$, a contradiction, since $\overline{\overline{\beta \times \beta}} = \beta$, as $\beta \geq \omega$. (Note that this argument used the axiom of choice). $\square$

A regular uncountable limit cardinal is also called weakly inaccessible. One cannot show in ZFC that such cardinals exist, and moreover, one cannot show that if ZFC is consistent then so is ZFC together with the assertion that there is a weakly inaccessible cardinal. The reason for this is that if κ is weakly inaccessible, then the model L_κ, an initial segment of Gödel's constructible universe, satisfies the ZFC axioms. One can then argue as in Theorem 5.6.2. We will explore in the following what goes wrong when trying to construct such cardinals.

Definition 5.6.8. Let α be a limit ordinal, or $\alpha = \infty$. $A \subseteq \alpha$ is *club* in α if A is closed and unbounded in α. If $F : \mathrm{On} \longrightarrow \mathrm{On}$ is a partial function, then an ordinal γ is *closed under F* if $F``\gamma \subseteq \gamma$.

Lemma 5.6.9. *An ordinal κ is inaccessible iff κ is uncountable, regular and closed under the function $\xi \mapsto 2^\xi$. (i.e., iff κ is an uncountable regular strong limit cardinal.)*

Proof. Recall that we defined that an uncountable cardinal κ is inaccessible if

1. Every $x \in \mathrm{V}_\kappa$ has cardinality less than κ.

2. If $u \subseteq \mathrm{V}_\kappa$ has cardinality less than κ, then $u \in \mathrm{V}_\kappa$.

Let's show that such a cardinal has the properties stated in the lemma. By definition, κ is uncountable. It is closed under $\xi \mapsto 2^\xi$, because if $\xi < \kappa$, then $\xi \subseteq \mathrm{V}_\xi$, so $\mathcal{P}(\xi) \subseteq \mathcal{P}(\mathrm{V}_\xi) = \mathrm{V}_{\xi+1}$. Since $\mathrm{V}_{\xi+1} \in \mathrm{V}_\kappa$, we have by (1) that $\overline{\overline{\mathrm{V}_{\xi+1}}} < \kappa$, and hence, $\overline{\overline{\mathcal{P}(\xi)}} = 2^\xi < \kappa$, as claimed. And κ must be regular, because otherwise, there would be an unbounded set $A \subseteq \kappa \subseteq \mathrm{V}_\kappa$ of cardinality less than κ. By (2), it would have to be that $A \in \mathrm{V}_\kappa$, which means there would have to be a $\xi < \kappa$ such that $A \in \mathrm{V}_\xi$. So $A \subseteq \mathrm{V}_\xi \cap \mathrm{On} = \xi$ (see Lemma 2.3.50), contradicting that A is unbounded in κ.

Vice versa, suppose that κ is uncountable, regular and closed under $\xi \mapsto 2^\xi$. By induction on $\xi < \kappa$, one can then show that $\overline{\overline{\mathrm{V}_\xi}} < \kappa$ - the successor step uses that $\overline{\overline{\mathrm{V}_{\xi+1}}} = 2^{\overline{\overline{\mathrm{V}_\xi}}}$, and the limit step uses that $\mathrm{V}_\lambda = \bigcup_{\xi<\lambda} \mathrm{V}_\xi$, so that $\overline{\overline{\mathrm{V}_\lambda}} \leq \overline{\overline{\lambda}} \cdot \sup_{\xi<\lambda} \overline{\overline{\mathrm{V}_\xi}}$. The supremum has to be less than κ if $\lambda < \kappa$, since for $\xi < \lambda$, $\overline{\overline{\mathrm{V}_\xi}} < \kappa$ and κ is regular. This implies then that clause 1 holds, because if $x \in \mathrm{V}_\kappa$, then $x \in \mathrm{V}_\xi$ for some $\xi < \kappa$, but then $x \subseteq \mathrm{V}_\xi$ and $\overline{\overline{\mathrm{V}_\xi}} < \kappa$, so $\overline{\overline{x}} < \kappa$. Clause 2 follows by regularity of κ: if $u \subseteq \mathrm{V}_\kappa$, then for every $x \in u$, we can let $f(x) < \kappa$ be least such that $x \in \mathrm{V}_{\alpha(x)}$. Since $\mathrm{cf}(\kappa) > \overline{\overline{u}}$, it follows that $\{\alpha(x) \mid x \in u\}$ is bounded by some $\beta < \kappa$. It follows that $u \subseteq \mathrm{V}_\beta$. $\square$

Lemma 5.6.10. *Let $F : \mathrm{On} \longrightarrow \mathrm{On}$. Then the class of α that are closed under F is a club class of ordinals.*

Proof. It is obvious that a limit of closure points of F is a closure point of F. To see unboundedness, given an ordinal α_0, we can let $\alpha_{n+1} = (\alpha_n + 1) \cup \sup_{\xi<\alpha_n} F(\xi)$, and define $\alpha_\omega = \bigcup_{n<\omega} \alpha_n$. Then $\alpha_\omega > \alpha_0$ is closed under F. $\square$

Lemma 5.6.11. *Let κ be an uncountable regular cardinal, and let $f : \kappa \longrightarrow \kappa$. Then the set of $\alpha < \kappa$ that are closed under f is club in κ.*

Proof. The argument of the proof of the previous lemma goes through. For unboundedness, we use the regularity of κ to show that $\alpha_{n+1} < \kappa$, and the fact that κ has uncountable cofinality in order to conclude that $\alpha_\omega < \kappa$. □

Consider the club class SL of $\alpha \in$ On that are closed under the function $\xi \mapsto 2^\xi$ (i.e., SL is the class of all strong limit cardinal). Any regular cardinal in S is inaccessible. Thus, we cannot prove in ZFC that S contains a regular cardinal.

Definition 5.6.12. Let α be a limit ordinal of uncountable cofinality. A set $S \subseteq \alpha$ is *stationary* if it intersects every club subset of α. This definition can be extended to $S \subseteq \infty$, but expressing that a proper class S is stationary becomes a scheme: for every class term, it contains the statement "if C is club in ∞, then $S \cap C \neq \emptyset$".

Lemma 5.6.13. *Suppose α is an ordinal of uncountable cofinality.*

1. *If $C, D \subseteq \alpha$ are club in α, then so is $C \cap D$. In fact, if $\lambda < \mathrm{cf}(\alpha)$ and $\langle C_i \mid i < \lambda\rangle$ is a sequence of club subsets of α, then $\bigcap_{i<\lambda} C_i$ is club in α.*
2. *If $S \subseteq \alpha$ is stationary and $C \subseteq \alpha$ is club, then $S \cap C$ is stationary in α.*
3. *If $A \subseteq \alpha$ is unbounded, then the set A' of limit points of A less than α is club in α.*

Proof. 1.) Let $\lambda < \mathrm{cf}(\alpha)$ and $\langle C_i \mid i < \lambda\rangle$ be a sequence of club subsets of α. It is obvious that $\bigcap_{i<\lambda} C_i$ is closed in α. To see that it is unbounded, let $\alpha_0 < \alpha$ be given. Define a strictly increasing sequence $\langle \alpha_n \mid 1 \le n \le \omega\rangle$ recursively as follows. Suppose α_n has been defined. For each $i < \lambda$, define $\beta_{n,i} = \min(C_i \setminus \alpha_n + 1)$. Since $\lambda < \mathrm{cf}(\alpha)$, it follows that $\alpha_{n+1} := \sup_{i<\lambda}(\beta_{n,i} + 1) < \alpha$. Finally, $\alpha_\omega = \sup_{n<\omega} \alpha_n < \alpha$, as $\mathrm{cf}(\alpha) > \omega$. It follows that $\alpha_\omega \in \bigcup_{i<\lambda} C_i$, since for each $i < \lambda$, $\alpha_\omega = \sup_{n<\omega} \beta_{n,i}$ is a limit point less than α of C_i.

2.) To show that $S \cap C$ is stationary in α, let D be club in α. We have to show that $(S \cap C) \cap D \neq \emptyset$. But $(S \cap C) \cap D = S \cap (C \cap D)$, and since by 1.), $C \cap D$ is club in α, the intersection $S \cap (C \cap D)$ is nonempty, as S is stationary.

3.) A' is closed, because limits of limit points of A are limit points of A. A' is unbounded, because given $\alpha_0 < \alpha$, we can enumerate the next ω many elements of A as $\langle \alpha_n \mid n < \omega\rangle$. The supremum α_ω of this sequence is then a limit point of A, and it is less than α, as $\mathrm{cf}(\alpha) > \omega$. □

It follows that the collection

$$\mathcal{C}_\alpha = \{A \subseteq \alpha \mid \exists C \subseteq \alpha(C \subseteq A \text{ and } C \text{ is club in } \alpha)\}$$

is a $\mathrm{cf}(\alpha)$-complete filter (if $\mathrm{cf}(\alpha) > \omega$ is as in the previous lemma). $\mathcal{C}_\alpha$ is called the *club filter* on α.

Definition 5.6.14. A cardinal κ is (strongly) Mahlo if it is inaccessible and the set $\{\alpha < \kappa \mid \alpha \text{ is regular}\}$ is stationary in κ. The axiom "∞ is Mahlo" is the scheme expressing that the class of regular cardinals is stationary in ∞.

Observation 5.6.15. *If κ is Mahlo, then the set of inaccessible cardinals less than κ is stationary in κ. Similarly, if ∞ is Mahlo, then the class of inaccessible cardinals in stationary.*

If κ is a regular uncountable cardinal, then the club filter has an additional closure property which turns it into a *normal* filter:

Definition 5.6.16. Let κ be a limit ordinal, and let $\vec{A} = \langle A_i \mid i < \kappa \rangle$ be a sequence of subsets of κ. Then

$$\mathop{\triangle}_{i<\kappa} A_i = \{\alpha < \kappa \mid \forall \beta < \alpha \quad \alpha \in A_\beta\}$$

is the *diagonal intersection* of $\vec{A}$.

Lemma 5.6.17 (Normality of the Club Filter)**.** *Let κ be uncountable and regular. Then $\mathcal{C}_\kappa$ is closed under diagonal intersections. In fact, if $\langle C_i \mid i < \kappa \rangle$ is a sequence of club subsets of κ, then $D = \triangle_{i<\kappa} C_i$ is club in κ.*

Proof. To see that D is unbounded in κ, let $\alpha_0 < \kappa$ be given. Let us define a sequence $\langle \alpha_n \mid 1 \le n \le \omega \rangle$ recursively by letting

$$\alpha_{n+1} = \min((\bigcap_{m<\alpha_n} C_j) \setminus (\alpha_n + 1))$$

if $n < \omega$, and setting $\alpha_\omega = \bigcup_{n<\omega} \alpha_n$. Then $\alpha_\omega > \alpha_0$, $\alpha_\omega < \kappa$, since $\mathrm{cf}(\kappa) > \omega$, and $\alpha_\omega \in D$, because α_ω is a limit ordinal of C_β whenever $\beta < \alpha_\omega$: given such a β, there is an $n < \omega$ such that $\beta < \alpha_n$. But then, for every natural number $l > n$, $\beta < \alpha_l \in C_\beta$, and $\alpha_l < \alpha_\omega$. Since C_β is closed in κ, it follows that $\alpha_\omega \in C_\beta$. This is true for every $\beta < \alpha_\omega$, so $\alpha_\omega \in D$.

To see that D is closed in κ, suppose that $\delta < \kappa$ is a limit point of D. To show that $\delta \in D$, we show that δ is a limit point (and hence a member) of C_β, for every $\beta < \delta$. So, fixing $\beta < \delta$, let $\xi < \delta$ be given. We have to find a $\gamma \in C_\beta \cap \delta$ with $\gamma > \xi$. Let $\delta' \in D \cap \delta$, $\delta' > \max(\xi, \beta)$. Then $\delta' \in C_\beta$ (by definition of D) and $\delta' > \xi$. □

This lemma has an interesting consequence.

Definition 5.6.18. Let S be a class of ordinals, and let $F : S \longrightarrow \mathrm{On}$. F is *regressive* if for all $\alpha \in S$, $F(\alpha) < \alpha$.

Lemma 5.6.19 (Fodor)**.** *Suppose $F : S \longrightarrow \kappa$ is a regressive function, where κ is uncountable and regular, and S is stationary. Then there is a stationary subset $\bar{S} \subseteq S$ such that $F{\restriction}\bar{S}$ is constant.*

Proof. If not, then for every $\alpha < \kappa$, the set $F^{-1}``\{\alpha\}$ is nonstationary. Thus, for every such $\alpha$, there is a club set $C_\alpha \subseteq \kappa$ disjoint from $F^{-1}``\{\alpha\}$. That is, C_α is club in κ and has the property that for all $\xi \in C_\alpha$, $F(\xi) \neq \alpha$. Now the set $D = \triangle_{\alpha<\kappa} C_\alpha$ is club in κ, and hence, there is a $\beta \in S \cap D$. Thus, $\beta \in C_\alpha$ for all $\alpha < \beta$. In particular, this is true for $\alpha = F(\beta)$. But then it can't be that $\beta \in C_\alpha$, since that would imply that $F(\beta) \neq \alpha$. □

Definition 5.6.20. Let $\alpha < \lambda$ be ordinals. Then

$$S^\lambda_\alpha = \{\gamma < \lambda \mid \mathrm{cf}(\gamma) = \alpha\}.$$

Lemma 5.6.21. *Let κ be an ordinal of uncountable cofinality, and let $\rho < \mathrm{cf}(\kappa)$ be regular. Then S^κ_ρ is stationary in κ.*

Proof. If $C \subseteq \kappa$ is club, then, letting f be its monotone enumeration, it follows that f is a normal function, and $\mathrm{dom}(f) \ge \mathrm{cf}(\kappa)$. Thus, $f{\restriction}\rho$ is the monotone enumeration of $C \cap f(\rho)$, which is club in $f(\rho)$. It is left to the reader to check that $\mathrm{cf}(f(\rho)) = \rho$. Thus, $f(\rho) \in S^\kappa_\rho \cap C$, showing that S^κ_ρ is stationary. □

In the following lemma, a cardinal κ is weakly Mahlo if it is regular, uncountable, and the set $\{\alpha < \kappa \mid \alpha \text{ is regular}\}$ is stationary in κ.

Lemma 5.6.22. *Let κ be a regular cardinal. The following are equivalent:*

1. *For every stationary subset $S \subseteq \kappa$, there is a regular $\rho < \kappa$ such that $S \cap S^\kappa_\rho$ is stationary.*
2. *κ is not weakly Mahlo.*

Proof. To see that clause 1 implies clause 2, let's show the contrapositive. Since κ is weakly Mahlo, $S = \{\alpha < \kappa \mid \alpha \text{ is regular}\}$ is stationary in κ. But for every regular cardinal $\rho < \kappa$, $S^\kappa_\rho \cap S = \{\rho\}$ is not stationary. So clause 1 fails.

To see that clause 2 implies clause 1: since κ is not Mahlo, there is a club $C \subseteq \kappa$ consisting of singular limit ordinals. Thus, $S_0 = S \cap C$ is a stationary set of singular limit ordinals. Now the function mapping $\xi \in S_0$ to $\mathrm{cf}(\xi)$ is regressive and hence constant on some stationary subset $\bar{S} \subseteq S_0$, by Fodor's Lemma. If ρ is the constant value, then $\bar{S} \subseteq S^\kappa_\rho$. So $\bar{S} \subseteq S \cap S^\kappa_\rho$ is stationary. □

Bibliography

[End72] Herbert B. Enderton. *A Mathematical Introduction to Logic.* Academic Press, New York, 1972.

[Jec03] Thomas Jech. *Set Theory: The Third Millenium Edition, Revised and Expanded.* Springer Monographs in Mathematics. Springer, Berlin, Heidelberg, 2003.

[Kun80] Kenneth Kunen. *Set Theory. An Introduction To Independence Proofs.* North Holland, 1980.

[Poh09] Wolfram Pohlers. *Proof Theory. The first Step into Impredicativity.* Springer, 2009.

[Sip06] Michael Sipser. *Introduction to the Theory of Computation.* Course Technology Cengage Learning, 2006.

[Soa80] Robert I. Soare. *Recursively Enumerable Sets and Degrees.* Springer, 1980.